



Citrix SD-WAN 11.4

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Notes de mise à jour de la version 11.4.0a de Citrix SD-WAN	11
Résolution des problèmes de réseau Citrix SD-WAN 110 SE	24
Notes de mise à jour pour Citrix SD-WAN version 11.4.1	25
Notes de mise à jour de la version 11.4.2a de Citrix SD-WAN	31
Notes de mise à jour de la version 11.4.2b de Citrix SD-WAN	37
Notes de mise à jour de la version 11.4.3a de Citrix SD-WAN	44
Notes de mise à jour pour Citrix SD-WAN version 11.4.4	50
Nouvelle interface utilisateur pour les appliances SD-WAN	52
Configuration système requise	84
Modèles de plates-formes SD-WAN et progiciels	85
Chemins d'accès	90
Mise à niveau du logiciel virtuel WAN vers la version 9.3.5 avec déploiement virtuel WAN	91
Mise à niveau vers la version 11.4 avec le déploiement Virtual WAN	95
Mise à niveau vers la version 11.4 sans travail de déploiement WAN virtuel	102
Réimager le logiciel de l'appliance Citrix SD-WAN	109
Mise à niveau logicielle partielle à l'aide de la gestion des changements locaux	111
Conversion WANOP vers Premium Edition avec USB	114
Convertir Standard Edition en Premium Edition	118
Utilitaire de réimageage USB	119
Options de licence Citrix SD-WAN	122
Licences locales	124
Licences distantes	124
Licences centralisées	126

Gestion des licences	130
Expiration de la licence	131
Configuration	132
Configuration initiale	134
Vue d'ensemble de la mise en page de l'interface Web	135
Configuration du matériel de l'appliance	142
Configurer l'adresse IP de gestion	143
Définir la date et l'heure	150
Expiration de session	152
Configurer les alarmes	155
Configurer la restauration	157
Configurer le nœud de contrôle maître	159
Présentation MCN	160
Passer à la console MCN	161
Configurer MCN	165
Activer et configurer la sécurité et le chiffrement du réseau étendu virtuel (facultatif)	187
Configurer le MCN secondaire	188
Gestion de la configuration MCN	190
Configuration des nœuds de succursale	202
Configurer le nœud de succursale	203
Cloner un site de succursale (Facultatif)	221
Audit de la configuration des succursales	223
Configuration du service de chemin d'accès virtuel entre le MCN et les sites clients	223
Déployer la configuration MCN	233

Exécuter la gestion des modifications MCN	234
Déployer la configuration dans les succursales	235
Démarrage One Touch	241
Connexion des appliances client à votre réseau	242
Installation des packages d'appliance SD-WAN sur les clients	244
Déployer Citrix SD-WAN Standard Edition dans OpenStack à l'aide de CloudInit	250
Configurer la fonctionnalité LTE sur l'appliance 210 SE LTE	260
Configurer la fonctionnalité LTE sur une appliance 110-LTE-WiFi	275
Configurer un modem LTE USB externe	289
Déploiements	294
Checklist et comment déployer	295
Recommandations	296
Mode passerelle	302
Mode Inline	317
Mode virtuel en ligne	323
Créer un réseau SD-WAN	339
Optimisation WAN uniquement avec l'édition Premium (Enterprise)	340
Mode deux boîtes	343
Haute disponibilité	353
Activer la haute disponibilité en mode Edge à l'aide d'un câble Y à fibre optique	362
Inscription sans contact	365
Installation locale sans intervention	387
AWS	387
Azure	399

Déploiement d'une région	419
Déploiement multi-régions	421
Guide de configuration des charges de travail Citrix Virtual Apps and Desktops	425
Système de noms de domaine	439
Serveur DHCP et relais DHCP	445
Configuration du serveur DHCP et du relais DHCP	446
Apprentissage des adresses IP de liaison WAN via le client DHCP	451
Personnalisation des fichiers PAC dynamique	456
tunnel GRE	460
Configurer les tunnels GRE pour le site MCN (facultatif)	461
Configurer les tunnels GRE pour un site de succursale	463
Gestion entrante et des sauvegardes	464
Accès Internet	475
Routage d'Internet direct à la succursale avec pare-feu intégré	476
Accès direct à Internet avec Secure Web Gateway	479
Backhauling d'Internet	480
Mode épingle à cheveux	482
Pare-feu hébergés	484
Intégration du pare-feu Palo Alto Networks sur la plate-forme SD-WAN 1100	485
Intégration du pare-feu Check Point sur la plate-forme SD-WAN 1100	508
Groupes d'agrégation de liens	524
Propagation de l'état de liaison	529
Mesure et liens WAN de secours	531
Optimisation d'Office 365	544

Optimisation des services Citrix Cloud et Gateway	557
Citrix SD-WAN Orchestrator pour la configuration locale sur l’appliance Citrix SD-WAN	563
Sessions PPPoE	572
Qualité du service	582
Classes	582
Règles par adresse IP et numéro de port	586
Règles par nom d’application	592
Ajouter des groupes de règles et activer MOS	600
Classification des demandes	602
Équité QoS (RED)	616
Files d’attente MPLS	618
Rapports	628
QoE des applications	628
QoE HDX	632
Collecteurs de flux net multiples	634
Statistiques d’itinéraire	638
Routage	640
Routage de superposition SD-WAN	641
Domaine de routage	668
Configurer le domaine de routage	669
Configurer les itinéraires	671
Utiliser l’interface de ligne de commande pour accéder au routage	672
Routage dynamique	673
OSPF	683

BGP	693
iBGP	701
eBGP	701
Itinéraire des applications	702
Filtrage d'itinéraire	707
Récapitulatif des itinéraires	712
Préférence de protocole	715
Routage multidiffusion	716
Configurer le coût de l'itinéraire du chemin virtuel	721
Configurer le protocole de redondance du routeur virtuel	724
Configurer les objets réseau	730
Prise en charge du routage pour la segmentation LAN	732
Service de domaine d'interroulage	732
Équilibrage de charge ECMP	738
Peering sécurisé	742
Peering automatique sécurisé vers une appliance PE à partir d'une appliance SD-WAN SE et WANOP autonomes sur le site DC	744
Peering automatique sécurisé lancé à partir de l'appliance PE sur le site DC et le site de succursale PE	749
Peering automatique sécurisé lancé à partir d'une appliance PE sur le site DC et la branche avec une appliance SD-WAN SE et WANOP autonomes	754
Peering manuel sécurisé lancé à partir de l'appliance PE sur le site DC et l'appliance Branch PE	759
Peering sécurisé manuel lancé à partir de l'appliance PE sur le site DC vers l'appliance SD-WAN autonome Branch et l'appliance WANOP	762
Création d'utilisateurs de jointure de domaine et de délégation	766

Sécurité	771
Terminaison du tunnel IPSec	772
Intégration de Citrix SD-WAN avec AWS Transit Gateway	772
Comment configurer les tunnels IPSec pour les chemins virtuels et dynamiques	784
Comment configurer le tunnel IPSec entre SD-WAN et des périphériques tiers	786
Comment ajouter des certificats IKE	794
Comment afficher la configuration du tunnel ipsec	795
Surveillance et journalisation IPsec	797
Éligibilité pour les routes de chemin non virtuel ipsec	800
Chiffrement nul IPsec	801
Conformité aux normes FIPS	802
Passerelle Web sécurisée Citrix SD-WAN	806
Intégration de Zscaler à l'aide des tunnels GRE et IPsec	807
Prise en charge de la redirection du trafic de pare-feu à l'aide de Forcepoint dans Citrix SD-WAN	818
Intégration de Palo Alto à l'aide de tunnels IPsec	822
Prise en charge du pare-feu avec état et NAT	828
Paramètres globaux du pare-feu	831
Paramètres avancés du pare-feu	832
Zones	834
Stratégies	837
Traduction d'adresses réseau (NAT)	843
NAT statique	843
NAT dynamique	851

Configurer le service WAN virtuel	858
Configurer la segmentation du pare-feu	861
Authentification par certificats	866
AppFlow et IPFIX	870
SNMP	881
Interface administrative	885
Publicité de routeur NDP et groupe de délégation de préfixe	891
Optimisation WAN	894
Citrix SD-WAN édition premium	895
Activer l'optimisation et configurer les paramètres de fonctionnalité par défaut	897
Configurer les paramètres de réglage par défaut de l'optimisation	901
Configurer les classificateurs d'applications par défaut d'optimisation	902
Configurer les classes de service par défaut d'optimisation	905
Configurer l'optimisation d'un site de succursale	912
Configurer les profils SSL	913
Plug-in client d'optimisation de Citrix WAN	917
Configuration matérielle et logicielle requise	918
Fonctionnement du plug-in WANOP	919
Déployer des appliances à utiliser avec des plug-ins	926
Personnaliser le fichier MSI du plug-in	930
Déployer des plug-ins sur les systèmes Windows	937
Commandes GUI du plug-in WANOP	942
Mettre à jour le plug-in WANOP	946
Résoudre les problèmes liés au plug-in WANOP	946

Connexion SMB 3.1.1	948
Comment les articles	949
Groupes d'interface	950
Configurer l'identité d'adresse IP virtuelle	951
Configurer l'interface d'accès	952
Configurer les adresses IP virtuelles	952
Configurer les tunnels GRE	953
Configuration des chemins dynamiques pour la communication de succursale à succursale	954
Surveillance et dépannage	958
Surveillance du réseau étendu virtuel	958
Affichage des informations statistiques	960
Affichage des informations de flux	962
Affichage de rapports	966
Affichage des statistiques du pare-feu	972
Diagnostics	975
Amélioration du mappage des chemins et de l'utilisation de la bande passante	992
Résolution des problèmes de gestion IP	997
Notifications HTTP basées sur la session	999
Test actif de la bande passante	1005
Détection adaptative de la bande passante	1007
Recommandations	1009
Sécurité	1009
Routage	1018
QoS	1019

Liens WAN	1019
Questions fréquentes	1021
Matériel de référence	1031

Notes de mise à jour de la version 11.4.0a de Citrix SD-WAN

November 16, 2022

Ce document de notes de mise à jour décrit les améliorations et modifications, ainsi que les problèmes résolus et connus qui existent pour Citrix SD-WAN version 11.4.0a.

Remarque

- Pour obtenir la liste des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.
- La version 11.4.0a de Citrix SD-WAN corrige les vulnérabilités de sécurité décrites dans <https://support.citrix.com/article/CTX319135> et remplace la version 11.4.0. Outre les améliorations et corrections de bogues disponibles dans la version 11.4.0, la version 11.4.0a contient les corrections de bogues suivantes : SDWANHELP-2106, SDWANHELP-2078, SDWANHELP-2066, NSSDW-35630, NSSDW-35596 et NSSDW-34670.
- La version 11.4.0 de Citrix SD-WAN est la dernière version principale qui prend entièrement en charge Citrix SD-WAN Center et l'éditeur de configuration SD-WAN. Citrix SD-WAN Center et SD-WAN Configuration Editor sont tous deux obsolètes. Notez que la dépréciation est une notification avancée de la suppression progressive de produits/fonctionnalités, mais qu'ils sont disponibles dès aujourd'hui et entièrement pris en charge. Dans la prochaine famille de versions de Citrix SD-WAN, Citrix SD-WAN Center et SD-WAN Configuration Editor seront supprimés et ne seront pas pris en charge. À leur place, Citrix vous recommande d'utiliser Citrix SD-WAN Orchestrator pour toutes vos exigences de configuration. Citrix SD-WAN Orchestrator prend en charge toutes les configurations actuellement effectuées via Citrix SD-WAN Center et l'Éditeur de configuration SD-WAN. Pour plus d'informations, consultez [Citrix SD-WAN Orchestrator Service](#) et [SD-WAN Orchestrator for On-premise](#).

Nouveautés

Les améliorations et modifications disponibles dans la version 11.4.0a.

Configuration et gestion

API NITRO Rest pour l'adresse IP statique pour les ports WAN dans la configuration de secours

À partir de la version 11.4.0 de Citrix SD-WAN, vous pouvez configurer des adresses IP statiques pour le port WAN dans la configuration de secours à l'aide des API NITRO REST. De nouveaux paramètres sont ajoutés dans l'API de configuration de secours existante.

[NSSDW-33255]

Nouvelles améliorations de l'interface utilisateur de Citrix SD-WAN

La nouvelle interface utilisateur Citrix SD-WAN inclut les améliorations suivantes :

- L'apparence de la nouvelle interface utilisateur Citrix SD-WAN est modifiée pour refléter la nouvelle couleur et la nouvelle police conformément au rebranding Citrix.
- La nouvelle interface utilisateur est activée, par défaut, sur toutes les appliances Citrix SD-WAN configurées en tant que clients.

Remarque

Le provisionnement des appliances Citrix SD-WAN en tant que MCN vous redirige vers l'interface utilisateur héritée.

- Vous pouvez afficher les détails de l'interface LAG LACP.
- Surveillance des statistiques de proxy DNS
- Surveillance des liaisons WAN SLAAC

[NSSDW-30842, NSSDW-28818, NSSDW-32030]

SNMP

Les MIB SNMP suivants sont ajoutés :

- Statistiques de l'appliance
 - Pourcentage d'UC utilisé pour l'appliance
 - Pourcentage de RAM utilisé pour l'appliance
- Tableau Statistiques de liaison WAN
 - Débit physique Max LAN vers WAN en Kbits/s pour la liaison WAN
 - Débit physique Max WAN vers LAN en Kbits/s pour la liaison WAN
 - Taux autorisé LAN vers WAN en Kbits/s pour la liaison WAN
 - Taux autorisé du WAN au réseau local, en Kbits/s pour la liaison WAN

[NSSDW-30592]

Gestion intrabande

La gestion in-band prend en charge les paires de périphériques haute disponibilité. Les appliances d'une paire haute disponibilité communiquent entre elles à l'aide d'un accès in-band.

[NSSDW-24534]

Politique NAT statique pour les services Internet et Intranet IPv6

Lors de la mise à niveau d'un dispositif exécutant Citrix SD-WAN version 11.3.1 vers la version 11.4.0, les stratégies NAT statiques existantes pour le service Internet/Intranet IPv6 doivent être mises à jour manuellement.

[NSSDW-33726]

Divers

Prise en charge des mises à niveau des correctifs pour les composants

Citrix SD-WAN Advanced Edition (AE) prend en charge le mécanisme de mise à niveau des correctifs qui permet la mise à niveau du sous-système Edge Security.

Si vous effectuez une mise à niveau à partir d'une version existante avec la sécurité Edge activée vers une version supérieure, qui inclut une version plus récente du composant de sécurité Edge, seule la parité des mises à jour du sous-système sera téléchargée et mise à niveau.

[NSSDW-26721]

Tableau de bord de SD-WAN Center

Dans le tableau de bord Citrix SD-WAN Center, le tableau de bord récapitulatif multi-région est visible lorsque jusqu'à 300 sites sont configurés.

[NSSDW-21753]

Réseau

Classes

Citrix SD-WAN affiche uniquement les classes dont le trafic circule sur les chemins virtuels et les chemins virtuels dynamiques. Si une classe est affichée et affiche 0 comme valeur, cela signifie que le trafic qui circulait précédemment est maintenant arrêté. Toutefois, si une classe n'est pas affichée du tout, cela signifie qu'il n'y a jamais eu de flux de trafic pour cette classe, car l'état du service de chemin virtuel a été réinitialisé (par exemple, mise à niveau ou redémarrage du logiciel).

[NSSDW-33974]

Prise en charge IPv6 pour IPFIX

Citrix SD-WAN prend en charge les adresses IPv6 pour IPFIX. Citrix SD-WAN utilise les modèles 615 et 616 pour exporter les données de flux IPv6 IPFIX. Vous pouvez choisir **IPFIX (Application Flow Info)** pour exporter des ensembles de données conformément au modèle 615. En cas de problèmes d'exportation des données de flux, choisissez **Propriétés de base (IPFIX)** qui exporte les données selon le modèle 616.

[NSSDW-29153]

Prise en charge IPv6 pour le proxy DNS et le redirecteur transparent DNS

Citrix SD-WAN prend en charge les adresses IPv6 pour la configuration du **proxyDNS et du transfert transparent**DNS. Vous pouvez définir le proxy DNS ou le transfert transparent DNS à l'aide des types de service DNS IPv6 suivants :

- **Staticv6** : Permet de configurer l'adresse IP du serveur DNS IPv6 statique. Vous pouvez créer interne, FAI, google ou tout autre service DNS open source. Le service DNS Staticv6 peut être configuré au niveau global et au niveau du site.
- **Dynamicv6** : permet de configurer l'adresse IP du serveur DNS IPv6 dynamique. Le service DNS Dynamicv6 peut être configuré uniquement au niveau du site. Un seul service Dynamicv6 est autorisé par site.

[NSSDW-29151]

Équilibrage de charge ECMP

Les groupes ECMP (Equal Cost Multi-Path) vous permettent de regrouper plusieurs itinéraires, avec le même coût, la destination et le même type de service. L'équilibrage de charge ECMP garantit :

- Répartition du trafic sur plusieurs connexions à coût égal.
- Utilisation optimale de la bande passante disponible.
- Transfert dynamique du trafic vers un autre itinéraire membre ECMP, si un itinéraire devient inaccessible.
- ECMP prend en charge les routes statiques sur les tunnels IPsec/GRE.
- Les groupes ECMP peuvent être formés via des chemins virtuels et des services Intranet.

[NSSDW-1238]

Plateforme et systèmes

Citrix Hypervisor 8.2

Citrix SD-WAN est pris en charge sur Citrix Hypervisor 8.2 à partir de la version 11.4.0.

[NSSDW-32037]

Catégories Office 365

Citrix SD-WAN 11.4.0 fournit une classification plus granulaire des catégories **Autoriser** et **Optimiser** Office 365, permettant la réservation sélective pour améliorer les performances du trafic Office 365 sensible au réseau. La direction du trafic sensible au réseau vers le SD-WAN dans le cloud (Cloud Direct ou un VPX SD-WAN sur Azure), ou d'un périphérique SD-WAN domestique vers un SD-WAN situé à proximité avec une connectivité Internet plus fiable, permet une qualité de service de qualité de service et une résilience de connexion supérieure par rapport à la simple direction du trafic vers le

plus proche Porte d'entrée Office 365, au prix d'une augmentation de la latence. Une solution SD-WAN avec QoS réduit les abandons et les déconnexions VoIP, réduit la gigue et améliore les scores d'opinion moyens de qualité médiatique pour Microsoft Teams.

La catégorie **Optimiser** est classée dans les sous-catégories suivantes :

- Teams Real-time
- Exchange Online
- Optimisation SharePoint

La catégorie **Autoriser** est classée dans les sous-catégories suivantes :

- Repli TCP des équipes
- Courrier Exchange
- Autoriser SharePoint
- Office365 Common

[NSSDW-27324]

[Prise en charge de Google Cloud Platform pour SD-WAN SE avec HA et débit élevé](#)

Vous pouvez désormais configurer une instance SD-WAN SE sur Google Cloud Platform (GCP) avec haute disponibilité. Une instance SD-WAN sur GCP prend également en charge un débit plus élevé de 1 Gbit/s.

[NSSDW-17179]

[Authentification filaire 802.1X](#)

Wired 802.1X est un mécanisme d'authentification qui exige que les clients s'authentifient avant de pouvoir accéder aux ressources LAN. Le service Citrix SD-WAN Orchestrator prend en charge la configuration de l'authentification 802.1X filaire sur les interfaces LAN.

Dans le réseau Citrix SD-WAN, les clients envoient des demandes d'authentification à l'appliance Citrix SD-WAN pour accéder aux ressources LAN. L'appliance Citrix SD-WAN agit en tant qu'authentificateur et envoie les demandes d'authentification au serveur d'authentification. Le service Citrix SD-WAN Orchestrator prend en charge uniquement les serveurs RADIUS à configurer en tant que serveurs d'authentification.

[NSSDW-1921]

Problèmes résolus

Les problèmes résolus dans la version 11.4.0a.

Configuration et gestion

Après l'ajout de certains objets réseau, l'audit de configuration et l'exportation échouaient. Le problème est résolu.

[SDWANHELP-2041]

L'importation d'une configuration réseau de grande taille de l'appliance Citrix SD-WAN vers Citrix SD-WAN Center a échoué, en raison des limites des ressources mémoire autorisées. Le problème est résolu.

[SDWANHELP-2034]

La notification par e-mail de Citrix SD-WAN ajoute un caractère « CR » supplémentaire dans la commande **AUTH**, ce qui entraîne la fin de la session SMTP.

[SDWANHELP-2028]

Pendant l'archivage de la base de données des grands réseaux, les enregistrements statistiques de l'appliance MCN n'étaient pas insérés dans les tables de base de données statistiques pendant quelques minutes.

[SDWANHELP-1872]

Pendant les modifications de l'interface, VRRP peut toujours utiliser les anciennes données d'interface, ce qui peut entraîner un vidage de base.

[SDWANHELP-1867]

La configuration du pare-feu hébergé sur l'interface graphique locale ne se charge pas lorsque la machine virtuelle du pare-feu est en état d'arrêt.

[SDWANHELP-1839]

Vous ne pouvez pas choisir le **réseau de gestion des sauvegardes** comme **Aucun** lors de la configuration des adresses IP virtuelles.

[SDWANHELP-1824]

Le champ **Adresse IPv4 publique** était grisé sous la section **Basic** de l'éditeur de configuration.

[SDWANHELP-1780]

Bien que l'apprentissage des adresses IP publiques soit activé sur une liaison WAN de branche, le RCN peut ne pas apprendre la nouvelle adresse IP publique et aboutit à un chemin mort si :

- Il y a une incompatibilité de version de configuration entre la branche et le RCN
- L'adresse IP publique de la liaison WAN de la branche a changé

[SDWANHELP-1580]

Lorsque le port de gestion du matériel est configuré avec DHCPv4, le passage à une adresse IPv4 statique échoue.

[NSSDW-35630]

Lorsqu'une appliance est configurée pour les adresses IPv4 DHCP et DHCP IPv6, mais que seul un serveur IPv6 DHCP est configuré sur le réseau, l'appliance continue d'attendre l'adresse IPv4 DHCP et n'est donc pas affectée à l'adresse IPv6 également.

[NSSDW-33741]

Les routes récapitulatives générées automatiquement créées pour un réseau RCN (Regional Control Node) se voient attribuer un coût de 30 000 au lieu de 65534.

[NSSDW-32629]

Les paramètres de l'appliance ne sont pas appliqués à Citrix SD-WAN lorsqu'ils sont poussés à partir de Citrix SD-WAN Center.

[NSSDW-32257]

Activer et désactiver le modem externe ne fonctionne pas à partir de l'interface utilisateur héritée.

[NSSDW-32221]

Une erreur d'audit pendant la configuration empêche les utilisateurs de configurer un service Internet sur un site, à moins que toutes les liaisons WAN ne soient configurées avec des interfaces d'accès de même type IP.

[NSSDW-32185]

Une liaison WAN configurée en tant que client DHCP entraîne une défaillance du chemin virtuel. Ce problème se produit lorsque le nom de la liaison WAN est modifié et la gestion des modifications est effectuée.

[NSSDW-32110]

Licence

Sur les plates-formes Citrix SD-WAN 110 et 210, si le port de gestion est configuré en tant que port de données, l'**ID d'hôte** peut changer après la mise à niveau vers une version plus récente. Les appliances SD-WAN utilisent la licence grâce si ce problème se produit.

[SDWANHELP-1866]

Divers

Lors du clonage d'un site avec plusieurs interfaces HA, la deuxième adresse IP de l'interface HA n'est pas clonée.

[SDWANHELP-2005]

Les journaux de l'interface graphique de Citrix SD-WAN Center consomment un espace disque excessif, ce qui entraîne une mise à niveau et une défaillance de STS.

[SDWANHELP-1960]

Lorsque vous affichez la page de connexion Citrix SD-WAN Center 11.3.0 sur un navigateur en mode plein écran, le logo Citrix et le nom du produit ne s'affichent pas correctement.

[SDWANHELP-1910]

Le rôle d'administrateur réseau a accès pour effectuer les activités spécifiques au rôle d'administrateur de sécurité qui ne doivent pas être autorisées conformément à la définition du rôle d'administrateur réseau.

[SDWANHELP-1906]

L'**importation** et l'**exportation** de configurations réseau volumineuses (lorsque la taille du fichier de configuration dépassait 16 Mo) sur Citrix SD-WAN Center échouaient.

[SDWANHELP-1787]

La notification par e-mail Centers Citrix SD-WAN ajoute un **CR** caractère supplémentaire dans la commande **AUTH**, ce qui entraîne la fin de la session SMTP.

[SDWANHELP-1736]

L'outil d'analyse de sécurité Qualys a provoqué l'utilisation par l'un des services de l'appliance Citrix SD-WAN d'une mémoire élevée, ce qui a entraîné une absence de réponse et un redémarrage de l'appliance. Le problème est résolu.

[SDWANHELP-1530]

Lorsque la licence interne des composants antivirus et anti-programme malveillant Edge Security expire, Citrix SD-WAN cesse de détecter le virus et les logiciels malveillants.

[NSSDW-35596]

Lors de la réauthentification, des valeurs négatives sont affichées pour le téléchargement et le téléchargement des données dans les rapports client Wi-Fi.

[NSSDW-31903]

Pour que Citrix SD-WAN Orchestrator gère localement les appliances SD-WAN fournies avec les logiciels 11.2.1 ou 11.2.2, vous devez mettre à niveau le logiciel de l'appliance SD-WAN vers la version 11.3.0.

[NSSDW-31612]

Réseau

Après la mise à niveau vers Citrix SD-WAN 11.3.1, le blocage MSS (Maximum Segment Size) échoue avec PPPoE lorsque la taille de l'unité de transmission maximale (MTU) est définie sur 1492 octets.

[SDWANHELP-2048]

Lorsque la gestion in-band est activée et que le serveur RADIUS est accessible via le plan de données, l'authentification Wi-Fi WPA2-Enterprise échoue.

[SDWANHELP-2032]

Les entrées liées à l'identification d'application pour les fonctionnalités de routage d'application, de QoS ou de DNS sont régulièrement ajoutées à la table de hachage First Packet Classifier (FPC). Lorsqu'une entrée obsolète est supprimée de la table, l'appliance Citrix SD-WAN peut parfois se bloquer.

[SDWANHELP-1980]

Lorsqu'un paquet reçu côté LAN ou sur un service local nécessitant une fragmentation est envoyé via LAN GRE, le service SD-WAN se bloque.

[SDWANHELP-1846]

Pour la découverte MTU de chemin, les événements de sonde MTU de chemin sont mis en file d'attente pour traitement lors d'un démarrage de minuterie. Un échec de segmentation se produit dans le cas où un événement de sonde n'est pas valide lorsque l'exécution réelle est tentée.

[SDWANHELP-1754]

Pour une route de service Internet dans un domaine de routage autre que par défaut et un chemin d'accès configuré, lorsque le chemin tombe en panne et que le site distant n'a pas configuré le domaine de routage donné, la route Internet n'est pas marquée inaccessible.

[SDWANHELP-1400]

Lorsque la configuration Citrix SD-WAN avec des routes récapitulatives est chargée, l'appliance peut se recharger en continu.

[NSSDW-34670]

Si l'appliance a une route statique configurée en tant qu'itinéraire récapitulatif et qu'il existe un autre itinéraire de préfixe identique appris dynamiquement, l'itinéraire récapitulatif ne résume pas les itinéraires.

[NSSDW-34355]

L'ajout de filtres d'importation pour supprimer des itinéraires OSPF/BGP précédemment importés peut provoquer un plantage de service.

[NSSDW-34207]

Une fois que SLAAC apprend une adresse IP et une adresse de passerelle à partir d'un routeur, sauf si l'adresse actuelle expire, SLAAC ne réapprendra pas l'IP si la passerelle change ou si nous modifions les segments réseau, même après le redémarrage de l'apppliance SD-WAN. Cela peut retarder l'obtention d'une adresse lors du déplacement des ports.

[NSSDW-33807]

Une fois que SLAAC apprend une adresse IP et une adresse de passerelle à partir d'un routeur, SLAAC ne réapprendra pas la passerelle si la passerelle change (sauf et jusqu'à ce que l'adresse actuelle expire).

Exemple :

- L'apppliance Branch apprend son IP et sa passerelle à partir de la passerelle -1.
- L'administrateur réseau décide de remplacer la passerelle -1 par une nouvelle passerelle -2. L'administrateur configure la passerelle -2 de la même manière que passerelle -1 de sorte que les annonces de routeur envoient les mêmes informations de préfixe que passerelle -1 envoyait. Cependant, la passerelle -2 a une adresse source différente de celle de passerelle -1.
- L'apppliance de branche n'apprendra pas automatiquement l'adresse IP de la passerelle -2. (sauf et jusqu'à ce que l'adresse actuelle expire)

[NSSDW-33802]

Une mise à jour de configuration peut entraîner le non-démarrage du serveur DHCP hébergé sur l'interface réseau virtuel de délégation de préfixe LAN. La délégation de préfixe n'est pas prise en charge avec Citrix SD-WAN version 11.3.1.

[NSSDW-33664]

L'activation d'un NAT statique sur un service Internet ou intranet avec NDP proxy peut amener le SD-WAN à répondre au NDP pour les adresses détenues et utilisées par d'autres hôtes du réseau.

[NSSDW-33653]

Le test de bande passante de diagnostic de site sous-couche n'est pas pris en charge dans Citrix SD-WAN 11.3.1 version.

[NSSDW-33597]

Lorsque le Service Internet est activé sur les liaisons WAN qui ont une interface d'accès IPv6, une interruption de service peut se produire après la mise à jour de la configuration.

[NSSDW-32212]

La fonctionnalité Wi-Fi ne prend pas en charge la haute disponibilité (HA) dans Citrix SD-WAN version 11.3.

[NSSDW-32197]

Le NAT dynamique peut ne pas fonctionner correctement ou provoquer une interruption de service lors de la mise à jour de la configuration s'il est utilisé à la fois pour IPv4 et IPv6 sur un service Internet avec l'équilibrage de charge Internet activé.

[NSSDW-32139]

Les modes DHCPv4 et DHCPv6 sur l'interface LTE peuvent entraîner la perte d'adresse IP du périphérique SD-WAN après les mises à jour de configuration.

[NSSDW-31998]

Plateforme et systèmes

Lorsqu'une appliance Citrix SD-WAN 4000 est mise à niveau vers la version 11.3.0, 11.3.1 ou 11.4.0, le service SD-WAN peut échouer en raison d'une situation de concurrence.

[SDWANHELP-2106]

Une validation de règle de stratégie de filtre est effectuée lors de la mise à jour de la configuration pour faire la distinction entre les règles nouvellement créées et modifiées. En raison d'une vérification de comparaison manquante pour « match_type », la plupart des connexions à Internet sont bloquées par le pare-feu en tant que « O_DENIED ».

La solution de contournement consiste à changer la règle par défaut de « Rejeter » à « Supprimer ».

[SDWANHELP-2078]

Lorsque le reporting HDX est activé et que le trafic HDX est exécuté via l'appliance Citrix SD-WAN, l'appliance Citrix SD-WAN peut parfois observer le vidage principal.

[SDWANHELP-1957]

Lorsque les informations NAT du pare-feu sont déversées à l'aide de l'interface de ligne de commande, l'appliance se bloque.

[SDWANHELP-1901]

Lorsque le transfert DSN transparent est activé, le traitement des paquets de réponse DNS volumineux peut entraîner un dépassement de pile en raison de l'absence de vérifications conditionnelles de limites appropriées. Un cas d'utilisation est lorsque le service cloud peut avoir besoin d'apprendre les adresses IP à partir du DNS pour activer la classification de la catégorie par défaut d'Office 365.

[SDWANHELP-1891]

Les règles de pare-feu autorisent la requête ping ICMP reçue sur une interface non approuvée, mais supprime la réponse ping et donc le service SD-WAN se bloque.

[SDWANHELP-1865]

Après la mise à niveau du périphérique Citrix SD-WAN vers la version 11.2.2, plusieurs périphériques VRRP agissent en tant que **maître** en raison de la taille de paquet de publicité VRRP erronée envoyée par le périphérique SD-WAN.

[SDWANHELP-1804]

Lors de la création du chemin virtuel dynamique (DVP), si le message de protocole arrive avec une valeur TOS (IP Type of Service) inattendue, cela peut entraîner un vidage principal.

[SDWANHELP-1783]

Lorsque deux adresses IP virtuelles (l'une privée et l'autre non privée) sont créées dans le même sous-réseau, un problème se produit que deux routes sont créées pour le même sous-réseau et que le sous-réseau n'est pas annoncé sur un site distant.

[SDWANHELP-1739]

Lorsque la capacité d'accès au tunnel GRE change de haut à bas, les routes du tunnel GRE éligibles au tunnel GRE ne sont pas mises à jour avec le changement d'état d'accessibilité.

[SDWANHELP-1623]

Les sessions SSH initiées à l'aide de l'interface de ligne de commande (CLI) avaient une valeur de délai d'attente codée en dur de 120 minutes. La durée plus longue de la période de délai d'attente est apparue comme si la session SSH n'était pas expiré. Le problème est résolu par l'ajout d'une nouvelle configuration dans l'interface graphique pour configurer la valeur de délai d'attente SSH (5 à 9999 minutes).

[SDWANHELP-1622]

Dans le déploiement HA Azure, les chemins SD-WAN ne s'affiche pas lorsque l'interface d'accès secondaire est configurée sur la liaison WAN.

[SDWANHELP-1578]

Certains transporteurs autorisent uniquement les sessions de données IPv6 si le protocole PDP (Packet Data Protocol) est activé pour IPv4 et (ou) IPv6.

[SDWANHELP-1777]

Problèmes connus

Les problèmes qui existent dans la version 11.4.0a.

Configuration et gestion

Si une application utilisée pour configurer une règle est obsolète, après la mise à niveau, l'interface graphique affiche la même règle sous une autre application.

[NSSDW-34618]

Si des interfaces de gestion hors bande sont connectées, le paramètre DNS peut être mis à jour uniquement à partir de l'interface utilisateur de l'appliance.

Si la gestion in-band est configurée, les paramètres DNS mis à jour à l'aide de l'interface utilisateur du matériel ne prennent pas effet. Vous pouvez mettre à jour les paramètres DNS uniquement à partir de l'interface utilisateur du service Citrix SD-WAN Orchestrator.

[NSSDW-33932]

La branche VPX passe en mode site unique, si la machine virtuelle nouvellement provisionnée est d'abord rétrogradée, puis mise à niveau vers la version sur laquelle la machine virtuelle a été provisionnée.

Solution :

Effectuez la gestion des modifications locales sur la branche concernée.

[NSSDW-29513]

Divers

Lorsque vous ajoutez un nouvel utilisateur local dans Citrix SD-WAN Center, une bannière jaune apparaît avec un message indiquant que l'accès au pare-feu passe d'Activé à ****Désactivé****.

[SDWANHELP-1737]

Les échecs d'authentification WPA3 ne sont pas signalés dans les alertes au niveau du site.

[NSSDW-32053]

Réseau

Les modifications fréquentes des tables de routage dans un site SD-WAN, ainsi que la mise à jour de la configuration ou la purge des itinéraires dynamiques, peuvent provoquer des problèmes de synchronisation de routage sur le site distant.

[SDWANHELP-2043]

Une modification de configuration apportée à une stratégie NAT dynamique de pare-feu ou à une règle de transfert de port peut entraîner un vidage de base.

[NSSDW-34603]

Plateforme et systèmes

Sur les plates-formes suivantes, lorsque le reporting HDX est activé, s'il y a une erreur d'analyse après que la connexion est classée dans HDX et démarre les statistiques, l'appliance se bloque lorsqu'il existe une nouvelle connexion HDX :

- Citrix SD-WAN 2100
- Citrix SD-WAN 4100
- Citrix SD-WAN 5100
- Citrix SD-WAN 6100

[SDWANHELP-1882]

Résolution des problèmes de réseau Citrix SD-WAN 110 SE

November 1, 2021

Cette section décrit les problèmes de connectivité réseau de l'appliance Citrix SD-WAN 110 SE, ainsi que des instructions de dépannage.

Symptôme

L'appliance Citrix SD-WAN 110 SE ne parvient pas à établir la connectivité réseau dans les conditions suivantes.

- L'appliance est gérée par SD-WAN Orchestrator et/ou mise en place par un déploiement sans intervention (ZTD).
- L'appliance est en état d'usine et les agents ZTD/SD-WAN Orchestrator ne sont pas installés.
- Le temps de l'appliance (CMOS ou matériel) est en avance sur l'heure réelle.
- L'heure de l'appliance est définie en arrière par le démon NTP avant le téléchargement/installation des agents ZTD/SD-WAN Orchestrator.

Solution

Après l'installation initiale (ou après la réinitialisation de l'unité à sa configuration d'usine d'origine), l'utilisateur final qui installe le SD-WAN 110 doit vérifier que l'appliance est correctement connectée au réseau de l'organisation. L'utilisateur final doit obtenir des instructions spécifiques à l'organisation avec l'appliance (par exemple, la tonalité sur le téléphone VoIP) pour vérifier la connectivité réseau. Si l'appliance ne se connecte pas au réseau, l'utilisateur final peut suivre les instructions ci-dessous :

1. Laissez l'appareil sous tension et attendez 30 minutes ou plus.
2. Appuyez brièvement mais fermement sur le bouton d'alimentation (1 à 2 secondes) pour l'éteindre.
3. Une fois que les voyants de l'apppliance sont tombés dans l'obscurité, appuyez de nouveau sur le bouton d'alimentation pour le rallumer. L'apppliance SD-WAN 110 redémarre et se connecte au réseau.

Notes de mise à jour pour Citrix SD-WAN version 11.4.1

November 1, 2021

Ce document de notes de mise à jour décrit les améliorations et les modifications, les problèmes résolus et connus qui existent pour Citrix SD-WAN version 11.4.1.

Remarques

Ce document de notes de mise à jour n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Améliorations et modifications disponibles dans la version 11.4.1.

Configuration et gestion

Serveur DHCP

Un agent relais est déclenché par interface virtuelle et un total de 16 serveurs DHCP peuvent être configurés par agent relais. Un maximum de 16 agents relais peuvent être configurés sur un site.

[NSSDW-34083]

Nom d'hôte utilisé comme option 12 dans les messages client DHCP

À partir de Citrix SD-WAN version 11.4.1, le nom d'hôte est identique au nom du site. Lorsque l'interface de gestion joue le rôle de client DHCP, le nom d'hôte est utilisé dans les messages du client DHCP en tant qu'option 12. À partir de Citrix SD-WAN version 11.2.3 et jusqu'à la version 11.4.1, le nom d'hôte a été défini comme **sdwan**.

[NSSDW-32523]

Plateforme et systèmes

Commandes AT

Les modèles de plate-forme Citrix SD-WAN qui prennent en charge la prise en charge LTE en exécutant des commandes AT. Les commandes AT aident à surveiller et à dépanner la configuration et l'état du modem LTE.

[NSSDW-35671]

Accès à la commande shell

Vous pouvez exécuter la `shell` commande directement, sur une console CLI SD-WAN, sans être invité à entrer les informations d'identification de connexion du compte statique CBVSSH. Cette fonctionnalité améliore la sécurité de votre appliance SD-WAN car elle supprime le mot de passe codé en dur du compte CBVSSH et le remplace à l'aide d'une méthode plus sécurisée. Cette fonctionnalité n'est prise en charge que pour les utilisateurs du compte Admin.

[NSSDW-34942]

Matériel de référence - bibliothèque de signatures d'application

La bibliothèque de signatures d'application DPI a été mise à jour.

[NSSDW-34527]

Problèmes résolus

Les problèmes qui sont résolus dans la version 11.4.1.

Configuration et gestion

Dans Citrix SD-WAN Center, les API de création de rapports pour les chemins d'accès et les chemins virtuels échouent lorsque tous les attributs sont récupérés et que l'intervalle de temps sélectionné est supérieur à une heure.

[SDWANHELP-2231]

Dans certains cas rares, les appliances Citrix SD-WAN peuvent perdre l'accès à la gestion en raison d'un problème de processus interne.

[SDWANHELP-2179]

Lors du clonage d'un site avec une interface LTE, l'interface utilisateur oblige à entrer l'adresse IP statique pour l'interface d'accès au lien WAN LTE. Lors de l'audit, la configuration est considérée comme incorrecte et les erreurs d'audit suivantes sont affichées :

EC601, EC343 et EC346

[SDWANHELP-2177]

Après chaque exportation de configuration depuis Citrix SD-WAN Center, les fichiers temporaires du **dossier tmp** n'étaient pas nettoyés.

[SDWANHELP-2057]

L'interface utilisateur Citrix SD-WAN n'affiche pas complètement la configuration du chemin d'accès sous **Configuration > Virtual WAN > Afficher la configuration > Chemins d'accès**. Seuls certains chemins sont affichés et les autres sont masqués.

[SDWANHELP-2050]

Lorsque des options TCP sont ajoutées dans une configuration HDX sur laquelle AppFlow est activé, la connexion TCP n'est pas établie.

[SDWANHELP-1741]

Lorsque le port de gestion du matériel est configuré avec DHCPv4, le passage à une adresse IPv4 statique échoue.

[NSSDW-35630]

Le problème se produit lorsque l'utilisateur a désactivé le modem et souhaite le réactiver avant que le mode de fonctionnement ne soit passé en mode de fonctionnement **Lower Power**.

Le correctif consiste à avertir l'utilisateur et à afficher le courant **Operating Mode** avant d'effectuer l'opération d'activation/de désactivation.

[NSSDW-25067]

Installation et mise à niveau

Lorsque les liaisons WAN MPLS sont configurées pour utiliser un modèle de lien WAN et activées pour le service Intranet/Internet, une erreur d'audit inattendue EC14203 se produit lors de la compilation de la configuration.

Citrix SD-WAN 11.3.1 et les versions antérieures peuvent ne pas générer d'erreur lorsque les débits autorisés de la liaison WAN sont définis sur une valeur inférieure à la bande passante réservée minimale requise pour tous les services utilisant la liaison WAN lors de la configuration des liaisons WAN MPLS avec des modèles de liaison WAN. Lors de la mise à niveau vers Citrix SD-WAN 11.3.2 ou versions ultérieures, l'erreur s'affiche. Définissez les taux autorisés de liaison WAN corrects et activez la configuration avant d'effectuer la mise à niveau.

[SDWANHELP-2134]

Divers

L'API REST de surveillance Citrix SD-WAN Center ne fonctionne pas lorsque les statistiques de liaison WAN sont interrogées.

[SDWANHELP-2274]

Lorsqu'une nouvelle configuration est importée dans Citrix SD-WAN Center, la configuration Zscaler n'est pas importée.

[SDWANHELP-2137]

Lorsque la licence interne des composants antivirus et anti-programme malveillant Edge Security expire, Citrix SD-WAN cesse de détecter le virus et les logiciels malveillants.

[NSSDW-35596]

Réseau

Lorsqu'un flux GRE possède une adresse IP source IPv4 et une adresse IP de destination IPv6, le trafic du tunnel GRE IPv4 peut être mal classé en tant que tunnel IPv6 sous **Surveillance > Flux** et être bloqué.

[SDWANHELP-2214]

Après la mise à niveau vers Citrix SD-WAN 11.3.1, le blocage MSS (Maximum Segment Size) échoue avec PPPoE lorsque la taille de l'unité de transmission maximale (MTU) est définie sur 1492 octets.

[SDWANHELP-2048]

Les modifications fréquentes des tables de routage dans un site SD-WAN, ainsi que la mise à jour de la configuration ou la purge des itinéraires dynamiques, peuvent provoquer des problèmes de synchronisation de routage sur le site distant.

[SDWANHELP-2043]

L'état du chemin de liaison WAN passe à l'état **DEAD** lorsqu'un dispositif Citrix SD-WAN ne parvient pas à détecter un nouveau port.

[SDWANHELP-1998]

Dans de rares cas, lorsqu'il y a un changement d'itinéraire dans la table de routage, le service Citrix SD-WAN est rechargé.

[NSSDW-36289]

Lorsque le traitement CRL est activé, un problème de mémoire dans la bibliothèque de cryptographie tierce peut entraîner un vidage de mémoire.

[NSSDW-35679]

Lorsque la configuration Citrix SD-WAN avec des routes récapitulatives est chargée, l'appliance peut se recharger en continu.

[NSSDW-34670]

Dans les scénarios suivants, lorsqu'un chemin virtuel statique entre deux sites est supprimé, les routes apprises sur les chemins virtuels statiques supprimés ne sont pas supprimées :

- Le chemin virtuel statique est supprimé dans le cadre d'une modification de la configuration.
- Lorsqu'un nouveau Geo-MCN devient client, les chemins virtuels statiques entre l'ancien Geo-MCN et les branches sont supprimés.

[NSSDW-34655]

Plateforme et systèmes

Le service Citrix Virtual WAN peut redémarrer lorsque le bundle STS est généré alors que les chemins virtuels dynamiques (DVP) sont en cours.

[SDWANHELP-2123]

Lorsqu'une appliance Citrix SD-WAN 4000 est mise à niveau vers la version 11.3.0, 11.3.1 ou 11.4.0, le service SD-WAN peut échouer en raison d'une situation de concurrence.

[SDWANHELP-2106]

La section **État du système** du tableau de bord de l'interface utilisateur héritée affiche le message d'erreur suivant lorsque le nom du site contient la chaîne **Terminé**.

Unable to obtain system data because the system is busy. Click Refresh to retry.

[SDWANHELP-2098]

Une validation de règle de stratégie de filtre est effectuée lors de la mise à jour de la configuration pour faire la distinction entre les règles nouvellement créées et modifiées. En raison d'une vérification de comparaison manquante pour **match_type**, la plupart des connexions à Internet sont bloquées par le pare-feu en tant que **O_DENIED**.

[SDWANHELP-2078]

Lorsque les statistiques en temps réel des itinéraires d'application sont récupérées à partir de l'SD-WAN Orchestrator ou du périphérique SD-WAN Branch, le périphérique perd sa connectivité et un plantage est observé. Cela se produit uniquement lorsque le nombre de routes d'application est supérieur à 16 (y compris les routes d'application générées automatiquement).

[SDWANHELP-2066]

Problèmes connus

Les problèmes qui existent dans la version 11.4.1.

Configuration et gestion

L'option permettant de basculer les colonnes affichées sous la page **Surveillance > Flux** ne fonctionne pas comme prévu. Malgré la sélection ou le filtrage des colonnes, le message suivant s'affiche :

`Please select at least one column.`

[SDWANHELP-2272]

Divers

Le processus de gestion des modifications de configuration de Zscaler a un délai d'expiration de deux heures. En cas d'erreur de configuration, l'ensemble du processus se bloque pendant deux heures.

[SDWANHELP-2249]

Les échecs d'authentification WPA3 ne sont pas signalés dans les alertes au niveau du site.

[NSSDW-32053]

Réseau

Dans de rares cas, si un site de branche possède l'une des liaisons WAN avec une adresse IP publique statique, la formation du chemin virtuel dynamique échoue.

Solution : redémarrez le service WAN virtuel sur le site de la succursale avec l'adresse IP publique statique.

[NSSDW-36429]

Dans la configuration BGP Citrix SD-WAN, lorsque l'ID de routeur d'un domaine de routage est modifié, le protocole de routage dynamique SD-WAN peut redémarrer.

[NSSDW-35657]

Une modification de configuration apportée à une stratégie NAT dynamique de pare-feu ou à une règle de transfert de port peut entraîner un vidage de base.

[NSSDW-34603]

Plateforme et systèmes

Le modem LTE redémarre en continu lorsque le processus proxy QMI reste dans un état défunt.

Solution : redémarrez l'appliance.

[SDWANHELP-2270]

Notes de mise à jour de la version 11.4.2a de Citrix SD-WAN

February 8, 2022

Ce document de notes de version décrit les améliorations et les modifications, les problèmes résolus et connus qui existent pour la version Citrix SD-WAN Build 11.4.2a.

Remarques

- Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.
- La version 11.4.2a de Citrix SD-WAN corrige les vulnérabilités de sécurité décrites dans <https://support.citrix.com/article/CTX330728> et remplace la version 11.4.2. En plus des améliorations et des corrections de bogues qui étaient disponibles dans la version 11.4.2, la version 11.4.2a contient les correctifs de bogues suivants : SDWANHELP-2480 et SDWANHELP-2456.

Nouveautés

Les améliorations et les modifications disponibles dans la version 11.4.2a.

Divers

Gestion intrabande

À partir de la version 11.4.2a de Citrix SD-WAN, il est obligatoire de configurer la gestion in-band sur l'appliance SD-WAN, afin d'établir la connectivité au service Citrix SD-WAN Orchestrator via un port de gestion in-band. Dans le cas contraire, l'appliance perd la connectivité au service Citrix SD-WAN Orchestrator lorsque le port de gestion n'est pas connecté et que l'adresse IP intrabande n'est pas non plus configurée.

[NSSDW-37174]

Interfaces LTE

Vous pouvez désormais configurer la liaison WAN basée sur l'interface LTE en tant que lien WAN Intranet privé à l'aide du service Citrix SD-WAN Orchestrator. Cette amélioration vous offre la flexibilité de configurer l'interface LTE en tant que lien WAN Internet public ou lien WAN intranet privé.

[NSSDW-37064]

État de connectivité d'Orchestrator

La nouvelle interface utilisateur du tableau de bord SD-WAN affiche l'état de connectivité d'Orchestrator suivant :

- État en ligne
- État du service
- État du DNS
- État de la passerelle locale
- Motif de l'échec
- Connecté via

[NSSDW-36434]

Plateforme et systèmes

Domaines et applications

Les applications basées sur le nom de domaine prennent désormais en charge les ports et le protocole configurables dans le service Citrix SD-WAN Orchestrator. Lorsque vous activez la case à cocher **Configurer le port**, vous pouvez modifier, ajouter ou supprimer n'importe quel port ou la plage de ports selon vos besoins. Vous pouvez également modifier/sélectionner le protocole en tant que TCP, UDP ou N'importe lequel. Auparavant (et avec la case à cocher **Configurer le port** désactivée), seuls les ports 80 et 443 et le protocole **Tout** étaient pris en charge pour les domaines regroupés sous une application.

[NSSDW-29930]

Problèmes résolus

Les problèmes qui sont traités dans la version 11.4.2a.

Divers

L'appliance se bloque lorsqu'une entrée apprise DNS pour une application basée sur un nom de domaine amène la première table de classification de paquets à atteindre la limite maximale.

[SDWANHELP-2480]

Lorsque le nombre de débits est constamment élevé et dépasse la limite de capacité de débit maximale d'un appareil, une modification du mappage de flux peut parfois entraîner le redémarrage du chemin de données.

[SDWANHELP-2456]

Pour un chemin non chiffré avec des balises VLAN, tels que des chemins de contrôle HA, certains paquets de contrôle SD-WAN ont été envoyés avec un en-tête Ethernet incorrect rendant les chemins instables ou morts.

[SDWANHELP-2384]

Une erreur d'audit s'affiche lors du déploiement de la MRC autonome sans aucune branche.

[SDWANHELP-2381]

Lorsque les sondes ICMP pour le service Internet sont activées à partir du service Citrix SD-WAN Orchestrator, le service SD-WAN est redémarré si la liaison WAN Internet tombe en panne, sur les appliances suivantes :

- Citrix SD-WAN 2100
- Citrix SD-WAN 4100
- Citrix SD-WAN 5100
- Citrix SD-WAN 6100

[SDWANHELP-2378]

Le tableau de bord Citrix SD-WAN Center ne charge aucune information.

[SDWANHELP-2373]

Lors de la transmission des modifications aux appliances réseau à partir du MCN via le processus de gestion des modifications, le service SD-WAN sur les appliances a redémarré la déconnexion de l'appliance pendant environ 2 minutes.

[SDWANHELP-2366]

Impossible de configurer les groupes LAG pour le modèle Citrix SD-WAN 5100.

[SDWANHELP-2339]

Impossible de télécharger le fichier PAC sur les modèles d'appliance Citrix SD-WAN prenant en charge PE.

[SDWANHELP-2336]

Lorsque le chiffrement du chemin est désactivé, un MTU élevé et une perte sont observés dans le chemin.

[SDWANHELP-2327]

Dans la configuration HA de SD-WAN Orchestrator, l'appliance de secours se bloque lorsque le logiciel de l'appliance est mis à niveau d'une version inférieure à 11.3.0 vers la version 11.4.1, 11.3.2 ou inférieure.

[SDWANHELP-2315]

On observe une augmentation progressive de la perte de paquets sur un site, qui présente des chemins virtuels morts avec d'autres sites distants, une liaison WAN configurée en mode veille et le rythme cardiaque désactivé.

[SDWANHELP-2276]

L'option permettant de basculer les colonnes affichées sous la page **Surveillance > Flux** ne fonctionne pas comme prévu. Malgré la sélection ou le filtrage des colonnes, le message suivant s'affiche :

Sélectionnez au moins une colonne.

[SDWANHELP-2272]

Le modem LTE redémarre en continu lorsque le processus proxy QMI reste dans un état défunt.

[SDWANHELP-2270]

Plusieurs demandes d'authentification pour le même utilisateur sont envoyées lorsqu'une connexion SSH au SD-WAN est établie à l'aide de l'authentification TACACS+, ce qui entraîne une journalisation excessive.

[SDWANHELP-2087]

Les notifications par e-mail ne peuvent pas être envoyées lorsque le nom du serveur SMTP est défini comme nom de domaine complet. Ce problème se produit lorsque le serveur DNS contient :

- Au moins 2 enregistrements IPv4 A pour le nom de domaine complet.
- Au moins 1 enregistrement AAAA IPv6 pour le nom de domaine complet.

[SDWANHELP-2027]

Dans de rares cas, lorsqu'il y a un changement d'itinéraire dans la table de routage, le service Citrix SD-WAN est rechargé.

[NSSDW-36289]

Lorsque le traitement CRL est activé, un problème de mémoire dans la bibliothèque de cryptographie tierce peut entraîner un vidage de mémoire.

[NSSDW-35679]

Lorsque la licence interne des composants antivirus et anti-programme malveillant Edge Security expire, Citrix SD-WAN cesse de détecter le virus et les logiciels malveillants.

[NSSDW-35596]

Lorsque la configuration Citrix SD-WAN avec des routes récapitulatives est chargée, l'apppliance peut se recharger en continu.

[NSSDW-34670]

Si l'apppliance a une route statique configurée en tant qu'itinéraire récapitulatif et qu'il existe un autre itinéraire de préfixe identique appris dynamiquement, l'itinéraire récapitulatif ne résume pas les itinéraires.

[NSSDW-34355]

L'interface utilisateur Citrix SD-WAN affiche une erreur si un nom en double est utilisé pour le proxy DNS sur le réseau.

[NSSDW-33842]

Une fois que SLAAC apprend une adresse IP et une adresse de passerelle à partir d'un routeur, sauf si l'adresse actuelle expire, SLAAC ne réapprendra pas l'IP si la passerelle change ou si nous modifions les segments réseau, même après le redémarrage de l'apppliance SD-WAN. Cela peut retarder l'obtention d'une adresse lors du déplacement des ports.

[NSSDW-33807]

Une fois que SLAAC apprend une adresse IP et une adresse de passerelle à partir d'un routeur, SLAAC ne réapprendra pas la passerelle si la passerelle change (sauf et jusqu'à ce que l'adresse actuelle expire).

Exemple :

- L'apppliance Branch apprend son IP et sa passerelle à partir de la passerelle -1.
- L'administrateur réseau décide de remplacer la passerelle -1 par une nouvelle passerelle -2. L'administrateur configure la passerelle -2 de la même manière que passerelle -1 de sorte que les annonces de routeur envoient les mêmes informations de préfixe que passerelle -1 envoyait. Cependant, la passerelle -2 a une adresse source différente de celle de passerelle -1.
- L'apppliance de branche n'apprendra pas automatiquement l'adresse IP de la passerelle -2. (sauf et jusqu'à ce que l'adresse actuelle expire)

[NSSDW-33802]

Les routes récapitulatives générées automatiquement créées pour un réseau RCN (Regional Control Node) se voient attribuer un coût de 30 000 au lieu de 65534.

[NSSDW-32629]

Les paramètres de l'apppliance ne sont pas appliqués à Citrix SD-WAN lorsqu'ils sont poussés à partir de Citrix SD-WAN Center.

[NSSDW-32257]

Problèmes connus

Les problèmes qui existent dans la version 11.4.2a.

Divers

La page **Connexions ICA** de l'interface utilisateur WANOP SD-WAN WANOP affiche une erreur et la page n'affiche aucune connexion.

[SDWANHELP-2431]

Si un dispositif utilisant un port hors bande pour le service SNMP passe au port intrabande, tous les services de gestion de l'apppliance se connectent à Internet via le port intrabande. Les demandes SNMP envoyées au port hors bande échouent.

Solution : configurez un service SNMP externe pour envoyer une demande au port intrabande en cas de défaillance du port hors bande.

[SDWANHELP-2358]

Impossible d'installer Citrix SD-WAN VPX sur l'hyperviseur VMware. Citrix SD-WAN VPX n'est pas pris en charge sur un processeur AMD Opteron (tm) ou une version antérieure du processeur AMD. Citrix SD-WAN est qualifié et recommandé sur le processeur AMD EPYC uniquement.

[SDWANHELP-2309]

Les débits de trafic affichés dans le tableau des classes de surveillance de l'interface utilisateur sont inférieurs d'environ 150 Kbits/s lorsque le trafic des types en temps réel, interactif haut, support interactif et faible classe interactive est initié en même temps.

[NSSDW-37568]

Lorsque le DNS configuré sur le port de gestion n'est pas valide ou n'est pas accessible, les appliances ne pourront pas se connecter au service SD-WAN Orchestrator en raison d'une erreur de résolution DNS, même si l'intrabande est configuré avec un proxy DNS et un service Internet

Solution : configurez un DNS valide sur le port de gestion ou effacez le DNS et laissez-le utiliser le DNS configuré par défaut (9.9.9.9).

[NSSDW-37467]

L'état de connectivité d'Orchestrator dans le nouveau tableau de bord de l'interface utilisateur est affiché comme Mauvais ou inconnu pour les appliances Citrix SD-WAN gérées via le MCN.

[NSSDW-37462]

La connectivité du service Citrix SD-WAN Orchestrator échoue lorsque le DNS fourni par un dongle LTE ou un port de gestion n'est pas accessible, même si le réseau est passé à la gestion in-band pour la connectivité.

[NSSDW-37428]

Dans de rares cas, si un site de branche possède l'une des liaisons WAN avec une adresse IP publique statique, la formation du chemin virtuel dynamique échoue.

Solution :

Redémarrez le service Virtual WAN sur le site de la succursale avec l'adresse IP publique statique.

[NSSDW-36429]

Dans la configuration BGP Citrix SD-WAN, lorsque l'ID de routeur d'un domaine de routage est modifié, le protocole de routage dynamique SD-WAN peut redémarrer.

[NSSDW-35657]

Une modification de configuration apportée à une stratégie NAT dynamique de pare-feu ou à une règle de transfert de port peut entraîner un vidage de base.

[NSSDW-34603]

Les échecs d'authentification WPA3 ne sont pas signalés dans les alertes au niveau du site.

[NSSDW-32053]

Notes de mise à jour de la version 11.4.2b de Citrix SD-WAN

June 8, 2022

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 11.4.2b de Citrix SD-WAN.

Remarques

- Ce document de notes de mise à jour n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.
- En plus des améliorations et des corrections de bogues qui étaient disponibles dans la version 11.4.2a, la version 11.4.2b contient le correctif de bogue suivant : SDWANHELP-2594.

Nouveautés

Améliorations et modifications disponibles dans Build 11.4.2b.

Interfaces LTE

Vous pouvez désormais configurer la liaison WAN basée sur l'interface LTE en tant que lien WAN Intranet privé à l'aide du service Citrix SD-WAN Orchestrator. Cette amélioration offre la flexibilité de configurer l'interface LTE en tant que lien WAN Internet public ou lien WAN Intranet privé.

[NSSDW-37064]

État de connectivité d'Orchestrator

La nouvelle interface utilisateur du tableau de bord de SD-WAN affiche l'état de connectivité d'Orchestrator suivant :

- État en ligne
- État du service
- État du DNS
- État de la passerelle locale
- Motif de l'échec
- Connecté via

[NSSDW-36434]

Paramètres de l'appliance

Le service Citrix SD-WAN Orchestrator introduit une option permettant de configurer la priorité du réseau de gestion. Vous pouvez sélectionner In-Band ou Out-of-band comme interface de gestion pour votre réseau. Cette option n'est disponible que si l'appliance SD-WAN exécute une version logicielle de la version 11.4.2 ou ultérieure.

[NSSDW-35774]

La prise en charge de la connectivité de gestion IPv6 avec SD-WAN Orchestrator pour local est disponible à partir de la version 11.4.2 du logiciel Citrix SD-WAN.

[NSSDW-35647]

Plateforme et systèmes

Les applications basées sur le nom de domaine prennent désormais en charge les ports et le protocole configurables dans le service Citrix SD-WAN Orchestrator. Lorsque vous activez la case à cocher **Configurer le port**, vous pouvez modifier, ajouter ou supprimer n'importe quel port ou la plage de ports selon vos besoins. Vous pouvez également modifier/sélectionner le protocole en tant que TCP, UDP ou N'importe lequel. Auparavant (et avec la case à cocher Configurer le port désactivée), seuls les ports 80 et 443 et le protocole **Any** étaient pris en charge pour les domaines regroupés sous une application.

[NSSDW-29930]

Problèmes résolus

Les problèmes résolus dans la version 11.4.2b.

Dans le cas d'un déploiement évolutif lors d'un changement de configuration sur un site ou une liaison WAN, le redémarrage du moteur de routage provoque l'arrêt des sessions BGP.

[SDWANHELP-2594]

L'appliance se bloque lorsqu'une entrée apprise DNS pour une application basée sur un nom de domaine amène la première table de classification de paquets à atteindre la limite maximale.

[SDWANHELP-2480]

Lorsque le nombre de flux est constamment élevé et dépasse la limite de capacité de débit maximale d'une appliance, une modification du mappage de flux peut parfois entraîner le redémarrage du chemin de données.

[SDWANHELP-2456]

Pour un chemin non chiffré avec des balises VLAN, tels que des chemins de contrôle HA, certains paquets de contrôle SD-WAN ont été envoyés avec un en-tête Ethernet incorrect rendant les chemins instables ou morts.

[SDWANHELP-2384]

Une erreur d'audit s'affiche lors du déploiement de RCN autonome sans aucune branche.

[SDWANHELP-2381]

Lorsque la sonde ICMP pour le service Internet est activée à partir du service Citrix SD-WAN Orchestrator, le service SD-WAN est redémarré si la liaison WAN Internet tombe en panne, sur les appliances suivantes :

- Citrix SD-WAN 2100
- Citrix SD-WAN 4100
- Citrix SD-WAN 5100
- Citrix SD-WAN 6100

[SDWANHELP-2378]

Le tableau de bord Citrix SD-WAN Center ne charge aucune information.

[SDWANHELP-2373]

Lors de la transmission des modifications aux appliances réseau à partir du MCN via le processus de gestion des modifications, le service SD-WAN sur les appliances a redémarré la déconnexion de l'appliance pendant environ 2 minutes.

[SDWANHELP-2366]

Impossible de configurer les groupes LAG pour le modèle Citrix SD-WAN 5100.

[SDWANHELP-2339]

Impossible de télécharger le fichier PAC sur les modèles d'apppliance Citrix SD-WAN prenant en charge PE.

[SDWANHELP-2336]

Lorsque le chiffrement du chemin est désactivé, un MTU élevé et une perte sont observés dans le chemin.

[SDWANHELP-2327]

Dans la configuration HA de SD-WAN Orchestrator, l'apppliance de secours se bloque lorsque le logiciel de l'apppliance est mis à niveau d'une version inférieure à 11.3.0 vers la version 11.4.1, 11.3.2 ou inférieure.

[SDWANHELP-2315]

On observe une augmentation progressive de la perte de paquets sur un site, qui présente des chemins virtuels morts avec d'autres sites distants, une liaison WAN configurée en mode veille et le rythme cardiaque désactivé.

[SDWANHELP-2276]

L'option permettant de basculer les colonnes affichées sous la page **Surveillance > Flux** ne fonctionne pas comme prévu. Malgré la sélection ou le filtrage des colonnes, le message suivant s'affiche :

Sélectionnez au moins une colonne.

[SDWANHELP-2272]

Le modem LTE redémarre en continu lorsque le processus proxy QMI reste dans un état défunt.

[SDWANHELP-2270]

Plusieurs demandes d'authentification pour le même utilisateur sont envoyées lorsqu'une connexion SSH au SD-WAN est établie à l'aide de l'authentification TACACS+, ce qui entraîne une journalisation excessive.

[SDWANHELP-2087]

Les notifications par e-mail ne peuvent pas être envoyées lorsque le nom du serveur SMTP est défini comme nom de domaine complet. Ce problème se produit lorsque le serveur DNS contient :

- Au moins 2 enregistrements IPv4 A pour le nom de domaine complet.
- Au moins 1 enregistrement AAAA IPv6 pour le nom de domaine complet.

[SDWANHELP-2027]

Dans la version 11.4.2 de Citrix SD-WAN, le téléchargement d'un certificat CSR signé depuis Citrix SD-WAN Orchestrator for On-premises échoue pour les fichiers portant l'extension .der.

[NSSDW-37813]

La connectivité du service Citrix SD-WAN Orchestrator échoue lorsque le DNS fourni par un dongle LTE ou un port de gestion n'est pas accessible, même si le réseau est passé à la gestion in-band pour la connectivité.

[NSSDW-37428]

Gestion intrabande

À partir de la version 11.4.2 de Citrix SD-WAN, il est obligatoire de configurer la gestion in-band sur l'appliance SD-WAN, afin d'établir la connectivité au service Citrix SD-WAN Orchestrator via un port de gestion in-band. Dans le cas contraire, l'appliance perd la connectivité au service Citrix SD-WAN Orchestrator lorsque le port de gestion n'est pas connecté et que l'adresse IP intrabande n'est pas non plus configurée.

[NSSDW-37174]

Le service Citrix SD-WAN peut se bloquer lorsque le serveur DHCP attribue une nouvelle adresse avec la configuration DVP et HA.

[NSSDW-36513]

L'interface utilisateur Citrix SD-WAN affiche une erreur si un nom en double est utilisé pour le proxy DNS sur le réseau.

[NSSDW-33842]

Plateforme et systèmes

L'ajout d'une chaîne de communauté SNMP personnalisée pour la première fois ne supprime pas la configuration de chaîne de communauté existante.

[SDWANHELP-2561]

Problèmes connus

Les problèmes qui existent dans la version 11.4.2b.

Divers

Si la mise à niveau partielle du site était désactivée, suivie d'une mise à niveau de l'ensemble du réseau vers une nouvelle version logicielle, certains sites pourraient être automatiquement corrigés vers l'ancienne version.

Solution : si une autre gestion des modifications est déclenchée, les sites rétrogradés sont mis à niveau vers la version logicielle attendue.

[SDWANHELP-2586]

L'ancienne interface graphique laisse les fichiers de session CGI dans un répertoire temporaire. Ces sessions CGI sont nettoyées pendant le démarrage, ce qui peut empêcher le service Citrix SD-WAN de s'exécuter.

Solution : Redémarrez l'appliance en appuyant sur le bouton d'alimentation pendant 4 secondes et remettez le boîtier sous tension, ou débranchez le câble d'alimentation et rebranchez-le après quelques secondes.

[SDWANHELP-2567]

Le service Citrix SD-WAN LTE peut se bloquer en raison d'erreurs de délai d'expiration de transaction du modem LTE.

Solution : redémarrez l'appliance.

[SDWANHELP-2565]

t2_app se bloque lorsque des statistiques sont demandées avec un index de base de données incorrect en raison d'une condition de concurrence rare dans l'interface utilisateur Citrix SD-WAN.

[SDWANHELP-2548]

La mémoire attribuée à la machine virtuelle Palo Alto (modèle VM-50) sur Citrix SD-WAN 1100 est augmentée à 5,5 Go.

[SDWANHELP-2534]

Une fuite de mémoire possible dans la classification ICA est corrigée.

[SDWANHELP-2527]

Le service Citrix SD-WAN peut parfois se bloquer sur la plate-forme Advanced Edition (AE) avec une configuration d'équilibrage de charge Internet.

Solution : configurez le service Internet en mode principal et secondaire.

[SDWANHELP-2521]

Les appliances Citrix SD-WAN autorisent uniquement le trafic souhaité sur le port de gestion, ce qui empêche les utilisateurs d'accéder à l'interface graphique de gestion MiRIC lorsqu'elle est activée.

[SDWANHELP-2479]

La tentative de saisie de l'**adresse IP** avec préfixe échouait aux validations des champs IP source/destination dans les **stratégies de filtrage de pare-feu**.

[SDWANHELP-2471]

Si une appliance utilisant un port hors bande pour le service SNMP passe au port in-band, tous les services de gestion de l'appliance se connectent à Internet via le port in-band. Les requêtes SNMP envoyées vers le port hors bande échouent.

Solution : configurez un service SNMP externe pour envoyer une demande au port intrabande en cas de défaillance du port hors bande.

[SDWANHELP-2358]

Dans la version 11.4.2 de Citrix SD-WAN, le téléchargement d'un certificat CSR signé depuis Citrix SD-WAN Orchestrator for On-premises échoue pour les fichiers portant l'extension .der.

Solution : le problème ne s'applique pas aux fichiers .pem. Utilisez le CSR signé .pem.

[NSSDW-37813]

Les débits de trafic affichés dans le tableau des classes de surveillance de l'interface utilisateur sont inférieurs d'environ 150 Kbits/s lorsque le trafic des types en temps réel, interactif haut, support interactif et faible classe interactive est initié en même temps.

[NSSDW-37568]

L'état de connectivité d'Orchestrator dans le nouveau tableau de bord de l'interface utilisateur est affiché comme Mauvais ou inconnu pour les appliances Citrix SD-WAN gérées via le MCN.

[NSSDW-37462]

La connectivité du service Citrix SD-WAN Orchestrator échoue lorsque le DNS fourni par un dongle LTE ou un port de gestion n'est pas accessible, même si le réseau est passé à la gestion in-band pour la connectivité.

[NSSDW-37428]

Dans de rares cas, si un site de branche possède l'une des liaisons WAN avec une adresse IP publique statique, la formation du chemin virtuel dynamique échoue.

Solution : redémarrez le service Virtual WAN sur le site de la succursale avec l'adresse IP publique statique.

[NSSDW-36429]

Dans la configuration BGP Citrix SD-WAN, lorsque l'ID de routeur d'un domaine de routage est modifié, le protocole de routage dynamique SD-WAN peut redémarrer.

[NSSDW-35657]

Une modification de configuration apportée à une stratégie NAT dynamique de pare-feu ou à une règle de transfert de port peut entraîner un vidage de base.

[NSSDW-34603]

Les échecs d'authentification WPA3 ne sont pas signalés dans les alertes au niveau du site.

[NSSDW-32053]

Plateforme et systèmes

L'ajout d'une chaîne de communauté SNMP personnalisée pour la première fois ne supprime pas la configuration de chaîne de communauté existante.

Solution : désactivez puis activez SNMP v1/v2 pour effacer la chaîne de communauté existante.

[SDWANHELP-2561]

Notes de mise à jour de la version 11.4.3a de Citrix SD-WAN

June 8, 2022

Ce document de notes de version décrit les améliorations et les modifications, les problèmes résolus et connus qui existent pour la version Citrix SD-WAN Build 11.4.3a.

Remarque

La version 11.4.3a de Citrix SD-WAN corrige les vulnérabilités de sécurité décrites dans <https://support.citrix.com/article/CTX370550> et remplace la version 11.4.3.

Nouveautés

Les améliorations et les modifications disponibles dans la version 11.4.3a.

Amélioration des journaux DHCP

L'appliance Citrix SD-WAN peut générer des journaux de serveur DHCP pour les adresses IP. Chaque fois que des adresses IP sont attribuées aux points de terminaison, des journaux sont générés. Les journaux contiennent des détails tels que l'horodatage de l'attribution de l'adresse IP et la durée du bail, l'adresse MAC, l'ID client, etc.

[NSSDW-36840]

Prise en charge de la surveillance du matériel : vous pouvez surveiller les composants matériels, tels que l'alimentation, le disque, l'état de santé et vérifier l'état via la commande **CLI** `hw_mon`. Les événements matériels graves sont enregistrés dans les événements Citrix SD-WAN.

[NSSDW-36660]

Améliorations des journaux NAT

À partir de la version 11.4.3 de Citrix SD-WAN, les journaux NAT statiques et dynamiques sont améliorés pour afficher des informations relatives aux adresses IP traduites et aux ports IP traduits. Voici les nouveaux champs introduits :

Adresse IP traduite

- **natsrc** —Adresse IP source traduite
- **natdest** - Adresse IP de destination traduite

Type de NAT

- **snat** - Lorsque snat vaut 1, cela signifie que la connexion passe par la traduction NAT source.
- **dnat** - Lorsque dnat vaut 1, cela signifie que la connexion passe par la traduction NAT de destination.

Port traduit

- **natsport** - Adresse du port source traduite
- **natdport** - Adresse du port de destination traduite

[NSSDW-34602]

Problèmes résolus

Les problèmes qui sont traités dans la version 11.4.3a.

En cas de déploiement évolutif lors d'un changement de configuration sur un site ou une liaison WAN, le redémarrage du moteur de routage provoque l'arrêt des sessions BGP.

[SDWANHELP-2594]

L'ancienne interface graphique laisse les fichiers de session CGI dans un répertoire temporaire. Ces sessions CGI sont nettoyées pendant le démarrage, ce qui peut empêcher le service Citrix SD-WAN de s'exécuter.

[SDWANHELP-2567]

Le service Citrix SD-WAN LTE peut se bloquer en raison d'erreurs de délai d'expiration de transaction du modem LTE.

[SDWANHELP-2565]

Un problème de fuite de mémoire possible est résolu lors de l'ajout d'une règle dynamique.

[SDWANHELP-2563]

t2_app se bloque lorsque des statistiques sont demandées avec un index de base de données incorrect en raison d'une condition de concurrence rare dans l'interface utilisateur Citrix SD-WAN.

[SDWANHELP-2548]

La mémoire attribuée à la machine virtuelle Palo Alto (modèle VM-50) sur Citrix SD-WAN 1100 est augmentée à 5,5 Go.

[SDWANHELP-2534]

Une fuite de mémoire possible dans la classification ICA est corrigée.

[SDWANHELP-2527]

L'appliance se bloque lorsqu'une entrée DNS apprise pour une application basée sur un nom de domaine fait que la première table de classification de paquets atteint la limite maximale.

[SDWANHELP-2480]

Les appliances Citrix SD-WAN autorisent uniquement le trafic souhaité sur le port de gestion, ce qui empêche les utilisateurs d'accéder à l'interface graphique de gestion MiRIC lorsqu'elle est activée.

[SDWANHELP-2479]

La tentative de saisie de l'**adresse IP** avec préfixe échouait aux validations des champs IP source/destination dans les **stratégies de filtrage de pare-feu**.

[SDWANHELP-2471]

Lorsque le nombre de flux est constamment élevé et dépasse la limite de capacité de débit maximale d'une appliance, une modification du mappage de flux peut parfois entraîner le redémarrage du chemin de données.

[SDWANHELP-2456]

Une fois le port de gestion abaissé/actif, l'adresse IP source de communication avec un serveur Syslog devient 169.254.200.2

[SDWANHELP-2450]

Le tableau de bord Citrix SD-WAN Center ne charge aucune information.

[SDWANHELP-2373]

Les routes statiques prennent en charge les tunnels GRE en tant que service de livraison. Les routes utilisant le service de distribution de tunnels GRE rencontrent des problèmes lorsque des tunnels GRE sont supprimés sans supprimer correctement les routes statiques au préalable.

Ce correctif supprime automatiquement les routes configurées à l'aide du tunnel GRE en tant que service de livraison lorsque les tunnels GRE sont supprimés.

[NSSDW-37846]

Dans la version 11.4.2 de Citrix SD-WAN, le téléchargement d'un certificat CSR signé depuis Citrix SD-WAN Orchestrator for On-premises échoue pour les fichiers portant l'extension .der.

[NSSDW-37813]

La fin du réseau 3G AT&T est prévue pour février 2022. Le modem Citrix SD-WAN 110 LTE est configuré sur Voice-Centric et ne prend pas en charge VoLTE après la fin de la 3G d'AT&T.

[NSSDW-37736]

La connectivité du service Citrix SD-WAN Orchestrator échoue lorsque le DNS fourni par un dongle LTE ou un port de gestion n'est pas accessible. Même si le réseau est passé à la gestion in-band pour la connectivité.

[NSSDW-37428]

Gestion intrabande

À partir de la version 11.4.2 de Citrix SD-WAN, il est obligatoire de configurer la gestion in-band sur l'appliance SD-WAN, afin d'établir la connectivité au service Citrix SD-WAN Orchestrator via un port de gestion in-band. Dans le cas contraire, l'appliance perd la connectivité au service Citrix SD-WAN Orchestrator lorsque le port de gestion n'est pas connecté et que l'adresse IP intrabande n'est pas non plus configurée.

[NSSDW-37174]

Le service Citrix SD-WAN peut se bloquer lorsque le serveur DHCP attribue une nouvelle adresse avec la configuration DVP et HA.

[NSSDW-36513]

Dans de rares cas, lorsqu'il y a un changement d'itinéraire dans la table de routage, le service Citrix SD-WAN est rechargé.

[NSSDW-36289]

Lorsque le traitement CRL est activé, un problème de mémoire dans la bibliothèque de cryptographie tierce peut entraîner un vidage de mémoire.

[NSSDW-35679]

Lorsque la licence interne des composants antivirus et anti-programme malveillant Edge Security expire, Citrix SD-WAN cesse de détecter le virus et les logiciels malveillants.

[NSSDW-35596]

Lorsque la configuration Citrix SD-WAN avec des routes récapitulatives est chargée, l'appliance peut se recharger en continu.

[NSSDW-34670]

Dans le cas où une appliance possède une route statique configurée en tant que route récapitulative et qu'une autre route préfixe identique est apprise dynamiquement, la route récapitulative ne résume pas les itinéraires.

[NSSDW-34355]

Citrix SD-WAN autorise uniquement DHCP sur les appareils haut débit mobiles, ce qui ne fonctionne pas pour les clients qui ont une attribution IP statique sur leur forfait de données.

[NSSDW-33971]

Une fois que SLAAC apprend une adresse IP et une adresse de passerelle à partir d'un routeur, sauf si l'adresse actuelle expire, SLAAC ne réapprendra pas l'IP si la passerelle change ou si nous modifions les segments réseau, même après le redémarrage de l'appliance SD-WAN. Cela peut retarder l'obtention d'une adresse lors du déplacement des ports.

[NSSDW-33807]

Une fois que SLAAC apprend une adresse IP et une adresse de passerelle à partir d'un routeur, SLAAC ne réapprendra pas la passerelle si la passerelle change (sauf et jusqu'à ce que l'adresse actuelle expire).

Exemple :

- L'appliance Branch apprend son IP et sa passerelle à partir de la passerelle -1.
- L'administrateur réseau décide de remplacer la passerelle -1 par une nouvelle passerelle -2. L'administrateur configure la passerelle -2 de la même manière que passerelle -1 de sorte que les annonces de routeur envoient les mêmes informations de préfixe que passerelle -1 envoyait. Cependant, la passerelle -2 a une adresse source différente de celle de passerelle -1.
- L'appliance de branche n'apprendra pas automatiquement l'adresse IP de la passerelle -2. (sauf et jusqu'à ce que l'adresse actuelle expire)

[NSSDW-33802]

Les routes récapitulatives générées automatiquement créées pour le réseau RCN (Regional Control Node) se voient attribuer un coût de 30 000 au lieu de 65534.

[NSSDW-32629]

Les paramètres de l'appliance ne sont pas appliqués à Citrix SD-WAN lorsqu'ils sont poussés à partir de Citrix SD-WAN Center.

[NSSDW-32257]

Les échecs d'authentification WPA3 ne sont pas signalés dans les alertes au niveau du site.

[NSSDW-32053]

Lors de la réauthentification, des valeurs négatives sont affichées pour le téléchargement et le téléchargement des données dans les rapports client Wi-Fi.

[NSSDW-31903]

Plateforme et systèmes

L'ajout d'une chaîne de communauté SNMP personnalisée pour la première fois ne supprime pas la configuration de chaîne de communauté existante.

[SDWANHELP-2561]

Problèmes connus

Les problèmes qui existent dans la version 11.4.3a.

Si la mise à niveau partielle du site était désactivée, suivie d'une mise à niveau de l'ensemble du réseau vers une nouvelle version logicielle, certains sites pourraient être automatiquement corrigés vers l'ancienne version.

Solution : si une autre gestion des modifications est déclenchée, les sites rétrogradés sont mis à niveau vers la version logicielle attendue.

[SDWANHELP-2586]

Le service Citrix SD-WAN peut parfois se bloquer sur la plate-forme Advanced Edition (AE) avec une configuration d'équilibrage de charge Internet.

Solution : configurez le service Internet en mode principal et secondaire.

[SDWANHELP-2521]

Si une appliance utilisant un port hors bande pour le service SNMP passe au port in-band, tous les services de gestion de l'appliance se connectent à Internet via le port in-band. Les requêtes SNMP envoyées vers le port hors bande échouent.

Solution : configurez un service SNMP externe pour envoyer une demande au port intrabande en cas de défaillance du port hors bande.

[SDWANHELP-2358]

Dans VPX, sans licence valide, le démon est redémarré automatiquement. Dans ce cas, le démon peut parfois se planter. Il n'y a aucun impact sur l'utilisateur car le démon fonctionne correctement automatiquement.

[NSSDW-37981]

Les débits de trafic affichés dans le tableau des classes de surveillance de l'interface utilisateur sont inférieurs d'environ 150 Kbits/s lorsque le trafic des types en temps réel, interactif haut, support interactif et faible classe interactive est initié en même temps.

[NSSDW-37568]

L'état de connectivité d'Orchestrator dans le nouveau tableau de bord de l'interface utilisateur est affiché comme Mauvais ou inconnu pour les appliances Citrix SD-WAN gérées via le MCN.

[NSSDW-37462]

Dans de rares cas, si un site de branche possède l'une des liaisons WAN avec une adresse IP publique statique, la formation du chemin virtuel dynamique échoue.

Solution :

Redémarrez le service Virtual WAN sur le site de la succursale avec l'adresse IP publique statique.

[NSSDW-36429]

Dans la configuration BGP Citrix SD-WAN, lorsque l'ID de routeur d'un domaine de routage est modifié, le protocole de routage dynamique SD-WAN peut redémarrer.

[NSSDW-35657]

Une modification de configuration apportée à une stratégie NAT dynamique de pare-feu ou à une règle de transfert de port peut entraîner un vidage de base.

[NSSDW-34603]

Lorsque l'utilisateur sélectionne pour afficher l'état du modem interne, l'interface utilisateur héritée affiche également l'état du modem externe.

[NSSDW-32219]

Notes de mise à jour pour Citrix SD-WAN version 11.4.4

June 18, 2024

Ces notes de publication décrivent les améliorations et les modifications, les problèmes résolus et connus qui existent pour la version Citrix SD-WAN Build 11.4.4.

Remarque

La version 11.4.4 de Citrix SD-WAN corrige les vulnérabilités de sécurité décrites dans <https://support.citrix.com/article/CTX617071>.

Nouveautés

Les améliorations et modifications disponibles dans la version 11.4.4.

Délai d'expiration par défaut fixé à 5 minutes

L'expiration du délai de session GUI/CLI par défaut des appliances Citrix SD-WAN est définie sur 5 minutes. Ce paramètre réduit le risque d'accès non autorisé aux appliances Citrix SD-WAN.

[NSSDW-36840]

Problèmes résolus

Les problèmes résolus dans la version 11.4.4.

Parfois, les appliances Citrix SD-WAN utilisent un tunnel GRE incorrect pour acheminer le trafic du centre de données.

[SDWANHELP-2488]

Dans certains cas, les utilisateurs peuvent rencontrer un retard dans le flux de trafic entre deux succursales. Ce problème se produit lorsque le chemin virtuel dynamique (DVP, Dynamic Virtual Path) est activé pour la communication de succursale à succursale, qu'une succursale utilise DVP et que l'autre succursale utilise MCN pour acheminer le trafic.

[SDWANHELP-2637, SDWANHELP-2749]

Dans certains cas, les appliances Citrix SD-WAN peuvent redémarrer brusquement si NetFlow et AppFlow sont activés avec plusieurs liaisons WAN.

[SDWANHELP-2745]

Dans certains cas, le nettoyage automatique de la base de données Citrix SD-WAN Center est interrompu en raison de dates de début et de fin de statistiques incorrectes.

[SDWANHELP-2751]

Les appliances Citrix SD-WAN peuvent redémarrer brusquement si la mise à jour de la configuration est effectuée pendant une charge élevée.

[SDWANHELP-2760]

La section « Site QoE » du tableau de bord Citrix SD-WAN Center ne charge pas les statistiques, car elle ne valide pas la plage de dates sélectionnée.

[SDWANHELP-2772]

Le tableau de bord Citrix SD-WAN n'affiche pas les données de temps d'activité précises si le temps d'activité remonte à plus d'un mois.

[SDWANHELP-2856]

L'appel de l'API REST du pare-feu Citrix SD-WAN pour modifier l'objet « firewall_dynamic_nat_policy » ne fonctionne pas si la stratégie NAT est configurée pour un service Internet.

[SDWANHELP-2862]

La page **Configuration > Zero Touch Deployment** sur Citrix SD-WAN Center est inaccessible lorsque les utilisateurs se connectent à Citrix Cloud à l'aide de Citrix SD-WAN Center pour la première fois.

[SDWANHELP-2923]

Problèmes connus

Les problèmes qui existent dans la version 11.4.4.

Dans certains cas, les appliances Citrix SD-WAN 2100 se bloquent en raison d'un problème lié à la bibliothèque DPDK. Ce problème se produit lorsque les appliances Citrix SD-WAN sont configurées avec des groupes d'agrégation de liens (LAG, Link Aggregation Group) et que LACP est activé.

Solution : désactivez le LAG avec LACP.

[NSSDW-38568]

Nouvelle interface utilisateur pour les appliances SD-WAN

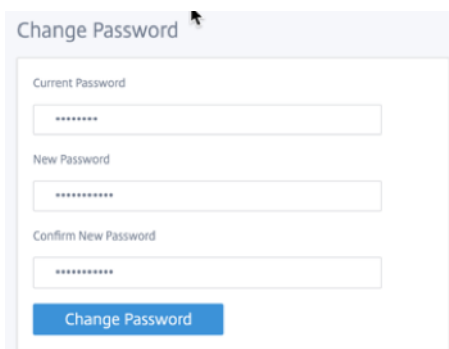
February 8, 2022

Une nouvelle interface utilisateur (UI) est introduite pour les appliances SD-WAN. La nouvelle interface utilisateur est construite en utilisant les dernières technologies d'interface utilisateur. La nouvelle conception de l'interface utilisateur améliore la sécurité, a un aspect et une sensation améliorés, il est plus performant, sécurisé et réactif. Mais la nouvelle interface utilisateur a conservé le flux et la mise en page de chaque entité de l'interface utilisateur héritée.

À partir de la version 11.4 de Citrix SD-WAN, la nouvelle interface utilisateur est activée, par défaut, sur toutes les appliances Citrix SD-WAN configurées en tant que clients.

Remarque

- Le provisionnement des appliances Citrix SD-WAN en tant que MCN vous redirige vers l'interface utilisateur héritée.
- Tous les utilisateurs locaux disposant d'un rôle d'administrateur et les utilisateurs d'administration distants peuvent accéder à la nouvelle interface utilisateur. Les comptes d'utilisateurs distants sont authentifiés via les serveurs d'authentification RADIUS ou TACACS+. Il est obligatoire de modifier le mot de passe du compte d'utilisateur administrateur par défaut lors du Provisioning de l'appliance SD-WAN. Le mot de passe par défaut est le numéro de série de l'appliance SD-WAN et doit être modifié la première fois après la connexion au périphérique.



L'interface utilisateur héritée est maintenue à des fins de compatibilité ascendante et est obsolète. L'interface utilisateur héritée est accessible à l'aide de l'URL **https : ///cgi-bin/login.cgi.< ip-address >** Le nom d'utilisateur et le mot de passe de l'**administrateur** utilisateur restent les mêmes sur les deux interfaces utilisateur (nouvelles/héritées), et les procédures de connexion pour la première fois peuvent être effectuées à l'aide de l'une ou l'autre interface. Les utilisateurs supplémentaires seront pris en charge dans les futures versions de la nouvelle interface utilisateur.

Nouvelle interface utilisateur Citrix SD-WAN

La nouvelle interface utilisateur est accessible à l'aide des navigateurs Google Chrome (version 81), Mozilla Firefox, Microsoft Edge (version 81+) et Microsoft Edge hérités (version 44+).

REMARQUE

Microsoft Internet Explorer, Apple Safari et d'autres navigateurs ne sont pas pris en charge.

Pour accéder à la nouvelle page de l'interface utilisateur, effectuez les opérations suivantes :

1. Ouvrez un nouvel onglet de navigateur et accédez à **https :// < management-ip >** pour accéder à la nouvelle interface utilisateur de l'appliance SD-WAN. Si vous accédez à une adresse IPv6, entrez **https ://<[IPv6 address]>**.

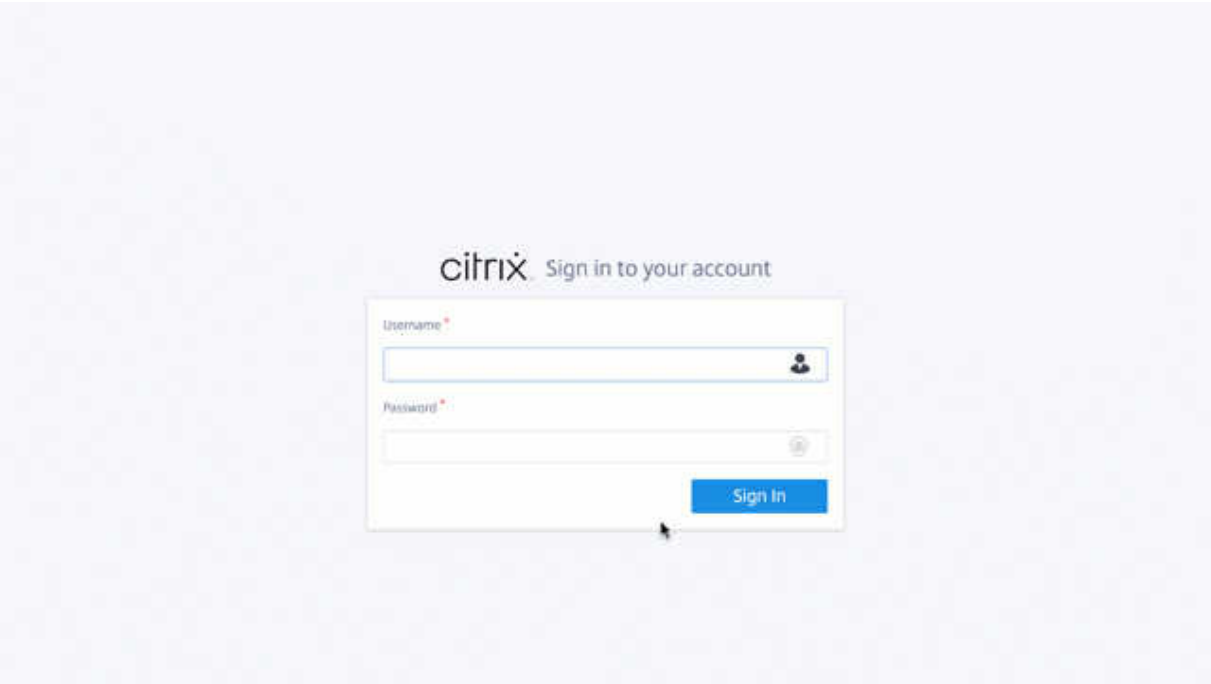
Exemple : **https :// [fd73:xxxx:yyyy:26::9]**

Remarque

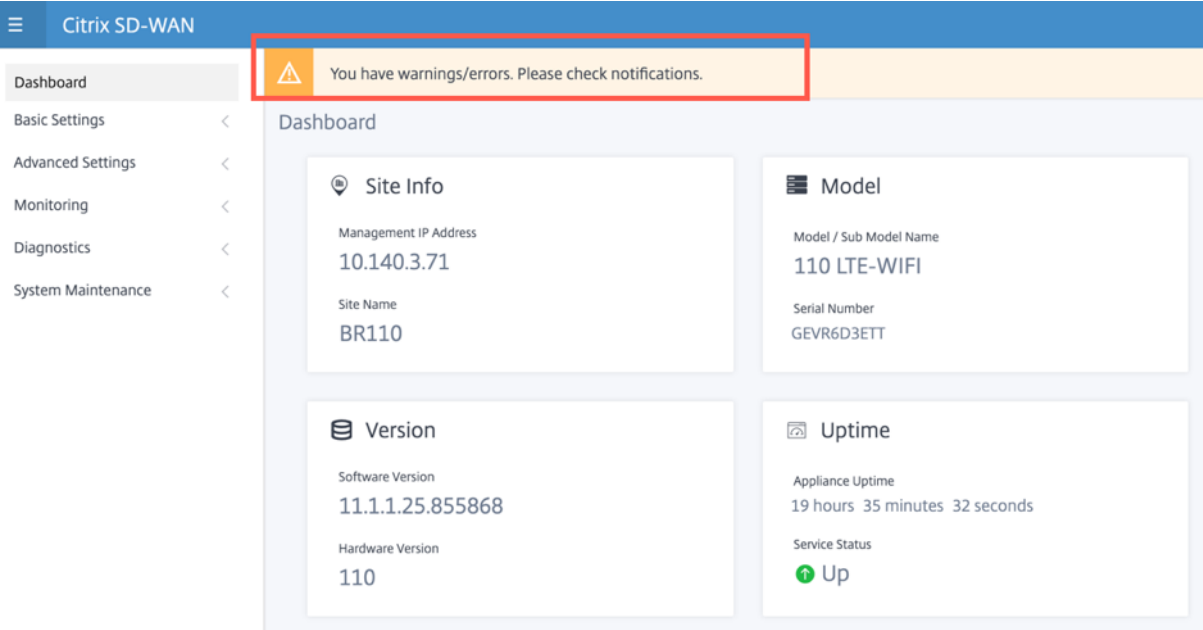
Dans le scénario où la gestion in-band est activée, l'adresse IP de l'interface peut être fournie dans **** < management-ip >** pour accéder à la nouvelle interface utilisateur. La gestion In-band peut être activée sur plusieurs interfaces de confiance qui sont activées pour être utilisées pour les services IP. Vous pouvez accéder à l'interface utilisateur à l'aide de l'adresse IP de gestion et des adresses IP virtuelles in-band.

1. Indiquez le nom d'utilisateur et le mot de passe. Cliquez sur **Sign In**.

La page de l'interface utilisateur Citrix SD-WAN s'affiche.



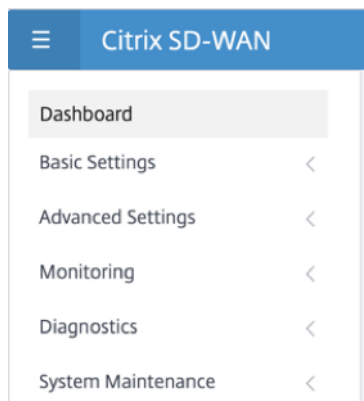
Une fois que vous êtes connecté, vous pouvez voir que le panneau de navigation se trouve sur le côté gauche. En outre, vous pouvez voir une bannière de notifications sur le tableau de bord s’il y a des avertissements ou des erreurs.



Navigation

La barre latérale de navigation gauche peut être masquée ou rendue visible en cliquant sur l’icône de hamburger. L’icône de hamburger dans le coin supérieur gauche fournit des liens vers le tableau de

bord, les paramètres **basiques/avancés**, la surveillance et les options liées à la gestion.



Barre de menus

Le menu utilisateur en haut à droite affiche les détails de l'utilisateur connecté. Vous pouvez ouvrir l'interface utilisateur héritée dans un nouvel onglet de navigateur en cliquant sur l'option **Ouvrir l'interface utilisateur SD-WAN héritée**. Cliquez sur l'icône de la cloche pour toute notification.

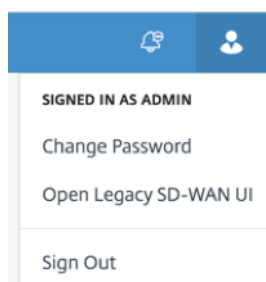
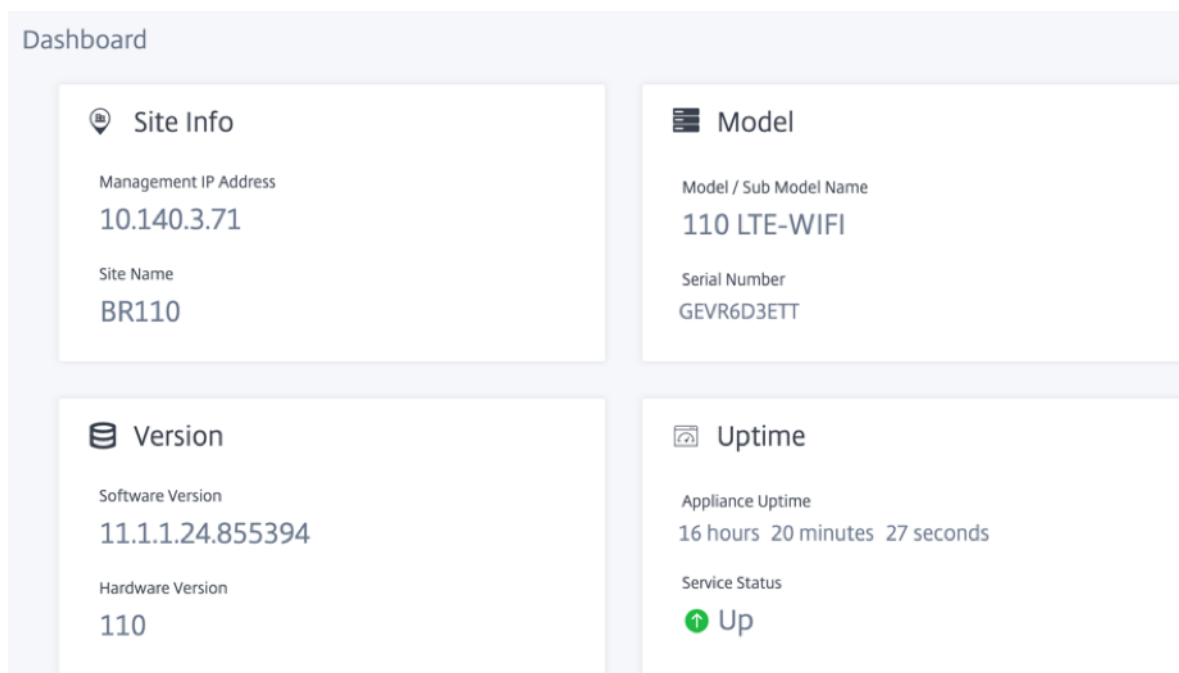


Tableau de bord

La page **Tableau de bord** affiche les informations de base suivantes de l'appliance SD-WAN sous forme de vignette :

- **Site** —Affiche les informations du site avec l'**adresse IP de gestion** et le **nom du site**
- **Modèle** —Affiche le **nom du modèle/du sous-modèle** et le **numéro de série**
- **Version** —Affiche la version **logicielle** et **matérielle**
- **Uptime** - Affiche le **temps de disponibilité de l'appliance**, l'état du **service Citrix Virtual WAN** et l'état de **connectivité Orchestrator**.
- **Haute disponibilité** : affiche l'état HA local et homologue de l'appliance ainsi que l'heure de réception de la dernière mise à jour HA.

- **Liens mesurés** —Affiche l'utilisation et les détails de facturation des liens sur lesquels la mesure est activée.
- **Connectivité Orchestrator** : affiche l'état de connectivité de l'appliance avec le service Citrix SD-WAN Orchestrator. Les informations d'état suivantes s'affichent :
 - **État en ligne** : indique l'état de la connexion entre l'appliance et le service Citrix SD-WAN Orchestrator. Des signaux de pulsation périodiques sont envoyés par l'appliance au service Citrix SD-WAN Orchestrator pour identifier l'état de la connexion comme bon ou mauvais.
 - **État du service**- Indique l'accessibilité https de l'appliance à tous les services SD-WAN Orchestrator requis tels que le téléchargement, l'accueil, la journalisation, les statistiques. Si l'état du service est mauvais, cela signifie que la connexion est établie mais que tous les services ou certains ne sont pas accessibles. Le nom du service inaccessible s'affiche.
 - **État DNS**- Indique l'état de résolution DNS des noms de domaine complets. Si l'état DNS est mauvais, cela signifie que la résolution DNS de l'un des noms de domaine complets échoue. Le nom du nom de domaine complet non résolu s'affiche.
 - **État de la passerelle locale** : indique l'état de la passerelle par défaut. Pour une connexion hors bande, l'état de la passerelle est déterminé en envoyant un ping à la passerelle par défaut. Pour une connexion In-Band, l'état de la passerelle est déterminé en envoyant un ping à l'adresse IP de l'interface Ethernet intrabande.
 - **Connecté via** : indique comment l'appliance atteint le service Citrix SD-WAN Orchestrator. Soit via Out-Band, qui est la configuration par défaut, soit via In-Band, si la gestion in-band est configurée.
 - **Raison de l'échec** : Raison de l'échec lors de la connexion au service SD-WAN Orchestrator.



Paramètres de base

Les **paramètres de base** du dispositif SD-WAN incluent la configuration des entités suivantes. La nouvelle interface utilisateur fournit une page distincte pour configurer chaque entité individuellement.

- Gestion et DNS
- Paramètres de l'interface
- Groupe LAG LACP
- Date et heure
- Serveur RADIUS
- Serveur TACACS+

Gestion et DNS

À partir de la page **Gestion et DNS**, vous pouvez configurer l'adresse IP de l'interface de gestion et les paramètres DNS. Pour plus d'informations, consultez la section [Configurer l'adresse IP de gestion](#).

La liste d'autorisation de l'interface de gestion est une liste approuvée d'adresses IP ou de domaines IP autorisés à accéder à votre interface de gestion. Une liste vide permet d'accéder à l'interface de gestion depuis tous les réseaux. Vous pouvez ajouter des adresses IP pour vous assurer que l'adresse IP de gestion est accessible uniquement par les réseaux approuvés.

Pour ajouter ou supprimer une adresse IPv4 à la liste autorisée, vous devez accéder à l'interface de gestion de l'appliance SD-WAN à l'aide d'une adresse IPv4 uniquement. De même, pour ajouter ou supprimer une adresse IPv6 à la liste autorisée, vous devez accéder à l'interface de gestion du matériel SD-WAN à l'aide d'une adresse IPv6 uniquement

The screenshot shows the Citrix SD-WAN management interface. The left sidebar has a menu with the following items: Dashboard, Basic Settings (with a dropdown arrow), Management & DNS (highlighted), Interface Settings, Date & Time, Advanced Settings (with a left arrow), Monitoring (with a left arrow), Diagnostics (with a left arrow), and System Maintenance (with a left arrow). The main content area is titled 'Network Adapters'. It contains three sections: 1. 'Management Interface IP' with a checkbox for 'Enable DHCP' (checked), and three input fields for 'IP Address', 'Subnet Mask', and 'Gateway IP Address', each with a 'Generate' button. 2. 'DNS Settings' with input fields for 'Primary DNS' and 'Secondary DNS', and a 'Clear' button. 3. 'Current DNS' showing the current 'Primary DNS' and 'Secondary DNS' values. A blue 'Save' button is at the bottom of the main content area.

Entrez l'**adresse IP**, le **masque de sous-réseau** et l'**adresse IP de la passerelle** de l'appliance que vous souhaitez configurer. Sous la section **Paramètres DNS**, indiquez les détails du serveur DNS principal et secondaire, puis cliquez sur **Enregistrer**.

Paramètres de l'interface

La page **Paramètres de l'interface** affiche les données de configuration du port Ethernet. Les ports en panne sont indiqués comme un point rouge par rapport à l'adresse MAC.

☰

Citrix SD-WAN

Dashboard
Basic Settings
Management & DNS
Interface Settings
Date & Time
Advanced Settings
Monitoring
Diagnostics
System Maintenance

Ethernet Interface Settings

Interface		MAC Address	Autonegotiate	Speed	Duplex
1/4-MGMT	●	08:35:71:11:bf:1f	<input checked="" type="checkbox"/>	100Mb/s	Full
1/1	●	08:35:71:11:bf:1c	<input checked="" type="checkbox"/>	Unknown	Half
1/2	●	08:35:71:11:bf:1d	<input checked="" type="checkbox"/>	1000Mb/s	Full
1/3	●	08:35:71:11:bf:1e	<input type="checkbox"/>	100Mb/s	Full
LAG0	●	Device not configured	<input checked="" type="checkbox"/>	Unknown	Unknown
LAG1	●	Device not configured	<input checked="" type="checkbox"/>	Unknown	Unknown

Save

Groupe LAG LACP

La fonctionnalité de groupes d'agrégation de liens (LAG) vous permet de regrouper deux ports ou plus de votre appliance SD-WAN afin qu'ils fonctionnent ensemble comme un seul port. Cela garantit une disponibilité accrue, une redondance de liaison et des performances améliorées.

Auparavant, seul le mode Active-Backup était pris en charge dans LAG. À partir de la version 11.3 de Citrix SD-WAN, les négociations basées sur le protocole LACP (Link Aggregation Control Protocol) 802.3AD sont prises en charge. Le LACP est un protocole standard et fournit plus de fonctionnalités pour les LAG.

En mode de sauvegarde active, à tout moment, un seul port est actif et les autres ports sont en mode sauvegarde. Les supports actifs et de sauvegarde s'appuient sur le package Data Plane Development Kit (DPDK) pour la fonctionnalité LAG.

Avec le LACP, vous pouvez envoyer le trafic à travers tous les ports simultanément. En tant qu'avantage, vous obtenez plus de bande passante avec le mécanisme de redondance des liens. L'implémentation LACP prend en charge le mode Active-Active. Maintenant, avec le mode Active-Sauvegarde, vous pouvez également sélectionner le mode ACTIF-actif LACP complet à partir de l'interface utilisateur SD-WAN.

La fonctionnalité LAG est disponible uniquement sur les plates-formes prises en charge par DPDK suivantes :

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE

- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100 et 5100 SE
- Citrix SD-WAN 6100 SE

Remarque

La fonctionnalité LAG n'est pas prise en charge sur les plates-formes VPX/VPXL.

Vous pouvez créer un maximum de 4 LAG avec un maximum de 4 ports regroupés dans chaque LAG sur les appliances Citrix SD-WAN.

Pour les appliances Citrix SD-WAN 210 et 410, un maximum de 3 LAG et pour l'appliance Citrix SD-WAN 110, un maximum de 2 LAG peuvent être créés.

Vous pouvez créer un LAG à l'aide de l'[interface utilisateur héritée](#) ou du [SD-WAN Orchestrator](#) uniquement. Dans la nouvelle interface utilisateur, vous ne pouvez afficher que les détails du LAG créé.

Pour afficher les détails du LAG, accédez à **Paramètres de base > Groupe LAG LACP**.

Vous pouvez afficher les détails du LAG LACP tels que l'état actuel, le système et les priorités de port des ports actifs et partenaires.

LAG0							
NAME	SELECTION	STATE	SYSTEM PRIORI...	PORT PRIORITY	PARTNER STATE	PARTNER SYST...	PARTNER PORT ...
1/1	Selected	ACT AGG SY...	65535	65280	AGG SYNC C...	128	128
1/4	Selected	ACT AGG SY...	65535	65280	AGG SYNC C...	128	128

LAG1							
NAME	SELECTION	STATE	SYSTEM PRIORI...	PORT PRIORITY	PARTNER STATE	PARTNER SYST...	PARTNER PORT ...
1/7	N/A	Inactive	N/A	N/A	N/A	N/A	N/A
1/8	N/A	Inactive	N/A	N/A	N/A	N/A	N/A

Date et heure

À partir de la page Paramètres de la **date et de l'heure**, vous devez définir la date et l'heure sur l'appliance. Pour plus d'informations, consultez la section [Définition de la date et de l'heure](#).

The screenshot displays the Citrix SD-WAN configuration interface. On the left is a navigation menu with options: Dashboard, Basic Settings (expanded), Management & DNS, Interface Settings, Date & Time, Advanced Settings, Monitoring, Diagnostics, and System Maintenance. The main panel is titled 'Date/Time Settings' and contains three sections: 1. A warning message: 'If the Appliance date/time is turned back due to NTP or manual changes, reporting artifacts may occur.' 2. 'NTP Settings' section with a checked 'Use NTP Server' checkbox and a 'Server Address' field containing '0.pool.ntp.org:1.pool.ntp.org:2.pool.ntp.org:3.pool.ntp.org'. 3. 'Date/Time Settings' section with a date/time field showing 'May 6, 2020 1:55 PM'. 4. 'Timezone Settings' section with a warning message about the need for a reboot after changing the timezone, a 'Timezone' dropdown menu set to 'UTC', and a 'Save' button.

Serveur RADIUS

Vous pouvez configurer une appliance SD-WAN pour authentifier l'accès utilisateur avec un ou plusieurs serveurs RADIUS.

Pour configurer le serveur RADIUS :

1. Activez la case à cocher **Activer RADIUS**.
2. Entrez l'**adresse IP du serveur** et le **port d'authentification**. Un maximum de trois adresses IP de serveur peut être configuré.

REMARQUE

Pour configurer une adresse IPv6, assurez-vous que le serveur RADIUS est également configuré avec une adresse IPv6.

3. Entrez la **clé du serveur** et confirmez.
4. Entrez la valeur **Délai** d'attente en secondes.
5. Cliquez sur **Save**.

Vous pouvez également tester la connexion au serveur RADIUS. Entrez le **nom d'utilisateur et le mot de passe**. Cliquez sur **Vérifier**.

RADIUS Server

Server Settings

☒ Enable RADIUS

Server 1 IP Address *

Authentication Port

Server 2 IP Address

Authentication Port

Server 3 IP Address

Authentication Port

Server Key

Confirm Server Key

Timeout(seconds)

Test RADIUS Server Connection

User Name

Password

Serveur TACACS+

Vous pouvez configurer un serveur TACACS+ pour l'authentification. Comme pour l'authentification RADIUS, TACACS+ utilise une clé secrète, une adresse IP et le numéro de port. Le numéro de port par défaut est 49.

Pour configurer le serveur TACACS+ :

1. Activez la case à cocher **Activer TACACS+**.
2. Entrez l'**adresse IP du serveur** et le **port d'authentification**. Un maximum de trois adresses IP de serveur peut être configuré.

REMARQUE

Pour configurer une adresse IPv6, assurez-vous que le serveur TACACS+ est également configuré avec une adresse IPv6.

3. Sélectionnez **PAP** ou **ASCII** comme Type d'authentification.
 - PAP : utilise le protocole PAP (Password Authentication Protocol) pour renforcer l'authentification des utilisateurs en attribuant un secret partagé fort au serveur TACACS+.
 - ASCII : utilise le jeu de caractères ASCII pour renforcer l'authentification des utilisateurs en attribuant un secret partagé fort au serveur TACACS+.
4. Entrez la **clé du serveur** et confirmez.
5. Entrez la valeur **Délai** d'attente en secondes.
6. Cliquez sur **Save**.

Vous pouvez également tester la connexion au serveur TACACS+. Entrez le **nom d'utilisateur et le mot de passe**. Cliquez sur **Vérifier**.

TACACS+ Server

Settings

☒ Enable TACACS+

Server 1 IP Address *	Authentication Port
<input type="text"/>	<input type="text" value="49"/>
Server 2 IP Address	Authentication Port
<input type="text"/>	<input type="text"/>
Server 3 IP Address	Authentication Port
<input type="text"/>	<input type="text"/>

Authentication Type ☐ PAP ☒ ASCII

Server Key

Confirm Server Key

Timeout(seconds)

Save

Test TACACS+ Server Connection

User Name

Password

Verify

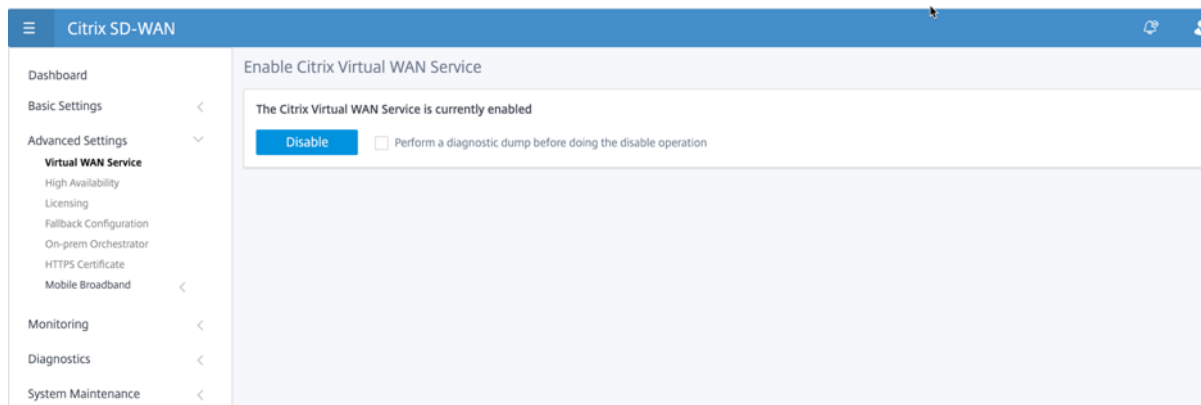
Paramètres avancés

Les **paramètres avancés** du dispositif SD-WAN incluent la configuration des entités suivantes.

- Service WAN virtuel Citrix
- Haute disponibilité
- Haut débit mobile
- Gestion des licences
- Configuration de secours
- Certificat HTTPS
- Orchestrator sur site

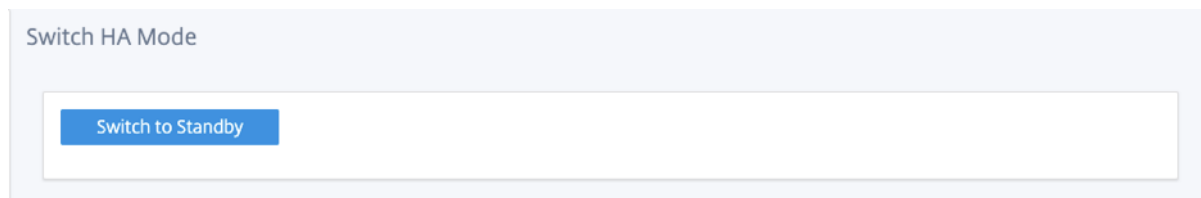
Citrix Virtual WAN Service

La page **Citrix Virtual WAN Service** vous permet d'activer/désactiver le service Citrix Virtual WAN. Pour plus d'informations, consultez la section [Configurer le service Virtual WAN](#).



Haute disponibilité

À partir de la page **Haute disponibilité**, vous pouvez basculer entre l'état actif et l'état de veille pour une configuration de haute disponibilité (HA) SD-WAN. L'état de haute disponibilité est disponible dans le tableau de bord (si la haute disponibilité est configurée). Pour plus d'informations, consultez la section [Mode haute disponibilité](#).



Haut débit mobile

Les appliances Citrix SD-WAN telles que les appliances Citrix SD-WAN 210 SE LTE et 110 LTE Wi-Fi disposent d'un modem LTE interne intégré. Vous pouvez également connecter un modem USB 3G/4G externe sur les appliances Citrix SD-WAN suivantes.

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE Wi-Fi SE

CDC Ethernet, MBIM et NCM sont les trois types de modems USB externes pris en charge.

Pour plus d'informations sur la configuration de LTE à l'aide de l'interface graphique héritée, consultez la rubrique suivante :

- [Configurer la fonctionnalité LTE sur l'appliance 210 SE LTE](#)
- [Configurer la fonctionnalité LTE sur une appliance 110-LTE-WiFi](#)
- [Configurer un modem LTE USB externe](#)

Pour un modem LTE interne, insérez la carte SIM dans l'emplacement pour carte SIM de l'appliance Citrix SD-WAN. Corrigez les antennes sur l'appliance Citrix SD-WAN. Pour plus d'informations, consultez [Installation des antennes LTE](#) et mise sous tension de l'appliance.

Remarque

L'appliance Citrix SD-WAN 110-LTE-WiFi dispose de deux emplacements SIM standard (2FF). Pour utiliser des SIM de taille Micro (3FF) et Nano (4FF), utilisez un adaptateur SIM. Accrochez la carte SIM la plus petite. Vous pouvez obtenir l'adaptateur auprès de Citrix en tant qu'unité remplaçable sur le terrain (FRU) ou auprès du fournisseur SIM. Le remplacement à chaud de la carte SIM pour le modem LTE interne est pris en charge uniquement sur l'appliance Citrix SD-WAN 110-LTE-WiFi.

Exigences pour modem LTE externe :

- Utilisez les dongles USB LTE pris en charge. Les modèles matériels de dongle pris en charge sont Verizon USB730L et AT&T USB800.
- Assurez-vous qu'une carte SIM est insérée dans le dongle USB LTE. Les dongles Ethernet LTE CDC sont préconfigurés avec une adresse IP statique, cela interfère avec la configuration et provoque une défaillance de la connexion ou une connexion intermittente, si la carte SIM n'est pas insérée.
- Avant d'insérer un dongle LTE Ethernet CDC dans l'appliance SD-WAN, connectez la clé USB externe à une machine Windows/Linux et assurez-vous qu'Internet fonctionne correctement avec une configuration APN et Mobile Data Roaming appropriée. Assurez-vous que le **mode de connexion** du dongle USB passe de la valeur par défaut **Manual** à **Auto**.

Remarque

- Les appliances Citrix SD-WAN prennent en charge un seul dongle USB LTE à la fois. Si plusieurs dongles USB sont branchés, débranchez tous les dongles et branchez un seul dongle.
- Les appliances Citrix SD-WAN ne prennent pas en charge le nom d'utilisateur et le mot de passe pour les modems USB. Assurez-vous que le nom d'utilisateur et le mot de passe sont désactivés sur le modem pendant l'installation.
- Le débranchement ou le redémarrage d'un dongle MBIM externe affecte la session de données du modem LTE interne. Il s'agit d'un comportement attendu.
- Lorsqu'un modem LTE externe est branché, l'appliance SD-WAN prend environ 3 minutes

pour le reconnaître.

Pour afficher l'état du haut débit mobile, sélectionnez le type de modem.

Dashboard

Basic Settings <

Advanced Settings >

Virtual WAN Service

High Availability

Mobile Broadband >

Status

Operations

Licensing

Fallback Configuration

HTTPS Certificate

On-prem Orchestrator

Monitoring <

Diagnostics <

System Maintenance <

Mobile Broadband Status

Modem TypeInternal ModemStatus OfDevice

Status	
Active SIM	SIM Two
Data Service Capability	non-simultaneous-cs-ps
ESN	0
Expected Data Format	802-3
Hardware Revision	10000
IMEI	867698040416771
MEID	86769804041677
MSISDN	
Manufacturer	QUALCOMM INCORPORATED
Max RX Channel Rate (bps)	100000000
Max TX Channel Rate (bps)	50000000
Model	QUECTEL Mobile Broadband Module
Networks	gsm,umts,lte
Operating Mode	online
Operating Mode HW Restricted	0
PRL Only Preference	0
PRL Version	0
Revision	EG25GGBR07A07M2G
SIM Capability	supported
Software Version	EG25GGBR07A07M2G
Type	110-WIFI-LTE

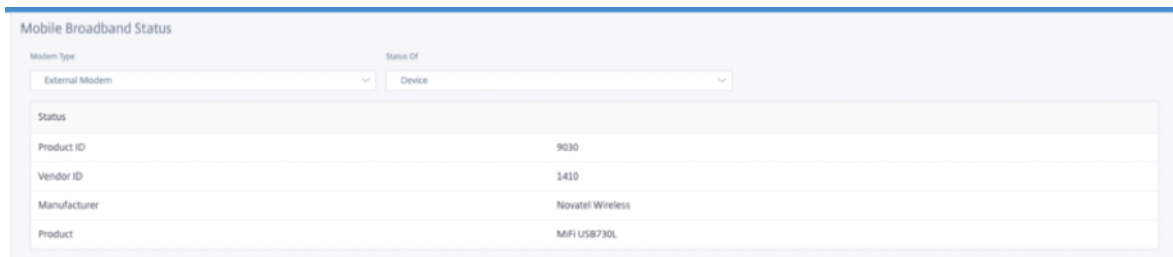
Voici quelques informations d'état utiles :

- **Type de modem** : sélectionnez le type de modem Externe ou Interne. Le modem interne affiche l'état sous **Mobile Broadband > Page État**. Toutes les autres sections telles que la préférence SIM, les paramètres APN, Activer/Désactiver le modem, Redémarrer le modem et Actualiser la carte SIM sont disponibles sous la page **Haut débit mobile > Opérations**.
- **SIM active** : à tout moment, une seule SIM peut être active. Affiche la carte SIM actuellement active.
- **Mode de fonctionnement** : affiche l'état du modem.

- **Capacités SIM** : indique si la carte SIM est prise en charge ou non.
- **Modèle** : affiche le nom du module haut débit mobile.

Si vous sélectionnez le modem **externe**, il affiche l'état du modem externe. Mais si le modem externe n'est pas configuré, il affiche un message d'avertissement car **Modem sélectionné n'est pas configuré sur ce périphérique**.

Détails du périphérique pour le modem externe Ethernet CDC.



The screenshot shows a window titled "Mobile Broadband Status". It contains two dropdown menus: "Modem Type" set to "External Modem" and "Status Of" set to "Device". Below these is a table with the following details:

Status	
Product ID	9030
Vendor ID	1410
Manufacturer	Novatel Wireless
Product	MIFI USB730L

Détails de l'appareil pour les modems externes MBIM et NCM. Le champ **Mode modem** affiche le type de dongle externe.

Mobile Broadband Status	
Modem Type	Status Of
External Modem	Device
Status	
Active SIM	SIM One
Data Service Capability	none
ESN	
Expected Data Format	unknown
Hardware Revision	
IMEI	866785032748294
MEID	
MSISDN	
Manufacturer	
Max RX Channel Rate (bps)	150000000
Max TX Channel Rate (bps)	150000000
Model	CL2E3372HM
Modem Mode	MBIM
Networks	gprs, edge, umts, hsdpa, hsupa, lte, custom
Operating Mode	online
Operating Mode HW Restricted	0
PRL Only Preference	0
PRL Version	0
Revision	
SIM Capability	not-supported
Software Version	
Product ID	157c
Vendor ID	12d1
Manufacturer	HUAWEI_MOBILE
Product	HUAWEI_MOBILE

Les détails de la carte SIM sont affichés uniquement pour les modems externes MBIM et NCM.

Mobile Broadband Status

Modem Type	Status Of	
External Modem	SIM One	
Status		
APN	internet	
APN Autodetect	Searching	
Application State	unknown	
Application Type	unknown	
Authentication	None	
Card State	present	
Connection Status	connected	
Home Network	Idea	
ICCID	89911100001445614166	
IMSI	404446068985937	
Address	10.2.250.171	
Gateway	10.2.250.169	
MTU	1500	
Netmask	255.255.255.248	
Primary DNS	112.110.241.1	
Secondary DNS	112.110.249.1	
Data Session	Not Available	
Enabled		
MCC	404	
MNC	44	
PIN Retries	0	
PIN State	disabled	
PUK Retries	0	
Radio Interface	lte	
Roaming Status	on	
Signal Strength	Excellent	
Username		

Opérations de haut débit mobile Opérations prises en charge sur les modems internes et externes :

Opérations	Modem interne	Modem externe - CDC Ethernet	Modem externe - MBIM et NCM
Préférence SIM	Oui - Pour les appliances prenant en charge la double SIM	Non	Non

Opérations	Modem interne	Modem externe - CDC Ethernet	Modem externe - MBIM et NCM
Code PIN de la carte SIM	Oui	Non	Non
Paramètres APN	Oui	Non	Oui
Paramètres réseau	Oui	Non	Non
Itinérant	Oui	Non	Non
Gérer le firmware	Oui	Non	Non
Activer/désactiver le modem	Oui	Non	Oui
Redémarrer le modem	Oui	Non	Non
Actualiser la carte SIM	Oui	Non	Non

Préférence SIM Vous pouvez insérer des cartes SIM doubles sur une appliance Citrix SD-WAN 110-LTE-WiFi. À un moment donné, une seule carte SIM est active. Sélectionnez la **préférence SIM** :

- **Carte SIM One préférée** : si deux cartes SIM sont insérées, au démarrage, le modem LTE utilise la carte SIM One, si disponible. Lorsque le modem LTE est en marche, il utilise la carte SIM (SIM One ou SIM Two) utilisable à ce moment et continuera à l'utiliser jusqu'à ce que la carte SIM soit active.
- **SIM Two préféré** : si deux SIM sont insérés, au démarrage, le modem LTE utilise SIM Two, si disponible. Lorsque le modem LTE est en marche, il utilise la carte SIM (SIM One ou SIM Two) utilisable à ce moment et continuera à l'utiliser jusqu'à ce que la carte SIM soit active.
- **SIM One** : Seul SIM One est utilisé, quel que soit l'état de la carte SIM sur les deux emplacements SIM. SIM One est toujours actif.
- **SIM Two** : Seul SIM Two est utilisé, quel que soit l'état de la carte SIM sur les deux emplacements SIM. La carte SIM Two est toujours active.

Remarque

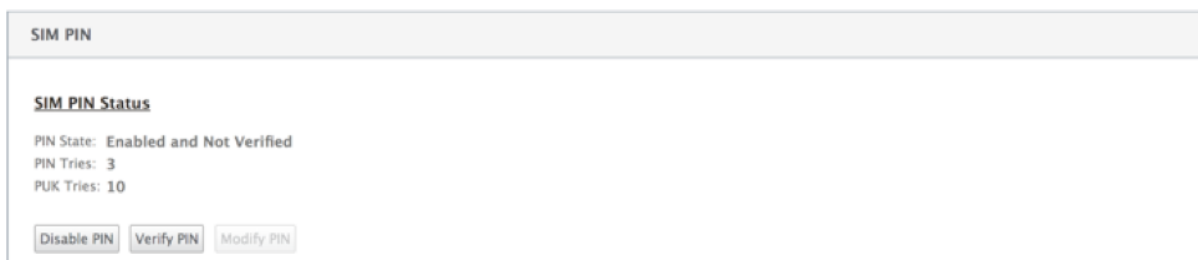
L'option Préférence SIM n'est pas disponible pour l'appliance Wi-Fi Citrix SD-WAN 210-SE LTE car elle ne possède qu'un seul emplacement pour carte SIM.

The screenshot shows a web interface for 'SIM Preference'. Under the heading 'Preferred SIM', there is a dropdown menu currently showing 'SIM Two'. Below this menu is a blue button labeled 'Apply'.

Code PIN de la carte SIM

Si vous avez inséré une carte SIM verrouillée avec un code PIN, l'état de la carte SIM est **activé et Non vérifié**. Vous ne pouvez pas utiliser la carte SIM tant qu'elle n'est pas vérifiée à l'aide du code PIN SIM. Vous pouvez obtenir le code PIN de la carte SIM auprès du transporteur.

Pour effectuer des opérations PIN de la carte SIM, accédez à **Paramètres avancés > Haut débit mobile > Opérations > Statut du code PIN SIM**.



SIM PIN

SIM PIN Status

PIN State: Enabled and Not Verified

PIN Tries: 3

PUK Tries: 10

Disable PIN Verify PIN Modify PIN

Vous pouvez effectuer les opérations suivantes :

- **Vérifier le code PIN SIM** : cliquez sur **Vérifier**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Vérifier**. Le statut passe à **Activé et Vérifié**.
- **Activer le code PIN** de la carte SIM : vous pouvez activer le code PIN SIM pour une carte SIM dont le code PIN Cliquez sur **Activer**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Activer**. Si l'état du code PIN de la SIM passe à **Activé et Non vérifié**, cela signifie que le code PIN n'est pas vérifié et que vous ne pouvez pas effectuer d'opérations liées à LTE tant que le code PIN n'est pas vérifié. Cliquez sur **Vérifier**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Vérifier**.
- **Désactiver le code PIN SIM** : Vous pouvez choisir de désactiver la fonctionnalité du code PIN SIM pour une carte SIM pour laquelle le code PIN SIM est activé et vérifié. Cliquez sur **Désactiver**. Entrez le code PIN de la carte SIM et cliquez sur **désactiver**.
- **Modifier le code PIN de la carte SIM** : une fois que le code PIN est activé et vérifié, vous pouvez choisir de modifier le code PIN. Cliquez sur **Modifier**. Entrez le code PIN SIM fourni par le transporteur. Entrez le nouveau code PIN SIM et confirmez-le. Cliquez sur **Modifier**.
- **Débloquer la carte SIM** - Si vous oubliez le code PIN SIM, vous pouvez réinitialiser le code PIN SIM à l'aide du PUK SIM obtenu auprès du transporteur. Pour débloquer une carte SIM, cliquez sur **Débloquer**. Entrez le code PIN et le code PUK de la carte SIM obtenus auprès de l'opérateur et cliquez sur **Débloquer**.

Remarque

La carte SIM est bloquée de façon permanente avec 10 tentatives infructueuses de PUK, tout en débloquent la carte SIM. Contactez le fournisseur de services de l'opérateur pour

obtenir une nouvelle carte SIM.

Paramètres APN

1. Pour configurer les paramètres APN, accédez à **Paramètres avancés > Haut débit mobile > Opérations** et accédez à la section **Paramètres APN**.

Remarque

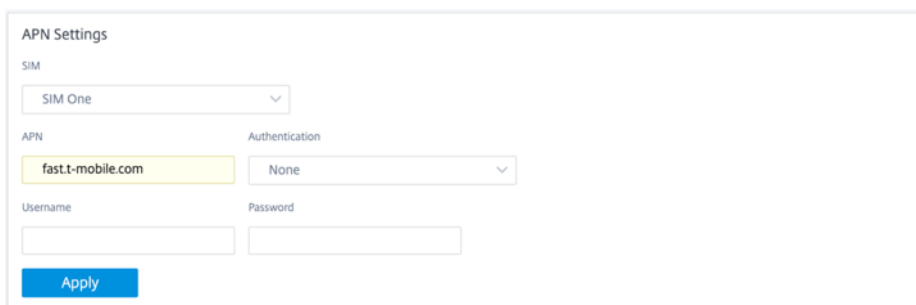
Obtenez les informations APN auprès du transporteur.

2. Sélectionnez la carte SIM, saisissez l'**APN**, le **nom d'utilisateur**, le **mot de passe** et l'**authentification** fournis par l'opérateur. Vous pouvez choisir parmi les protocoles d'authentification PAP, CHAP, PAPCHAP. Si le transporteur n'a fourni aucun type d'authentification, définissez-le sur **Aucun**.

Remarque

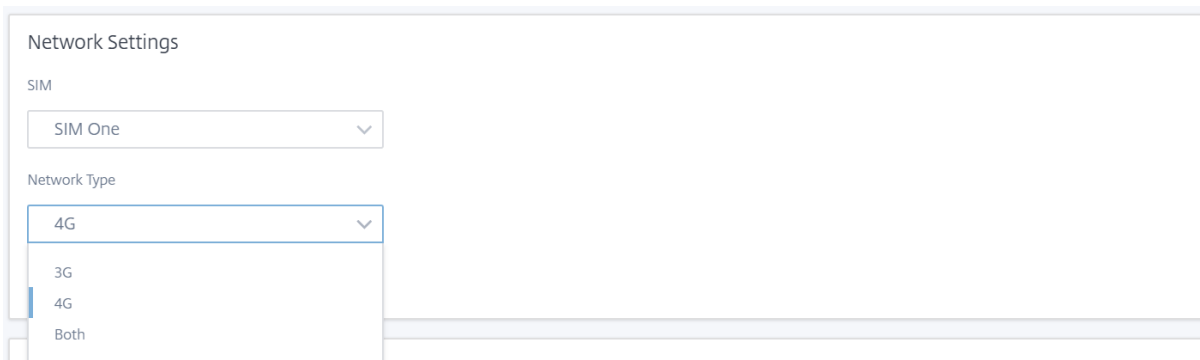
Tous ces champs sont facultatifs.

3. Cliquez sur **Apply**.



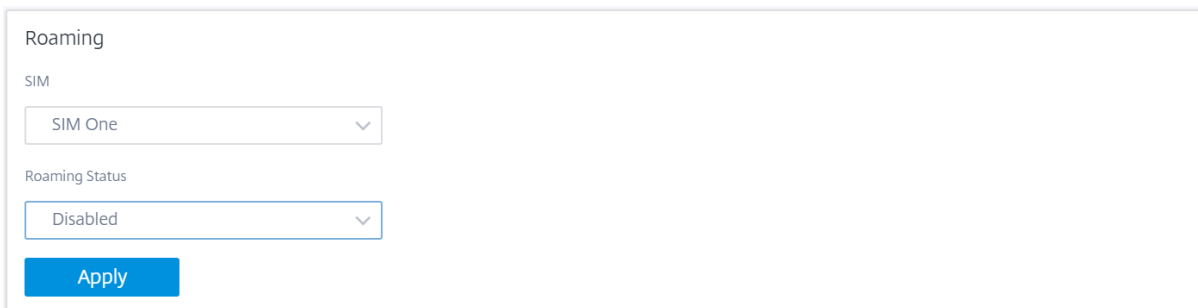
The screenshot shows the 'APN Settings' window. It contains the following fields: 'SIM' with a dropdown menu showing 'SIM One'; 'APN' with a text field containing 'fast.t-mobile.com'; 'Authentication' with a dropdown menu showing 'None'; 'Username' with an empty text field; and 'Password' with an empty text field. At the bottom, there is a blue 'Apply' button.

Paramètres réseau Vous pouvez sélectionner le réseau mobile sur les appliances Citrix SD-WAN prenant en charge le modem LTE interne. Les réseaux pris en charge sont 3G, 4G ou les deux.



The screenshot shows the 'Network Settings' window. It contains the following fields: 'SIM' with a dropdown menu showing 'SIM One'; and 'Network Type' with a dropdown menu showing '4G'. The 'Network Type' dropdown is open, showing options: '3G', '4G', and 'Both'.

Itinérant L'option d'itinérance est activée par défaut sur vos appliances LTE, vous pouvez choisir de la désactiver.

The image shows a configuration panel for Roaming. At the top, the word 'Roaming' is displayed. Below it, the label 'SIM' is followed by a dropdown menu currently showing 'SIM One'. Further down, the label 'Roaming Status' is followed by a dropdown menu currently showing 'Disabled'. At the bottom of the panel is a blue button labeled 'Apply'.

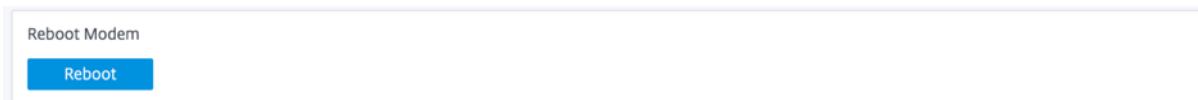
Gérer le firmware

Chaque appliance compatible LTE dispose d'un ensemble de microprogrammes disponibles. Vous pouvez sélectionner dans la liste existante du firmware ou télécharger un firmware et l'appliquer. Si vous ne savez pas quel firmware utiliser, sélectionnez l'option **AUTO-SIM**. L'option AUTO-SIM permet au modem LTE de choisir le firmware le plus adapté en fonction de la carte SIM insérée.

Activer/désactiver le modem Activer/désactiver le modem en fonction de votre intention d'utiliser la fonctionnalité LTE. Par défaut, le modem LTE est activé.

The image shows a configuration panel titled 'Enable/Disable Modem'. It contains a single blue button labeled 'Enable'.

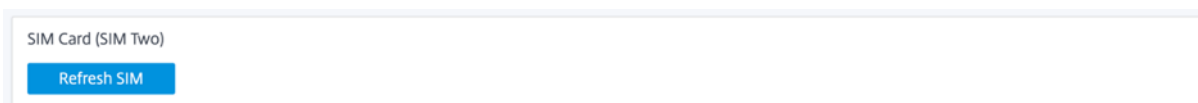
Redémarrer le modem Redémarre le modem. L'opération de redémarrage peut prendre jusqu'à 7 minutes.

The image shows a configuration panel titled 'Reboot Modem'. It contains a single blue button labeled 'Reboot'.

Actualiser la carte SIM Utilisez l'option **Actualiser la carte SIM** lorsque la carte SIM n'est pas détectée correctement par le modem LTE-WiFi.

Remarque

L'opération d'actualisation de la carte SIM s'applique uniquement à la carte SIM active.

The image shows a configuration panel titled 'SIM Card (SIM Two)'. It contains a single blue button labeled 'Refresh SIM'.

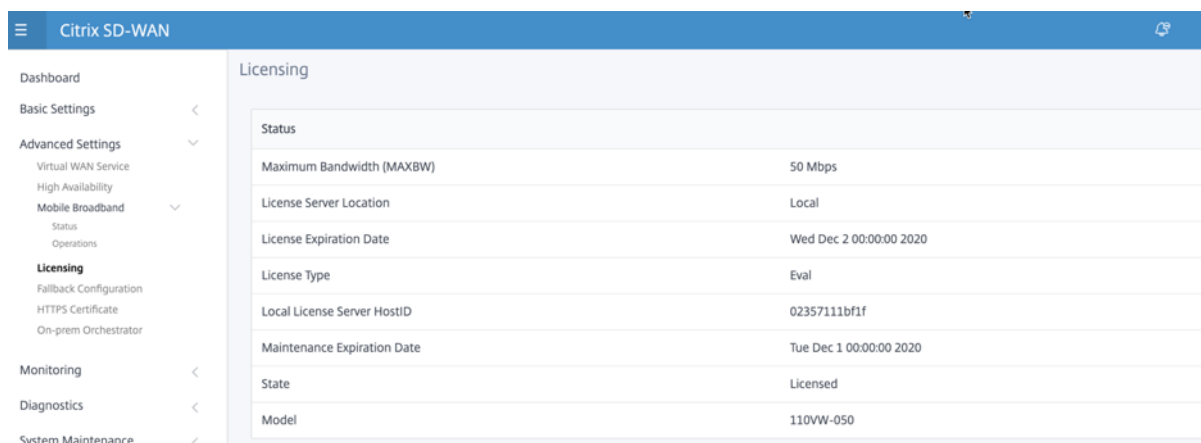
Vous pouvez afficher et gérer à distance tous les sites LTE de votre réseau à l'aide du Centre Citrix SD-WAN. Pour plus d'informations, reportez-vous à la section [Gestion de sites LTE distants](#).

Pour plus d'informations sur la configuration LTE, consultez [Configurer la fonctionnalité LTE sur l'appliance 110-LTE-WiFi](#) et [Configurer la fonctionnalité LTE sur l'appliance 210 SE LTE](#).

Pour plus d'informations sur la configuration d'un modem LTE externe, consultez la section [Configurer un modem USB LTE externe](#).

Gestion des licences

La page **Licence** affiche les détails de licence tels que l'emplacement du serveur, le modèle, le type de licence, etc.



Licensing	
Status	
Maximum Bandwidth (MAXBW)	50 Mbps
License Server Location	Local
License Expiration Date	Wed Dec 2 00:00:00 2020
License Type	Eval
Local License Server HostID	02357111bf1f
Maintenance Expiration Date	Tue Dec 1 00:00:00 2020
State	Licensed
Model	110VW-050

Remarque

Lors de l'installation et de l'application d'une licence à partir de SD-WAN Center, assurez-vous que votre appliance spécifique prend en charge l'édition d'appliance SD-WAN que vous souhaitez activer et que la version logicielle appropriée est disponible.

Configuration par défaut/de secours

La page **Configuration par défaut/secours** affiche les données de configuration de secours stockées. Si la configuration de secours est désactivée, vous pouvez l'activer en activant le commutateur **Activer la configuration de secours**.

☰

Citrix SD-WAN

🔔

👤

Dashboard

Basic Settings

Advanced Settings

Virtual WAN Service

High Availability

Mobile Broadband

Status

Operations

Licensing

Fallback Configuration

HTTPS Certificate

On-prem Orchestrator

Monitoring

Diagnostics

System Maintenance

Fallback Configuration

The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.

🟢 Enable Fallback Configuration

Reset

WAN Settings

WAN settings are currently not configurable. WAN ports are configured as independent WAN Links using DHCP client and monitor the Quad9 DNS service to determine WAN connectivity.

LAN Settings

VLAN ID

IP Address

0

192.168.0.1/24

☐ Enable DHCP Server

DHCP Start

DHCP End

192.168.0.50

192.168.0.250

☒ Dynamic DNS Servers

DNS Server

Alt DNS Server

9.9.9.9

149.112.112.112

☐ Internet Access

Port Settings

Port	Mode	
1/1	<input type="radio"/> WAN <input checked="" type="radio"/> LAN <input type="radio"/> Disabled	
1/2	<input checked="" type="radio"/> WAN <input type="radio"/> LAN <input type="radio"/> Disabled	9.9.9.9
1/3	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled	
1/4-MGMT	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled	
LTE-1	<input checked="" type="radio"/> WAN <input type="radio"/> LAN <input type="radio"/> Disabled	9.9.9.9
LTE-E1	<input checked="" type="radio"/> WAN <input type="radio"/> LAN <input type="radio"/> Disabled	9.9.9.9

Unassigned Port Bypass Mode

Fail to Block

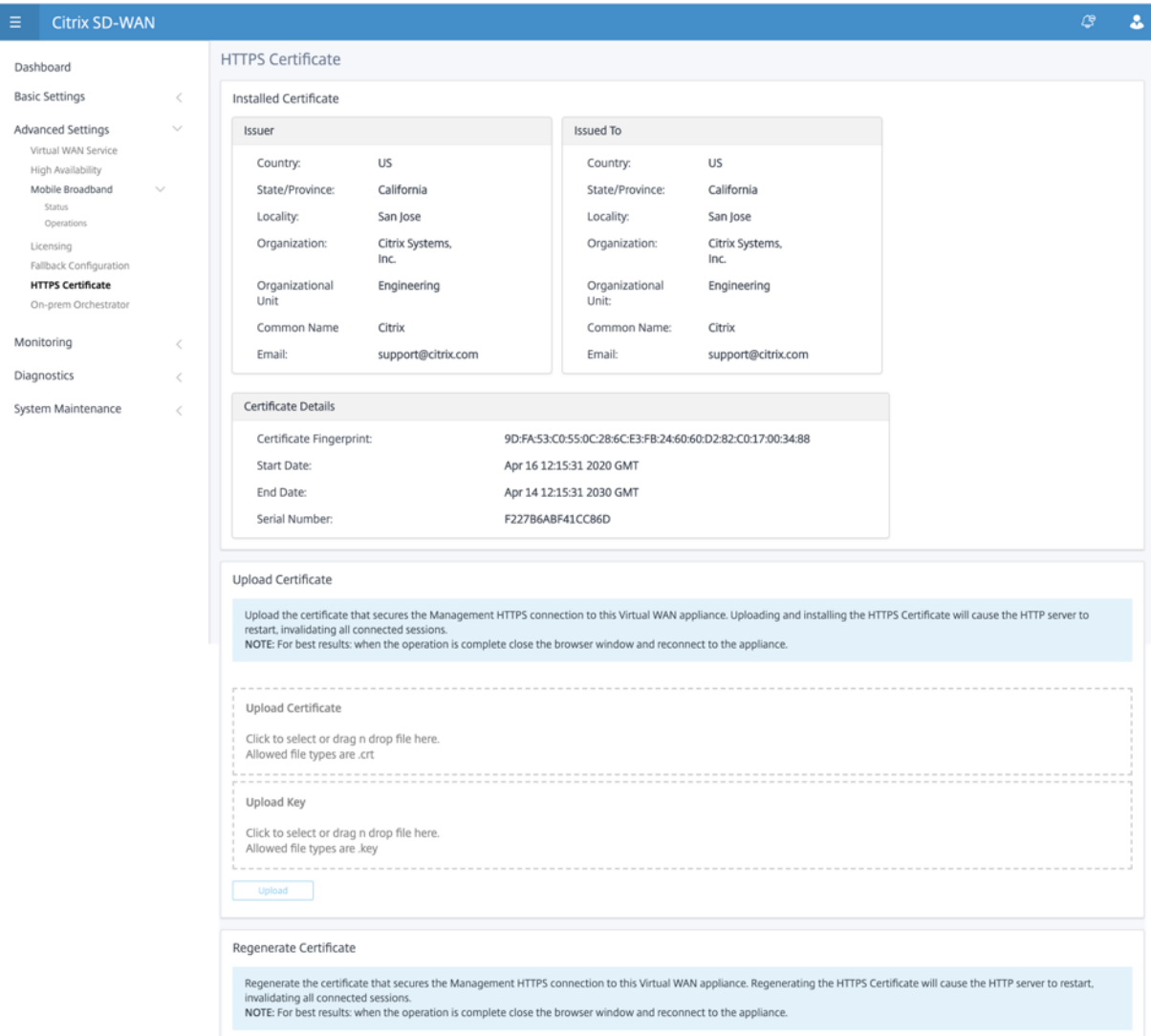
Remarque

Les interfaces LTE ne peuvent pas être configurées avec une adresse IP statique.

Pour plus d’informations, reportez-vous à la section [Configuration par défaut/de secours](#).

Certificat HTTPS

Un certificat HTTPS est requis pour établir une connexion sécurisée. La page **Certificat HTTPS** affiche les détails du certificat HTTPS déjà installé. Pour plus d’informations, consultez la section [Certificats HTTPS](#).



Orchestrator sur site

Citrix On-Prem SD-WAN Orchestrator est la version logicielle locale du service Citrix SD-WAN Orchestrator. Citrix On-Prem SD-WAN Orchestrator fournit un panneau unique de plate-forme de gestion du verre permettant aux partenaires Citrix de gérer plusieurs clients de manière centralisée, avec des contrôles d'accès basés sur les rôles appropriés.

Vous pouvez établir une connexion entre votre appliance Citrix SD-WAN et Citrix On-Prem SD-WAN Orchestrator en activant la connectivité Orchestrator et en spécifiant l'identité SD-WAN Orchestrator sur site.

Remarque

- La fonctionnalité de **configuration de l'appliance SD-WAN Orchestrator sur site SD-WAN**

est un activateur pour Citrix On-Prem SD-WAN Orchestrator. La fonctionnalité de configuration SD-WAN Orchestrator sur site de Citrix sur l'appliance SD-WAN n'est actuellement pas disponible. Il est prévu pour une prochaine version.

- Le déploiement sans contact ne fonctionnera pas si la **configuration de l'appliance SD-WAN Orchestrator sur site** sur site est configurée sur les appliances SD-WAN.

Pour activer la connectivité Orchestrator :

1. Dans l'interface graphique de l'appliance, accédez à **Paramètres avancés > Orchestrator sur site > Identité**.
2. **Activez la case à cocher Activer la connectivité SD-WAN Orchestrator** sur site.

3. Entrez soit l'adresse IP SD-WAN Orchestrator sur site, soit le domaine, soit les deux (adresse IP et domaine) pour la configuration.

Si le client configure uniquement le domaine, il doit s'assurer d'ajouter l'enregistrement DNS dans son serveur DNS local et configurer l'adresse IP du serveur DNS sur les appliances SD-WAN. Pour configurer, accédez à **Configuration > Cartes réseau > Adresse IP**.

Par exemple, si le domaine SD-WAN Orchestrator sur site est configuré en tant que **citrix.com**, vous devez créer un enregistrement DNS dans le serveur DNS pour le nom de domaine complet et l'adresse IP SD-WAN Orchestrator ci-dessous :

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

En cas de configuration avancée :

Par exemple : si le domaine Orchestrator sur site est configuré en tant que **citrix.com**, le domaine du service de gestion des téléchargements est configuré **en tant que download.citrix.com** et le domaine du service de gestion des statistiques est configuré en tant que **statistics.citrix.com**. Ensuite, vous devez créer un enregistrement DNS dans le serveur DNS pour le nom de domaine complet ci-dessous et l'adresse IP correspondante :

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

On-Prem Orchestrator peut prendre en charge des services en cours d'exécution tels que le téléchargement, les statistiques sur les instances de serveur indépendantes, afin d'améliorer l'évolutivité pour les grands réseaux. Vous pouvez sélectionner la **configuration avancée** et configurer le service de **gestion des téléchargements et le service de gestion des statistiques**.

Activez la case à cocher **Configuration avancée** et fournissez les détails suivants :

- **Download Management Service IP/domaine** : Fournissez l'adresse/domaine IP qui aide à télécharger le logiciel SD-WAN et les aspects de téléchargement de configuration à une instance de serveur indépendante, afin de permettre une meilleure évolutivité pour les grands réseaux.
- **Service de gestion statistique IP/domaine** : Fournissez l'adresse/domaine IP qui aide à télécharger la collecte et la gestion des statistiques SD-WAN des périphériques vers une instance de serveur indépendante, afin de permettre une meilleure évolutivité pour les grands réseaux.

4. Cliquez sur **Apply**.

Pour régénérer, télécharger et charger l'appliance SD-WAN ou le certificat SD-WAN Orchestrator sur site, accédez à **Paramètres avancés > On-Prem Orchestrator > Certificat**.

Si le **type d'authentification** Orchestrator sur site est désactivé, l'appliance peut se connecter à l'Orchestrator sur site via **Aucune authentification ou Authentification unidirectionnelle ou Authentification bidirectionnelle**.

Si le **type d'authentification** Orchestrator sur site est activé, l'appliance peut uniquement se connecter à l'Orchestrator sur site via l'**authentification bidirectionnelle**.

Lors de la désactivation du **type d'authentification** dans On-Prem Orchestrator de l'état d'activation, les appliances existantes en mode Authentification unidirectionnelle passent à l'état déconnecté. Les clients doivent changer le type d'authentification de l'appliance en authentification bidirectionnelle et télécharger le certificat de l'appliance SD-WAN sur l'Orchestrator On-Prem Orchestrator pour le connecter.

Remarque

- Les certificats générés sont des certificats auto-signés X509.
- Le client doit régénérer les certificats si le certificat est expiré ou compromis.
- La validité du certificat est de 10 ans.
- Vous pouvez afficher les détails du certificat tels que l'empreinte digitale, la date de début et la date de fin

- Le client doit s'assurer que les certificats sont régénérés et échangés entre On-Prem Orchestrator et l'apppliance SD-WAN afin d'éviter la perte de connectivité de l'apppliance avec On-Prem Orchestrator.

5. Sélectionnez le **type d'authentification**. Voici les types d'authentification pris en charge entre l'apppliance SD-WAN et la connectivité SD-WAN Orchestrator sur site :

- **Aucune authentification** : aucune authentification entre l'apppliance SD-WAN Orchestrator sur site et le dispositif SD-WAN, et il n'est pas nécessaire d'utiliser l'apppliance SD-WAN ou le certificat SD-WAN Orchestrator sur site. Mais vous pouvez utiliser cette option si vous disposez d'un réseau sécurisé tel que MPLS.

The screenshot shows the 'Secure Connectivity' configuration page. It contains three options: 'No Authentication', 'One-way Authentication', and 'Two-way Authentication'. The 'No Authentication' option is selected in the dropdown menu. Below the dropdown is an 'Apply' button.

Secure Connectivity

No Authentication – Insecure connection. Use this option if you have a secure network. For eg: MPLS

One-way Authentication – On-prem Orchestrator certificates have to be uploaded to all the appliances. Appliance will trust On-prem Orchestrator using the uploaded certificates.

Two-way Authentication – On-prem Orchestrator and Appliance certificates have to be exchanged. Appliance and On-prem Orchestrator will trust each other using the exchanged certificates.

Authentication Type

No Authentication

Apply

- **Authentification unidirectionnelle** : lorsque vous sélectionnez le type d'authentification unidirectionnelle, vous devez télécharger le certificat Orchestrator sur site. Téléchargez l'Orchestrator On-Prem Orchestrator à partir de l'Orchestrator sur site et cliquez sur Charger. L'apppliance SD-WAN approuve l'Orchestrator On-Prem à l'aide des certificats téléchargés.

The screenshot shows the 'Secure Connectivity' configuration page with 'One-Way Authentication' selected. Below the authentication options, there is a section for 'On-prem SD-WAN Orchestrator Certificate' which displays certificate details and an upload area.

Secure Connectivity

No Authentication – Insecure connection. Use this option if you have a secure network. For eg: MPLS

One-way Authentication – On-prem Orchestrator certificates have to be uploaded to all the appliances. Appliance will trust On-prem Orchestrator using the uploaded certificates.

Two-way Authentication – On-prem Orchestrator and Appliance certificates have to be exchanged. Appliance and On-prem Orchestrator will trust each other using the exchanged certificates.

Authentication Type

One-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

Certificate Fingerprint:	0D:37:24:A6:99:B6:D4:8F:CB:55:C1:3C:AB:42:9E:7F:19:EB:23:53
Start Date:	May 21 13:34:50 2020 GMT
End Date:	May 19 13:34:50 2030 GMT

Click here to select the file or drag and drop the selected file.
Allowed file type is .pem

Upload

- **Authentification bidirectionnelle** : les certificats d'Orchestrator et d'appliance sur site doivent être échangés les uns avec les autres. Pour **l'authentification bidirectionnelle**, vous devez régénérer, télécharger et charger le certificat de l'appliance SD-WAN sur l'Orchestrator sur site. L'appliance SD-WAN et On-Prem Orchestrator se font confiance à l'aide des certificats échangés.

Secure Connectivity

No Authentication – Insecure connection. Use this option if you have a secure network. For eg: MPLS
 One-way Authentication – On-prem Orchestrator certificates have to be uploaded to all the appliances. Appliance will trust On-prem Orchestrator using the uploaded certificates.
 Two-way Authentication – On-prem Orchestrator and Appliance certificates have to be exchanged. Appliance and On-prem Orchestrator will trust each other using the exchanged certificates.

Authentication Type
 Two-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

Certificate Fingerprint:	0D:37:24:A6:99:B6:D4:8F:CB:55:C1:3C:AB:42:9E:7F:19:EB:23:53
Start Date:	May 21 13:34:50 2020 GMT
End Date:	May 19 13:34:50 2030 GMT

Click here to select the file or drag and drop the selected file.
 Allowed file type is .pem

Upload

SD-WAN Appliance Certificate

Certificate Details:

Certificate Fingerprint:	FC:36:3C:E5:EF:C2:F8:ED:48:20:0C:28:6C:5D:BA:82:55:CE:04:DD
Start Date:	Jul 21 06:07:08 2020 GMT
End Date:	Jul 19 06:07:08 2030 GMT

Regenerate Download

Remarque

Il est recommandé d'utiliser uniquement l'authentification unidirectionnelle ou l'authentification bidirectionnelle. S'il n'y avait pas d'authentification, vous devez choisir le serveur DNS sécurisé.

Pour désactiver la connectivité SD-WAN Orchestrator sur site, désactivez **Activer la connectivité SD-WAN Orchestrator locale**, puis cliquez sur **Appliquer**. Pour convertir le réseau géré sur site Orchestrator en réseau géré Cloud Orchestrator ou MCN, vous devez désactiver la connectivité SD-WAN Orchestrator sur site et effectuer la réinitialisation de la configuration. Pour réinitialiser la configuration, accédez à **Configuration > Maintenance système > Réinitialisation de configuration**.

Mise à niveau et rétrogradation

- Après la mise à niveau de l'appliance SD-WAN de la version 11.1.1/11.2.0/10.2.7 vers la version logicielle 11.2.1, vous devez échanger les certificats appliance et On-Prem Orchestrator.
- Après avoir rétrogradé l'appliance SD-WAN de la version 11.2.1 à la version logicielle 11.1.1/11.2.0/10.2.7, vous devez appliquer à nouveau les paramètres d'identité sur l'interface utilisateur de l'appliance Citrix SD-WAN. En cas de problème lié à la configuration SD-WAN Orchestrator sur site ou à la connectivité de l'appliance SD-WAN, désactivez la connectivité SD-WAN Orchestrator sur site, puis réactivez la connectivité SD-WAN Orchestrator sur site.

Le type d'authentification SD-WAN Orchestrator sur site doit être désactivé pour gérer les appliances SD-WAN exécutant la version 10.2.7/11.1.1/11.2.0 du logiciel.

Surveillance

Dans la section Surveillance, vous pouvez afficher les statistiques **ARP (Address Resolution Protocol)**, **Route**, **Ethernet**, **Ethernet MAC** ainsi que les **liens WAN client DHCP**, **SLAAC WAN Links**, **Server/Relais DHCP**, **Connexions pare-feu**, **flux** et **statistiques DNS**.

- **Statistiques ARP, Route, Ethernet et Ethernet MAC** : Vous pouvez voir les informations statistiques pour ARP, Route, Ethernet et Ethernet MAC. À l'aide des informations statistiques, vous pouvez vérifier toute erreur de trafic ou d'interface. Pour plus d'informations, consultez la section [Affichage des informations statistiques](#).
- **Liens WAN client DHCP** : La page **LiensWAN** du client DHCP fournit l'état des adresses IP apprises. Vous pouvez demander le renouvellement de l'adresse IP, qui actualise la durée du bail. Vous pouvez également choisir de **libérer le renouvellement**, ce qui émet une nouvelle adresse IP avec un nouveau bail. Pour plus d'informations, consultez la section [Surveillance des liaisons WAN du client DHCP](#).
- **Liens WAN SLAAC** : La page Liens WAN SLAAC fournit des détails sur les adresses IPv6 que SLAAC attribue aux interfaces virtuelles. Vous pouvez également sélectionner **Release Renew** pour autoriser SLAAC à attribuer une nouvelle adresse IP ou la même adresse IP avec un nouveau bail au client IPv6.
- **Serveur/relais DHCP** : Vous pouvez utiliser l'appliance SD-WAN en tant que serveurs DHCP ou agents relais DHCP.
 - La fonctionnalité de serveur DHCP permet aux périphériques du même réseau que l'interface LAN/WAN de l'appliance SD-WAN d'obtenir leur configuration IP à partir de l'appliance SD-WAN.

- La fonction de relais DHCP permet à vos appliances SD-WAN de transférer des paquets DHCP entre le client DHCP et le serveur.

Pour plus d'informations, consultez [Serveur DHCP et relais DHCP](#).

- **Connexions pare-feu** : la page **Connexions au pare-feu** fournit les statistiques de connexion au pare-feu. Vous pouvez voir comment les stratégies de pare-feu agissent sur le trafic de chaque application. Pour plus d'informations, consultez la section [Affichage des statistiques de pare-feu](#).
- **Flux** : la section **Flux** fournit des instructions de base pour afficher les informations de flux WAN virtuel. Pour plus de détails, consultez la section [Affichage des informations de flux](#).
- **Statistiques de proxy DNS** : Cette page fournit des détails sur les proxy DNS configurés. Cliquez sur **Actualiser** pour obtenir les données actuelles. Pour plus d'informations, consultez la section [Système de noms de domaine](#).

Diagnostics

La section **Diagnostics** fournit les options permettant de tester et d'étudier les problèmes de connectivité. Pour plus d'informations, consultez la section [Diagnostics](#).

Remarque

Pour l'appliance Citrix SD-WAN 110, un seul package de diagnostic peut être présent à la fois. Pour l'appliance Citrix SD-WAN 210, un maximum de cinq packages de diagnostic sont autorisés.

Maintenance du système

Utilisez la section **Maintenance du système** pour effectuer des activités de maintenance. La page **Maintenance du système** contient les options suivantes :

- **Supprimer les fichiers** : vous pouvez supprimer les fichiers journaux, les fichiers de sauvegarde et les bases de données archivées. Sélectionnez le fichier à supprimer dans le menu déroulant et cliquez sur le bouton Supprimer.
- **Redémarrer le système** : vous pouvez redémarrer le service WAN virtuel ou redémarrer le système.
- **Gestion locale des modifications** : le processus de **gestion locale des modifications** vous permet de télécharger un nouveau package d'appliance vers cette appliance individuelle.
- **Réinitialisation de la configuration** : Vous pouvez réinitialiser la configuration. Cette option efface les données utilisateur, les journaux, l'historique et les données de configuration locale de cette appliance.

- **Réinitialisation d'usine : utilisez l'option de réinitialisation** d'usine pour réinitialiser l'appliance SD-WAN à la version livrée.

Remarque

Toutes ces fonctionnalités sont déjà expliquées en détail dans la documentation [SD-WAN](#) existante.

Plateformes non prises en charge

La nouvelle interface utilisateur ne prend pas en charge les appliances SD-WAN suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

Configuration système requise

May 6, 2021

Configuration matérielle requise

Les instructions d'installation des appliances SD-WAN sont fournies à la section [Configuration des appliances SD-WAN](#).

Exigences du firmware

Tous les modèles d'appliances Citrix SD-WAN dans un environnement Virtual WAN doivent exécuter la même version de microprogramme Citrix SD-WAN.

Remarque

Les appliances exécutant des versions logicielles antérieures ne peuvent pas établir de connexion Virtual Path à l'appliance exécutant SD-WAN version 11.4. Pour plus d'informations, contactez l'équipe de support Citrix.

Configuration logicielle requise

Pour plus d'informations sur les exigences de licence, reportez-vous à la section [Système de licences](#).

Exigences du navigateur

Les cookies doivent être activés et JavaScript doit être installé et activé.

L'interface Web de gestion SD-WAN est prise en charge sur les navigateurs suivants :

- Mozilla Firefox 49+
- Google Chrome 51+
- Microsoft Internet Explorer 11+
- Microsoft Edge 13+
- Safari 9+

Les navigateurs pris en charge doivent avoir les cookies activés et JavaScript installé et activé.

Hyperviseur

Citrix SD-WAN SE/PE VPX peut être configuré sur les hyperviseurs suivants :

- Serveur VMware ESXi, version 5.5.0 ou ultérieure.
- Citrix Hypervisor 6.5 ou supérieur.
- Microsoft Hyper-V 2012 R2 ou supérieur.
- Linux KVM

Plate-forme Cloud

Citrix SD-WAN SE/PE VPX peut être configuré sur les plates-formes cloud suivantes :

- Microsoft Azure
- Amazon Web Services
- Plate-forme Google Cloud

Modèles de plates-formes SD-WAN et logiciels

September 26, 2023

Cette section fournit des informations sur le téléchargement des packages logiciels Citrix SD-WAN.

Remarque

Avant de télécharger le logiciel, vous devez obtenir et enregistrer une licence de logiciel Citrix SD-WAN. Pour plus d'informations, consultez l'article [Licences](#).

Un package de matériel SD-WAN contient le package logiciel SD-WAN pour un modèle particulier d'appliance fourni avec un package de configuration SD-WAN spécifique. Les deux packages sont regroupés et distribués aux clients à l'aide de l'assistant de **gestion des modifications** dans l'interface Web de gestion exécutée sur le nœud de contrôle principal (MCN).

S'il s'agit d'une installation initiale, vous devez charger, mettre en scène et activer manuellement le package de matériel approprié sur chacune des appliances clientes résidant sur votre réseau SD-WAN. Si vous mettez à jour la configuration d'un déploiement SD-WAN existant, le MCN distribue et active automatiquement le package de matériel approprié sur chacun des clients existants, lorsque les chemins virtuels vers les clients deviennent opérationnels.

Télécharger les progiciels

Il existe un package logiciel Citrix SD-WAN différent pour chaque modèle d'appliance. Vous devez télécharger le progiciel approprié pour chaque modèle d'appliance que vous souhaitez inclure dans votre réseau.

Pour télécharger les packages logiciels Citrix SD-WAN, accédez à l'URL ; [téléchargements de produits](#). Les instructions pour télécharger le logiciel sont fournies sur ce site.

Packages logiciels Citrix SD-WAN

Il existe un progiciel Citrix SD-WAN différent pour chaque modèle d'appliance SD-WAN pris en charge. Vous devez acquérir le package approprié pour chaque modèle d'appliance que vous envisagez d'incorporer dans votre réseau.

Modèles d'appliances SD-WAN pris en charge

Il existe trois catégories principales d'appliances Citrix SD-WAN :

- Modèles de matériel SD-WAN
 - WANOP, Édition Standard et Édition Premium
- Appliances virtuelles SD-WAN VPX (SD-WAN VPX)
 - Édition Standard et Édition WANOP

Remarque

Tous les modèles d'appiances SD-WAN dans un environnement SD-WAN doivent exécuter la même version de microprogramme SD-WAN. Pour plus d'informations, contactez le support client Citrix SD-WAN.

Pour obtenir une description complète des appliances SD-WAN, reportez-vous à la [fiche technique](#) de l'édition de la plate-forme de produits SD-WAN sur le site de téléchargement des produits.

Dispositifs matériels SD-WAN édition standard

Voici les modèles d'appliance matérielle SD-WAN Standard Edition pris en charge :

MODÈLE DE PLATE-FORME SD-WAN SE	RÔLE
110-SE/110-LTE-WiFi/110-WiFi-SE	Appliance de succursale de petite taille
210-SE/210-SE LTE	Appliance de succursale de petite taille
410-SE	Appliance de succursale de petite taille
1000-SE	Appliance de succursale de petite taille
1100-SE	Appliance de succursale de grande taille
2000-SE	Appliance de succursale de grande taille
2100-SE	Appliance de succursale de grande taille
4100-SE	Centre de données - Appliance MCN (Master Control Node)
5100-SE	Centre de données - Appliance MCN (Master Control Node)
6100-SE	Centre de données - Appliance MCN (Master Control Node)

Dispositifs matériels d'optimisation WAN SD-WAN (SD-WAN WANOP)

Voici les modèles d'appliance SD-WAN WAN Optimization (WANOP) pris en charge :

MODÈLES DE PLATE-FORME SD-WAN WANOP	RÔLE
WANOP 4100	Appliance de centre de données
WANOP 5100	Appliance de centre de données

Appliances virtuelles SD-WAN VPX (SD-WAN VPX-SE)

Voici les modèles d'appliance virtuelle SD-WAN VPX (VPX-SE) pris en charge :

MODÈLES DE PLATE-FORME SD-WAN VPX-SE	RÔLE
VPX 20-SE	MCN ou appliance cliente, petite succursale
VPX 50-SE	MCN ou appliance cliente, petite succursale
VPX 100-SE	MCN ou appliance cliente, petite succursale
VPX 200-SE	MCN ou appliance cliente, petite succursale
VPX 500-SE	MCN ou appliance cliente, petite succursale
VPX 1000-SE	MCN ou appliance cliente, petite succursale

Pour plus d'informations, consultez les [conditions préalables](#) de Citrix SD-WAN Virtual VPX Standard Edition.

Appliances virtuelles SD-WAN WANOP (SD-WAN VPX-WANOP)

Voici les modèles d'appliance virtuelle SD-WAN WANOP (VPX-WANOP) pris en charge :

SD-WAN VPX WANOP MODÈLES DE PLATE-FORME	RÔLE
WANOP VPX-2	Appliance de succursale de petite taille
WANOP VPX-6	Appliance de succursale de petite taille
WANOP VPX-10	Appliance de succursale de petite taille
WANOP VPX-20	Appliance de succursale de petite taille
WANOP VPX-50	Appliance de succursale de grande taille
WANOP VPX-100	Appliance de succursale de grande taille
WANOP VPX-200	Appliance de succursale de grande taille

Important

Dans la version 10.1, l'édition Enterprise Platform est rebaptisée « Premium Edition ».

Dispositifs matériels SD-WAN édition premium (SD-WAN PE)

Voici les modèles d'appliance SD-WAN Premium (Enterprise) Edition (SD-WAN PE) pris en charge :

MODÈLES DE PLATE-FORME SD-WAN EE	RÔLE
1000-PE	Grande succursale, appliance de centre de données
1100-PE	Grande succursale, appliance de centre de données
2000-PE	Grande succursale, appliance de centre de données
2100-PE	Grande succursale, appliance de centre de données
5100-PE	Grande succursale, appliance de centre de données
6100-PE	Grande succursale, appliance de centre de données

Fonctionnalités non prises en charge

Les fonctionnalités suivantes ne sont pas prises en charge sur les appliances Citrix SD-WAN 1000 SE/PE, Citrix SD-WAN 2000 SE/PE et Citrix SD-WAN 4000 SE :

- [IPv6](#)
- [Nouvelle interface utilisateur pour les appliances SD-WAN](#)
- [Modem USB LTE externe](#)
- [Gestion Inband](#)
- [Port de gestion utilisé comme interface de données](#)
- [Service proxy DNS](#)
- [Prise en charge 802.1x](#)
- [Configuration de secours](#)
- [Paramètres Day-0/Day-N](#)
- [ID de routeur dynamique](#)
- [Édition avancée](#)
- [Wi-Fi](#)
- [LTE](#)
- [Service Cloud Direct](#)
- [Équilibrage de charge ECMP](#)
- [LACP LAG](#)

Chemins d'accès

November 1, 2021

Le tableau suivant fournit des détails sur toutes les versions du logiciel Citrix SD-WAN vers lesquelles vous pouvez mettre à niveau, à partir des versions précédentes.

SD-WAN	11.1	11.0	10.2	10.1	10	9.3.5	9.3.4	9.3	9.2
SD-WAN 11.0	✓								
SD-WAN 10.2	✓	✓							
SD-WAN 10.1	✓	✓	✓						
SD-WAN 10	✓	✓	✓	✓					
SD-WAN 9.3.5	✓	✓	✓	✓	✓				
SD-WAN 9.3.4	—	—	—	—	—	✓			
SD-WAN 9.3	—	—	—	—	—	✓	✓		
SD-WAN 9.2	—	—	—	—	—	✓	✓	✓	
SD-WAN 9.1	—	—	—	—	—	✓	✓	✓	✓

Les informations sur les chemins de mise à niveau sont également disponibles dans le [Guide de mise à niveau Citrix](#).

Remarque

- Il est recommandé aux clients effectuant une mise à niveau depuis Citrix SD-WAN version 9.3.x d'effectuer une mise à niveau vers la version 10.2.8 avant de procéder à une mise à niveau vers une version majeure.
- Lors de la mise à niveau du logiciel, assurez-vous que la mise à niveau vers tous les sites connectés est terminée avant de procéder à l'activation. Si l'activation est effectuée avant la fin de la préparation en activant Ignorer incomplet, il se peut que le chemin virtuel ne parvienne pas avec MCN pour les sites vers lesquels la préparation était encore en cours. Pour restaurer le réseau, il est nécessaire d'effectuer manuellement la gestion locale des modifications pour ces sites.
- À partir de Citrix SD-WAN version 11.0.0, le système d'exploitation sous-jacent du logiciel SD-WAN est mis à niveau vers une version plus récente. Il nécessite un redémarrage automatique pour être effectué pendant le processus de mise à niveau. Par conséquent, le temps

prévu pour la mise à niveau de chaque appliance est augmenté d'environ 100 secondes. En outre, en incluant le nouveau système d'exploitation, la taille du package de mise à niveau transféré à chaque appliance de succursale est augmentée d'environ 90 Mo.

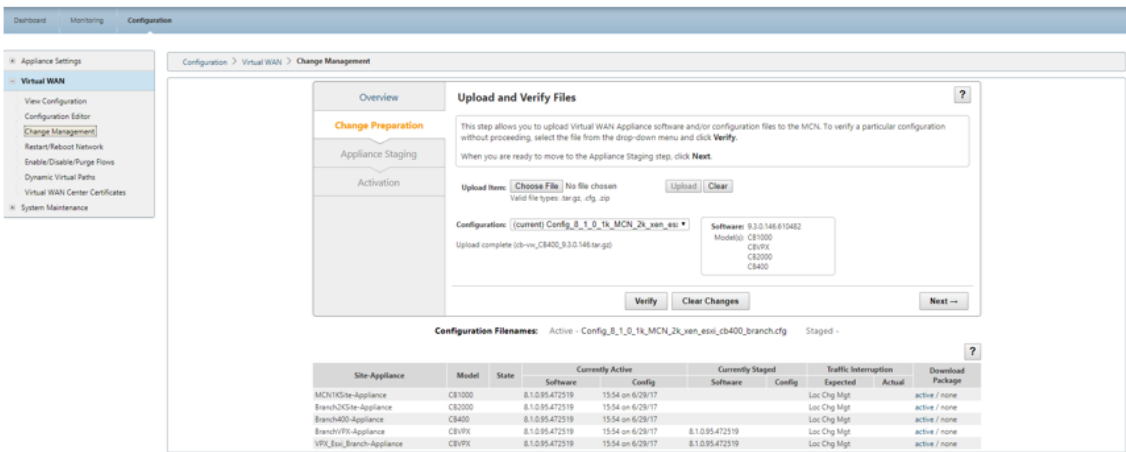
Mise à niveau du logiciel virtuel WAN vers la version 9.3.5 avec déploiement virtuel WAN

May 6, 2021

Remarque :

Avoir une configuration de réseau étendu virtuel fonctionnant sous la version 9.3.4 ou inférieure, avec des chemins virtuels établis à partir de MCN vers les sites de succursale.

1. Sur l'appliance MCN, accédez à **Configuration > Réseau étendu virtuel > Gestion des modifications**.
2. Obtenez le fichier `cb-vw-<ApplianceModel>-9.3.5.23.tar.gz` applicable à tous les sites du réseau WAN virtuel à partir de [page de téléchargement Citrix](#)
3. Téléchargez le fichier `cb-vw-<ApplianceModel>-9.3.5.23.tar.gz` pour les succursales définies dans le fichier de configuration pour lesquelles la mise à niveau doit être effectuée. Exécutez la gestion des modifications dans l'interface Web SD-WAN pour l'appliance MCN et terminez le processus de gestion des modifications.



4. Cliquez sur **Suivant** pour continuer.

The screenshots illustrate the 'Upload and Verify Files' process in the Citrix SD-WAN 11.4 interface. The first screenshot shows the 'Upload and Verify Files' dialog with a file selected. The second screenshot shows a 'Verification Results' dialog indicating success. The third screenshot shows a 'License' dialog with the Citrix License Agreement.

Configuration File Names: Active - Config_8_1_0_1k_MCN_2k_ven_esi_cb400_branch.cfg Staged -

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1Site-Appliance	CB1000	8.1.0.95.472519	1554 on 6/29/17				Loc Chg Mgt	active / none	
Branch2Site-Appliance	CB2000	8.1.0.95.472519	1554 on 6/29/17				Loc Chg Mgt	active / none	
Branch400-Appliance	CB400	8.1.0.95.472519	1554 on 6/29/17				Loc Chg Mgt	active / none	
BranchVPX-Appliance	CBVPX	8.1.0.95.472519	1554 on 6/29/17		8.1.0.95.472519		Loc Chg Mgt	active / none	
VPX_Esi_Branch-Appliance	CBVPX	8.1.0.95.472519	1554 on 6/29/17		8.1.0.95.472519		Loc Chg Mgt	active / none	

Verification Results

Status: Validation Success

This Configuration is valid. (version 1498754288)

Files created:

- Config_8_1_0_1k_MCN_2k_ven_esi_cb400_branch.xml
- Config_8_1_0_1k_MCN_2k_ven_esi_cb400_branch.xml.lst
- config_id_file.txt

License

CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). Your location of receipt of Citrix product (hereinafter "PRODUCT") and software maintenance (hereinafter "MAINTENANCE") determines the providing entity hereunder. Citrix Systems, Inc., a Delaware corporation, licenses the PRODUCT and provides MAINTENANCE in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., licenses the PRODUCT and provides MAINTENANCE in Europe, the Middle East, and Africa. Citrix Systems Asia Pacific Pty Ltd, licenses the PRODUCT and provides MAINTENANCE in Asia and the Pacific (excluding Japan). Citrix Systems Japan KK licenses the PRODUCT and provides MAINTENANCE in Japan. BY INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT.

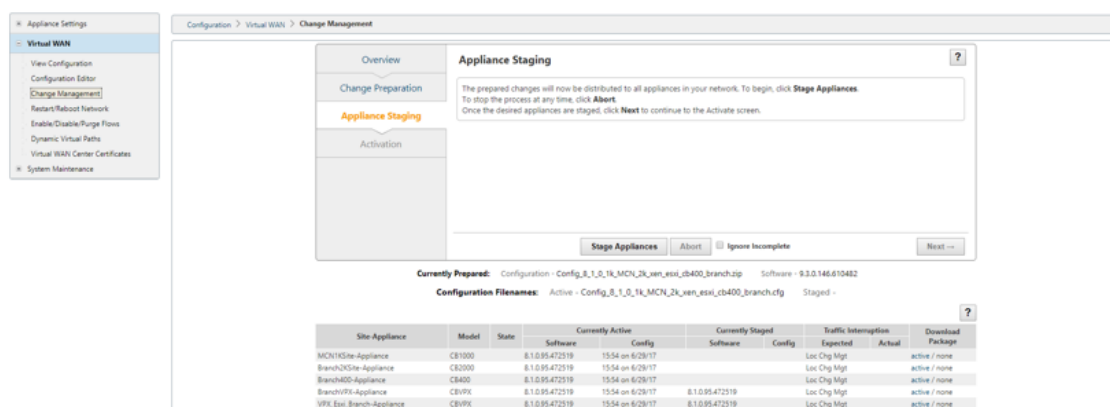
1. PRODUCT LICENSES.

a. End User Licenses. The PRODUCT is made available by CITRIX under the license models identified at <http://www.citrix.com/buy/licensing/product.html>. Notwithstanding anything set forth in this AGREEMENT or at the referenced website, your use of Open Source software shall in all ways be exclusively governed by the open source license indicated as applicable to the code at <http://www.citrix.com/buy/licensing/open-source.html>. "Open Source Software" means those portions of the PRODUCT that are made available by CITRIX under an open source license (e.g., a version of a GNU General Public License).

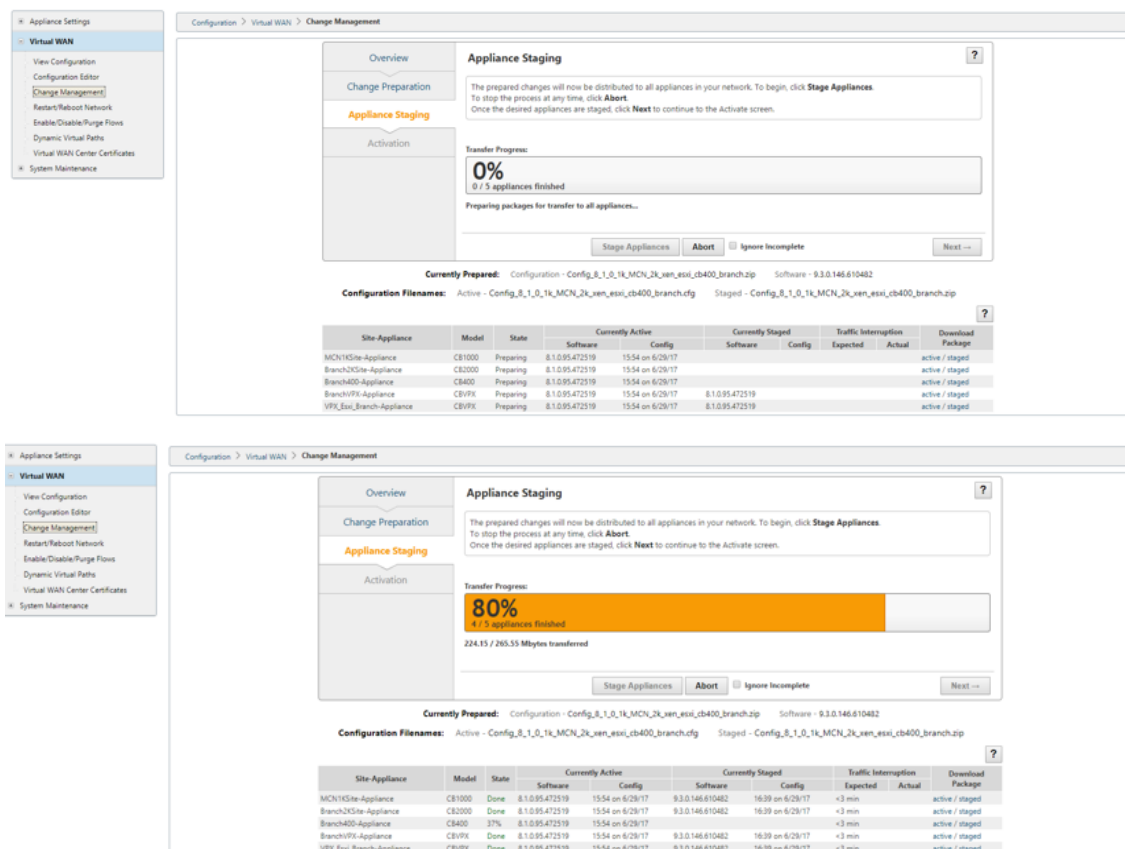
You must accept the license terms before installing the new package.

☒ I accept the End User License Agreement.

5. Après avoir accepté le contrat de licence, vous accédez à **Appliance Staging**, où les appliances peuvent être déployées en cliquant sur **Appliances Stage**.



6. L'état de progression du transfert s'affiche dans le cadre de la préparation et du transfert des packages logiciels vers les appliances.



7. Cliquez sur **Suivant** lorsque la progression du transfert affiche 100 %, et le bouton est activé pour continuer.

Configuration > Virtual WAN > Change Management

Overview

Appliance Staging

The prepared changes will now be distributed to all appliances in your network. To begin, click **Stage Appliances**. To stop the process at any time, click **Abort**. Once the desired appliances are staged, click **Next** to continue to the Activate screen.

Transfer Progress: **100%**

Appliance Staging complete. You may now proceed to Activation.

Stage Appliances Abort Ignore Incomplete Next →

Currently Prepared: Configuration - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.zip Software - 9.3.0.146.610482

Configuration Filenames: Active - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.cfg Staged - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.zip

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1Site-Appliance	CB1000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch2Site-Appliance	CB2000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch400-Appliance	CB400	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
BranchVPX-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
VPX_Essl_Branch-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged

8. Dans la page **Activation**, cliquez sur **Activer le déploiement** pour commencer l'activation.

Configuration > Virtual WAN > Change Management

Overview

Activate

You may now activate the changes that have been distributed across your network. Each appliance will apply the changes and restart the Virtual WAN Service.

Note: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve.

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds ▼

Activate Staged Abort Done

Currently Prepared: Configuration - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.zip Software - 9.3.0.146.610482

Configuration Filenames: Active - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.cfg Staged - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.zip

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1Site-Appliance	CB1000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch2Site-Appliance	CB2000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch400-Appliance	CB400	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
BranchVPX-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
VPX_Essl_Branch-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged

Citrix CloudBridge 1000-100-VW

10.105.199.28 says:

This will switch the Currently Active software/configuration on the network to the version in the Currently Staged area. Are you sure you want to begin Activation?

OK Cancel

Configuration > Virtual WAN > Change Management

Overview

Activate

You may now activate the changes that have been distributed across your network. Each appliance will apply the changes and restart the Virtual WAN Service.

Note: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve.

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds ▼

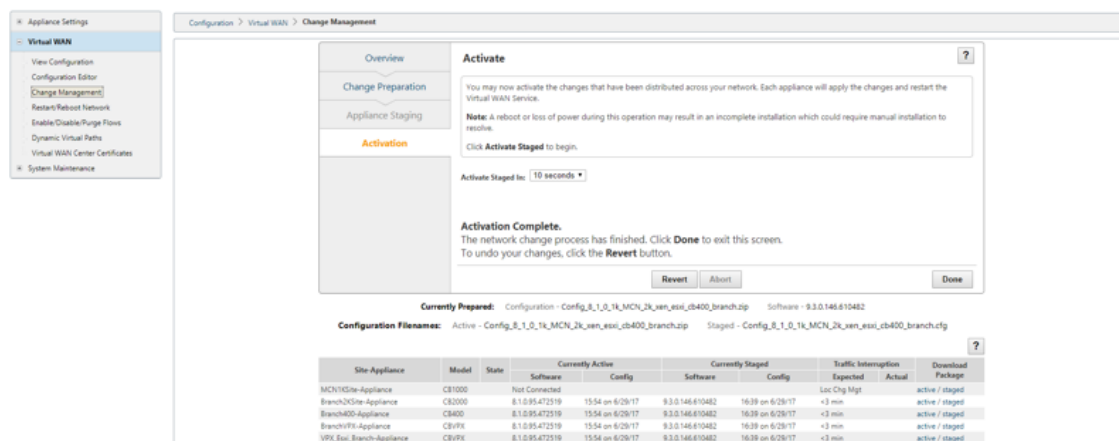
Activate Staged Abort Done

Currently Prepared: Configuration - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.zip Software - 9.3.0.146.610482

Configuration Filenames: Active - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.cfg Staged - Config_8_1_0_1k_MCN_2k_van_essl_cb400_branch.zip

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1Site-Appliance	CB1000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch2Site-Appliance	CB2000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch400-Appliance	CB400	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
BranchVPX-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
VPX_Essl_Branch-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged

9. Après l'achèvement du compte à rebours d'activation de 180 s cliquez sur **Terminé**.



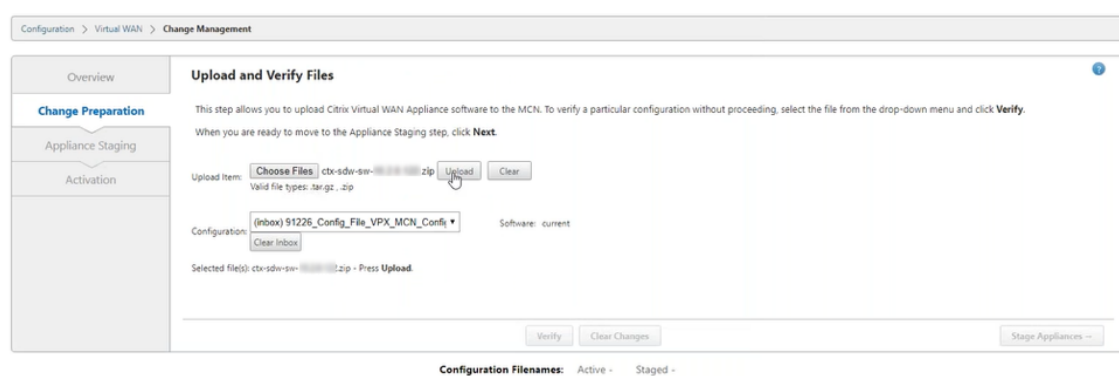
Mise à niveau vers la version 11.4 avec le déploiement Virtual WAN

November 1, 2021

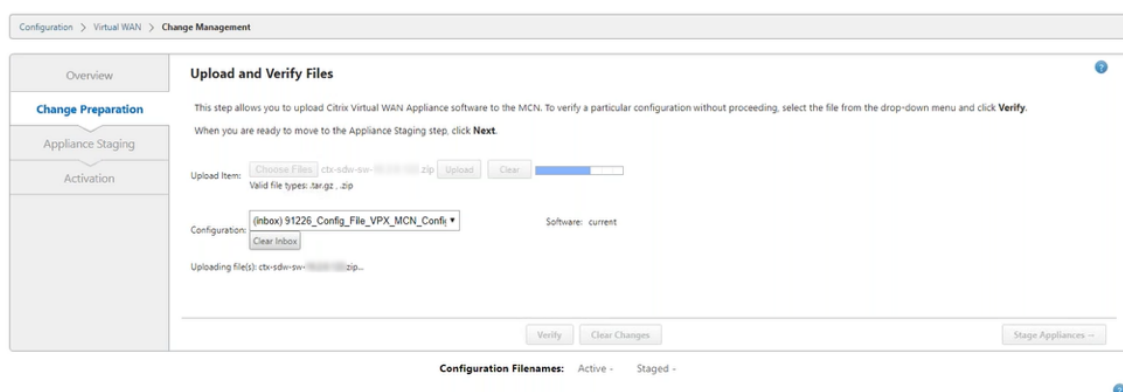
1. Dans la page **Gestion des modifications > Préparation** des modifications, cliquez sur **Choisir les fichiers** et sélectionnez le fichier de package logiciel *ctx-sdw-sw-11.4.0.x.zip* . Cliquez sur **Charger**.

Remarque :

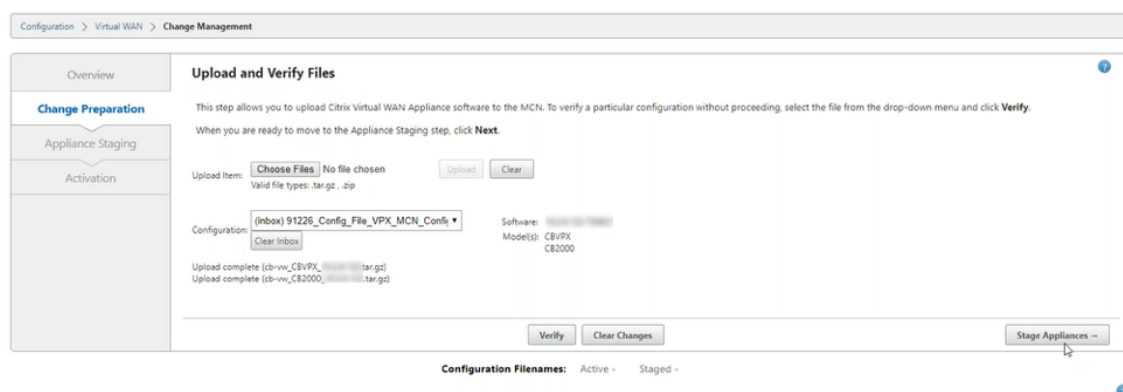
Vous pouvez télécharger le package logiciel Citrix SD-WAN version 11.4 à partir de la page [Téléchargements](#) .



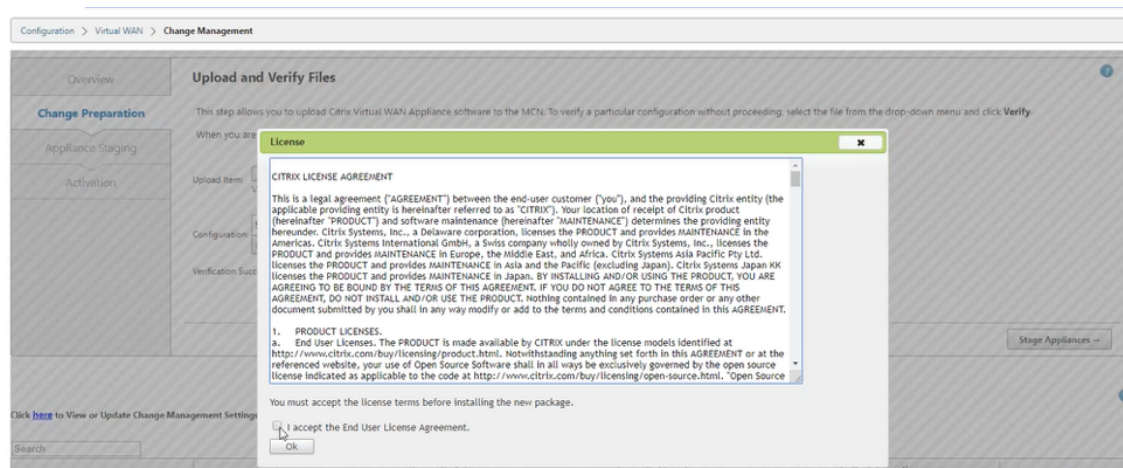
Une barre de progression apparaît pour afficher la progression actuelle du téléchargement.



2. Une fois le processus de téléchargement réussi, les modèles d'appliance appropriés s'affichent. Les appliances seront mises à niveau en fonction du fichier de configuration.



3. Cliquez sur **Stage Appliance** pour procéder à la validation du fichier de configuration. La page Contrat de licence pour l'acceptation de l'utilisateur s'affiche. Cliquez sur **J'accepte le contrat de licence de l'utilisateur final**, puis cliquez sur **OK**.



4. Le processus **de préparation de l'appliance** est lancé. Les modifications sont distribuées à toutes les appliances du réseau. La barre de progression du transfert apparaît et la table des détails du site est mise à jour.

Overview

Change Preparation

Appliance Staging

Activation

Appliance Staging

The prepared changes will now be distributed to all appliances in your network.
To stop the process at any time, click **Abort**.
Once the desired appliances are staged, click **Next** to continue to the Activate screen.

Transfer Progress:

0%

0 / 3 appliances finished

Prepare Packages (0 / 3 packages prepared)

Stage Packages

Done

Abort

Ignore Incomplete

Next

Currently Prepared: Configuration - 91226_Config_File_VPX_MCN_Config_test.zip Software -

Configuration Filenames: Active - Staged -

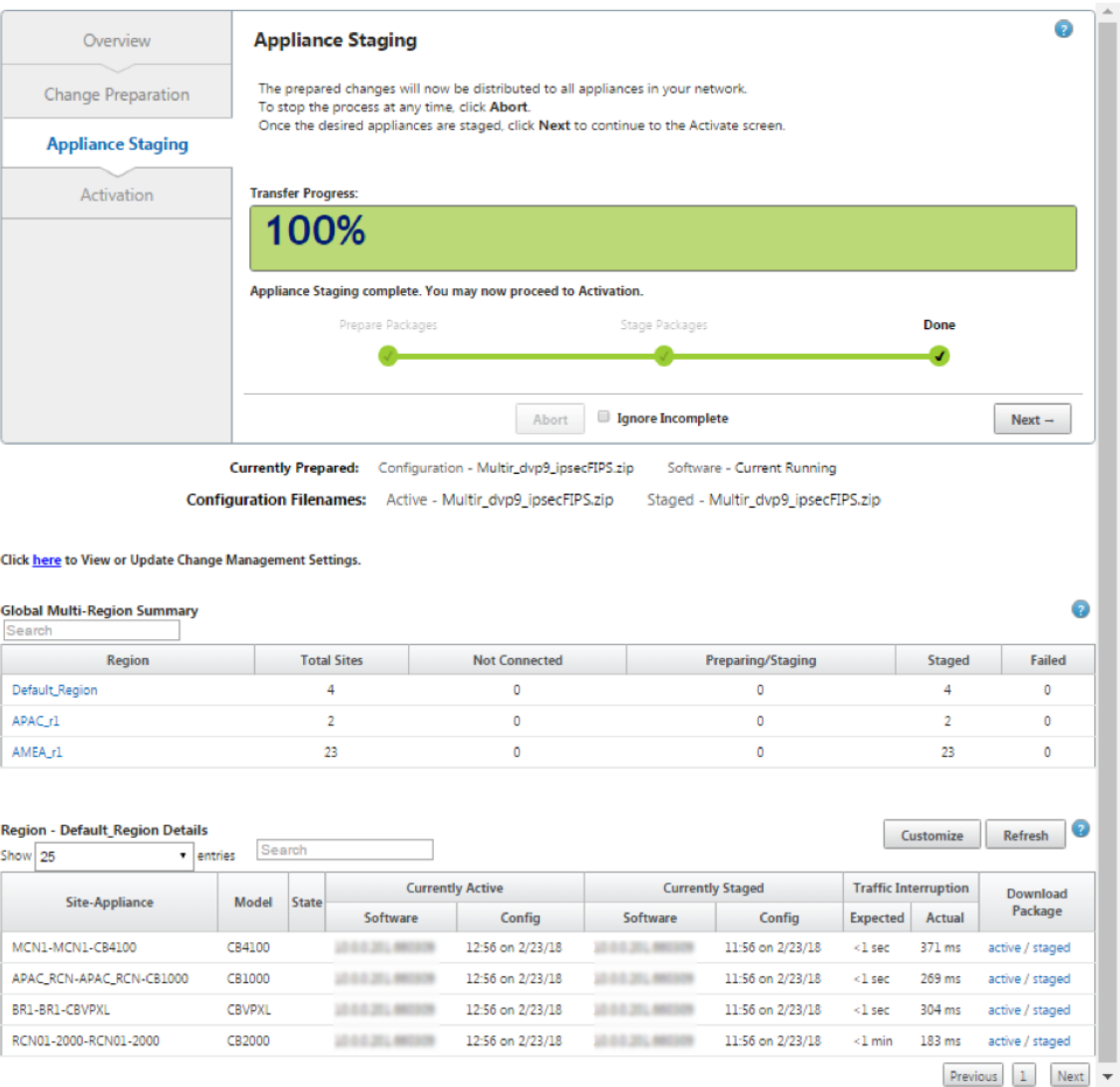
Click [here](#) to View or Update Change Management Settings.

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
CB2k8Branch-Branch	CB2000	Preparing	Not Connected				Loc Chg Mgt		none / staged
CBVPXBranch-Branch	CBVPX	Preparing	Not Connected				Loc Chg Mgt		none / staged
CBVPX_MCN-Appliance	CBVPX	Preparing	Not Connected				Loc Chg Mgt		none / staged

Activate Windows

5. Une fois la progression du transfert terminée à 100 %, cliquez sur **Suivant** pour passer à l'activation.



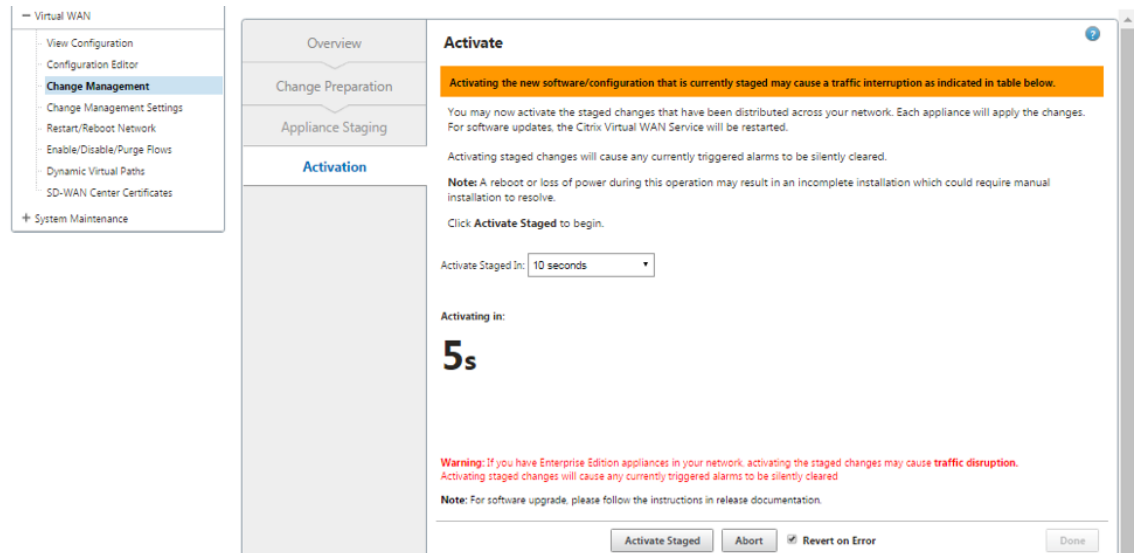
Les différents états de configuration des progiciels affichés dans le tableau récapitulatif indiquent ce qui suit :

- **Préparation** : traitement local pour préparer le package de mise à jour en vue de son transfert vers l’appliance.
- **Préparation des packages de région** - Traitement local pour préparer le package de mise à jour en vue de son transfert vers RCN. (Applicable si RCN fait partie du réseau).
- **Pourcentage : pourcentage** du package transféré vers l’appliance.
- **Décompression** : traitement à distance de l’appliance pour appliquer le package de mise à jour.
- **Transfert de région** - Le package est en cours de transfert vers RCN. (Applicable si RCN fait partie du réseau).
- **Échec** : transfert incomplet détecté à distance.
- **Annulé** - Annulé par l’utilisateur lorsque la case « Ignorer incomplet » a été cochée pendant

les appliances Stage

- **Non nécessaire** - Le package préparé ne comprend pas ce nom de site-appliance.
- **Non connecté** : le service local ne peut pas voir les informations du package actif de la télécommande.

6. Cliquez sur **Activate Staged** pour activer le logiciel mis en scène.



7. Après le compte à rebours, un message indique que l'activation est terminée. Cliquez sur **Terminé**.

View Configuration

Configuration Editor

Change Management

Change Management Settings

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

System Maintenance

Overview

Change Preparation

Appliance Staging

Activation

Activate

Activating the new software/configuration that is currently staged may cause a traffic interruption as indicated in table below.

You may now activate the staged changes that have been distributed across your network. Each appliance will apply the changes. For software updates, the Citrix Virtual WAN Service will be restarted.

Activating staged changes will cause any currently triggered alarms to be silently cleared.

Note: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve.

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Activation Complete.
The network change process has finished. Click **Done** to exit this screen.
To undo your changes, click the **Revert** button.

Revert Abort Done

Currently Prepared: Configuration - Multir_dvp9_ipsecFIPS.zip Software - Current Running

Configuration Filenames: Active - Multir_dvp9_ipsecFIPS.zip Staged - Multir_dvp9_ipsecFIPS.zip

Click [here](#) to View or Update Change Management Settings.

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	4	0	0	0	0
AMEA_r1	23	0	0	0	0
APAC_r1	2	0	0	0	0

Region - Default_Region Details

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	13:15 on 2/23/18	13:15 on 2/23/18	13:43 on 2/23/18	13:43 on 2/23/18	0 sec		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	13:15 on 2/23/18	13:15 on 2/23/18	13:43 on 2/23/18	13:43 on 2/23/18	0 sec		active / staged
BR1-BR1-CBV9XL	CBV9XL	Done	13:15 on 2/23/18	13:15 on 2/23/18	13:43 on 2/23/18	13:43 on 2/23/18	0 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	13:15 on 2/23/18	13:15 on 2/23/18	13:43 on 2/23/18	13:43 on 2/23/18	0 sec		active / staged

Previous 1 Next

8. Accédez à la page **Gestion des modifications** pour afficher l'état du transfert.

Configuration > Virtual WAN > Change Management

Details

Active Configuration:
_MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Staged Configuration:
_MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Prepared Configuration:
_MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Overview

Change Preparation

Appliance Staging

Activation

Step 1
Upload Files to MCN

Step 2
Transfer Files to Clients

Step 3
Activate Change

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a previously-staged appliance package (if present).

Activate Staged

Begin →

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Connected	Traffic Impacted	No Traffic Impact	Staging		
						In Progress	Completed	Failed
Default_Region	4	0	4	4	0	2	0	
region2	2	1	1	0	2	1	0	
region1	4	1	3	2	2	1	0	

Region - region1 Details of Traffic Impacted Sites

Show 25 entries Search

Customize

Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
R1-Site1-BLR-R1-Site1-BLR-CBVPX	VPX		10.2.0.116.790215	11:34 on 12/10/18	10.2.0.117.790216	6:30 on 12/10/18	<3 min	194 ms	active / staged
R1-Site1-BLR-New_HA_Appliance	VPX		10.2.0.116.790215	11:34 on 12/10/18	10.2.0.117.790216	6:30 on 12/10/18	<3 min	192 ms	active / staged

Previous

1

Next

Le tableau récapitulatif multi-régions fournit les détails suivants :

- **Region** : nom de la région
- **Site total** : nombre total de sites dans la région.
- **Non connecté** : nombre total de sites non connectés dans la région.
- **Connected** : nombre total de sites connectés dans la région.
- **Traffic impacted** : nombre total de sites sur lesquels le trafic est impacté dans la région.
- **Aucun impact sur le trafic** : nombre total de sites sur lesquels le trafic n'est pas affecté dans la région.
- **Staging In Progress** : nombre total de sites pour lesquels le traitement local tente de préparer le package de mise à jour pour le transfert dans la région.
- **Staging Completed** : nombre total de sites pour lesquels la préparation est terminée dans la région.
- **Échec de la préparation** : nombre total de sites pour lesquels le transfert incomplet a été supprimé dans la région.

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Connected	Traffic Impacted	No Traffic Impact	Staging		
						In Progress	Completed	Failed
Default_Region	4	0	4	4	0	0	2	0
region2	2	1	1	0	2	0	1	0
region1	4	1	3	2	2	0	1	0

Cliquez sur le lien d’entrée de la table **Global Multi-Region Summary** pour filtrer les rapports de configuration spécifiques à la région.

Region - Default_Region Details of Connected Sites

Customize Refresh

Show 25 entries Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-NY-MCN-NY-CB2000	2000		10.0.0.116.7500/16	11:34 on 12/10/18	10.0.0.117.7500/16	6:30 on 12/10/18	<3 min	82 s	active / staged
Def-Site1-SC-Def-Site1-SC-CBVPX	VPX		10.0.0.116.7500/16	11:34 on 12/10/18	10.0.0.117.7500/16	6:30 on 12/10/18	<3 min	209 s	active / staged
R1-RCN-MUM-R1-RCN-MUM-CBVPX	VPX	Done(auto)	10.0.0.116.7500/16	11:34 on 12/10/18	10.0.0.117.7500/16	6:30 on 12/10/18	<3 min	195 s	active / staged
R2-RCN-SA-R2-RCN-SA-CBVPX	VPX	Done(auto)	10.0.0.116.7500/16	11:34 on 12/10/18	10.0.0.117.7500/16	6:30 on 12/10/18	<3 min	199 s	active / staged

Previous 1 Next

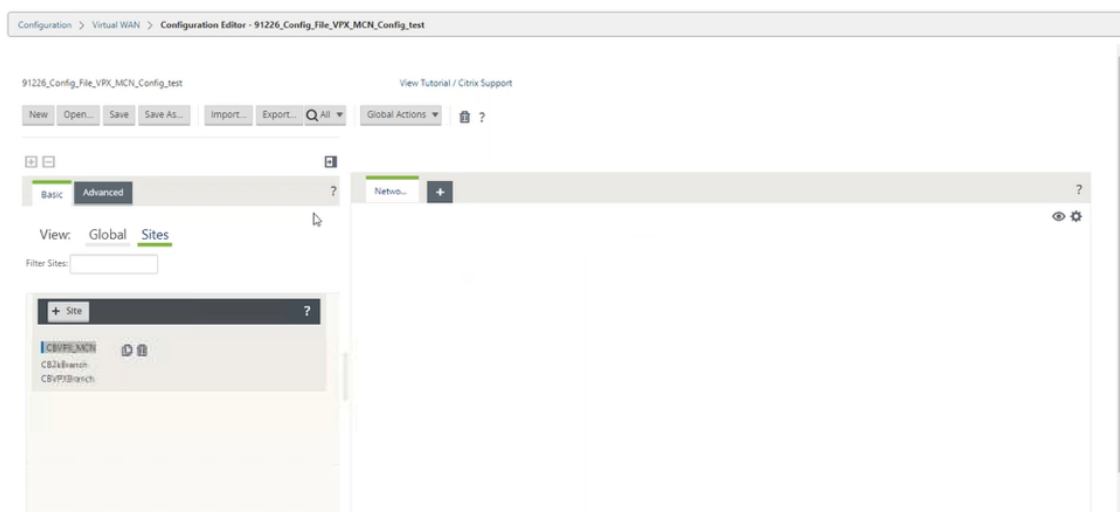
Pour un déploiement multirégion, sur chaque RCN, accédez à la page **Paramètres de gestion des modifications** et planifiez l’installation des composants dépendants. Par défaut, le MCN/RCN attribue des programmes d’installation qui doivent être tentés tous les jours à 21h20 en fonction de la disponibilité du logiciel dans les succursales.Pour plus d’informations, voir [Paramètres de gestion des modifications](#)

Mise à niveau vers la version 11.4 sans travail de déploiement WAN virtuel

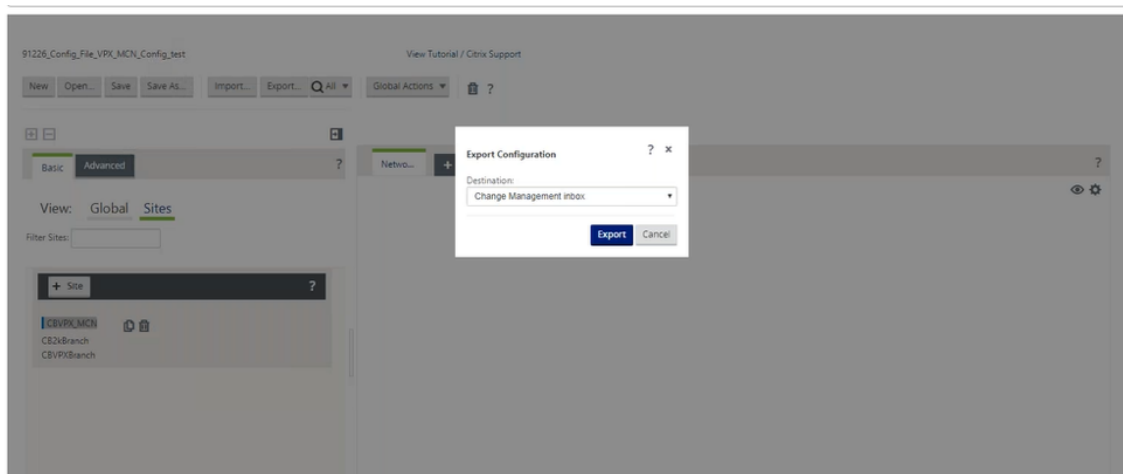
November 1, 2021

Remarque : Pour configurer les dernières fonctionnalités de la version 11.4, réimager l’appliance MCN vers le logiciel 11.4. Pour plus d’informations, voir [Réimager le logiciel de l’appliance Citrix SD-WAN](#)

1. Préparez la configuration à l’aide **de l’Éditeur** de configuration et enregistrez la configuration avec un nom valide. Pour plus d’informations, consultez [la rubrique Configuration](#) .



2. Exportez la configuration enregistrée vers Change Management. Cliquez sur **Exporter** et sélectionnez **Boîte de réception Change Management** comme destination. Cliquez sur **Exporter**.



3. Dans la page **Gestion des modifications > Préparation** des modifications, cliquez sur **Choisir les fichiers** et sélectionnez le fichier de package logiciel *ctx-sdw-sw-11.4.0.x.zip* . Cliquez sur **Charger**.

Remarque :

Vous pouvez télécharger le package logiciel Citrix SD-WAN version 11.4 à partir de la page [Téléchargements](#) .

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

This step allows you to upload Citrix Virtual WAN Appliance software to the MCN. To verify a particular configuration without proceeding, select the file from the drop-down menu and click **Verify**.

When you are ready to move to the Appliance Staging step, click **Next**.

Upload Item:

Choose Files

 ctx-sdw-sw-...zip

Upload

Clear

Valid file types: .tar.gz, .zip

Configuration:

(inbox) 91226_Config_File_VPX_MCN_Config

Clear Inbox

 Software: current

Selected file(s): ctx-sdw-sw-10.20.122.zip - Press **Upload**.

Verify

Clear Changes

Stage Appliances --

Configuration Filenames: Active - Staged -

Click [here](#) to View or Update Change Management Settings.

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Change Management was unable to display the sites in your network. This can occur if there is no configuration file on your appliance.									

Une barre de progression apparaît pour afficher la progression actuelle du téléchargement.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

This step allows you to upload Citrix Virtual WAN Appliance software to the MCN. To verify a particular configuration without proceeding, select the file from the drop-down menu and click **Verify**.

When you are ready to move to the Appliance Staging step, click **Next**.

Upload Item:

Choose Files

 ctx-sdw-sw-...zip

Upload

Clear

Valid file types: .tar.gz, .zip

Configuration:

(inbox) 91226_Config_File_VPX_MCN_Config

Clear Inbox

 Software: current

Uploading file(s): ctx-sdw-sw-...zip...

Verify

Clear Changes

Stage Appliances --

Configuration Filenames: Active - Staged -

Click [here](#) to View or Update Change Management Settings.

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Change Management was unable to display the sites in your network. This can occur if there is no configuration file on your appliance.									

4. Une fois le processus de téléchargement réussi, les modèles pertinents sont affichés et doivent être mis à niveau en fonction du fichier de configuration contenant des informations sur chaque modèle de plate-forme de branche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

104

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

This step allows you to upload Citrix Virtual WAN Appliance software to the MCN. To verify a particular configuration without proceeding, select the file from the drop-down menu and click **Verify**. When you are ready to move to the Appliance Staging step, click **Next**.

Upload Item: **Choose Files** No file chosen **Upload** **Clear**

Valid file types: tar.gz, .zip

Configuration: **(inbox) 91226_Config_File_VPX_MCN_Config** **Clear Inbox**

Software: **CBVPX**
Model(s): **CB2000**

Upload complete (cb-vw, CBVPX, tar.gz)
Upload complete (cb-vw, CB2000, tar.gz)

Verify **Clear Changes** **Stage Appliances**

Configuration Filenames: Active - Staged -

Click [here](#) to View or Update Change Management Settings.

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Change Management was unable to display the sites in your network. This can occur if there is no configuration file on your appliance.									

5. Cliquez sur **Stage Appliance** pour procéder à la validation du fichier de configuration. La page Contrat de licence pour l'acceptation de l'utilisateur s'affiche. Cliquez sur **J'accepte le contrat de licence de l'utilisateur final**, puis cliquez sur **OK**.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

This step allows you to upload Citrix Virtual WAN Appliance software to the MCN. To verify a particular configuration without proceeding, select the file from the drop-down menu and click **Verify**. When you are ready to move to the Appliance Staging step, click **Next**.

Upload Item: **Choose Files** No file chosen **Upload** **Clear**

Valid file types: tar.gz, .zip

Configuration: **(inbox) 91226_Config_File_VPX_MCN_Config** **Clear Inbox**

Software: **CBVPX**
Model(s): **CB2000**

Upload complete (cb-vw, CBVPX, tar.gz)
Upload complete (cb-vw, CB2000, tar.gz)

Verify **Clear Changes** **Stage Appliances**

Configuration Filenames: Active - Staged -

Click [here](#) to View or Update Change Management Settings.

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Change Management was unable to display the sites in your network. This can occur if there is no configuration file on your appliance.									

CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). Your location of receipt of Citrix product (hereinafter "PRODUCT") and software maintenance (hereinafter "MAINTENANCE") determines the providing entity hereunder. Citrix Systems, Inc., a Delaware corporation, licenses the PRODUCT and provides MAINTENANCE in the Americas, Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., licenses the PRODUCT and provides MAINTENANCE in Europe, the Middle East, and Africa. Citrix Systems Asia Pacific Pty Ltd. licenses the PRODUCT and provides MAINTENANCE in Asia and the Pacific (excluding Japan). Citrix Systems Japan KK licenses the PRODUCT and provides MAINTENANCE in Japan. BY INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT.

1. PRODUCT LICENSES.

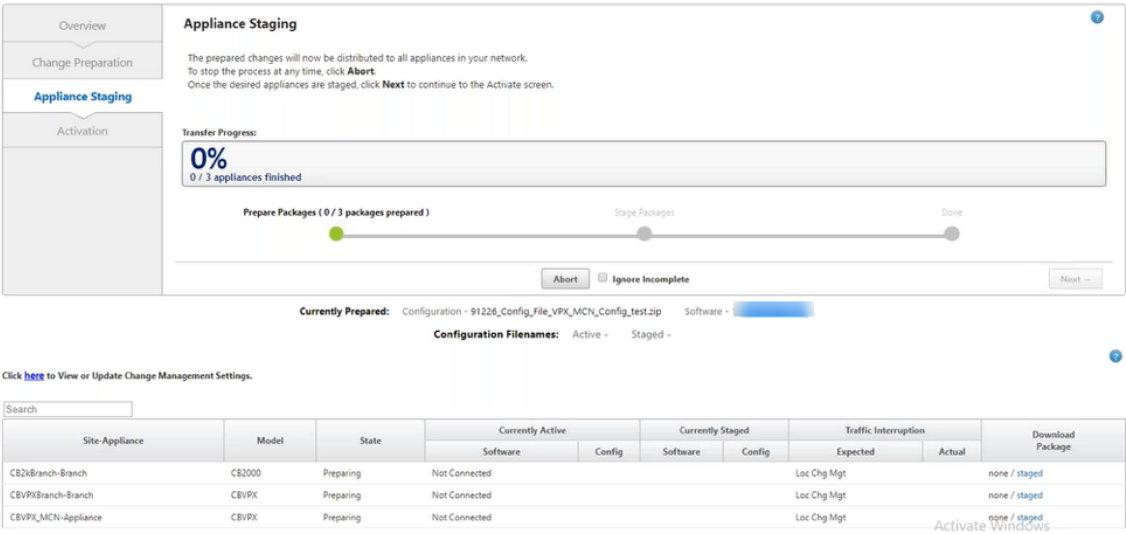
a. End User Licenses. The PRODUCT is made available by CITRIX under the license models identified at <http://www.citrix.com/buy/licensing/product.html>. Notwithstanding anything set forth in this AGREEMENT or at the referenced website, your use of Open Source Software shall in all ways be exclusively governed by the open source license indicated as applicable to the code at <http://www.citrix.com/buy/licensing/open-source.html>. "Open Source"

You must accept the license terms before installing the new package.

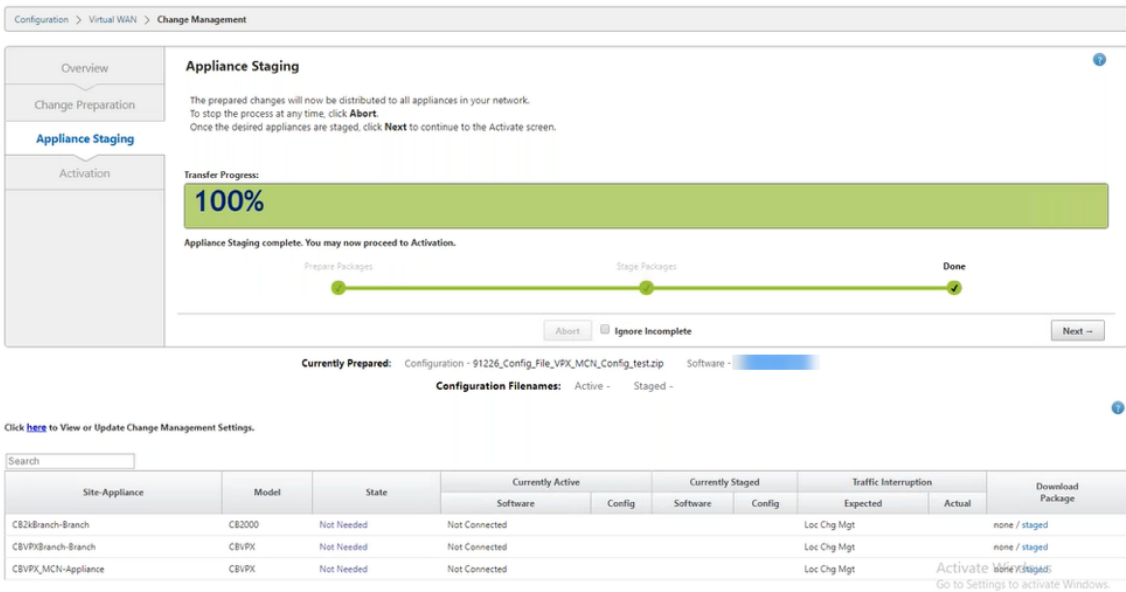
☐ I accept the End User License Agreement.

Ok

6. Le processus **de préparation de l'appliance** est lancé, les modifications seront distribuées à toutes les appliances du réseau. La barre de progression du transfert apparaît et la table des détails du site est mise à jour.

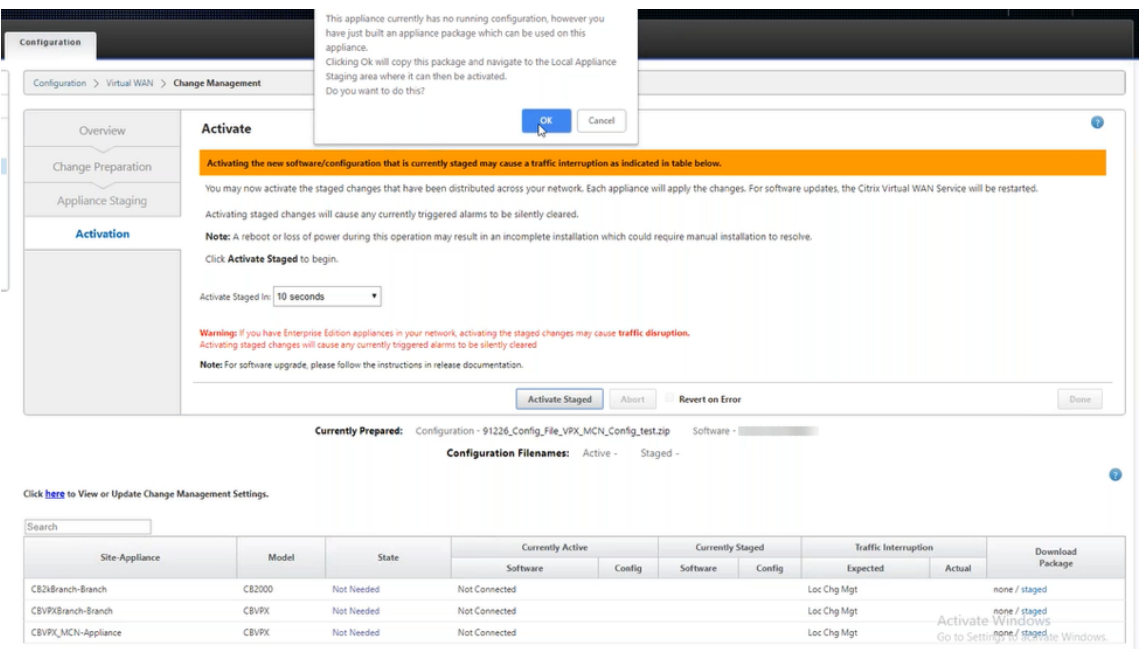


7. Une fois la progression du transfert terminée à 100 %, cliquez sur **Suivant** pour passer à l'activation.

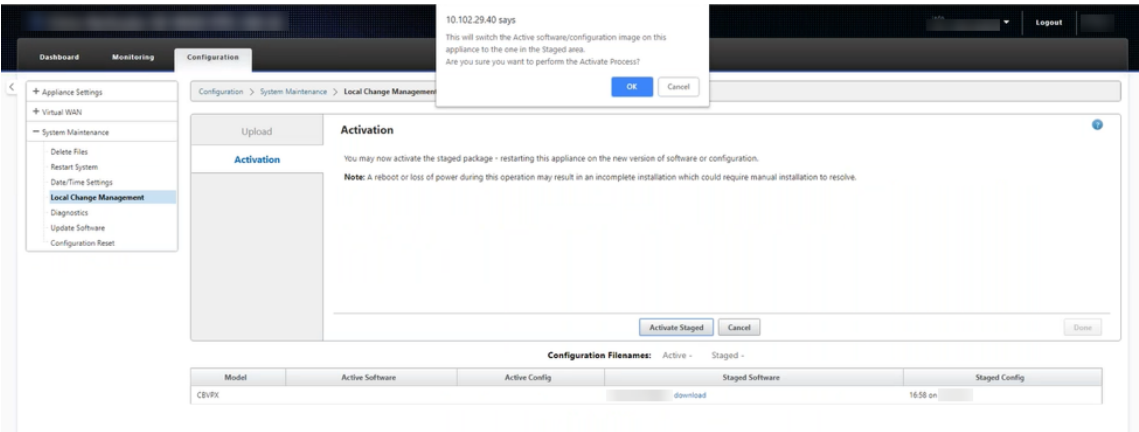


8. Cliquez sur **Activer le déploiement**. Un message contextuel d'acceptation de l'utilisateur s'affiche, car c'est la première fois que l'appliance est préparée.

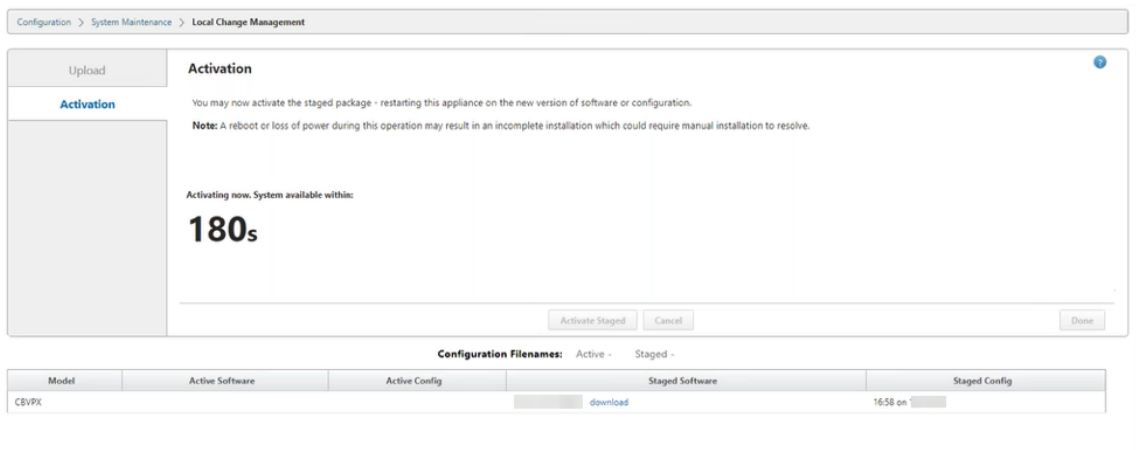
Vous êtes redirigé vers la page **Gestion des modifications locales** pour activer l'appliance locale. Cliquez sur **OK** pour continuer.



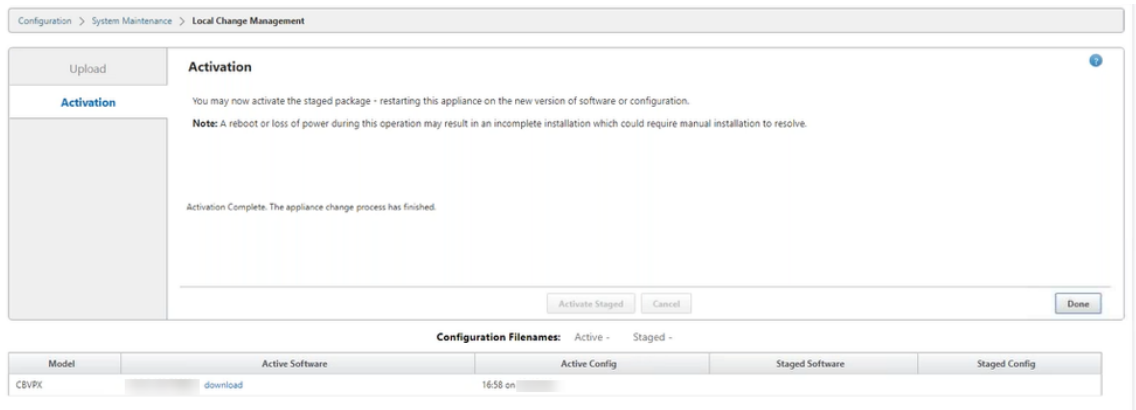
9. Cliquez sur **Activer la zone de** transition dans la gestion locale des modifications. Un message de confirmation d'activation s'affiche. Cliquez sur **OK**.



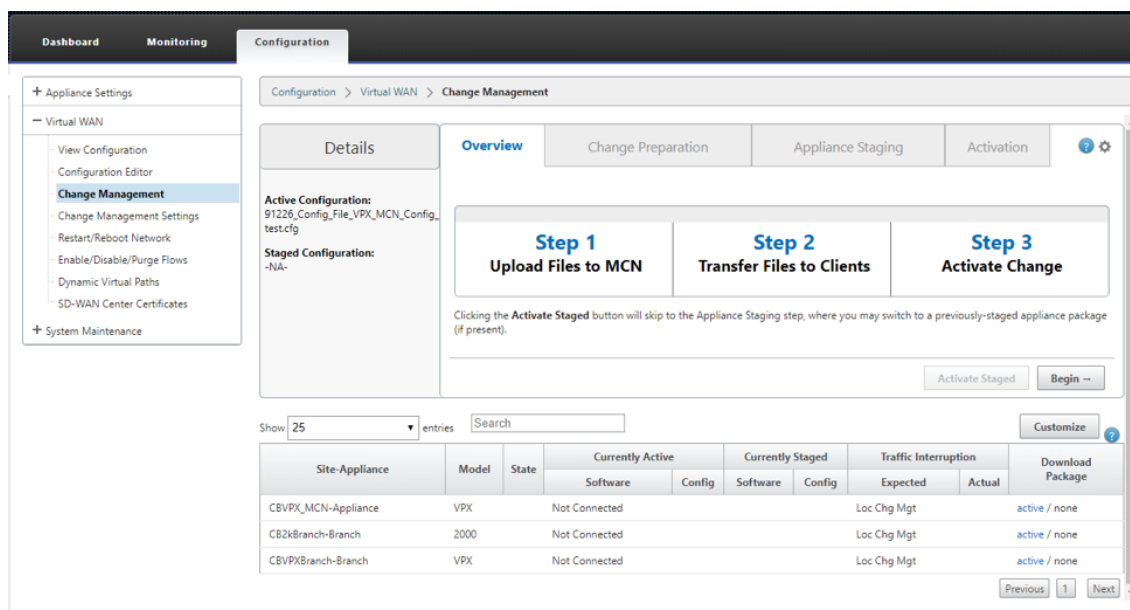
L'activation commence par un compte à rebours de 180 secondes.



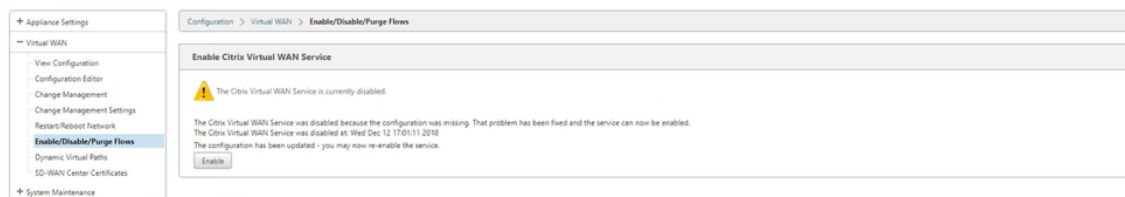
10. Après le compte à rebours, un message indique que l'activation est terminée. Cliquez sur **Terminé**, l'appliance redémarre.



11. Après le redémarrage de l'appliance, accédez à la page **Gestion des modifications** pour télécharger les packages locaux de gestion des modifications pour les branches respectives dont vous avez besoin pour démarrer sur le réseau avec la mise à niveau du logiciel Virtual WAN uniquement.



12. Activez le service SD-WAN sur l'apppliance. Accédez à **Virtual WAN > Activer/Désactiver/Purger les flux**, puis cliquez sur **Activer**.



Pour poursuivre la configuration et l'ajout de nouveaux sites au réseau, suivez la procédure décrite dans la rubrique [Configurer le nœud de branche](#).

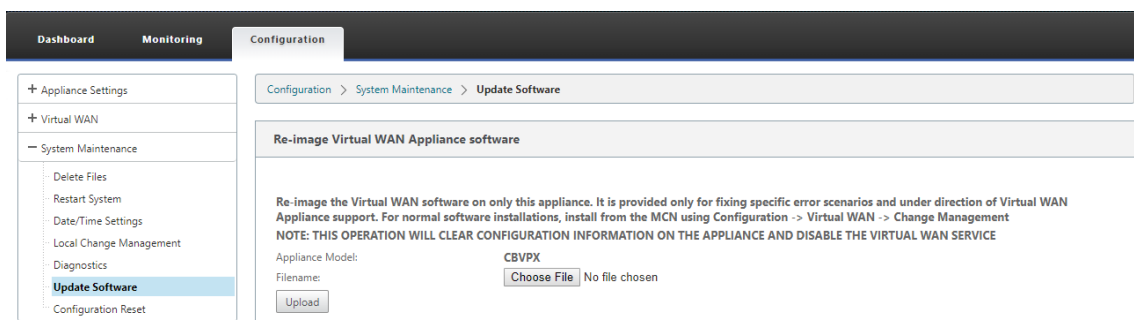
Réimager le logiciel de l'apppliance Citrix SD-WAN

May 6, 2021

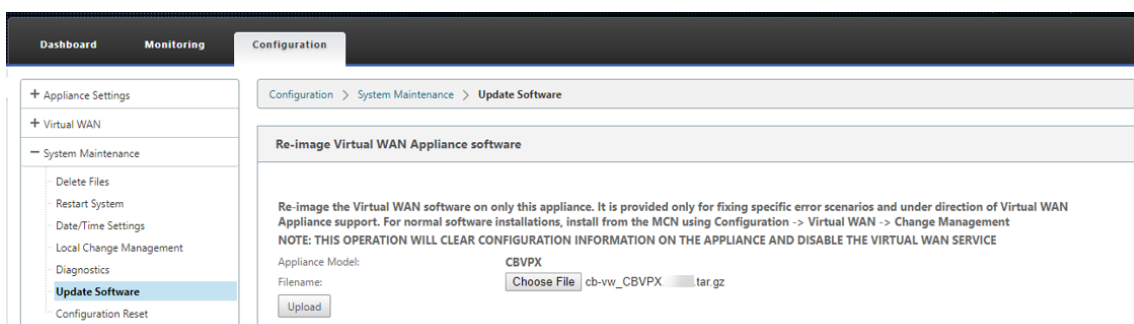
Téléchargez le fichier *.tar.gz* de la version et de la plate-forme logicielle Citrix SD-WAN requises à partir du [Téléchargements de Citrix](#) portail.

Pour réimager le logiciel de l'apppliance Citrix SD-WAN :

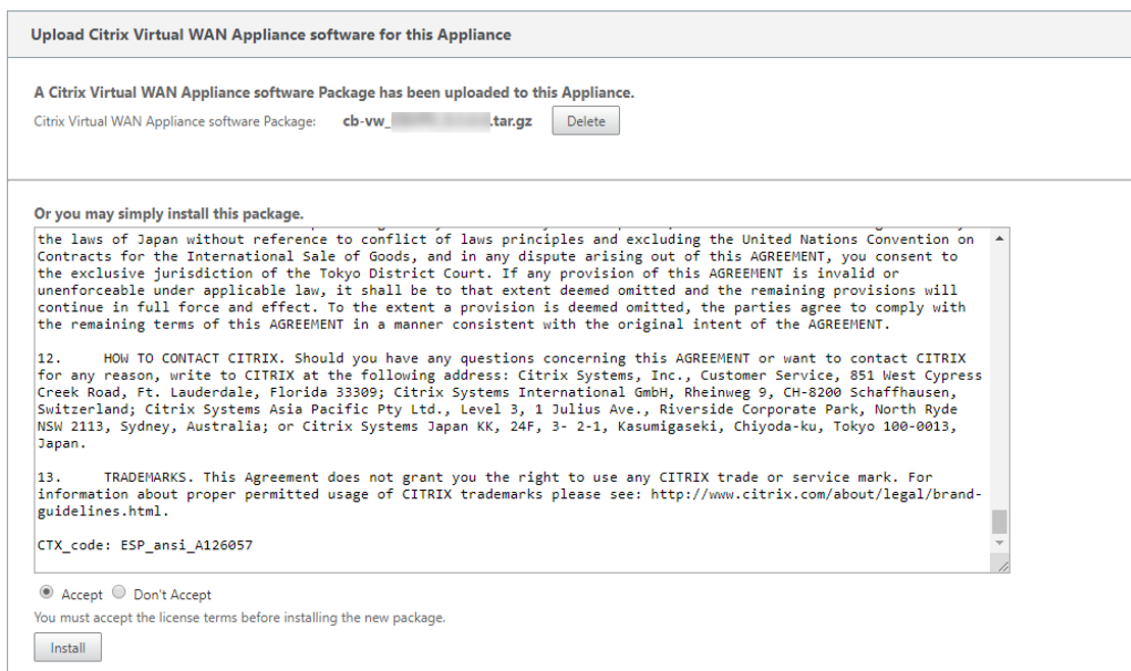
1. Dans l'interface graphique de l'apppliance SD-WAN, accédez à **Configuration > Maintenance du système > Mise à jour du logiciel**.



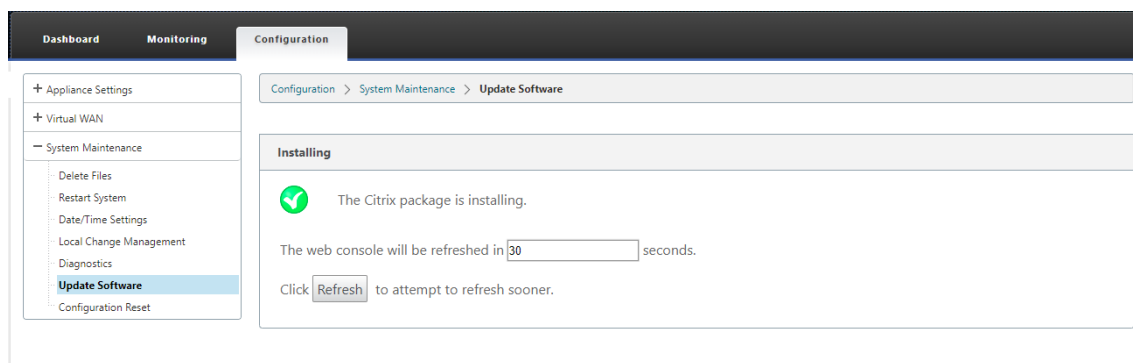
2. Cliquez sur **Choisir un fichier** et sélectionnez le logiciel Citrix SD-WAN téléchargé. Cliquez sur **Upload**.



3. Lire et accepter les termes de la licence. Cliquez sur **Accepter**, puis sur **Installer**.



La mise à jour logicielle prend environ 35 secondes, après quoi l'appliance redémarre.



Mise à niveau logicielle partielle à l'aide de la gestion des changements locaux

May 6, 2021

Important

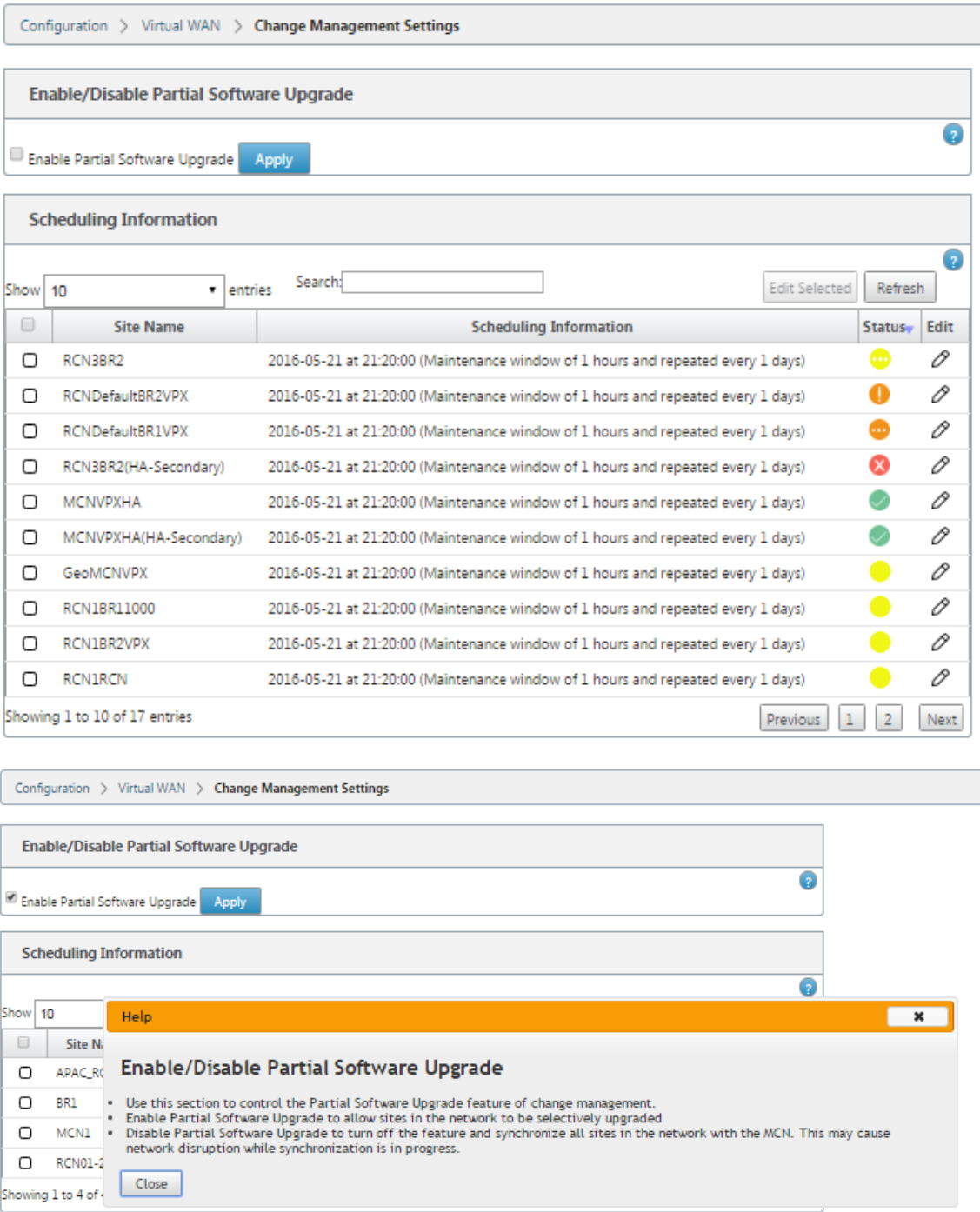
Par défaut, l'option **Mise à niveau logicielle partielle** est désactivée.

Vous pouvez installer une version plus récente du logiciel SD-WAN sur un sous-ensemble de sites clients à l'aide de l'option **Gestion des modifications locales**. Ceci est réalisé grâce à la fonctionnalité de mise à niveau logicielle partielle qui permet à l'administrateur réseau de mettre à niveau sélectivement le logiciel sur les sites du réseau sans avoir besoin de mettre à niveau tous les sites simultanément. Un cas d'utilisation spécifique de cette fonctionnalité est un administrateur qui teste le nouveau logiciel sur quelques sites de succursales avant de l'installer sur tous les sites du réseau.

Conditions préalables et exigences

Avant de procéder à une mise à niveau partielle du logiciel, consultez les exigences suivantes :

1. Avoir un logiciel SD-WAN actif version 10.0 ou plus récent. Activez la case **à cocher Activer la mise à niveau logicielle partielle**. Si vous décochez cette case, le logiciel actuellement en cours d'exécution sur l'appliance MCN est appliqué aux branches qui ont des chemins virtuels actifs en cours d'exécution.



2. Étapez une nouvelle version du logiciel à l'aide du processus de **gestion des modifications** MCN avec le même numéro de version Major que le logiciel actif et la même configuration que la configuration active.
3. Le nouveau logiciel devrait être la même version majeure du logiciel que le logiciel actif. La version mineure peut être une version différente du logiciel.
4. Le nouveau logiciel doit d'abord être remonté sur tous les sites à partir du MCN. Arrêter à l'étape

Activer l'étape Staged de gestion des modifications.

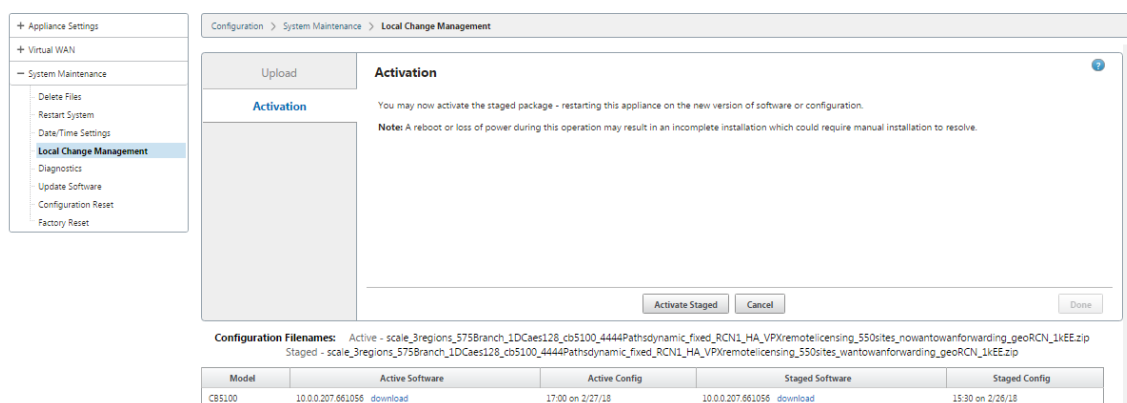
Pour la configuration du site Actif et Partiel, le logiciel doit être identique sur les sites MCN et Branch. Il n'est pas possible d'activer un jeu de fonctionnalités différent sur les sites partiellement mis à niveau. Passez à des sites individuels pour effectuer la **gestion des changements locaux**. Reportez-vous aux instructions ci-dessous pour le déploiement de haute disponibilité.

Pour effectuer une mise à niveau partielle du logiciel SD-WAN :

Il existe deux scénarios dans lesquels vous pouvez effectuer une mise à niveau logicielle SD-WAN partielle sur un nœud de succursale : le mode Haute disponibilité et le mode Non-Haute disponibilité.

Mise à niveau du nœud de succursale sans mode haute disponibilité

1. Dans l'interface de gestion Web Citrix SD-WAN, accédez au site de branche, qui doit être mis à niveau via le processus de mise à niveau partielle du site.
2. Ouvrez **Gestion des changements locaux**. Cliquez sur **Suivant**.
3. Cliquez sur **Activer le déploiement**. Chaque site de succursale sera maintenant installé avec une nouvelle version du logiciel.



Mise à niveau du nœud de succursale en mode haute disponibilité

1. Dans l'interface de gestion Web SD-WAN, accédez au site de la succursale, qui doit être mis à niveau via la mise à niveau partielle du site.
2. Désactivez le service sur l'appliance de secours.
3. Sur l'appliance principale, ouvrez **Gestion des modifications locales**.
4. Cliquez sur **Activer le déploiement**. cette appliance sera désormais installée avec une nouvelle version du logiciel.
5. Sur l'appliance de secours, ouvrez **Gestion des modifications locales**.

6. Cliquez sur **Activer le déploiement**. L'appliance de secours sera maintenant installée avec une nouvelle version logicielle.
7. Une fois que les appliances principales et de secours ont terminé le processus d'activation, activez le service sur l'appliance de secours.

Mise à niveau du réseau

Lorsque vous êtes prêt à synchroniser le réseau, accédez à l'écran de gestion des modifications du réseau MCN, puis cliquez sur **Activer le réseau préparé pour être déployé**.

Conversion WANOP vers Premium Edition avec USB

May 6, 2021

Remarque

Seules les appliances SD-WAN 1000 et 2000 WANOP peuvent être converties en appliances SD-WAN Premium Edition.

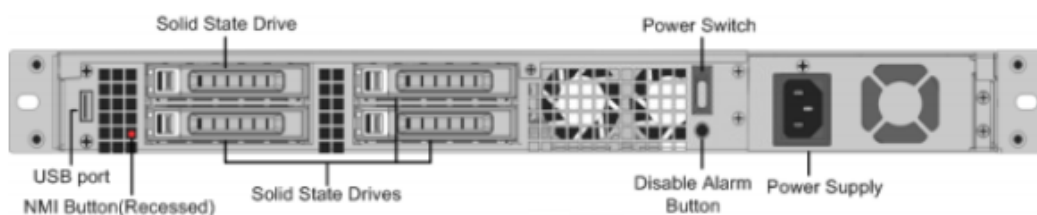
Avant de commencer

- Assurez-vous que vous convertissez uniquement l'appliance 1000, et non le 1000 WS. L'appliance 1000 WS ne prend pas en charge la conversion vers l'appliance SD-WAN Premium (Enterprise) Edition.
- Assurez-vous que vous disposez des informations d'identification par défaut pour vous connecter au *Dom-0 - root/nsroot* existant.

Procédure de mise à niveau

La procédure de conversion est un processus en deux étapes comprenant les étapes suivantes :

- Insérez une clé USB incluse dans l'appliance Citrix SD-WAN.
- Vérifiez que la console série est connectée et continuez le processus de conversion.



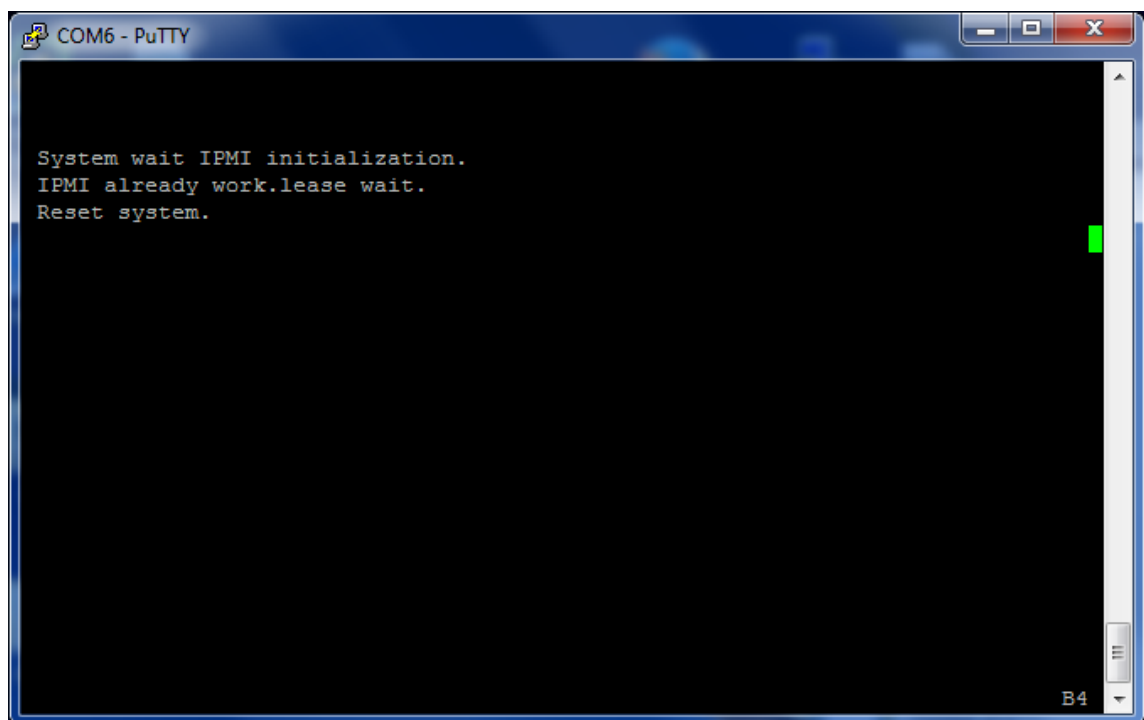
Comment convertir avec clé USB

Pour mettre à niveau l'appliance à l'aide d'une clé USB :

1. Insérez la clé USB incluse dans l'appliance Citrix SD-WAN.
2. Connectez-vous à la console série de l'appliance.
3. Redémarrez l'appliance.
4. Pendant le processus de démarrage, lorsque le curseur se déplace sur l'écran, procédez comme suit :
 - a) Appuyez longuement sur la touche **Echap** .
 - b) Appuyez longuement sur la **touche MAJ** .
 - c) Appuyez sur la touche numéro **1** (MAJ +1 = !) et relâchez toutes les touches.
 - d) Répétez les étapes a, b et c jusqu'à ce que le curseur cesse de se déplacer.

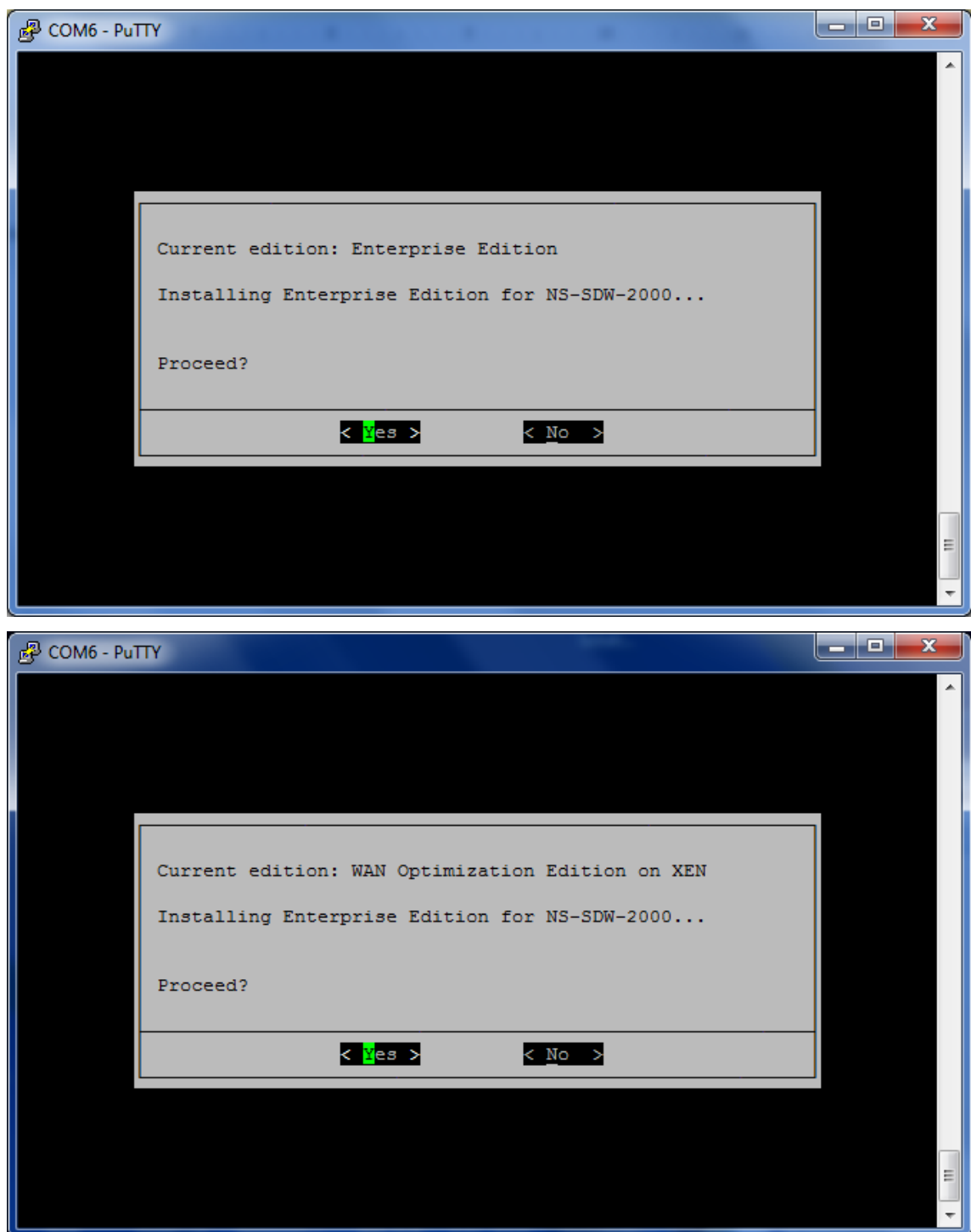
Remarque

Les étapes ci-dessus doivent être exécutées pendant le processus de redémarrage de l'appliance. Les coups de touche doivent se produire lors de la post-phase du BIOS, comme décrit à l'étape 4.



5. Lorsque le BIOS se charge, choisissez le lecteur USB externe, par exemple, PNY USB 2.0 FD 1100 pour démarrer l'appliance. Le lecteur USB externe est expédié par Citrix si vous l'avez commandé.

Vous devez choisir l'édition de la plate-forme que vous souhaitez utiliser, si la plate-forme prend en charge plusieurs éditions, telles que 1000 et 2000. Par conséquent, choisissez Premium (Enterprise) Edition d'abord avant de confirmer.



6. Choisissez l'option de mise à niveau logicielle **Enterprise Edition** lorsque vous y êtes invité.
7. Le processus de mise à niveau est terminé en 20-30 minutes. Le système redémarre après 1-2 minutes et l'invite de connexion s'affiche. Pour l'édition de la plate-forme 1000, le processus de mise à niveau est d'environ une heure car la mise à jour de la clé USB interne elle-même prend environ une demi-heure.

8. Débranchez la clé USB une fois la procédure terminée.



Références

- Pour obtenir des licences sur les produits Citrix SD-WAN, consultez le lien de support à l'adresse suivante : <http://support.citrix.com/article/ctx131110>
- Pour plus d'informations sur la documentation et les notes de mise à jour sur Citrix SD-WAN, consultez ; </en-us/citrix-sd-wan.html>.

Convertir Standard Edition en Premium Edition

May 6, 2021

Important

Dans la version 10.1, l'édition de la plate-forme « Enterprise » est rebaptisée « Premium ».

Pour effectuer la conversion de plate-forme de Standard Edition à Premium (Enterprise) Edition :

1. Exportez la configuration localement.
2. Téléchargez le **package actif** à partir de la page **Gestion des modifications**.
3. Mettez à niveau l'appliance à l'aide du package téléchargé à partir de **Maintenance du système** > **Mise à jour du logiciel** > **Réimager logiciel de l'appliance virtuelle WAN**.

4. Cliquez sur **Choisir un fichier** pour fournir le fichier *CB-VW_CB1000_x.x.x.tar.gz*. Où x.x.x.x est la version du logiciel SD-WAN.
5. Cliquez sur **Charger**. Sélectionnez **Accepter** et cliquez sur **Installer** pour continuer.
6. Installez la licence Premium (Enterprise) Edition.
7. Exécutez la **gestion locale des modifications** sur l'appliance à l'aide du package actif téléchargé à l'étape 2 ci-dessus.

Les conditions suivantes pour le provisionnement de l'optimisation WAN sont les suivantes :

1. Si le rôle de site est MCN, le provisionnement d'optimisation WAN se produit uniquement :
 - La mise à niveau logicielle est effectuée à l'aide du package .zip (SSUP)
 - La licence est PE
 - Le service WAN virtuel est activé
2. Si le rôle de site est Client, le provisionnement de l'optimisation WAN se produit uniquement :
 - La mise à niveau logicielle est effectuée à l'aide du package .zip (SSUP)
 - Le service WAN virtuel est activé
 - La licence est PE
 - Le chemin virtuel est formé avec MCN
3. Pour le provisionnement immédiat de l'optimisation WAN, définissez la valeur de la fenêtre de maintenance sur 0 dans la page Paramètres de gestion des modifications du site correspondant.

Utilitaire de réimageage USB

May 6, 2021

L'utilitaire de réimage USB SD-WAN permet de réutiliser le matériel en installant une image d'usine propre à partir d'une clé USB amorçable. Citrix fournit une clé USB Field Replaceable Unit (FRU) avec une image logicielle SD-WAN préchargée. Utilisez la FRU USB pour ré-image de l'appliance aux éditions prises en charge requises (SE/PE/AE). La licence ou la configuration de l'appliance utilisée détermine l'édition de l'appliance.

Le tableau suivant fournit des détails sur les images FRU USB disponibles et les éditions prises en charge par les appliances SD-WAN.

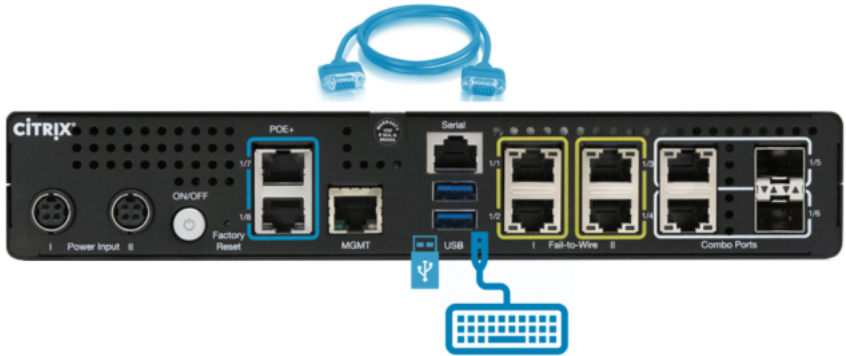
Appliance	Image FRU USB	Éditions supportées
Citrix SD-WAN 110	11.1.1.39	SE
Citrix SD-WAN 210	10.2.7.17	SE, AE
Citrix SD-WAN 410	10.2.3.32	SE
Citrix SD-WAN 1100	10.2.7.17	SE, PE, AE
Citrix SD-WAN 2100	10.2.7.17	SE, PE
Citrix SD-WAN 4100	10.2.7.17	SE
Citrix SD-WAN 5100	10.2.7.17	SE, PE
Citrix SD-WAN 6100	10.2.7.17	SE, PE

Pour effectuer une réimage USB :

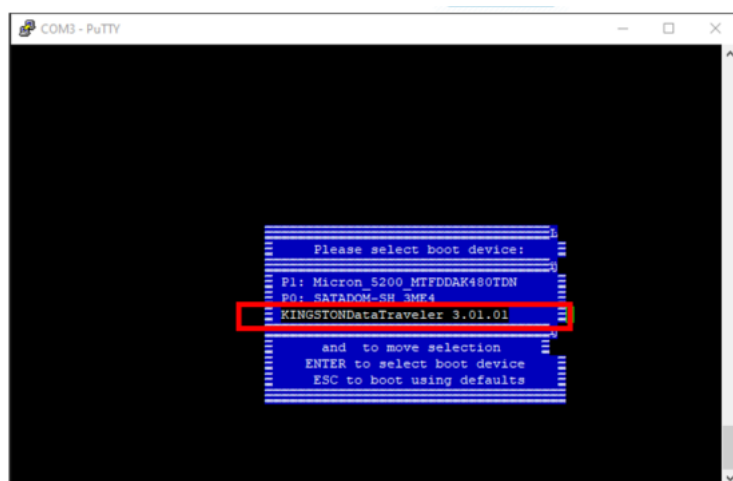
1. Insérez la clé USB fournie par Citrix dans l'un des ports USB de l'appliance.
2. Connectez un clavier USB à un autre port USB.

Conseil

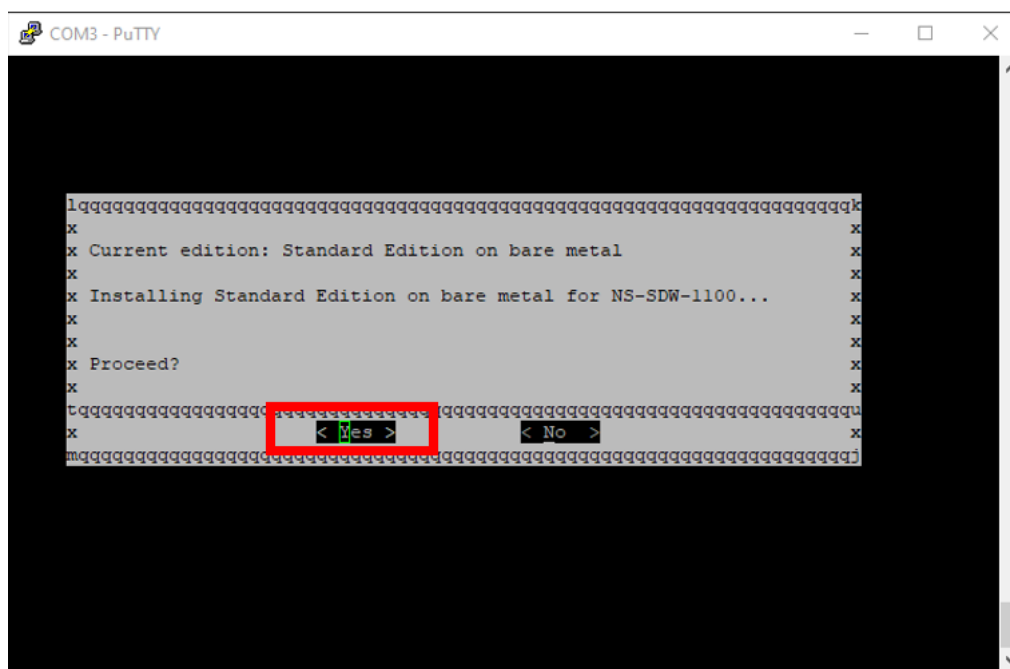
S'il y a un seul port USB sur l'appliance, utilisez un séparateur USB pour connecter à la fois la clé USB et le clavier USB.



3. Connectez-vous à la console série en tant qu'administrateur et émettez la commande reboot appliance via l'interface de ligne de commande.
4. Au démarrage, appuyez continuellement sur la touche **F11** du clavier connecté USB ou **SHIFT+ESC+1** via la connexion à la console série.
5. Sélectionnez le lecteur USB dans le menu du périphérique de démarrage et appuyez sur Entrée.



6. Selon l'édition prise en charge pour la plate-forme, un écran s'affiche pour demander l'autorisation de procéder à l'installation. Sélectionnez **Oui**.



Remarque

Pour le réimageage PE et AE, l'appliance peut apparaître dans l'interface graphique en tant que Standard Edition jusqu'à ce que l'installation de la licence PE/AE et du système d'exploitation approprié soit terminée.

L'installation prend 30 minutes. Ne mettez pas l'appliance hors tension pendant le processus de réimagerie. Il peut redémarrer plusieurs fois.

7. DHCP est activé par défaut sur l'image d'usine. L'adresse IP de gestion par défaut sur toutes les plates-formes est 192.168.100.1. Utilisez-le pour accéder à l'interface graphique SD-WAN.

Vous pouvez également configurer manuellement l'adresse IP de gestion à partir de la console série en exécutant les commandes suivantes :

Commande d'émission '*management_ip*'

Commande d'émission '*set interface 192.168.100.1 255.255.255.0 192.168.100.254*'

Émettre la commande '*appliquer*'

8. Par défaut, le logiciel est mis à niveau vers SE. Installez la licence PE ou AE selon les besoins en fonction des éditions prises en charge par l'appliance.

Remarque

Vous pouvez configurer et gérer les fonctionnalités AE via SD-WAN Orchestrator uniquement. Pour plus d'informations, veuillez consulter la section [Sécurité Edge](#).

Options de licence Citrix SD-WAN

May 6, 2021

Il existe quatre éditions Citrix SD-WAN chacune avec un ensemble ou un sous-ensemble différent de fonctionnalités SD-WAN. Le type de licence que vous installez détermine l'édition de la plate-forme - Standard Edition, WANOP Edition, Premium Edition et Advanced Edition.

Remarque

Lors de l'installation et de l'application d'une licence, assurez-vous que votre appliance spécifique prend en charge l'édition de l'appliance SD-WAN que vous souhaitez activer et que la version logicielle correcte est disponible.

Prise en charge logicielle de la plate-forme Citrix SD-WAN

Le tableau suivant illustre les plates-formes Citrix SD-WAN prises en charge pour chacune des versions logicielles SD-WAN disponibles.

Remarque

Dans la version 10.2, l'édition Enterprise Platform est rebaptisée édition **Premium**.

Version	Édition d'optimisation WAN	Édition Standard	Édition Premium	Édition Advanced
Version 7.x	Oui	Non	Non	Non
Version 8.x	Non	Oui	Non	Non
Version 9.0, 9.1, 9.2, 9.3	Oui	Oui	Oui	Non
Version 10.0, 10.1, 10.2	Oui	Oui	Oui	Non
Version 11.0, 11.1	Oui	Oui	Oui	Non
Version 11.2	Oui	Oui	Oui	Oui
Version 11.3	Oui	Oui	Oui	Oui

Pour afficher tous les modèles d'appliance pris en charge dans Citrix SD-WAN version 11.3, reportez-vous à la section [Fiche technique Citrix SD-WAN](#).

Avant de pouvoir télécharger le logiciel, vous devez obtenir et enregistrer une licence logicielle Citrix SD-WAN. Pour obtenir des instructions sur l'obtention d'une licence logicielle SD-WAN, contactez le support clientèle Citrix. Les instructions relatives au téléchargement et à l'installation du fichier de licence sur vos appliances sont fournies dans la section, [Téléchargement et installation du fichier de licence du logiciel SD-WAN](#). Avant d'installer la licence, vous devez d'abord configurer le matériel de l'appliance et définir la date et l'heure de l'appliance.

La procédure de licence pour l'Provisioning de licences pour les éditions de plates-formes SD-WAN couvre les rubriques suivantes :

- Modèle de licence SD-WAN pris en charge : Local, Remote et Centralized.
- Prise en charge du serveur de licences distant pour les appliances SD-WAN.
- Prérequis pour l'utilisation du serveur de licences distantes.

Remarque

À compter du 4 novembre 2020, il y a un changement au processus de retour et de modification des licences Citrix. Avec ce nouveau processus, vous ne pouvez pas renvoyer ou modifier vos licences via le portail Gérer les licences sur Citrix.com et Mes outils de licence sur Partner Central. Pour plus d'informations et la liste des cas d'utilisation, reportez-vous à la section [Article KB CTX285157](#).

Licences locales

May 6, 2021

Avec la licence locale, vous devez vous connecter à chaque appliance du réseau et charger le fichier de licence. Même avec le service ZTD, l'appliance devient disponible uniquement avec une licence Grace. Vous devrez télécharger un fichier de licence pour une connexion réseau active. Les fichiers de licence sont générés en fonction des ID d'hôte des appliances individuelles.

Vous pouvez installer et configurer la licence pour les appliances SD-WAN à l'aide de l'interface de gestion Web SD-WAN.

Importation de licences pour les appliances SD-WAN déployées sur les plates-formes XenServer/ESXi/Hyper-V :

1. Dans l'interface de gestion Web SD-WAN, accédez à **Configuration > Paramètres de l'appliance > Licences**.
2. Sélectionnez **Local** et téléchargez la licence. Cliquez sur **Charger et installer**.
3. Enregistrez vos modifications en cliquant sur **Appliquer les paramètres**.

The screenshot shows the 'License Configuration' section of the SD-WAN management interface. It features two radio buttons: 'Local' (selected) and 'Remote'. Below this is a section titled 'Upload License for this Appliance'. It contains a 'Filename:' label, a 'Choose File' button, and the text 'No file chosen'. To the right is an 'Upload and Install' button. Below this section is a 'Licenses Uploaded' section. It displays a 'Filename:' label followed by 'CCB_4100VW-2000_SSERVER_Retail.lic' and a small square icon. At the bottom of this section are two buttons: 'Delete Selected Licenses' and 'Apply Settings'.

Licences distantes

May 6, 2021

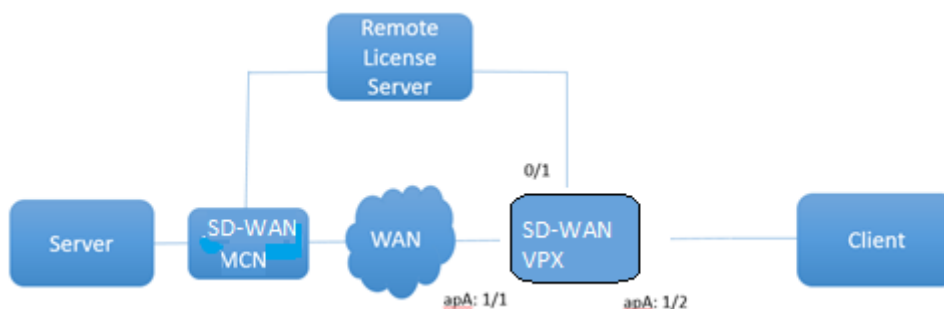
Conditions préalables à l'utilisation du serveur de licences distantes pour les appliances SD-WAN.

- NTP doit être configuré pour le serveur de licences et le SD-WAN (la date et l'heure doivent être synchronisées)

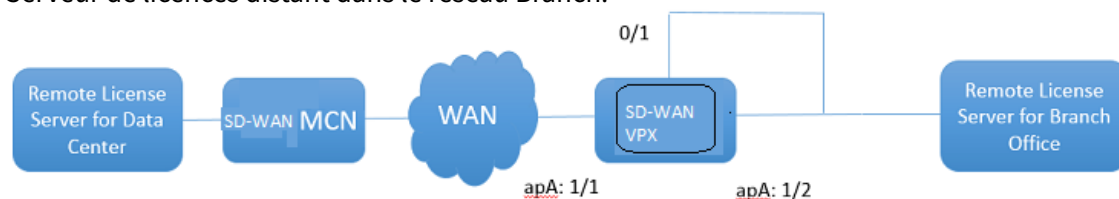
- Il est recommandé d'utiliser la dernière version du serveur de licences :
 - Version 9.1, 9.2 : 11.13.1 L.S
 - Version 10.0, 10.1, 10.2, 11.0, 11.0.1, 11.0.2 : 11.14.1 L.S.
 - Version 11.0.3, 11.1, 11.2 : 11.16.3 L.S

Cas d'utilisation :

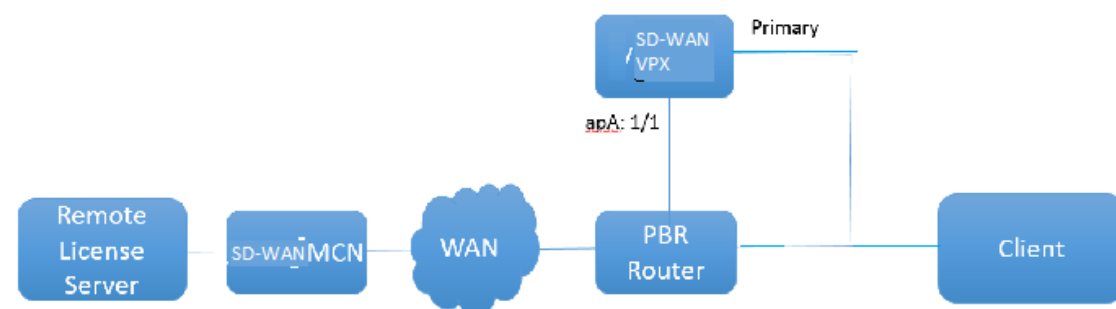
1. Serveur de licences distant accessible via le réseau de gestion sans utiliser de ports de données/APA.



2. Serveur de licences distant dans le réseau Branch.

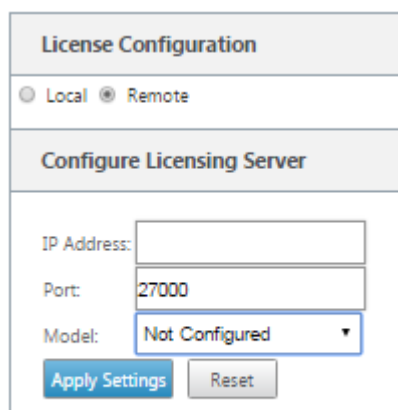


3. SD-WAN VPX-SE - Déploiement de PBR dans le bureau de la succursale.



Licence à distance :

1. Dans l'interface de gestion Web SD-WAN, accédez à **Configuration > Paramètres de l'appliance > Licences**.
2. Sélectionnez **Remote** et entrez les détails de l'adresse IP du serveur distant.



License Configuration

☐ Local ☒ Remote

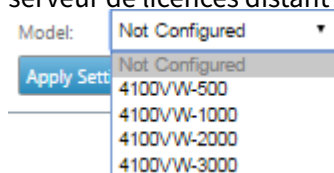
Configure Licensing Server

IP Address:

Port:

Model:

3. Sélectionnez le **modèle** d'appliance souhaité dans le menu déroulant. Le port par défaut du serveur de licences distant est 27000.



Model:

- Not Configured
- 4100V/W-500
- 4100V/W-1000
- 4100V/W-2000
- 4100V/W-3000

Important

- Si vous souhaitez installer des licences distantes pour l'appliance SD-WAN à l'aide de SD-WAN Center, assurez-vous d'activer les licences centralisées sur l'appliance MCN SD-WAN dans les paramètres globaux de l'éditeur de configuration de l'interface de gestion Web SD-WAN.
- Citrix SD-WAN Center ne prend pas en charge l'adresse IPv6.

Licences centralisées

May 6, 2021

Au fur et à mesure que les déploiements réseau augmentent avec un grand nombre de nœuds réseau, la gestion et l'octroi de licences des appliances deviennent lourdes. Afin de simplifier ce processus afin d'intégrer efficacement les appliances SD-WAN et de faciliter les opérations réseau, un modèle de licence centralisé pour le réseau SD-WAN a été introduit.

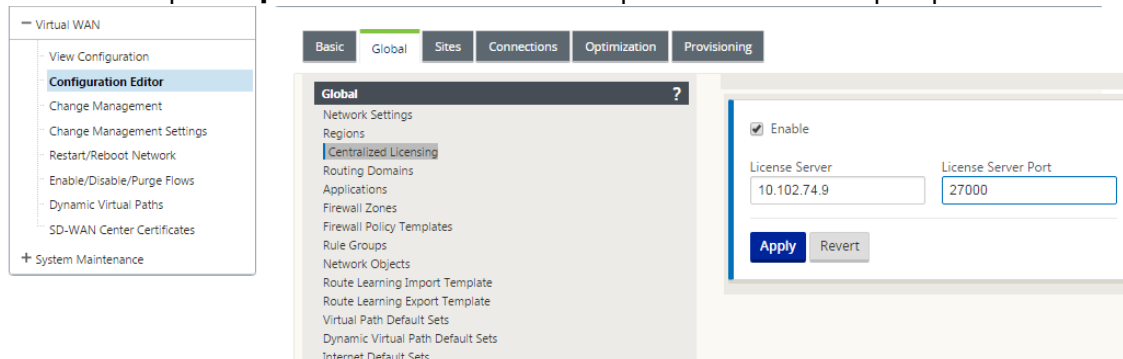
Dans le nouveau modèle de licence centralisé, l'interface de gestion Web de SD-WAN Center (portail de gestion et de reporting des appliances SD-WAN) fournit des services de licence à des appliances SD-WAN individuelles du réseau sans que vous ayez à vous connecter à l'appliance.

L'adresse IP de SD-WAN Center est fournie dans l'interface graphique de l'apppliance SD-WAN sous **Global > Licences centralisées**. Cette adresse IP est propagée aux appliances individuelles via les packages de configuration ou les mises à jour. Lorsque l'adresse IP est modifiée, vous devez passer par le processus de gestion des modifications pour pousser les appliances. Le paramètre global peut être remplacé par les paramètres du site local.

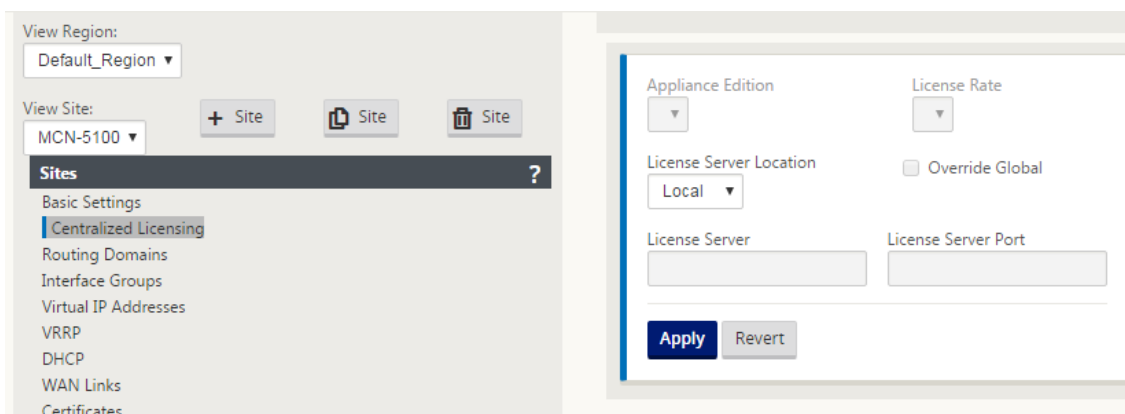
La bande passante de la licence peut être sélectionnée avec le modèle d'apppliance pour les paramètres du site. La bande passante des liaisons WAN est vérifiée par rapport à la licence sélectionnée.

Pour activer les licences centralisées dans l'interface graphique de l'apppliance SD-WAN :

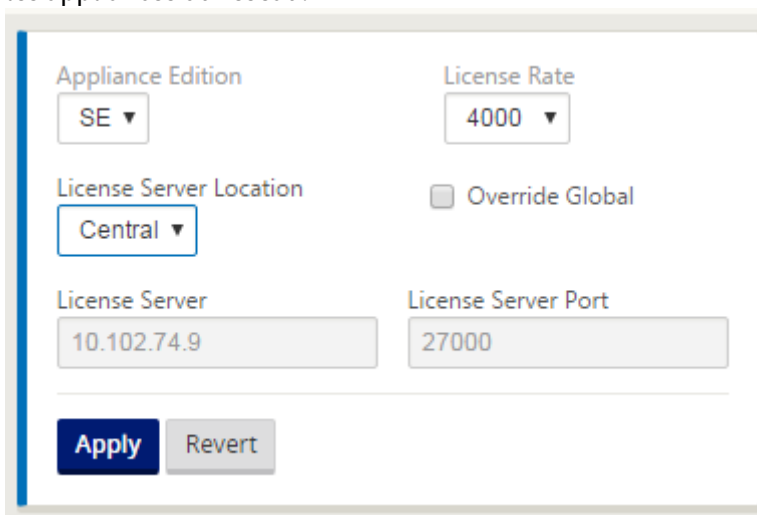
1. Accédez à **Configuration > Réseau étendu virtuel > Éditeur de configuration**. Ouvrez un package de configuration WAN virtuel existant ou créez un package de configuration. Le package de configuration s'ouvre.
2. Accédez à l'onglet **Global**. Sélectionnez **Licences centralisées**. Cliquez sur **Activer**.
3. Entrez l'adresse IP du serveur de licences à partir de laquelle vous pouvez télécharger et gérer des licences SD-WAN. Fournissez l'adresse IP de gestion SD-WAN Center, afin que le package de configuration du MCN SD-WAN ou des appliances de succursale puisse télécharger la licence à partir de SD-WAN Center.
4. Entrez **27000** pour le **port du serveur de licences** qui est un numéro de port par défaut.



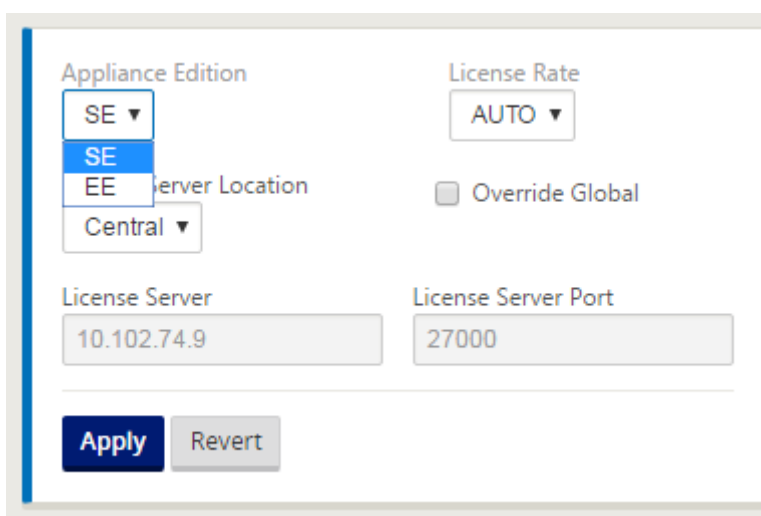
5. Cliquez sur **Appliquer**.
6. Accédez à l'onglet **Sites**. Sélectionnez Site MCN ou Site de succursale sous **Afficher le site**, en fonction de la région et du site pour lesquels vous souhaitez gérer les licences centrales.
7. Sélectionnez **Licences centralisées**. L'affichage des options de licence centrale s'affiche. Par défaut, l'option **Local** est sélectionnée pour l'**emplacement du serveur de licences**.



8. Cliquez sur le menu déroulant et sélectionnez **Central** pour modifier l'emplacement du serveur de licences par défaut. Cela affiche l'adresse IP et les informations de port que vous avez fournies pour le serveur de licences lorsque vous activez la licence centrale dans les paramètres globaux. Par exemple, ; le serveur de licences peut être l'adresse IP de SD-WAN Center qui gère les appliances du réseau.



9. Choisissez l'**Édition Appliance** et le **taux de licence** en fonction des appliances à installer. Cliquez sur **Appliquer**.



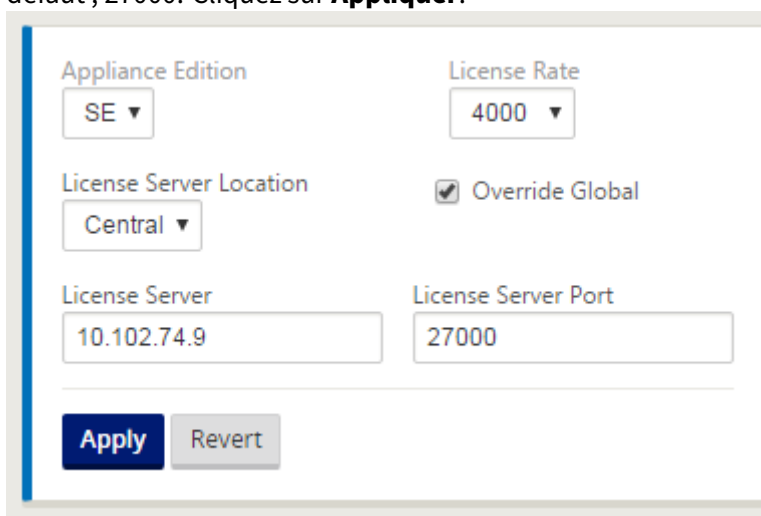
The screenshot shows a configuration window with the following fields and values:

Field	Value
Appliance Edition	SE
License Rate	AUTO
License Server Location	Central
Override Global	<input type="checkbox"/>
License Server	10.102.74.9
License Server Port	27000

Buttons: Apply, Revert

Remarque : Vous pouvez choisir de remplacer les informations du serveur de licences fournies dans les paramètres globaux de la configuration.

10. Sélectionnez **Remplacer Global** pour remplacer les paramètres globaux. Configurez la nouvelle adresse IP du serveur de licences. Conservez le numéro de port du serveur de licences par défaut ; 27000. Cliquez sur **Appliquer**.



The screenshot shows the same configuration window as before, but with the following changes:

Field	Value
Appliance Edition	SE
License Rate	4000
License Server Location	Central
Override Global	<input checked="" type="checkbox"/>
License Server	10.102.74.9
License Server Port	27000

Buttons: Apply, Revert

Vous pouvez désormais gérer les licences pour tous les nœuds des sites de succursale et MCN configurés pour un package de configuration d'appliance SD-WAN spécifique à partir du serveur de licences que vous avez configuré.

Le serveur de licences peut être un portail de gestion SD-WAN Center qui acquiert les licences obtenues à partir de la configuration réseau vers les sites via le processus de gestion des modifications.

Licence basée sur l'allocation de bande passante :

Chaque appliance peut choisir une licence dont le niveau de bande passante est supérieur ou égal à

la bande passante configurée. Si la licence de bande passante configurée n'est pas disponible, la possibilité pour une appliance de choisir la licence de bande passante supérieure suivante est ajoutée. Cette fonctionnalité est valable pour les fonctionnalités centralisées et distantes du serveur de licences. Par exemple :

- Si vous disposez de trois licences de 410 à 200 Mbps. Vous utiliserez les mêmes licences pour toutes les allocations de bande passante associées à l'appliance 410. Le site A (20 Mbps), le site B (50 Mbps) et le site C (200 Mbps) doivent tous pouvoir utiliser des licences de 410 à 200 Mbps.
- Si vous disposez d'une licence de 410 à 20 Mbps et d'une licence de 410 à 200 Mbps. Le site A est configuré pour consommer 50 Mbps, puis le site A peut utiliser une licence de 410 à 200 Mbps.

Période de grâce de licence :

Le délai de grâce autorisé est de 30 jours lorsque le fichier de licence ou la configuration de licence est supprimé de l'appliance. Les alertes de grâce sont prises en charge pour Syslog et les e-mails.

Remarque

Lorsque le taux de licence sélectionné ne correspond pas au taux de liaison WAN configuré, le message suivant s'affiche sur l'interface graphique de l'appliance pour les événements de licence.

Message : Le débit autorisé total configuré (LAN to WAN) NNNN (Kbps) ne doit pas dépasser le double du taux de licence qui est NNNN (Kbps)

Gravité : AVERTISSEMENT

Événements : Syslog, Email

Gestion des licences

May 6, 2021

Les licences des appliances Citrix SD-WAN sont gérées en communiquant avec le service de licences distant pour vérifier la présence de licences. Si l'appliance est sous licence, les opérations réseau se poursuivent sans interruption. Si l'appliance n'est pas sous licence, le mode de licence Grace est lancé.

Processus de gestion des licences de l'appliance SD-WAN :

1. Chaque site communique avec le serveur distant ou SD-WAN Center à l'aide de l'interface de gestion Web. Cette communication se fait via un mécanisme de pulsation pour surveiller la connectivité et un mécanisme de récupération qui vérifie l'état de la licence.

2. Heartbeats sont envoyés sur une connexion TCP au serveur de licences toutes les 10 à 20 minutes pour vérifier la connectivité.
3. Après une perte de deux Heartbeats consécutifs, l'appliance passe en mode grâce. La méthode d'extraction détermine l'état de la licence. Ce statut peut être « Réel », « Grace » ou « Refusé » envoyé à l'appliance à partir de SD-WAN Center. Chaque fois qu'une appliance accède à SD-WAN Center pour connaître l'état de la licence, elle accède à la nouvelle licence. Si SD-WAN Center ne reçoit pas deux battements cardiaques, SD-WAN Center libère la licence allouée au site dans le pool. Le délai de grâce est de 30 jours, donc après la perte de 2 battements cardiaques, l'appareil entre dans la période de grâce. Pendant ces 30 jours, la communication doit être rétablie. Une fois restaurée, l'appliance revient au mode de fonctionnement normal. Si la communication n'est PAS restaurée, l'appliance est mise à l'état non autorisé et suit la procédure d'expiration de la licence non licenciée/de la licence.

Licences prêtes à l'emploi (OOB) pour l'appliance MCN :

- l'appliance MCN n'aura pas de délai de grâce initial. Elle a besoin d'une licence pour être disponible.

Licences prêtes à l'emploi (OOB) pour l'appliance client :

- Le nœud client offre une période de grâce de 30 jours avec ou sans fonctionnalité ZTD.
- L'appliance est activée avec un fichier de licence OOB valide pendant 30 jours.
- Vous disposez de 30 jours pour charger un fichier de licence ou obtenir une licence via le serveur de licences centralisées.
- Si l'appliance est sous licence, elle fonctionne normalement et fait partie du réseau.
- Si l'appliance n'est pas sous licence dans les 30 jours, la procédure d'expiration de la licence est suivie.

La seule façon de réinitialiser l'appliance pour obtenir une licence OOB est d'effectuer une « Réinitialisation d'usine ».

Expiration de la licence

May 6, 2021

L'appliance SD-WAN est soumise à un délai de grâce de 30 jours et vous devez télécharger la licence après l'expiration de la licence.

Pendant le délai de grâce, toutes les opérations fonctionnent normalement. Si la licence n'est pas téléchargée dans le temps (30 jours après expiration), Virtual WAN Service est désactivé.

Les licences centralisées ont un fichier journal pour suivre le fonctionnement de la période de grâce, sans licence, sous licence, l'état de communication et les échecs.

Dans l'interface graphique de l'appliance SD-WAN, sous diagnostic, la fonctionnalité de test de connectivité MCN dans SD-WAN Center vers d'autres sites est disponible. Cela peut être utilisé pour tester si chaque appliance peut atteindre le serveur de licences. Les sites, l'état des licences et la table d'état sont disponibles pour la gestion et le suivi des licences.

Période de grâce :

1. Une période de grâce de 30 jours est fournie pour les nœuds clients prêts à l'emploi. La notification indique que l'appliance est en mode Out-of-Box et nécessite une licence valide. Cette option utilise un fichier de licence grâce.
2. Expiration de la licence : Une fois la licence expirée, un délai de grâce de 30 jours est accordé. La notification indique que la raison du délai de grâce est l'expiration de la licence et nécessite un renouvellement.
3. Perte de communication avec SD-WAN Center : Après 2 battements cardiaques, l'appareil passe en mode grâce pendant 30 jours. La notification indique que la raison du délai de grâce est un échec de communication.

Configuration

November 1, 2021

Après avoir installé le logiciel et les licences SD-WAN, vous pouvez configurer les paramètres de l'appliance SD-WAN pour commencer à gérer votre réseau et votre déploiement.

La configuration de l'appliance SD-WAN comprend les éléments suivants :

Configurer le MCN : le MCN sert de point de distribution pour la configuration système initiale et toute modification de configuration ultérieure. Vous effectuez la plupart des procédures de mise à niveau via l'interface Web de gestion sur le MCN. Il ne peut y avoir qu'un seul MCN actif dans un WAN virtuel. Par défaut, les solutions matérielles-logicielles ont le rôle de client pré-attribué. Pour établir une appliance en tant que MCN, vous devez d'abord ajouter et configurer le site MCN, puis mettre en scène et activer la configuration et le package logiciel approprié sur l'appliance MCN désignée.

Configurer la branche : La procédure d'ajout d'un site de branche est similaire à la création et à la configuration du site MCN. Cependant, certaines étapes et paramètres de configuration varient légèrement pour un site de succursale. En outre, une fois que vous avez ajouté un site de branche initial, pour les sites qui ont le même modèle d'appliance, vous pouvez utiliser la fonctionnalité **Cloner** (dupliquer) pour simplifier le processus d'ajout et de configuration de ces sites. Comme pour la création du site MCN, pour configurer un site de branche, vous devez utiliser l'**éditeur de configuration**

dans l'interface Web de gestion de l'appliance MCN. L'**éditeur de configuration** n'est disponible que lorsque l'interface est définie sur le mode **Console MCN**.

Configurer le chemin virtuel entre le MCN et les sites de succursale : Configurez le service de chemin virtuel entre le MCN et chacun des sites clients (succursales). Pour ce faire, vous utilisez les formulaires et paramètres de configuration disponibles dans l'arborescence de configuration de la section **Connexions** de l'**éditeur de configuration**.

Activer et configurer l'optimisation WAN : cette section fournit des instructions détaillées sur l'activation et la configuration des fonctionnalités d'optimisation WAN SD-WAN Premium (Enterprise) Edition pour votre Virtual WAN. Pour ce faire, utilisez les formulaires de la section **Optimisation** de l'**éditeur de configuration** de l'interface de gestion Web sur le MCN.

REMARQUE Les

services Citrix SD-WAN Orchestrator ne prennent pas en charge les adresses IPv6.

Les fonctionnalités suivantes des appliances Citrix SD-WAN prennent en charge l'adresse IPv6 de Citrix SD-WAN version 11.3 :

- Fonctions du plan de gestion
 - [Interface de gestion](#)
 - [Serveur RADIUS](#)
 - [Serveur TACACS+](#)
 - [Serveur SMTP](#)
 - [Serveur Syslog](#)
 - [Serveur HTTP](#)
 - [Serveur DNS](#)
 - [Flux d'application/IPfix](#)
 - [SNMP](#)
 - [Licences distantes](#)
 - [Licences centralisées](#)
 - [Serveur NTP](#)
 - [Liste verte](#)
 - [Nouvelle interface utilisateur pour les appliances SD-WAN](#)
 - [Diagnostics](#)

REMARQUE

Après avoir configuré les fonctionnalités répertoriées ci-dessus avec l'adresse IPv6 de gestion, si vous désactivez le protocole IPv6 sous **Paramètres du matériel > Cartes réseau**, les fonctionnalités ne fonctionnent pas comme prévu.

- Fonctions de plan de données

- Routage statique
- [Service Internet via des liaisons WAN IPv6](#)
- [Service Intranet sur liaisons WAN IPv6](#)
- [Publicités de routeur](#)
- [Client DHCP](#)
- [Serveur/relais DHCP](#)
- [QoS des applications](#)
- [Pare-feu](#)
- [Gestion in-band](#)
- [Haute disponibilité](#)
- [Règles IP](#)
- [IPv6 pris en charge par des liens LTE](#)

REMARQUE

- Les adresses IPv6 ne sont pas prises en charge sur les appliances Citrix Citrix SD-WAN 1000 SE/PE, Citrix SD-WAN 2000 SE/PE et Citrix SD-WAN 4000 SE.
- Les adresses IPv6 ne sont pas prises en charge dans les configurations suivantes :
 - Dynamic Routing (OSPF/BGP)
 - Virtual Router redundancy protocol
 - Premium edition or Two-Box support
 - Cloud direct
 - VNF/3rd Party Firewall
 - Netflow
 - Header compression for IPv6 packets
 - Application Routing
 - Office-365 support
 - Prefix delegation group

Configuration initiale

September 26, 2023

Ces procédures doivent être effectuées pour chaque appliance que vous souhaitez ajouter à votre SD-WAN. Par conséquent, ce processus nécessitera une certaine coordination avec vos administrateurs de site sur l'ensemble de votre réseau, afin de s'assurer que les appliances sont prêtes à être déployées en temps voulu. Toutefois, une fois que le nœud de contrôle maître (MCN) est configuré et déployé, vous pouvez ajouter des appliances client (nœuds clients) à votre SD-WAN à tout moment.

Pour chaque appliance que vous souhaitez ajouter à votre réseau étendu virtuel, vous devez effectuer les opérations suivantes.

1. Configurez le matériel SD-WAN Appliance et les appliances virtuelles SD-WAN VPX (SD-WAN VPX-VW) que vous allez déployer.
2. Définissez l'adresse IP de gestion de l'appliance et vérifiez la connexion.
3. Définissez la date et l'heure sur l'appliance.
4. Définissez le seuil de **temporisation** de la session de la console sur une valeur élevée ou maximale.

Avertissement

Si votre session de console expire ou si vous vous déconnectez de l'interface Web de gestion avant d'enregistrer votre configuration, les modifications de configuration non enregistrées seront perdues. Vous devez ensuite vous reconnecter au système et répéter la procédure de configuration dès le début. Pour cette raison, il est fortement recommandé de définir l'intervalle de **temporisation de la session de console** sur une valeur élevée lors de la création ou de la modification d'un package de configuration ou lors de l'exécution d'autres tâches complexes.

5. Téléchargez et installez le fichier de licence logicielle sur l'appliance.

Pour obtenir des instructions sur l'installation d'un dispositif virtuel SD-WAN (SD-WAN VPX), reportez-vous aux sections suivantes :

- [À propos du SD-WAN VPX.](#)
- [Installation et déploiement d'un VPX-SE SD-WAN sur ESXi.](#)

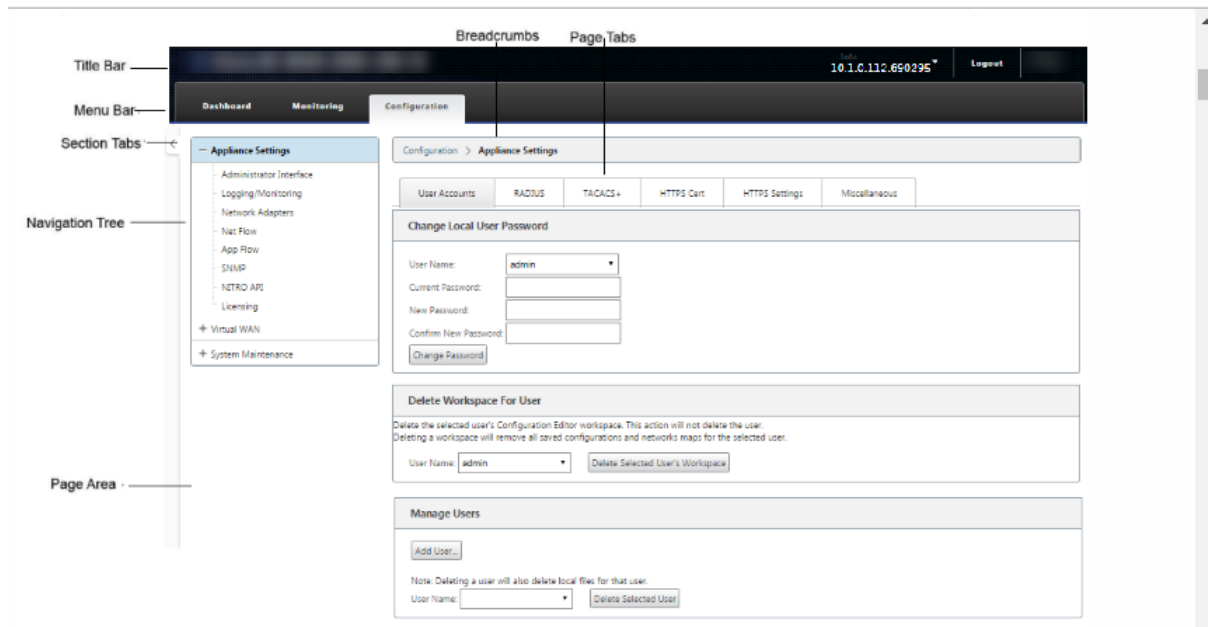
Vue d'ensemble de la mise en page de l'interface Web

May 6, 2021

Cette section fournit des instructions de navigation de base et une feuille de route de navigation de la hiérarchie des pages de l'interface de gestion Web SD-WAN. Des instructions de navigation spécifiques pour l'**éditeur de configuration** et l'**assistant Gestion des modifications** sont également fournies.

Navigation de base

La figure ci-dessous décrit les éléments de navigation de base de l'interface de gestion Web et la terminologie utilisée pour les identifier.



Les éléments de navigation de base sont les suivants :

- **Barre de titre** : affiche le numéro de modèle de l'appliance, l'adresse IP de l'hôte de l'appliance, la version du package logiciel en cours d'exécution sur l'appliance et le nom d'utilisateur de la session de connexion en cours. La barre de titre contient également le bouton **Déconnexion** pour terminer la session.
- **Barre de menu principale** : il s'agit de la barre affichée sous la barre de titre sur chaque écran de l'interface Web de gestion. Il contient les onglets de section permettant d'afficher l'arborescence de navigation et les pages d'une section sélectionnée.
- **Onglets de section** : les onglets de section se trouvent dans la barre de menu principale en haut de la page. Il s'agit des catégories de niveau supérieur pour les pages et les formulaires de l'interface de gestion Web. Chaque section a sa propre arborescence de navigation pour naviguer dans la hiérarchie des pages de cette section. Cliquez sur un onglet de **section** pour afficher l'arborescence de navigation de cette section.
- **Arborescence de navigation** : l'arborescence de navigation se trouve dans le volet gauche, sous la barre de menus principale. L'arborescence de navigation d'une section s'affiche. Cliquez sur un onglet de section pour afficher l'arborescence de navigation de cette section. L'arborescence de navigation offre les options d'affichage et de navigation suivantes :
 - Cliquez sur un onglet de section pour afficher l'arborescence de navigation et la hiérarchie des pages de cette section.

- Cliquez sur + (signe plus) en regard d'une succursale dans l'arborescence pour afficher les pages disponibles pour cette rubrique de succursale.
 - Cliquez sur un nom de page pour afficher cette page dans la zone de page.
 - Cliquez sur — (signe moins) en regard d'un élément de succursale pour fermer la branche.
- **Preadcrumbs** : affiche le chemin de navigation vers la page active. Les chapelures sont en haut de la zone de page, juste en dessous de la barre de menu principale. Les liens de navigation actifs s'affichent en police bleue. Le nom de la page en cours est affiché en caractères gras noirs.
- **Zone de page** : il s'agit de l'affichage de la page et de la zone de travail de la page sélectionnée. Sélectionnez un élément dans l'arborescence de navigation pour afficher la page par défaut de cet élément.
- **Onglets de page** : certaines pages contiennent des onglets permettant d'afficher d'autres pages enfants pour ce sujet ou formulaire de configuration. Ceux-ci sont situés en haut de la zone de page, juste en dessous de l'affichage de la chapelure. Parfois (comme pour l'Assistant **Gestion des modifications**), les onglets se trouvent dans le volet gauche de la zone de page, entre l'arborescence de navigation et la zone de travail de la page.
- **Redimensionnement de la zone de page** : pour certaines pages, vous pouvez agrandir ou réduire la largeur de la zone de page (ou des sections de celle-ci) pour afficher d'autres champs dans un tableau ou un formulaire. Dans ce cas, une barre de redimensionnement verticale grise se trouve sur la bordure droite d'un volet de zone de page, d'un formulaire ou d'un tableau. Faites défiler votre curseur sur la barre de redimensionnement jusqu'à ce que le curseur devienne une flèche bidirectionnelle. Ensuite, cliquez et faites glisser la barre vers la droite ou la gauche pour augmenter ou réduire la largeur de la zone.

Si la barre de redimensionnement n'est pas disponible pour une page, vous pouvez cliquer et faire glisser le bord droit de votre navigateur pour afficher la page complète.

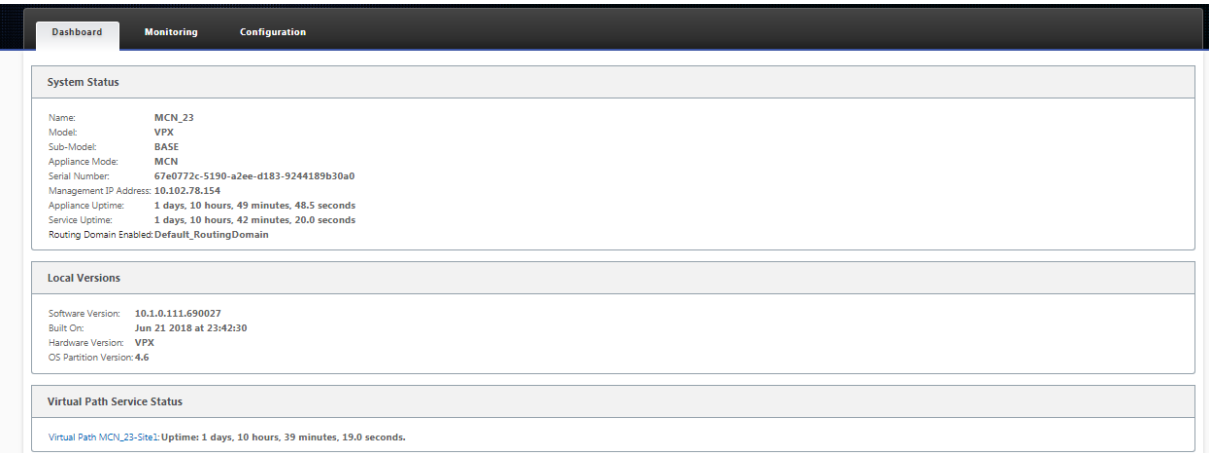
Tableau de bord de l'interface Web

Cliquez sur l'onglet de section Tableau de **bord** pour afficher les informations de base de l'appliance locale.

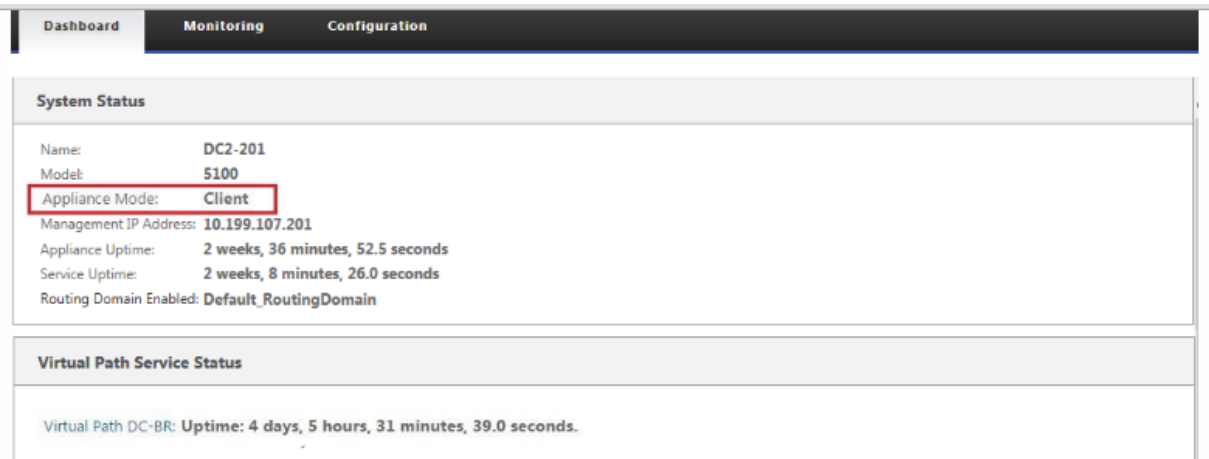
La page **Tableau de bord** affiche les informations de base suivantes pour l'appliance :

- État du système
- Statut du service Virtual Path
- Informations sur la version du package logiciel de l'appliance locale

La figure suivante illustre un exemple d’affichage du tableau de **bord** de l’appliance MCN (Master Control Node).



La figure suivante illustre un exemple d’affichage du tableau de bord de l’appliance client.



Éditeur de configuration

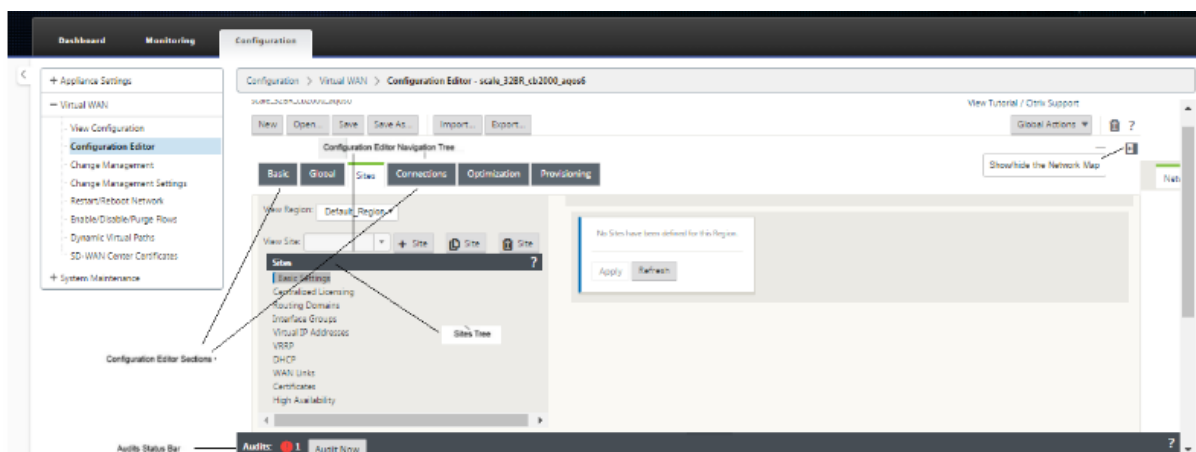
L’éditeur de configuration vous permet d’ajouter et de configurer des sites d’appliance Virtual WAN, des connexions, de l’optimisation et du Provisioning, ainsi que de créer et de définir la configuration de réseau étendu virtuel.

L’Éditeur de configuration est disponible uniquement lorsque l’interface de gestion Web est en mode console MCN. Par défaut, l’interface Web d’une nouvelle appliance est définie sur le mode client. Vous devez modifier le paramètre de mode sur console MCN avant de pouvoir accéder à l’éditeur de configuration. Pour obtenir des instructions, reportez-vous à la section [Basculer l’interface Web de gestion en mode console MCN](#).

Pour accéder à l’**Éditeur de configuration**, procédez comme suit :

1. Connectez-vous à l'interface de gestion Web sur l'appliance MCN.1. Sélectionnez l'onglet **Configuration**.1. Dans l'arborescence de navigation, cliquez sur **+** en regard de la succursale **Virtual WAN** dans l'arborescence. Ceci affiche les pages disponibles pour la catégorie **Virtual WAN**.1. Dans la branche WAN virtuel de l'arborescence, sélectionnez **Éditeur de configuration**.

La figure suivante décrit les éléments de navigation de base et de page de l'**éditeur de configuration**, ainsi que la terminologie utilisée pour les identifier.



Voici les principaux éléments de navigation de l'**Éditeur de configuration** référencés dans ce guide :

- **Barre de menu de l'Éditeur de configuration** —Ceci est en haut de la zone de page, juste en dessous des liens de chapeliure. La barre de menus contient les boutons d'activité principaux pour les opérations de l'**Éditeur de configuration**. En outre, à l'extrême droite de la barre de menus se trouve le bouton de lien **Afficher le didacticiel** pour lancer le didacticiel de l'**Éditeur de configuration**. Le didacticiel vous guide à travers une série de descriptions de bulles pour chaque élément de l'affichage de l'**Éditeur de configuration**.
- **Arborescence des sections de l'Éditeur de configuration** : il s'agit de la pile de barres gris foncé située dans le volet gauche de la zone de page de l'**Éditeur de configuration**. Chaque barre grise représente une section de niveau supérieur. Cliquez sur le nom d'une section pour afficher les sous-branches de cette section.
- **Succursales de l'arborescence des sections** : cliquez sur le nom d'une section dans l'arborescence des sections pour ouvrir une succursale de section. Chaque branche de section contient une ou plusieurs sous-branches de catégories de configuration et de formulaires, qui à son tour peuvent contenir plus de succursales et de formulaires enfants.
- **Arborescence des sites** : répertorie les nœuds de site qui ont été ajoutés à la configuration actuellement ouverte dans l'**Éditeur de configuration**. Dans l'arborescence de la section. Cliquez sur un nom de site pour ouvrir la branche de ce site. Cliquez sur le site pour fermer

une succursale. Pour obtenir des instructions détaillées sur la navigation et l'utilisation de l'arborescence **Sites** et des formulaires de configuration, consultez les sections suivantes :

- [Configuration du site MCN \(Master Control Node\)](#)
- [Ajout et configuration des sites de succursale](#)
- **Barre d'état des audits** : il s'agit de la barre grise foncée située au bas de la page de l'**Éditeur de configuration** et couvrant toute la largeur de l'écran de l'interface Web de gestion. La barre d'état **Audits** n'est disponible que lorsque l'**Éditeur de configuration** est ouvert. Une icône d'alerte d'audit (point rouge ou delta de verge d'or) située à l'extrême gauche de la barre d'état indique une ou plusieurs erreurs présentes dans la configuration actuellement ouverte. Cliquez sur la barre d'état pour afficher la liste complète de toutes les alertes d'audit non résolues pour cette configuration.

Assistants de gestion des modifications

Les assistants **Gestion des modifications** vous guident tout au long du processus de téléchargement, de transfert et d'activation du logiciel et de la configuration Virtual WAN sur l'appliance MCN (Master Control Node) et les appliances clientes. Il existe deux versions de l'Assistant **Gestion des modifications**, l'une pour la gestion des modifications à l'échelle du système Virtual WAN (« globale ») et l'autre pour la gestion des modifications locales, comme suit :

- **Assistant Gestion des modifications MCN (Global)** — L'**assistant Gestion globale des modifications MCN** est la version principale (principale) et est disponible uniquement dans l'interface de gestion Web de l'appliance MCN. Utilisez cette option pour générer les packages d'appliance Virtual WAN à déployer pour chaque type d'appliance Virtual WAN de votre réseau. Vous pouvez également utiliser l'Assistant pour propager automatiquement les modifications de configuration aux appliances déjà déployées dans votre réseau étendu virtuel. Les instructions de navigation de base sont fournies dans la section « Utilisation de l'Assistant Gestion globale des modifications MCN » ci-dessous. Les instructions relatives à l'utilisation de l'assistant de **gestion globale des modifications** MCN pour créer les packages d'appliance sont fournies dans la section [Préparation des packages d'appliance virtuelle WAN sur le MCN](#).
- **Assistant Gestion des modifications locales** : l'**Assistant Gestion des modifications locales** est disponible dans l'interface de gestion Web exécutée sur le MCN et sur tous les dispositifs de nœud client. Utilisez cette option pour télécharger, préparer le déploiement et activer le package d'appliance Virtual WAN approprié sur une appliance locale à ajouter à votre réseau WAN virtuel. Vous pouvez également utiliser cet Assistant pour télécharger un package d'appliance mis à jour spécifiquement sur le MCN local ou sur une appliance virtuelle WAN locale déjà déployée sur votre réseau.

Utilisation de l'assistant de gestion globale des modifications MCN

Pour ouvrir l'Assistant **Gestion globale des modifications** MCN, procédez comme suit :

1. Connectez-vous à l'interface de gestion Web sur l'appliance MCN.
2. Sélectionnez l'onglet **Configuration**. Dans l'arborescence de navigation, cliquez sur **+** en regard de la succursale **Virtual WAN** dans l'arborescence.
3. Dans la branche **Virtual WAN** . Sélectionnez **Gestion des modifications**.

Cette page affiche la première page de l'Assistant **Gestion des modifications**, la page **Vue d'ensemble du processus de modification**, comme illustré dans la figure suivante.

Configuration Filenames: Active - MCN_VPX_23_Site_VPX_JL8_20180517_1430.zip Staged - MCN_VPX_23_Site_VPX_JL8_20180517_1430.zip

Global Multi-Region Summary

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	10	2	0	8	0
r3	7	1	0	6	0
r1	552	1	0	0	0
r4	Data not available				

Region - Default Region Details

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN_23_Appliance	CBVPX	10.1.0.111.690027	11:56 on 6/26/18	10.0.2.32.685295	17:59 on 6/6/18	<3 min	137 s	active / staged	
Site1_Appliance	CBVPX	10.1.0.111.690027	11:56 on 6/26/18	10.0.2.32.685295	17:59 on 6/6/18	<3 min	162 s	active / staged	

4. Pour démarrer l'Assistant, cliquez sur **Commencer**.

Pour obtenir des instructions complètes sur l'utilisation de l'assistant pour télécharger, configurer et activer le logiciel SD-WAN et la configuration sur les appliances, reportez-vous aux sections suivantes :

- [Préparation des packages d'appliance virtuelle WAN sur le MCN](#)
- [Installation des packages Virtual WAN Appliance sur les clients](#)

L'Assistant **Gestion des modifications** contient les éléments de navigation suivants :

- **Zone de page** : affiche les formulaires, les tables et les boutons d'activité de chaque page de l'Assistant **Gestion des modifications** .
- **Onglets de page de l'Assistant Gestion des modifications** : les onglets de page se trouvent dans le volet gauche de la zone de page de chaque page de l'Assistant. Les onglets sont réper-

torisés dans l'ordre dans lequel les étapes correspondantes se produisent dans le processus de l'Assistant. Lorsqu'un onglet est actif, vous pouvez cliquer dessus pour revenir à une page précédente de l'Assistant. Si un onglet est actif, le nom s'affiche en police bleue. La police grise indique un onglet inactif. Les onglets sont inactifs jusqu'à ce que toutes les dépendances (étapes précédentes) aient été remplies sans erreur.

- **Tableau Appliance-Site** : se trouve en bas de la zone de page de l'Assistant, sur la plupart des pages de l'Assistant. Le tableau contient des informations sur chaque site d'appliance configuré, ainsi que des liens permettant de télécharger les packages d'appliance actifs ou reproduits pour ce modèle et site d'appliance. Un package dans ce contexte est un ensemble de fichiers Zip contenant le package logiciel SD-WAN approprié pour ce modèle d'appliance et le package de configuration spécifié. La section **Nom des fichiers de configuration** située au-dessus du tableau indique le nom du package des packages actifs et reproduits actuels sur l'appliance locale.
- **Liens de téléchargement actif/par étapes** : ils se trouvent dans le champ **Télécharger le package** (colonne à droite) de chaque entrée du tableau **Appliance-Site**. Cliquez sur un lien dans une entrée pour télécharger le package actif ou intermédiaire pour ce site de l'appliance.
- **Commencer** — Cliquez sur **Commencer** pour lancer le processus **de l'Assistant Gestion des modifications** et passez à l'onglet **Préparation des modifications**.
- **Activer la configuration intermédiaire** : s'il ne s'agit pas d'un déploiement initial et que vous souhaitez activer la configuration en cours, vous avez la possibilité de passer directement à l'étape **Activation**. Cliquez sur **Activer Staged** pour accéder directement à la page Activation et lancer l'activation de la configuration en cours.

Configuration du matériel de l'appliance

May 6, 2021

Pour configurer le matériel de l'appliance Citrix SD-WAN (matériel physique), procédez comme suit :

1. Configurez le châssis.

Les appliances Citrix SD-WAN peuvent être installées dans un rack standard. Pour l'installation de bureau, placez le châssis sur une surface plane. S'assurer qu'il y a au moins 2 pouces de dégagement sur les côtés et à l'arrière de l'appareil, pour une bonne ventilation.

2. Connectez l'alimentation.

- a) Assurez-vous que le bouton d'alimentation est réglé sur Off.
- b) Branchez le cordon d'alimentation à l'appliance et à une prise secteur.

- c) Appuyez sur le bouton d'alimentation situé à l'avant de l'appareil.
- 3. Branchez l'alimentation.
 - a) Assurez-vous que le bouton d'alimentation est réglé sur Off.
 - b) Branchez le cordon d'alimentation à l'apppliance et à une prise secteur.
 - c) Appuyez sur le bouton d'alimentation situé à l'avant de l'appareil.
- 4. Connectez le port de gestion de l'apppliance à un ordinateur personnel.

Vous devez connecter l'apppliance à un PC en prévision de la procédure suivante, en définissant l'adresse IP de gestion de l'apppliance.

Remarque

Avant de connecter l'apppliance, vérifiez que le port Ethernet est activé sur le PC. Utilisez un câble Ethernet pour connecter le port de gestion de l'apppliance SD-WAN au port Ethernet par défaut sur un ordinateur personnel.

Port de gestion SD-WAN VPX-SE

L'apppliance virtuelle SD-WAN VPX-SE est une machine virtuelle, il n'y a donc pas de port de gestion physique. Toutefois, si vous n'avez pas configuré l'adresse IP de gestion pour le SD-WAN VPX-SE lorsque vous avez créé la machine virtuelle VPX, vous devez le faire maintenant, comme indiqué dans la section, [Configuration de l'adresse IP de gestion pour le VPX-SE SD-WAN](#).

L'apppliance virtuelle SD-WAN VPX-SE est une machine virtuelle, il n'y a donc pas de port de gestion physique. Toutefois, si vous n'avez pas configuré l'adresse IP de gestion pour le SD-WAN VPX-SE lorsque vous avez créé la machine virtuelle VPX, vous devez le faire maintenant, comme indiqué dans la section, [Configuration de l'adresse IP de gestion pour le VPX-SE SD-WAN](#).

Configurer l'adresse IP de gestion

September 26, 2023

Pour activer l'accès à distance à une appliance SD-WAN, vous devez spécifier une adresse IP de gestion unique pour l'apppliance. Pour ce faire, vous devez d'abord connecter l'apppliance à un PC. Vous pouvez ensuite ouvrir un navigateur sur le PC et vous connecter directement à l'interface Web de gestion de l'apppliance, où vous pouvez définir l'adresse IP de gestion de cette appliance. L'adresse IP de gestion doit être unique pour chaque appliance.

Les appliances Citrix SD-WAN prennent en charge les protocoles IPv4 et IPv6. Vous pouvez configurer IPv4, IPv6 ou les deux (double pile). Lorsque les protocoles IPv4 et IPv6 sont configurés, le protocole IPv4 a priorité sur le protocole IPv6.

REMARQUE

- Pour configurer une adresse IPv4 ou IPv6 dans des configurations spécifiques à une fonctionnalité, assurez-vous que le même protocole est activé et configuré en tant que protocole d'interface de gestion. Par exemple, si vous souhaitez configurer une adresse IPv6 pour un serveur SMTP, assurez-vous qu'une adresse IPv6 est configurée comme adresse d'interface de gestion.
- Les adresses locales de liaison (adresses IPv6 commençant par « fe80 ») ne sont pas autorisées.
- Pour configurer une adresse IPv6, vous devez disposer d'un routeur dans le réseau qui annonce l'adresse IPv6.

Les procédures sont différentes pour définir l'adresse IP de gestion d'une appliance SD-WAN matérielle et d'une appliance virtuelle VPX (Citrix SD-WAN VPX-SE). Pour obtenir des instructions sur la configuration de l'adresse pour chaque type d'appliance, reportez-vous aux rubriques suivantes :

- **Appliance virtuelle SD-WAN VPX :** reportez-vous aux sections [Configuration de l'adresse IP de gestion pour le SD-WAN VPX-SE](#) et [Différences entre une installation SD-WAN VPX-SE et SD-WAN WANOP VPX](#).

Pour configurer l'adresse IP de gestion pour une appliance SD-WAN matérielle, procédez comme suit :

Remarque

Vous devez répéter la procédure suivante pour chaque appliance matérielle que vous souhaitez ajouter à votre réseau.

1. Si vous configurez une appliance SD-WAN matérielle, connectez physiquement l'appliance à un PC.
 - Si vous ne l'avez pas encore fait, connectez une extrémité d'un câble Ethernet au port de gestion de l'appliance et l'autre extrémité au port Ethernet par défaut sur le PC.

Remarque

Assurez-vous que le port Ethernet est activé sur le PC que vous utilisez pour vous connecter à l'appliance.

2. Enregistrez les paramètres de port Ethernet actuels du PC que vous utilisez pour définir l'adresse IP de gestion du matériel.

Vous devez modifier les paramètres du **port Ethernet** sur le PC avant de pouvoir définir l'adresse IP de gestion de l'appliance. Veillez à enregistrer les paramètres d'origine afin de pouvoir les restaurer après avoir configuré l'adresse IP de gestion.

3. Modifiez l'adresse IP du PC.

Sur le PC, ouvrez les paramètres de l'interface réseau et modifiez l'adresse IP de votre PC comme suit :

- 192.168.100.50

4. Modifiez le paramètre **Masque de sous-réseau** sur votre PC comme suit :

- 255.255.0.0

5. Sur le PC, ouvrez un navigateur et entrez l'adresse IP par défaut de l'appliance. Entrez l'adresse IP suivante dans la ligne d'adresse du navigateur :

- 192.168.100.1

Remarque

Il est recommandé d'utiliser le navigateur Google Chrome lorsque vous vous connectez à une appliance SD-WAN.

Ignorer les avertissements de certificat de navigateur pour l'Interface Web de gestion.

L'écran de connexion de l'interface Web de gestion SD-WAN s'ouvre sur l'appliance connectée.

6. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur **Connexion**.

- Nom d'utilisateur administrateur par défaut : *admin*
- Mot de passe de l'administrateur par défaut

Remarque

Il est recommandé de modifier le mot de passe par défaut. Veillez à enregistrer le mot de passe dans un emplacement sécurisé, car la récupération de mot de passe peut nécessiter une réinitialisation de la configuration.

Une fois connecté à l'interface Web de gestion, la page **Tableau de bord** s'affiche, comme illustré ci-dessous.

The screenshot shows the 'Dashboard' tab of the Citrix SD-WAN 11.4 interface. It contains three main sections:

- System Status:**
 - Name: MCN_23
 - Model: VPX
 - Sub-Model: BASE
 - Appliance Mode: MCN
 - Serial Number: 67e0772c-5190-a2ee-d183-9244189b30a0
 - Management IP Address: 10.102.78.154
 - Appliance Uptime: 1 days, 10 hours, 49 minutes, 48.5 seconds
 - Service Uptime: 1 days, 10 hours, 42 minutes, 20.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions:**
 - Software Version: 10.1.0.111.690027
 - Built On: Jun 21 2018 at 23:42:30
 - Hardware Version: VPX
 - OS Partition Version: 4.6
- Virtual Path Service Status:**
 - Virtual Path MCN_23-Site: Uptime: 1 days, 10 hours, 39 minutes, 19.0 seconds.

La première fois que vous vous connectez à l'interface Web de gestion sur une appliance, le **tableau de bord** affiche une icône d'alerte (delta de la verge d'or) et un message d'alerte indiquant que le service SD-WAN est désactivé et que la licence n'a pas été installée. Pour l'instant, vous pouvez ignorer cette alerte. L'alerte sera résolue après avoir installé la licence et terminé le processus de configuration et de déploiement de l'appliance.

7. Dans la barre de menus principale, sélectionnez l'onglet **Configuration**.

L'arborescence de navigation **Configuration** s'affiche dans le volet gauche de l'écran. L'arborescence de navigation **Configuration** contient les trois branches principales suivantes :

- Paramètres de l'appliance
- Réseau étendu virtuel
- Maintenance du système

Lorsque vous sélectionnez l'onglet **Configuration**, la branche **Paramètres de l'appliance** s'ouvre automatiquement, avec la page **Interface Administrateur** présélectionnée par défaut, comme illustré dans la figure ci-dessous.

The screenshot shows the 'Configuration' tab of the Citrix SD-WAN 11.4 interface. The left sidebar shows the navigation tree with 'Administrator Interface' selected. The main content area displays the 'Administrator Interface' configuration page, which includes several sections:

- User Accounts:** Includes tabs for User Accounts, RADIUS, TACACS+, HTTPS Cert, HTTPS Settings, and Miscellaneous.
- Change Local User Password:** A form with fields for User Name (admin), Current Password, New Password, and Confirm New Password, with a 'Change Password' button.
- Delete Workspace For User:** A section with a warning message and a form to delete a user's workspace, including a 'Delete Selected User's Workspace' button.
- Manage Users:** A section with an 'Add User...' button, a note about deleting users, and a 'Delete Selected User' button.

8. Dans la branche **Paramètres du matériel** de l'arborescence de navigation, sélectionnez **Cartes réseau**. Cela affiche la page Paramètres **des cartes réseau** avec l'onglet **Adresse IP** présélectionné par défaut, comme illustré dans la figure ci-dessous.

The screenshot displays the 'Network Adapters' configuration page in the Citrix SD-WAN 11.4 interface. The left sidebar shows the navigation tree with 'Network Adapters' selected. The main content area is divided into several sections: 'Management Interface IP' (with 'DHCP' and 'Manual' tabs), 'DNS Settings', 'Management Interface Whitelist', 'Management Interface DHCP Server', and 'Management Interface DHCP Relay'. The 'IP Address' tab is active, showing the 'DHCP' settings with 'Enable DHCP' checked and the 'Manual' settings with IP Address: 10.102.78.154, Subnet Mask: 255.255.255.0, and Gateway IP Address: 10.102.78.1. The 'Management Interface DHCP Server' section shows 'DHCP Server Status: stopped' and 'Enable DHCP Server' checked. The 'Management Interface DHCP Relay' section is at the bottom.

9. Dans l'onglet Adresse IP, activez l'une des options suivantes :

- **Protocole IPv4** : pour activer l'adresse IPv4, **activez la case à cocher Activer IPv4** . Le protocole DHCP (Dynamic Host Control Protocol) attribue une adresse IP et d'autres paramètres de configuration réseau dynamiquement à chaque périphérique du réseau. Sélectionnez **Activer le protocole DHCP** pour affecter dynamiquement l'adresse IP. Pour configurer manuellement l'adresse IP, fournissez les détails suivants :
 - Adresse IP
 - Masque de sous-réseau
 - Adresse IP de la passerelle

- **Protocole IPv6** : pour activer l'adresse IPv6, **activez la case à cocher Activer IPv6**. Vous pouvez configurer manuellement l'adresse IPv6 ou activer DHCP ou SLAAC pour attribuer automatiquement l'adresse IP.

Pour configurer manuellement, fournissez les détails suivants :

- Adresse IP
- Préfixe

Pour configurer SLAAC, activez la case à cocher **SLAAC**. SLAAC attribue automatiquement une adresse IPv6 à chaque périphérique du réseau. SLAAC permet à un client IPv6 de générer ses propres adresses à l'aide d'une combinaison d'informations disponibles localement et d'informations annoncées par les routeurs via NDP (Neighbor Discovery Protocol).

Pour configurer DHCP, activez la case à cocher **DHCP**. Pour activer le protocole DHCP sans état, activez les cases à cocher **SLAAC** et **DHCP**.

- **Protocoles IPv4 et IPv6** : **activez les cases à cocher Activer IPv6 et Activer IPv4** pour activer les protocoles IPv4 et IPv6. Dans de tels scénarios, l'apppliance SD-WAN dispose d'une adresse IP de gestion IPv4 et d'une adresse de gestion IPv6.

REMARQUE

- L'adresse IP de gestion doit être unique pour chaque appliance.
- Les sections **Serveur DHCP** et **Relais DHCP de l'interface de gestion** de l'onglet Adresse IP ne s'appliquent que si le protocole IPv4 est activé dans l'interface de gestion.
- Lorsque l'interface de gestion joue le rôle de client DHCP, le nom d'hôte est utilisé dans les messages du client DHCP en tant qu'option 12. À partir de Citrix SD-WAN version 11.2.3 et jusqu'à la version 11.4.1, le nom d'hôte a été défini comme **sdwan**. À partir de Citrix SD-WAN version 11.4.1, le nom d'hôte est identique au nom du site. Si le nom du site est modifié ou configuré pour la première fois, jusqu'à ce que la mise à jour de la configuration soit terminée et que le service WAN virtuel soit en service, l'ancien nom de site ou **sdwan** est utilisé comme nom d'hôte dans les messages du client DHCP. Une fois la mise à jour de la configuration terminée et le service WAN virtuel est en service, les messages du client DHCP suivants utilisent le nouveau nom de site.

10. Cliquez sur **Modifier les paramètres**. Une boîte de dialogue de confirmation s'affiche et vous invite à vérifier que vous souhaitez modifier ces paramètres.
11. Cliquez sur **OK**.
12. Remplacez les paramètres d'interface réseau de votre PC par les paramètres d'origine.

Remarque

La modification de l'adresse IP de votre PC ferme automatiquement la connexion à l'appliance et met fin à votre session de connexion sur l'interface Web de gestion.

13. Déconnectez l'appliance du PC et connectez-la à votre routeur ou commutateur réseau. Déconnectez le câble Ethernet du PC, mais ne le déconnectez pas de votre appliance. Connectez l'extrémité libre du câble à votre routeur ou commutateur réseau.

L'appliance SD-WAN est désormais connectée à votre réseau et disponible sur celui-ci.

14. Testez la connexion. Sur un PC connecté à votre réseau, ouvrez un navigateur et entrez l'adresse IP de gestion que vous avez configurée pour l'appliance au format suivant :

Pour l'adresse IPv4 : `https://<IPv4 address>`

Exemple : `https://10.10.2.3`

Pour l'adresse IPv6 : `https://<[IPv6 address]>`

Exemple : `https://[fd73:xxxx:yyyy:26::9]`

Si la connexion réussit, l'écran de **connexion** de l'interface Web de gestion SD-WAN de l'appliance que vous avez configurée s'affiche.

Conseil

Après avoir vérifié la connexion, ne vous déconnectez pas de l'interface Web de gestion. Vous l'utilisez pour effectuer les tâches restantes décrites dans les sections suivantes.

Vous avez maintenant défini l'adresse IP de gestion de votre appliance SD-WAN et vous pouvez vous connecter à l'appliance depuis n'importe quel emplacement de votre réseau.

Liste d'autorisation de l'interface de gestion

La liste autorisée est une liste approuvée d'adresses IP ou de domaines IP autorisés à accéder à votre interface de gestion. Une liste vide permet d'accéder à l'interface de gestion depuis tous les réseaux. Vous pouvez ajouter des adresses IP pour vous assurer que l'adresse IP de gestion est accessible uniquement par les réseaux approuvés.

Pour ajouter ou supprimer une adresse IPv4 à la liste autorisée, vous devez accéder à l'interface de gestion de l'appliance SD-WAN à l'aide d'une adresse IPv4 uniquement. De même, pour ajouter ou supprimer une adresse IPv6 à la liste autorisée, vous devez accéder à l'interface de gestion du matériel SD-WAN à l'aide d'une adresse IPv6 uniquement.

Management Interface Whitelist

An empty Whitelist allows Management Interface to be accessed from all networks.

V4 networks can be added/removed only from a V4 network.

V6 networks can be added/removed only from a V6 network.

Add Network(s):

[Change Settings](#)

Définir la date et l'heure

May 6, 2021

Avant d'installer la licence logicielle SD-WAN sur une appliance, vous devez définir la date et l'heure de l'appliance.

Remarque

- Vous devez répéter ce processus pour chaque appliance que vous souhaitez ajouter à votre réseau.
- Si l'heure actuelle est modifiée manuellement ou via le serveur NTP et que l'heure nouvellement définie est supérieure à la temporisation de la session, la session d'interface utilisateur est déconnectée.

Pour définir la date et l'heure, procédez comme suit :

1. Connectez-vous à l'interface Web de gestion de l'appliance que vous configurez.
2. Dans la barre de menus principale, sélectionnez l'**onglet Configuration**.
L'arborescence de navigation **Configuration** s'affiche dans le volet gauche de l'écran.
3. Ouvrez la **branche Maintenance du système** dans l'arborescence de navigation.
4. Sous la **branche Maintenance du système**, sélectionnez **Paramètres de date/heure**. La page **Paramètres de date/heure** s'affiche comme suit.

Configuration

Configuration > System Maintenance > Date/Time Settings

Note: If the Appliance date/time is turned back due to NTP or manual changes, Reporting artifacts may occur. These can be cleared by creating a new archive of the current database on the Reports screens.

NTP Settings

Use NTP Server ☒

Server Address:

[Change Settings](#)

Date/Time Settings

Date:

Time:

[Change Date](#)

Timezone Settings

Note: After changing the timezone setting, a reboot will also be necessary for any timezone changes to take full effect. Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.

Time Zone:

[Change Timezone](#)

5. Sélectionnez le fuseau **horaire** dans le **menu déroulant du champ Fuseau** horaire en bas de la page.

Remarque

Si vous devez modifier le paramètre de fuseau horaire, vous devez le faire avant de définir la date et l'heure, sinon vos paramètres ne persistent pas comme ils sont entrés.

6. Cliquez sur **Modifier le fuseau horaire**. Cela met à jour le fuseau horaire et recalcule en conséquence la date et l'heure actuelles. Si vous définissez la date et l'heure correctes avant cette étape, vos paramètres ne sont plus corrects. Une fois la mise à jour du fuseau horaire terminée, une icône Alerte de succès (coche verte) et un message d'état s'affichent dans la partie supérieure de la page.
7. (Facultatif) Activer le service Serveur NTP.
 - a) Sélectionnez **Utiliser le serveur NTP**.
 - b) Entrez l'adresse du serveur dans le champ **Adresse du serveur**.
 - c) Cliquez sur **Modifier les paramètres**.
Une icône d'alerte de succès (coche verte) et un message d'état s'affichent lorsque la mise à jour est terminée.
8. Sélectionnez le mois, le jour et l'année dans les menus déroulants du champ **Date**.

9. Sélectionnez l'heure, les minutes et les secondes dans les menus déroulants du champ **Heure**.
10. Cliquez sur **Modifier la date**.

Remarque :

Cela met à jour le paramètre de date et d'heure, mais n'affiche pas d'icône d'alerte de succès ou de message d'état.

L'étape suivante consiste à définir le seuil de **temporisation** de la session de la console sur la valeur maximale. Cette étape est facultative, mais recommandée. Cela empêche la session de se terminer prématurément pendant que vous travaillez sur la configuration, ce qui peut entraîner une perte de travail. Les instructions relatives à la définition de la valeur **Délai d'expiration** de session de console sont fournies dans la section suivante. Si vous ne souhaitez pas réinitialiser le seuil de délai d'expiration, vous pouvez passer directement à la section, [Téléchargement et installation du fichier de licence du logiciel SD-WAN](#).

Avertissement

Si votre session de console expire ou si vous vous déconnectez de l'interface Web de gestion avant d'enregistrer votre configuration, les modifications de configuration non enregistrées sont perdues. Reconnectez-vous au système et répétez la procédure de configuration dès le début.

Expiration de session

May 6, 2021

Si votre session de console expire ou si vous vous déconnectez de l'interface Web de gestion avant d'enregistrer votre configuration, les modifications de configuration non enregistrées sont perdues. Vous devez ensuite vous reconnecter au système et répéter la procédure de configuration dès le début. Pour cette raison, il est recommandé de définir l'intervalle de **délai d'attente de session de console** sur une valeur élevée lors de la création ou de la modification d'un package de configuration ou de l'exécution d'autres tâches complexes. La valeur par défaut est 60 minutes. Le maximum est de 9 999 minutes. Pour des raisons de sécurité, vous devez ensuite le réinitialiser à un seuil inférieur après avoir terminé ces tâches.

Pour réinitialiser l'intervalle de **temporisation** de la session de la console, procédez comme suit :

1. Sélectionnez l'onglet **Configuration**, puis sélectionnez la branche **Paramètres de l'appliance** dans l'arborescence de navigation.

La page **Paramètres de l'appliance** s'affiche, avec l'onglet **Comptes d'utilisateurs** présélectionné par défaut.

Configuration > Appliance Settings

User Accounts | RADIUS | TACACS+ | HTTPS Cert | **Miscellaneous**

Change Local User Password

User Name: admin ▼

Current Password:

New Password:

Confirm New Password:

- Sélectionnez l'onglet **Divers** (dans le coin droit).

La page de l'onglet **Divers** s'affiche.

Configuration > Appliance Settings

User Accounts | RADIUS | TACACS+ | HTTPS Cert | **Miscellaneous**

Change Web Console Timeout

Timeout: 60 Enter the new timeout value in minutes (1-9999).

Switch to Client Console

Switch the mode of the Web Console to enable configuration of Client functionality.

- Entrez la valeur **Délai d'expiration de** la console.

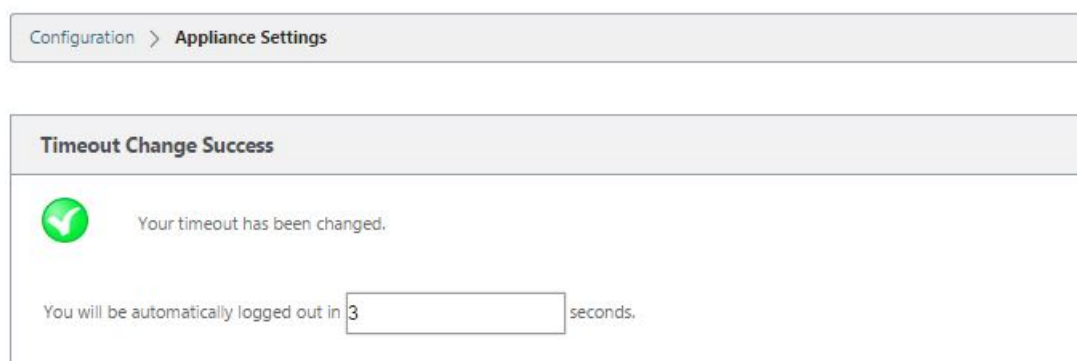
Dans le champ Délai d'**expiration** de la section **Modifier le délai d'expiration de la console Web**, entrez une valeur supérieure (en minutes) jusqu'à la valeur maximale de 9999. La valeur par défaut est 60, ce qui est beaucoup trop bref pour une session de configuration initiale.

Remarque

Pour des raisons de sécurité, veuillez à réinitialiser cette valeur à un intervalle inférieur après avoir terminé la configuration et le déploiement.


- Cliquez sur **Modifier le délai d'expiration**.

Cela réinitialise l'intervalle de **temporisation** de la session et affiche un message de réussite lorsque l'opération est terminée.



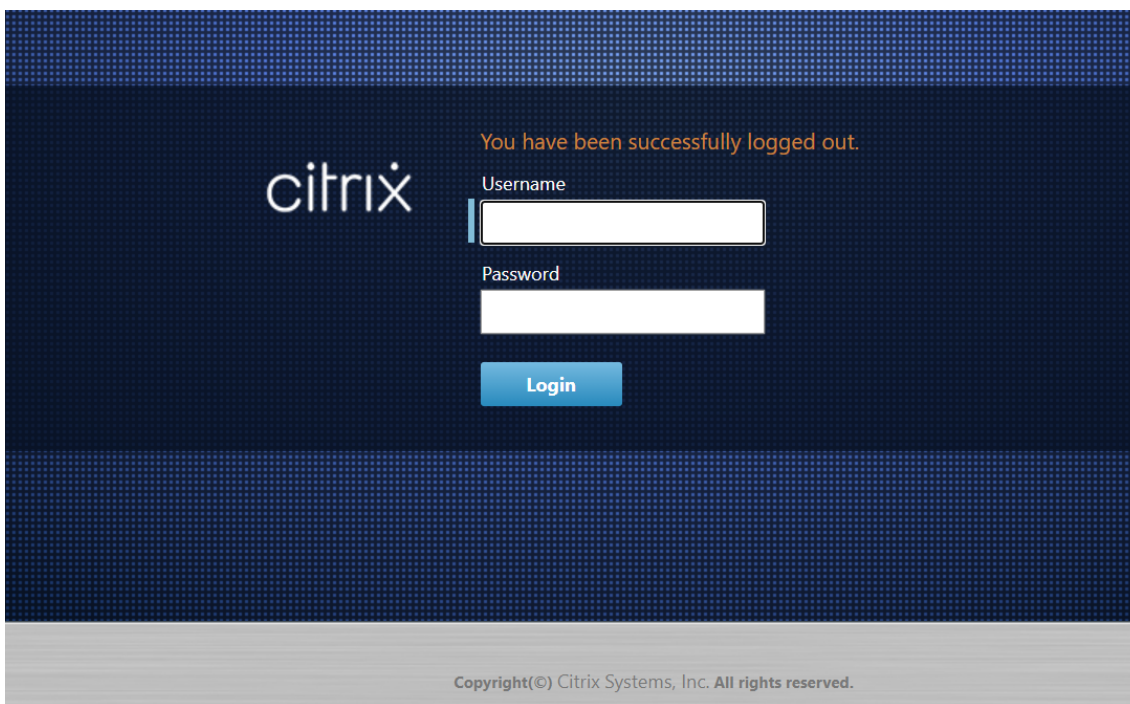
Configuration > Appliance Settings

Timeout Change Success

 Your timeout has been changed.

You will be automatically logged out in seconds.

Après un bref intervalle (quelques secondes), la session est interrompue et vous êtes automatiquement déconnecté de l'interface Web de gestion. La page Connexion apparaît.





You have been successfully logged out.

Username

Password

Login

Copyright(©) Citrix Systems, Inc. All rights reserved.

5. Entrez le nom d'utilisateur administrateur (*admin*) et le mot de passe (*mot de passe*), puis cliquez sur **Connexion**.

L'étape suivante consiste à télécharger et installer le fichier de licence du logiciel SD-WAN sur l'appliance.

Configurer les alarmes

May 6, 2021

Vous pouvez désormais configurer votre appliance SD-WAN pour identifier les conditions d'alarme en fonction de votre réseau et de vos priorités, générer des alertes et recevoir des notifications par e-mail, syslog ou interruptions SNMP.

Une alarme est une alerte configurée comprenant un type d'événement, un état de déclenchement, un état d'effacement et une gravité.

Pour configurer les paramètres d'alarme :

1. Dans l'interface de gestion Web SD-WAN, accédez à **Configuration > Paramètres de l'appliance > Logging/Monitoring**, puis cliquez sur **Options d'alarme**.
2. Cliquez sur **Ajouter une alarme pour** ajouter une nouvelle alarme.

Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog	SNMP
PATH	DEAD	0	GOOD	0	EMERGENCY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VIRTUAL PATH	DEAD	0	GOOD	0	CRITICAL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN LINK	DEAD	0	GOOD	0	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

3. Sélectionnez ou entrez des valeurs pour les champs suivants :

- **Type d'événement** : l'appliance SD-WAN peut déclencher des alarmes pour des sous-systèmes ou des objets particuliers du réseau, appelés types d'événements. Les types d'événements disponibles sont SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL et IPSEC_TUNNEL.
- **État de déclenchement** : état de l'événement qui déclenche une alarme pour un type d'événement. Les options d'état de déclenchement disponibles dépendent du type d'événement choisi.
- **Durée du déclenchement** : la durée en secondes détermine la vitesse à laquelle l'appliance déclenche une alarme. Entrez '0' pour recevoir des alertes immédiates ou entrez une valeur comprise entre 15 et 7200 secondes. Les alarmes ne sont pas déclenchées si d'autres événements se produisent sur le même objet au cours de la période Trigger

Duration. D'autres alarmes sont déclenchées uniquement si un événement persiste plus longtemps que la durée du déclenchement.

- **Effacer l'état** : état de l'événement qui efface une alarme pour un type d'événement après le déclenchement de l'alarme. Les options d'effacement disponibles dépendent de l'état de déclenchement choisi.
- **Effacer la durée** : durée en secondes, cela détermine la durée d'attente avant d'effacer une alarme. Entrez '0' pour effacer immédiatement l'alarme ou entrez une valeur comprise entre 15 et 7200 secondes. L'alarme n'est pas effacée si un autre événement d'état d'effacement se produit sur le même objet dans le délai spécifié.
- **Gravité** : champ défini par l'utilisateur qui détermine l'urgence d'une alarme. La gravité est affichée dans les alertes envoyées lorsque l'alarme est déclenchée ou effacée et dans le récapitulatif de l'alarme déclenchée.
- **Email** : Le déclencheur d'alarme et les alertes effacées pour le type d'événement sont envoyées par e-mail.
- **Syslog** : le déclencheur d'alarme et les alertes effacées pour le type d'événement sont envoyées via Syslog.
- **SNMP** : le déclencheur d'alarme et les alertes effacées pour le type d'événement sont envoyées via l'interception SNMP.

4. Continuez à ajouter des alarmes au besoin.

5. Cliquez sur **Appliquer les paramètres**.

Affichage des alarmes déclenchées

Pour afficher un résumé de toutes les alarmes déclenchées :

Dans l'interface de gestion Web SD-WAN, accédez à **Configuration > Maintenance du système > Diagnostics > Alarmes**.

Une liste de toutes les alarmes déclenchées s'affiche.

System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Alarms

Enable Auto Refresh

Time Interval5seconds

Refresh

Clear Checked Alarms

Clear All Alarms

Triggered Alarms Summary

Filters

Any column

Apply

Show100entries

Showing 1 to 11 of 11 entries

FirstPrevious1NextLast

Severity	Event Type	Object Name	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Clear Action
EMERGENCY	PATH	Client-1-WL-1-3G->MCN-WL-1-MPLS	DEAD	0	GOOD	0	<input type="checkbox"/>
EMERGENCY	PATH	Client-1-WL-1-MPLS->MCN-WL-1-MPLS	DEAD	0	GOOD	0	<input type="checkbox"/>
CRITICAL	VIRTUAL_PATH	MCN-DC:Client-1	DEAD	0	GOOD	0	<input type="checkbox"/>
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-1-WL-1-3G	DEAD	0	GOOD	0	<input type="checkbox"/>
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-1-WL-1-MPLS	DEAD	0	GOOD	0	<input type="checkbox"/>
EMERGENCY	PATH	Client-2-WL-1-MPLS->MCN-WL-1-MPLS	DEAD	0	GOOD	0	<input type="checkbox"/>
EMERGENCY	PATH	Client-2-WL-1-3G->MCN-WL-1-MPLS	DEAD	0	GOOD	0	<input type="checkbox"/>
CRITICAL	VIRTUAL_PATH	MCN-DC:Client-2	DEAD	0	GOOD	0	<input type="checkbox"/>
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-2-WL-1-3G	DEAD	0	GOOD	0	<input type="checkbox"/>
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-2-WL-1-MPLS	DEAD	0	GOOD	0	<input type="checkbox"/>
ERROR	WAN_LINK	MCN-WL-1-MPLS	DEAD	0	GOOD	0	<input type="checkbox"/>

Showing 1 to 11 of 11 entries

FirstPrevious1NextLast

Effacement des alarmes déclenchées

Pour effacer manuellement les alarmes déclenchées :

1. Dans l’interface de gestion Web SD-WAN, accédez à **Configuration > Maintenance du système > Diagnostics > Alarmes.**

2. Dans la colonne **Effacer l’action**, sélectionnez les alarmes à effacer.

3. Cliquez sur **Effacer les alarmes cochées**. Vous pouvez également cliquer sur **Effacer toutes les alarmes** pour effacer toutes les alarmes.

Configurer la restauration

May 6, 2021

La fonction de restauration de la configuration permet au système de gestion des modifications de détecter et de récupérer les erreurs logiciels/de configuration suivantes en revenant au logiciel/con-figuration précédemment actif :

- Après une mise à niveau logicielle, le chemin virtuel est mort et le service est désactivé si le logiciel se bloque.

• Après avoir apporté les modifications de configuration, Virtual Path est mort sans aucun plan-tage logiciel.

• Si la configuration de l’appliance MCN elle-même provoque un problème de réseau sur le site MCN, elle ne détecte pas la panne et ne se retourne pas en arrière. Cependant, tous les autres clients du réseau se retrouvent en arrière car ils n’ont pas pu se connecter au MCN.

La fonction d'annulation de configuration est activée par défaut, pour désactiver cette fonctionnalité, désactivez l'option **Rétablir en cas d'erreur** dans l'onglet **Activation** de l'Assistant Gestion des modifications.

Configuration > Virtual WAN > Change Management

Activate

Activating the new software/configuration that is currently staged may cause a traffic interruption as indicated in table below.

You may now activate the staged changes that have been distributed across your network. Each appliance will apply the changes. For software updates, the Citrix Virtual WAN Service will be restarted.

Activating staged changes will cause any currently triggered alarms to be silently cleared.

Note: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve.

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Warning: If you have Enterprise Edition appliances in your network, activating the staged changes may cause **traffic disruption**.
Activating staged changes will cause any currently triggered alarms to be silently cleared

Note: For software upgrade, please follow the instructions in release documentation.

Activate Staged Abort ☒ **Revert on Error** Done

Currently Prepared: Configuration - Config-30May.cfg Software - Current Running

Si une erreur de configuration système se produit sur un client lors de l'activation du package de mise en scène à partir d'un MCN, le client revient à la configuration logicielle précédente et un message d'erreur s'affiche comme illustré dans la capture d'écran suivante.

Le client génère un événement de gravité critique pour l'objet SOFTWARE_UPDATE si un plantage de matériel est détecté, ou génère un événement de gravité critique pour l'objet CONFIG_UPDATE si une panne réseau est détectée.

Dashboard Monitoring Configuration

Click here to collapse the navigation tree

- Logging/Monitoring
- Network Adapters
- Net Flow
- SNMP
- Licensing
- + Virtual WAN
- + System Maintenance

Configuration > Appliance Settings > Administrator Interface

Error:

- This appliance experienced a network outage after an update. Local Change Management has rolled back to the staged software and configuration to resolve the problem.

User Accounts RADIUS TACACS+ HTTPS Cert HTTPS Settings Miscellaneous

Change Local User Password

User Name: admin

Current Password:

New Password:

Confirm New Password:

Change Password

Delete Workspace For User

Delete the selected user's Configuration Editor workspace. This action will not delete the user. Deleting a workspace will remove all saved configurations and network maps for the selected user.

User Name: admin Delete Selected User's Workspace

Manage Users

Add User...

Note: Deleting a user will also delete local files for that user.

User Name: Delete Selected User

Si l’option **Rétablir en cas d’erreur** est activée, les appliances clientes se surveillent pendant environ 30 minutes. Si le logiciel se bloque dans les 30 minutes ou si le réseau est en panne (impossible d’établir un chemin virtuel vers le MCN) pendant 30 minutes, une restauration est déclenchée.

Sur le MCN, un message d’erreur apparaît comme illustré dans la capture d’écran suivante. Lorsque les clients rejoignent le réseau, il signale le type d’erreur rencontrée. Un compte récapitulatif du nombre d’erreurs s’affiche dans le message d’erreur.

Appliance Settings

Virtual WAN

View Configuration

Configuration Editor

Change Management

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

System Maintenance

Configuration > Virtual WAN > Change Management

Error:

This MCN has rolled back the network software and/or configuration to the previous version due to errors detected on the network. A summary of problems follows.

Software Errors : 1

Configuration Errors : 1

Please view [Change Management](#) for a complete list of branch nodes. The nodes with errors will be marked.

Overview

Change Process Overview

The Change Management process allows a user to upload changes to the network, whether it be a configuration, software, or both. This three-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied in a reliable, fail-safe way.

Step 1

Change Preparation

Upload Files to MCN

MCN

Step 2

Appliance Staging

Transfer Files to Clients

MCN

Step 3

Activation

Activate Change

MCN

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a previously-staged appliance package (if present).

Activate Staged

Begin --

Configuration Filenames:

Active - Basic_Valid_Config.zip

Staged - Basic_Valid_Config.zip

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Dallas_MCN-Appliance	CBVPX	Software Error	9.3.0.952.99998118	4:37 on 6/12/17	9.3.0.952.99998118	10:56 on 6/12/17	0 sec		active / staged
Dallas_MCN-Dallas_HA_secondary	CBVPX		9.3.0.952.99998118	4:37 on 6/12/17	9.3.0.952.99998118	10:56 on 6/12/17	0 sec	0 ms	active / staged
Bangalore-Bangalore-CBVPX	CBVPX		9.3.0.952.99998118	4:37 on 6/12/17	9.3.0.952.99998118	10:56 on 6/12/17	0 sec	0 ms	active / staged
Bangalore-BLR_HA_secondary	CBVPX		9.3.0.952.99998118	4:37 on 6/12/17	9.3.0.952.99998118	10:56 on 6/12/17	0 sec	0 ms	active / staged
Beijing-Appliance	CBVPX		9.3.0.952.99998118	4:37 on 6/12/17	9.3.0.952.99998118	10:56 on 6/12/17	0 sec	0 ms	active / staged
SanJose-Appliance	CB2000	Configuration Error	9.3.0.952.99998118	4:37 on 6/12/17	9.3.0.952.99998118	10:56 on 6/12/17	0 sec	63 ms	active / staged

Dans la fenêtre **Gestion des modifications** du MCN, vous pouvez voir l’état des appliances de site indiquant si ce site a rencontré une erreur logicielle ou une erreur de configuration.

Configurer le nœud de contrôle maître

May 6, 2021

Le **SD-WAN Master Control Node (MCN)** est l’appliance de tête de ligne du réseau étendu virtuel. En général, il s’agit d’une appliance Virtual WAN 4000 ou 5100 déployée dans le datacenter de l’entreprise. Le MCN sert de point de distribution pour la configuration initiale du système et toute modification ultérieure de configuration. En outre, vous effectuez la plupart des procédures de mise à niveau via l’interface Web de gestion sur le MCN. Il ne peut y avoir qu’un seul MCN actif dans un WAN virtuel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

159

Par défaut, les appliances ont le rôle préassigné de client. Pour établir une appliance en tant que MCN, vous devez d'abord ajouter et configurer le site MCN, puis configurer et activer la configuration et le package logiciel approprié sur l'appliance MCN désignée.

Informations supplémentaires sur le déploiement du site MCN

Les articles de support de la Base de connaissances suivants sont recommandés :

- Étapes de déploiement du mode PBR virtuel WAN ([CTX201577](http://support.citrix.com/article/CTX201577))
<http://support.citrix.com/article/CTX201577>
- Étapes de déploiement du mode passerelle WAN virtuelle ([CTX201576](http://support.citrix.com/article/CTX201576))
<http://support.citrix.com/article/CTX201576>

Présentation des procédures de configuration du site MCN

Les étapes d'ajout et de configuration du site MCN sont les suivantes :

1. Basculez l'interface Web de gestion en mode **console MCN** .
2. Ajoutez le site MCN.
3. Configurez les groupes d'interface virtuelle pour le site MCN.
4. Configurez les adresses IP virtuelles pour le site MCN.
5. (Facultatif) Configurez les tunnels GRE LAN pour le site.
6. Configurez les liens WAN pour le site MCN.
7. Configurez les interfaces d'accès pour le site MCN.
8. Configurez les itinéraires pour le site MCN.
9. (Facultatif) Configurez la haute disponibilité pour le site MCN.
10. (Facultatif) Configurez la sécurité et le chiffrement Virtual WAN.
11. Nommez et enregistrez la configuration du site MCN.

Les instructions pour chacune de ces tâches sont fournies dans les sections suivantes.

Présentation MCN

May 6, 2021

Le **MCN (Master Control Node)** est le dispositif virtuel WAN central qui agit en tant que Contrôleur maître du Virtual WAN et point d'administration central pour les nœuds clients. Toutes les activités de configuration, ainsi que la préparation des packages d'appliance et leur distribution aux clients, sont effectuées sur le MCN. De plus, certaines informations de surveillance Virtual WAN ne sont disponibles que sur le MCN. Le MCN peut surveiller l'intégralité du réseau étendu virtuel, tandis que les nœuds clients ne peuvent surveiller que leurs intranets locaux, ainsi que certaines informations pour les clients avec lesquels ils sont connectés.

L'objectif principal du MCN est d'établir et d'utiliser des chemins virtuels avec un ou plusieurs nœuds clients situés sur le réseau WAN virtuel, pour les communications de site à site d'entreprise. Un MCN peut administrer et disposer de chemins virtuels vers plusieurs nœuds clients. Il peut y avoir plus d'un MCN, mais un seul peut être actif à un moment donné.

La figure ci-dessous illustre les rôles de base et le contexte des appliances MCN (centre de données) et client (nœud de succursale) pour un déploiement Virtual WAN Edition.



Passer à la console MCN

May 6, 2021

Pour ajouter et configurer le site MCN, vous devez d'abord vous connecter à l'interface Web de gestion de l'appliance que vous promouvez vers le rôle MCN, puis basculer l'interface Web de gestion en mode **Console MCN**. Le mode **Console MCN** permet d'accéder à l'éditeur de configuration dans l'interface Web de gestion à laquelle vous êtes actuellement connecté. Vous pouvez ensuite utiliser l'**Éditeur de configuration** pour ajouter et configurer le site MCN.

Remarque

Le passage en mode **Console MCN** modifie uniquement le mode de fonctionnement du mode Interface Web de gestion, et non le rôle actif de l'appliance elle-même. Pour promouvoir une appliance en tant que MCN, vous devez d'abord ajouter et configurer le site MCN et activer la configuration et le package logiciel sur l'appliance MCN désignée.

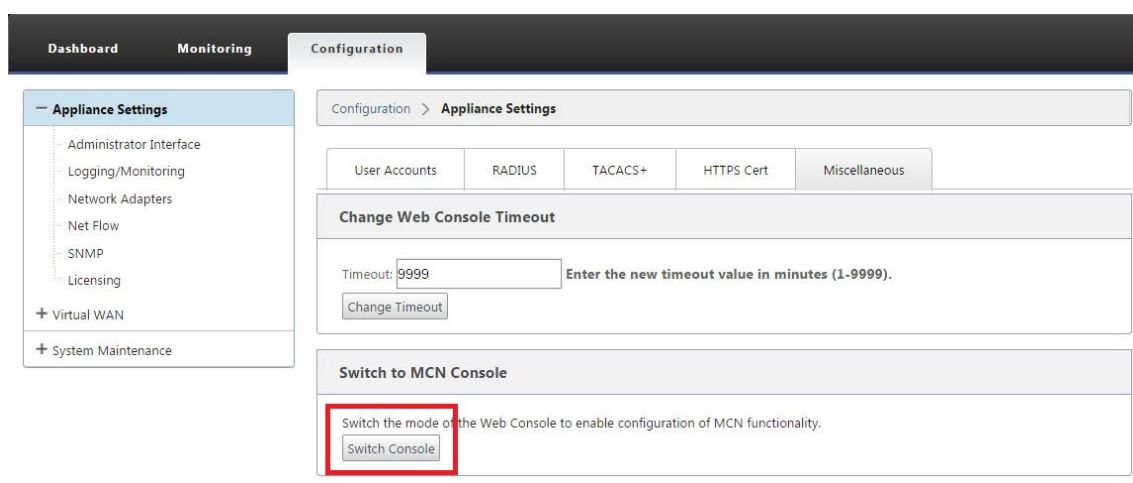
Pour basculer l'interface Web de gestion en mode **console MCN**, procédez comme suit :

1. Connectez-vous à l'interface Web de gestion sur l'appliance que vous souhaitez configurer en tant que MCN.
2. Cliquez sur **Configuration** dans la barre de menus principale de l'écran principal de l'interface Web de gestion (barre bleue en haut de la page).
3. Dans l'arborescence de navigation (volet gauche), ouvrez la branche **Paramètres de l'appliance** et cliquez sur **Interface administrateur**.

La page Interface Administrateur s'affiche dans le volet central.

4. Sélectionnez l'onglet **Divers**.

La page Paramètres administratifs divers s'affiche.



Au bas de l'onglet **Divers** se trouve la section **Basculer vers [Client > MCN Console]**. Cette section contient le bouton **Switch Console** permettant de basculer entre les modes de console de l'appliance.

L'en-tête de section indique le mode console actuel, comme suit :

- En mode **Console client** (par défaut), l'en-tête de section est **Switch to MCN Console**.
- En mode **Console MCN**, l'en-tête de section est **Switch to Client Console**.

Par défaut, une nouvelle appliance est définie en mode **Console client**.

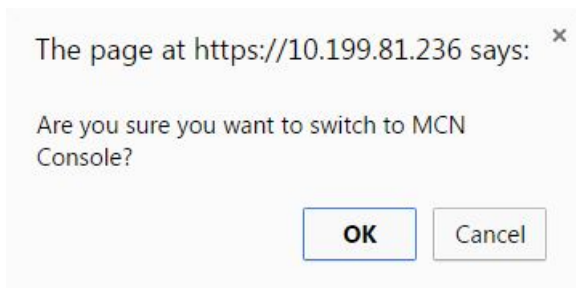
Le mode **Console MCN** active la branche **Éditeur de configuration** dans l'arborescence de navigation. L'**Éditeur de configuration** est disponible uniquement sur l'appliance MCN.

Remarque

Avant de passer à l'étape suivante, assurez-vous que l'appliance est toujours définie sur la valeur par défaut (mode **Console client**). L'en-tête de la section doit être : **Passer à la console MCN**.

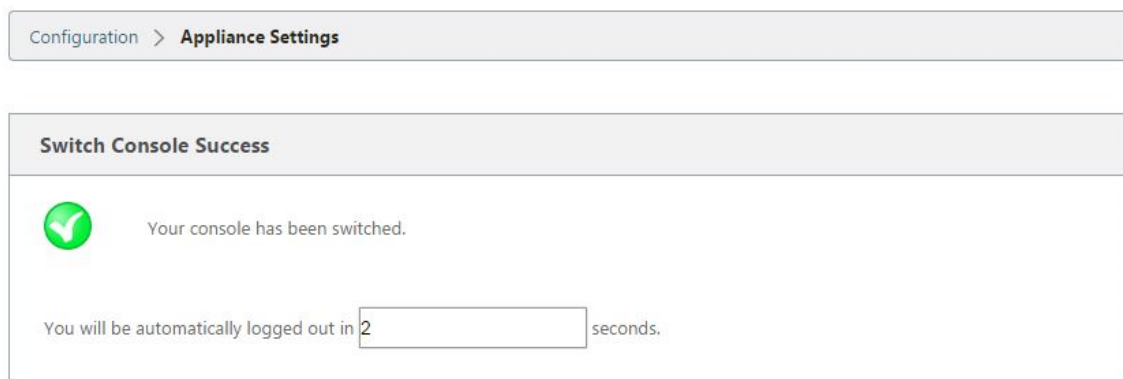
5. Cliquez sur **Mode de commutation** pour définir le mode de l'apppliance en mode **console MCN**.

Une boîte de dialogue vous invite à confirmer que vous souhaitez passer en mode MCN.



6. Cliquez sur **OK**.

Cela bascule le mode console en mode **console MCN** et met fin à la session en cours. Un message de réussite s'affiche, ainsi qu'un état de compte à rebours indiquant le nombre de secondes restant avant la fin de la session.



Une fois le compte à rebours terminé, la session est terminée et la page de connexion apparaît.



7. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur **Connexion**.

- Nom d'utilisateur administrateur par défaut : *admin*
- Mot de passe administrateur par défaut : *mot de passe*

Une fois connecté, le **tableau de bord** s'affiche, indiquant maintenant que l'appliance est en mode MCN.

The screenshot displays the Citrix SD-WAN 11.4 web interface. At the top, there are three tabs: **Dashboard**, **Monitoring**, and **Configuration**. The **Dashboard** tab is selected. Below the tabs, there are three main sections:

- System Status**: This section displays various system details:
 - Name: MCN_23
 - Model: VPX
 - Sub-Model: BASE
 - Appliance Mode: MCN
 - Serial Number: 67e0772c-5190-a2ee-d183-9244189b30a0
 - Management IP Address: 10.102.78.154
 - Appliance Uptime: 1 days, 10 hours, 49 minutes, 48.5 seconds
 - Service Uptime: 1 days, 10 hours, 42 minutes, 20.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions**: This section displays version information:
 - Software Version: 10.1.0.111.690027
 - Built On: Jun 21 2018 at 23:42:30
 - Hardware Version: VPX
 - OS Partition Version: 4.6
- Virtual Path Service Status**: This section displays the status of the virtual path service:
 - Virtual Path MCN_23-Site1: Uptime: 1 days, 10 hours, 39 minutes, 19.0 seconds.

L'étape suivante consiste à ouvrir une nouvelle configuration et à ajouter le site MCN à la table Sites, puis à commencer à configurer le nouveau site MCN.

Configurer MCN

May 6, 2021

La première étape consiste à ouvrir un nouveau package de configuration et à ajouter le site MCN à la nouvelle configuration.

Remarque

L'**Éditeur de configuration** est disponible uniquement en mode **Console MCN**. Si l'option **Éditeur de configuration** n'est pas disponible dans la branche Virtual WAN de l'arborescence de navigation, reportez-vous à la section [Basculer l'interface Web de gestion en mode console MCN](#), pour obtenir des instructions sur la modification du mode console.

Il est recommandé d'enregistrer le package de configuration souvent, ou à des points clés de

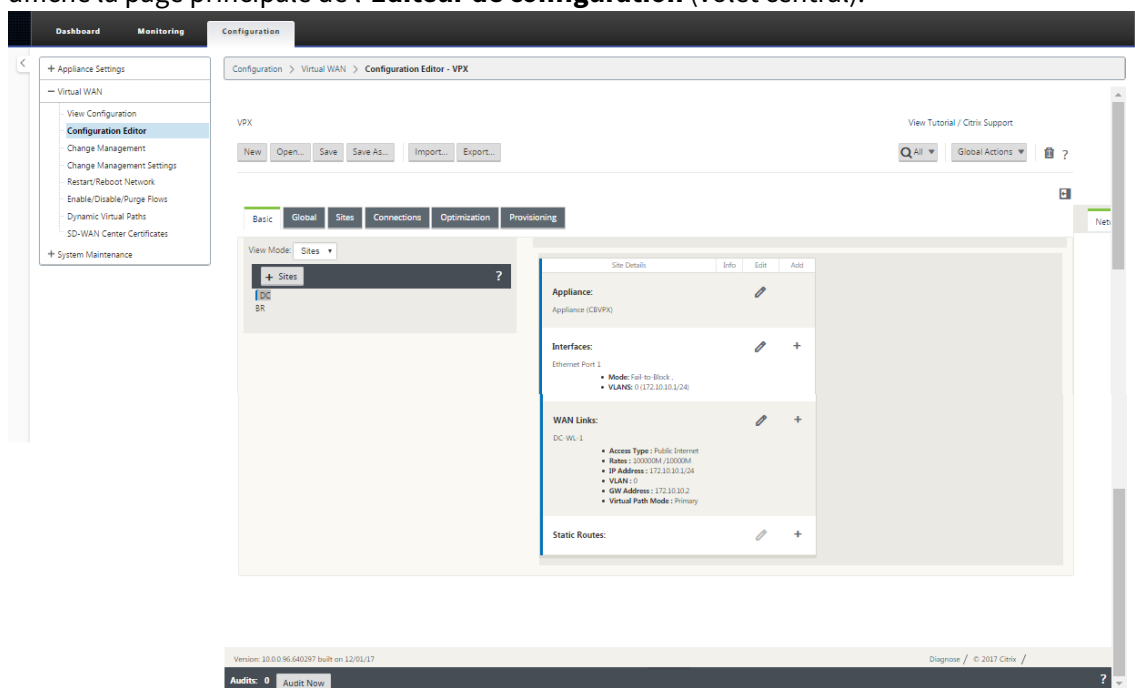
la configuration. Les instructions sont fournies dans la section [Nomination, enregistrement et sauvegarde de la configuration du site MCN](#).

Avertissement

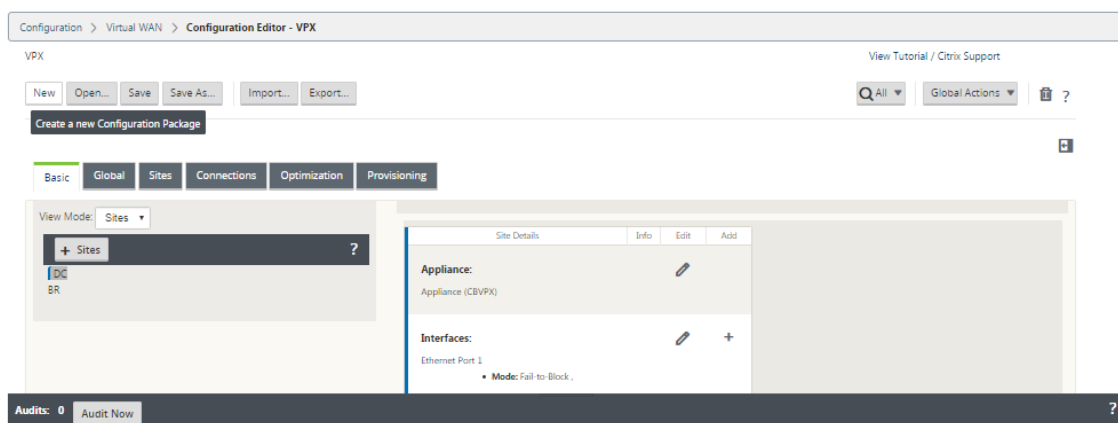
Si la session de console expire ou si vous vous déconnectez de l'interface Web de gestion avant d'enregistrer votre configuration, les modifications de configuration non enregistrées sont perdues. Vous devez ensuite vous reconnecter au système et répéter la procédure de configuration dès le début. Pour cette raison, il est recommandé de définir l'intervalle de temporisation de la session de console sur une valeur élevée lors de la création ou de la modification d'un package de configuration ou lors de l'exécution d'autres tâches complexes. La valeur par défaut est 60 minutes. Le maximum est de 9,999 minutes. Pour des raisons de sécurité, vous devez ensuite le réinitialiser à un seuil inférieur après avoir terminé ces tâches. Pour obtenir des instructions, reportez-vous à la section [Définition de l'intervalle de temporisation de la session de la console \(facultatif\)](#)

Pour ajouter et commencer à configurer le site de l'appliance MCN, procédez comme suit :

1. Dans l'arborescence de navigation, accédez à **Virtual WAN > Éditeur de configuration** . Cela affiche la page principale de l'**Éditeur de configuration** (volet central).



2. Cliquez sur **Nouveau** pour commencer à définir une nouvelle configuration. La page **Nouveaux** paramètres de configuration s'affiche.



3. Cliquez sur **+ Sites** dans la barre **Sites** pour commencer l'ajout et la configuration du site MCN. La boîte de dialogue **Ajouter un site** s'affiche.

4. Entrez les informations du site.

Procédez comme suit :

1. Entrez le **nom du site** et la **clé sécurisée**.
2. Sélectionnez le **modèle** de l'apppliance.
3. Sélectionnez le **mode**.
4. Sélectionnez **MCN principal** comme mode.

Remarque

Le menu Options du **modèle** répertorie les noms de modèles génériques des modèles d'apppliance pris en charge. Les noms génériques n'incluent pas le suffixe de modèle Standard Edition, mais correspondent aux modèles d'apppliance SD-WAN équivalents. Sélectionnez le numéro de modèle correspondant à ce modèle d'apppliance SD-WAN. (Par exemple, sélectionnez 4000 s'il s'

agit d'une appliance SD-WAN 4000-SE.)

Les entrées ne peuvent pas contenir d'espaces et doivent être au format Linux.

Pour ajouter un site :

1. Cliquez sur **Ajouter** pour ajouter le site. Cela ajoute le nouveau site à l'arborescence **Sites** et affiche le formulaire de configuration des **paramètres de base** du nouveau site.

The screenshot shows the Citrix SD-WAN configuration interface. The 'Sites' tab is selected in the top navigation bar. On the left, a sidebar lists various configuration options under 'Sites', with 'Basic Settings' highlighted. The main area displays the 'Basic Settings' form for a new site. The form includes fields for 'Site Name' (NA-DC), 'Appliance Name' (NA-DC-CBVPX), 'Secure Key' (8a483b0fed92c1a), 'Model' (CBVPX), 'Mode' (primary MCN), 'Site Location', 'Default Direct Route Cost' (5), 'Gateway ARP Timer (ms)' (1000), and 'Host ARP Timer (ms)' (1000). There is also a checkbox for 'Enable Source MAC Learning'. At the bottom of the form are 'Apply' and 'Refresh' buttons.

Après avoir cliqué sur **Appliquer**, des avertissements d'audit s'affichent indiquant qu'une action supplémentaire est requise. Un point rouge ou une icône delta de couleur jaune paille indique une erreur dans la section où il apparaît. Vous pouvez utiliser ces avertissements pour identifier les erreurs ou les informations de configuration manquantes. Faites glisser votre curseur sur une icône d'avertissement d'audit pour afficher une brève description des erreurs dans cette section. Vous pouvez également cliquer sur la barre d'état **des audits** gris foncé (en bas de la page) pour afficher la liste complète de tous les avertissements d'audit non résolus. Le minuteur ARP hôte configurable (ms) est ajouté au niveau du site pendant la configuration. La valeur par défaut actuelle est de 1 000 ms. La plage configurable est de 1 000 ms à 180 000 ms. La configuration du minuteur Host ARP ne s'applique pas au port de gestion.

2. Entrez les paramètres de base du nouveau site ou acceptez les valeurs par défaut. Dans les déploiements Citrix SD-WAN tels que Gateway et One-Arm, lorsque les demandes ARP sont

fréquemment reçues, les points d'accès deviennent surchargés, ce qui affecte le flux de trafic. Vous pouvez maintenant configurer les temporisateurs ARP pour envoyer les requêtes ARP avec des intervalles spécifiques. L'intervalle de temps est configuré en secondes. Vous pouvez configurer des intervalles de temps ARP lors de la configuration du site du centre de données sous l'onglet **Paramètres de base** de l'interface graphique du dispositif Citrix SD-WAN.

3. (Facultatif, recommandé) Enregistrez la configuration en cours.

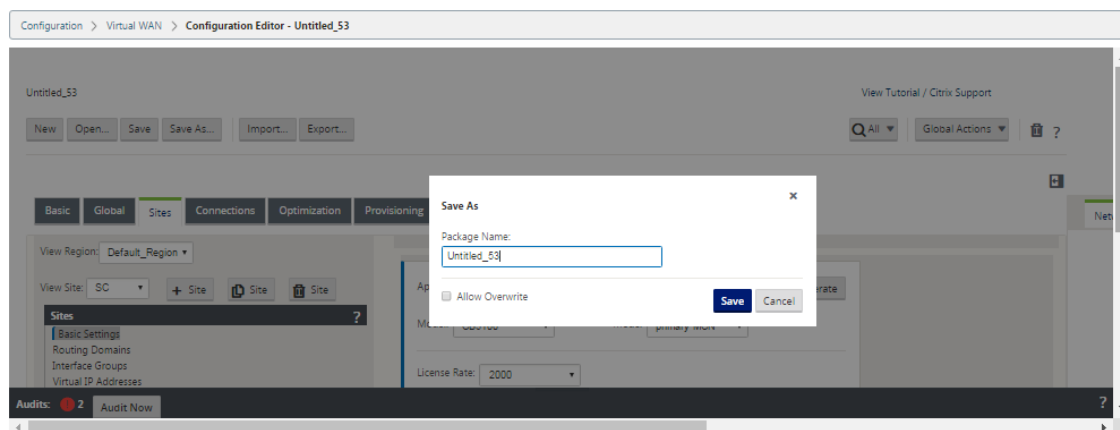
Si vous ne pouvez pas terminer la configuration en une session, vous pouvez l'enregistrer à tout moment, de sorte que vous pouvez revenir à la terminer ultérieurement. La configuration est enregistrée dans votre Workspace sur l'appliance locale. Pour reprendre le travail dans une configuration enregistrée, cliquez sur **Ouvrir** dans la barre de menus de l'**Éditeur de configuration** (haut de la page). Une boîte de dialogue vous permet de sélectionner la configuration à modifier.

Remarque

Par mesure de précaution supplémentaire, il est recommandé d'utiliser **Enregistrer sous**, plutôt que **Enregistrer**, pour éviter d'écraser le mauvais package de configuration.

Pour enregistrer le package de configuration actuel, procédez comme suit :

1. Cliquez sur **Enregistrer sous** (en haut du volet central de l'**Éditeur de configuration**). La boîte de dialogue **Enregistrer sous** s'ouvre.



2. Entrez le nom du package de configuration. Si vous enregistrez la configuration dans un package existant, veillez à sélectionner **Autoriser l'écrasement** avant d'enregistrer.
3. Cliquez sur **Enregistrer**.

Comment configurer des groupes d'interface pour le MCN

Après avoir ajouté le nouveau site MCN, l'étape suivante consiste à créer et configurer les groupes d'interface virtuelle pour le site.

Voici quelques instructions pour configurer des groupes d'interface virtuelle :

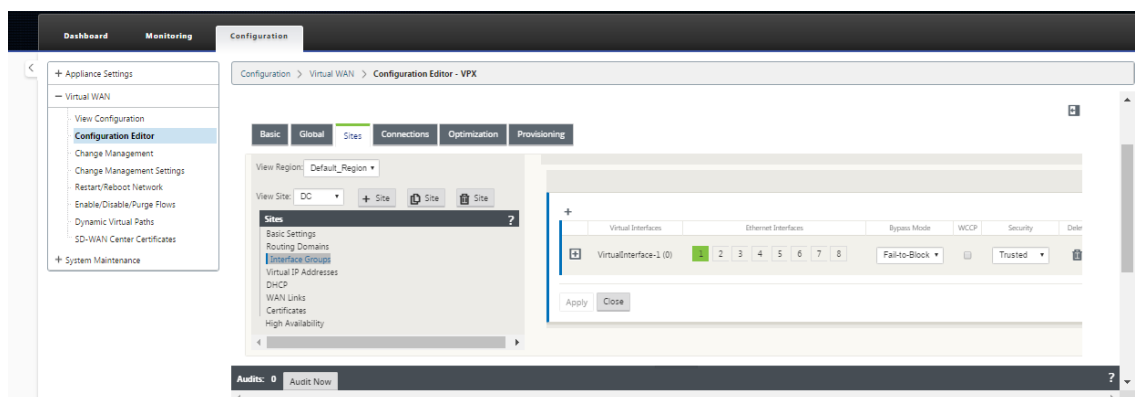
- Utilisez des noms logiques qui décriront le mieux le groupe.
- Les réseaux approuvés sont des réseaux protégés derrière un pare-feu.
- Les interfaces virtuelles associent des interfaces aux paires Fail to Wire (FTW).
- Les interfaces WAN simples ne peuvent pas être dans une paire FTW.
- L'adresse IPv6 est introduite dans la version 11.1.0 et elle n'est prise en charge que pour les interfaces non approuvées. Les interfaces non approuvées ne sont pas routables et utilisées pour le trafic de chemin virtuel.

Remarque

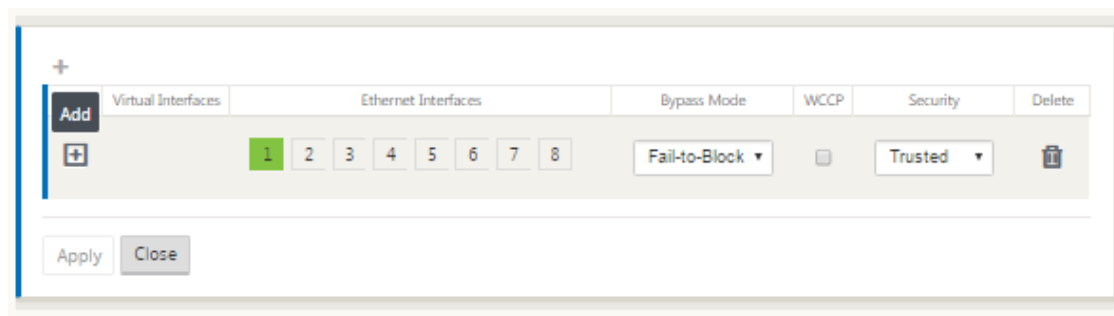
Pour plus d'instructions et d'informations sur la configuration des groupes d'interface virtuelle, consultez la section Routage et transfert virtuels.

Pour ajouter un groupe d'interface virtuelle au nouveau site MCN, procédez comme suit :

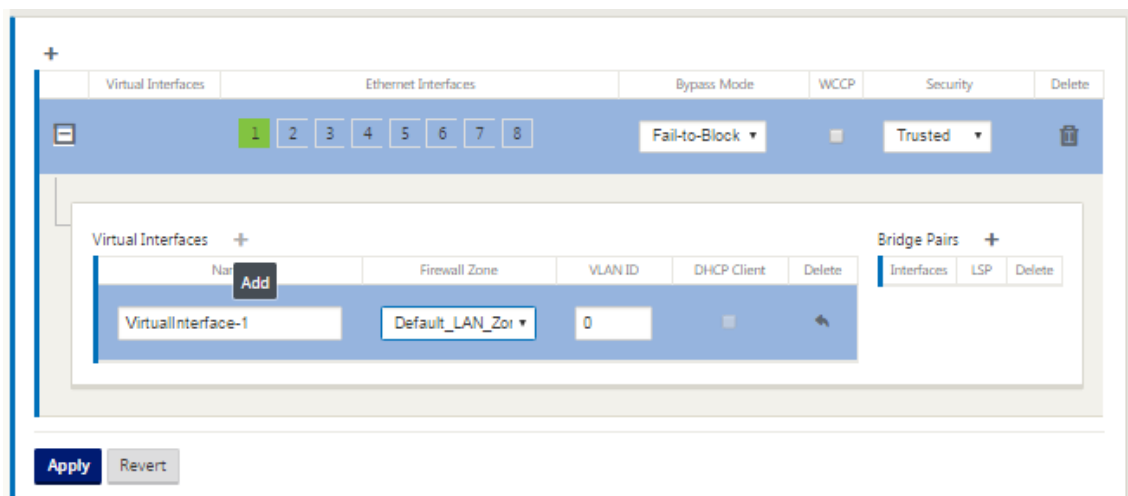
1. Dans la vue **Sites** de l'**Éditeur de configuration**, sélectionnez le site dans le menu déroulant **Afficher le site**. Cela ouvre la vue de configuration du site que vous avez sélectionné.



2. Cliquez sur **+** pour ajouter le **groupe d'interface virtuelle**. Cela ajoute une nouvelle entrée de groupe d'interface virtuelle vide à la table et l'ouvre pour modification.



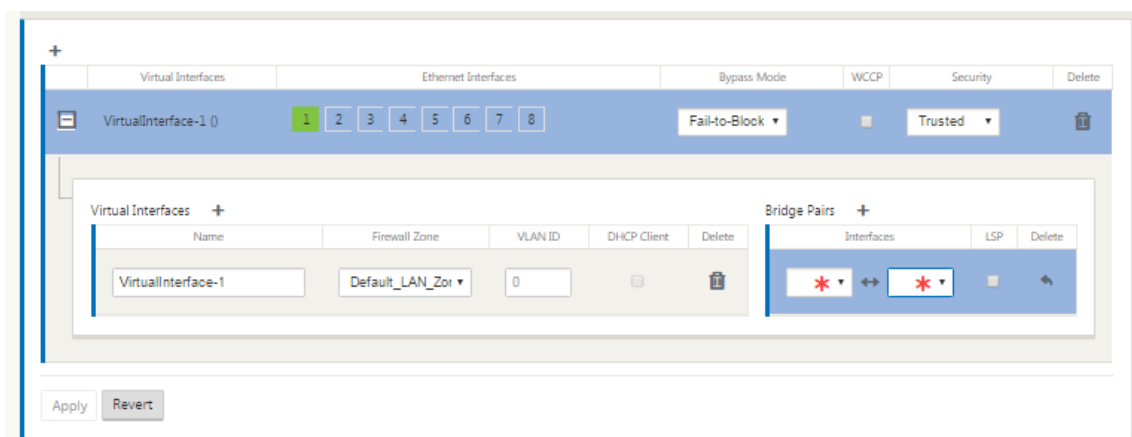
3. Cliquez sur **+** à droite de **Virtual Interfaces**. Cela ajoute une nouvelle entrée de groupe vide à la table et l'ouvre pour modification.



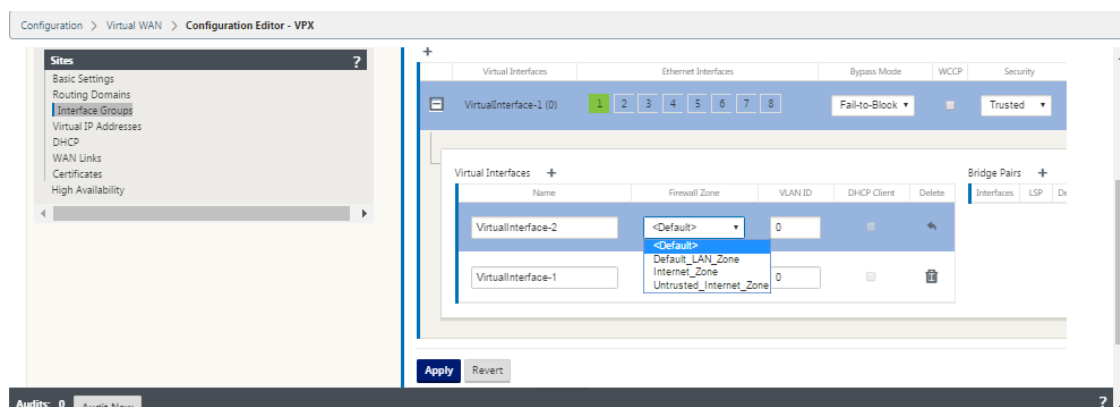
4. Sélectionnez les **interfaces Ethernet** à inclure dans le groupe. Sous **Interfaces Ethernet**, cliquez sur une interface pour inclure/exclure cette interface. Vous pouvez sélectionner n'importe quel nombre d'interfaces à inclure dans le groupe.



5. Sélectionnez le **mode de contournement** dans le menu déroulant (pas par défaut). Le **mode de contournement** spécifie le comportement des interfaces jumelées par pont dans le groupe d'interfaces virtuelles, en cas de défaillance ou de redémarrage d'une appliance ou d'un service. Les options sont : **Fail-to-Wire** ou **Fail-to-Block**.
6. Sélectionnez le **niveau de sécurité** dans le menu déroulant. Indique le niveau de sécurité du segment réseau du groupe d'interface virtuelle. Les options sont les suivantes : **Approuvé** ou **Non approuvé**. Les segments approuvés sont protégés par un pare-feu (par défaut est approuvé).
7. Cliquez sur **+** dans le bord gauche de l'interface virtuelle que vous avez ajoutée. Le tableau **Interfaces virtuelles** s'affiche.



8. Cliquez sur **+** à droite de **Virtual Interfaces**. Cela révèle le **nom**, la **zone de pare-feu**, l'**ID VLAN**, la **diffusion dirigée**, le **mode client** et la **configuration automatique des adresses sans état (SLAAC)**.



9. Entrez le **nom** et l'**ID VLAN** de ce groupe d'interface virtuelle.
- **Nom** —Il s'agit du nom par lequel cette interface virtuelle est référencée.
 - **Zone de pare-feu** : sélectionnez une zone de pare-feu dans le menu déroulant.
 - **ID VLAN** : il s'agit de l'ID permettant d'identifier et de marquer le trafic vers et en provenance de l'interface virtuelle. Utilisez un ID de 0 (zéro) pour le trafic natif/non étiqueté.
 - **Mode client** : sélectionnez le mode client dans le menu déroulant.
 - **Diffusion dirigée** - Sur l'interface virtuelle, les paquets Diffusions dirigées peuvent être transférés pour les sous-réseaux IP virtuels en activant la case à cocher.
 - **SLAAC** —Activation de la case à cocher **SLAAC (Stateless Address Auto-Configuration)** sur une interface virtuelle lui permet d'obtenir automatiquement une adresse IPv6 globale à partir du routeur connecté. Les interfaces virtuelles avec **SLAAC** activées ne nécessitent pas d'adresse IP virtuelle configurée.

REMARQUE

L'option SLAAC ne peut être activée que sur un site de succursale sur une interface non approuvée.

Vous avez la possibilité de libérer ou de renouveler les adresses IP pour SLAAC.

10. Cliquez sur **+** à droite de **Bridge Pairs**. Cela ajoute une nouvelle entrée **Bridge Pairs** et l'ouvre pour modification.
11. Sélectionnez les interfaces Ethernet à associer dans les menus déroulants. Pour ajouter d'autres paires, cliquez à nouveau sur **+** en regard de **Paires de pont**.
12. Cliquez sur **Appliquer**. Cela applique vos paramètres et ajoute le nouveau groupe d'interface virtuelle à la table. À ce stade, une icône d'alerte d'audit delta jaune s'affiche à droite de la nouvelle entrée de groupe d'interface virtuelle. En effet, vous n'avez pas encore configuré d'adresses IP virtuelles (VIP) pour le site. Pour l'instant, vous pouvez ignorer cette alerte, car elle est résolue automatiquement lorsque vous avez correctement configuré les adresses IP virtuelles pour le site.
13. Pour ajouter d'autres groupes d'interface virtuelle, cliquez sur **+** à droite de la succursale **Groupes d'interface**, puis procédez comme indiqué ci-dessus.

Comment configurer l'adresse IP virtuelle pour le MCN

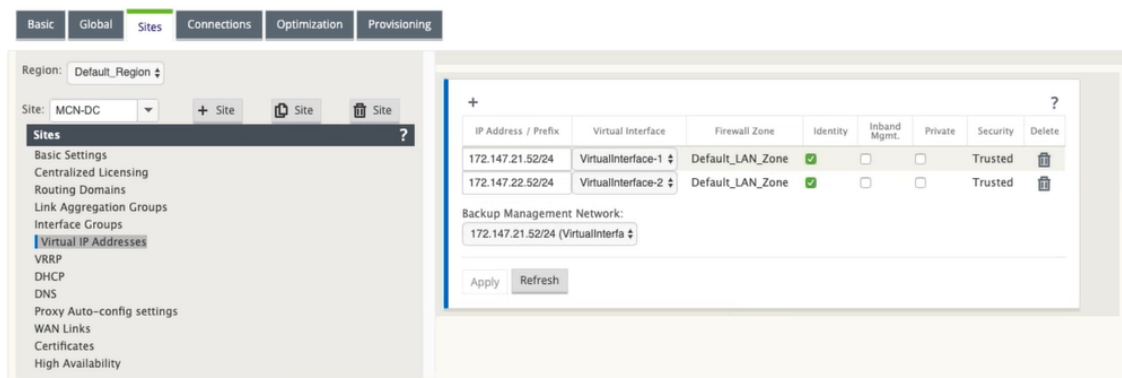
L'étape suivante consiste à configurer les adresses IP virtuelles pour le site et à les affecter au groupe approprié.

1. En continuant dans l'affichage **Sites** du nouveau site MCN, cliquez sur **+** à gauche des **adresses IP virtuelles**. Le tableau **Adresses IP virtuelles** du nouveau site s'affiche.
2. Cliquez sur **+** à droite de **Virtual IP Adresses** pour ajouter une adresse. Cela ouvre le formulaire permettant d'ajouter et de configurer une nouvelle adresse IP virtuelle.
3. Entrez les informations **Adresse IP / Préfixe**, puis sélectionnez l'**interface virtuelle** à laquelle l'adresse est associée. L'adresse IP virtuelle doit inclure l'adresse hôte complète et le masque réseau.
4. Sélectionnez les paramètres souhaités pour l'adresse IP virtuelle, tels que la zone de pare-feu, l'identité, le privé et la sécurité.
5. Sélectionnez **Gestion Inband** pour permettre à l'adresse IP virtuelle de se connecter à des services de gestion tels que l'interface utilisateur Web et SSH.

Remarque :

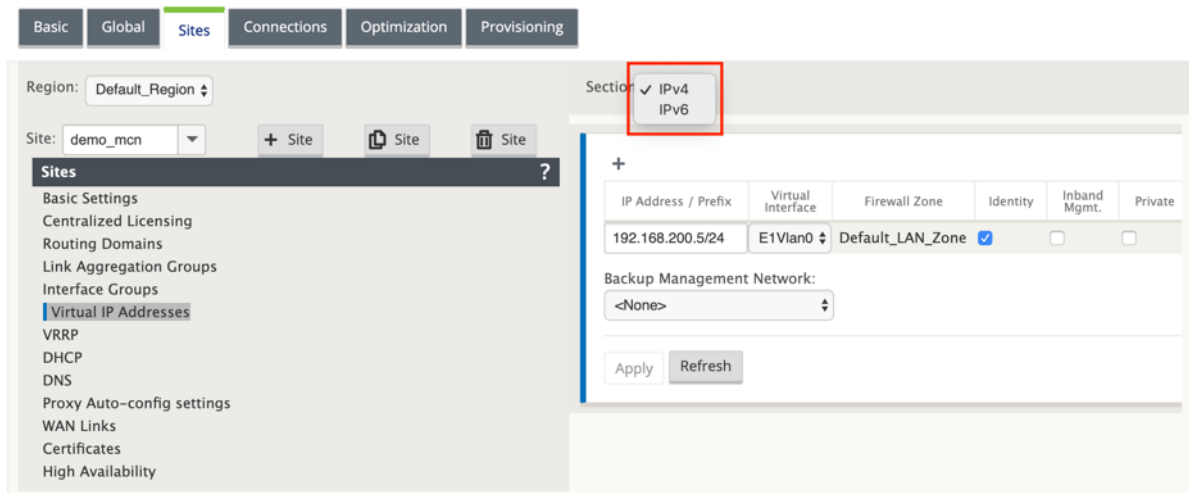
L'interface doit être de type de sécurité **Autorisé** et **Identité** activée.

- Sélectionnez une adresse IP virtuelle en tant que **réseau de gestion des sauvegardes**. Cela vous permet d'utiliser l'adresse IP virtuelle pour la gestion si le port de gestion n'est pas configuré avec une Gateway par défaut.



- Cliquez sur **Appliquer**. Cela ajoute les informations d'adresse au site et les inclut dans le tableau **Adresses IP virtuelles** du site.
- Pour ajouter d'autres adresses IP virtuelles, cliquez sur **+** à droite des **adresses IP virtuelles**, puis procédez comme ci-dessus.

À partir de la version 11.1.0, deux sous-sections sont disponibles sous l'**adresse IP virtuelle** : les adresses **IPv4** et **IPv6**.

**Limitations**

- Une seule paire de chemins est créée si les interfaces d'accès IPv4 et IPv6 sont configurées sur le même lien WAN.

- Si le chemin IPv6 tombe en panne, il n'y a pas de retour à IPv4 pour le même lien WAN.
- Le suivi des adresses IPv6 ne sont pas pris en charge pour la version 11.1.0.
- IPv6 n'est pris en charge que pour la communication entre les périphériques SD-WAN via Virtual Path. Les services Internet et Intranet ne sont pas pris en charge. Aucun support pour le plan de gestion dans la version 11.1.0.
- IPv6 ne sera pas pris en charge pour les liaisons LTE sur 210 périphériques pour la version 11.1.0.
- Le client et le serveur DHCPv6 n'est pas pris en charge pour IPv6. Vous pouvez configurer SLAAC pour l'adressage automatique.

Vous devez ajouter une adresse IP virtuelle pour l'interface non approuvée nouvellement créée ou vous pouvez activer SLAAC s'il s'agit d'un site de succursale. Pour ajouter une adresse IP virtuelle :

1. Sélectionnez IPv6 dans le menu déroulant Section.
2. Définissez les champs suivants :
3. Adresse IP/Préfixe —Fournit l'adresse hôte complète et le masque réseau.
4. Interface virtuelle : sélectionnez l'une des interfaces virtuelles associées dans le menu déroulant.
5. Zone de pare-feu : zone de pare-feu de l'interface virtuelle.
6. Lien local (Facultatif) - Si la case à cocher Lien local est activée, cette adresse IP virtuelle IPv6 peut être utilisée comme adresse locale de lien pour l'interface virtuelle.

REMARQUE

Si la case à cocher Lier Local n'est pas activée, l'appliance génère et attribue automatiquement une adresse locale de lien.

Section: IPv6

IP Address / Prefix	Virtual Interface	Firewall Zone	Link Local	Private	Security	Delete
2607:f0d0:2001:0...	E2Vlan0	Untrusted_Internet_Zone	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Untrusted	

Apply Refresh

REMARQUE

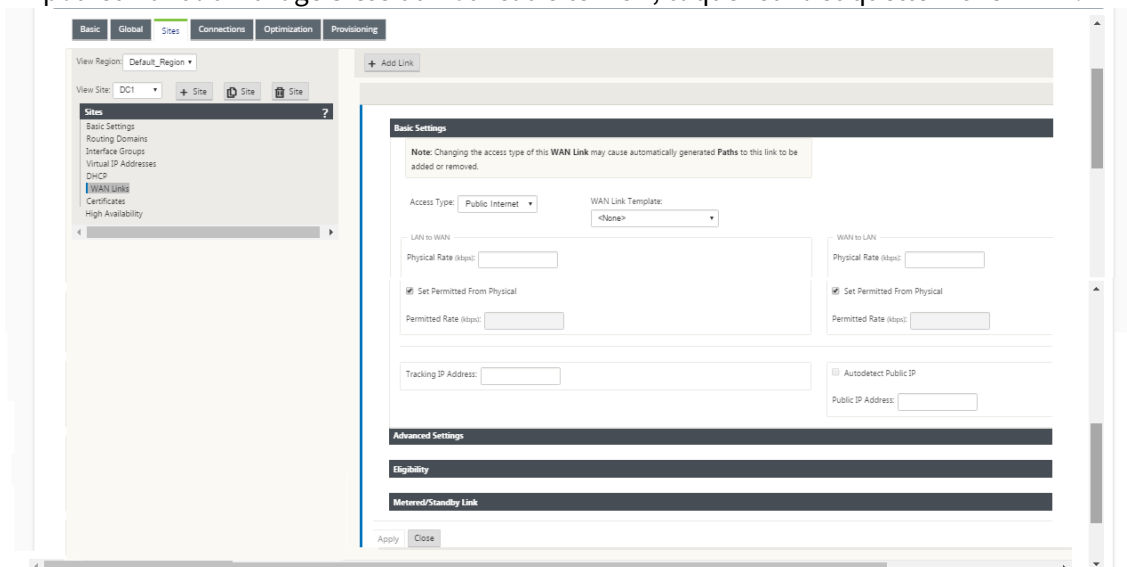
Le protocole NDP (Neighbor Discovery Protocol) est pris en charge par IPv6.

Si les interfaces d'accès IPv4 et IPv6 sont définies sur le site local et distant, le chemin d'accès est formé en utilisant uniquement l'adresse IPv6.

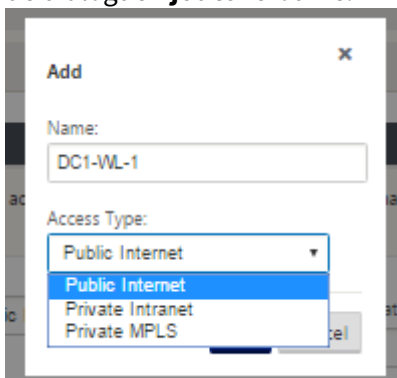
Comment configurer les liens WAN pour le MCN

L'étape suivante consiste à configurer les liens WAN pour le site.

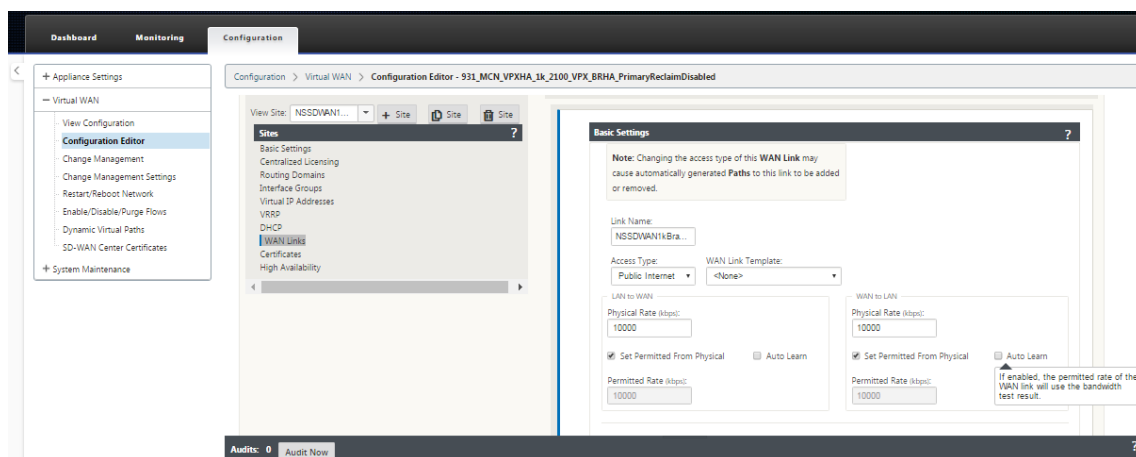
1. En poursuivant l'affichage **Sites** du nouveau site MCN, cliquez sur l'étiquette **Liens WAN**.



2. Cliquez sur **Ajouter un lien** à droite des **liens WAN** pour ajouter un nouveau lien WAN. La boîte de dialogue **Ajouter** s'ouvre.

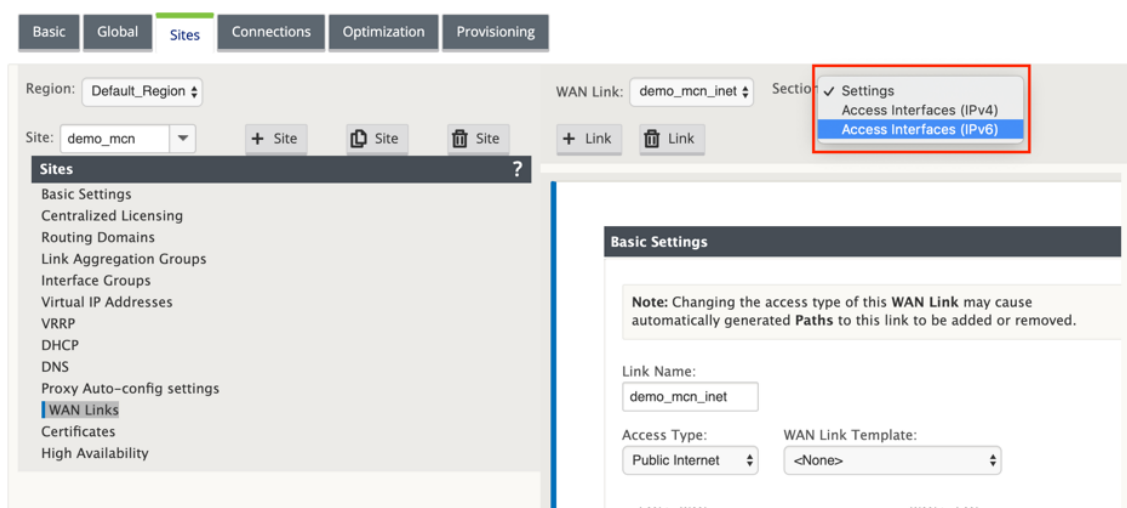


3. (Facultatif) Entrez un nom pour le lien WAN si vous ne souhaitez pas utiliser la valeur par défaut. La valeur par défaut est le nom du site, ajouté avec le suffixe suivant : WL- <number>, où <number> est le nombre de liens WAN pour ce site, incrémenté d'un.
4. Sélectionnez le **Type d'accès** dans le menu déroulant. Les options sont **Internet public**, **Intranet privé** ou **MPLS privé**.
5. Cliquez sur **Ajouter**. Ceci affiche la page de configuration des paramètres de base des **liens WAN** et ajoute le nouveau lien WAN non configuré à la page.



Seul le chemin IPv6 entre deux sites est formé lorsque les interfaces d'accès IPv4 et IPv6 sont configurées pour le même lien WAN.

1. Sélectionnez **Interfaces d'accès (IPv6)** dans le menu déroulant **Paramètres**.



2. Définissez les champs suivants :

- **Nom** —Indiquez le nom de l'interface d'accès.
- **Interface virtuelle** : une fois qu'un domaine de routage est sélectionné, sélectionnez l'une des interfaces virtuelles associées dans le menu déroulant.
- **Adresse IP** —Fournissez une adresse IP statique pour le point de terminaison de l'interface d'accès sur le SD-WAN.
- **Adresse IP de passerelle** —Indiquez l'adresse IP du routeur de passerelle.

REMARQUE

Vous ne pouvez pas configurer l'adresse IP et l'adresse IP de la passerelle lorsque l'appliance virtuelle est configurée pour utiliser le mode SLAAC.

- **Mode Chemin virtuel** - Sélectionnez le mode chemin virtuel dans le menu déroulant pour déterminer la priorité du trafic de chemin virtuel sur cette liaison WAN.
- **Liaison d'adresse MAC de passerelle : si la case à cocher Liaison d'adresses MAC** de passerelle est activée, l'adresse MAC source des paquets reçus sur les services Internet ou intranet doit correspondre à l'adresse MAC de la passerelle.

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Gateway MAC Address Binding	Delete
demo_mcn_inet...	E2Vlan0	2607:fd0:2001:000a:0000:00...	2607:fd0:2001:000a:0000:00...	Primary	<input checked="" type="checkbox"/>	

Une fois l'interface IPv6 créée pour la liaison WAN, vous pouvez utiliser cette interface pour communiquer avec le fournisseur de services Internet (FAI).

REMARQUE

Étant donné que l'offre IPv6 initiale est uniquement la connectivité Virtual Path, nous ne pouvons pas envoyer de paquets IPv6 côté LAN.

Apprentissage automatique de la consommation de bande passante

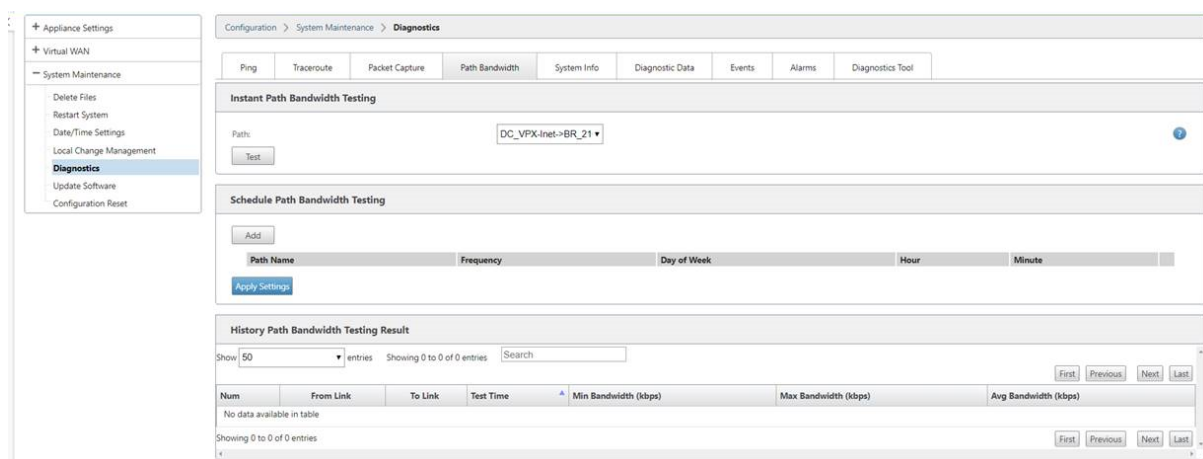
L'apprentissage automatique s'exécute au démarrage du système et se répète toutes les cinq minutes jusqu'à ce qu'un résultat réussi soit observé. L'apprentissage automatique s'exécute également après que des modifications de configuration des liens WAN ont été apportées à partir de l'éditeur de configuration.

Vous pouvez exécuter des tests manuellement ou planifier des tests dans l'interface graphique SD-WAN. Les résultats de ces tests devraient également s'appliquer au taux autorisé lorsque le test est réussi et que l'apprentissage automatique est activé.

Lors de l'utilisation de l'apprentissage automatique sur de grands réseaux, si le changement de configuration redémarre, tous les sites exécutent des tests simultanément sur le MCN, ce qui entraîne une utilisation élevée de la bande passante conduisant à des résultats inexacts. Il est recommandé de planifier des tests de bande passante une ou deux fois par jour, généralement lorsque le volume de trafic est faible.

Remarque

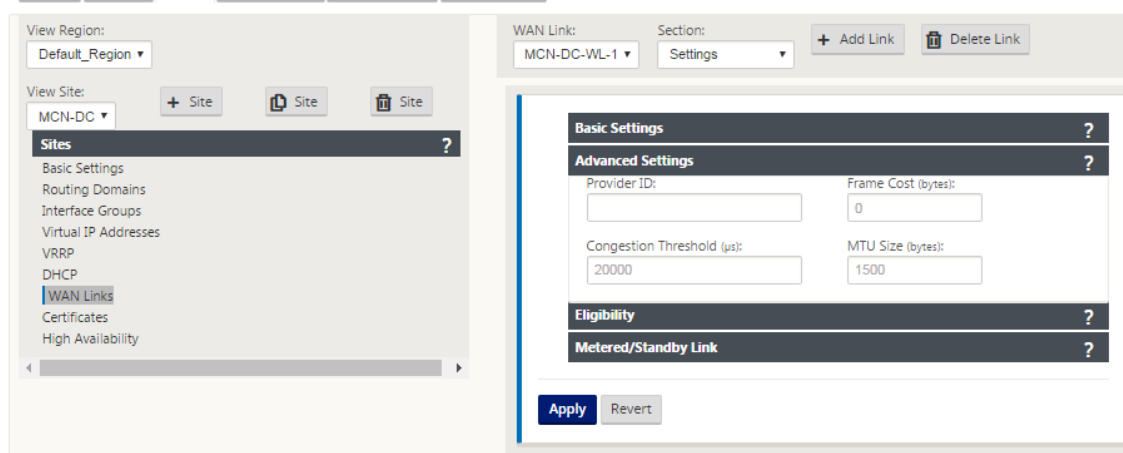
La détection automatique de la bande passante WAN Link est applicable uniquement sur les succursales et non applicable pour MCN/RCN.



1. Entrez les détails du lien pour le nouveau lien WAN. Configurez les paramètres LAN vers WAN, WAN vers **LAN**. Voici quelques lignes directrices :

- Certains liens Internet peuvent être asymétriques.
- Une mauvaise configuration de la vitesse autorisée peut nuire aux performances de cette liaison
- Évitez d'utiliser des vitesses de rafale supérieures au taux engagé.
- Pour les liaisons WAN Internet, assurez-vous d'ajouter l'adresse IP publique.

2. Cliquez sur la barre de section **Paramètres avancés** grise. Cela ouvre l'écran **Paramètres avancés** du lien.



3. Entrez les **paramètres avancés** pour le lien :

- **ID** du fournisseur —(Facultatif) Entrez un numéro d'identification unique 1—100 pour désigner les liaisons WAN connectées au même fournisseur de services. Virtual WAN utilise l'ID du fournisseur pour différencier les chemins lors de l'envoi de paquets en double.
- **Coût de trame (octets)** : saisissez la taille (en octets) de l'en-tête/remorque ajouté à chaque paquet. Par exemple, la taille en octets des remorques Ethernet IPG ou AAL5

ajoutées.

- **Seuil de congestion** —Entrez le seuil de congestion (en microsecondes) après quoi la liaison WAN limite la transmission des paquets pour éviter d’autres congestion.
- **Taille MTU (octets)** : saisissez la plus grande taille de paquet brut (en octets), sans inclure le coût de trame.

4. Cliquez sur la barre de section grise **Éligibilité**. Cela ouvre l’écran Paramètres **d’éligibilité** pour le lien.

5. Sélectionnez les paramètres **d’éligibilité** pour le lien.

The screenshot shows the configuration interface for a WAN link. On the left, the 'View Site' dropdown is set to 'MCN-DC'. The 'WAN Links' menu item is selected. The main panel displays the 'Eligibility' settings for the selected link. The 'Eligibility' section is expanded, showing a table with columns for 'LAN to WAN' and 'WAN to LAN'. The table has three rows: 'Realtime', 'Interactive', and 'Bulk'. All three rows have checkboxes checked in both columns. Below the table, the 'Metered/Standby Link' section is also expanded. The 'Apply' button is visible at the bottom.

	LAN to WAN	WAN to LAN
Realtime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Interactive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bulk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

6. Cliquez sur la barre de section **Lien mesuré** grise. Cela ouvre l’écran Paramètres du **lien mesuré** pour le lien.

7. (Facultatif) Sélectionnez **Activer la mesure** pour activer la mesure pour ce lien. Les champs **Activer les paramètres de mesure** s’affichent.

The screenshot shows the configuration interface for a WAN link, specifically the 'Metered/Standby Link' settings. The 'Metered/Standby Link' section is expanded, showing the 'Metering' and 'Standby' options. The 'Enable Metering' checkbox is checked. The 'Standby Mode' dropdown menu is open, showing the following options: 'Disabled', 'Last-Resort', and 'On-Demand'. The 'Apply' button is visible at the bottom.

The screenshot displays three configuration sections in a light gray box:

- Metering:** Contains two checked checkboxes: "Enable Metering" and "Disable if Data Cap reached". Below them are three fields: "Data Cap (MB):" with a value of "0", "Billing Cycle:" with a dropdown menu set to "Monthly", and "Starting From:" with a date input field showing "MM/DD/YYYY".
- Standby:** Contains a "Standby Mode:" dropdown menu set to "Disabled".
- Heartbeat Interval:** Features a yellow warning box stating "Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure." Below this is an "Active Heartbeat Interval:" dropdown menu set to "DEFAULT".

8. Configurez les paramètres de mesure pour le lien. Saisissez ce qui suit :

- **Capuchon de données (Mo)** : saisissez l'allocation de plafond de données pour le lien, en mégaoctets.
- **Cycle** de facturation : sélectionnez **Mensuel** ou **Hebdomadaire** dans le menu déroulant.
- À **partir de** : saisissez la date de début du cycle de facturation.
- Définir le **dernier recours** — Sélectionnez cette option pour activer ce lien en tant que lien de dernier recours en cas de défaillance de tous les autres liens disponibles. Dans des conditions WAN normales, Virtual WAN envoie uniquement un trafic minimal sur les liaisons mesurées, pour vérifier l'état de la liaison. Toutefois, en cas de panne, le SD-WAN peut utiliser des liaisons compteurs actives en dernier recours pour acheminer le trafic de production.

Cliquez sur **Appliquer**. Cela applique vos paramètres spécifiés à la nouvelle liaison WAN.

L'étape suivante consiste à configurer les interfaces d'accès pour la nouvelle liaison WAN. Une interface d'accès se compose d'une interface virtuelle, d'une adresse IP du point de terminaison WAN, d'une adresse IP de passerelle et d'un mode chemin virtuel défini collectivement comme une interface pour une liaison WAN spécifique. Chaque liaison WAN doit avoir au moins une interface d'accès.

Comment configurer l'interface d'accès :

1. Sélectionnez **Interfaces d'accès** dans la page de configuration du lien WAN pour le lien. Cela ouvre la vue **Interfaces d'accès** pour le site.

The screenshot shows a configuration bar for a WAN Link. It includes a "WAN Link:" dropdown set to "DC1-WL-1", a "Section:" dropdown menu with "Settings" and "Access Interfaces" options (where "Access Interfaces" is highlighted in blue), and two buttons: "+ Add Link" and "Delete Link".

2. Cliquez sur **+** pour ajouter une interface. Cela ajoute une entrée vide à la table et l'ouvre pour modification. Entrez les paramètres **des interfaces d'accès** pour le lien. Chaque liaison WAN doit avoir au moins une interface d'accès.

3. Saisissez ce qui suit :

- **Nom** —Il s'agit du nom par lequel cette interface d'accès est référencée. Entrez un nom pour la nouvelle interface d'accès ou acceptez la valeur par défaut. La valeur par défaut utilise la convention de dénomination suivante :
WAN_LINK_NAME-AI-Number : Où *WAN_LINK_Name* est le nom du lien WAN que vous associez à cette interface, et numéro correspond au nombre d'interfaces d'accès actuellement configurées pour ce lien, incrémenté de 1.

Remarque

Si le nom apparaît tronqué, vous pouvez placer votre curseur dans le champ, puis cliquer longuement et rouler la souris vers la droite ou la gauche pour voir la partie tronquée.

- **Interface virtuelle** : il s'agit de l'interface virtuelle utilisée par cette interface d'accès. Sélectionnez une entrée dans le menu déroulant des interfaces virtuelles configurées pour ce site de succursale.
- **Domaine de routage** - Domaine de routage que vous souhaitez choisir pour l'interface d'accès.
- **Adresse IP** : il s'agit de l'adresse IP du point de terminaison de l'interface d'accès entre l'appliance et le réseau étendu.
- **Adresse IP de la Gateway** : il s'agit de l'adresse IP du routeur de la passerelle.
- **Mode Chemin d'accès virtuel** : spécifie la priorité du trafic Chemin d'accès virtuel sur cette liaison WAN. Les options sont : **Principal**, **Secondaire** ou **Exclude**. Si cette option est définie sur

Exclude, cette interface d'accès est utilisée uniquement pour le trafic Internet et Intranet.

- **Proxy ARP** —Activez la case à cocher pour activer. Si cette option est activée, Virtual WAN Appliance répond aux demandes ARP pour l'adresse IP de la Gateway, lorsque la passerelle est inaccessible.

1. Cliquez sur **Appliquer**.

Vous avez maintenant terminé de configurer la nouvelle liaison WAN. Répétez ces étapes pour ajouter et configurer d'autres liens WAN pour le site.

L'étape suivante consiste à ajouter et configurer les itinéraires pour le site.

Comment configurer les itinéraires pour le MCN

Pour ajouter et configurer les itinéraires pour le site, procédez comme suit :

1. Cliquez sur l'affichage **Connexions** du nouveau site MCN et sélectionnez **Itinéraires** . Ceci affiche la vue **Itinéraires** du site.
2. Cliquez sur **+** à droite de **Itinéraires** pour ajouter un itinéraire. La boîte de dialogue **Itinéraires** s'ouvre à modifier.

The screenshot shows a dialog box titled "Add" with a close button (X) and a help button (?). It contains the following fields and options:

- Network IP Address**: A text input field with a red asterisk indicating it is required.
- Cost**: A text input field containing the value "5".
- Service Type**: A dropdown menu currently set to "Local".
- Gateway IP Address**: A text input field with a red asterisk indicating it is required.
- Export Route**: A checked checkbox.
- Summary Route**: An unchecked checkbox.
- Eligibility Based On Path**: An unchecked checkbox.
- Path**: A dropdown menu currently set to "<None>".
- Eligibility Based On Gateway**: An unchecked checkbox.
- Buttons**: "Add" and "Cancel" buttons at the bottom right.

3. Entrez les informations de configuration de l'itinéraire pour la nouvelle route. Saisissez ce qui suit :
 - **Adresse IP réseau** —Entrez l'**adresse IP réseau** .
 - **Coût** —Saisissez un poids de 1 à 15 pour déterminer la priorité d'itinéraire pour cet itinéraire. Les itinéraires à moindre coût ont priorité sur les itinéraires à coût élevé. La valeur par défaut est 5.

- **Type de service** : sélectionnez le type de service de l'itinéraire dans le menu déroulant correspondant à ce champ.
 - **Chemin virtuel** : ce service gère le trafic sur les chemins virtuels. Un chemin virtuel est un lien logique entre deux liaisons WAN. Il comprend une collection de chemins WAN combinés pour fournir une communication de niveau de service élevé entre deux nœuds SD-WAN. Ceci est réalisé en mesurant constamment et en s'adaptant à l'évolution de la demande des applications et des conditions WAN. Les appliances SD-WAN mesurent le réseau par chemin d'accès. Un chemin virtuel peut être statique (existe toujours) ou dynamique (n'existe que lorsque le trafic entre deux appliances SD-WAN atteint un seuil configuré).
 - **Internet** —Ce service gère le trafic entre un site d'entreprise et des sites d'Internet public. Le trafic de ce type n'est pas encapsulé. Pendant les périodes de congestion, le SD-WAN gère activement la bande passante en limitant le trafic Internet par rapport au chemin virtuel et le trafic Intranet selon la configuration SD-WAN établie par l'administrateur.
 - **Intranet** : ce service gère le trafic Intranet d'entreprise qui n'a pas été défini pour la transmission sur un chemin virtuel. Comme pour le trafic Internet, il reste non encapsulé, et le SD-WAN gère la bande passante en limitant le débit de ce trafic par rapport aux autres types de services pendant les périodes de congestion. Dans certaines conditions, et s'il est configuré pour l'Intranet Fallback sur le chemin virtuel, le trafic qui circule habituellement par un chemin virtuel peut être traité comme du trafic intranet, afin de maintenir la fiabilité du réseau.
 - **Passthrough** : ce service gère le trafic qui doit être transmis via le réseau étendu virtuel. Le trafic dirigé vers le service de transmission comprend les diffusions, les ARP et tout autre trafic non IPv4, ainsi que le trafic sur le sous-réseau local de l'appliance Virtual WAN, les sous-réseaux configurés ou les règles appliquées par l'administrateur réseau. Ce trafic n'est pas retardé, façonné ou modifié par le SD-WAN. Par conséquent, vous devez vous assurer que le trafic Passthrough ne consomme pas de ressources importantes sur les liaisons WAN que l'appliance SD-WAN est configurée pour utiliser pour d'autres services.
 - **Local** : ce service gère le trafic IP local vers le site qui ne correspond à aucun autre service. Le SD-WAN ignore le trafic provenant et destiné à une route locale.
 - **Tunnel GRE** —Ce service gère le trafic IP destiné à un tunnel GRE et correspond au tunnel GRE LAN configuré sur le site. La fonction Tunnel GRE vous permet de configurer les appliances SD-WAN pour qu'elles terminent les tunnels GRE sur le réseau local. Pour un itinéraire avec le type de service GRE Tunnel, la Gateway doit résider dans l'un des sous-réseaux de tunnel du tunnel GRE local.
 - **Tunnel IPsec LAN** —Ce service gère le trafic IP destiné au tunnel IPsec.
 - **Routage inter** - Ce service permet la fuite d'itinéraire entre des domaines de routage au sein d'un site ou entre différents sites. Cela élimine le besoin d'un routeur de bord pour gérer les fuites de route.

- **Adresse IP de la passerelle** —Entrez l'**adresse IP de la passerelle** pour cet itinéraire.
- **Admissibilité** - Basé sur le chemin (case à cocher) —(Facultatif) Si cette option est activée, l'itinéraire ne reçoit pas de trafic lorsque le chemin sélectionné est en panne.
- **Chemin d'accès** : spécifie le chemin à utiliser pour déterminer l'éligibilité de l'itinéraire.

Selon le « Type de service », les paramètres suivants s'affichent :

Type de service	Paramètres du type de service
Chemin virtuel	Site de saut suivant : indique le site distant vers lequel les paquets de chemin virtuel sont dirigés.
Internet	Exporter l'itinéraire : Activer/Désactiver pour exporter les itinéraires vers d'autres sites connectés, Éligibilité basée sur le chemin
Intranet	Route d'exportation, service intranet, éligibilité basée sur le chemin, éligibilité basée sur le tunnel
Passthrough	Éligibilité basée sur le chemin d'accès
Locaux	Exporter l'itinéraire, l'itinéraire récapitulatif, l'éligibilité basée sur le chemin
Tunnel GRE	Route d'exportation, éligibilité basée sur le chemin d'accès, éligibilité basée sur la passerelle
Tunnel IPSec	Route d'exportation, Éligibilité basée sur le chemin d'accès, Tunnel IPSec, Éligibilité basée sur le tunnel
Abandonner	Exporter l'itinéraire, l'itinéraire récapitulatif
Routage inter	Service de domaine de routage inter

1. Cliquez sur **Appliquer**.

Remarque

Après avoir cliqué sur **Appliquer**, des avertissements d'audit peuvent apparaître indiquant que d'autres actions sont nécessaires. Un point rouge ou une icône delta de couleur jaune paille indique une erreur dans la section où il apparaît. Vous pouvez utiliser ces avertissements pour identifier les erreurs ou les informations de configuration manquantes. Faites glisser votre curseur sur une icône d'avertissement d'audit pour afficher une brève description des erreurs dans cette section. Vous pouvez également cliquer sur la barre d'état **des audits** gris foncé (en bas de la page) pour afficher la liste complète de tous les avertissements d'audit.

+

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	0.0.0.0/0	5	Virtual Path	Branch1				
2	172.147.21.52/24	5	Local					
3	172.147.22.52/24	5	Local					
4	0.0.0.0/0	65535	Passthrough					

1

Apply

Close

Vous pouvez également modifier les itinéraires configurés comme suit.

Edit

Network IP Address

0.0.0.0/0

Cost

5

Service Type

Virtual Path

Gateway IP Address

Next Hop Site:

Branch1

☒ Eligibility Based On Path

Path:

Branch1-WL-1->MCN-DC-WL-1

Apply

Cancel

Pour ajouter d'autres itinéraires pour le site, cliquez sur **+** à droite de la succursale **Routes**, puis procédez comme ci-dessus.

Vous avez maintenant terminé de saisir les informations de configuration principale pour le nouveau site MCN. Les deux sections suivantes fournissent des instructions pour d'autres étapes facultatives :

- [Configuration de la haute disponibilité \(HA\) pour le site MCN \(facultatif\).](#)
- [Activation et configuration de la sécurité et du chiffrement du réseau étendu virtuel \(facultatif\).](#)

Si vous ne souhaitez pas configurer ces fonctionnalités maintenant, vous pouvez passer directement à la section [Nommer, enregistrer et sauvegarder la configuration du site MCN](#).

Activer et configurer la sécurité et le chiffrement du réseau étendu virtuel (facultatif)

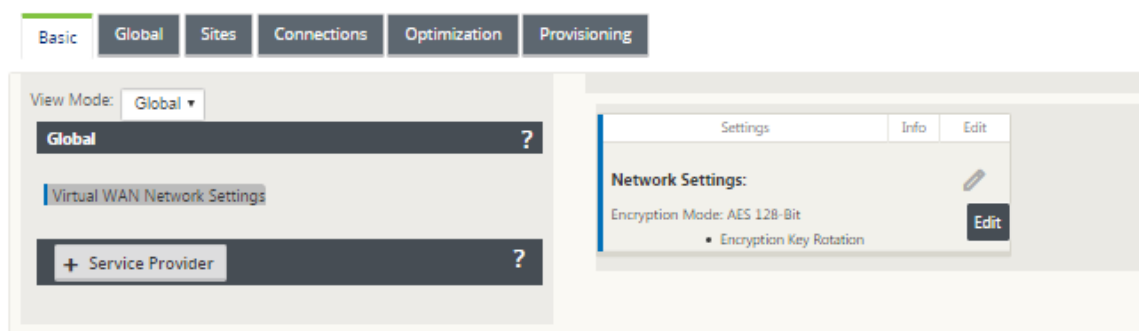
May 6, 2021

Pour activer et configurer la sécurité et le chiffrement Virtual WAN, procédez comme suit :

Remarque

L'activation de la sécurité et du chiffrement Virtual WAN est facultative.

1. Accédez à l'onglet **Basic** dans l'**Éditeur de configuration**, Sélectionner **Global** dans le mode **Affichage** . L'écran de configuration des paramètres de réseau virtuel s'affiche.



2. Cliquez sur **Modifier** (icône en forme de crayon) pour activer la modification du formulaire.

Edit

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode:
AES 128-Bit

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type:
32-Bit Checksum

Apply Cancel

3. Entrez vos paramètres de sécurité globaux. Les options sont les suivantes :

- **Mode de chiffrement réseau** —Il s'agit de l'algorithme de chiffrement utilisé pour les chemins chiffrés. Sélectionnez l'une des options suivantes dans le menu déroulant : **AES 128 bits** ou **AES 256 bits**.
- **Activer la rotation des clés de chiffrement** : lorsque cette option est activée, les clés de chiffrement sont tournées à des intervalles de 10 à 15 minutes.
- **Activer l'en-tête Extended Packet Encryption** : Lorsqu'il est activé, un compteur chiffré de 16 octets est ajouté au trafic chiffré pour servir de vecteur d'initialisation, et le chiffrement aléatoire des paquets.
- **Activer la remorque d'authentification étendue des paquets** : lorsqu'elle est activée, un code d'authentification est ajouté au contenu du trafic chiffré pour vérifier que le message est remis sans modification.
- **Type de remorque d'authentification des paquets étendue** : Il s'agit du type de remorque utilisé pour valider le contenu des paquets. Sélectionnez l'une des options suivantes dans le menu déroulant : **Somme de contrôle 32 bits** ou **SHA-256**.

4. Cliquez sur **Appliquer** pour appliquer vos paramètres à la configuration.

Ceci termine la configuration du site MCN. L'étape suivante consiste à nommer et enregistrer la nouvelle configuration de site MCN (facultatif, mais recommandé), comme décrit dans la section suivante.

Avertissement

Si votre session de console expire ou si vous vous déconnectez de l'interface Web de gestion avant d'enregistrer votre configuration, les modifications de configuration non enregistrées sont perdues. Vous devez ensuite vous reconnecter au système et répéter la procédure de configuration dès le début. Pour cette raison, il est recommandé d'enregistrer le package de configuration souvent, ou à des points clés de la configuration.

Configurer le MCN secondaire

November 1, 2021

Vous pouvez configurer un site en tant que MCN secondaire pour prendre en charge la redondance MCN. Le MCN secondaire surveille en permanence l'état du MCN primaire. Si le MCN principal échoue, le MCN secondaire assume le rôle du MCN. Pour créer un MCN secondaire, tout en ajoutant un nouveau site dans l'option **Mode**, sélectionnez MCN secondaire. Vous pouvez configurer manuellement l'interface virtuelle, l'adresse IP virtuelle, le lien WAN et d'autres paramètres. De même, vous pouvez également configurer un RCN secondaire.

Remarque

Ne confondez pas la configuration MCN secondaire avec la configuration High Availability. Dans la configuration MCN secondaire, une succursale ou un site client situé dans un emplacement géographique différent est configuré en tant que MCN secondaire pour permettre la reprise après sinistre. Dans la configuration HA, deux appliances sont configurées avec le même sous-réseau ou emplacement géographique pour garantir la tolérance aux pannes. Pour plus d'informations sur la configuration de la haute disponibilité, consultez la section [Déploiement de la haute disponibilité](#).

Vous pouvez choisir un modèle d'appliance pour le MCN secondaire en fonction de l'utilisation, de la bande passante requise et du nombre de sites à prendre en charge.

Le basculement MCN principal vers MCN secondaire se produit après 15 secondes après que le MCN principal soit inactif. Vous ne pouvez pas configurer la récupération principale pour le MCN secondaire, la récupération principale se produit automatiquement après la remise en marche de l'appliance principale et l'expiration du délai de mise en attente.

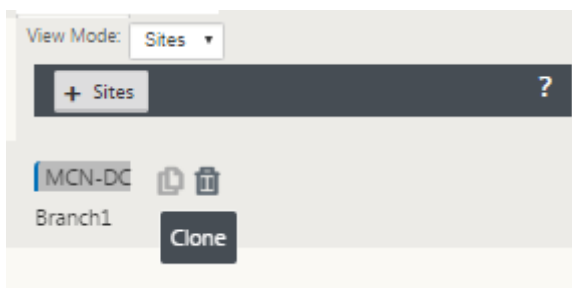
La meilleure façon de configurer un MCN secondaire serait de cloner le MCN existant car il conserve la plupart de la configuration MCN. Lorsqu'un site est cloné, l'ensemble des paramètres de configuration du site sont copiés et affichés dans un seul écran de formulaire. Vous pouvez ensuite modifier les paramètres en fonction des exigences rapidement et facilement.

Remarque

Vous pouvez cloner un MCN pour créer un MCN secondaire ou des sites de branche. Vous ne pouvez configurer qu'un seul MCN secondaire.

Pour cloner un site MCN et créer un MCN secondaire :

1. Dans l'éditeur de configuration, accédez à **Basic > Sites**, puis cliquez sur l'icône de clonage du site MCN.



2. Entrez les paramètres de configuration du nouveau site.

Clone

Please review the following fields and make the appropriate changes for the new Site.

Site Name:

MCN-DC

Appliance Name:

Appliance

Mode:

secondary MCN

Secure Key:

250bcca02112f3b6

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
VirtualInterface-1	0	<input type="checkbox"/>
VirtualInterface-2	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	VirtualInterface-1	172.147.21.52/24
<input checked="" type="checkbox"/>	VirtualInterface-2	172.147.22.52/24

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type
<input checked="" type="checkbox"/>	MCN-DC-WL-1	

Access Interfaces

Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	MCN-DC-WL-1-...	VirtualInterface-1	172.147.21.52	172.147.21.1

| ☒ | MCN-DC-WL-2 | | | |

GRE Tunnels

Include	Name	Source IP	Destination IP	Tunnel IP / Prefix
---------	------	-----------	----------------	--------------------

Clone

Cancel

Remarque :

Un champ en surbrillance avec une icône d’alerte d’audit (point rouge) indique un paramètre obligatoire dont la valeur doit être différente du paramètre actuel.

3. Dans le champ **Mode**, sélectionnez **MCN secondaire**. Résoudre toutes les alertes d’audit.
4. Cliquez sur **Cloner** pour créer le site MCN secondaire.

Gestion de la configuration MCN

May 6, 2021

L’étape suivante consiste à nommer et enregistrer la nouvelle configuration, également considérée comme un package de configuration. Cette étape est facultative à ce stade de la configuration, mais

recommandée. Le package de configuration est enregistré dans votre Workspace sur l'apppliance locale. Vous vous déconnectez ensuite de l'interface Web de gestion et continuez le processus de configuration ultérieurement. Toutefois, si vous vous déconnectez, vous devez rouvrir la configuration enregistrée lorsque vous recommencerez. Les instructions pour ouvrir une configuration enregistrée sont fournies ci-dessous.

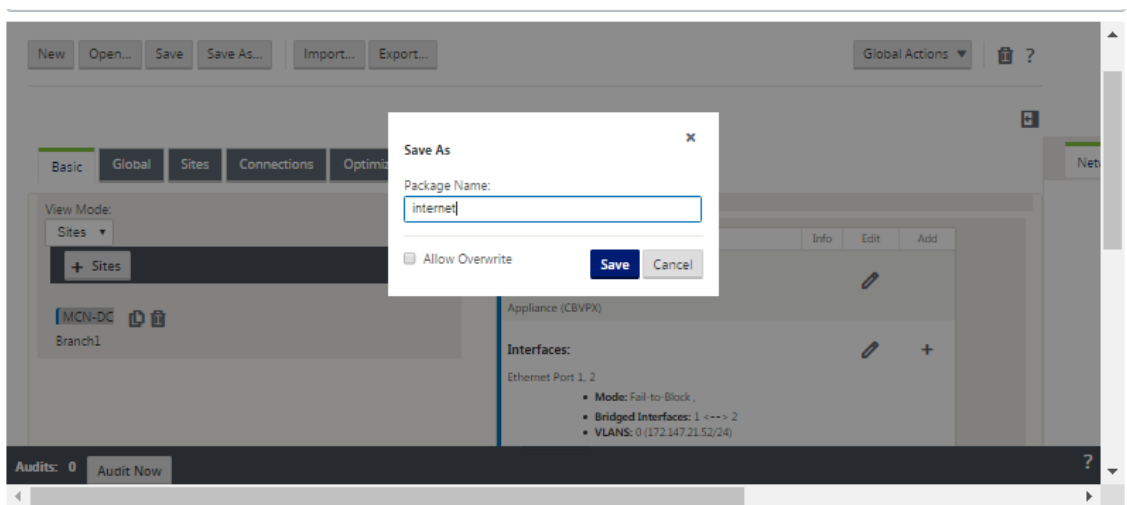
Avertissement

Si la session de la console expire ou si vous vous déconnectez de l'interface Web de gestion avant d'enregistrer votre configuration, les modifications de configuration non enregistrées sont perdues. Vous devez vous reconnecter au système et répéter la procédure de configuration dès le début. Pour cette raison, il est recommandé d'enregistrer le package de configuration souvent, ou à des points clés de la configuration.

Conseil :

Par précaution supplémentaire, il est recommandé d'utiliser **Enregistrer sous**, plutôt que **Enregistrer**, pour éviter d'écraser le mauvais package de configuration .

1. Cliquez sur **Enregistrer sous** (en haut du volet central de l'**Éditeur de configuration**). La boîte de dialogue **Enregistrer sous** s'ouvre.



2. Tapez le nom du package de configuration.

Remarque

Si vous enregistrez la configuration dans un package de configuration existant, veillez à sélectionner **Autoriser l'écrasement** avant d'enregistrer.

3. Cliquez sur **Enregistrer**.

Remarque

Après avoir enregistré le fichier de configuration, vous pouvez vous déconnecter de l'interface Web de gestion et poursuivre le processus de configuration ultérieurement. Toutefois, si vous vous déconnectez, vous devez rouvrir la configuration enregistrée lorsque vous recommencerez. Les instructions sont fournies dans la section [Chargement d'un package de configuration enregistré dans l'éditeur de configuration](#).

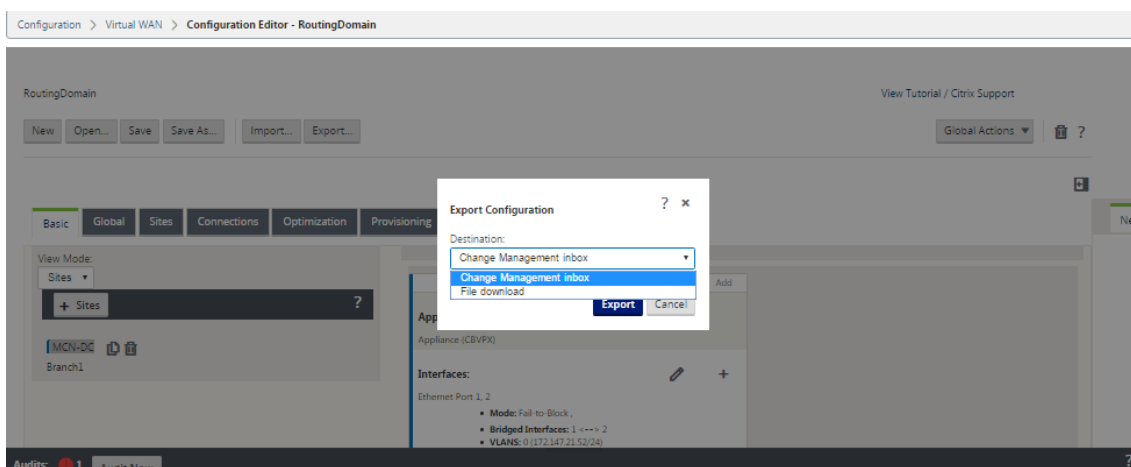
Vous avez maintenant terminé la configuration du site MCN et créé un nouveau package de configuration SD-WAN. Vous êtes maintenant prêt à ajouter et configurer les sites de succursale. Les instructions sont fournies dans [Configuration Branch Sites](#) (/en-us/citrix-sd-wan/current-release/configuration/setup-branch-nodes.html).

Exporter une copie de sauvegarde du package de configuration

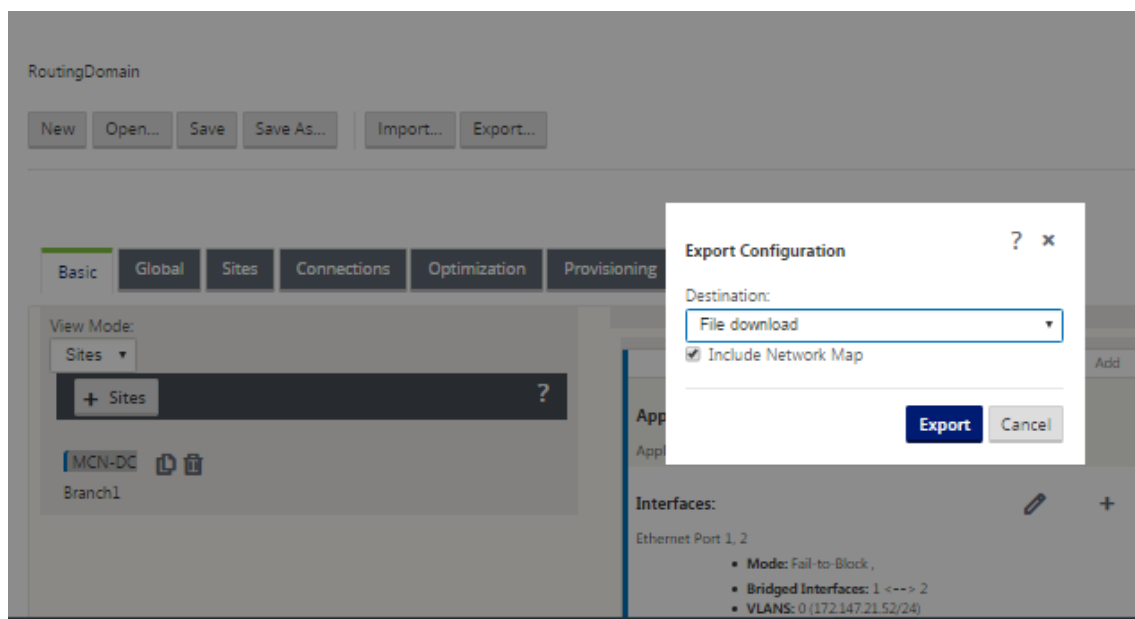
Outre l'enregistrement de la configuration en cours dans l'Workspace de votre appliance, il est recommandé de sauvegarder périodiquement la configuration sur votre PC local.

Pour exporter le package de configuration actuel sur votre PC, procédez comme suit :

1. Cliquez sur **Exporter**. La boîte de dialogue **Exporter la configuration** s'affiche.



2. Sélectionnez **Téléchargement de fichier** dans le menu déroulant **Destination :** . Cette option permet d'**afficher l'option Inclure le mappage réseau**, sélectionnée par défaut.



3. Acceptez la valeur par défaut, puis cliquez sur **Exporter**. Cela inclut les informations de **carte réseau** dans le package de configuration et ouvre un navigateur de fichiers pour spécifier le nom et l'emplacement d'enregistrement de la configuration.
4. Accédez à l'emplacement de sauvegarde sur votre PC et cliquez sur **Enregistrer**. Cela enregistre le package de configuration sur votre PC.

Remarque

Pour récupérer un package de configuration sauvegardé, vous pouvez utiliser une opération d'**importation** pour importer le package à partir de votre PC et le charger dans l'**éditeur de configuration**. Vous pouvez ensuite enregistrer le package importé dans votre Workspace Management Web Interface pour une utilisation ultérieure.

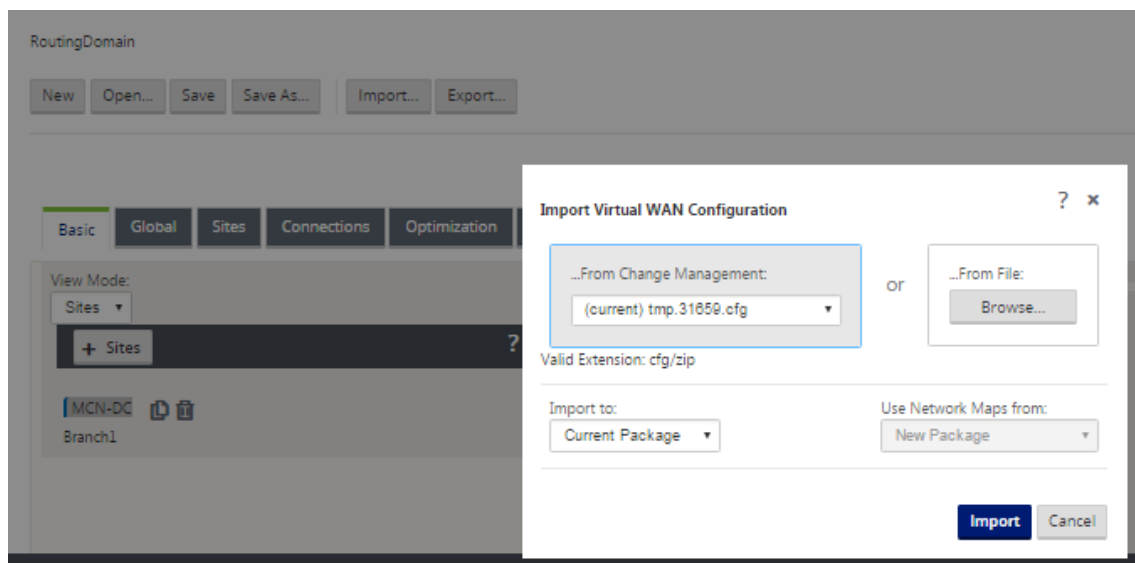
Importer le package de configuration sauvegardé

Parfois, vous pouvez revenir à une version antérieure d'un package de configuration. Si vous avez enregistré une copie de la version antérieure sur votre PC local, vous pouvez l'importer à nouveau dans l'Éditeur de configuration, puis l'ouvrir pour modification. S'il ne s'agit pas d'un déploiement initial, vous pouvez également importer un package de configuration existant à partir de la boîte de réception globale de gestion des modifications sur le MCN actuel. Les instructions relatives à ces deux procédures sont fournies ci-dessous.

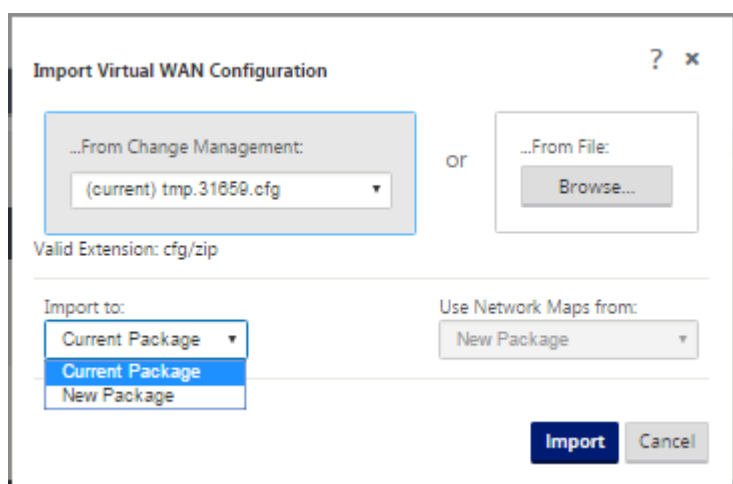
Pour importer un package de configuration, procédez comme suit :

1. Ouvrez l'**éditeur de configuration**.
2. Dans la barre de menus de l'**Éditeur de configuration**, cliquez sur **Importer**.

La boîte de dialogue **Importer la configuration du réseau étendu virtuel** s'affiche.



3. Sélectionnez l'emplacement à partir duquel importer le package.
 - Pour importer un package de configuration depuis Change Management : sélectionnez le package dans le menu déroulant **From Change Management** (dans le coin supérieur gauche).
 - Pour importer un package de configuration depuis votre PC local : cliquez sur **Parcourir** pour ouvrir un navigateur de fichiers sur votre PC local. Sélectionnez le fichier et cliquez sur **OK**.
4. Sélectionnez la destination d'importation (le cas échéant). Si un package de configuration est déjà ouvert dans l'**éditeur de configuration**, le menu déroulant **Importer vers** : sera disponible.

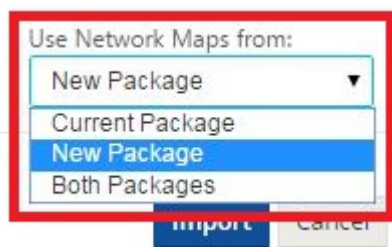


Sélectionnez l'une des options suivantes :

Package actuel : sélectionnez cette option pour remplacer le contenu du package de configuration actuellement ouvert par le contenu du package importé et conserver le nom du package ouvert. Toutefois, le contenu de la version enregistrée du package actuel n'est pas écrasé tant que vous n'avez pas explicitement enregistré le package modifié. Si vous utilisez **Enregistrer sous** pour enregistrer le package, sélectionnez **Autoriser l'écrasement** pour activer l'écrasement de la version précédente.

- **Nouveau package** : sélectionnez cette option pour ouvrir un nouveau package de configuration vide et le remplir avec le contenu du package importé. Le nouveau package prend automatiquement le même nom que le package importé.

5. Spécifiez les cartes réseau à inclure (le cas échéant). Si un package de configuration est déjà ouvert dans l'**éditeur de configuration**, le menu déroulant **Utiliser les cartes réseau à partir de** est disponible.



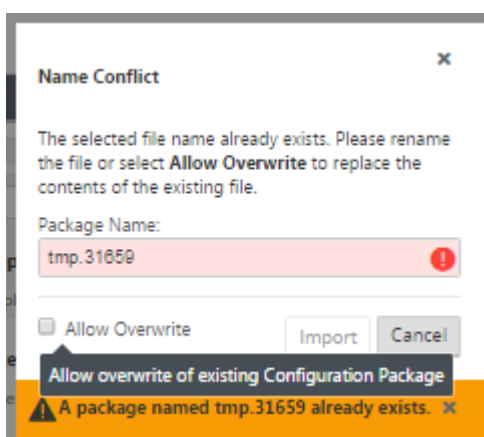
Sélectionnez l'une des options suivantes :

- **Package actuel** : conserve les mappages réseau actuellement configurés dans le package désormais disponible dans l'Éditeur de configuration et rejette les mappages réseau du package importé.
- **Nouveau package** : remplace les mappages réseau actuellement configurés dans le package actuellement ouvert par les mappages réseau (le cas échéant) du package importé.
- **Les deux packages** : cela inclut toutes les cartes réseau du package actuel et du package importé.

6. Cliquez sur **Importer**. Le fichier importé est chargé dans l'**Éditeur de configuration**, selon vos spécifications.

Remarque

Si un package portant le même nom existe dans votre Workspace, la boîte de dialogue **Conflit de noms** s'affiche.



Pour spécifier le nom à utiliser pour le package importé, effectuez l'une des opérations suivantes :

- Tapez un autre nom dans le champ **Nom du package** pour renommer le nouveau package et activer le bouton **Importer** . Le package importé est chargé dans l'**éditeur de configuration** avec le nom spécifié. Le nom du package est maintenant enregistré dans votre Workspace, mais le contenu du package est enregistré dans votre Workspace jusqu'à ce que vous ayez explicitement enregistré le package.
- Sélectionnez **Autoriser l'écrasement** pour confirmer que vous souhaitez conserver le nom existant et activer l'écrasement du contenu du package enregistré. Toutefois, le contenu de la version enregistrée du package actuel ne sera pas écrasé tant que vous n'avez pas explicitement enregistré le package modifié.

Cela active également le bouton **Importer** dans la boîte de dialogue **Conflit de noms** . Cliquez sur **Importer** pour terminer l'opération d'importation.

Charger le package de configuration enregistré

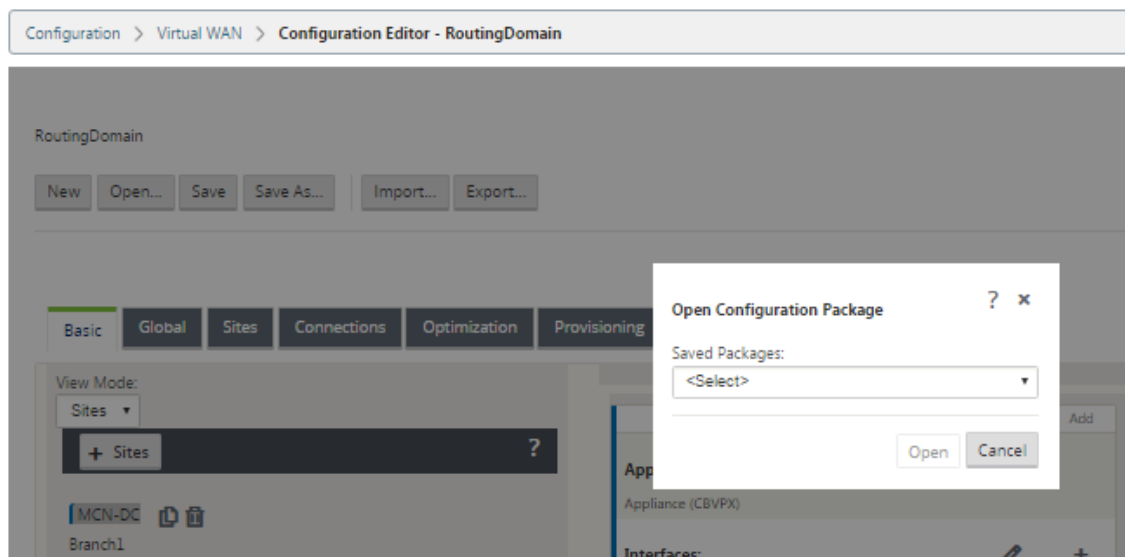
Pour reprendre le travail sur un package de configuration enregistré, vous devez d'abord ouvrir le package et le charger dans l'**Éditeur de configuration**.

Pour charger un package de configuration enregistré, procédez comme suit :

1. Connectez-vous à l'interface Web de gestion et accédez à l'**éditeur de configuration**. La page principale de l'**Éditeur de configuration** s'ouvre pour une nouvelle session.

Si vous êtes de nouveau connecté à l'interface Web de gestion, l'**Éditeur de configuration** s'ouvre initialement pour une nouvelle session, sans package de configuration chargé. Vous pouvez démarrer une nouvelle configuration (**Nouveau**), ouvrir une configuration enregistrée existante (**Ouvrir**) ou importer (**Importer**), puis ouvrir (**Ouvrir**) une configuration précédemment sauvegardée sur votre PC local.

2. Cliquez sur **Ouvrir**. La boîte de dialogue **Ouvrir le package de configuration** s'affiche.



3. Sélectionnez le package à ouvrir dans le menu déroulant **Packages enregistrés**.

Remarque

Si vous avez ouvert l'**Éditeur de configuration**, il peut prendre quelques secondes, une minute ou deux pour que le menu **Packages enregistrés** soit rempli, selon le nombre de configurations que vous avez enregistrées dans votre Workspace. Dans l'intervalle, le champ de menu **Packages enregistrés** peut afficher le message **Aucun package enregistré**. Si cela se produit, cliquez sur **Annuler** pour fermer la boîte de dialogue, attendez quelques instants et cliquez à nouveau sur **Ouvrir** pour rouvrir la boîte de dialogue.

4. Cliquez sur **Ouvrir**.

Remarque

Cela ouvre le package de configuration spécifié et le charge dans l'**éditeur de configuration** pour modification uniquement. Cela ne prépare pas ou n'active pas la configuration sélectionnée sur l'appareil local.

Renommer les sites

Si vous modifiez le nom du site MCN dans l'éditeur de configuration, vous devez appliquer la configuration avec le site renommé au réseau MCN et SD-WAN. Selon le rôle MCN et si la haute disponibilité est activée ou désactivée, les scénarios suivants s'appliquent à la configuration réseau SD-WAN lors du renommage des sites.

- MCN

- MCN avec haute disponibilité
- GEO
- GEO avec haute disponibilité
- RCN
- RCN avec haute disponibilité

Renommer le site MCN

Après avoir renommé le MCN, vous devez charger la nouvelle configuration avec le site renommé.

Pour télécharger une nouvelle configuration pour le site renommé :

1. Depuis le MCN, préparer le déploiement le réseau avec la nouvelle configuration.
2. Téléchargez le package de configuration intermédiaire pour le MCN renommé.
3. Accédez à la page **Gestion des modifications locales** du MCN.
 - a) Téléchargez le package téléchargé plus tôt.
 - b) Cliquez sur **Suivant** une fois le traitement terminé.
 - c) Cliquez sur **Activer**.

Remarque

Une fois l'étape 3 (c) terminée, le processus de gestion des modifications active automatiquement le logiciel intermédiaire pour les appliances (nœuds) du réseau.

Renommer le site MCN avec haute disponibilité

Après avoir renommé le MCN pour lequel la haute disponibilité est activée, vous devez charger la nouvelle configuration.

1. Depuis le MCN, préparer le déploiement le réseau avec une nouvelle configuration.
2. Téléchargez le package de configuration intermédiaire pour les appliances MCN actives et haute disponibilité avec un nouveau nom.
3. Désactivez le service sur l'appliance MCN de secours.
4. Accédez à la page **Gestion des modifications locales** du MCN actif.
 - a) Téléchargez le package téléchargé plus tôt.
 - b) Cliquez sur **Suivant** lorsque le traitement est terminé.
 - c) Cliquez sur **Activer**.
 - d) Répétez les étapes i, ii, iii, iv pour l'appliance MCN de secours désactivée haute disponibilité.
 - e) Activez le service sur l'appliance MCN de secours.

Remarque

Une fois l'étape 4 (c) terminée, le processus de gestion des modifications active automatiquement le logiciel préparé pour être déployé pour les appliances du réseau.

Renommer le site GEO

Pour télécharger une nouvelle configuration pour un site GEO renommé :

1. À partir du MCN, déployez le réseau avec une nouvelle configuration contenant le site GEO renommé.
2. Depuis le MCN, téléchargez le package de configuration intermédiaire pour le site GEO renommé.
3. Sur le **MCN**, sélectionnez **Activate Staged** pour le réseau. Cela désactive le site renommé et le site devient indisponible.
4. Accédez à la page **Gestion des changements locaux** sur le site GEO.
 - a) Téléchargez le package téléchargé plus tôt.
 - b) Cliquez sur **Suivant** lorsque le traitement du package est terminé.
 - c) Cliquez sur **Activer**.

Renommer le site GEO avec haute disponibilité

Pour télécharger une nouvelle configuration avec un site GEO renommé activé avec une haute disponibilité :

1. À partir du MCN, déployez le réseau avec une nouvelle configuration contenant le site GEO renommé.
2. Depuis le MCN, téléchargez le package de configuration intermédiaire pour les appliances actives et haute disponibilité avec le site GEO renommé.
3. Sur le **MCN**, sélectionnez **Activate Staged** pour le réseau. Cela désactive le site renommé et le site devient indisponible.
4. Accédez à l'appliance GEO active.
 - a) Accédez à la page Gestion des changements locaux.
 - b) Téléchargez le package téléchargé plus tôt.
 - c) Cliquez sur **Suivant** lorsque le traitement du package est terminé.
 - d) Cliquez sur **Activer**.
 - e) Répétez les étapes a, b, c et d pour l'appliance de secours.

Renommer le site RCN

Pour télécharger une nouvelle configuration avec un site RCN renommé :

1. À partir du MCN, préparer le déploiement le réseau avec une nouvelle configuration contenant le site RCN renommé.
2. Depuis le MCN, téléchargez le package intermédiaire pour le site RCN renommé.
3. Sur le **MCN**, sélectionnez **Activer Staged** pour le réseau. Cela désactive le site RCN renommé et le site de région devient indisponible sur le MCN. Le site des RCN et les succursales de la région communiquent entre elles, mais tant que l'étape 4 n'est pas terminée, la région ne peut pas communiquer avec le MCN (à moins qu'il n'y ait une RCN GEO qui n'est pas renommée).
4. Accédez à la page Gestion des modifications locales du RCN:
 - a) Téléchargez le package téléchargé plus tôt.
 - b) Cliquez sur **Suivant** lorsque le traitement du package est terminé.
 - c) Cliquez sur **Activer**.

Remarque

les succursales de la région prennent un certain temps pour devenir disponibles, car le déploiement de la région ne se produit qu'après la fin de l'étape 4 (c). Le processus de gestion du changement du RCN gère la zone intermédiaire.

Renommer le site RCN avec une haute disponibilité

Pour télécharger une nouvelle configuration avec un site RCN renommé activé avec une haute disponibilité.

1. À partir du MCN, préparer le déploiement le réseau avec une nouvelle configuration contenant le site RCN renommé.
2. Depuis le MCN, téléchargez le package intermédiaire pour les appliances actives et haute disponibilité avec site RCN renommé. Cela désactive le site RCN renommé et le site de région devient indisponible sur le MCN. Le site des RCN et les succursales de la région communiquent entre elles, mais tant que l'étape 4 n'est pas terminée, la région ne peut pas communiquer avec le MCN (à moins qu'il n'y ait une RCN GEO qui n'est pas renommée).
3. Sur le **MCN**, sélectionnez **Activer la mise en scène pour le réseau**.
4. Désactivez le service sur l'appliance RCN de secours.
5. Accédez à la page **Gestion des modifications locales** du RCN actif :
 - a) Téléchargez le package téléchargé plus tôt.

- b) Cliquez sur **Suivant** lorsque le traitement du package est terminé.
 - c) Cliquez sur **Activer**.
 - d) Répétez les étapes a, b et c pour l'apppliance RCN de secours désactivée.
6. Activez le service sur l'apppliance RCN de secours.

Renommer le site GEO RCN

Pour télécharger une nouvelle configuration avec le site GEO RCN renommé :

1. Depuis le MCN, préparer le déploiement le réseau avec une nouvelle configuration avec renommé site GEO RCN.
2. Depuis le MCN, téléchargez le package de transit pour le site GEO RCN renommé.
3. Sur le **MCN**, sélectionnez **Activate Staged** pour le réseau. Cela désactive le site renommé et le site devient indisponible. Si la RCN principale est en ligne, la région reste connectée au réseau lors du renommage du site GEO RCN.
4. Accédez à la page **Gestion des changements locaux** de GEO RCN :
 - a) Téléchargez le package téléchargé plus tôt.
 - b) Cliquez sur **Suivant** lorsque le traitement du package est terminé.
 - c) Cliquez sur **Activer**.

Renommer le site GEO RCN avec une haute disponibilité

1. Depuis le MCN, préparer le déploiement le réseau avec une nouvelle configuration avec renommé site GEO RCN.
2. Depuis le MCN, téléchargez le package intermédiaire pour l'apppliance active et haute disponibilité pour le site GEO RCN renommé.
3. Sur le **MCN**, sélectionnez **Activate Staged** pour le réseau. Cela désactive le site renommé et le site devient indisponible. Si la RCN principale est en ligne, la région reste connectée au réseau lors du renommage du site GEO RCN.
4. Accédez à la page **Gestion des changements locaux** de GEO RCN active :
 - a) Téléchargez le package téléchargé plus tôt.
 - b) Cliquez sur **Suivant** lorsque le traitement du package est terminé.
 - c) Cliquez sur **Activer**.
 - d) Répétez les étapes a, bande c pour l'apppliance de secours.

Configuration des nœuds de succursale

May 6, 2021

Ce chapitre fournit des instructions pour l'ajout et la configuration des sites de succursale. La procédure d'ajout d'un site de succursale est très similaire à la création et à la configuration du site MCN. Cependant, certaines étapes et paramètres de configuration varient légèrement pour un site de succursale. En outre, une fois que vous avez ajouté un site de succursale initial, pour les sites qui ont le même modèle d'appliance, vous pouvez utiliser la fonctionnalité **Cloner** (dupliquer) pour rationaliser le processus d'ajout et de configuration de ces sites.

Comme pour la création du site MCN pour configurer un site de succursale, vous devez utiliser l'**Éditeur de configuration** dans l'interface Web de gestion sur l'appliance MCN. L'**Éditeur de configuration** n'est disponible que lorsque l'interface est définie en mode **Console MCN**.

Informations supplémentaires sur le déploiement du site de la Direction générale

En plus de ce guide, les articles suivants de support de la Base de connaissances sont également recommandés :

- Étapes de déploiement du mode PBR virtuel WAN ([CTX201577](http://support.citrix.com/article/CTX201577))
<http://support.citrix.com/article/CTX201577>
- Étapes de déploiement du mode passerelle WAN virtuelle ([CTX201576](http://support.citrix.com/article/CTX201576))
<http://support.citrix.com/article/CTX201576>

Présentation des procédures de configuration des sites de succursale

Les étapes à suivre pour mener à bien ce processus sont les suivantes :

1. Ajoutez le site de la succursale.
2. Configurez les groupes d'interface virtuelle pour le site de succursale.
3. Configurez les adresses IP virtuelles pour le site de succursale.
4. (Facultatif) Configurez les tunnels GRE LAN pour le site de la succursale.
5. Configurez les liens WAN pour le site de succursale.
6. Configurez les itinéraires pour le site de succursale.
7. (Facultatif) Configurez la haute disponibilité pour le site de succursale.

8. (Facultatif) Cloner le nouveau site de succursale pour créer et configurer des sites supplémentaires.

Remarque

Le clonage du site est facultatif. Les modèles d'appliance Virtual WAN doivent être les mêmes pour les sites d'origine et les sites clonés. Vous ne pouvez pas modifier le modèle d'appliance spécifié pour un clone. Si le modèle d'appliance est différent pour un site, vous devez ajouter manuellement le site.

9. Résoudre les alertes d'audit de configuration.
10. Enregistrez la configuration terminée.

Configurer le nœud de succursale

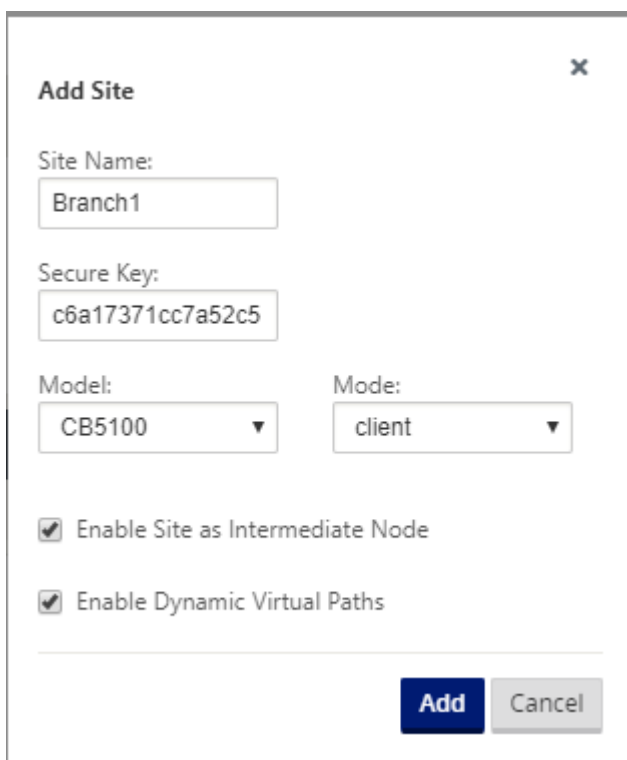
May 6, 2021

Pour ajouter un nouveau site de succursale à la table **Sites** et commencer à configurer le site, procédez comme suit :

Remarque

Si vous vous êtes déconnecté du MCN après avoir créé et enregistré le nouveau package de configuration, vous devrez vous reconnecter et rouvrir la configuration avant de pouvoir continuer. Pour ce faire, cliquez sur **Ouvrir** dans la barre de menus de l'**Éditeur de configuration** (haut de la zone de page). Une boîte de dialogue vous permet de sélectionner la configuration à modifier.

1. En continuant dans l'**Éditeur de configuration**, cliquez sur **Ajouter** dans la barre **Sites** pour commencer l'ajout et la configuration du nouveau site de succursale. La boîte de dialogue **Ajouter un site** s'affiche.



2. Tapez les informations de site suivantes.

Remarque

Les entrées ne peuvent pas contenir d'espaces et doivent être au format Linux.

- **Nom du site** : saisissez un nom pour le site.
 - **Nom de l'appliance** : saisissez le nom que vous souhaitez attribuer à l'appliance.
 - **Clé sécurisée** — Il s'agit d'une clé hexadécimale de 8 à 32 chiffres utilisée pour le chiffrement et la vérification de l'appartenance dans l'appliance SD-WAN. Par défaut, ce champ est prérempli avec une clé de sécurité générée automatiquement. Acceptez la valeur par défaut ou tapez un format hexadécimal personnalisé.
 - **Modèle** : sélectionnez le modèle d'appliance dans le menu déroulant.
 - **Mode** — Sélectionnez le client comme mode.
3. Cliquez sur **Ajouter** pour ajouter le site. Le nouveau site est ajouté à l'arborescence **Sites** et ouvre l'écran de configuration des **paramètres de base** pour le site.

4. Tapez les paramètres de base du site, puis cliquez sur **Appliquer**.

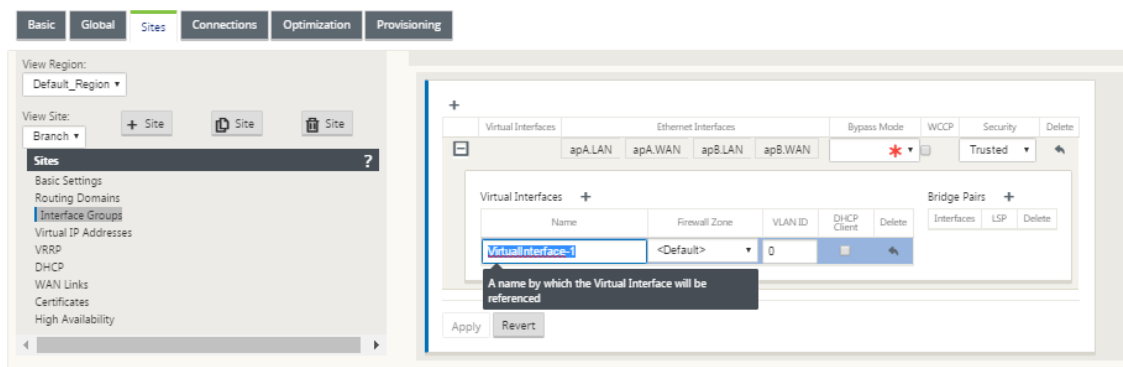
L'étape suivante consiste à ajouter et configurer les groupes d'interface pour le nouveau site de succursale.

Comment configurer des groupes d'interface pour la branche

Pour ajouter un groupe d'interface au nouveau site de succursale, procédez comme suit :

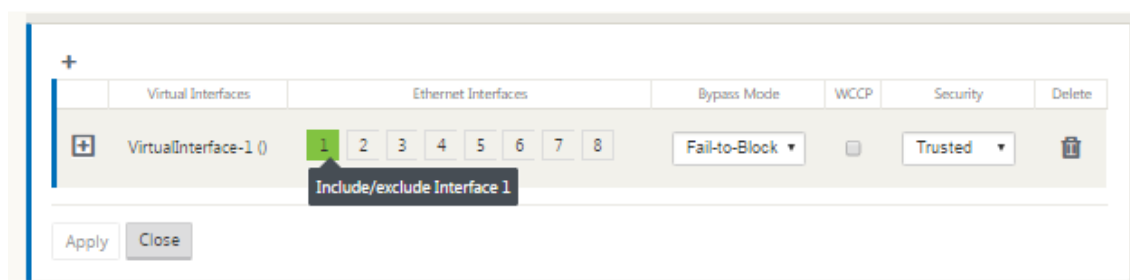
1. En continuant dans la vue **Sites** de l'**Éditeur de configuration**, sélectionnez le site de branche dans le menu déroulant **Site**. Cela ouvre la vue de configuration du site que vous avez sélectionné.

2. Cliquez sur **+** pour ajouter le **groupe d'interface virtuelle**. Une nouvelle entrée de groupe d'interface virtuelle vide est ajoutée à la table et s'ouvre pour modification.
3. Cliquez sur **+** à droite de **Virtual Interfaces**. Une nouvelle entrée de groupe vide est ajoutée à la table et s'ouvre pour modification.



4. Sélectionnez les **interfaces Ethernet** à inclure dans le groupe.

Sous **Interfaces Ethernet**, cliquez sur une interface pour inclure/exclure cette interface. Vous pouvez sélectionner n'importe quel nombre d'interfaces à inclure dans le groupe.



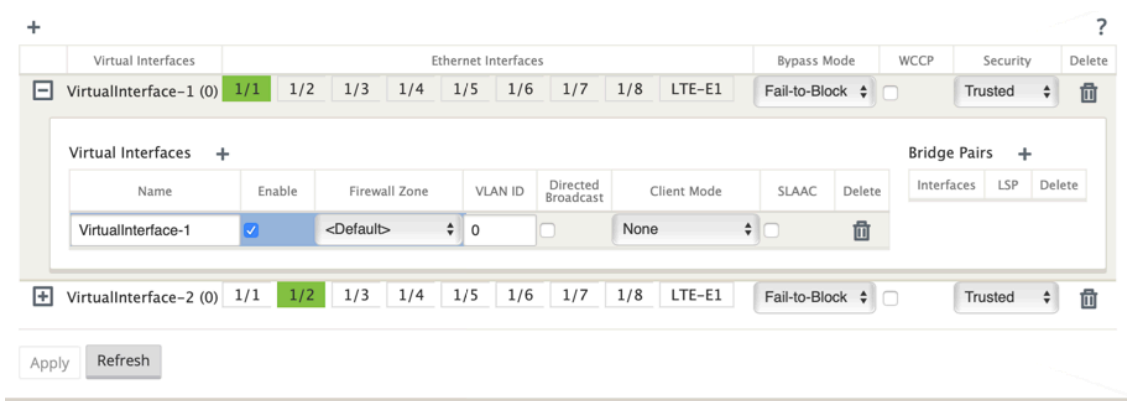
5. Sélectionnez le **mode de contournement** dans le menu déroulant (pas par défaut).

Le **mode de contournement** spécifie le comportement des interfaces jumelées par pont dans le groupe d'interfaces virtuelles, en cas de défaillance ou de redémarrage d'une appliance ou d'un service. Les options sont : **Fail-to-Wire** ou **Fail-to-Block**.

6. Sélectionnez le **niveau de sécurité** dans le menu déroulant.

Indiquez le niveau de sécurité du segment réseau du groupe d'interface virtuelle. Les options sont les suivantes : **Approuvé** ou **Non approuvé**. Les segments approuvés sont protégés par un pare-feu (par défaut est approuvé).

7. Cliquez sur **+** dans le bord gauche de l'interface virtuelle que vous avez ajoutée. Le tableau **Interfaces virtuelles** s'affiche.



8. Cliquez sur **+** à droite de **Virtual Interfaces**. Les ID **Nom**, **Zone de pare-feu** et **ID VLAN** apparaissent.

9. Tapez le **nom** et l'**ID VLAN** de ce groupe d'interface virtuelle.

- **Nom** : nom par lequel ces interfaces virtuelles sont référencées.
- **Activer** - Par défaut, la case à cocher **Activer** est activée pour toutes les interfaces virtuelles. Si vous souhaitez désactiver l'interface virtuelle, **désactivez** la case à cocher Activer.

Remarque

- L'option de désactivation d'une interface virtuelle n'est disponible que si elle n'est pas utilisée par une interface d'accès de liaison WAN. Si l'interface virtuelle est utilisée par une interface d'accès de liaison WAN, la case à cocher est en lecture seule et activée par défaut.
- Lors de la configuration d'autres fonctionnalités, ainsi que des interfaces virtuelles activées, les interfaces virtuelles désactivées sont également répertoriées, sauf sous **Interfaces d'accès** pour un **lien WAN**. Même si vous sélectionnez une interface virtuelle désactivée, l'interface virtuelle n'est pas prise en compte et n'a pas d'impact sur la configuration du réseau.

- **Zone de pare-feu** : sélectionnez une zone de pare-feu dans le menu déroulant.
- **IDVLAN : ID** permettant d'identifier et de marquer le trafic à destination et en provenance de l'interface virtuelle. Utilisez un ID de 0 (zéro) pour le trafic natif/non marqué.

10. Cliquez sur **+** à droite de **Bridge Pairs**. Une nouvelle entrée **Bridge Pairs** est ajoutée et s'ouvre pour modification.

11. Sélectionnez les interfaces Ethernet à associer dans les menus déroulants. Pour ajouter d'autres paires, cliquez à nouveau sur **+** en regard de **Paires de pont**.

12. Cliquez sur **Appliquer**. Vos paramètres sont appliqués et ajoutés au nouveau groupe d'interface virtuelle de la table.

Remarque

À ce stade, une icône d'alerte d'audit delta jaune s'affiche à droite de la nouvelle entrée de groupe d'interface virtuelle. En effet, vous n'avez pas encore configuré d'adresses IP virtuelles (VIP) pour le site. Pour l'instant, vous pouvez ignorer cette alerte, car elle est résolue automatiquement lorsque vous avez correctement configuré les adresses IP virtuelles pour le site.

13. Pour ajouter d'autres groupes d'interface virtuelle, cliquez sur **+** à droite de la succursale **Groupes d'interface**, puis procédez comme ci-dessus.

Comment configurer l'adresse IP virtuelle pour le site de la succursale

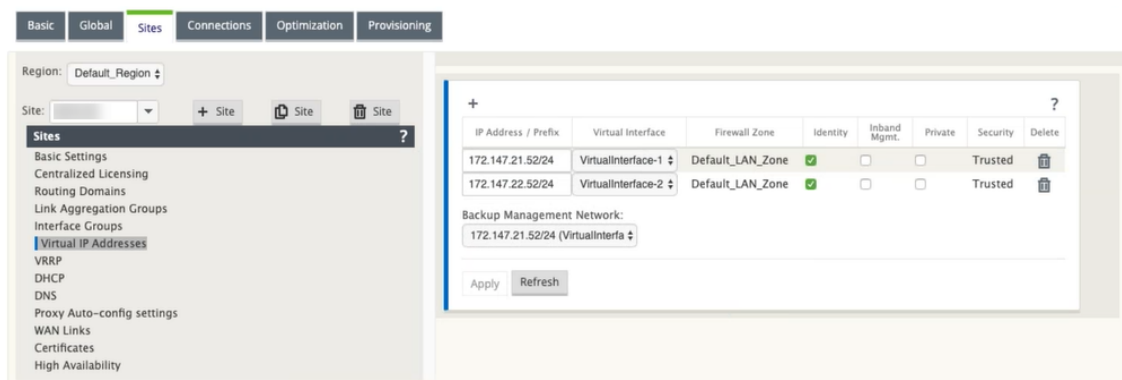
L'étape suivante consiste à configurer les adresses IP virtuelles pour le site et à les affecter au groupe approprié.

1. En continuant dans l'affichage **Sites** du nouveau site Branch, cliquez sur **+** à gauche des **Adresses IP virtuelles**. Le tableau **Adresses IP virtuelles** du nouveau site s'affiche.
2. Cliquez sur **+** à droite de **Virtual IP Adresses** pour ajouter une adresse. Le formulaire d'ajout et de configuration d'une nouvelle adresse IP virtuelle s'affiche.
3. Tapez les informations **Adresse IP / Préfixe**, puis sélectionnez l'**interface virtuelle** à laquelle l'adresse est associée. L'adresse IP virtuelle doit inclure l'adresse hôte complète et le masque réseau.
4. Sélectionnez les paramètres souhaités pour l'adresse IP virtuelle, tels que la zone de pare-feu, l'identité, le privé et la sécurité.
5. Sélectionnez **Gestion Inband** pour permettre à l'adresse IP virtuelle de se connecter à des services de gestion tels que l'interface utilisateur Web et SSH.

Remarque :

L'interface doit être du type de sécurité **approuvé** et **Identité** activée.

6. Sélectionnez une adresse IP virtuelle en tant que **réseau de gestion des sauvegardes**. Cela vous permet d'utiliser l'adresse IP virtuelle pour la gestion si le port de gestion n'est pas configuré avec une Gateway par défaut.

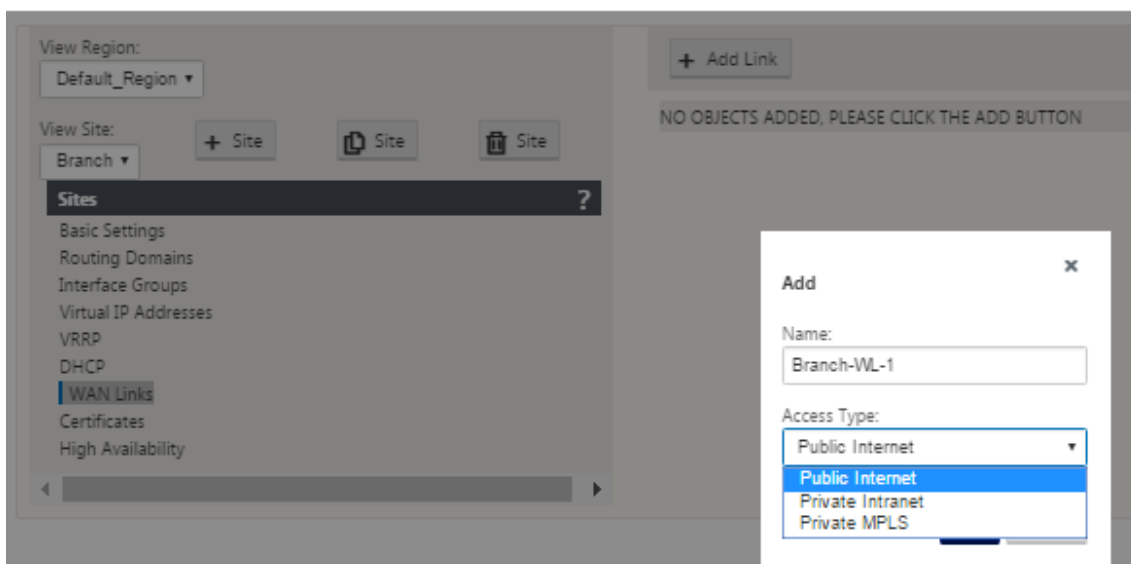


7. Cliquez sur **Appliquer**. Les informations d'adresse au site sont ajoutées et les incluent dans le tableau **Adresses IP virtuelles** du site.
8. Pour ajouter d'autres adresses IP virtuelles, cliquez sur **+** à droite des **adresses IP virtuelles**, puis procédez comme ci-dessus.

Comment configurer les liens WAN pour la branche

L'étape suivante consiste à configurer les liens WAN pour le site.

1. En poursuivant l'affichage **Sites** du nouveau site Branch, cliquez sur l'étiquette **Liens WAN**.
2. Cliquez sur **Ajouter un lien** à droite des **liens WAN** pour ajouter un nouveau lien WAN. La boîte de dialogue **Ajouter** s'affiche.



3. (Facultatif) saisissez un nom pour le lien WAN si vous ne souhaitez pas utiliser la valeur par défaut.

La valeur par défaut est le nom du site, ajouté avec le suffixe suivant :

<number>-WL-

Où <number> est le nombre de liens WAN pour ce site, incrémenté d'un.

4. Sélectionnez le **Type d'accès** dans le menu déroulant.

Les options sont **Internet public**, **Intranet privé** ou **Changement d'étiquette multiprotocole privé**.

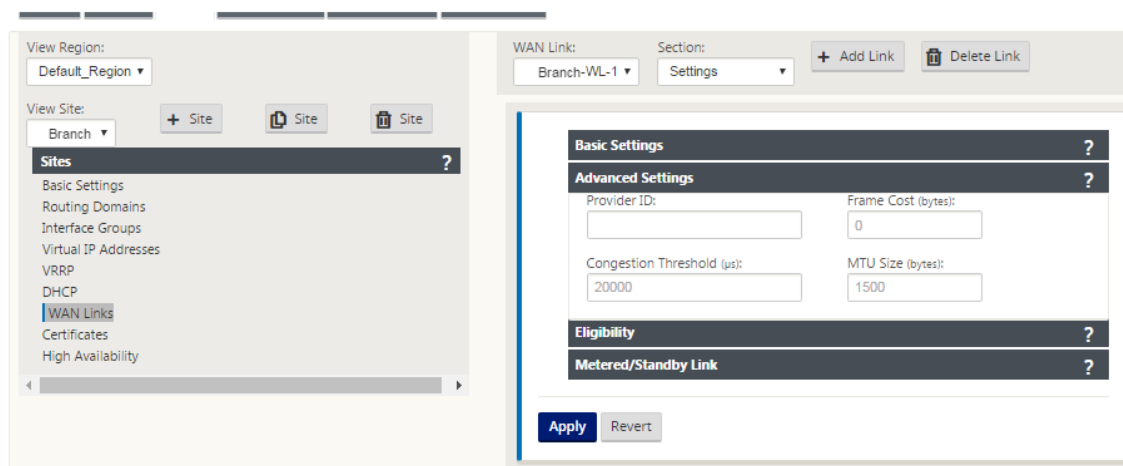
5. Cliquez sur **Ajouter**. La page de configuration des paramètres de base des **liens WAN** s'affiche et ajoute le nouveau lien WAN non configuré à la page.

6. Tapez les détails du lien pour le nouveau lien WAN. Configurez les paramètres LAN vers WAN, WAN vers **LAN**.

Voici quelques lignes directrices :

- Certains liens Internet peuvent être asymétriques. Une mauvaise configuration de la vitesse autorisée peut nuire aux performances de cette liaison.
- Évitez d'utiliser des vitesses de rafale supérieures au taux engagé.
- Pour les liaisons WAN Internet, assurez-vous d'ajouter l'adresse IP publique.

7. Cliquez sur la barre de section **Paramètres avancés** grise. Cela ouvre l'écran **Paramètres avancés** du lien.

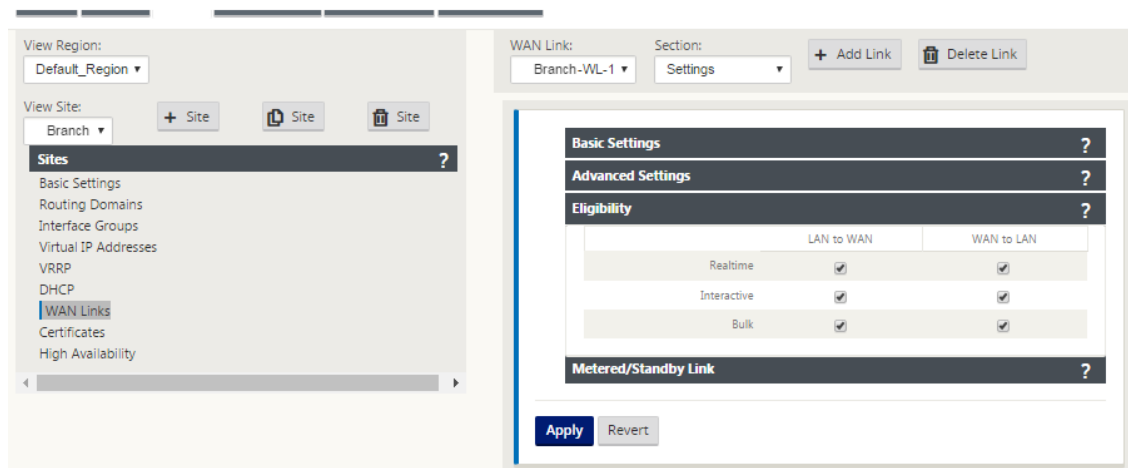


8. Tapez les **paramètres avancés** du lien.

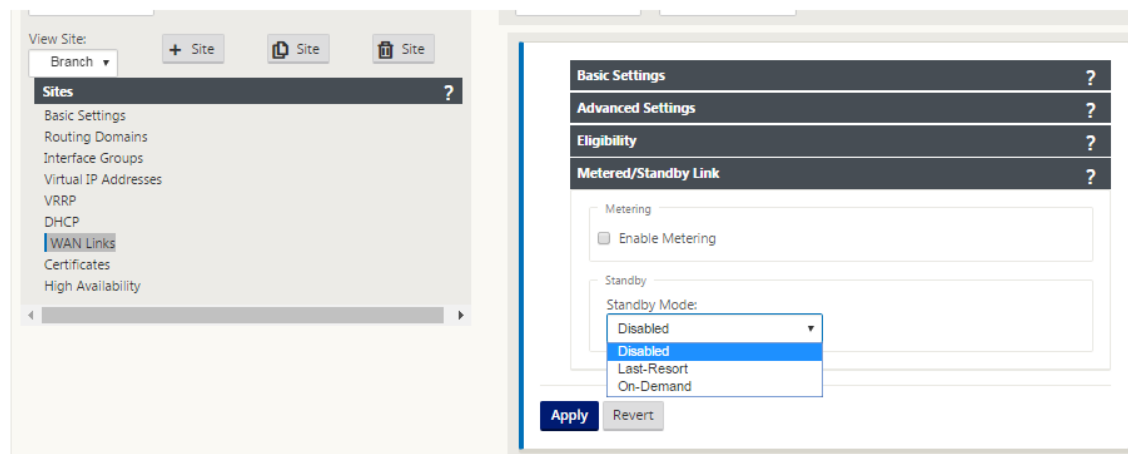
- **ID du fournisseur** —(Facultatif) saisissez un numéro d'identification unique 1—100 pour désigner les liaisons WAN connectées au même fournisseur de services. Virtual WAN utilise l'ID du fournisseur pour différencier les chemins lors de l'envoi de paquets en double.
- **Coût de trame (octets)** : saisissez la taille (en octets) de l'en-tête/remorque ajouté à chaque paquet. Par exemple, la taille en octets des remorques Ethernet IPG ou AAL5 ajoutées.
- **Seuil de congestion** : saisissez le seuil de congestion (en microsecondes) après quoi la liaison WAN limite la transmission des paquets pour éviter toute congestion supplémentaire.
- **Taille MTU (octets)** : saisissez la plus grande taille de paquet brut (en octets), sans inclure le coût de trame.

9. Cliquez sur la barre de section grise **Éligibilité**. Cela ouvre l'écran Paramètres **d'éligibilité** pour le lien.

10. Sélectionnez les paramètres **d'éligibilité** pour le lien.



11. Cliquez sur la barre de section **Lien mesuré** grise. Cela ouvre l'écran Paramètres du **lien mesuré** pour le lien.
12. (Facultatif) Sélectionnez **Activer la mesure** pour activer la mesure pour ce lien. Les champs **Activer les paramètres de mesure** s'affichent.



The screenshot displays three configuration sections in a light gray box:

- Metering:** Contains two checked checkboxes: "Enable Metering" and "Disable if Data Cap reached". Below these are three fields: "Data Cap (MB):" with a value of "0", "Billing Cycle:" with a dropdown menu set to "Monthly", and "Starting From:" with a date format "MM/DD/YYYY".
- Standby:** Contains a "Standby Mode:" dropdown menu set to "Disabled".
- Heartbeat Interval:** Features a yellow warning box stating "Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure." Below this is an "Active Heartbeat Interval:" dropdown menu set to "DEFAULT".

13. Configurez les paramètres de mesure pour le lien. Tapez ce qui suit :

- **Data Cap (Mo)** : saisissez l'allocation de plafond de données pour le lien, en Mo.
- **Cycle de facturation** : sélectionnez **Mensuel ou Hebdomadaire** dans le menu déroulant.
- **À partir de** : saisissez la date de début du cycle de facturation.
- **Définir le dernier recours** —Sélectionnez cette option pour activer ce lien en tant que lien de dernier recours en cas d'échec de tous les autres liens disponibles. Dans des conditions WAN normales, Virtual WAN envoie uniquement un trafic minimal sur les liaisons mesurées, pour vérifier l'état de la liaison. Toutefois, en cas de panne, le SD-WAN peut utiliser des liaisons compteurs actives en dernier recours pour acheminer le trafic de production.

14. Cliquez sur **Appliquer**. Cela applique vos paramètres spécifiés à la nouvelle liaison WAN.

L'étape suivante consiste à configurer les interfaces d'accès pour la nouvelle liaison WAN. Une interface d'accès se compose d'une interface virtuelle, d'une adresse IP du point de terminaison WAN, d'une adresse IP de passerelle et d'un mode chemin virtuel défini collectivement comme une interface pour une liaison WAN spécifique. Chaque liaison WAN doit avoir au moins une interface d'accès.

Remarque

Une option permettant de provisionner automatiquement les partages en tenant compte de la bande passante distante est ajoutée pour configurer les liaisons WAN. L'option Définir le provisioning à l'aide de la bande passante distante permet aux utilisateurs disposant de grands réseaux et de différentes configurations de bande passante de gérer le Provisioning de la bande passante pour les sites de centres de données de manière dynamique.

15. Sélectionnez **Interfaces d'accès** dans la page de configuration du lien WAN pour le lien. Cela

ouvre la vue **Interfaces d'accès** pour le site.

The screenshot shows the configuration interface for a WAN link. At the top, there's a 'WAN Link:' dropdown set to 'Branch-WL-1' and a 'Section:' dropdown set to 'Settings'. To the right are '+ Add Link' and 'Delete Link' buttons. A dropdown menu is open under 'Section:', showing 'Settings' and 'Access Interfaces' (highlighted in blue). Below this, the 'Section:' dropdown is now set to 'Access Interfaces'. Underneath, there's a table with columns: Routing Domain, Virtual Interface, IP Address, Gateway IP Address, Virtual Path Mode, Proxy ARP, Internet Access for All Routing Domains, and Delete. An 'Add' button is on the left of the table. Below the table are 'Apply' and 'Close' buttons.

16. Cliquez sur **+** pour ajouter une interface. Une entrée vide dans le tableau est ajoutée et s'ouvre pour modification. Tapez les paramètres **des interfaces d'accès** pour le lien.

Remarque

Chaque liaison WAN doit avoir au moins une interface d'accès.

The screenshot shows the configuration interface for a WAN link. At the top, there's a 'WAN Link:' dropdown set to 'Branch-WL-1' and a 'Section:' dropdown set to 'Access Interfaces'. To the right are '+ Add Link' and 'Delete Link' buttons. Below this, there's a table with columns: Name, Virtual Interface, IP Address, Gateway IP Address, Virtual Path Mode, Proxy ARP, Internet Access for All Routing Domains, and Delete. The table has one row with the following values: 'Branch-WL-1' (Name), 'VirtualInterface-1' (Virtual Interface), '172.10.10.1' (IP Address), '172.10.10.2' (Gateway IP Address), 'Primary' (Virtual Path Mode), and checkboxes for 'Proxy ARP' and 'Internet Access for All Routing Domains'. Below the table are 'Apply' and 'Close' buttons.

17. Tapez ce qui suit :

- **Nom** : Il s'agit du nom par lequel cette interface d'accès est référencée. Tapez un nom pour la nouvelle interface d'accès ou acceptez la valeur par défaut. La valeur par défaut utilise la convention de dénomination suivante :

WAN_link_name-AI-number

Où *WAN_link_name* est le nom de la liaison WAN que vous associez à cette interface, et le nombre est le nombre d'interfaces d'accès actuellement configurées pour ce lien, incrémenté de 1.

Remarque

Si le nom apparaît tronqué, vous pouvez placer votre curseur dans le champ, puis cliquer longuement et rouler la souris vers la droite ou la gauche pour voir la partie tronquée.

- **Interface virtuelle : Interface** virtuelle utilisée par cette interface d'accès. Sélectionnez une entrée dans le menu déroulant des interfaces virtuelles configurées pour ce site de succursale.
- **Adresse IP : adresse** IP du point de terminaison de l'interface d'accès entre l'appliance et le réseau étendu.
- **Adresse IP de la Gateway** - Il s'agit de l'adresse IP du routeur de la passerelle.
- **Mode Chemin d'accès virtuel** : priorité pour le trafic Chemin d'accès virtuel sur cette liaison WAN. Les options sont : **Principal**, **Secondaire** ou **Exclure**. Si cette option est définie sur **Exclure**, cette interface d'accès est utilisée uniquement pour le trafic Internet et Intranet.
- **Proxy ARP** —Activez la case à cocher pour activer. Si cette option est activée, Virtual WAN Appliance répond aux demandes ARP pour l'adresse IP de la Gateway, lorsque la passerelle est inaccessible.

18. Cliquez sur **Appliquer**.

Vous avez maintenant terminé de configurer la nouvelle liaison WAN. Répétez ces étapes pour ajouter et configurer des liens WAN supplémentaires pour le site.

L'étape suivante consiste à ajouter et configurer les itinéraires pour le site.

Comment configurer des itinéraires pour la branche

Pour ajouter et configurer les itinéraires pour le site, procédez comme suit :

1. Cliquez sur l'affichage **Connexions** du nouveau site Branch et sélectionnez **Itinéraires** . Ceci affiche la vue **Itinéraires** du site.
2. Cliquez sur **+** à droite de **Itinéraires** pour ajouter un itinéraire. La boîte de dialogue **Itinéraires** s'ouvre à modifier.

The screenshot shows the 'Add' configuration window for a new route. The fields are as follows:

Field	Value
Network IP Address	[Empty]
Cost	5
Service Type	Local
Gateway IP Address	[Empty]

Below the input fields, there are several options:

- ☒ Export Route
- ☐ Summary Route
- ☐ Eligibility Based On Path
- Path:
- ☐ Eligibility Based On Gateway

At the bottom right, there are 'Add' and 'Cancel' buttons.

3. Tapez les informations de configuration d'itinéraire pour la nouvelle route.

- **Adresse IP réseau** : saisissez l'adresse IP réseau.
- **Coût** : saisissez un poids de 1 à 15 pour déterminer la priorité de l'itinéraire pour cet itinéraire. Les itinéraires à moindre coût ont priorité sur les itinéraires à coût élevé. La valeur par défaut est 5.
- **Type de service** : sélectionnez le type de service de l'itinéraire dans le menu déroulant correspondant à ce champ. Les options sont les suivantes :
 - **Chemin virtuel** : ce service gère le trafic sur les chemins virtuels. Un chemin virtuel est un lien logique entre deux liaisons WAN. Il comprend une collection de chemins WAN combinés pour fournir une communication de niveau de service élevé entre deux nœuds SD-WAN. Ceci est fait en mesurant constamment et en s'adaptant à l'évolution de la demande des applications et des conditions WAN. Les appliances SD-WAN mesurent le réseau par chemin d'accès. Un chemin virtuel peut être statique (existe toujours) ou dynamique (n'existe que lorsque le trafic entre deux appliances SD-WAN atteint un seuil configuré).
 - **Internet** —Ce service gère le trafic entre un site d'entreprise et des sites d'Internet public. Le trafic de ce type n'est pas encapsulé. Pendant les périodes de congestion, le SD-WAN gère activement la bande passante en limitant le trafic Internet par rapport au chemin virtuel et le trafic Intranet selon la configuration SD-WAN établie par l'administrateur.
 - **Intranet** : ce service gère le trafic Intranet d'entreprise qui n'a pas été défini pour la transmission sur un chemin virtuel. Comme pour le trafic Internet, il reste non encapsulé, et le SD-WAN gère la bande passante en limitant le débit de ce trafic par rap-

port aux autres types de services pendant les périodes de congestion. Dans certaines conditions, et s'il est configuré pour l'Intranet Fallback sur le chemin virtuel, le trafic qui circule habituellement avec un chemin virtuel peut être traité comme du trafic intranet, afin de maintenir la fiabilité du réseau.

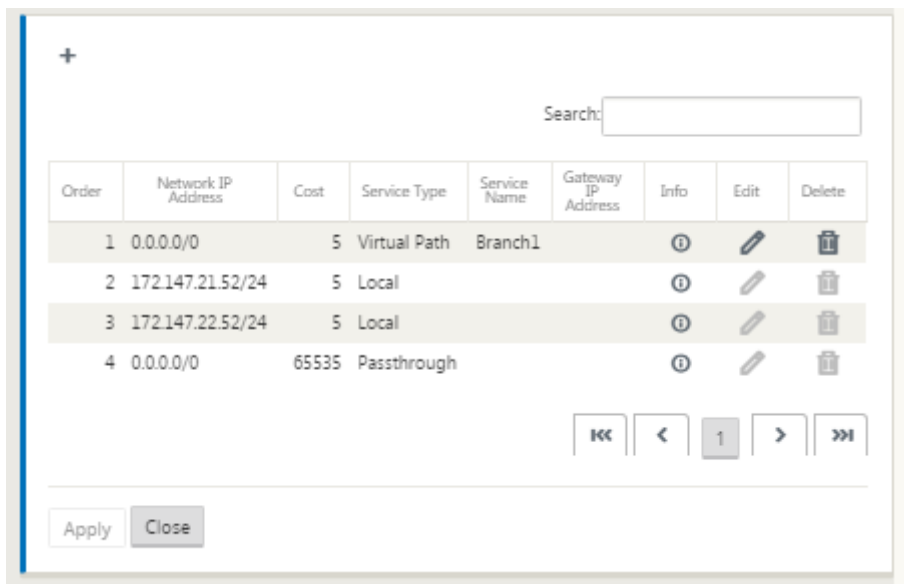
- **Passthrough** : ce service gère le trafic qui doit être transmis via le réseau étendu virtuel. Le trafic dirigé vers le service de transmission comprend les diffusions, les ARP et tout autre trafic non IPv4, ainsi que le trafic sur le sous-réseau local de l'appliance Virtual WAN, les sous-réseaux configurés ou les règles appliquées par l'administrateur réseau. Ce trafic n'est pas retardé, façonné ou modifié par le SD-WAN. Par conséquent, vous devez vous assurer que le trafic Passthrough ne consomme pas de ressources importantes sur les liaisons WAN que l'appliance SD-WAN est configurée pour utiliser pour d'autres services.
 - **Local** : ce service gère le trafic IP local vers le site qui ne correspond à aucun autre service. Le SD-WAN ignore le trafic provenant et destiné à une route locale.
 - **Tunnel GRE** —Ce service gère le trafic IP destiné à un tunnel GRE et correspond au tunnel GRE LAN configuré sur le site. La fonction Tunnel GRE vous permet de configurer des appliances SD-WAN pour mettre fin aux tunnels GRE sur le réseau local. Pour un itinéraire avec le type de service GRE Tunnel, la Gateway doit résider dans l'un des sous-réseaux de tunnel du tunnel GRE local.
 - **Tunnel IPsec LAN** —Ce service gère le trafic IP destiné au tunnel IPsec.
 - **Routage inter** - Ce service permet la fuite d'itinéraire entre des domaines de routage au sein d'un site ou entre différents sites. Cela élimine le besoin d'un routeur de bord pour gérer les fuites de route.
- **Adresses IP de la passerelles** : saisissez l'adresse IP de la passerelle pour cet itinéraire.
 - **Éligibilité basée sur le chemin** (case à cocher) —(Facultatif) Si cette option est activée, l'itinéraire ne reçoit pas de trafic lorsque le chemin sélectionné est en panne.
 - **Chemin d'accès** : spécifie le chemin à utiliser pour déterminer l'éligibilité de l'itinéraire.

4. Cliquez sur **Appliquer**.

Remarque

Après avoir cliqué sur **Appliquer**, des avertissements d'audit peuvent apparaître indiquant que d'autres actions sont nécessaires. Un point rouge ou une icône delta de couleur jaune paille indique une erreur dans la section où il apparaît. Vous pouvez utiliser ces avertissements pour identifier les erreurs ou les informations de configuration manquantes. Faites glisser votre curseur sur une icône d'avertissement d'audit pour afficher une brève description des erreurs dans cette section. Vous pouvez également

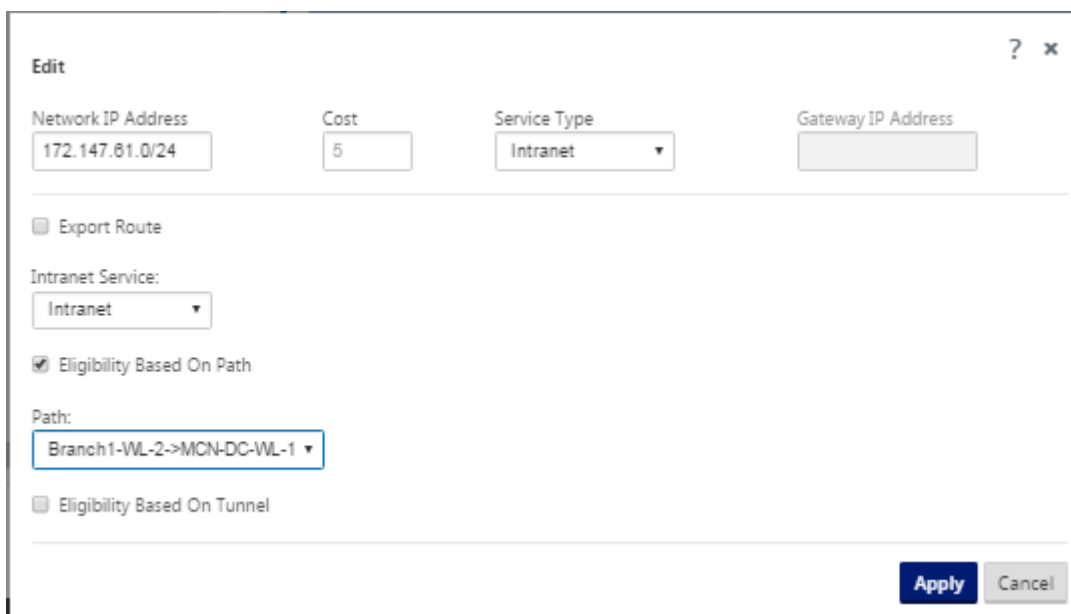
cliquer sur la barre d'état **des audits** gris foncé (en bas de la page) pour afficher la liste complète de tous les avertissements d'audit.



The screenshot shows a window titled with a '+' icon. It contains a search bar and a table of audit entries. The table has columns: Order, Network IP Address, Cost, Service Type, Service Name, Gateway IP Address, Info, Edit, and Delete. There are four entries in the table. Below the table are navigation buttons (first, previous, 1, next, last) and 'Apply' and 'Close' buttons.

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	0.0.0.0/0	5	Virtual Path	Branch1				
2	172.147.21.52/24	5	Local					
3	172.147.22.52/24	5	Local					
4	0.0.0.0/0	65535	Passthrough					

Vous pouvez également modifier les itinéraires configurés comme indiqué ci-dessous.



The screenshot shows an 'Edit' configuration window. It contains fields for Network IP Address (172.147.61.0/24), Cost (5), Service Type (Intranet), and Gateway IP Address. There are checkboxes for 'Export Route', 'Eligibility Based On Path' (checked), and 'Eligibility Based On Tunnel'. The 'Intranet Service' dropdown is set to 'Intranet'. The 'Path' dropdown is set to 'Branch1-WL-2->MCN-DC-WL-1'. 'Apply' and 'Cancel' buttons are at the bottom right.

Vous avez maintenant terminé les étapes requises pour configurer un site client. Vous pouvez également choisir d'effectuer quelques étapes supplémentaires, facultatives, avant de passer à la phase suivante du déploiement. Une liste de ces étapes et des liens vers les instructions sont fournis ci-dessous. Si vous ne souhaitez pas configurer ces fonctionnalités maintenant, vous pouvez passer directement à [Préparation des packages d'appliance SD-WAN sur le MCN](#).

Les étapes facultatives sont les suivantes :

- **Configurer la haute disponibilité** : la haute disponibilité est une configuration dans laquelle deux appliances WAN virtuels d'un site servent dans une capacité de partenariat actif/de secours à des fins de redondance. Si vous n'implémentez pas la haute disponibilité pour ce site, vous pouvez ignorer cette étape. Pour obtenir des instructions, reportez-vous à la section [Configuration de la haute disponibilité \(haute disponibilité\) pour le site de succursale \(facultatif\)](#).
- **Cloner le nouveau site de succursale** : vous avez la possibilité de cloner le site de succursale que vous avez configuré et de l'utiliser comme modèle pour ajouter un autre site. Les modèles d'appliance pour le site d'origine et le clone doivent être les mêmes. Pour obtenir des instructions, veuillez consulter la section [Clonage du site de succursale \(facultatif\)](#).
- **Configurer l'optimisation WAN** : si votre licence Citrix SD-WAN Virtual WAN inclut des fonctionnalités d'optimisation WAN, vous avez la possibilité d'activer et d'ajouter ces fonctionnalités à votre configuration. Pour ce faire, vous devez remplir la section **Optimisation** dans l'**Éditeur de configuration** et enregistrer la configuration modifiée.

Enregistrer la configuration

L'étape suivante consiste à enregistrer la configuration Sites terminée. La configuration est enregistrée dans votre Workspace sur l'appliance locale.

Avertissement

Si la session de console expire ou si vous vous déconnectez de l'interface Web de gestion avant d'enregistrer votre configuration, les modifications de configuration non enregistrées sont perdues. Vous devez ensuite vous reconnecter au système et répéter la procédure de configuration dès le début. Pour cette raison, il est recommandé d'enregistrer le package de configuration souvent, ou à des points clés de la configuration.

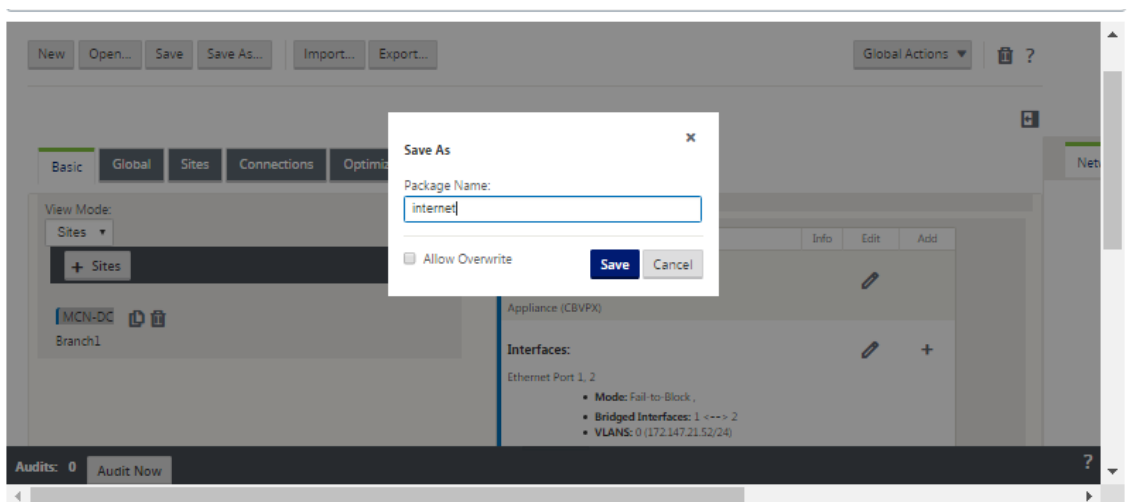
Remarque

Par mesure de précaution supplémentaire, il est recommandé d'utiliser **Enregistrer sous**, plutôt que **Enregistrer**, pour éviter d'écraser le mauvais package de configuration.

Après avoir enregistré le fichier de configuration, vous avez la possibilité de vous déconnecter de l'interface Web de gestion et de poursuivre le processus de configuration ultérieurement. Toutefois, si vous vous déconnectez, vous devez rouvrir la configuration enregistrée lorsque vous reprenez. Les instructions sont fournies dans la section **Configurer MCN** ; [Chargement d'un package de configuration enregistré dans l'éditeur de configuration](#).

Pour enregistrer le package de configuration actuel, procédez comme suit :

1. Cliquez sur **Enregistrer sous** (en haut du volet central de l'**Éditeur de configuration**). La boîte de dialogue **Enregistrer sous** s'ouvre.



2. Tapez le nom du package de configuration. Cliquez sur **Enregistrer**.

Remarque

Si vous enregistrez la configuration dans un package de configuration existant, veuillez à sélectionner **Autoriser l'écrasement** avant d'enregistrer.

L'étape suivante consiste à configurer le service Virtual Paths et Virtual Path Service entre le MCN et les sites clients. Les instructions sont fournies dans le [Configuration du service de chemin d'accès virtuel entre le MCN et les sites clients](#).

Renommer le site de succursale

Après avoir renommé le site de la branche, vous devez télécharger un nouveau package de configuration sur le réseau.

1. À partir du MCN, préparer le déploiement le réseau avec une nouvelle configuration contenant le site de succursale renommé.
2. Téléchargez le package intermédiaire pour le site de succursale renommé.
3. Sur le **MCN**, sélectionnez **Activer le réseau intermédiaire**. Cela désactive le site renommé et le site devient indisponible.
4. Accédez à la page **Gestion des changements locaux** de succursale.
5. Téléchargez le package téléchargé plus tôt. Cliquez sur **Suivant**, puis sur **Activer**.

Renommer un site de succursale avec une haute disponibilité

Pour télécharger une nouvelle configuration après avoir renommé un site de succursale activé avec une haute disponibilité :

1. À partir du MCN, mettre en place le réseau avec une nouvelle configuration qui contient le site de succursale renommé.
2. Téléchargez le package intermédiaire pour l'appliance active et haute disponibilité avec un site de succursale renommé.
3. Sur le **MCN**, sélectionnez **Activate Staged** pour le réseau. Cela désactive le site renommé et le site devient indisponible.
4. Accédez à l'appliance active au niveau de la succursale. Accédez à la page **Gestion des modifications locales**.
5. Téléchargez le package téléchargé plus tôt. Cliquez sur **Suivant**, puis sur **Activer**.
6. Répétez les étapes 4 (a) et 4 (b) pour l'appliance de secours.

Cloner un site de succursale (Facultatif)

May 6, 2021

Cette section fournit des instructions pour le clonage du nouveau site de succursale à utiliser comme modèle partiel pour ajouter d'autres sites de succursale.

Remarque

Le clonage du site est facultatif. Les modèles d'appliance Virtual WAN doivent être les mêmes pour les sites d'origine et les sites clonés. Vous ne pouvez pas modifier le modèle d'appliance spécifié pour un clone. Si le modèle d'appliance est différent pour un site, vous devez ajouter manuellement le site, comme indiqué dans les sections précédentes.

Le clonage d'un site simplifie le processus d'ajout et de configuration d'autres nœuds de succursale. Lorsqu'un site est cloné, l'ensemble complet des paramètres de configuration du site est copié et affiché dans une seule page de formulaire. Vous pouvez ensuite modifier les paramètres en fonction des exigences du nouveau site. Certains paramètres d'origine peuvent être conservés, le cas échéant. Cependant, la plupart des paramètres doivent être uniques pour chaque site.

Pour cloner un site, procédez comme suit :

1. Dans l'arborescence **Sites** (volet central) de l'**Éditeur de configuration**, cliquez sur le site de succursale que vous souhaitez dupliquer.

Cela ouvre cette branche de site dans l'arborescence **Sites** et révèle le bouton **Cloner** (icône double page) et le bouton Supprimer (icône corbeille).

2. Cliquez sur l'**icône Cloner** située à droite du nom du site de succursale dans l'arborescence.
La page de configuration du **site de clonage** s'ouvre.

Clone

Please review the following fields and make the appropriate changes for the new Site.

Site Name: **BR1** ! Appliance Name: Mode: Secure Key: Region:

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
VirtualInterface-1	<input type="text" value="0"/>	<input type="checkbox"/>
VirtualInterface-2	<input type="text" value="0"/>	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	VirtualInterface-1	172.110.0.5/24 !
<input checked="" type="checkbox"/>	VirtualInterface-2	192.110.0.5/24 !

Local Routes

Include ☐ Network Address ☐ Routing Domain ☐ Gateway ☐

WAN Links

Include Link	WAN Link	Access Type										
<input checked="" type="checkbox"/>	BR1-WL-1 !											
<p>Access Interfaces</p> <table border="1"> <thead> <tr> <th>Include Interface</th> <th>Access Interface</th> <th>Virtual Interface</th> <th>Virtual IP Address</th> <th>Gateway</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>BR1-WL-1-AI-1</td> <td>VirtualInterface-1</td> <td>172.110.0.5 !</td> <td>172.110.0.1 !</td> </tr> </tbody> </table>			Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway	<input checked="" type="checkbox"/>	BR1-WL-1-AI-1	VirtualInterface-1	172.110.0.5 !	172.110.0.1 !
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway								
<input checked="" type="checkbox"/>	BR1-WL-1-AI-1	VirtualInterface-1	172.110.0.5 !	172.110.0.1 !								
<input checked="" type="checkbox"/>	BR1-WL-2 !											
<p>Access Interfaces</p> <table border="1"> <thead> <tr> <th>Include Interface</th> <th>Access Interface</th> <th>Virtual Interface</th> <th>Virtual IP Address</th> <th>Gateway</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>BR1-WL-2-AI-1</td> <td>VirtualInterface-2</td> <td>192.110.0.5 !</td> <td>192.110.0.1 !</td> </tr> </tbody> </table>			Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway	<input checked="" type="checkbox"/>	BR1-WL-2-AI-1	VirtualInterface-2	192.110.0.5 !	192.110.0.1 !
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway								
<input checked="" type="checkbox"/>	BR1-WL-2-AI-1	VirtualInterface-2	192.110.0.5 !	192.110.0.1 !								

GRE Tunnels

Include ☐ Name Source IP Destination IP Tunnel IP / Prefix

3. Entrez les paramètres de configuration du nouveau site.

Un champ rose avec une icône d'alerte d'audit (point rouge) indique un paramètre obligatoire qui doit avoir une valeur différente de celle du site cloné d'origine. Habituellement, cette valeur doit être unique.

Conseil

Pour rationaliser davantage le processus de clonage, utilisez une convention de dénomination cohérente et prédéfinie lorsque vous nommez les clones.

4. Résolvez les alertes d'audit.

Pour diagnostiquer une erreur, faites défiler votre curseur sur l'icône **Alerte d'audit** (point rouge ou delta de verge d'or) pour afficher l'aide de bulles pour cette alerte spécifique.

5. Cliquez sur **Cloner** (dans le coin droit) pour créer le site et l'ajouter à la table **Sites**.

Remarque

Le bouton **Cloner** reste indisponible tant que vous n'avez pas saisi toutes les valeurs requises et que la nouvelle configuration du site n'a pas d'erreur.

6. (Facultatif.) Enregistrez vos modifications dans la configuration.

Remarque

Par mesure de précaution supplémentaire, il est recommandé d'utiliser **Enregistrer sous**, plutôt que **Enregistrer**, pour éviter d'écraser le mauvais package de configuration. Veillez à sélectionner **Autoriser l'écrasement** avant d'enregistrer dans une configuration existante, sinon vos modifications ne sont pas enregistrées.

Répétez les étapes jusqu'à ce point pour chaque site de succursale que vous souhaitez ajouter.

Une fois que vous avez terminé d'ajouter tous les sites, l'étape suivante consiste à vérifier la configuration des alertes d'audit et à apporter des corrections ou des ajouts au besoin.

Audit de la configuration des succursales

May 6, 2021

Une icône d'alerte d'audit (un point rouge ou un delta de verge d'or) à côté d'un élément indique une erreur de configuration ou des informations manquantes sur les paramètres pour cet élément. Un nombre en regard de l'icône indique le nombre d'erreurs associées à cette alerte. Pour voir l'aide de bulles pour une alerte particulière, faites défiler votre curseur sur l'icône d'alerte. Ceci affiche une brève description des erreurs spécifiques signalées par cette alerte. Vous devez résoudre toutes les alertes d'audit de la configuration, sinon vous ne serez pas en mesure de vérifier, de préparer le déploiement et d'activer le package de configuration, plus tard dans le processus de déploiement.

La résolution de toutes les alertes d'audit (le cas échéant) termine la phase **Sites** de la configuration. L'étape suivante consiste à enregistrer la configuration **Sites** terminée.

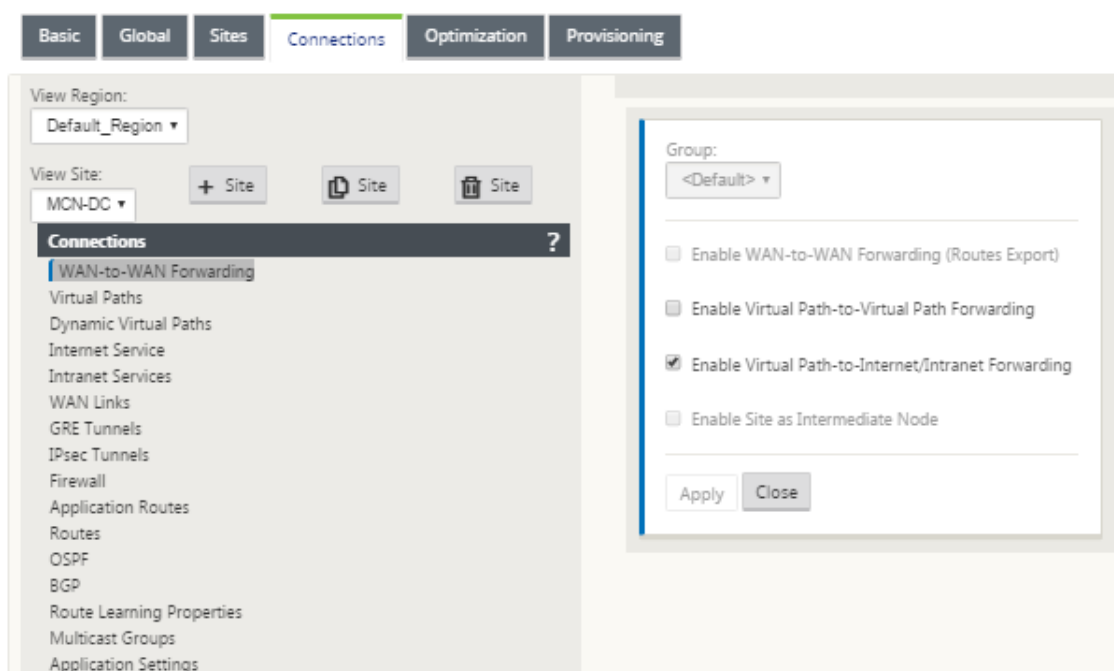
Configuration du service de chemin d'accès virtuel entre le MCN et les sites clients

May 6, 2021

L'étape suivante consiste à configurer le service Virtual Path entre le MCN et chacun des sites client (branche). Pour ce faire, vous utilisez les formulaires de configuration et les paramètres disponibles dans l'arborescence de configuration de la section **Connexions** de l'**Éditeur de configuration**.

Pour configurer le service de chemin d'accès virtuel entre le MCN et un site client, procédez comme suit :

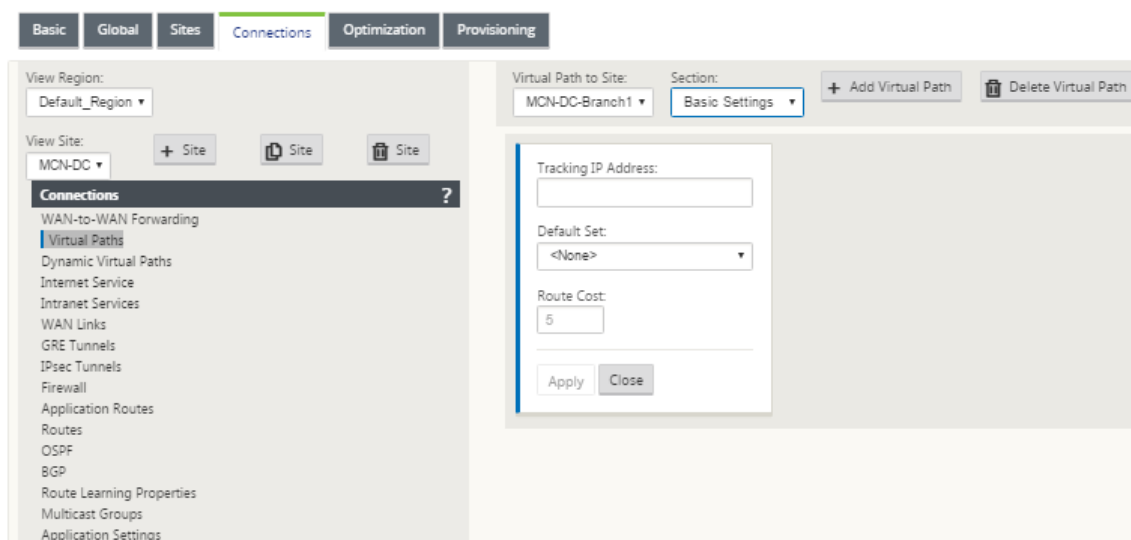
1. En poursuivant dans l'**Éditeur de configuration**, cliquez sur l'onglet **Connexions**. L'arborescence de configuration de la section **Connexions** s'affiche.
2. Sélectionnez le **MCN** dans le menu déroulant **Afficher le site** de la page de la section **Connexions**. Cela ouvre le site MCN dans la configuration **Connexions**.



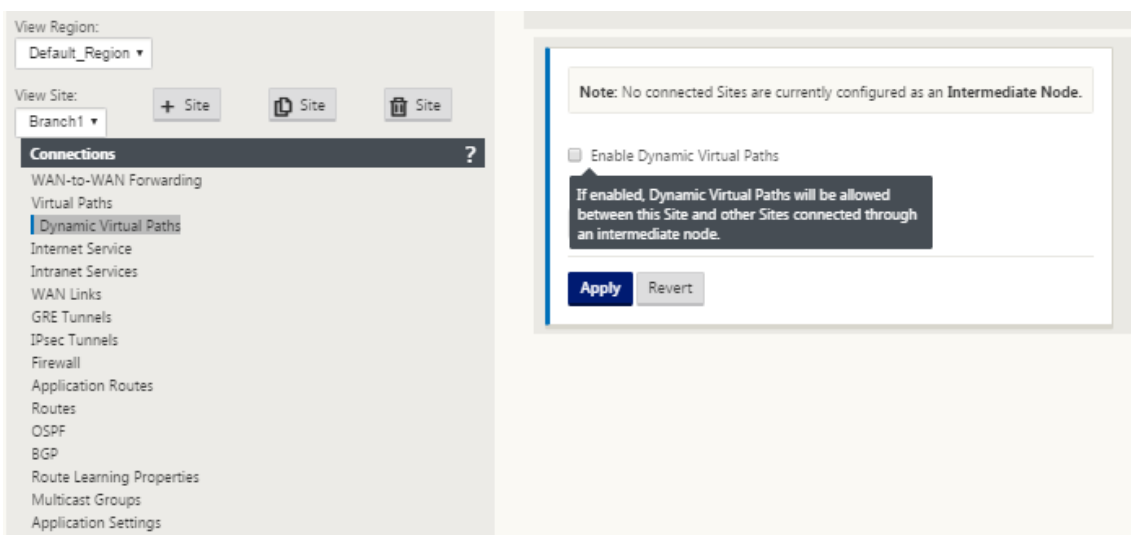
Remarque

Les groupes de transfert WAN vers WAN sont pris en charge uniquement dans une région et non entre les régions. Vous pouvez utiliser les régions pour séparer les réseaux au lieu de vous fier aux groupes de transfert WAN vers WAN.

3. Cliquez sur **Chemins virtuels**. Cela ouvre la section de **configuration des chemins virtuels** (branche enfant) pour le site MCN. Cette section fournit des paramètres et des formulaires pour configurer le service de chemin d'accès virtuel entre le MCN et chacun des sites clients virtuels WAN. La figure suivante illustre un exemple de section Chemins virtuels pour un site MCN.



La figure suivante illustre un exemple de section **Chemins virtuels dynamiques** pour un site Branch.



La section **Chemins virtuels dynamiques** permet de configurer les éléments suivants :

- **Chemins virtuels dynamiques** —(Facultatif) Les paramètres de cette section vous permettent d'activer et de désactiver les chemins virtuels dynamiques et de définir le nombre maximal de chemins virtuels dynamiques autorisés pour le site. Les chemins virtuels dynamiques sont des chemins virtuels établis directement entre les sites, en fonction d'un seuil configuré. Le seuil est généralement basé sur la quantité de trafic qui se produit entre ces sites. Les chemins virtuels dynamiques ne sont opérationnels qu'une fois le seuil spécifié atteint. Les chemins virtuels dynamiques ne sont pas requis pour un fonctionnement normal. La configuration de cette section est donc facultative.
- **<MCN_Site_Name>_<Branch_Site_Name>** —Le système ajoute initialement automatiquement un chemin virtuel statique entre le MCN et un site client, car ce chemin virtuel

est requis. Le nom du chemin d'accès utilise la forme suivante :

<MCN_Site_Name>_<Branch_Site_Name>

Où :

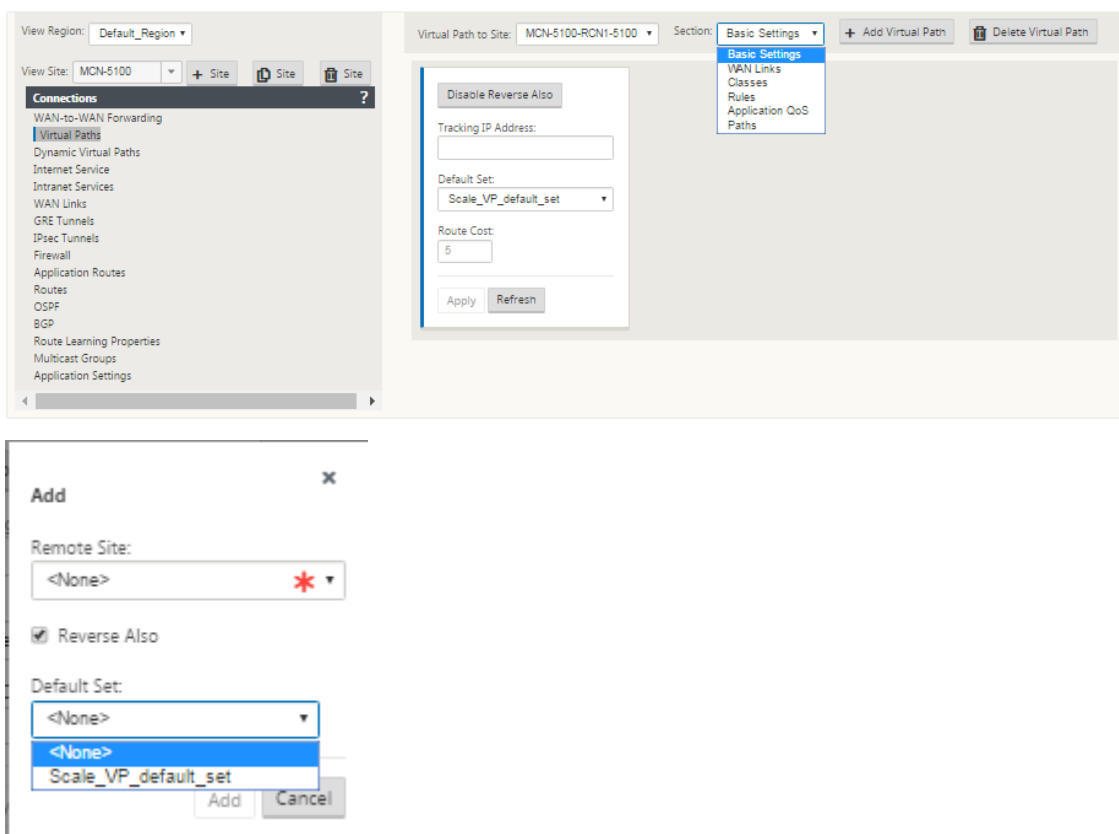
MCN_site_name est le nom du MCN pour ce réseau WAN virtuel.

Branch_Site_Name est le nom d'un site client identifié dans le package de configuration actuel.

Les paramètres par défaut configurables par l'utilisateur sont initialement appliqués au chemin virtuel statique, tel que défini dans la section **Chemin virtuel > Jeux par défaut** de l'arborescence de configuration **Connexions**. Toutefois, vous pouvez personnaliser ou ajouter les **ensembles par défaut** définis, ainsi que personnaliser la configuration d'un site spécifique et d'un chemin virtuel.

Remarque

Pour ajouter des chemins virtuels statiques supplémentaires pour un site, vous devez le faire manuellement. Les instructions relatives à l'ajout manuel d'un chemin virtuel statique sont incluses dans les étapes suivantes.

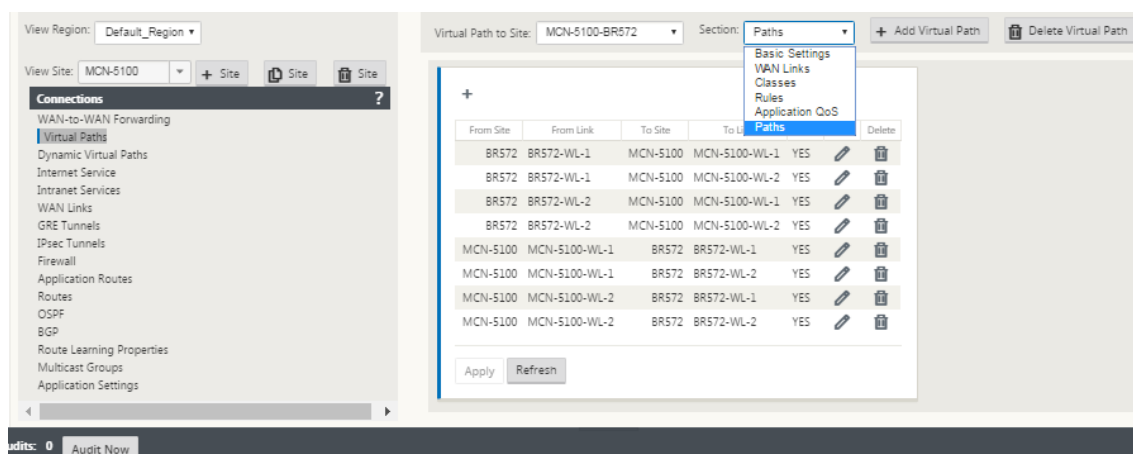


4. Cliquez sur **+ Ajouter un chemin virtuel** en regard du nom du chemin virtuel statique dans la section **Chemins virtuels**. Cela révèle plus de configuration pour le chemin virtuel statique :

- a) **Site distant** : cette section vous permet d’afficher et de configurer les paramètres du **chemin virtuel** du point de vue d’un site distant. Vous pouvez afficher, personnaliser et ajouter une **classe** ou des **règles** selon les besoins pour ce chemin virtuel spécifique. Vous pouvez également ajouter des chemins virtuels au site distant, si nécessaire.
- b) **Reverse aussi** - Lorsque cette option est activée, les classes et les règles sont mises en miroir sur les deux sites le chemin virtuel.
- c) **Jeu par défaut** - Nom du jeu par défaut Chemin virtuel utilisé pour remplir les règles et les classes du chemin virtuel sur le site.

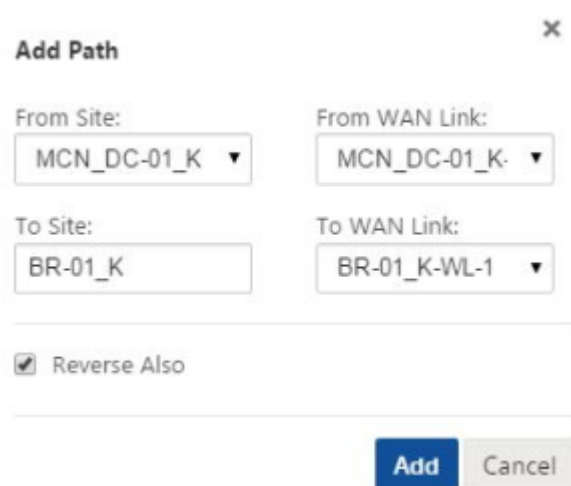
La figure suivante montre un exemple de succursale MCN statique Virtual Path et de succursales enfants.

5. Sélectionnez **Chemins** dans le menu déroulant **Section** .



6. Cliquez sur + (Ajouter) au-dessus du tableau **Chemins** .

La boîte de dialogue **Ajouter un chemin** (écran de configuration) s’affiche.



7. Spécifiez les informations de site source et de destination pour le nouveau chemin d’accès virtuel.

8. Spécifiez les éléments suivants dans les menus déroulants disponibles :

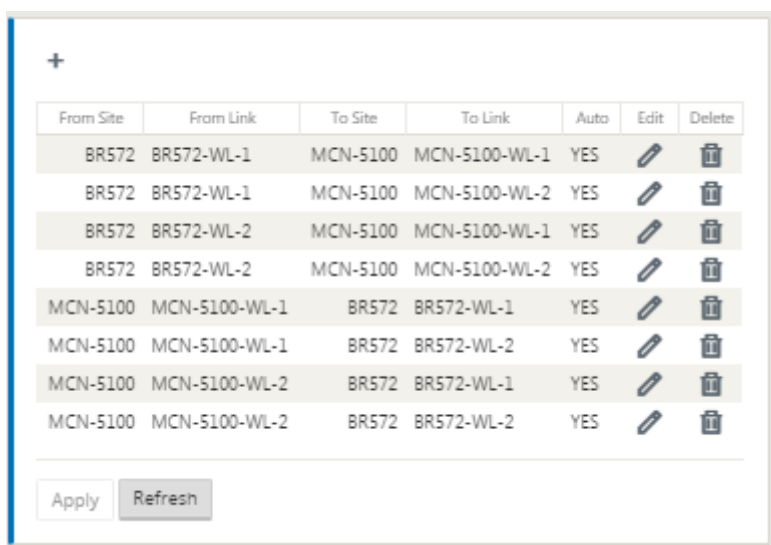
Remarque

Selon la façon dont les liens WAN sont configurés pour les sites, certains champs sont en lecture seule. Les champs configurables fournissent un menu déroulant des sélections disponibles.

- **À partir du site** : il s'agit du site source du chemin virtuel. Pour le chemin virtuel statique requis, il est configuré comme site MCN par défaut.
- **From WAN Link** : il s'agit de la liaison WAN d'origine pour le chemin virtuel.
- **Vers le site** : il s'agit du site de destination du chemin d'accès virtuel.
- **Lien vers WAN** : il s'agit de la liaison WAN de destination pour le chemin virtuel.

9. Cliquez sur **Ajouter**.

Cela ajoute le chemin d'accès virtuel configuré au MCN et au site client associé dans l'arborescence **Connexions > Chemins d'accès virtuels**. Cela ouvre également automatiquement l'écran de configuration des paramètres des **chemins** pour le **site From** du chemin virtuel (dans ce cas, le MCN).



From Site	From Link	To Site	To Link	Auto	Edit	Delete
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-2	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-2	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-2	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-2	YES		

Apply Refresh

10. Cliquez sur Modifier (icône en forme de crayon), à droite de l'étiquette Chemin virtuel MCN vers client. Cela ouvre l'écran de configuration du service de chemin d'accès virtuel pour modification.
11. Configurez les paramètres du chemin d'accès virtuel ou acceptez les valeurs par défaut.

L'écran de configuration des **chemins** contient les paramètres suivants :

- **À partir de la section Site** :

- **Site** —Il s’agit du site source du chemin d’accès virtuel. Pour le chemin virtuel statique requis, il est configuré comme site MCN par défaut.
- **Lien WAN** : il s’agit de la liaison WAN d’origine pour le chemin virtuel.
- **Section vers le site :**
 - **Site** —Il s’agit du site de destination du chemin virtuel.
 - **Lien WAN** : il s’agit de la liaison WAN de destination pour le chemin virtuel.
- **Inverser aussi** - Cochez cette case pour activer Inverser également pour ce chemin virtuel. Si cette option est activée, le système crée automatiquement un chemin virtuel dans la direction opposée du chemin configuré, en utilisant les mêmes liaisons WAN que celles configurées pour le chemin d’accès d’origine.
- **Balises IP DSCP** —Sélectionnez une balise dans le menu déroulant. Indique la balise DSCP à définir dans l’en-tête IP pour le trafic circulant sur ce chemin virtuel.
- **Activer le chiffrement** : cochez cette case pour activer le chiffrement des paquets envoyés le long de ce chemin virtuel.
- **Sensible à la perte - Bad** : sélectionnez un paramètre dans le menu déroulant. Les options sont les suivantes :
 - **Activer**—(par défaut) Si cette option est activée, les chemins sont marqués **BAD** en raison d’une perte et entraînent une pénalité de notation de chemin.
 - **Désactiver** —**Désactiver** la fonctionnalité **Bad Loss Sensitive** peut être utile lorsque la perte de bande passante est intolérable.
 - **Personnalisé** : sélectionnez Personnalisé pour spécifier le pourcentage de perte au fil du temps requis pour marquer un chemin comme étant BAD. La sélection de cette option permet d’afficher les paramètres suivants :
 - ★ **Pourcentage de perte (%)** —Indique le pourcentage de seuil de perte avant qu’un chemin soit marqué BAD, tel que mesuré sur la durée spécifiée. Par défaut, le pourcentage est basé sur les 200 derniers paquets reçus.
 - ★ **Au fil du temps (ms)** : spécifie la période (en millisecondes) sur laquelle mesurer la perte de paquets. Sélectionnez une option comprise entre 100 et 2000 dans le menu déroulant de ce champ.
 - **Période de silence (ms)** : spécifie la durée (en millisecondes) avant que l’état du chemin passe de **GOOD** à **BAD** .

La valeur par défaut est de 150 millisecondes. Sélectionnez une option comprise entre 150 et 1000 dans le menu déroulant de ce champ.

- **Période de probation du chemin (ms)** : indique le temps d'attente (en millisecondes) avant qu'un chemin passe de BAD à GOOD. Sélectionnez une option comprise entre 500 et 60000 dans le menu déroulant de ce champ. La valeur par défaut est 10 000 millisecondes.
 - **Sensible à l'instabilité** : cochez cette case pour l'activer. Si cette option est activée, les pénalités de latence dues à un état de chemin de **BAD** et d'autres pics de latence sont prises en compte dans l'algorithme de notation de chemin.
 - **Suivi de l'adresse IP** : saisissez une adresse IP virtuelle sur le chemin virtuel qui peut faire l'objet d'une commande ping pour déterminer l'état du chemin d'accès.
 - **Adresse IP de suivi inverse**: si l'option **Inverser également** est activée pour le chemin d'accès virtuel, entrez une adresse IP virtuelle sur le chemin d'accès qui peut faire l'objet d'une commande ping pour déterminer l'état du chemin d'accès inverse.
12. Cliquez sur **Appliquer**. Cela révèle que les deux nouveaux chemins virtuels **de site** et **de site** de site entre le MCN et le site client ont été ajoutés à la table Chemins d'accès.

Edit ✕

Convert to Static Path

Convert Path, AND all other Paths associated by WAN Link, Generated by an Autopath Group, to a Static Path. This action cannot be undone

MCN-5100

WAN Link:
BR572-WL-1

BR572

WAN Link:
MCN-5100-WL-1

☒ Reverse Also
 ☒ Enable Encryption

IP DSCP Tagging:
Any ▼

Bad Loss Sensitive:
Enable (Default) ▼

Silence Period (ms):
DEFAULT ▼

Path Probation Period (ms):
10000 (Default) ▼

☒ Instability Sensitive

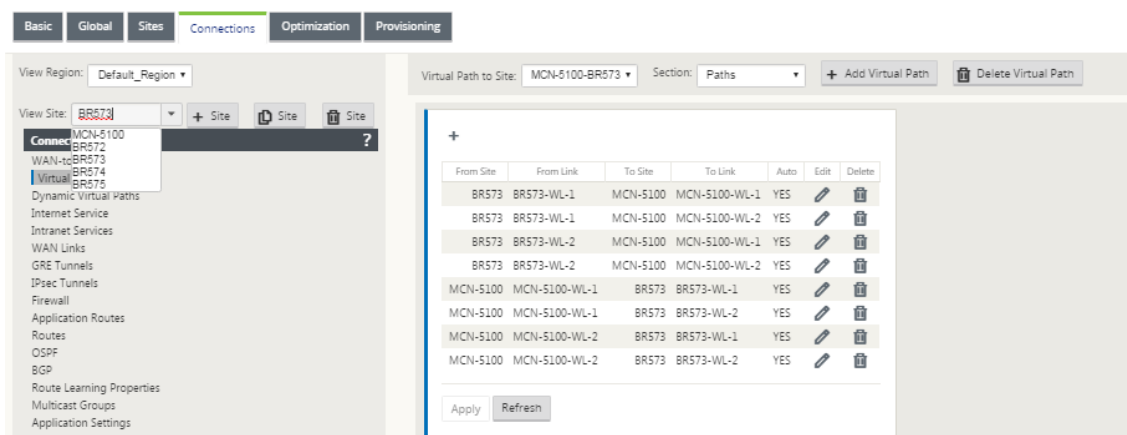
Tracking IP Address:

Reverse Tracking IP Address:

13. Répétez les étapes ci-dessus pour chaque branche que vous souhaitez connecter au MCN.

Ensuite, vous avez la possibilité de personnaliser les configurations de chemins virtuels pour les sites clients, ainsi que d'ajouter et de configurer d'autres chemins entre les clients. Les instructions sont fournies dans les étapes suivantes, ci-dessous.

14. Sélectionnez une succursale de site client dans le menu déroulant **Afficher le site**. La configuration de la succursale de site client dans l'arborescence **Connexions** s'ouvre.

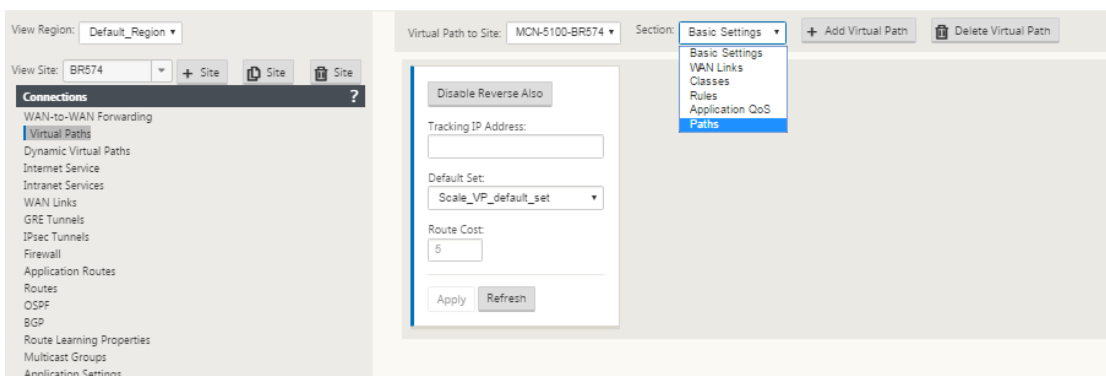


15. Accédez à l'écran de configuration des paramètres des **chemins** d'accès pour tout site client. Chemin virtuel que vous souhaitez configurer.

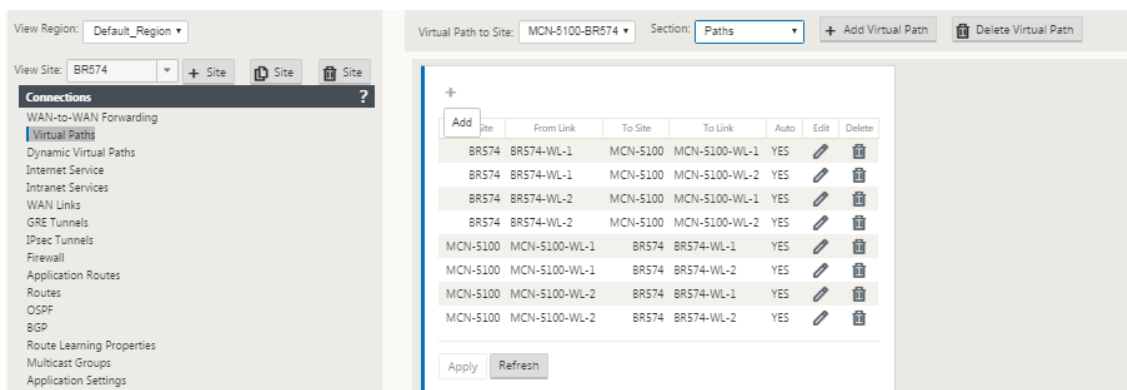
Pour accéder à l'écran Paramètres des **chemins** d'accès pour le site client, procédez comme suit :

16. Sélectionnez **Chemins** dans l'onglet **Section** de la page de succursale pour le site client.

La figure suivante illustre un exemple de configuration des **chemins** d'accès pour le nouveau chemin **d'accès du site** ajouté dans les étapes précédentes.



17. Configurez les paramètres de chaque chemin à personnaliser. Suivez les mêmes étapes que pour configurer les chemins d'accès virtuels pour le site MCN.



Ceci termine la configuration de base des chemins virtuels entre les sites clients et le MCN.

Remarque

Pour plus d'informations sur la configuration de paramètres supplémentaires dans les sections **Connexions** ou **Provisioning** de l'**Éditeur de configuration**, reportez-vous à l'aide en ligne de l'interface Web de gestion pour ces sections. Si vous ne souhaitez pas configurer ces paramètres actuellement, vous pouvez passer à l'étape appropriée indiquée ci-dessous.

L'étape suivante dépend de la licence SD-WAN Edition que vous avez activée pour votre déploiement, comme suit :

- **Édition SD-WAN Premium (Enterprise)** — L'édition Premium (Enterprise) inclut l'ensemble complet des fonctionnalités d'optimisation WAN. Si vous souhaitez configurer l'optimisation WAN pour vos sites, veuillez passer à la rubrique [Activation et configuration de l'optimisation WAN](#). Sinon, vous pouvez passer directement à [Installation des packages d'appliance SD-WAN sur les clients](#).
- **Édition SD-WAN** — Cette édition n'inclut pas les fonctionnalités d'optimisation WAN. Vous pouvez maintenant passer directement à [Installation des packages d'appliance SD-WAN sur les clients](#).

Déployer la configuration MCN

May 6, 2021

L'étape suivante consiste à préparer les packages d'appliance SD-WAN pour distribution vers les nœuds clients. Cela implique les deux procédures suivantes :

1. Exportez le package de configuration vers Gestion des modifications.

Avant de pouvoir générer les packages d'appliance, vous devez d'abord exporter le package de configuration terminé à partir de l'**Éditeur de configuration** vers la boîte de réception globale de la **gestion des modifications** sur le MCN. Les instructions sont fournies dans la section [Exécuter la gestion des modifications](#).

2. Générer et préparer le déploiement des packages d'appliance.

Après avoir ajouté le nouveau package de configuration à la boîte de réception **Gestion des modifications**, vous pouvez générer et préparer le déploiement des packages d'appliance. Pour ce faire, vous allez utiliser l'Assistant **Gestion des modifications** dans l'interface Web de gestion sur le MCN. Les instructions sont fournies dans la section [Déployer la configuration dans les succursales](#).

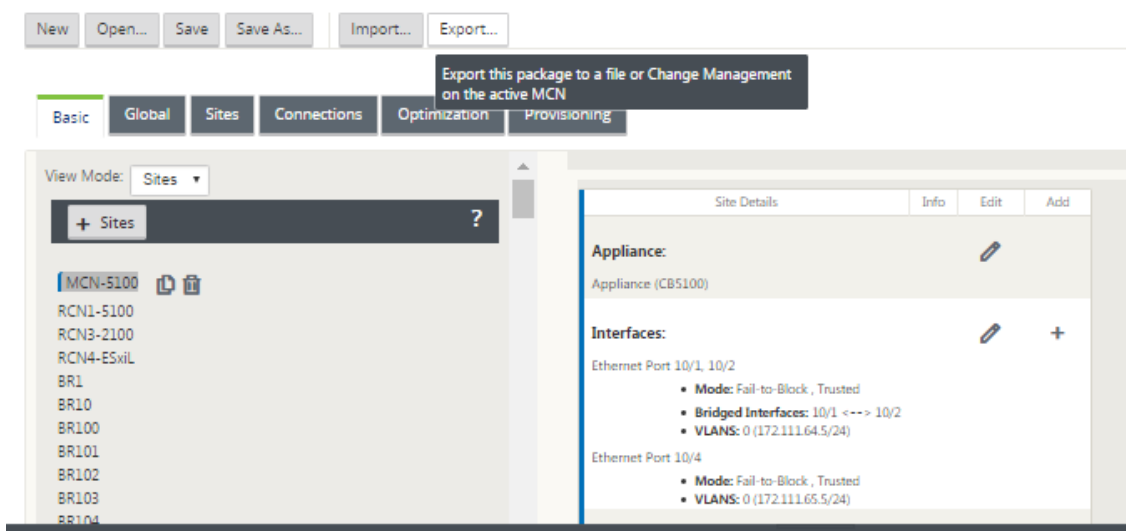
Exécuter la gestion des modifications MCN

May 6, 2021

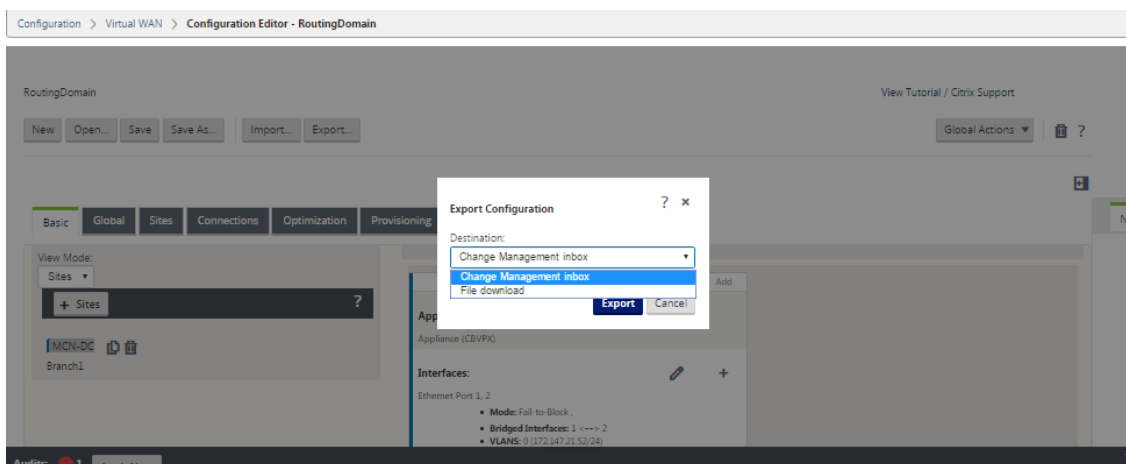
Avant de pouvoir générer les packages d'appliance, vous devez d'abord exporter le package de configuration terminé vers le système de gestion des **modifications de l'interface Web de gestion**.

Pour exporter le package de configuration vers **Gestion des modifications**, procédez comme suit :

1. Dans la page **Éditeur de configuration**, cliquez sur **Exporter** (en haut de la page).



La boîte de dialogue **Exporter la configuration** s'ouvre.



2. Sélectionnez **Change Management** Boîte de réception comme destination d'exportation. Utilisez le menu déroulant du champ **Destination** pour effectuer votre sélection.
3. Cliquez sur **Exporter**.

Une fois l'opération d'exportation terminée, un message vert d'état de réussite s'affiche en haut de la page.

Conseil

Vous pouvez cliquer sur le lien bleu **Gestion des modifications** dans le message de réussite pour accéder directement à la page **Préparation des modifications —Chargement et vérification des fichiers** (deuxième page) de l'Assistant **Gestion des modifications**. Vous devrez accéder à cette page pour effectuer l'étape suivante du processus de configuration. Toutefois, le message de réussite s'affiche pendant quelques secondes seulement, après quoi vous devez utiliser l'arborescence de navigation pour ouvrir l'Assistant, puis passer à cette page. Les instructions sont fournies dans la section suivante.

Vous êtes maintenant prêt à charger les packages logiciels SD-WAN vers l'appliance MCN et à préparer les packages d'appliance pour distribution vers les nœuds clients.

Déployer la configuration dans les succursales

May 6, 2021

Après avoir préparé la configuration à l'aide de l'éditeur de configuration et exporté le package de configuration vers la boîte de réception de gestion des modifications, l'étape suivante consiste à préparer les packages d'appliance SD-WAN pour distribution vers les nœuds clients. Utilisez l'Assistant **Gestion des modifications** dans l'interface Web de gestion sur le MCN.

Il existe un logiciel SD-WAN différent pour chaque modèle d'appliance SD-WAN. Un package d'appliance se compose du package logiciel d'un modèle spécifique, fourni avec le package de configuration que vous souhaitez déployer. Par conséquent, un package d'appliance différent doit être préparé et généré pour chaque modèle d'appliance de votre réseau.

Remarque

Si vous n'avez pas encore téléchargé les packages logiciels SD-WAN requis sur un PC connecté à votre réseau, vous pouvez le faire maintenant. Pour plus d'informations sur l'acquisition et le téléchargement du logiciel, consultez la section [Acquisition des logiciels SD-WAN](#)

Pour télécharger et installer le package et la configuration sur le MCN, procédez comme suit :

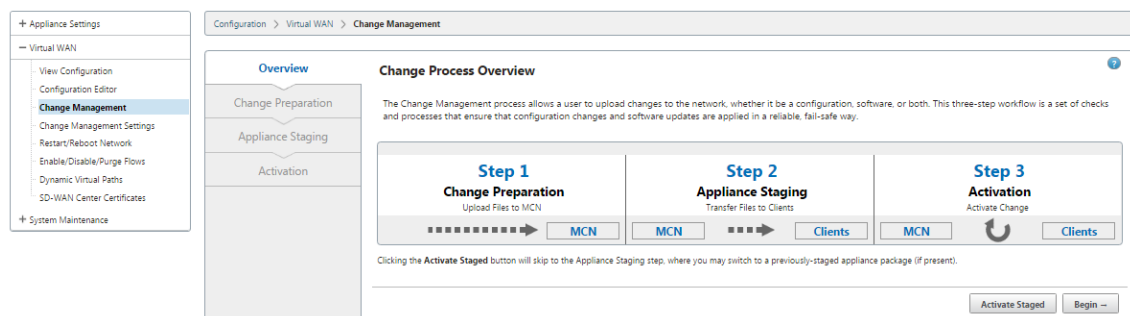
1. Connectez-vous à l'interface Web de gestion sur l'appliance MCN.

Remarque

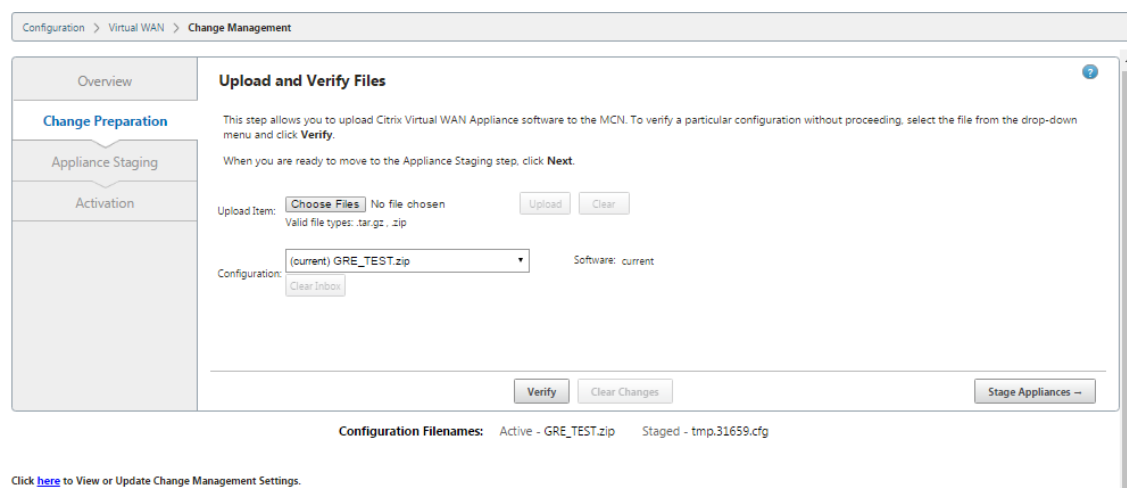
Vous téléchargez les packages logiciels que vous avez précédemment téléchargés sur le PC

connecté. Pour plus de commodité, vous pouvez utiliser ce même PC pour vous connecter à nouveau au MCN.

- Sélectionnez l'onglet **Configuration**.
- Dans le volet gauche, ouvrez la section **Virtual WAN** et sélectionnez **Gestion des modifications**. La première page de l'Assistant **Gestion des modifications**, la page **Vue d'ensemble du processus de modification** s'affiche.

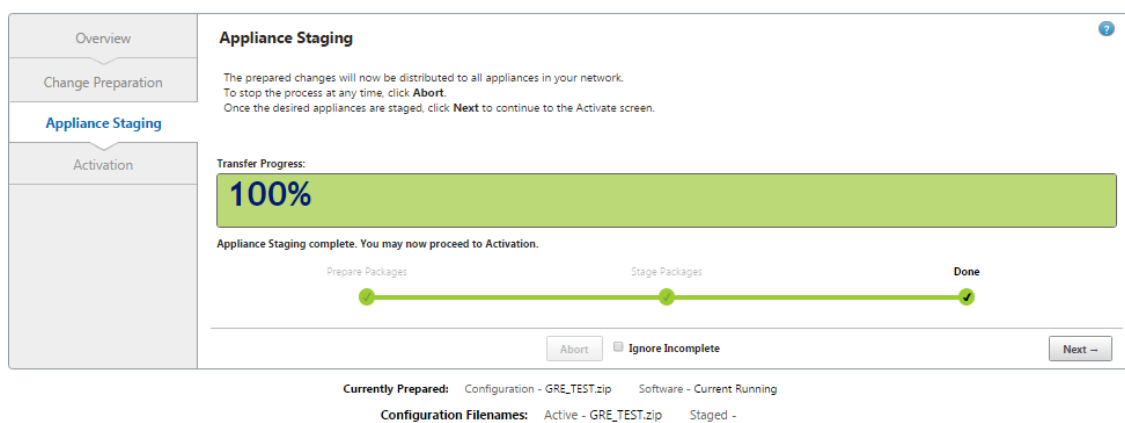


- Cliquez sur **Commencer**. Page **Préparation des modifications** pour le téléchargement et la vérification de l'affichage de la configuration et des packages logiciels spécifiés.



- Téléchargez chacun des progiciels SD-WAN requis pour votre réseau.
Pour chaque package logiciel SD-WAN que vous souhaitez déployer, procédez comme suit :
 - Cliquez sur **Choisir un fichier en regard du champ** Charger l'élément. Cela ouvre un navigateur de fichiers permettant de sélectionner un package logiciel SD-WAN à télécharger.
 - Sélectionnez un package logiciel SD-WAN, puis cliquez sur **OK**.
 - Accédez aux packages logiciels SD-WAN que vous avez téléchargés précédemment sur le PC local et sélectionnez le package à télécharger.
 - Cliquez sur **Charger**.

- e) Répétez les étapes (i) à (iii) pour chacun des progiciels SD-WAN requis pour votre réseau.
6. Dans le menu déroulant Champ **Configuration**, sélectionnez le nouveau package de configuration que vous venez d'exporter vers **Gestion des modifications**.
 7. Cliquez sur **Préparer déploiement de l'appliance**. le déploiement de l'appliance lance les actions suivantes :
 - Transfère le package logiciel sélectionné et la configuration au MCN.
 - Génère un package d'appliance pour chaque modèle d'appliance identifié dans la configuration sélectionnée.
 - Ajoute les nouveaux packages d'appliance à la liste des packages disponibles dans la table Site-Appliance.
 - Étapes la nouvelle configuration et le progiciel approprié sur le MCN.
 8. Cliquez sur **Suivant**. Cela passe à la page **Phase intermédiaire de l'appliance**.



Lorsque l'opération de transfert est terminée, la table Site-Appliance** est renseignée avec les informations sur les packages d'appliance nouvellement préparés pour déploiement.

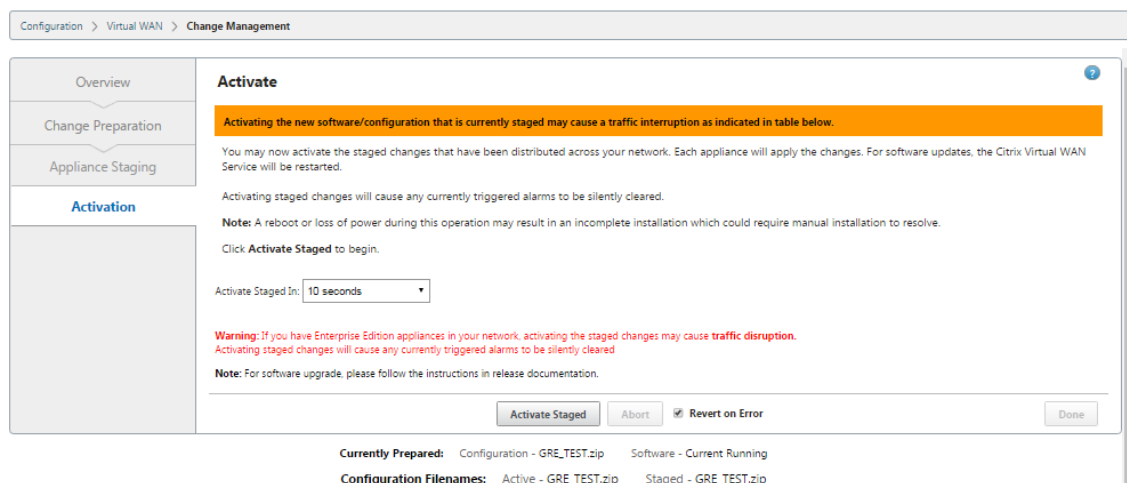
Remarque

S'il s'agit d'un déploiement initial, seul le MCN est mis à jour et préparé en vue d'être déployé maintenant. Si vous mettez à jour un déploiement existant et que les chemins d'accès virtuels fonctionnent déjà entre les sites déployés, cela distribue également les packages d'appliance appropriés aux nœuds clients déployés et lance le transfert sur ces nœuds. Toutefois, si vous ajoutez de nouveaux nœuds clients à un déploiement Virtual WAN existant, vous devez tout de même charger manuellement, préparer le déploiement et activer le package d'appliance approprié sur chaque nouveau client, comme indiqué dans les étapes restantes de cette procédure.

Si le site est affiché comme **non connecté** dans la page de gestion des modifications, il est

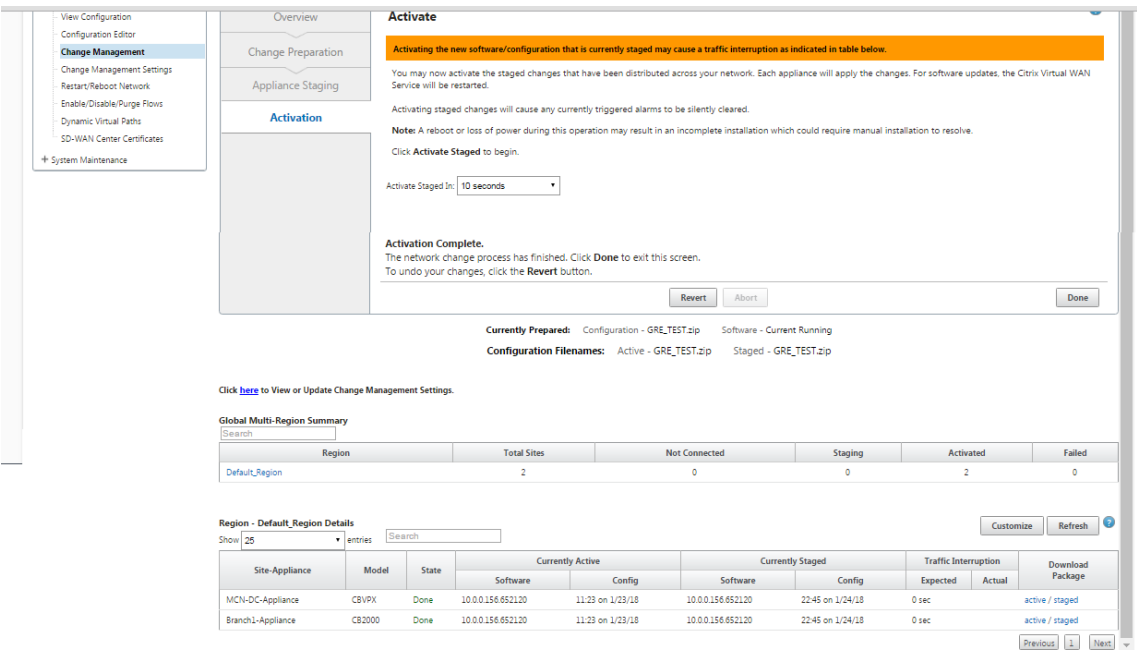
marqué comme ayant échoué pendant le processus de transit et la barre de progression est terminée à 100 %. Une fois que le site **non connecté** est de retour en ligne et connecté, MCN le corrige automatiquement.

9. Sélectionnez **Rétablir en cas d'erreur** pour revenir au package d'application précédent en cas d'erreur. Pour plus d'informations, voir Restauration de la configuration.
10. Cliquez sur **Activer le déploiement**.



Les résultats et les étapes suivantes diffèrent à ce stade, selon qu'il s'agit d'une configuration initiale ou que vous mettez à jour ou remplacez une configuration existante, comme suit :

- Si vous mettez à jour ou modifiez la configuration sur un déploiement existant.
 - S'il ne s'agit pas d'une configuration initiale, la nouvelle configuration et le package de matériel approprié sur l'appliance MCN sont activés. Le package de matériel approprié est ensuite distribué et activé automatiquement sur chaque client de votre SD-WAN. Cette opération peut prendre plusieurs secondes.

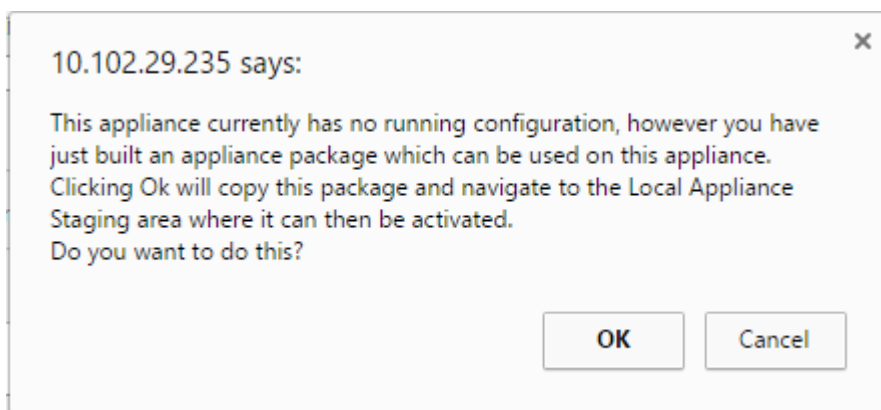


Une fois l'activation terminée, un message d'état **Activation terminée** s'affiche et le bouton **Terminé** est activé. En outre, la ligne d'état des **noms de fichiers de configuration** (au-dessus du tableau) affiche désormais le nom du package nouvellement activé dans le champ **Actif**.

11. Cliquez sur ****Terminé** et passez à l'une des options suivantes :
- Si vous n'ajoutez pas de nouveaux nœuds à votre SD-WAN, la préparation, la distribution et l'activation des nouveaux packages d'appliance dans votre SD-WAN est terminée. Vous pouvez procéder directement à [Activation du service WAN virtuel](#).
 - Si vous souhaitez ajouter de nouveaux nœuds client à votre SD-WAN, passez à [Connexion des appliances client à votre réseau](#).
 - Si vous activez une configuration initiale, le nouveau package de configuration n'est pas activé à ce stade, et il y a d'autres étapes que vous devez effectuer. L'étape suivante consiste à copier le package de configuration dans la zone de transit de l'appliance locale, en préparation du transfert et de l'activation du package de configuration sur le MCN.

Procédez comme suit :

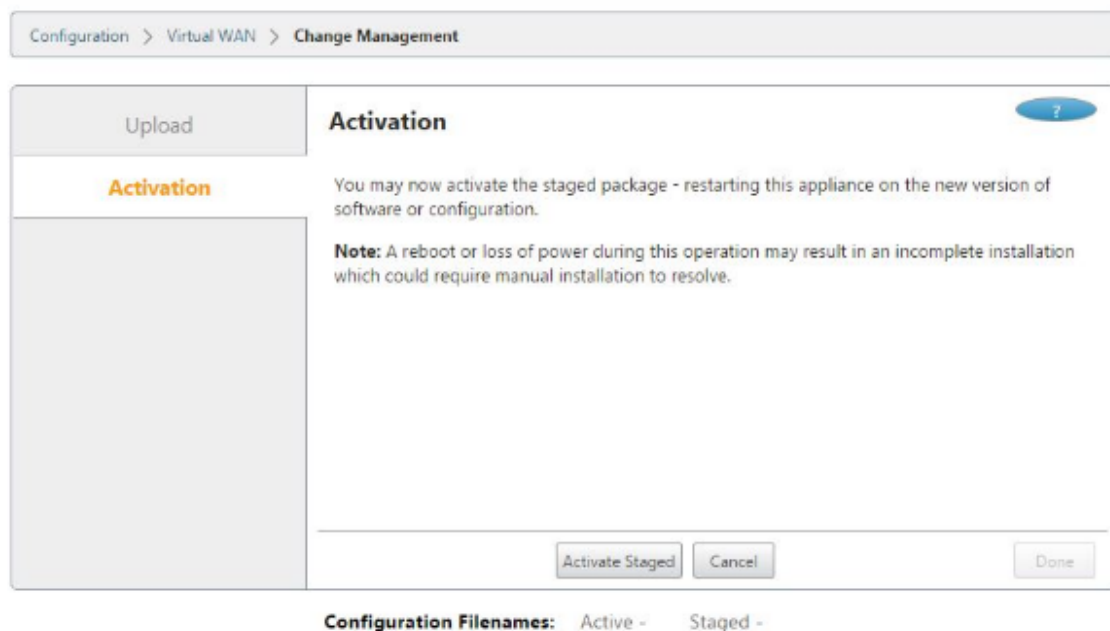
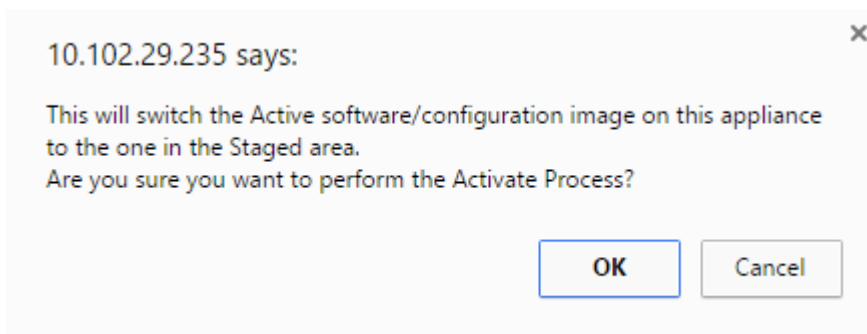
12. Une fois que vous cliquez sur **Activer préparation du déploiement**, le message suivant s'affiche.



13. Cliquez sur **OK**.

14. Cliquez sur **Activer préparation du déploiement**.

Cela affiche une boîte de dialogue vous demandant de confirmer l'opération d'activation.



15. Cliquez sur **OK**.

Cela déclenche l'activation du package de configuration de préparation du déploiement. Ce

processus prend plusieurs secondes, au cours desquelles un message d'état de progression s'affiche.

Une fois l'activation terminée, un message d'état s'affiche indiquant que l'activation est terminée, et le bouton **Terminé** est activé.

16. Cliquez sur **Terminé**. Cela passe à la page Tableau de **bord de** l'interface Web de gestion, où vous pouvez afficher les résultats d'activation.

Vous avez maintenant terminé la préparation des packages de matériel SD-WAN sur le MCN. Passez à (</en-us/citrix-sd-wan/current-release/configuration/connecting-client-appliances-to-network.html>) pour connecter les appliances client à votre réseau.

Conseil

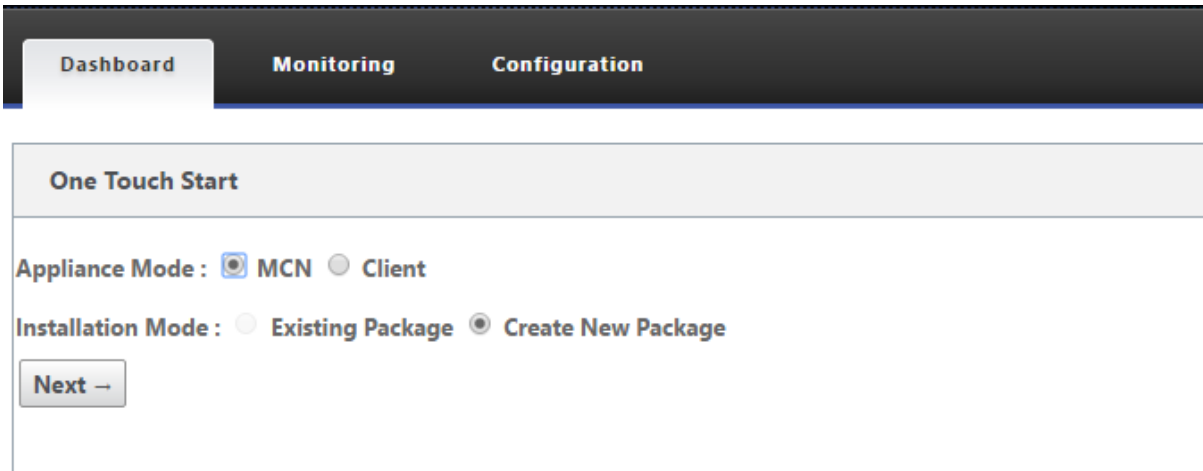
L'assistant **Gestion des modifications** vous permet de rechercher la table Site-Appliance. Cela vous permet de rechercher des sites sur un grand réseau avec plusieurs sites et de télécharger la configuration intermédiaire requise. Vous pouvez également rechercher des états d'erreur, par exemple : « Échec » ou « Non connecté ». Cela vous donne une liste de tous les sites dans cet état.

Démarrage One Touch

May 6, 2021

Le démarrage instantané vous permet de configurer facilement et rapidement votre appliance SD-WAN en tant que client lors du premier démarrage.

l'option de démarrage en une seule touche s'affiche lorsque votre appliance démarre pour la première fois.



The screenshot shows the 'One Touch Start' configuration page in the Citrix SD-WAN management interface. At the top, there is a navigation bar with three tabs: 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' tab is currently selected. Below the navigation bar, the 'One Touch Start' section is displayed. It contains two configuration options: 'Appliance Mode' with radio buttons for 'MCN' (selected) and 'Client'; and 'Installation Mode' with radio buttons for 'Existing Package' and 'Create New Package' (selected). At the bottom of this section, there is a 'Next →' button.

Remarque

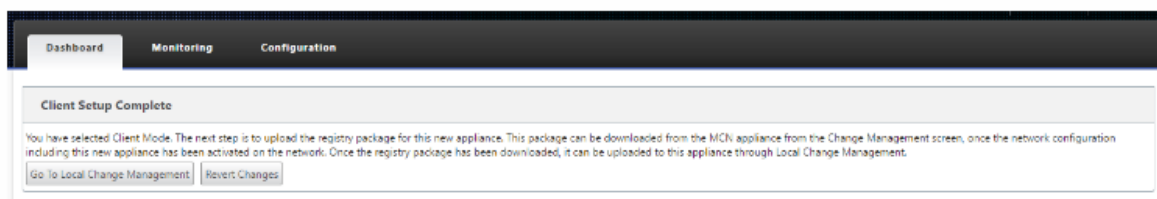
Pour configurer l'appliance SD-WAN en tant que MCN, créez une configuration ou importez une configuration existante à l'aide de l'**Éditeur de configuration**. Pour plus d'informations, [Préparation des packages d'appliance SD-WAN sur le MCN](#) consultez

Pour configurer votre appliance SD-WAN en tant que client à l'aide d'un fichier de configuration existant :

1. Sélectionnez **Client** comme mode d'appliance.
2. Sélectionnez Mode d'installation **du package existant** . L'administrateur doit enregistrer périodiquement la configuration du MCN pour utiliser un package existant du MCN.
3. Cliquez sur **Choisir un fichier** pour sélectionner le package de configuration à partir de votre ordinateur local.
4. Cliquez sur **Charger et installer**.

Pour configurer votre appliance SD-WAN en tant que client à l'aide de la gestion des modifications locales :

1. Sélectionnez **Client** comme mode d'appliance.
2. Sélectionnez **Créer un package** pour charger le package de configuration de cette appliance à l'aide de la gestion des modifications locales. Le package peut être téléchargé à partir de l'appliance MCN à partir de l'écran Gestion des modifications.
3. Cliquez sur **Suivant**.
4. Cliquez sur **Accéder à la gestion des modifications locales**.



Suivez la procédure décrite dans la rubrique [Installation des packages d'appliance SD-WAN sur les clients](#).

Connexion des appliances client à votre réseau

November 1, 2021

Pour un déploiement initial ou si vous ajoutez des nœuds clients à un SD-WAN existant, l'étape suivante consiste à permettre aux administrateurs de site de branche de connecter les appliances clientes

au réseau de leurs sites de succursales respectifs. Ceci est en préparation pour le téléchargement et l'activation des packages de matériel SD-WAN appropriés vers les clients. Connectez chaque administrateur de site de succursale pour lancer et coordonner ces procédures.

Pour connecter les appliances de site au SD-WAN, les administrateurs de site doivent effectuer les opérations suivantes :

1. Si vous ne l'avez pas encore fait, configurez les appliances clientes.

Pour chaque appliance que vous souhaitez ajouter à votre SD-WAN, procédez comme suit :

- a) Configurez le matériel matériel SD-WAN et les appliances virtuelles SD-WAN VPX (SD-WAN VPX-SE) que vous déployez.
 - b) Définissez l'adresse IP de gestion de l'appliance et vérifiez la connexion.
 - c) Définissez la date et l'heure de l'appliance. Définissez le seuil de délai d'expiration de session de console sur une valeur élevée ou maximale.
 - d) Téléchargez et installez le fichier de licence du logiciel sur l'appliance.
2. Connectez l'appliance au réseau local de la succursale. Connectez une extrémité d'un câble Ethernet à un port configuré pour le réseau local de l'appliance SD-WAN. Connectez ensuite l'autre extrémité du câble au commutateur LAN.
 3. Connectez l'appliance au WAN. Connectez une extrémité d'un câble Ethernet à un port configuré pour le WAN de l'appliance SD-WAN. Connectez ensuite l'autre extrémité du câble au routeur WAN.

L'étape suivante consiste à permettre aux administrateurs de site de succursale d'installer et d'activer le package de matériel SD-WAN approprié sur leurs clients respectifs.

Accès à la commande shell

À partir de la version 11.4.1 de SD-WAN, les utilisateurs du compte Admin peuvent exécuter la commande shell directement depuis la console de l'interface de ligne de commande SD-WAN, sans être invités à entrer les informations d'identification de connexion du compte statique CBVWSSH. Cette fonctionnalité améliore la sécurité de vos appliances SD-WAN car elle supprime le mot de passe codé en dur du compte CBVWSSH et le remplace à l'aide d'une méthode plus sécurisée. Pour exécuter la commande shell, connectez-vous à la console de l'interface de ligne de commande SD-WAN et tapez `shell`.

Remarque

- Cette fonctionnalité n'est prise en charge que pour les utilisateurs du compte Admin. Il n'est pas pris en charge par les administrateurs réseau, les administrateurs de sécurité ou les utilisateurs du compte Viewer.

- Cette fonctionnalité est destinée à des fins de dépannage uniquement. Toutes les modifications spécifiques au système effectuées via la `shell` commande sont supervisées par Citrix.

Mise à niveau

Lorsque vous mettez à niveau votre appliance SD-WAN vers la version 11.4.1, le mot de passe du compte d'administrateur par défaut est synchronisé avec le compte CBVSSH. Cette synchronisation entre le compte CBVSSH et le compte d'administrateur par défaut a lieu chaque fois que vous modifiez/mettez à jour le compte administrateur.

rétrograder

Lorsque vous rétrogradez votre appliance SD-WAN de la version 11.4.1 vers une version antérieure, vous avez la possibilité de réinitialiser le mot de passe du compte administrateur par défaut. Toutefois, le nouveau mot de passe n'est pas synchronisé avec le compte CBVSSH. Par conséquent, pour pouvoir accéder à la `shell` commande même après une mise à niveau antérieure, il est obligatoire de mémoriser le mot de passe actuel avant de rétrograder votre appliance.

Installation des packages d'appliance SD-WAN sur les clients

May 6, 2021

Une fois que vous avez préparé les packages d'appliance et connecté le MCN, et que les administrateurs de site de succursale ont connecté leurs appliances clientes respectives au LAN et au WAN, l'étape suivante consiste à télécharger et activer le package d'appliance SD-WAN approprié sur chaque client. L'assistant Gestion des modifications vous guide tout au long de ce processus.

Pour installer et activer le logiciel et la configuration sur une appliance client, procédez comme suit

1. Sur un PC connecté, ouvrez un navigateur et connectez-vous à l'interface Web de gestion de l'appliance MCN.

Entrez l'adresse IP de gestion du MCN dans le champ Adresse du navigateur. La page Tableau de **bord** de l'interface Web de gestion s'affiche pour l'appliance MCN.

2. Sélectionnez l'onglet **Configuration**. Dans le volet de navigation de gauche, sélectionnez **Virtual WAN**, puis **Gestion des modifications**.

Cette page affiche la page **Vue d'ensemble du processus de modification (première page de l'assistant Gestion des modifications)**.

DashboardMonitoringConfiguration

+ Appliance Settings

Virtual WAN

View Configuration

Configuration Editor

Change Management

Change Management Settings

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

+ System Maintenance

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Activate

Activating the new software/configuration that is currently staged may cause a traffic interruption as indicated in table below.

You may now activate the staged changes that have been distributed across your network. Each appliance will apply the changes. For software updates, the Citrix Virtual WAN Service will be restarted.

Activating staged changes will cause any currently triggered alarms to be silently cleared.

Notes: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve.

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Warning: If you have Enterprise Edition appliances in your network, activating the staged changes may cause traffic disruption. Activating staged changes will cause any currently triggered alarms to be silently cleared.

Note: For software upgrade, please follow the instructions in release documentation.

Activate StagedAbortRevert on ErrorDone

Currently Prepared: Configuration - scale_3regions_5758branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN1_k1EE.zip Software - Current Running

Configuration Filenames: Active - scale_3regions_5758branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN1_k1EE.zip Staged - scale_3regions_5758branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN1_k1EE.zip

Click [here](#) to View or Update Change Management Settings.

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	10	2	0	8	0
r1	552	4	4	547	0
r3	8	2	1	5	0
r4	Data not available				

Region - Default_Region Details

Show 25 entries

CustomizeRefresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MICN-S100-Appliance	CB5100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR572-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR573-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR574-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR575-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN1-S100-Appliance	CB5100	Transferring Region	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN1-S100-RCN1_HA-Appliance	CB5100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN3-Z100-Appliance	CB2100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN3Geo-Z100-Appliance	CB2100	Cancelled	Not Connected					Loc Chg Mgt	active / staged
RCN4-ESXL-Appliance	CBVPXL	Cancelled	Not Connected					Loc Chg Mgt	active / staged

PreviousNext

Au bas de cette page, vous pouvez voir un tableau répertoriant les sites et les appliances individuels. À l'extrême droite de la table dans la colonne **Télécharger le package**, se trouvent des liens pour les packages **Active** (si disponibles) et **Staged appliance**.

Traffic Interruption		Download Package
Expected	Actual	
0 sec		active / staged
Loc Chg Mgt		active / staged

Remarque

S'il s'agit d'une installation initiale, les liens **actifs** ne sont pas encore disponibles et sont remplacés par un marqueur de texte brut **none**.

3. Cliquez sur le lien **Staged** pour le package que vous souhaitez télécharger.
- Dans le tableau **Site-Appliance**, recherchez l'entrée de votre appliance de site, puis cliquez sur le lien **Staged** dans la colonne **Download Package** de cette entrée. Un navigateur de fichiers permettant de sélectionner l'emplacement de téléchargement (sur le PC local) s'affiche.
4. Sélectionnez l'emplacement de téléchargement et cliquez sur **OK**.

5. (Facultatif.) Une fois le téléchargement terminé, déconnectez-vous de l'interface Web de gestion MCN.
6. Ouvrez un navigateur et entrez l'adresse IP du client vers lequel vous souhaitez télécharger le fichier .zip du package d'appliance.

Remarque

Veuillez ignorer les avertissements de certificat de navigateur pour l'interface Web de gestion.

L'écran de connexion de l'interface Web de gestion Citrix SD-WAN s'ouvre sur l'appliance client.



7. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur **Connexion**. Le nom d'utilisateur Administrateur par défaut est *admin*. Le mot de passe par défaut est *mot de passe*.

La page Tableau de **bord** de l'interface Web de gestion s'affiche pour l'appliance cliente.

Dashboard

Monitoring

Configuration

System Status

Name:

MCN-5100

Model:

5100

Appliance Mode:

MCN

Serial Number:

4H30GCPD0

Management IP Address:

10.199.107.201

Appliance Uptime:

1 weeks, 4 minutes, 45.3 seconds

Service Uptime:

1 days, 1 hours, 1 minutes, 42.0 seconds

Routing Domain Enabled:

Default_RoutingDomain

Local Versions

Software Version:

10.0.0.184.657939

Built On:

Feb 13 2018 at 17:32:49

Hardware Version:

5100

OS Partition Version:

4.6

Virtual Path Service Status

Virtual Path MCN-5100-BR572:

Uptime: 1 hours, 55 minutes, 42.0 seconds.

Virtual Path MCN-5100-BR573:

Uptime: 1 hours, 55 minutes, 44.0 seconds.

Virtual Path MCN-5100-BR574:

Uptime: 1 hours, 55 minutes, 23.0 seconds.

Virtual Path MCN-5100-BR575:

Uptime: 1 hours, 55 minutes, 41.0 seconds.

Virtual Path MCN-5100-RCN1-5100:

Uptime: 21 hours, 40 minutes, 32.0 seconds.

Virtual Path MCN-5100-RCN3-5100:

Uptime: 1 hours, 54 minutes, 49.0 seconds.

Virtual Path 'MCN-5100-RCN4-ESX1' is currently dead.

Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.

Remarque

S’il s’agit d’une installation initiale ou si vous avez temporairement désactivé le service WAN virtuel sur cette appliance, vous pouvez voir une icône d’alerte d’audit en verge d’or avec un message d’état indiquant que le service WAN virtuel est inactif ou désactivé. Vous pouvez ignorer cette alerte pour le moment. L’alerte restera sur la page **Tableau de bord** jusqu’à ce que vous démarriez manuellement le service, après avoir terminé l’installation.

- 8. Sélectionnez l’onglet **Configuration**.
- 9. Ouvrez la branche Maintenance du système dans l’arborescence de navigation (volet gauche), puis sélectionnez **Gestion des modifications locales**.

La page **Chargement du processus de modification d’appliance locale** s’affiche pour le chargement d’un package d’appliance.

Dashboard

Monitoring

Configuration

+ Appliance Settings

+ Virtual WAN

System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Factory Reset

Configuration > System Maintenance > Local Change Management

Upload

Activation

Local Appliance Change Process

The Local Change Management process allows a user to upload a new appliance package to this individual appliance. This two-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied to the appliance in a reliable, fail-safe way.

Note: This process does not update any other appliances on the network. For that purpose, use the Configuration -> Virtual WAN -> Change Management screen on the MCN.

Upload Item:

Choose File

No file chosen

Valid file types: ".zip"

Upload

Next ->

Configuration Filenames:

Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip

Staged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip

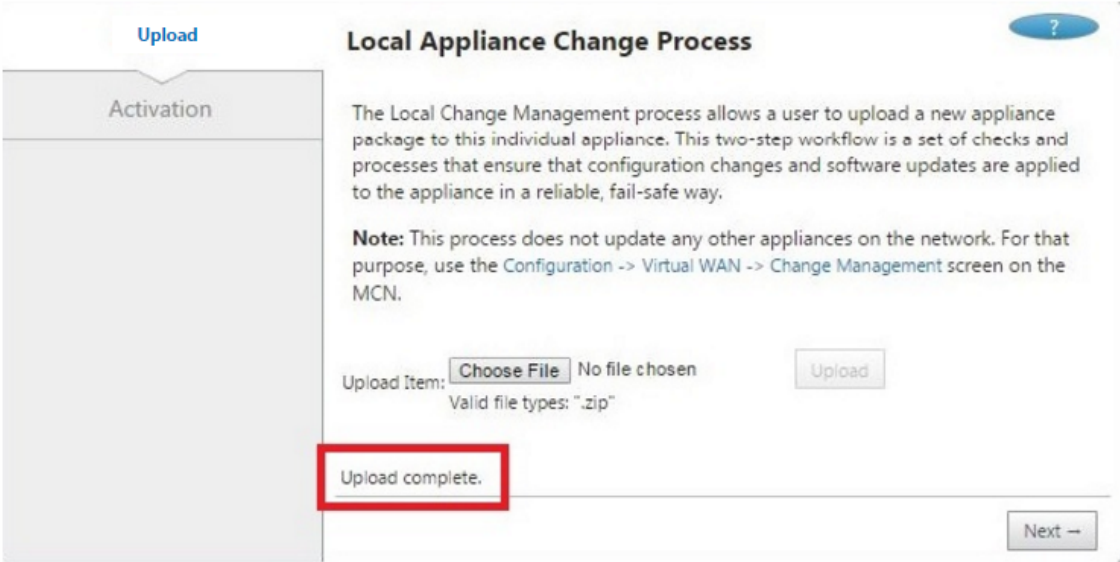
Model	Active Software	Active Config	Staged Software	Staged Config
CB5100	10.0.0.184.657939 download	13:18 on 2/14/18	10.0.0.184.657939 download	14:58 on 2/14/18

- 10. Cliquez sur **Choisir un fichier** en regard de l’étiquette **Charger l’élément**.

Cela ouvre un navigateur de fichiers permettant de sélectionner le package de matériel que vous souhaitez télécharger sur le client.

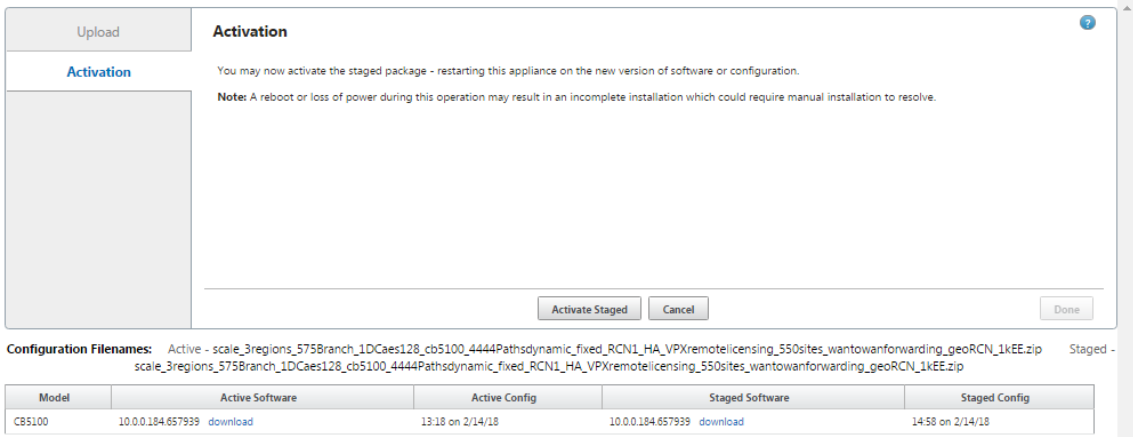
11. Accédez au fichier zip du package d'appliance SD-WAN que vous venez de télécharger à partir du MCN, sélectionnez-le et cliquez sur **OK**.
12. Cliquez sur **Upload**.

Le processus de téléchargement prend quelques secondes. Une fois terminé, un message d'état s'affiche (au milieu de la page à gauche), indiquant que le **chargement est terminé**.



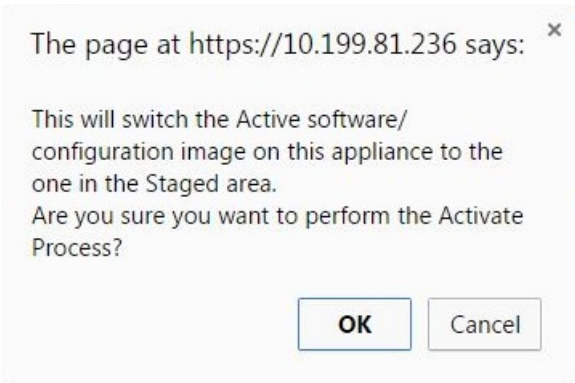
13. Cliquez sur **Suivant**.

Cette opération télécharge le package logiciel spécifié et affiche la page **Activation** de la gestion des modifications locales.



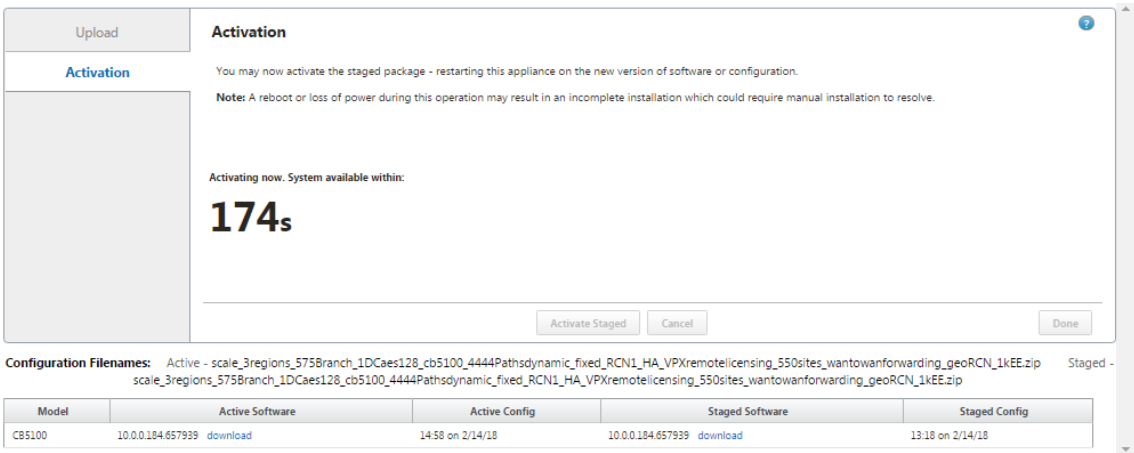
14. Cliquez sur **Activer le déploiement**.

Une boîte de dialogue vous invite à confirmer l'opération d'activation.

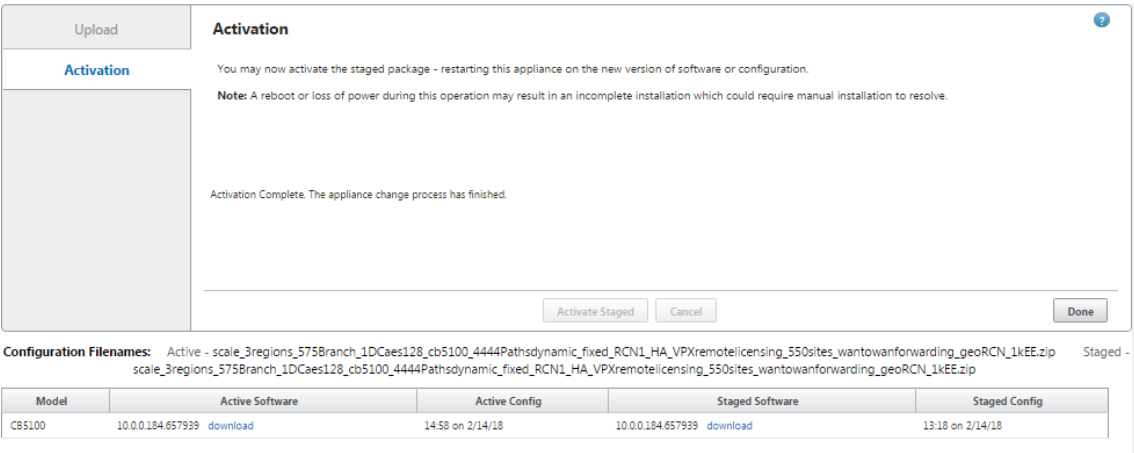


15. Cliquez sur **OK**.

Cette opération active le package nouvellement installé et, s'il ne s'agit pas d'un déploiement initial, démarre le service Virtual WAN sur l'appliance client. Ce processus prend plusieurs secondes, au cours desquelles un message d'état de progression s'affiche.



Une fois l'activation terminée, un message d'état s'affiche indiquant **Activation terminée**, et le bouton **Terminé** devient disponible.

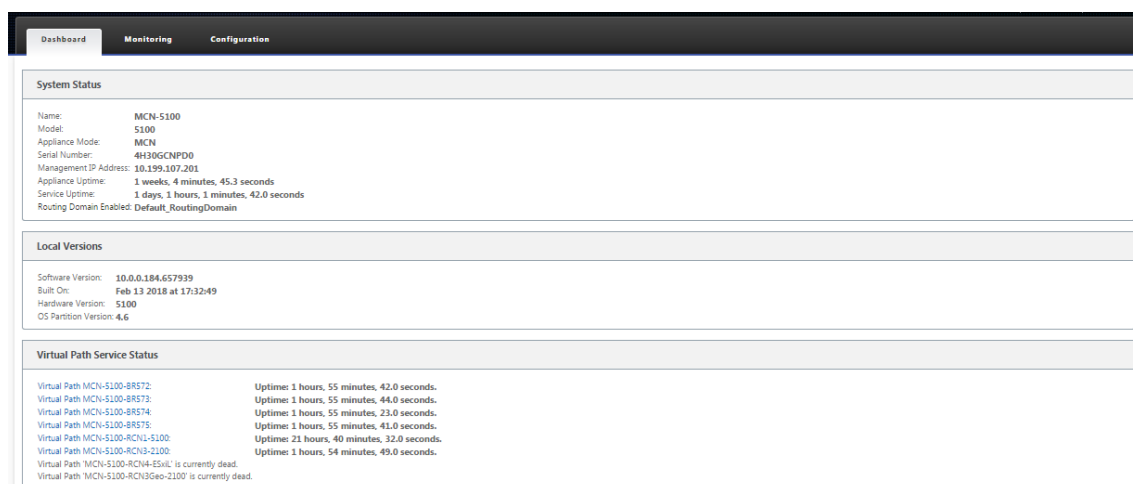


16. Cliquez sur **Terminé** pour quitter l'Assistant et afficher les résultats de l'activation.

Une fois l'activation terminée, cliquez sur **Terminé** dans la page **Activation** pour revenir à la page Tableau de **bord** de l'interface Web de gestion.

S'il ne s'agit pas d'un déploiement initial, cette page doit désormais afficher les informations mises à jour pour la version active du package logiciel, la partition du système d'exploitation et l'état du chemin d'accès virtuel. S'il s'agit d'une installation initiale, il y aura une icône d'alerte d'audit en verge d'or, ainsi qu'un message d'état indiquant que le service WAN virtuel est inactif ou désactivé. Dans ce cas, vous devez activer manuellement le service, comme décrit à la section [Activation du service WAN virtuel](#).

La figure ci-dessous montre un exemple de page de **tableau de bord** du client affichant l'icône d'alerte et le message d'état.



La dernière étape pour terminer un déploiement SD-WAN initial consiste à activer le service WAN virtuel. Les instructions sont fournies dans la section [Activation du service WAN virtuel](#).

Déployer Citrix SD-WAN Standard Edition dans OpenStack à l'aide de CloudInit

May 6, 2021

Vous pouvez désormais déployer Citrix SD-WAN Standard Edition (SE) dans un environnement Open-Stack. Pour cela, l'image Citrix SD-WAN doit prendre en charge la fonctionnalité de config-drive.

REMARQUE

Créez une image Citrix pour prendre en charge la fonctionnalité de config-drive.

La fonctionnalité ConfigDrive prend en charge la configuration de paramètres suivante pour établir la communication avec Citrix Orchestrator via le réseau de gestion :

- Adresse ipv4 de gestion
- Passerelle Mgmt.
- Name-server1
- Name-server2
- Numéro de série - Utilisé pour l'authentification et il doit être réutilisé pour la nouvelle instance. Le numéro de série transmis dans le cloud doit remplacer le numéro d'évaluation généré automatiquement dans l'instance VPX.

Remarque

- Pour réutiliser le numéro de série, un script d'initialisation est incorporé dans le SD-WAN qui s'exécute sur un OpenStack et modifie le numéro de série dans `/etc/default/family`.
- Orchestrator doit avoir un numéro de série unique avec les appliances SD-WAN pour fonctionner.

Le script Cloudinit prend en charge la contextualisation pour le déploiement SD-WAN dans OpenStack avec config-drive.

Dans le processus de contextualisation, l'infrastructure met le contexte à la disposition de la machine virtuelle et la machine virtuelle interprète le contexte. Lors de la contextualisation, la machine virtuelle peut démarrer certains services, créer des utilisateurs ou définir des paramètres de mise en réseau et de configuration.

Pour une instance SD-WAN dans OpenStack, les entrées nécessaires pour Management IP, DNS et numéro de série des utilisateurs. Le script Cloudinit analyse ces entrées et provisionne l'instance avec les informations données.

Lors du lancement d'instances dans un environnement cloud OpenStack, l'appliance Citrix SD-WAN doit prendre en charge deux technologies, données utilisateur et CloudInit, pour prendre en charge la configuration automatisée des instances au démarrage.

Procédez comme suit pour Provisioning SD-WAN SE dans un environnement OpenStack :

Conditions préalables

Accédez à **Images** et cliquez sur **Créer une image**.

Create Image

Image Details
Specify an image to upload to the Image Service.

Image Name
i

Image Description

Image Source
File
Browse...

Format

Image Requirements

Kernel
Choose an image

Ramdisk
Choose an image

Architecture

Minimum Disk (GB)
0

Minimum RAM (MB)
0

Image Sharing

Visibility
Public Private

Protected
Yes No

Cancel < Back Next > Create Image

- **Nom de l'image** - Indiquez le nom de l'image.
- **Description de l'image** —Ajoute une description de l'image.
- **Fichier** - Recherchez le fichier image kvm.qcow2 à partir de votre lecteur local et sélectionnez-le.
- **Format** : sélectionnez le format de disque QCOW2 —QEMU Emulator dans la liste déroulante.

Cliquez sur **Créer une image**.

Le port réseau et le port réseau doivent être créés initialement et prédéfinis. Pour créer un port réseau :

1. Sélectionnez **Réseaux** sous **Réseau** et accédez à l'onglet **Port**.
2. Cliquez sur **Créer un port**, fournissez les détails nécessaires, puis cliquez sur Créer.

Create Port

Info

Security Groups

Name

Mgt-port

☒ Enable Admin State

Device ID

Device Owner

Specify IP address or subnet

Fixed IP Address

Fixed IP Address

10.106.36.xx

MAC Address

☒ Port Security

VNIC Type

Normal

Description:

You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.

Cancel

Create

Si vous sélectionnez **Adresse IP fixe**, vous devez fournir l'adresse IP du sous-réseau pour le nouveau port.

Project

API Access

Compute

Volumes

Network

Network Topology

Networks

Routers

Security Groups

Floating IPs

Trunks

Object Store

Admin

Project / Network / Networks / public

public

Overview Subnets Ports

Filter

Create Port

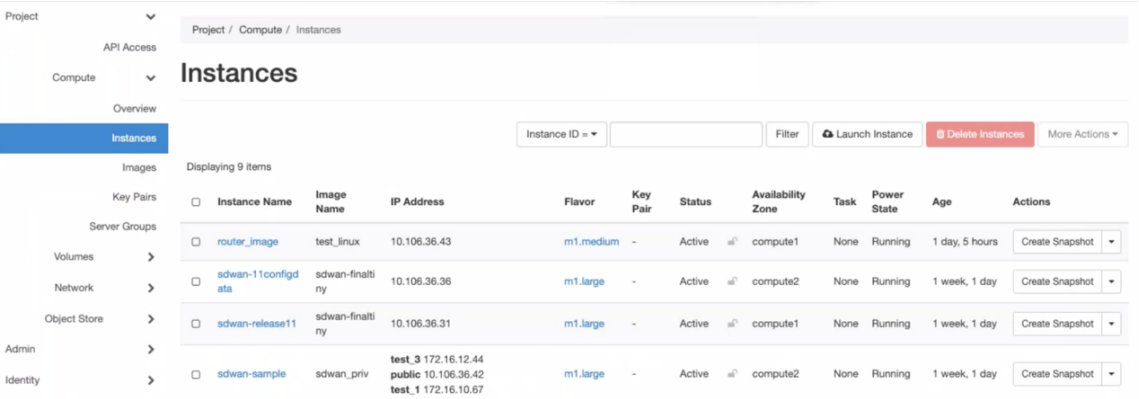
Delete Ports

Displaying 12 items

Name	Fixed IPs	MAC Address	Attached Device	Status	Admin State	Actions
Mgt-Port	10.106.36.41	fa:16:3e:24:8a:8c	Detached	Down	UP	Edit Port
(0b1273e8-1205)	10.106.36.31	fa:16:3e:c4:bc:eb	compute:compute1	Active	UP	Edit Port
test1	10.106.36.36	fa:16:3e:52:2d:8b	compute:compute2	Active	UP	Edit Port
tiny_mgmt	10.106.36.44	fa:16:3e:8d:83:04	Detached	Down	UP	Edit Port

Le port est créé et comme il n'est connecté à aucun périphérique, l'état actuel affiche Détaché. Créez une instance OpenStack pour activer le lecteur de configuration et transmettez le fichier user_data.

3. Connectez-vous à OpenStack et configurez les instances.



4. Téléchargez le fichier **kvm.qcow2.gz** et décompressez le.

5. Accédez à **Instances** et cliquez sur **Lancer l'instance**.

REMARQUE

Vous pouvez revenir à **Instances** et cliquer sur **Lancer l'instance** ou, à partir de l'écran Images, cliquer sur **Lancer** une fois l'image créée.

<input type="checkbox"/>	>	admin	sdwan-finality	Image	Active	Public	No	QCOW2	1.33 GB	<div>Launch</div>
<input type="checkbox"/>	>	admin	sdwan_mtu_check	Image	Active	Public	No	QCOW2	1.32 GB	<div>Launch</div>
<input type="checkbox"/>	>	admin	sdwan_priv	Image	Active	Public	No	QCOW2	1.29 GB	<div>Launch</div>

6. Sous l'onglet **Détails**, fournissez les informations suivantes :

- **Nom de l'instance** —Indiquez le nom d'hôte de l'instance.
- **Description** —Ajoute une description pour l'instance.
- **Zone de disponibilité** : sélectionnez la zone de disponibilité dans la liste déroulante où vous souhaitez déployer l'instance.
- **Count** : entrez le nombre d'instances. Vous pouvez augmenter le nombre pour créer plusieurs instances avec les mêmes paramètres. Cliquez sur **Suivant**.

Launch Instance

Details

Source *

Flavour *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *

sdwan-openstack

Description

Availability Zone

Any Availability Zone

Count *

1

Total Instances (30 Max)

40%

11 Current Usage

1 Added

18 Remaining

✕ Cancel

< Back

Next >

Launch Instance

7. Dans l'onglet **Source**, sélectionnez **Non** sous **Créer un nouveau volume**, puis cliquez sur **Suivant**. La source d'instance est le modèle utilisé pour créer une instance.

Launch Instance

Details

Source *

Flavour *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source

Image

Create New Volume

Yes

No

Allocated

Name	Updated	Size	Type	Visibility
Select an item from Available items below				

Available 10

Select one

Click here for filters or full text search.

Name	Updated	Size	Type	Visibility
cirros	8/7/19 9:25 PM	12.65 MB	qcow2	Public
sdwan-finaltiny	11/7/19 10:42 AM	1.33 GB	qcow2	Public
sdwan_mtu_check	8/19/19 1:34 PM	1.32 GB	qcow2	Public
sdwan_priv	11/5/19 10:34 AM	1.29 GB	qcow2	Public
SDWAN_VPX_IMG_NEW	8/8/19 8:31 PM	1.31 GB	qcow2	Public
test_branch_1	10/4/19 10:07 AM	1.72 GB	qcow2	Public
test_brnach_2	10/4/19 10:08 AM	1.72 GB	qcow2	Public
test_dynamips	10/4/19 10:06 AM	1.72 GB	qcow2	Public
test_linux	10/4/19 10:07 AM	1.72 GB	qcow2	Public
test_mcn	10/4/19 10:08 AM	1.72 GB	qcow2	Public

Cancel

Back

Next >

Launch Instance

8. Sélectionnez **Flavour** pour l'instance et cliquez sur Suivant. La version que vous sélectionnez pour une instance gère la quantité de capacité de calcul, de stockage et de mémoire de l'instance.

REMARQUE

La version que vous sélectionnez doit disposer de suffisamment de ressources allouées pour prendre en charge le type d'instance que vous essayez de créer. Les versions qui ne fournissent pas suffisamment de ressources pour votre instance sont identifiées sur le tableau disponible avec une icône d'avertissement jaune.

Les administrateurs sont responsables de la création et de la gestion des versions. Cliquez sur la flèche (à droite) pour allouer.

Launch Instance

Details

Source *

Flavour

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Flavours manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> m1.large	4	8 GB	80 GB	80 GB	0 GB	Yes	↓

▼ Available 4

Select one

Q Click here for filters or full text search.

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> m1.tiny	1	512 MB	1 GB	1 GB	0 GB	Yes	↑
> m1.small	1	2 GB	20 GB	20 GB	0 GB	Yes	↑
> m1.medium	2	4 GB	40 GB	40 GB	0 GB	Yes	↑
> m1.xlarge	8	16 GB	160 GB	160 GB	0 GB	Yes	↑

✕ Cancel

< Back

Next >

Launch Instance

9. Sélectionnez le réseau et cliquez sur **Suivant**. Les réseaux fournissent les canaux de communication pour les instances.

REMARQUE

Un administrateur est créé les réseaux du fournisseur et ces réseaux sont mappés à un réseau physique existant dans le centre de données. De même, les réseaux de projet sont créés par les utilisateurs et ces réseaux sont entièrement isolés et spécifiques au projet.

Launch Instance

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud.

▼ Allocated 1

Select networks from those listed below.

	Network	Subnets Associated	Shared	Admin State	Status	
1	public	public_subnet	Yes	Up	Active	▼

▼ Available 30

Select at least one network

Q

Click here for filters or full text search.

×

	Network	Subnets Associated	Shared	Admin State	Status	
>	08c39ca9-c86e-4e80-8dd2-5b775497069c	09408ac1-6dfb-4381-bd2b-34c128f5280c	No	Up	Active	↑
>	0ce9e8b1-ad5d-4210-87dc-62917c827c17	76268f54-7faf-45ff-ae2a-b97fb72e3d6b	No	Up	Active	↑
>	26a6e41d-6f64-4f6b-b510-810938d9a669	c81c3a0e-e84e-46b1-9e29-3300b8e7323c	No	Up	Active	↑
>	272165f0-443b-4f81-9358-38a9e2ea0fa3	373b775b-9576-484d-abd8-9011362284da	No	Up	Active	↑
>	test_4	subnet_4	No	Up	Active	↑
>	8b69e4a3-c47a-4821-bb17-09aca96a4fe9	ab3c53f6-ca4b-4958-aedf-7c444b21c257	No	Up	Active	↑
>	test_1	subnet_1	No	Up	Active	↑
>	Hw_provider3_vlan20	provider3_subnet	No	Up	Active	↑
>	f1d4edbe-8272-400c-bba1-c350864eecd	366f5024-cf0a-4648-8053-c3fe946df958	No	Up	Active	↑
>	f3158a09-c8dc-421a-9e8f-04814860b955	736e9da4-7526-4072-aa93-666071df24f8	No	Up	Active	↑
>	test_3	subnet_3	No	Up	Active	↑
>	network_ipv6	subnetwork_ipv6 ipv4_subnet	No	Up	Active	↑

✕ Cancel

< Back

Next >

Launch Instance

10. Sélectionnez un port réseau pour l'instance et cliquez sur **Suivant**. Les ports réseau fournissent des canaux de communication supplémentaires aux instances.

REMARQUE

Vous pouvez sélectionner des ports au lieu de réseaux ou une combinaison des deux.

Launch Instance

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both.

▼ Allocated 1

Select ports from those listed below.

Name	IP	Admin State	Status
tiny_mgmt	10.106.36.44 on subnet public_subnet	Up	Down

▼ Available 31

Select one

Filter

Name	IP	Admin State	Status
3865f021-d8df-40a9-964a-7bb7f3728353	192.168.234.239 on subnet	Up	Down
3f7888d2-dd2b-487d-ad88-6cf3261ebf8b	192.168.234.113 on subnet	Up	Down
7847377d-6f82-4a7f-9e8d-26703bfc7b0b	192.168.234.240 on subnet	Up	Down
2bd26300-4af2-4503-8ec8-728ad5967c5f	192.168.237.88 on subnet	Up	Down
6ca1aeab-4b38-41f3-86cc-8973a3bfc3bd	192.168.240.223 on subnet	Up	Down
9dc0d02b-7933-4689-92a3-18c3177c7c0d	192.168.240.251 on subnet	Up	Down
c378ba39-0c61-4e35-8a2c-0419fa8c2989	192.168.240.4 on subnet	Up	Down
958ad235-94b0-4ccd-8f07-88539bc5b584	172.16.22.1 on subnet	Up	Down
Mgt-Port	10.106.36.41 on subnet public_subnet	Up	Down

Cancel

Back

Next

Launch Instance

11. Accédez à **Configuration** et cliquez sur **Choisir un fichier**. Sélectionnez le `user_data` fichier. Vous pouvez afficher les informations sur l'**adresse IP de gestion**, le **DNS** et le **numéro de série** dans le fichier `user_data`.
12. Activez la case à **cocher Configuration Drive**. En activant le lecteur de configuration, vous pouvez placer les métadonnées de l'utilisateur dans l'image.

Launch Instance

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

You can customise your instance after it has launched using the options available here. "Customisation Script" is analogous to "User Data" in other systems.

Load Customisation Script from a file

No file chosen

Customisation Script (Modified) Content size: 213 bytes of 16.00 KB

```
#config
management_ip
address 10.106.36.43
netmask 255.255.255.0
gateway 10.106.36.1
dns
```

Disk Partition

Automatic

☒ **Configuration Drive**

13. Cliquez sur **Lancer l'instance**.

Configurer la fonctionnalité LTE sur l'apppliance 210 SE LTE

September 26, 2023

Vous pouvez connecter un dispositif Citrix SD-WAN 210-SE LTE à votre réseau à l'aide d'une connexion LTE. Cette rubrique fournit des détails sur la configuration des paramètres haut débit mobile, la configuration des appliances de centre de données et de succursales pour LTE, etc. Pour plus d'informations sur la plate-forme matérielle Citrix SD-WAN 210-SE LTE, consultez la section [Appliances Citrix SD-WAN 210 Standard Edition](#).

Remarque

La connectivité LTE dépend du réseau de l'opérateur SIM ou du fournisseur de services.

Démarrer avec Citrix SD-WAN 210-SE LTE

1. Insérez la carte SIM dans l'emplacement pour carte SIM du Citrix SD-WAN 210-SE LTE.

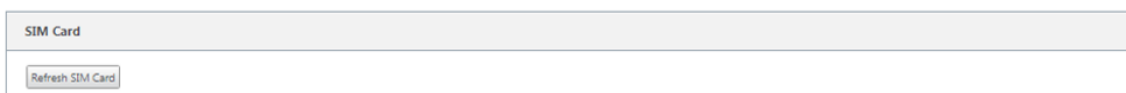
Remarque :

Seule une carte SIM standard ou 2FF (15 x 25 mm) est prise en charge.

2. Corrigez les antennes sur l'apppliance Citrix SD-WAN 210-SE LTE. Pour plus d'informations, consultez [la section Installation des antennes LTE](#).
3. Mettez l'appareil sous tension.

Remarque

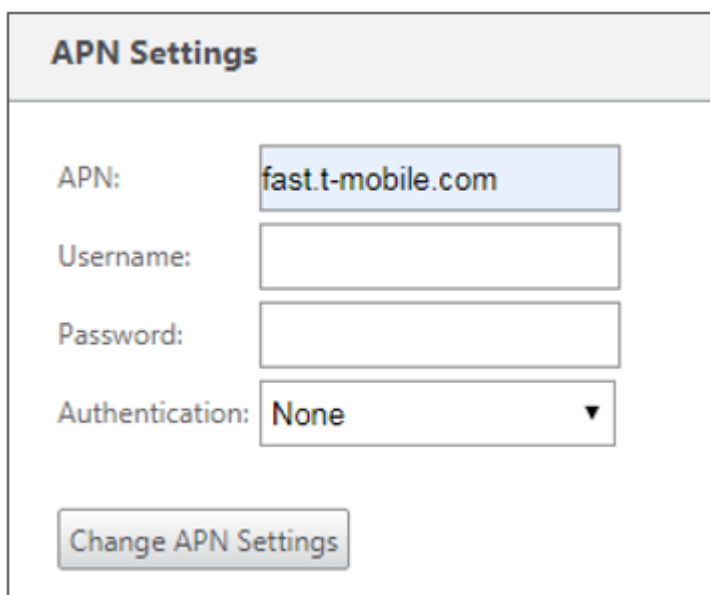
Si vous avez inséré la carte SIM dans une appliance déjà sous tension et démarrée, accédez à **Configuration > Paramètres de l'apppliance > Adaptateurs réseau > Haut débit mobile > Carte SIM**, puis cliquez sur **Actualiser la carte SIM**.



4. Configurez les paramètres APN. Dans l'interface graphique SD-WAN, accédez à **Configuration > Paramètres du matériel > Adaptateurs réseau > Haut débit mobile > Paramètres APN**.

Remarque :

obtenez les informations APN auprès du transporteur.



5. Entrez l'**APN**, le **nom d'utilisateur**, le **mot de passe** et l'**authentification** fournis par l'opérateur. Vous pouvez choisir parmi les protocoles d'authentification PAP, CHAP, PAPCHAP. Si le transporteur n'a fourni aucun type d'authentification, définissez-le sur **Aucun**.
6. Cliquez sur **Modifier les paramètres APN**.
7. Dans l'interface graphique de l'apppliance SD-WAN, accédez à **Configuration > Paramètres de l'apppliance > Adaptateurs réseau > Haut débit mobile**.

Vous pouvez afficher les informations d'état des paramètres haut débit mobile.

Status Info			Refresh
Modem	Cellular network	Network	
Type: 210-LTE-R1	Home Network: T-Mobile	IP Address/Gateway: 100.234.16.66/ 100.234.16.65	
IMEI Number: 359073060554999	Radio Interface: LTE	Primary/Secondary DNS: 10.177.0.34/ 10.177.0.210	
Status: Enabled	Signal Strength: Excellent		
Active Firmware: 02.24.05.06_GENERIC	Session State: CONNECTED		
IMEI Number: 310260186289688	APN Name: fast.t-mobile.com		
MS ISDN: 16692121835	Profile Name:		Detailed info

Voici quelques informations d'état utiles :

- **Mode de fonctionnement** : affiche l'état du modem.
- **SIM active** : à tout moment, une seule SIM peut être active. Affichage de la carte SIM actuellement active.
- **État de la carte** : Présent indique que la carte SIM est correctement insérée.
- **Force du signal** : Qualité de la force du signal - excellent, bon, juste, mauvais, ou pas de signal.
- **Réseau domestique** : Porteur de la carte SIM insérée.
- **Nom APN** : nom du point d'accès utilisé par le modem LTE.
- **État de la session** : Connected indique que le périphérique a rejoint le réseau. Si l'état de la session est déconnecté, vérifiez auprès du transporteur si le compte a été activé si le plan de données est activé.

Status Info

Refresh

Modem

Manufacturer: Sierra Wireless, Incorporated

Modem Type: 210-LTE-R1

Modem Status: Enabled

Active Firmware: 02.24.05.06_GENERIC

Model Id: EM7455

Firmware Revisions: SWI9X30C.02.24.05.06 r7040 CARMD-EV-FRMWR2 2017/05/19 06:23:09

Boot Revisions: SWI9X30C.02.24.05.06 r7040 CARMD-EV-FRMWR2 2017/05/19 06:23:09

PRI Revisions: 9907721 001.000 Generic-M2M

PRI Version: 1

PRI Preference: 0

ICCID Number: 89012601837628968847

ESN Number: 808BAD97

IMEI Number: 359073060554999

MEID Number: 359073060554999

BMSI Number: 310260186289688

MS ISDN: 16692121835

Hardware Revision: 1.0

Device State: READY

Cellular Network

Home Network: T-Mobile

Roaming Status: Home

Session State: CONNECTED

Data Bearer: GPRS

Dormancy Status: Traffic Channel Active

LU Reject Cause: 0

Card State: Ready

Call Statistics

Call Status: CONNECTED

Bytes Transferred: 317984

Bytes Received: 0

RF Information

Radio Interface: LTE

Active Band Class: 123

Active Channel: 2300

Signal Strength: Excellent

ECIO: 0

IO: 0

SINR: 0

RSRQ: -19

Profile

PDP Type: IPv4

Authentication: 0

Profile Name:

APN Name: fast.t-mobile.com

User Name:

IP Address: 100.234.16.66

Gateway Address: 100.234.16.65

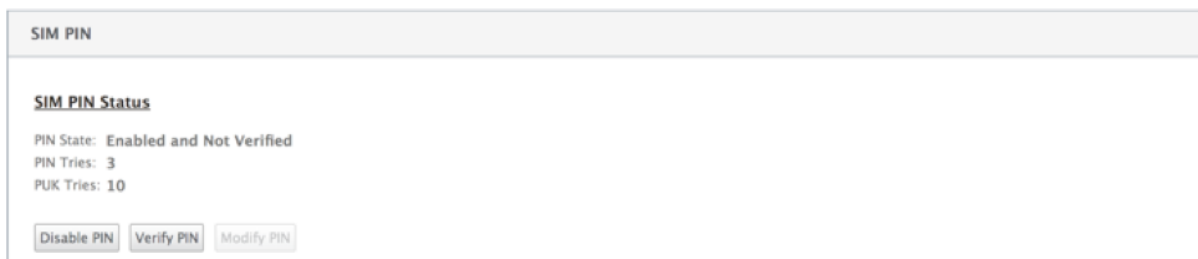
Primary DNS: 10.177.0.34

Secondary DNS: 10.177.0.210

Code PIN de la carte SIM

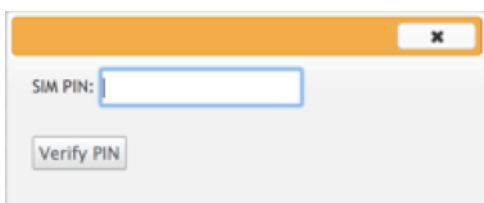
Si vous avez inséré une carte SIM verrouillée avec un code PIN, l'état de la carte SIM est **Activé et Non vérifié****. Vous ne pouvez pas utiliser la carte SIM tant qu'elle n'est pas vérifiée à l'aide du code PIN SIM. Vous pouvez obtenir le code PIN de la carte SIM auprès du transporteur.

Pour effectuer des opérations PIN de la carte SIM, accédez à **Configuration > Paramètres de l'appareil > Cartes réseau > Haut débit mobile > PIN de la carte SIM**.



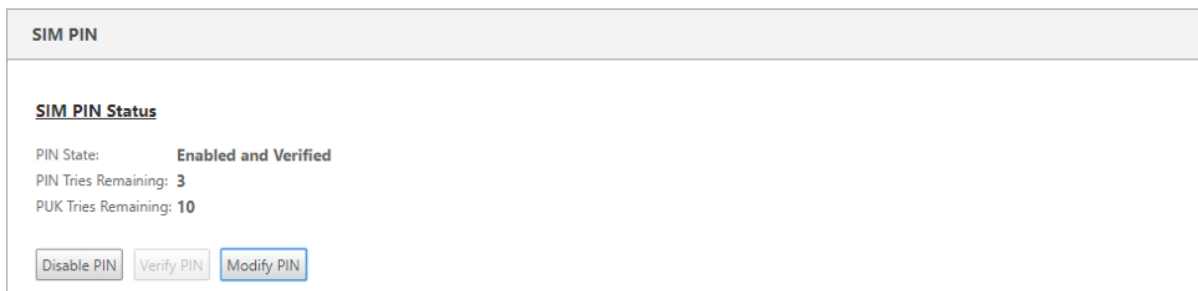
The screenshot shows the 'SIM PIN' configuration page. At the top, it says 'SIM PIN'. Below that, the 'SIM PIN Status' is displayed: 'PIN State: Enabled and Not Verified', 'PIN Tries: 3', and 'PUK Tries: 10'. At the bottom, there are three buttons: 'Disable PIN', 'Verify PIN', and 'Modify PIN'.

Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.



The screenshot shows a dialog box for verifying the PIN. It has a title bar with a close button. Inside, there is a label 'SIM PIN:' followed by a text input field. Below the input field is a 'Verify PIN' button.

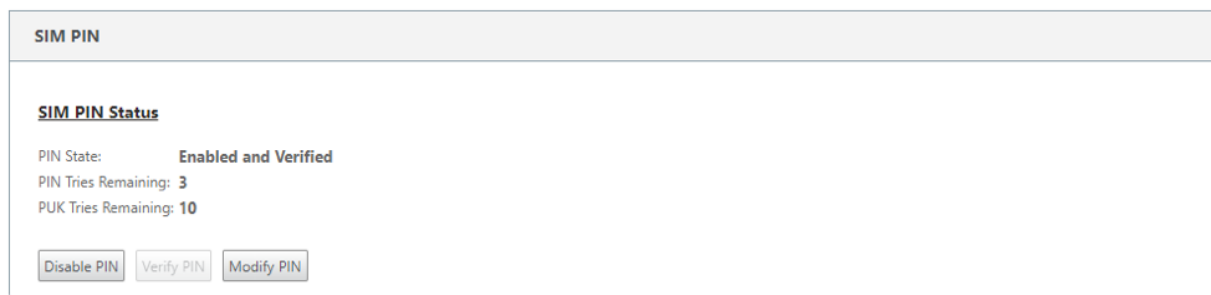
Le statut passe à **Activé et Vérifié**.



The screenshot shows the 'SIM PIN' configuration page after verification. The 'SIM PIN Status' is now: 'PIN State: Enabled and Verified', 'PIN Tries Remaining: 3', and 'PUK Tries Remaining: 10'. The buttons 'Disable PIN', 'Verify PIN', and 'Modify PIN' are still present.

Désactiver le PIN SIM

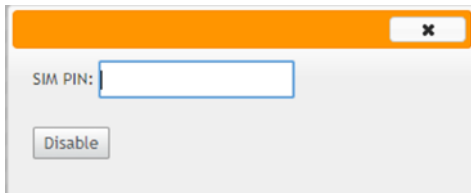
Vous pouvez choisir de désactiver la fonctionnalité PIN SIM pour une SIM pour laquelle le PIN SIM est activé et vérifié.



SIM PIN

SIM PIN Status

PIN State: **Enabled and Verified**
PIN Tries Remaining: **3**
PUK Tries Remaining: **10**

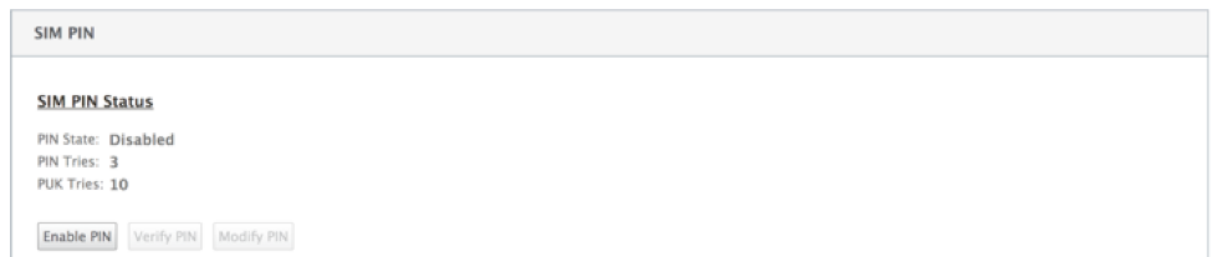


SIM PIN:

Cliquez sur **Désactiver le code PIN**. Entrez le **code PIN de la carte SIM** et cliquez sur

Activer le PIN SIM

Le code PIN SIM peut être activé pour la carte SIM pour laquelle il est désactivé.

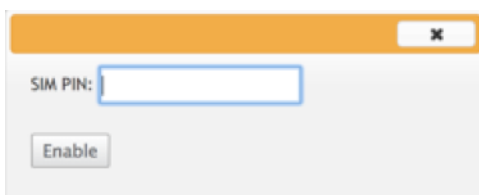


SIM PIN

SIM PIN Status

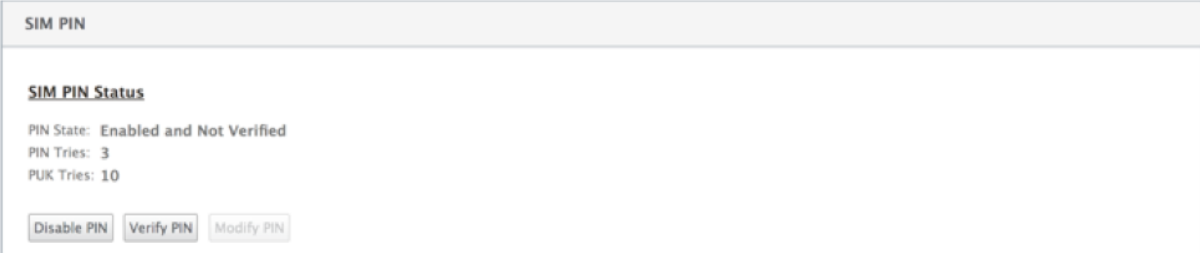
PIN State: **Disabled**
PIN Tries: **3**
PUK Tries: **10**

Cliquez sur **Activer le code PIN**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Activer**.



SIM PIN:

Si l'état du code PIN de la SIM passe à **Activé et Non vérifié**, cela signifie que le code PIN n'est pas vérifié et que vous ne pouvez pas effectuer d'opérations liées à LTE tant que le code PIN n'est pas vérifié.



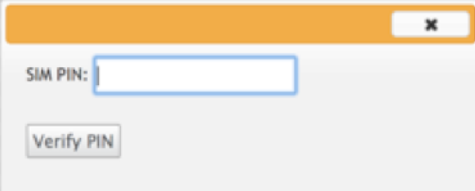
SIM PIN

SIM PIN Status

PIN State: Enabled and Not Verified
PIN Tries: 3
PUK Tries: 10

Disable PIN Verify PIN Modify PIN

Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.

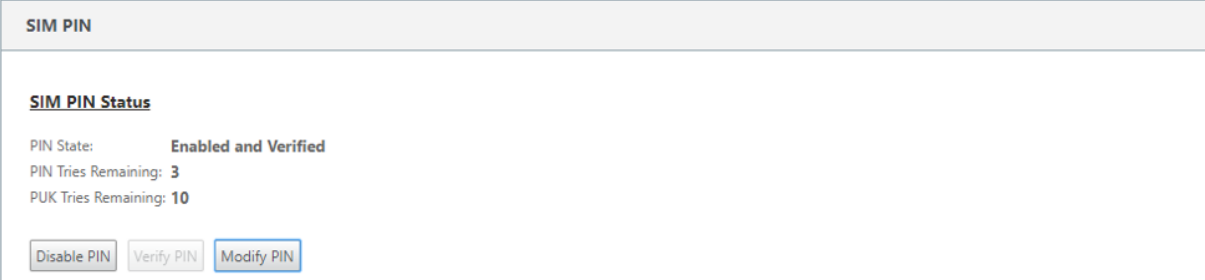


SIM PIN:

Verify PIN

Modifier le code PIN SIM

Une fois que le code PIN est **activé et vérifié**, vous pouvez choisir de le modifier.



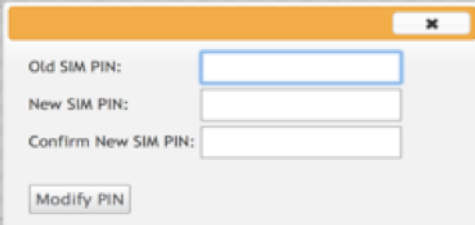
SIM PIN

SIM PIN Status

PIN State: Enabled and Verified
PIN Tries Remaining: 3
PUK Tries Remaining: 10

Disable PIN Verify PIN Modify PIN

Cliquez sur **Modifier le code PIN**. Entrez le code PIN SIM fourni par le transporteur. Entrez le nouveau code PIN SIM et confirmez-le. Cliquez sur **Modifier le code PIN**.



Old SIM PIN:

New SIM PIN:

Confirm New SIM PIN:

Modify PIN

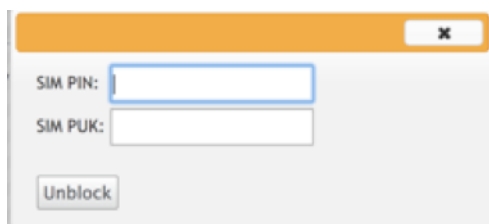
Débloquer la carte SIM

Si vous oubliez le code PIN de la carte SIM, vous pouvez réinitialiser le code PIN de la carte SIM à l'aide de la carte SIM PUK obtenue auprès du transporteur.



The screenshot shows the 'Mobile Broadband' tab selected. Under 'Status Info', a message states: 'This SIM Card is **Blocked**. Please contact the carrier service for a PUK code to unblock the SIM card.' Below this, the status is detailed: 'PIN State: Blocked', 'PIN Tries: 3', and 'PUK Tries: 10'. An 'Unblock' button is visible at the bottom left of the status area.

Pour débloquer une carte SIM, cliquez sur **Débloquer**. Saisissez le **code PIN SIM et le PUK SIM** obtenus auprès de l'opérateur, puis cliquez sur **Débloquer**.



The dialog box has a title bar with a close button. It contains two input fields: 'SIM PIN:' and 'SIM PUK:'. Below these fields is an 'Unblock' button.

Remarque :

La carte SIM est bloquée de façon permanente avec 10 tentatives infructueuses de PUK, tout en débloquent la carte SIM. Contactez le fournisseur de services de l'opérateur pour obtenir une nouvelle carte SIM.

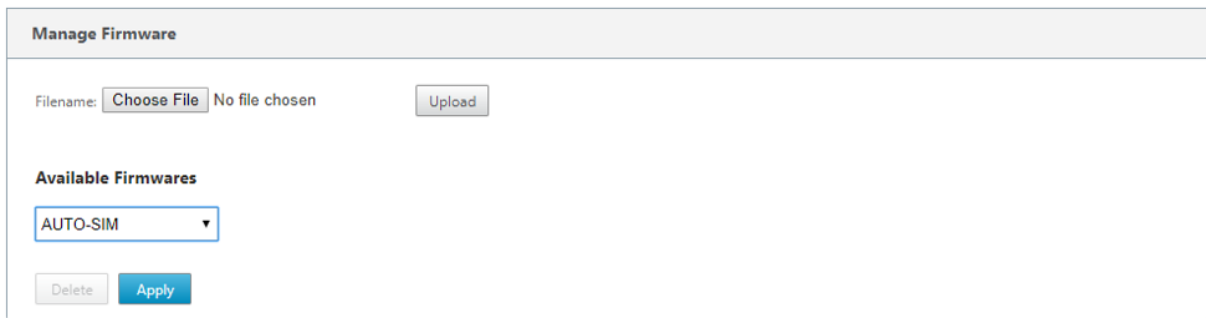


The screenshot shows the 'Configuration > Appliance Settings > Network Adapters' path. The 'Mobile Broadband' tab is selected. Under 'Status Info', a message states: 'This SIM Card is **Permanently Blocked**. Please contact the carrier service for a new SIM card.'

Gérer le firmware

Chaque appliance sur laquelle LTE est activée dispose d'un ensemble de microprogrammes disponibles. Vous pouvez sélectionner dans la liste existante du firmware ou télécharger un firmware et l'appliquer.

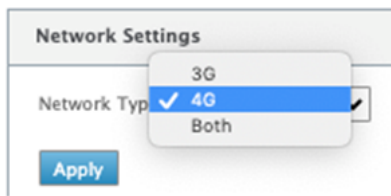
Si vous ne savez pas quel firmware utiliser, sélectionnez l'option AUTO-SIM pour permettre au modem LTE de choisir le firmware le plus adapté en fonction de la carte SIM insérée.



The 'Manage Firmware' interface includes a file upload section with a 'Filename:' label, a 'Choose File' button, the text 'No file chosen', and an 'Upload' button. Below this is the 'Available Firmwares' section, which features a dropdown menu currently set to 'AUTO-SIM'. At the bottom of this section are 'Delete' and 'Apply' buttons.

Paramètres réseau

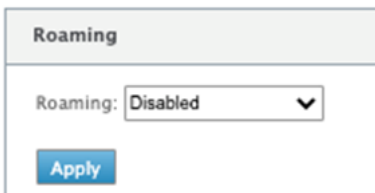
Vous pouvez sélectionner le réseau mobile sur les appliances Citrix SD-WAN qui prennent en charge les modems LTE internes. Les réseaux pris en charge sont 3G, 4G ou les deux.



The 'Network Settings' interface shows a 'Network Type' dropdown menu with a list of options: '3G', '4G' (which is selected and marked with a checkmark), and 'Both'. An 'Apply' button is located at the bottom left of the settings panel.

Itinérant

L'option d'itinérance est activée par défaut sur vos appliances LTE, vous pouvez choisir de la désactiver.



The 'Roaming' interface features a 'Roaming:' label followed by a dropdown menu set to 'Disabled'. An 'Apply' button is positioned at the bottom left.

Activer/désactiver le modem

Activez/désactivez le modem en fonction de votre intention d'utiliser la fonctionnalité LTE. Par défaut, le modem LTE est activé.

Redémarrer le modem

Redémarre le modem. La fin de l'opération de redémarrage peut prendre jusqu'à 3 à 5 minutes.

Actualiser la carte SIM

Utilisez cette option lorsque vous permutez à chaud la carte SIM pour détecter la nouvelle carte SIM par le modem 210-SE LTE.

The screenshot shows the Citrix SD-WAN web interface with the following sections:

- Manage Firmware:** Includes a 'Filename' field with a 'Choose File' button and 'No file chosen' text, an 'Upload' button, and an 'Available Firmwares' dropdown menu currently set to 'AUTO-SIM'. There are 'Delete' and 'Apply' buttons below the dropdown.
- Enable/Disable Modem:** Contains a 'Disable Mobile Broadband' button.
- Reboot Modem:** Contains a 'Reboot Modem' button.
- SIM Card:** Contains a 'Refresh SIM Card' button.

Vous pouvez afficher et gérer à distance tous les sites LTE de votre réseau à l'aide de Citrix SD-WAN Center. Pour plus d'informations, reportez-vous à la section [Gestion de sites LTE distants](#).

Configurer la fonctionnalité LTE à l'aide de la CLI

Pour configurer le modem LTE 210-SE à l'aide de l'interface de ligne de commande.

1. Connectez-vous à la console de l'apppliance Citrix SD-WAN.
2. À l'invite, tapez le nom d'utilisateur et le mot de passe pour accéder à l'interface CLI.
3. À l'invite, tapez la commande **lte**. Tapez **>help**. Affiche la liste des commandes LTE disponibles pour la configuration.

```

site210>lte
lte>help
status                # Show status
show                  # Show settings
disable               # Disable LTE modem
enable                # Enable LTE modem
apn <apn> [<user name> [<password> [<PAP|CHAP|PAPCHAP>]]] # Set APN
sim-power <off|on|reset> # Off, on, reset SIM card power
sim-pin <show>         # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin> # Modify SIM card PIN
sim-pin <unlock> <sim puk> <sim pin> # Unblock SIM card PIN
reboot                # Reboot modem
ping                  # Check if modem manager ready
list-fw               # List available firmware
apply-fw <fw>         # Apply the specified firmware

```

Le tableau suivant répertorie les descriptions des commandes **LTE**.

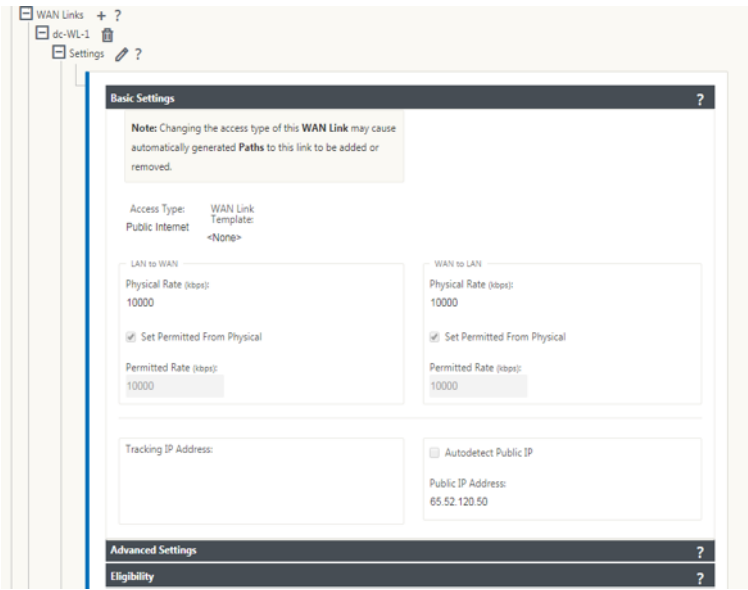
Commande	Description
Help {lte>help}	Répertorie les commandes et paramètres LTE disponibles
Status {lte>status}	Affiche l'état de la connectivité LTE
Show {lte>show}	Affiche les paramètres LTE
Disable {lte>disable}	Désactive le modem LTE
Enable {lte>enable}	Active le modem LTE
Apn {lte>apn}	Configure les informations sur les paramètres APN
Mise hors tension, marche, réinitialisation de la carte SIM > {lte>sim-power off, on, reset}	Éteint la carte SIM, allume la carte SIM, actualise la carte SIM
SIM PIN {lte>sim-pin}	Éteint la carte SIM, allume la carte SIM, actualise la carte SIM
Reboot {lte>reboot}	Redémarre le modem LTE
Ping {lte>ping}	Modem LTE Pings
list-fw {lte>list-fw}	Répertorie les micrologiciels disponibles sur les modems R1 ou R2 LTE
Apply-fw {lte>apply-fw}	Applique le microprogramme spécifique à un transporteur

Configurer MCN pour LTE

Vous ne pouvez pas configurer une appliance 210-LTE en tant que MCN. Toutefois, pour qu'un MCN fonctionne avec un dispositif de branche LTE, effectuez les configurations suivantes sur l'appliance MCN.

Pour configurer un MCN :

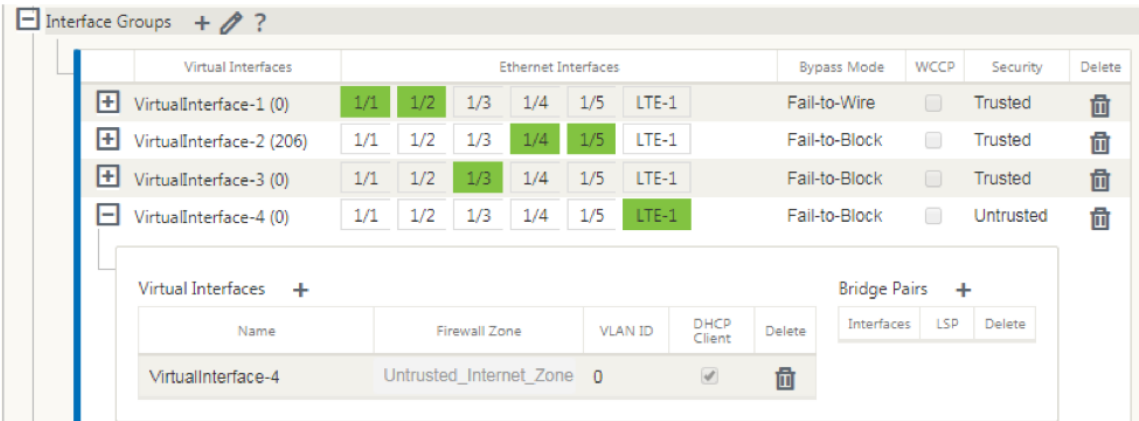
1. Connectez-vous à l'interface graphique de l'appliance SD-WAN. Accédez à l'éditeur de configuration. Configuration complète du site MCN, voir [Configurer MCN](#).
2. Assurez-vous de fournir une adresse IP publique routable dans le cadre de la configuration de la liaison WAN. Il n'est pas nécessaire de configurer une adresse IP publique pour les appliances clientes.



Configurer la branche pour LTE

Pour configurer l’appliance LTE 210-SE en tant que site de succursale, procédez comme suit :

1. Dans l’interface graphique de l’appliance SD-WAN, accédez à l’éditeur de configuration. Voir [Configurer la branche](#).
 - Créer des groupes d’interfaces.
 - Créez jusqu’à une interface virtuelle et un groupe d’interfaces pour l’adaptateur LTE afin de configurer la liaison WAN en sélectionnant les éléments suivants :
 - Interface Ethernet —LTE 1
 - Sécurité —non fiable (par défaut)
 - Client DHCP —Activé (par défaut)



2. Activez la configuration **AutoDetect Public IP** for WAN link lors de la configuration de la liaison WAN à l’aide de l’interface virtuelle créée pour l’interface LTE.

br210-WL-4

Settings

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Access Type: WAN Link

Public Internet Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

☒ Autodetect Public IP

Public IP Address:

Advanced Settings

3. Par défaut, lorsque vous essayez de configurer la liaison WAN à l'aide de l'interface LTE, la liaison WAN est marquée en tant que lien limité et en mode veille de dernier recours. Vous pouvez modifier ces paramètres par défaut, si nécessaire.

Advanced Settings

Eligibility

Metered/Standby Link

Metering

☒ Enable Metering

Data Cap (MB): 0

Billing Cycle: Monthly

Starting From: MM/DD/YYYY

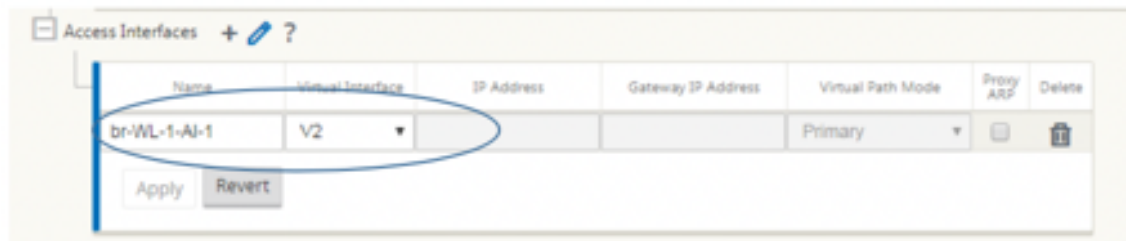
Standby

Standby Mode: Last-Resort

Priority: 1

L'adresse IP et l'adresse de Gateway de l'interface d'accès de la liaison WAN n'ont pas besoin

d'être configurées car elles reçoivent ces informations du transporteur via DHCP.



- Terminez le reste de la configuration de branche requise pour l'apppliance LTE 210-SE. Voir [Configurer Branch](#).
- Effectuez la gestion des modifications en téléchargeant le logiciel SD-WAN. Consultez la [procédure de gestion des modifications](#).
- Activez la configuration via le processus de gestion des modifications locales. Lorsque vous effectuez la gestion des modifications, la configuration est activée et la configuration requise est appliquée.

Déploiement sans contact sur LTE

Prérequis pour activer le service de déploiement zéro touche sur LTE

- Installez l'antenne et la carte SIM de l'apppliance 210-SE LTE.
- Assurez-vous que la carte SIM dispose d'un plan de données activé.
- Assurez-vous que le port de gestion n'est pas connecté.
 - Si le port de gestion est connecté, déconnectez le port de gestion, puis redémarrez l'apppliance.
 - Si une adresse IP statique sur l'interface de gestion est configurée, vous devez configurer l'interface de gestion avec DHCP, appliquer la configuration, puis déconnecter le port de gestion et redémarrer l'apppliance.
- Assurez-vous que le service Internet est défini pour l'interface LTE dans la configuration de l'apppliance 210-SE.

Lorsque l'apppliance est mise sous tension, le service de déploiement sans intervention utilise le port LTE pour obtenir la dernière configuration du logiciel SD-WAN et du SD-WAN uniquement lorsque le port de gestion n'a pas été connecté.

Vous pouvez utiliser l'interface graphique SD-WAN Center pour déployer et configurer l'apppliance LTE 210-SE pour le service de déploiement sans intervention.

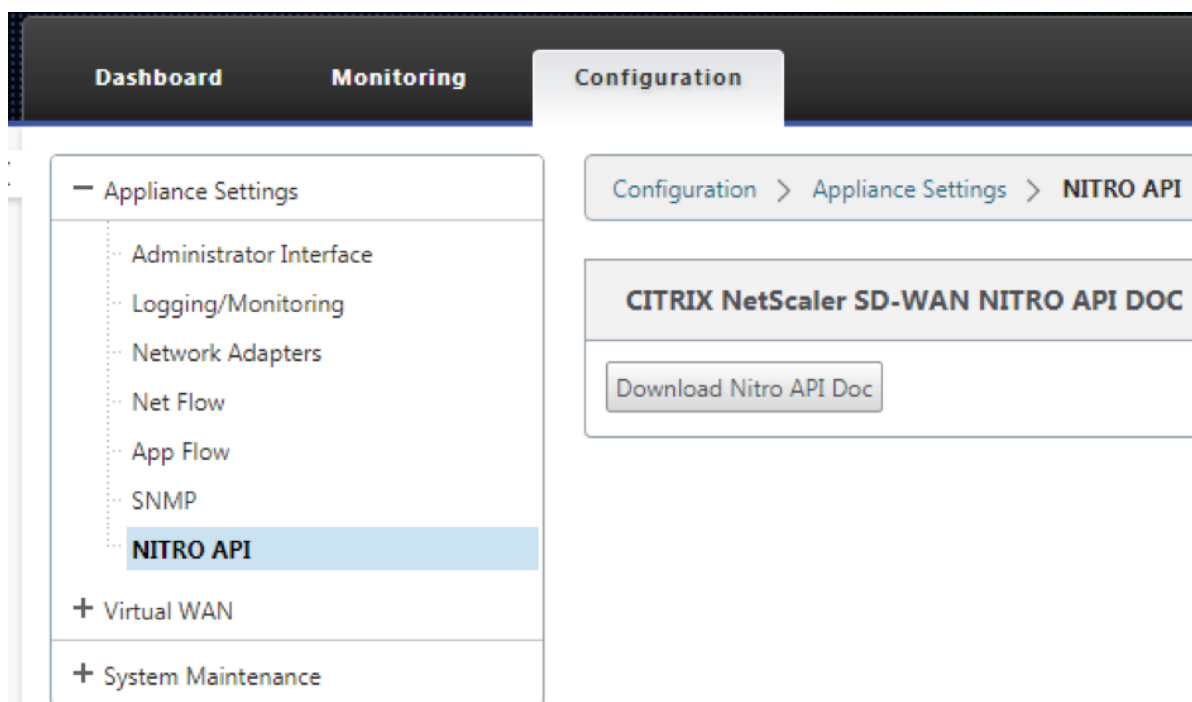
Consultez la [procédure de déploiement sans intervention](#) pour plus d'informations sur le déploiement et la configuration de l'apppliance LTE 210-SE à l'aide de SD-WAN Center.

Déploiement sans contact Service sur interface de gestion pour l'appliance 210-SE LTE

Connectez le port de gestion et utilisez la [procédure de déploiement sans intervention](#) standard prise en charge sur toutes les autres plates-formes non LTE.

API LTE REST

Pour plus d'informations sur l'API REST LTE, accédez à l'interface graphique SD-WAN et accédez à **Configuration > Appliance Settings > NITRO API**. Cliquez sur **Télécharger Nitro API Doc**. L'API REST pour la fonctionnalité PIN SIM est introduite dans Citrix SD-WAN 11.0.



Commandes AT

Les commandes AT aident à surveiller et à dépanner la configuration et l'état du modem LTE. AT est l'abréviation de **ATTension**. Comme chaque ligne de commande commence par **at**, elles sont appelées commandes AT. Les modèles de plate-forme Citrix SD-WAN qui prennent en charge la prise en charge LTE en exécutant des commandes AT. Les commandes AT sont spécifiques au modem et, par conséquent, la liste des commandes AT varie d'une plate-forme à l'autre.

Pour exécuter des commandes AT, effectuez les opérations suivantes :

1. Connectez-vous à la console de l'appliance Citrix SD-WAN.
2. À l'invite, tapez le nom d'utilisateur et le mot de passe pour accéder à l'interface CLI.
3. À l'invite, tapez **lte**.

4. Entrez **at**, puis entrez la commande AT.

Voici un exemple :

- **at at+cpin** —Fournit des informations sur l'état de la carte SIM.

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
+CPIN: READY
OK
success
```

- **at at!gstatus** - Fournit des informations sur l'état du modem LTE.

```
lte> at at!gstatus?
Running at!gstatus? command
AT command state: success
!GSTATUS:
Current Time: 1279298           Temperature: 62
Reset Counter: 1               Mode:          ONLINE
System mode:  LTE              PS state:    Attached
LTE band:     B5               LTE bw:      10 MHz
LTE Rx chan:  2559             LTE Tx chan: 20559
LTE CA state: NOT ASSIGNED
EMM state:    Registered       Normal Service
RRC state:    RRC Connected
IMS reg state: Full Srv        IMS mode:     Normal
PCC RxM RSSI: -73              RSRP (dBm): -112
PCC RxD RSSI: -73              RSRP (dBm): -107
Tx Power:     --               TAC:         1F00 (7936)
RSRQ (dB):    -17.3            Cell ID:     00798912 (7964946)
SINR (dB):    0.2
OK
Success
```

- **at at!impref?** - Fournit des informations sur le microprogramme du modem et l'opérateur réseau.

```
lte> at at!impref?
Running at!impref? command
AT command state: success
!IMPREF:
  preferred fw version:      00.00.00.00
  preferred carrier name:    AUTO-SIM
  preferred config name:     AUTO-SIM_000.000_000
  preferred subpri index:    000
  current fw version:        02.33.03.00
  current carrier name:      VERIZON
  current config name:       VERIZON_002.079_001
  current subpri index:      000
OK
success
```

Configurer la fonctionnalité LTE sur une appliance 110-LTE-WiFi

November 1, 2021

Vous pouvez connecter un dispositif Citrix SD-WAN 110-LTE-WiFi à votre réseau à l'aide d'une connexion LTE. Cette rubrique fournit des détails sur la configuration des paramètres haut débit mobile, la configuration des appliances de centre de données et de succursales pour LTE, etc. Pour plus d'informations sur la plate-forme matérielle Citrix 110-LTE-WiFi, consultez la section [Appliances Citrix SD-WAN 110 Standard Edition](#).

Remarque

La connectivité LTE dépend du réseau de l'opérateur SIM ou du fournisseur de services.

Démarrer avec Citrix SD-WAN 110-LTE-WiFi

1. Mettez l'appliance sous tension et insérez la carte SIM dans l'emplacement pour carte SIM de l'appliance Citrix SD-WAN 110-LTE-WiFi.

Remarque

L'appliance Citrix SD-WAN 110-LTE-WiFi dispose de deux emplacements SIM standard (2FF). Pour utiliser des SIM de taille Micro (3FF) et Nano (4FF), utilisez un adaptateur SIM. Accrochez la carte SIM la plus petite. Vous pouvez obtenir l'adaptateur auprès de Citrix en tant qu'unité remplaçable sur le terrain (FRU) ou auprès du fournisseur SIM.

2. Corrigez les antennes sur l'appliance Citrix SD-WAN 110-LTE-WiFi. Pour plus d'informations, consultez [la section Installation des antennes LTE](#).

3. Mettez l'appareil sous tension.
4. Configurez les paramètres APN. Dans l'interface graphique SD-WAN, accédez à **Configuration > Paramètres du matériel > Adaptateurs réseau > Haut débit mobile > Paramètres APN**.

Remarque

Obtenez les informations APN auprès du transporteur.

APN Settings

SIM:

SIM One

▼

APN:

fast.t-mobile.com

Username:

Password:

Authentication:

None

▼

Change APN Settings

5. Sélectionnez la carte SIM, saisissez l'**APN**, le **nom d'utilisateur**, le mot de **passet l'authentification** fournis par l'opérateur. Vous pouvez choisir parmi les protocoles d'authentification PAP, CHAP, PAPCHAP. Si le transporteur n'a fourni aucun type d'authentification, définissez-le sur **Aucun**.

Remarque

Tous ces champs sont facultatifs.

6. Cliquez sur **Modifier les paramètres APN**.
7. Dans l'interface graphique de l'apppliance SD-WAN, accédez à **Configuration > Paramètres de l'apppliance > Cartes réseau > Haut débit mobile**.

Vous pouvez afficher les informations d'état des paramètres haut débit mobile.

IP Address

Ethernet

Mobile Broadband

Status Info

Modem

Operating Mode: **online**

IMEI Number: **867698040397609**

Active SIM: **SIM One**

IMSI Number: **404450986042323**

ICCID Number: **8991000902637718627f**

Card State (SIM One): **present**

Cellular network

Home Network: **airtel**

Radio Interface: **lte**

Signal Strength: **Excellent**

Session State: **connected**

APN Name:

Network

IP Address/Gateway: **100.105.88.189/100.105.88.190**

Primary/Secondary DNS: **125.22.47.102/59.144.144.106**

Refresh

Detailed info

Voici quelques informations d'état utiles :

- **Mode de fonctionnement** : affiche l'état du modem.
- **SIM active** : à tout moment, une seule SIM peut être active. Affichage de la carte SIM actuellement active.
- **État de la carte** : Présent indique que la carte SIM est correctement insérée.
- **Force du signal** : Qualité de la force du signal - excellent, bon, juste, mauvais, ou pas de signal.
- **Réseau domestique** : Porteur de la carte SIM insérée.
- **Nom APN** : nom du point d'accès utilisé par le modem LTE.
- **État de la session** : Connected indique que le périphérique a rejoint le réseau. Si l'état de la session est déconnecté, vérifiez auprès du transporteur si le compte est activé et si le plan de données est activé.

Préférence SIM

Vous pouvez insérer deux SIM sur une appliance Citrix SD-WAN 110-LTE-WiFi. À un moment donné, une seule carte SIM est active. Sélectionnez la **préférence SIM** :

- **Carte SIM One préférée** : si deux cartes SIM sont insérées, au démarrage, le modem LTE utilise la carte SIM One, si disponible. Lorsque le modem LTE est en marche, il utilise la carte SIM (SIM One ou SIM Two) utilisable à ce moment. Il continue à l'utiliser jusqu'à ce que la carte SIM soit active.
- **SIM Two préféré** : si deux SIM sont insérés, au démarrage, le modem LTE utilise SIM Two, si disponible. Lorsque le modem LTE est en marche, il utilise la carte SIM (SIM One ou SIM Two) utilisable à ce moment. Il continue à l'utiliser jusqu'à ce que la carte SIM soit active.
- **SIM One** : Seul SIM One est utilisé, quel que soit l'état de la carte SIM sur les deux emplacements SIM. SIM One est toujours actif.
- **SIM Two** : Seul SIM Two est utilisé, quel que soit l'état de la carte SIM sur les deux emplacements SIM. La carte SIM Two est toujours active.

SIM Preference

Preferred SIM: SIM One preferred ▼

Apply

Code PIN de la carte SIM

Si vous avez inséré une carte SIM verrouillée avec un code PIN, l'état SIM est **activé, non vérifié**. Vous ne pouvez pas utiliser la carte SIM tant qu'elle n'est pas vérifiée à l'aide du code PIN SIM. Vous pouvez obtenir le code PIN de la carte SIM auprès du transporteur.

Remarque

Les opérations de code PIN de la carte SIM sont applicables uniquement pour la carte SIM active.

Pour effectuer des opérations PIN de la carte SIM, accédez à **Configuration > Paramètres de l'appliance > Cartes réseau > Haut débit mobile > PIN de la carte SIM**.

The screenshot shows the 'SIM PIN' configuration page. At the top, there's a header 'SIM PIN'. Below it, the 'SIM PIN Status' section displays the following information: 'PIN State: enabled-not-verified', 'PIN Retries Remaining: 3', and 'PUK Retries Remaining: 10'. At the bottom of this section, there are four buttons: 'Disable PIN', 'Verify PIN', 'Modify PIN', and 'Unblock'.

Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.

The screenshot shows a small dialog box with an orange header bar and a close button (X). Inside the dialog, there is a label 'SIM PIN:' followed by a text input field. Below the input field is a button labeled 'Verify PIN'.

L'état devient **activé vérifié**.

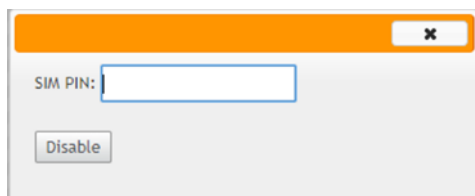
This screenshot is identical to the one above, but the 'PIN State' now shows 'enabled-verified' instead of 'enabled-not-verified'.

Désactiver le PIN SIM

Vous pouvez choisir de désactiver la fonctionnalité PIN SIM pour une SIM pour laquelle le PIN SIM est activé et vérifié.

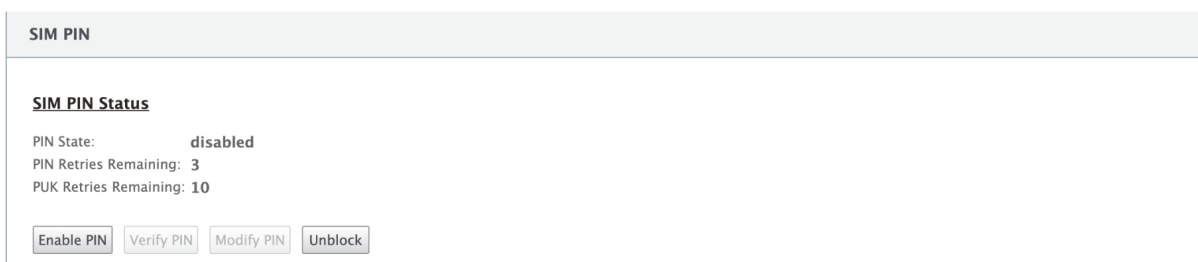
This screenshot is identical to the one above, showing the 'SIM PIN' configuration page with the status 'enabled-verified'.

Cliquez sur **Désactiver le code PIN**. Entrez le **code PIN de la carte SIM** et cliquez sur

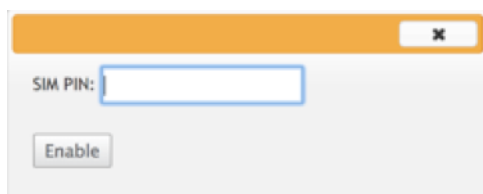


Activer le PIN SIM

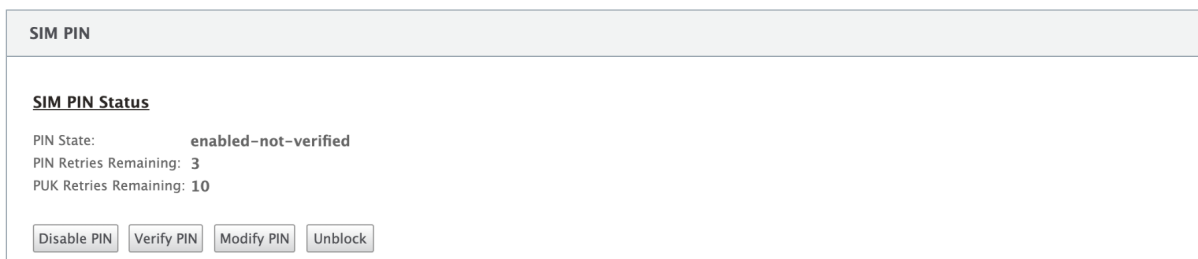
Le code PIN SIM peut être activé pour la carte SIM pour laquelle il est désactivé.



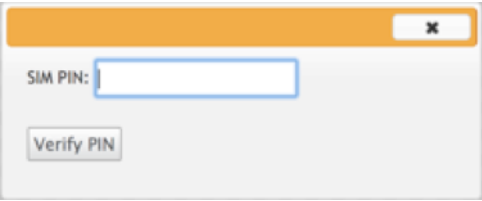
Cliquez sur **Activer le code PIN**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Activer**.



Si l'état du code PIN de la carte SIM devient **activé non vérifié**, cela signifie que le code PIN n'est pas vérifié et que vous ne pouvez pas effectuer d'opérations liées à LTE tant que le code PIN n'est pas vérifié.

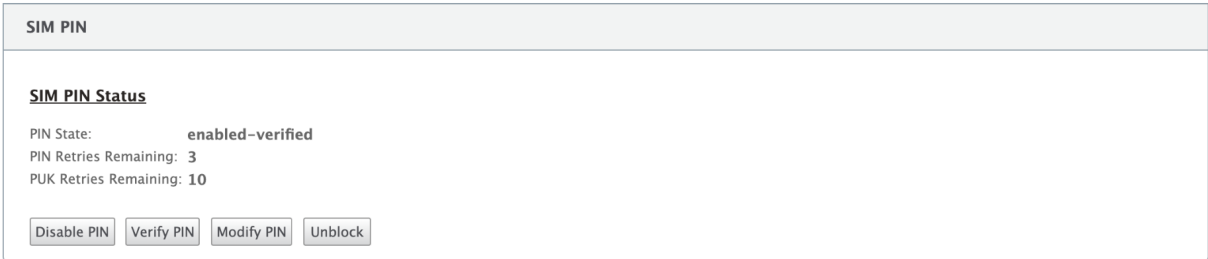


Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.

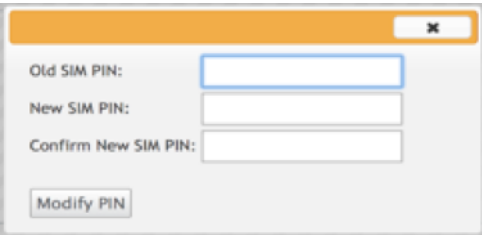
A small dialog box with an orange header bar containing a close button (X). The main area is light gray and contains the text "SIM PIN:" followed by a text input field. Below the input field is a button labeled "Verify PIN".

Modifier le code PIN SIM

Une fois que le code PIN est à l'état **validé activé**, vous pouvez choisir de modifier le code PIN.

A panel titled "SIM PIN" with a light gray header. Below the header, the text "SIM PIN Status" is underlined. The status information shows: "PIN State: enabled-verified", "PIN Retries Remaining: 3", and "PUK Retries Remaining: 10". At the bottom, there are four buttons: "Disable PIN", "Verify PIN", "Modify PIN", and "Unblock".

Cliquez sur **Modifier le code PIN**. Entrez le code PIN SIM fourni par le transporteur. Entrez le nouveau code PIN SIM et confirmez-le. Cliquez sur **Modifier le code PIN**.

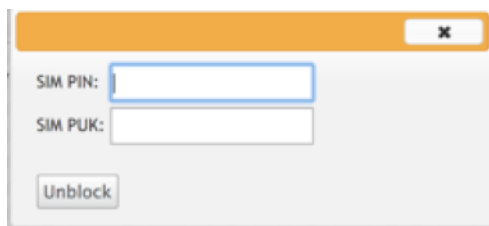
A dialog box with an orange header bar and a close button (X). It contains three text input fields labeled "Old SIM PIN:", "New SIM PIN:", and "Confirm New SIM PIN:". Below the input fields is a button labeled "Modify PIN".

Débloquer la carte SIM

Si vous oubliez le code PIN de la carte SIM, vous pouvez réinitialiser le code PIN de la carte SIM à l'aide de la carte SIM PUK obtenue auprès du transporteur.

A panel with tabs at the top: "IP Address", "Ethernet", and "Mobile Broadband". The "Mobile Broadband" tab is selected. The panel is titled "Status Info". The status message reads: "This SIM Card is Blocked. Please contact the carrier service for a PUK code to unblock the SIM card." Below this, the status information shows: "PIN State: Blocked", "PIN Tries: 3", and "PUK Tries: 10". At the bottom, there is a button labeled "Unblock".

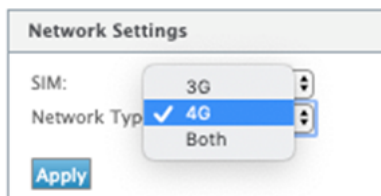
Pour débloquer une carte SIM, cliquez sur **Débloquer**. Entrez le **code PIN SIM** de votre choix. Entrez le **PUK SIM** obtenu auprès du transporteur et cliquez sur **Débloquer**.

A dialog box with an orange header bar and a close button (X) in the top right corner. It contains two input fields: 'SIM PIN:' and 'SIM PUK:'. Below these fields is an 'Unblock' button.**Remarque :**

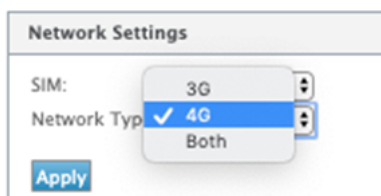
La carte SIM est bloquée de façon permanente avec 10 tentatives infructueuses de PUK, tout en débloquant la carte SIM. Vous devez contacter le fournisseur de services de l'opérateur pour obtenir une nouvelle carte SIM.

A screenshot of the 'Network Adapters' configuration page. The breadcrumb trail at the top reads 'Configuration > Appliance Settings > Network Adapters'. Below this are three tabs: 'IP Address', 'Ethernet', and 'Mobile Broadband'. The 'Mobile Broadband' tab is selected. Under the 'Status Info' section, a message states: 'This SIM Card is Permanently Blocked. Please contact the carrier service for a new SIM card.'**Paramètres réseau**

Vous pouvez sélectionner le réseau mobile sur les appliances Citrix SD-WAN qui prennent en charge les modems LTE internes. Les réseaux pris en charge sont 3G, 4G ou les deux.

A 'Network Settings' dialog box. It has a 'SIM:' label and a 'Network Type' dropdown menu. The dropdown menu is open, showing three options: '3G', '4G' (which is selected with a checkmark), and 'Both'. There is an 'Apply' button at the bottom left.**Itinérant**

L'option d'itinérance est activée par défaut sur vos appliances LTE, vous pouvez choisir de la désactiver.

A 'Network Settings' dialog box, identical to the one above, showing the 'Network Type' dropdown menu with '4G' selected.

Activer/désactiver le modem

Activer/désactiver le modem en fonction de votre intention d'utiliser la fonctionnalité LTE. Par défaut, le modem LTE est activé.

Enable/Disable Modem
<input type="button" value="Enable Mobile Broadband"/>

Redémarrer le modem

Redémarre le modem. L'opération de redémarrage peut prendre jusqu'à 7 minutes.

Actualiser la carte SIM

Utilisez cette option lorsque la carte SIM n'est pas détectée correctement par le modem 110-LTE-WiFi.

Remarque

L'opération Actualiser la carte SIM s'applique uniquement à la carte SIM active.

SIM Card (SIM One)
<input type="button" value="Refresh SIM Card"/>

Vous pouvez afficher et gérer à distance tous les sites LTE de votre réseau à l'aide de Citrix SD-WAN Center. Pour plus d'informations, reportez-vous à la section [Gestion de sites LTE distants](#).

Configurer la fonctionnalité LTE à l'aide de la CLI

Pour configurer le modem 110-LTE-WiFi à l'aide de l'interface de ligne de commande.

1. Connectez-vous à la console de l'appliance Citrix SD-WAN.
2. À l'invite, tapez le nom d'utilisateur et le mot de passe pour accéder à l'interface CLI.
3. À l'invite, tapez la commande **lte**. Tapez **>help**. Affiche la liste des commandes LTE disponibles pour la configuration.

```
lte> help
Usage
  ?|help                # Print this message
  status [default|verbose] # Show status
  show                  # Show configuration
  select [1|2] [1|2]    # Show or choose modem and/or sim to work
  enable                # Enable the selected modem
  disable                # Disable the selected modem
  apn <apn> [<username> [<password> [<NONE|PAP|CHAP|PAPCHAP>]]] # Set APN
  sim-prefer <prefer|use> <1|2> # Prefer to use or use SIM one or two
  sim-power <show|off|on|reset> # Show, off, on, reset SIM card power
  sim-pin <show>         # SIM card pin status
  sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
  sim-pin <modify> <old pin> <new pin> # Modify SIM card PIN
  sim-pin <unlock> <sim puk> <sim pin> # Unblock SIM card PIN
  reboot                # Reboot modem
  list-fw                # List available firmware
  upload-fw <fw file>   # Upload firmware file
  apply-fw <fw> [keep-AUTO-SIM] # Apply firmware
  delete-fw <fw>        # Delete firmware
  session <show|stop|start> # Show/stop/start data session
  exit|quit              # Exit LTE CLI
```

Le tableau suivant répertorie les descriptions des commandes **LTE** .

Commande	Description
Help {lte>help}	Répertorie les commandes et paramètres LTE disponibles
Status {lte>status}	Affiche l'état de la connectivité LTE
Show {lte>show}	Affiche les paramètres LTE
Disable {lte>disable}	Désactive le modem LTE
Enable {lte>enable}	Active le modem LTE
Apn {lte>apn}	Configure les informations sur les paramètres APN
Mise hors tension, marche, réinitialisation de la carte SIM > {lte>sim-power off, on, reset}	Mise hors tension de la carte SIM, mise sous tension de la carte SIM, actualisation de la carte SIM
Sélectionnez [1 2] [1 2] {lte>select [1 2] [1 2]}	Sélectionnez la carte SIM du modem LTE.
SIM-prefer {lte>sim-prefer}	Sélectionnez la carte SIM préférée ou à utiliser.
SIM PIN {lte>sim-pin}	Opérations relatives au PIN SIM
Reboot {lte>reboot}	Redémarre le modem LTE

Remarque

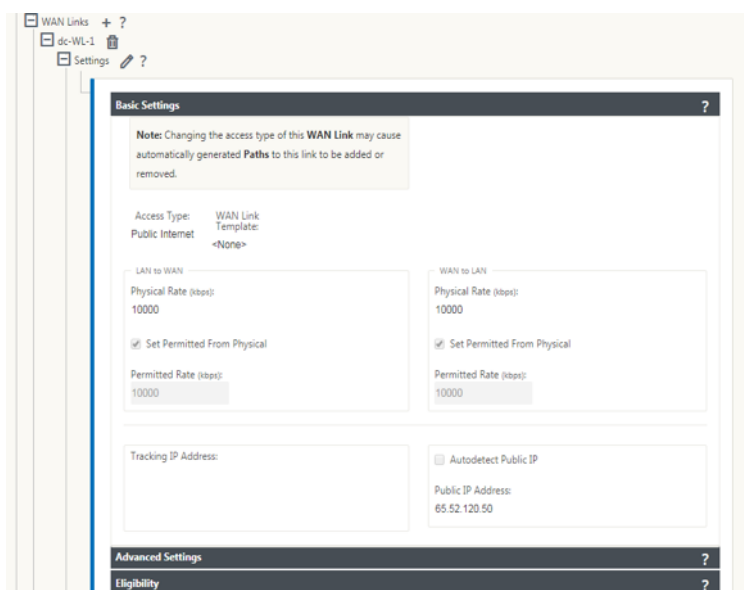
Les opérations liées au microprogramme ne sont pas prises en charge sur l'apppliance 110-LTE-WiFi.

Configurer MCN pour LTE

Vous ne pouvez pas configurer une appliance 110-LTE-WiFi en tant que MCN. Toutefois, pour qu'un MCN fonctionne avec un dispositif de branche LTE, effectuez les configurations suivantes sur l'apppliance MCN.

Pour configurer un MCN :

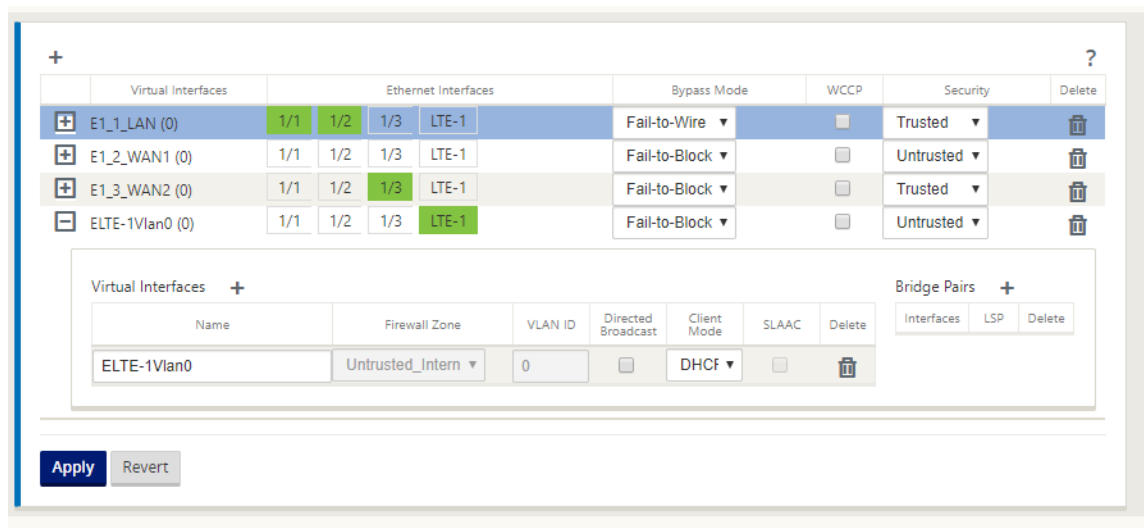
1. Connectez-vous à l'interface graphique de l'apppliance SD-WAN. Accédez à l'éditeur de configuration. Terminez la configuration du site MCN. Reportez-vous à la section [Configurer MCN](#).
2. Assurez-vous de fournir une adresse IP publique routable dans le cadre de la configuration de la liaison WAN. Il n'est pas nécessaire de configurer une adresse IP publique pour les appliances clientes.

**Configurer la branche pour LTE**

Pour configurer l'apppliance 110-LTE-WiFi en tant que site de succursale :

1. Dans l'interface graphique de l'apppliance SD-WAN, accédez à l'éditeur de configuration. Voir [Configurer la branche](#).
 - Créer des groupes d'interfaces.

- Créez jusqu'à une interface virtuelle et un groupe d'interfaces pour l'adaptateur LTE afin de configurer la liaison WAN en sélectionnant les éléments suivants :
 - Interface Ethernet —LTE 1
 - Sécurité —non fiable (par défaut)
 - Client DHCP —Activé (par défaut)



2. Activez la configuration **AutoDetect Public IP** for WAN link lors de la configuration de la liaison WAN à l'aide de l'interface virtuelle créée pour l'interface LTE.

br210-WL-4

Settings

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Access Type: WAN Link

Public Internet Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

☒ Autodetect Public IP

Public IP Address:

Advanced Settings

3. Par défaut, lorsque vous essayez de configurer la liaison WAN à l'aide de l'interface LTE, la liaison WAN est marquée en tant que lien limité et en mode veille de dernier recours. Vous pouvez modifier ces paramètres par défaut, si nécessaire.

Advanced Settings

Eligibility

Metered/Standby Link

Metering

☒ Enable Metering

Data Cap (MB): 0

Billing Cycle: Monthly

Starting From: MM/DD/YYYY

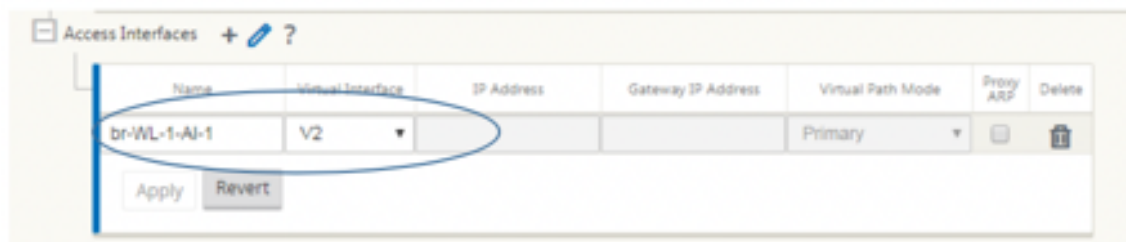
Standby

Standby Mode: Last-Resort

Priority: 1

L'adresse IP et l'adresse de Gateway de l'interface d'accès de la liaison WAN n'ont pas besoin

d'être configurées car elles reçoivent ces informations du transporteur via DHCP.



- Terminez le reste de la configuration de branche requise pour l'apppliance 110-LTE-WiFi. Voir [Configurer Branch](#).
- Effectuez la gestion des modifications en téléchargeant le logiciel SD-WAN. Consultez la [procédure de gestion des modifications](#).
- Activez la configuration via le processus de gestion des modifications locales. Lorsque vous effectuez la gestion des modifications, la configuration est activée et la configuration requise est appliquée.

Déploiement sans contact sur LTE

L'apppliance SD-WAN 110 SE prend en charge le Provisioning jour-0 et la gestion jour-n des appliances SD-WAN via les ports de gestion et de données

Conditions préalables pour activer le service de déploiement zéro touche sur LTE :

- Installez l'antenne, mettez l'appareil sous tension et insérez la carte SIM.
- Assurez-vous que la carte SIM dispose d'un plan de données activé.
- Assurez-vous que le port de gestion/données n'est pas connecté.
 - Si le port de gestion/données est connecté, déconnectez le port de gestion/données.
 - Si une adresse IP statique sur l'interface de gestion/données est configurée, vous devez configurer l'interface de gestion/données avec DHCP, appliquer la configuration, puis déconnecter le port de gestion/données.
- Assurez-vous que la configuration de l'apppliance 110-LTE-WiFi dispose du service Internet défini pour l'interface LTE.

Lorsque l'apppliance est sous tension, le service de déploiement zéro touche utilise le port LTE pour obtenir les derniers logiciels SD-WAN et la configuration SD-WAN.

Vous pouvez utiliser l'interface graphique SD-WAN Center pour déployer et configurer l'apppliance 110-LTE-WiFi pour le service de déploiement sans intervention.

Consultez la [procédure de déploiement sans intervention](#) pour plus d'informations sur le déploiement et la configuration de l'apppliance 110-LTE-WiFi à l'aide du SD-WAN Center.

Service de déploiement sans contact sur interface de gestion/données pour l'appliance 110-SE LTE

Connectez le port de gestion/de données à Internet et utilisez la [procédure de déploiement standard sans contact](#) prise en charge sur toutes les autres plates-formes non LTE.

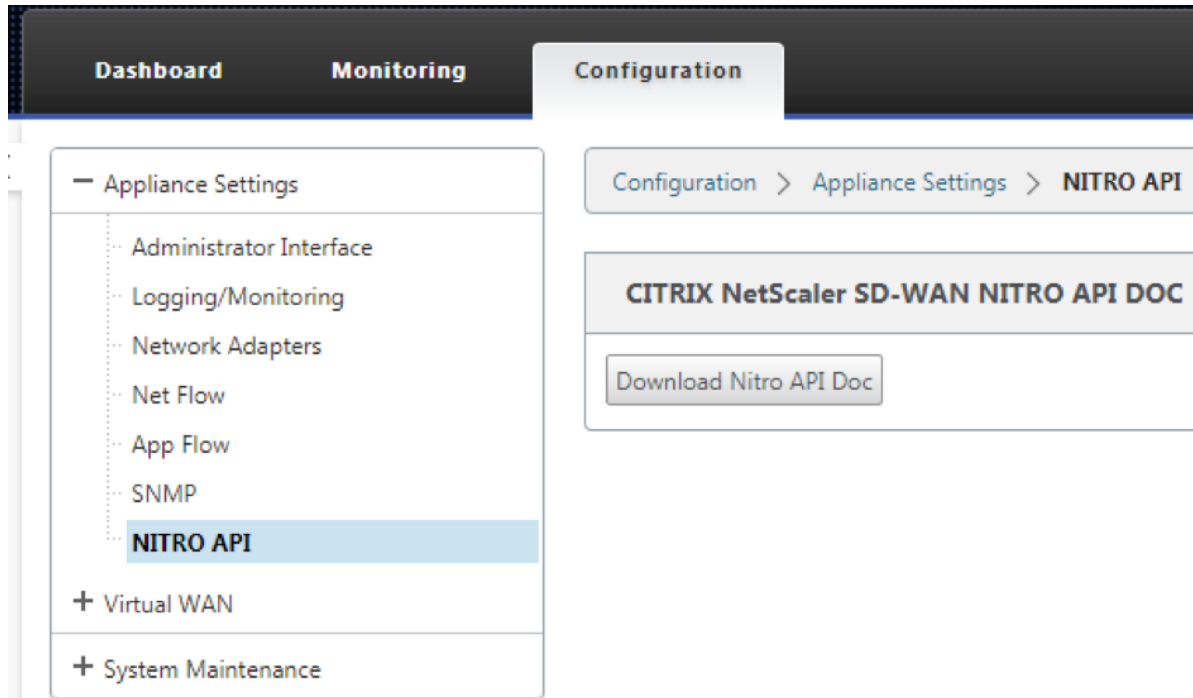
Plateformes non prises en charge

Le provisionnement Day-0 et la gestion Day-N ne sont pas pris en charge sur les appliances SD-WAN suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

API LTE REST

Pour plus d'informations sur l'API REST LTE, accédez à l'interface graphique SD-WAN et accédez à **Configuration > Appliance Settings > NITRO API**. Cliquez sur **Télécharger Nitro API Doc**. L'API REST pour la fonctionnalité PIN SIM est introduite dans Citrix SD-WAN 11.0.



Commandes AT

Les commandes AT aident à surveiller et à dépanner la configuration et l'état du modem LTE. AT est l'abréviation de **Attension**. Comme chaque ligne de commande commence par **at**, elles sont appelées commandes AT. Les modèles de plate-forme Citrix SD-WAN qui prennent en charge la prise en charge LTE en exécutant des commandes AT. Les commandes AT sont spécifiques au modem et, par conséquent, la liste des commandes AT varie d'une plate-forme à l'autre.

Pour exécuter des commandes AT, effectuez les opérations suivantes :

1. Connectez-vous à la console de l'appareil Citrix SD-WAN.
2. À l'invite, tapez le nom d'utilisateur et le mot de passe pour accéder à l'interface CLI.
3. À l'invite, tapez **lte**.
4. Entrez **at**, puis entrez la commande AT.

Voici un exemple :

- **at at+cpin** —Fournit des informations sur l'état de la carte SIM.

```
lte> at at+cpin?  
Running at+cpin? command  
AT command state: success  
+CPIN: READY  
OK  
success
```

Configurer un modem LTE USB externe

November 1, 2021

Vous pouvez connecter un modem USB 3G/4G externe sur certains appareils Citrix SD-WAN. Les appliances utilisent le réseau 3G/4G ainsi que d'autres connexions pour former un réseau virtuel qui agrège la bande passante et assure la résilience. En cas de panne de connectivité sur les autres interfaces, le trafic est automatiquement redirigé via le modem USB LTE. Les appliances suivantes prennent en charge un modem USB externe :

- Citrix SD-WAN 210 SE/AE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 Wi-Fi SE

- Citrix SD-WAN 110 LTE Wi-Fi SE
- Citrix SD-WAN 1100 SE/PE/AE
- Citrix SD-WAN 2100 SE/PE

Les appliances [Citrix SD-WAN 210 SE LTE](#) et [Citrix SD-WAN 110 LTE Wi-Fi SE](#) sont dotées d'un modem LTE intégré. Le double LTE actif est pris en charge sur ces appliances.

Les solutions matérielles-logicielles suivantes ne prennent pas en charge un modem USB externe :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

CDC Ethernet, MBIM et NCM sont les trois types de modems USB externes pris en charge. Vous pouvez configurer les paramètres **APN** et Activer/Désactiver le modem sur les modems USB MBIM et NCM. Les opérations haut débit mobiles ne sont pas prises en charge sur les modems USB CDC Ethernet.

Remarque

Les dongles LTE externes avec le type de modem en tant que MBIM ne fonctionnent pas sur la plate-forme Citrix SD-WAN 2100.

Connexion du modem USB

Activez et testez le modem USB conformément aux instructions fournies par votre opérateur sans fil.

Exigences pour modem LTE externe :

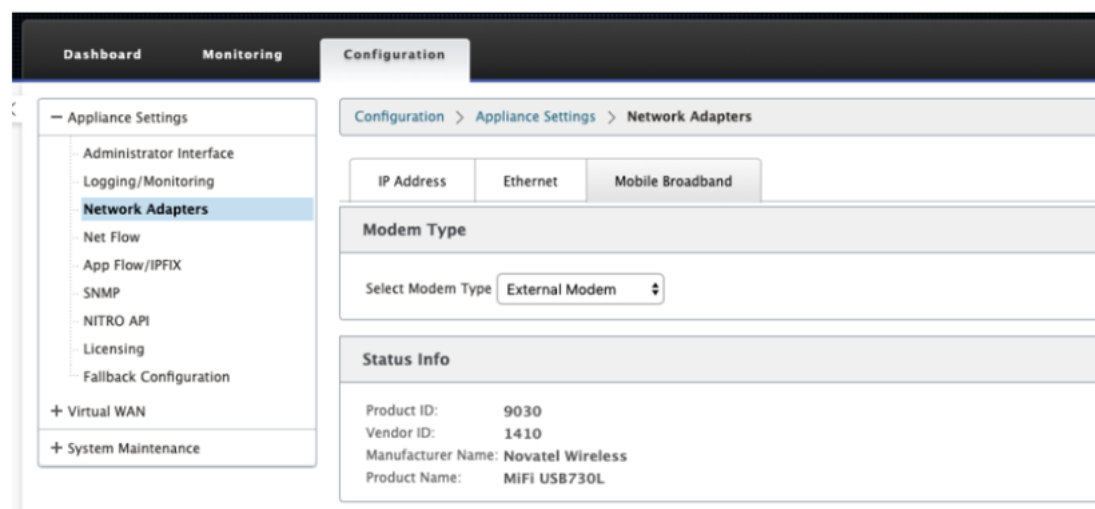
- Utilisez les dongles USB LTE pris en charge. Les modèles matériels de dongle pris en charge sont Verizon USB730L et AT&T USB800.
- Assurez-vous qu'une carte SIM est insérée dans le dongle USB LTE. Les dongles Ethernet LTE CDC sont préconfigurés avec une adresse IP statique, cela interfère avec la configuration et provoque une défaillance de la connexion ou une connexion intermittente, si la carte SIM n'est pas insérée.
- Avant d'insérer un dongle LTE Ethernet CDC dans l'appliance SD-WAN, connectez la clé USB externe à une machine Windows/Linux et assurez-vous qu'Internet fonctionne correctement avec une configuration APN et Mobile Data Roaming appropriée. Assurez-vous que le **mode de connexion** du dongle USB passe de la valeur par défaut **Manual** à **Auto**.

Remarque

- Les appliances Citrix SD-WAN prennent en charge un seul dongle USB LTE à la fois. Si plusieurs dongles USB sont branchés, débranchez tous les dongles et branchez un seul dongle.

- Les appliances Citrix SD-WAN ne prennent pas en charge le nom d'utilisateur et le mot de passe pour les modems USB. Assurez-vous que le nom d'utilisateur et le mot de passe sont désactivés sur le modem pendant l'installation.
- Le débranchement ou le redémarrage d'un dongle MBIM externe affecte la session de données du modem LTE interne. Il s'agit d'un comportement attendu.
- Lorsqu'un modem LTE externe est branché, l'appliance SD-WAN prend environ 3 minutes pour le reconnaître.

Pour afficher les détails du modem externe, dans l'interface utilisateur de l'appliance, accédez à **Configuration > Paramètres du matériel > Cartes réseau > Mobile Broadband**. Sélectionnez **Modem externe** comme type de modem.



Remarque

Le numéro de modèle du dongle USB LTE n'est pas affiché dans la section **Informations sur l'état**.

Opérations de haut débit mobile

Opérations prises en charge sur les modems externes CDC Ethernet et MBIM/NCM :

Opérations	Modem externe - CDC Ethernet	Modem externe - MBIM et NCM
Préférence SIM	Non	Non
Code PIN de la carte SIM	Non	Non
Paramètres APN	Non	Oui
Paramètres réseau	Non	Non

Opérations	Modem externe - CDC Ethernet	Modem externe - MBIM et NCM
Itinérant	Non	Non
Gérer le firmware	Non	Non
Activer/désactiver le modem	Non	Oui
Redémarrer le modem	Non	Non
Actualiser la carte SIM	Non	Non

Vous pouvez afficher et gérer à distance tous les sites LTE de votre réseau à l’aide du Centre Citrix SD-WAN. Pour plus d’informations, reportez-vous à la section [Gestion de sites LTE distants](#).

Configurer le modem USB externe

Pour configurer un modem USB externe, dans l’Éditeur de configuration, accédez à Sites, sélectionnez un site et cliquez sur **Grouper d’interface**. L’interface externe du modem USB LTE-E1 est disponible pour être configurée. Pour plus d’informations sur la configuration d’une branche pour LTE, consultez [Configurer une branche pour LTE](#).



Déploiement sans contact sur LTE

Prérequis pour activer le service de déploiement zéro contact via un modem LTE USB :

- Insérez le modem USB dans l’appliance Citrix SD-WAN. Pour plus d’informations, consultez la section Connexion du modem USB.
- Assurez-vous que la carte SIM du modem USB dispose d’un plan de données activé.

- Assurez-vous que le port de gestion/données n'est pas connecté. Si le port de gestion/données est connecté, déconnectez-le.
- Assurez-vous que le service Internet est défini pour l'interface LTE dans la configuration de l'appliance.

Lorsque l'appliance est sous tension, le service de déploiement zéro contact utilise le port LTE-E1 pour obtenir la dernière configuration et le logiciel SD-WAN les plus récents.

Utilisez l'interface graphique SD-WAN Center pour déployer et configurer l'appliance pour le service de déploiement zéro touche. Pour plus d'informations, consultez la section [Déploiement Zero Touch](#). Pour plus d'informations sur le déploiement sans intervention via le SD-WAN Orchestrator, reportez-vous à la section [Déploiement sans intervention](#).

Modems USB pris en charge

Les modems suivants sont compatibles avec les appliances Citrix SD-WAN.

Remarque

Citrix ne contrôle pas les mises à jour du microprogramme de l'opérateur sans fil. Par conséquent, la compatibilité du nouveau firmware du modem avec le logiciel Citrix SD-WAN n'est pas garantie. Le client contrôle la mise à jour du firmware du modem. Citrix recommande de tester une mise à jour du micrologiciel sur un seul site avant de la pousser sur l'ensemble du réseau.

Région	Transporteur sans fil/ Fabricant	Modem USB	Type de modem pris en charge	Interfaces
États-Unis	Verizon	Modem mondial USB730L	cdc_ether	4G uniquement
États-Unis	AT&T	Modem AT&T Global USB800	cdc_ether	4G uniquement

Commandes AT

Les commandes AT aident à surveiller et à dépanner la configuration et l'état du modem LTE. AT est l'abréviation de **At**tention. Comme chaque ligne de commande commence par **at**, elles sont appelées commandes AT. Les modèles de plate-forme Citrix SD-WAN qui prennent en charge la prise en charge LTE en exécutant des commandes AT. Les commandes AT sont spécifiques au modem et, par conséquent, la liste des commandes AT varie d'une plate-forme à l'autre.

Pour exécuter des commandes AT, effectuez les opérations suivantes :

1. Connectez-vous à la console de l'apppliance Citrix SD-WAN.
2. À l'invite, tapez le nom d'utilisateur et le mot de passe pour accéder à l'interface CLI.
3. À l'invite, tapez **lte**.
4. Entrez **at**, puis entrez la commande AT.

Voici un exemple :

at at+cpin —Fournit des informations sur l'état de la carte SIM.

```
lte> at at+cpin?  
Running at+cpin? command  
AT command state: success  
+CPIN: READY  
OK  
success
```

Déploiements

May 6, 2021

Voici quelques-uns des scénarios de cas d'utilisation implémentés à l'aide des appliances Citrix SD-WAN :

- [Déploiement du SD-WAN en mode passerelle](#)
- [Mode Inline](#)
- [Déploiement du SD-WAN en mode PBR \(mode virtuel en ligne\)](#)
- [Chemins dynamiques pour la communication de succursale à succursale](#)
- [Transfert WAN vers WAN](#)
- [Création d'un réseau SD-WAN](#)
- [Routage pour la segmentation LAN](#)
- [Utilisation de l'apppliance Premium Edition pour fournir des services d'optimisation WAN uniquement](#)
- [Mode deux appliances](#)
- [Déploiement sans intervention](#)
- [Déploiement d'une région unique](#)

- [Déploiement de plusieurs régions](#)
- [Haute disponibilité](#)

Checklist et comment déployer

August 31, 2022

Il est fortement recommandé qu'avant de commencer l'installation, vous lisiez d'abord le Guide de planification du déploiement de Citrix Virtual WAN. Cet article traite des concepts et fonctionnalités essentiels de Virtual WAN et fournit des instructions pour la planification de votre déploiement.

Préparer le déploiement

La liste suivante décrit les étapes et procédures du déploiement des éditions Standard et Premium (Enterprise) SD-WAN.

Pour consulter certains exemples d'utilisation du déploiement, consultez la section [Déploiements](#).

1. Rassemblez vos informations de déploiement Citrix SD-WAN.
2. Configurez les appliances Citrix SD-WAN.
 - Pour chaque appliance matérielle que vous souhaitez ajouter à votre déploiement SD-WAN, vous devez effectuer les tâches suivantes :
 - Configurez le matériel matériel de l'appliance.
 - Définissez l'adresse IP de gestion de l'appliance et vérifiez la connexion.
 - Définissez la date et l'heure de l'appliance.
 - (Facultatif) Définissez l'intervalle de **temporisation de la session de console** sur une valeur élevée ou maximale.
3. Téléchargez et installez le fichier de licence du logiciel sur l'appliance.

Checklist d'installation et de configuration

Rassemblez les informations suivantes pour chaque site SD-WAN que vous souhaitez déployer :

- Les informations de licence de votre produit
- Adresses IP réseau requises pour chaque appliance à déployer :

- Adresse IP de gestion
- Adresses IP virtuelles
- Nom du site
- Nom de l'apppliance (un par site)
- Modèle d'apppliance SD-WAN (pour chaque appliance à déployer)
- Mode de déploiement (MCN ou client)
- Topologie
- MPLS de passerelle
- Informations sur le tunnel GRE
- Itinéraires
- VLAN
- Bande passante sur chaque site pour chaque circuit

Recommandations

May 6, 2021

Cet article décrit les meilleures pratiques de déploiement pour la solution Citrix SD-WAN. Il fournit des conseils généraux, des avantages et des cas d'utilisation pour le mode de déploiement Citrix SD-WAN suivant.

Mode Bord/Passerelle

Recommandations

Voici les recommandations pour le déploiement en mode **passerelle** :

1. Le mode passerelle est mieux utilisé pour les succursales SD-WAN où la consolidation du routeur se produit et les clients sont prêts à autoriser le SD-WAN à être le périphérique périphérique qui termine les connexions.
2. Une excellente architecture réseau peut être rendue avec une conception scrupuleuse lorsqu'un projet est construit à partir de zéro.

Remarque

Le mode Passerelle peut être utilisé du côté du centre de données pour les projets existants avec une certaine perturbation de l'infrastructure.

Avantages/Cas d'utilisation

Voici les avantages/cas d'utilisation pour le déploiement en mode passerelle :

1. Meilleur cas d'utilisation pour la consolidation des éléments routeur/pare-feu/réseau dans la branche client.
2. Gestion simple et facile des hôtes LAN via DHCP.
 - Permet au SD-WAN de devenir le prochain saut et d'offrir l'adressage IP basé sur DHCP à tous les hôtes LAN pour les ports de données.
3. Toutes les connexions se terminent à la bordure SD-WAN et la gestion devient facile.
4. Le SD-WAN est le point focal du routage périphérique et est dirigé de tout le trafic. Les décisions sont prises sur la périphérie de la rupture, du back-haul ou de la superposition, y compris la comptabilisation de la bande passante et de la capacité.
5. Tous les hôtes de sous-réseaux LAN comme hôtes LAN sont autorisés à avoir le protocole VIP SD-WAN LAN comme saut suivant. Si SD-WAN LAN se connecte à un commutateur central, vous pouvez exécuter un routage dynamique pour obtenir une visibilité sur tous les sous-réseaux LAN.
6. Grande flexibilité pour la haute disponibilité (HA) - recommandation stricte pour le mode Gateway afin que le site fonctionne avec un mode actif/veille. En outre, il aide à prévenir le trou noir de trafic si le périphérique SD-WAN tombe en panne.
 - Commutateurs disponibles dans la branche - La haute disponibilité parallèle peut fonctionner en mode Gateway.
 - Commutateurs non disponibles dans la succursale - Le SD-WAN peut également fonctionner en mode haute disponibilité de périphérie SD-WAN (mode haute disponibilité via fil) où les deux boîtiers SD-WAN sont enchaînés pour utiliser les ports Fail-to-WAN pour agir comme une paire convergente haute disponibilité.
7. Autoriser l'Internet à être défini comme **des interfaces UNTRUSTED** qui créent automatiquement un NAT dynamique pour la connexion NAT breakout et source NAT afin que la réponse revienne au SD-WAN.
8. Les considérations de sécurité pour les interfaces **UNTRUSTED** sont naturellement implicites, en ce sens que seuls les paquets de contrôle ICMP/ARP/UDP sur 4980 sont autorisés.

Précautions

Voici les informations dont vous devez faire attention en mode Passerelle :

- **Conception soignée et architecture réseau** - Le mode Passerelle peut nécessiter des considérations de conception et de mise en réseau minutieuses, car l'ensemble du réseau branche/périphérie est en SD-WAN. Que bloquer, ce qu'il faut acheminer, comment mettre en réseau LAN, comment mettre fin aux réseaux WAN, et ainsi de suite.
- **Défaillance du périphérique** - Le mode Edge ne peut pas avoir la fonction de défaillance au fil. Toute la branche tombe en panne lorsque l'appareil est en panne.
- **Posture de sécurité** - Comme le routage est géré à la périphérie, les postures de sécurité telles que le pare-feu, les considérations d'effacement/backhaul sont cruciales et doivent être conçues avec le client.
- **Haute disponibilité —La haute disponibilité** Fail-to-Wire doit tenir compte de certaines considérations de disponibilité des ports et, en fonction des déploiements, peut devenir difficile à concevoir.
 - Le SD-WAN 110 n'est PAS une option car il n'a pas de ports de connexion à fil.

Par exemple, si vous avez besoin de 2 liaisons WAN pour fonctionner, vous avez besoin de 5 ports, dont un port dédié pour l'interface haute disponibilité, y compris l'interface LAN.

Mode Inline —Fail-to-fil/Fail-to-Block

Recommandations

Voici les recommandations pour le déploiement en mode **Inline** :

1. Le mode en ligne est idéal pour les branches où l'infrastructure existante ne doit pas être modifiée et où le SD-WAN est intégré de manière transparente au segment LAN.
2. Les datacenters peuvent également utiliser une haute disponibilité en ligne ou parallèle en ligne, car il est extrêmement important de s'assurer que les charges de travail du datacenter ne sont pas noircies en raison de l'arrêt ou du plantage de l'appareil.

Avantages et cas d'utilisation

Voici les avantages/cas d'utilisation pour le déploiement en mode Inline :

1. Garder le routeur MPLS donc fail-to-wire est une belle fonctionnalité. Les périphériques compatibles Fail-to-Wire permettent un basculement sans faille pour placer l'infrastructure en sous-couche en cas de panne de la boîte.

- Si vos périphériques prennent en charge le câblage (SD-WAN 210 et supérieur), cela permet de placer un seul SD-WAN en ligne sur le matériel contourner le trafic LAN vers le routeur périphérique du client lorsque le SD-WAN se bloque ou tombe en panne.
 - Si les liens MPLS sont présents qui donnent une extension naturelle au LAN/intranet du client, le port de paire de pont fail-à-fil est le meilleur choix (paires compatibles fail-to-wire) de telle sorte que, lorsque le périphérique se bloque ou descend le trafic LAN, le matériel est contourné vers le routeur périphérique client (toujours maintenu le prochain houblon).
2. Le réseautage est simple.
 3. Le SD-WAN voit tout le trafic via le mode en ligne, donc c'est le meilleur scénario pour la comptabilisation de la bande passante et de la capacité appropriée.
 4. Peu d'exigences d'intégration car vous n'avez besoin que d'une adresse IP du segment L2. Les segments LAN sont bien connus car vous avez un bras à l'interface LAN. Si vous vous connectez à un commutateur central, vous pouvez également exécuter un routage dynamique pour obtenir une visibilité sur tous les sous-réseaux LAN.
 5. Les attentes du client sont que le SD-WAN doit se fondre dans l'infrastructure existante en tant que nouveau nœud réseau (rien d'autre ne change).
 6. **Proxy ARP** —En mode en ligne, c'est une bénédiction pour le SD-WAN de fournir par proxy des requêtes ARP au prochain saut LAN si la passerelle est tombée en panne ou si l'interface SD-WAN vers le saut suivant est tombée en panne.
 - Généralement, en mode en ligne avec paire de pont (fail-to-block ou fail-to-wire) avec plusieurs connexions WAN (MPLS/Internet), il est recommandé d'activer Proxy ARP pour l'interface de paire de ponts qui connecte les hôtes LAN à leur passerelle de saut suivant.
 - Pour quelque raison que ce soit lorsque le saut suivant est en panne ou que l'interface SD-WAN au saut suivant est en panne rendant la Gateway inaccessible, le SD-WAN agit comme un proxy pour les requêtes ARP permettant aux hôtes LAN d'envoyer des paquets de manière transparente et d'utiliser les connexions WAN restantes qui conservent le chemin virtuel vers le haut.
 7. **Haute disponibilité** - Si l'option Fail-to-Wire n'est pas une option, les périphériques peuvent être placés dans des périphériques parallèles à haute disponibilité (interfaces LAN et WAN communes pour les Active/Veille) pour obtenir une redondance.
 - Si vos appliances ne prennent pas en charge le câblage par défaut, comme le SD-WAN 110, vous devez opter pour une haute disponibilité parallèle en ligne qui permet de lancer un périphérique de secours en cas de panne du périphérique principal.

Précautions

Voici les informations dont vous devez faire attention dans le mode **Inline** :

- Réseau de plomberie avec deux bras au SD-WAN (côté LAN et WAN), nécessite un certain temps d'arrêt car le réseau doit être plongé dans deux bras.
- Il faut s'assurer que si le câblage est utilisé, il se trouve derrière un routeur/pare-feu côté client dans une zone **TRUSTED** afin que la sécurité ne soit pas compromise.
- MPLS QoS change un peu dans ce sens car les stratégies QoS précédentes peuvent dépendre des adresses IP source ou DSCP qui seront désormais masquées en raison d'une superposition.
- Il faut prendre soin de réutiliser le routeur MPLS avec une bande passante réservée spécifique au SD-WAN avec une balise DSCP spécifique, de sorte que la QoS de SD-WAN s'occupe de prioriser le trafic et envoie des applications hautement prioritaires immédiatement suivies par d'autres classes (mais être en mesure de tenir compte de l'ensemble des bande passante réservée au SD-WAN sur le routeur MPLS). Les files d'attente MPLS sont une alternative ou MPLS avec un seul DSCP défini sur le groupe de chemins automatiques qui peut s'occuper de cela.
- Si les interfaces Internet sont **TRUSTED** au fur et à mesure que les liens se terminent sur le routeur périphérique client, pour utiliser le service Internet, vous devez écrire une règle NAT dynamique exclusive pour activer la séparation Internet à partir de l'appliance.
- Si les liens Internet sont les seules connexions WAN et se terminent toujours sur le routeur Edge client, il est toujours correct de contourner les connexions si le routeur Edge client prend des précautions pour diriger les paquets via son infrastructure de sous-couche existante.
 - Des précautions appropriées doivent être prises pour tenir compte du flux de contournement du trafic LAN sur une paire de ponts avec une connexion Internet et lorsque l'appliance est en panne. Étant donné qu'il s'agit d'un trafic intranet d'entreprise sensible, à la veille de l'échec, le client doit savoir comment le gérer.

Mode virtuel en ligne/à un bras

Recommandations

Voici les recommandations pour le déploiement en mode **virtuel en ligne** :

1. Le mode virtuel en ligne est idéal pour la mise en réseau du datacenter, car la plomberie réseau SD-WAN peut être travaillée en parallèle pendant que le datacenter dessert ses charges de travail existantes avec l'infrastructure existante.
2. Le SD-WAN est dans une interface à bras unique qui est gérée avec un suivi SLA sur les VIP. Si le suivi tombe en panne, le trafic reprend le routage via l'infrastructure de sous-couche existante.

3. Les branches peuvent également être déployées en mode virtuel en ligne, mais elles sont plus prédominantes avec les déploiements Inline/Gateway.

Avantages et cas d'utilisation

Voici les avantages/cas d'utilisation pour le déploiement en mode **virtuel en ligne** :

1. Le moyen le plus simple et recommandé de mettre en réseau le SD-WAN dans le centre de données.
 - Le mode virtuel en ligne permet la plomberie réseau parallèle du SD-WAN avec le routeur principal.
 - Le mode virtuel en ligne nous permet de définir facilement PBRS pour détourner le trafic LAN doit passer par SD-WAN et obtenir des avantages de superposition.
2. Basculement transparent vers l'infrastructure sous-jacente en cas de défaillance du SD-WAN et transfert transparent vers SD-WAN pour des avantages de superposition dans des conditions normales.
3. Exigences de **mise en réseau** et **d'intégration** simples L'interface à un bras unique du routeur tête de main au SD-WAN en ligne virtuelle.
4. Routage dynamique facile à déployer en **mode Importation uniquement** (n'exportez rien) pour obtenir une visibilité des sous-réseaux LAN afin qu'ils puissent être envoyés aux appliances homologues SD-WAN distantes.
5. Facile à définir PBR sur les routeurs (1 par WAN VIP) pour indiquer comment choisir le physique.

Précautions

Voici les informations dont vous devez faire attention dans le mode **Virtual Inline** :

- Des précautions appropriées doivent être prises pour MAP distinctement le VIP logique SD-WAN d'une liaison WAN définie à la bonne interface physique (sinon cela pourrait causer des problèmes indésirables dans l'évaluation des métriques WAN et le choix des chemins WAN).
- Des considérations de conception appropriées doivent être prises en compte pour savoir si tout le trafic est détourné via le SD-WAN ou seulement un trafic spécifique.
- Cela signifie que le SD-WAN doit être dédié une part de bande passante exclusivement pour lui-même qui doit être définie sur les interfaces de sorte que la capacité du SD-WAN n'est pas utilisée par d'autres trafic non-SD-WAN provoquant des résultats indésirables.
 - Des problèmes de comptabilisation de la bande passante et des problèmes de congestion peuvent se produire si la capacité des liaisons WAN SD-WAN est mal définie.

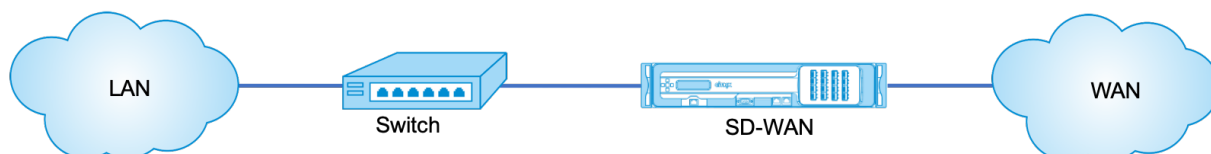
- Le routage dynamique peut causer certains problèmes s'il est mal conçu, où si le SD-WAN achemine les VIP du centre de données et de la branche sont exportés vers le headend et si le routage est influencé vers SD-WAN, les paquets de superposition commencent à boucler et provoquent des résultats indésirables.
- Le routage dynamique doit être correctement administré en tenant compte de tous les facteurs potentiels de ce qu'il faut apprendre ou de ce qu'il faut faire de la publicité.
- L'interface physique à un bras peut parfois devenir un goulot d'étranglement. Nécessite quelques considérations de conception dans ces lignes car il s'adapte à la fois au téléchargement/téléchargement et agit également comme le trafic LAN vers LAN et LAN vers WAN/WAN vers LAN à partir du SD-WAN.
- Un trafic LAN à LAN excessif peut être un point à noter lors de la conception.
- Si le routage dynamique n'est pas utilisé, il faut faire attention à l'administration de tous les sous-réseaux LAN, ce qui, sinon, peut causer des problèmes de routage indésirables.
- Il existe des problèmes potentiels de boucle de routage si vous définissez une route par défaut (0.0.0.0/0) sur le SD-WAN dans le virtuel en ligne pour pointer vers le routeur principal. Dans de telles situations, si le chemin virtuel est tombé en panne, tout trafic provenant du réseau local du centre de données (comme la surveillance du trafic) est renvoyé à la tête de ligne et de retour vers le SD-WAN causant des problèmes de routage indésirables (si le chemin virtuel est en panne, les sous-réseaux de branche distante deviennent accessibles **NO** provoquant le route par défaut à être HIT, ce qui provoque les problèmes de boucle).

Mode passerelle

May 6, 2021

Le mode Gateway place l'appliance SD-WAN physiquement dans le chemin (déploiement à deux bras) et nécessite des modifications dans l'infrastructure réseau existante pour faire de l'appliance SD-WAN la passerelle par défaut de l'ensemble du réseau LAN de ce site. Mode passerelle utilisé pour les nouveaux réseaux et le remplacement du routeur. Le mode passerelle permet aux appliances SD-WAN :

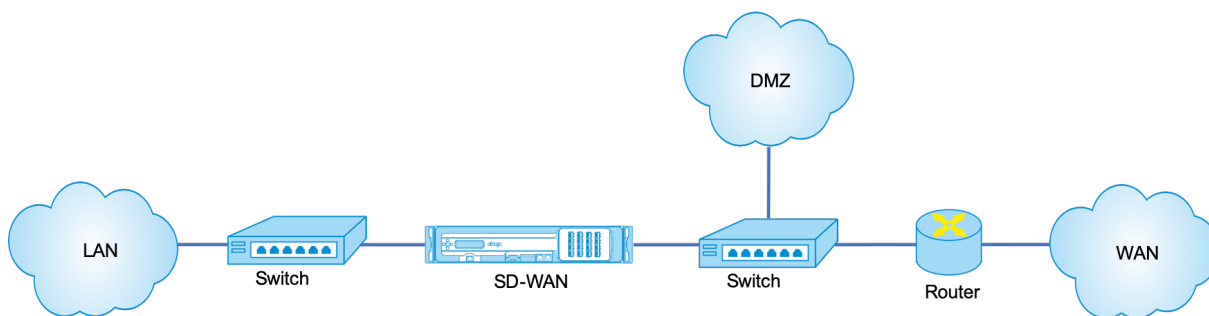
- Pour afficher tout le trafic à destination et en provenance du WAN
- Pour effectuer un routage local



Remarque

Un SD-WAN déployé en mode Passerelle agit comme un périphérique de couche 3 et ne peut pas effectuer de fail-to-wire. Toutes les interfaces impliquées seront configurées pour **Fail-to-Block**. En cas de défaillance de l'apppliance, la Gateway par défaut du site échoue également, provoquant une panne jusqu'à ce que l'apppliance et la Gateway par défaut soient restaurées.

En mode **Inline**, l'apppliance SD-WAN semble être un pont Ethernet. La plupart des modèles d'appiances SD-WAN incluent une fonction de contournement Ethernet pour le mode intégré. En cas de panne de courant, un relais se ferme et les ports d'entrée et de sortie sont connectés électriquement, ce qui permet au signal Ethernet de passer d'un port à un autre. En mode Fail-to-wire, l'apppliance SD-WAN ressemble à un câble croisé reliant les deux ports. Mode Inline utilisé pour s'intégrer dans des réseaux déjà bien définis.

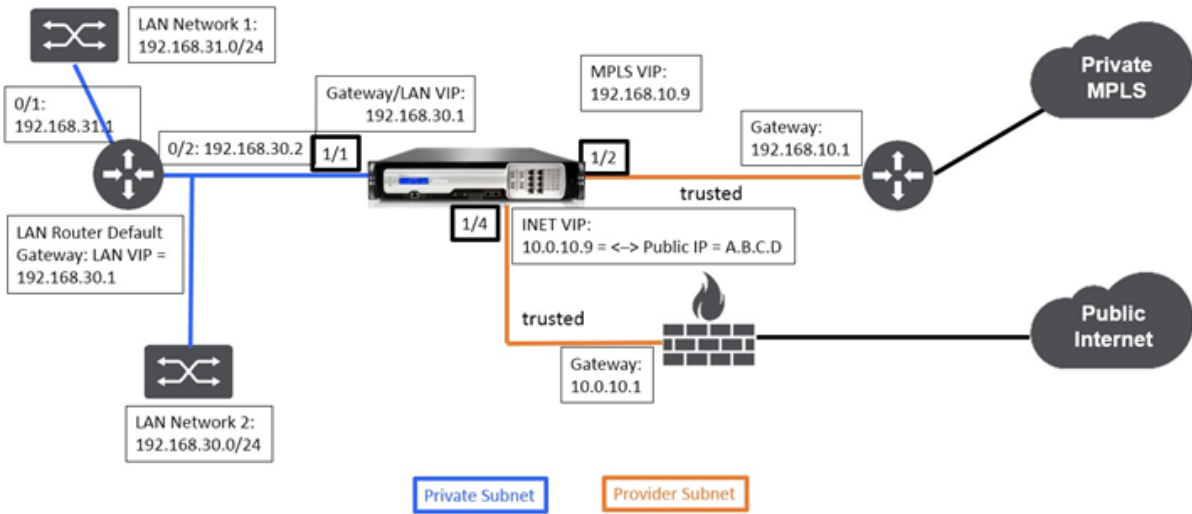


Cet article fournit une procédure étape par étape pour configurer un dispositif SD-WAN en mode passerelle dans un exemple de configuration réseau. Le déploiement en ligne est également décrit pour le côté de la branche pour terminer la configuration. Un réseau peut continuer à fonctionner si un périphérique Inline est supprimé, mais perd tout accès si le périphérique Gateway est supprimé.

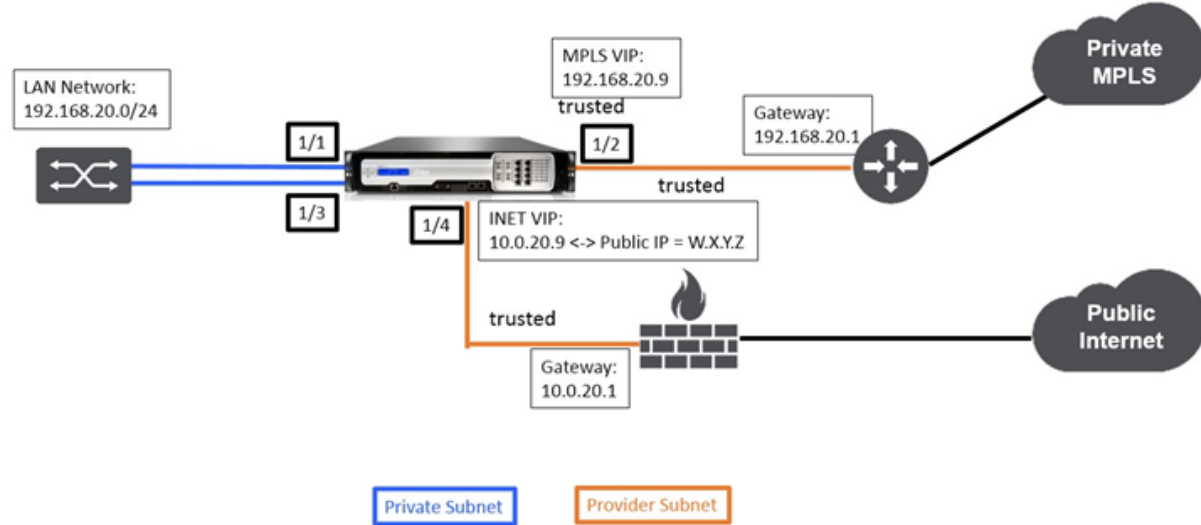
Topologie

Les illustrations suivantes décrivent les topologies prises en charge dans un réseau SD-WAN.

Data Center dans le déploiement de la Gateway



Succursale en déploiement en ligne



Exigences de déploiement

Les exigences de déploiement et les informations connexes sont décrites ci-dessous pour vous aider à créer la configuration.

Nom de site	Site DataCenter	Site de succursale
Nom de l'appliance	A_DC1	A_BR1

Nom de site	Site DataCenter	Site de succursale
Gestion IP	172.30.2.10/24	172.30.2.20/24
Clé de sécurité	Le cas échéant	Le cas échéant
Modèle/Edition	4000	2 000
Mode	Passerelle	Inline
Topologie	2 x Chemin WAN	2 x Chemin WAN
Adresse VIP	192.168.10.9/24 –MPLS, 10.0.10.9/24 –Internet (IP publique –A.B.C.D), 192.168.30.1/24 - LAN	192.168.20.9/24 - MPLS, 10.0.20.9/24 –Internet (IP publique –W.X.Y.Z)
Passerelle MPLS	192.168.10.1	192.168.20.1
Passerelle Internet	10.0.10.1	10.0.20.1
Vitesse de liaison	MPLS —100 Mbps, Internet — 20 Mbps	MPLS —10 Mbps, Internet —2 Mbps
Itinéraire	Adresse IP réseau - 192.168.31.0/24, Type de service - Local, Adresse IP de passerelle - 192.168.30.2	Le cas échéant
VLAN	Le cas échéant	Le cas échéant

Prérequis pour la configuration

- Activez l’appliance SD-WAN en tant que nœud de contrôle maître.
- La configuration est effectuée uniquement sur le nœud de contrôle maître (MCN) de l’appliance SD-WAN.

Pour activer une appliance en tant que nœud de contrôle maître :

1. Dans l’interface de gestion Web SD-WAN, accédez à **Configuration > Paramètres de l’appliance > Interface administrateur > onglet Divers > Switch Console**.

Remarque

Si **Basculer vers la console client** s’affiche, l’appliance est déjà en mode MCN. Il ne doit y avoir qu’un seul MCN actif dans un réseau SD-WAN.

2. Démarrez Configuration en accédant à **Configuration > Réseau étendu virtuel > Éditeur de configuration**. Cliquez sur **Nouveau** pour commencer la configuration.

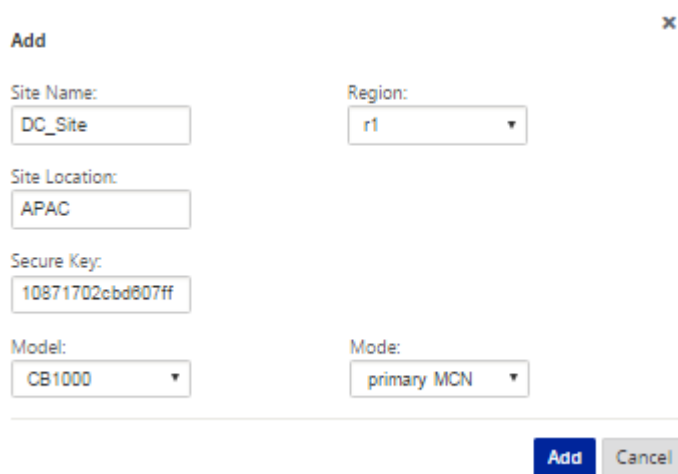
Configuration du mode Gateway de site du datacenter

Voici les étapes de configuration de haut niveau pour configurer le déploiement de la passerelle de site de centre de données :

1. Créez un site DC.
2. Remplissez les groupes d'interface en fonction des interfaces Ethernet connectées.
3. Créez une adresse IP virtuelle pour chaque interface virtuelle.
4. Remplissez les liaisons WAN en fonction du débit physique et non de la vitesse en rafale à l'aide des liaisons Internet et MPLS.
5. Remplissez les itinéraires s'il y a plus de sous-réseaux dans l'infrastructure du réseau local.

Pour créer un site de contrôleur de domaine

1. Accédez à **Configuration Editor > Sites**, puis cliquez sur le **bouton+ Ajouter**.
2. Remplissez les champs comme indiqué ci-dessous.
3. Conservez les paramètres par défaut sauf instructions contraires.



Add ✕

Site Name:

Region:

Site Location:

Secure Key:

Model:

Mode:

Add **Cancel**

The screenshot displays the 'Basic Settings' configuration page for a site named 'MCN-5100'. On the left, a sidebar menu lists various configuration options: Sites, Basic Settings (selected), Centralized Licensing, Routing Domains, Interface Groups, Virtual IP Addresses, VRRP, DHCP, WAN Links, Certificates, and High Availability. The main configuration area on the right includes the following fields and controls:

- Site Name:** MCN-5100
- Appliance Name:** Appliance
- Secure Key:** 2e8867413a24728, with a **Regenerate** button.
- Model:** CB5100 (dropdown menu)
- Mode:** primary MCN (dropdown menu)
- Site Location:** (empty text field)
- Default Direct Route Cost:** 5
- Gateway ARP Timer (ms):** 1000
- Enable Source MAC Learning:** (unchecked checkbox)
- Buttons:** **Apply** and **Revert**

Pour configurer des groupes d'interfaces basés sur des interfaces Ethernet connectées

1. Dans l'**Éditeur de configuration**, accédez à **Sites > Afficher le site > [Nom du site] > Groupes d'interface**. Cliquez sur **+** pour ajouter des interfaces destinées à être utilisées. Pour le mode passerelle, chaque groupe d'interfaces se voit attribuer une seule interface Ethernet.
2. Le mode de contournement est défini sur **Fail-to-block** car une seule interface Ethernet/Physique est utilisée par interface virtuelle. Il n'y a pas non plus de paires de ponts.
3. Dans cet exemple, trois groupes d'interfaces sont créés, l'un faisant face au réseau local et deux autres faisant face à chaque liaison WAN respective. Reportez-vous à l'exemple de topologie « DC Gateway Mode » ci-dessus et remplissez les champs Groupes d'interface comme indiqué ci-dessous.

Virtual Interfaces

Ethernet Interfaces

12345678

Bypass Mode

Fail-to-Block

WCCP

Security

Trusted

Delete

Virtual Interfaces

Name	Firewall Zone	VLAN ID	DHCP Client	Delete
DC-LAN-1-1	Default_LAN_Zon	0	<input type="checkbox"/>	

Bridge Pairs

Interfaces	LSP	Delete
1 ↔ 2	<input type="checkbox"/>	

VirtualInterface-1 (0)

12345678

Fail-to-Block

Trusted

Virtual Interfaces

Name	Firewall Zone	VLAN ID	DHCP Client	Delete
INET_DC-WAN-1-4	<Default>	0	<input type="checkbox"/>	

Bridge Pairs

Interfaces	LSP	Delete
1 ↔ 2	<input type="checkbox"/>	

VirtualInterface-2 (0)

12345678

Fail-to-Block

Trusted

Virtual Interfaces

Name	Firewall Zone	VLAN ID	DHCP Client	Delete
MPLS-DC-WAN-1-2	<Default>	0	<input type="checkbox"/>	

Bridge Pairs

Interfaces	LSP	Delete

Apply

Revert

Pour créer une adresse IP virtuelle (VIP) pour chaque interface virtuelle

- 1. Créez un VIP sur le sous-réseau approprié pour chaque liaison WAN. Les VIP sont utilisés pour la communication entre deux appliances SD-WAN dans l’environnement Virtual WAN.
- 2. Créez une adresse IP virtuelle à utiliser comme adresse de passerelle pour le réseau LAN.

+

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.0.10.9/24	INET_DC-WAN-1-4 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.10.9/24	MPLS-DC-WAN-1-2 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.30.1/24	DC-LAN-1-1 (0)	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply

Refresh

Pour remplir les liens WAN en fonction de la vitesse physique et non de la vitesse de rafale à l’aide de la liaison Internet :

- 1. Accédez à **Liens WAN**, cliquez sur le **bouton+ Ajouter un lien** pour ajouter un lien WAN pour le lien Internet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

308

2. Remplissez les détails du lien Internet, y compris l'adresse IP publique fournie, comme indiqué ci-dessous. L'**adresse IP publique** AutoDetect ne peut pas être sélectionnée pour l'appliance SD-WAN configurée en tant que MCN.
3. Accédez à **Interfaces d'accès**, à partir du menu déroulant de section, puis cliquez sur le **bouton+ Ajouter** pour ajouter des détails d'interface spécifiques au lien Internet.
4. Remplissez l'interface d'accès pour les adresses IP et de Gateway comme indiqué ci-dessous.

WAN Link: BR571-WL-1 Section: Settings + Add Link Delete Link

Basic Settings ?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name: BR571-WL-1

Access Type: Public Internet WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_DC-INET-AI-1	INET_DC-WAN-1-4	10.0.10.9	10.0.10.1	Primary	<input type="checkbox"/>	

Pour créer un lien MPLS

1. Accédez à **Liens WAN**, cliquez sur le **bouton+** pour ajouter un lien WAN pour le lien MPLS.
2. Remplissez les détails du lien MPLS comme indiqué ci-dessous.
3. Accédez à **Interfaces d'accès**, cliquez sur le **bouton+** pour ajouter des détails d'interface spécifiques au lien MPLS.

4. Remplissez l’interface d’accès pour les adresses IP et de Gateway comme indiqué ci-dessous.

Basic Settings ?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:
BR571-WL-1

Access Type:
Private MPLS

WAN Link Template:
<None>

LAN to WAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

Permitted Rate (kbps):
10000

WAN to LAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

Permitted Rate (kbps):
10000

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_DC-MPLS-...	MPLS-DC-WAN-1-2	192.168.10.9	192.168.10.1	Primary	<input type="checkbox"/>	

Pour remplir les itinéraires

Les itinéraires sont créés automatiquement en fonction de la configuration ci-dessus. L’exemple de topologie de LAN DC ci-dessus a un sous-réseau LAN supplémentaire qui est **192.168.31.0/24**. Un itinéraire doit être créé pour ce sous-réseau. L’adresse IP de la passerelle doit être dans le même sous-réseau que le VIP du LAN DC comme indiqué ci-dessous.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

310

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	192.168.31.0/24	5	Local		192.168.30.2			
2	192.175.58.0/24	5	Virtual Path	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5	Local					
9	0.0.0.0/0	65535	Passthrough					

1

Configuration du déploiement en ligne du site de succursale

Voici les étapes de configuration de haut niveau pour configurer le site Branch pour le déploiement en ligne :

1. Créer un site Branch.
2. Remplissez les groupes d'interface en fonction des interfaces Ethernet connectées.
3. Créez une adresse IP virtuelle pour chaque interface virtuelle.
4. Remplissez les liaisons WAN en fonction du débit physique et non de la vitesse en rafale à l'aide des liaisons Internet et MPLS.
5. Remplissez les itinéraires s'il y a plus de sous-réseaux dans l'infrastructure du réseau local.

Pour créer un site Branch

1. Accédez à l'**Éditeur de configuration > Sites**, puis cliquez sur le bouton **«+» Ajouter**.
2. Remplissez les champs comme indiqué ci-dessous.
3. Conservez les paramètres par défaut sauf instructions contraires.

Add

Site Name:

BR_Site

Secure Key:

dd40529b4c910e...

Model:

210

Sub Model:

BASE

Mode:

client

Site Location:

Add

Cancel

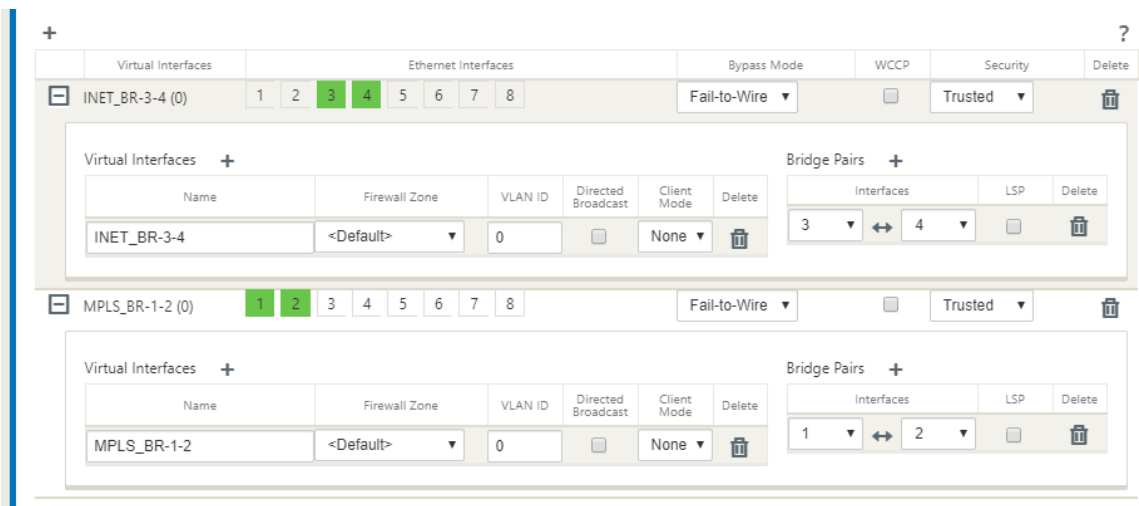
The screenshot displays the Citrix SD-WAN configuration interface. At the top, there are tabs for 'Basic', 'Global', 'Sites' (selected), 'Connections', 'Optimization', and 'Provisioning'. Below the tabs, the 'Region' is set to 'Default_Region'. The 'Site' dropdown shows 'BR_Site', with buttons for '+ Site', 'Site', and 'Site'. A sidebar on the left lists various configuration options under the 'Sites' heading, with 'Basic Settings' selected. The main configuration area for 'BR_Site' includes the following fields:

- Site Name:** BR_Site
- Appliance Name:** BR_Site-210
- Secure Key:** dd40529b4c910e... (with a 'Regenerate' button)
- Model:** 210
- Sub Model:** BASE
- Mode:** client
- Site Location:** (empty field)
- Default Direct Route Cost:** 5
- Gateway ARP Timer (ms):** 1000
- Host ARP Timer (ms):** 1000
- ☐ Enable Source MAC Learning

At the bottom of the configuration area are 'Apply' and 'Refresh' buttons.

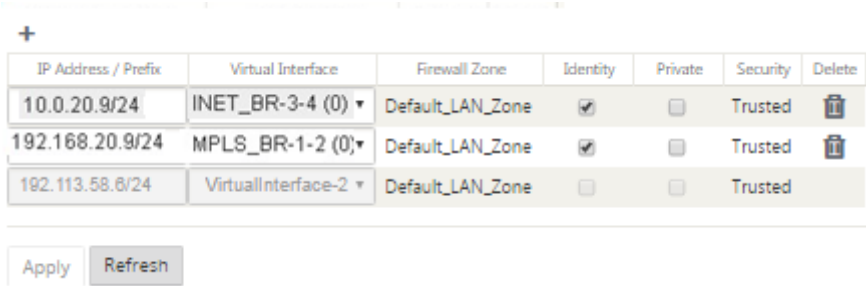
Pour remplir des groupes d'interfaces basés sur des interfaces Ethernet connectées

1. Dans l'**Éditeur de configuration**, accédez à **Sites > Afficher le site > [Nom du site client] > Groupes d'interface**. Cliquez sur **+** pour ajouter des interfaces destinées à être utilisées. Pour le mode Inline, chaque groupe d'interfaces se voit attribuer deux interfaces Ethernet.
2. Le mode de contournement est réglé sur **Fail-to-wire** et Bridge Pair est créé à l'aide des deux interfaces Ethernet.
3. Reportez-vous à l'exemple de topologie « Mode Inline Site distant » ci-dessus et remplissez les champs Groupes d'interface comme indiqué ci-dessous.



Pour créer une adresse IP virtuelle (VIP) pour chaque interface virtuelle

- 1. Créez une adresse IP virtuelle sur le sous-réseau approprié pour chaque liaison WAN. Les VIP sont utilisés pour la communication entre deux appliances SD-WAN dans l’environnement Virtual WAN.



Pour remplir les liens WAN en fonction de la vitesse physique et non de la vitesse de rafale à l’aide de la liaison Internet :

- 1. Accédez à **Liens WAN**, cliquez sur le **bouton+**pour ajouter un lien WAN pour le lien Internet.
- 2. Remplissez les détails du lien Internet, y compris l’adresse IP publique Détecter automatiquement, comme indiqué ci-dessous.
- 3. Accédez à **Interfaces d’accès**, cliquez sur le bouton + pour ajouter des détails d’interface spécifiques au lien Internet.
- 4. Remplissez l’interface d’accès pour l’adresse IP et la passerelle comme indiqué ci-dessous.

WAN Link: BR571-WL-1

Section: Settings

+ Add Link

Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:
BR571-WL-1

Access Type:
Public Internet

WAN Link Template:
<None>

LAN to WAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):
10000

WAN to LAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):
10000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-INET-AI-1	INET_BR-3-4	10.0.20.9	10.0.20.1	Primary	<input checked="" type="checkbox"/>	

Pour créer un lien MPLS

1. Accédez à Liens WAN, cliquez sur le bouton+ pour ajouter un lien WAN pour le lien MPLS.
2. Remplissez les détails du lien MPLS comme indiqué ci-dessous.
3. Accédez à Interfaces d'accès, cliquez sur le bouton+ pour ajouter des détails d'interface spécifiques au lien MPLS.
4. Remplissez l'interface d'accès pour l'adresse IP et la passerelle comme indiqué ci-dessous.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

315

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Private MPLS

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-MPLS-...	MPLS_BR-1-2	192.168.20.9	192.168.20.1	Primary	<input checked="" type="checkbox"/>	

Pour remplir les itinéraires

Les itinéraires sont créés automatiquement en fonction de la configuration ci-dessus. Dans le cas où il y a plus de sous-réseaux spécifiques à cette succursale distante, des itinéraires spécifiques doivent être ajoutés pour identifier la Gateway vers le trafic direct pour atteindre ces sous-réseaux back-end.

+

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.0.20.9/24	5	Local					
2	192.168.20.9/24	5	Local	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5						
9	0.0.0.0/0	65535	Passthrough					

«

<

1

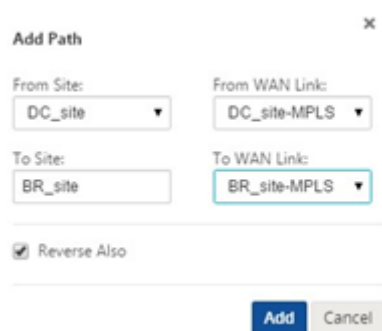
>

»

Résoudre les erreurs d'audit

Une fois la configuration terminée pour les sites DC et Branch, vous serez invité à résoudre les erreurs d'audit sur les sites DC et BR.

Par défaut, le système génère des chemins pour les liaisons WAN définies comme type d'accès Internet public. Vous devez utiliser la fonction de groupe de chemins d'accès automatiques ou activer manuellement les chemins pour les liaisons WAN avec un type d'accès Internet privé. Les chemins des liens MPLS peuvent être activés en cliquant sur Ajouter un opérateur (dans le rectangle vert).



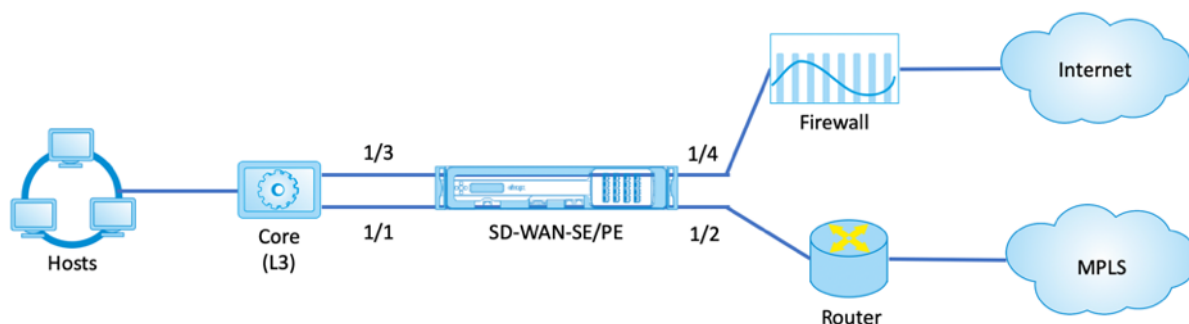
Après avoir terminé toutes les étapes ci-dessus, passez à [Préparation des packages d'appliance SD-WAN](#).

Mode Inline

May 6, 2021

Cet article fournit des détails sur la configuration d'une branche avec le mode **Déploiement en ligne**. Dans ce mode, l'appliance SD-WAN semble être un pont Ethernet. La plupart des modèles d'appliances SD-WAN **incluent une fonction** de contournement Ethernet pour le mode en ligne. En cas de panne de courant, un relais se ferme et les ports d'entrée et de sortie sont connectés électriquement, ce qui permet au signal Ethernet de passer d'un port à un autre. En mode Fail-to-wire, l'appliance SD-WAN ressemble à un câble croisé reliant les deux ports.

Dans le diagramme suivant, les interfaces 1/1 et 1/2 sont des paires de contournement matériel et connectent le noyau au routeur MPLS de bord. Les interfaces 1/3 et 1/4 sont également des paires de contournement matériel et connectent le Core au pare-feu de bord.



Configuration du déploiement en ligne du site de succursale

Voici les étapes de configuration de haut niveau pour configurer le site Branch pour le déploiement en ligne :

1. Créer un site Branch.
2. Remplissez les groupes d'interface en fonction des interfaces Ethernet connectées.
3. Créez une adresse IP virtuelle pour chaque interface virtuelle.
4. Remplissez les liaisons WAN en fonction du débit physique et non de la vitesse en rafale à l'aide des liaisons Internet et MPLS.
5. Remplissez les itinéraires s'il y a plus de sous-réseaux dans l'infrastructure du réseau local.

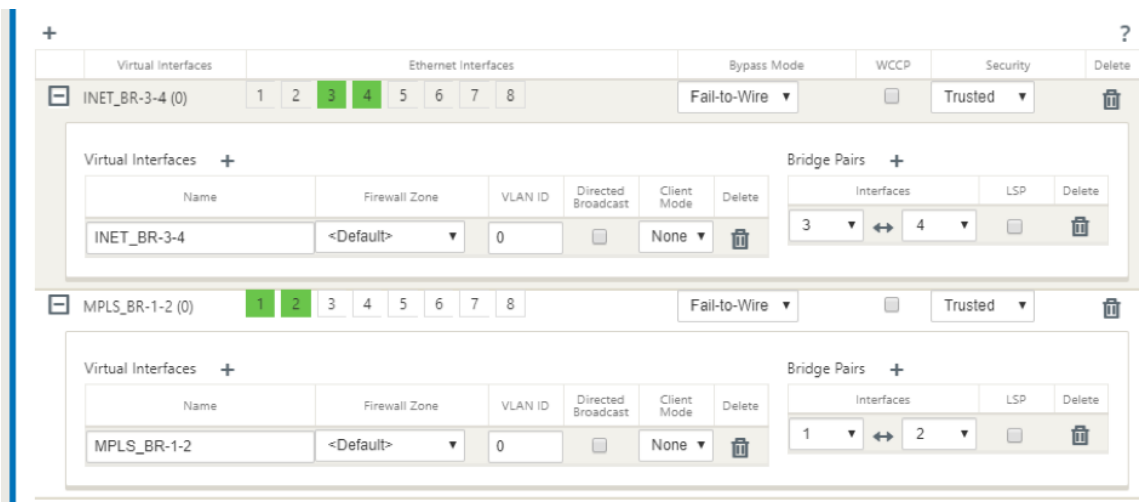
Pour créer un site de branche

1. Accédez à **Configuration Editor > Sites**, puis cliquez sur le bouton **+ Ajouter**.
2. Conservez les paramètres par défaut sauf instructions contraires.

The screenshot shows the Citrix SD-WAN configuration interface. At the top, there are tabs: Basic, Global, Sites (selected), Connections, Optimization, and Provisioning. Below the tabs, the 'Region' is set to 'Default_Region'. The 'Site' dropdown is set to 'BR_Site'. To the right of the dropdown are buttons: '+ Site', 'Site' (with a copy icon), and 'Site' (with a delete icon). Below these is a list of configuration options for the selected site: Basic Settings (selected), Centralized Licensing, Routing Domains, Link Aggregation Groups, Interface Groups, Virtual IP Addresses, VRRP, DHCP, DNS, Proxy Auto-config settings, WAN Links, Certificates, and High Availability. To the right of this list is a large configuration panel for the selected site. The panel has a title bar 'Site Name: BR_Site' with a help icon. Below the title bar are fields for 'Appliance Name' (BR_Site-210) and 'Secure Key' (dd40529b4c910e...) with a 'Regenerate' button. Below these are 'Model' (210) and 'Sub Model' (BASE) dropdowns. Further down are 'Mode' (client) and 'Site Location' fields. Below these are 'Default Direct Route Cost' (5), 'Gateway ARP Timer (ms)' (1000), and 'Host ARP Timer (ms)' (1000). At the bottom of the panel is a checkbox 'Enable Source MAC Learning' and 'Apply' and 'Refresh' buttons.

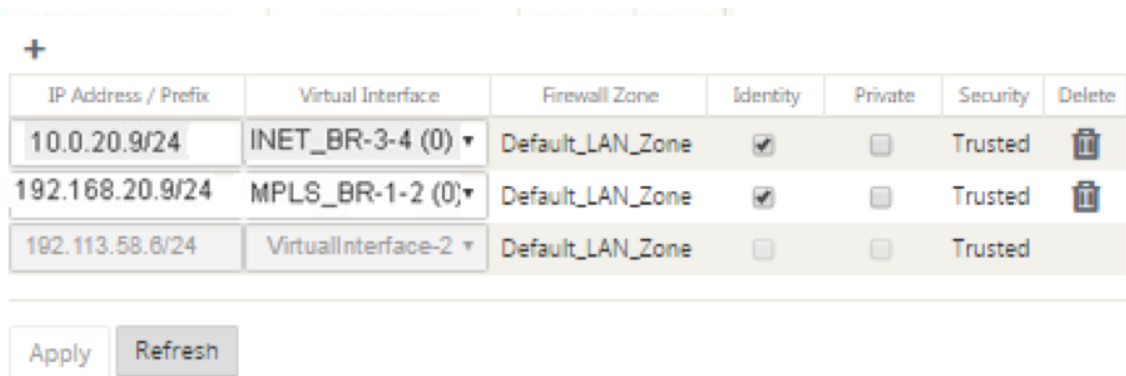
Pour remplir des groupes d'interfaces basés sur des interfaces Ethernet connectées

1. Dans l'Éditeur de configuration, accédez à **Sites > Afficher le site > [Nom du site client] > Groupes d'interface**. Cliquez sur **+** pour ajouter des interfaces destinées à être utilisées. Pour le mode Inline, chaque groupe d'interfaces se voit attribuer deux interfaces Ethernet.
2. Le mode de contournement est réglé sur **Fail-to-wire** et Bridge Pair est créé à l'aide des deux interfaces Ethernet.
3. Reportez-vous à l'exemple de topologie ci-dessus et remplissez les champs Groupes d'interface comme indiqué ci-dessous.



Pour créer une adresse IP virtuelle (VIP) pour chaque interface virtuelle

1. Créez une adresse IP virtuelle sur le sous-réseau approprié pour chaque liaison WAN. Les VIP sont utilisés pour la communication entre deux appliances SD-WAN dans l’environnement Virtual WAN.



Pour remplir les liens WAN en fonction du débit physique et non de la vitesse de rafale à l’aide d’un lien Internet

1. Accédez à **Liens WAN**, cliquez sur le **bouton+** pour ajouter un lien WAN pour le lien Internet.
2. Remplissez les détails du lien Internet, y compris l’adresse IP publique Détecter automatiquement, comme indiqué ci-dessous.
3. Accédez à **Interfaces d’accès**, cliquez sur le **bouton+** pour ajouter des détails d’interface spécifiques au lien Internet.
4. Remplissez l’interface d’accès pour l’adresse IP et la passerelle comme indiqué ci-dessous.

WAN Link: BR571-WL-1

Section: Settings

+ Add Link

Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Public Internet

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):

10000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-INET-AI-1	INET_BR-3-4	10.0.20.9	10.0.20.1	Primary	<input checked="" type="checkbox"/>	

Pour créer un lien MPLS

1. Accédez à **Liens WAN**, cliquez sur le bouton + pour ajouter un lien WAN pour le lien MPLS.
2. Remplissez les détails du lien MPLS comme indiqué ci-dessous.
3. Accédez à **Interfaces d'accès**, cliquez sur le bouton + pour ajouter des détails d'interface spécifiques au lien MPLS.
4. Remplissez l'interface d'accès pour l'adresse IP et la passerelle comme indiqué ci-dessous.

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Private MPLS

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy/ARP	Delete
SJC_BR-MPLS-...	MPLS_BR-1-2	192.168.20.9	192.168.20.1	Primary	<input checked="" type="checkbox"/>	

Pour remplir les itinéraires

Les itinéraires sont créés automatiquement en fonction de la configuration ci-dessus. Dans le cas où il y a plus de sous-réseaux spécifiques à cette succursale distante, des itinéraires spécifiques doivent être ajoutés afin d’identifier la Gateway vers le trafic direct pour atteindre ces sous-réseaux back-end.

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.0.20.9/24	5	Local					
2	192.168.20.9/24	5	Local	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5						
9	0.0.0.0/0	65535	Passthrough					

1

Mode virtuel en ligne

November 1, 2021

En mode virtuel en ligne, le routeur utilise un protocole de routage tel que PBR, OSPF ou BGP pour rediriger le trafic WAN entrant et sortant vers l'apppliance, et l'apppliance transfère les paquets traités au routeur.

L'article suivant décrit la procédure pas à pas pour configurer deux appliances SD-WAN (SD-WAN SE) :

- Appliance de centre de données en mode virtuel en ligne
- Appliance Branch en mode Inline
- Le protocole de routage doit être configuré au niveau du commutateur principal ou plus en amont au niveau du routeur. Le routeur doit surveiller l'intégrité de l'apppliance SD-WAN afin que l'apppliance puisse être contournée en cas de défaillance.
- Le mode virtuel en ligne place l'apppliance SD-WAN physiquement hors du chemin (déploiement à un bras), c'est-à-dire qu'une seule interface Ethernet doit être utilisée (exemple : interface 1/5) avec le mode de contournement défini sur Fail-to-Block (FTB).

L'apppliance Citrix SD-WAN doit être configurée pour transmettre le trafic à la Gateway appropriée. Le trafic destiné au chemin virtuel est dirigé vers l'apppliance SD-WAN, puis encapsulé et dirigé vers la liaison WAN appropriée.

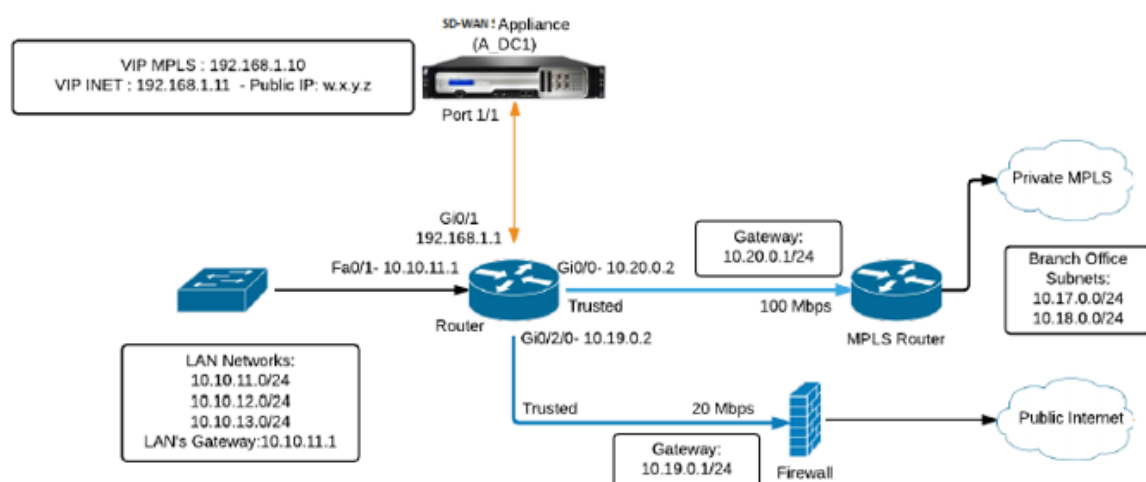
Recueillir

Recueillez les informations suivantes nécessaires à la configuration du mode virtuel en ligne :

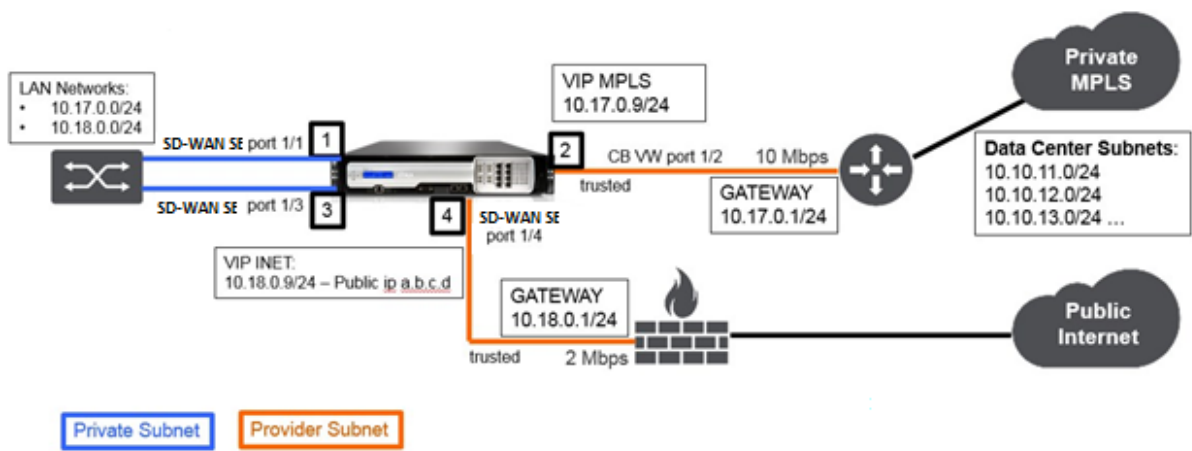
- Diagramme de réseau précis de vos sites locaux et distants, y compris :
 - Les liaisons WAN locales et distantes et leurs largeurs de bande passante dans les deux sens, leurs sous-réseaux, les adresses IP virtuelles et les passerelles de chaque lien, les routes et les réseaux locaux virtuels.
- Tableau de déploiement

Voici un exemple de diagramme de réseau et de table de déploiement :

Topologie du centre de données — Mode virtuel en ligne



Topologie de succursale —mode en ligne



Nom du site	Site du centre de données	Site de succursale
Nom de l'apppliance	SJC-DC	SJC-BR
Gestion IP	172.30.2.10/24	172.30.2.20/24
Clé de sécurité	Le cas échéant	Le cas échéant
Modèle/Édition	4000	2 000
Mode	Mode Virtual Inline	Inline
Topologie	2 x Chemin WAN	2 x Chemin WAN
Adresse VIP	192.168.1.10/24 —MPLS, 192.168.2.10/24 —Internet, IP publique w.x.y.z	10.17.0.9/24 - MPLS, 10.18.0.9/24 - Internet, IP publique a.b.c.d
MPLS de passerelle	10.20.0.1	10.17.0.1
Passerelle Internet	10.19.0.1	10.18.0.1
Vitesse de liaison	MPLS —100 Mbps, Internet — 20 Mbps	MPLS —10 Mbps, Internet —2 Mbps

Nom du site	Site du centre de données	Site de succursale
Itinéraire	<p>Vous devez ajouter un itinéraire sur l'apppliance SD-WAN SE sur la façon d'atteindre les sous-réseaux LAN (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc.) via l'une des interfaces physiques : Gi0/1 - 192.168.1.1, Configuration > Virtual WAN > Éditeur de configuration > SJC_DC \ > Routes. Dans cet exemple, l'interface 192.168.1.1 a été utilisée n/w adresse : 10.10.13.0/24, 10.10.12.0/24, 10.10.11.0/24, - Type de service : local, - Adresse IP de passerelle : 192.168.1.1</p>	Aucune route supplémentaire n'a été ajoutée
VLAN	MPLS - VLAN 10, Internet - VLAN 20	Aucun (valeur par défaut 0)

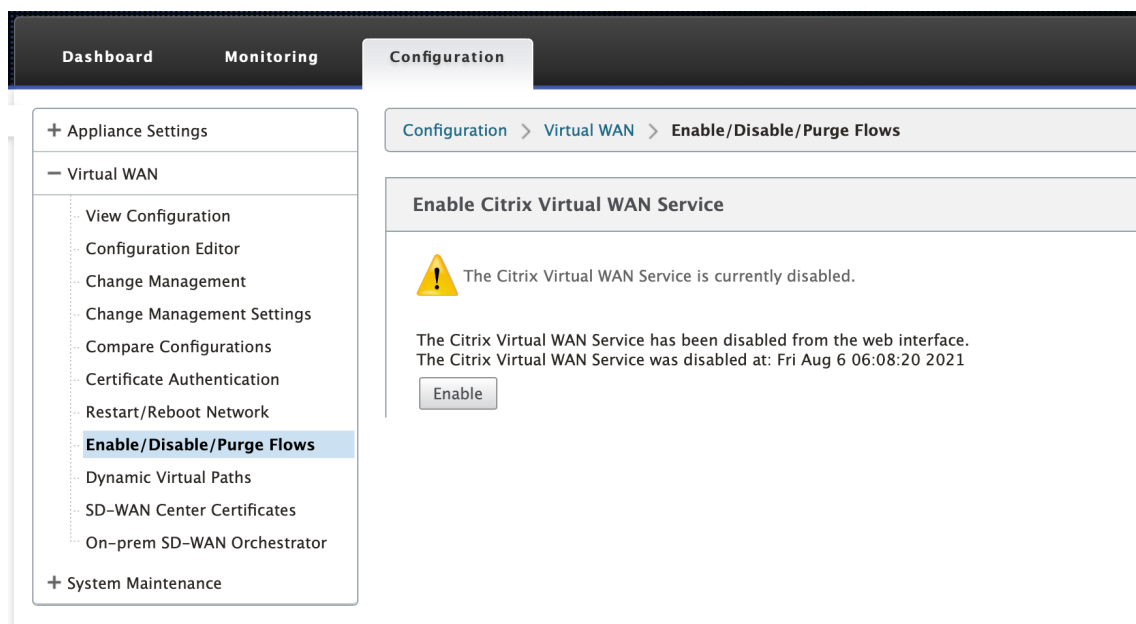
Conditions préalables

1. Dans l'interface de gestion Web de l'apppliance SD-WAN, accédez à **Configuration > Paramètres de l'apppliance > Interface administrateur > Onglet Divers**, puis cliquez sur **Switch Console**.

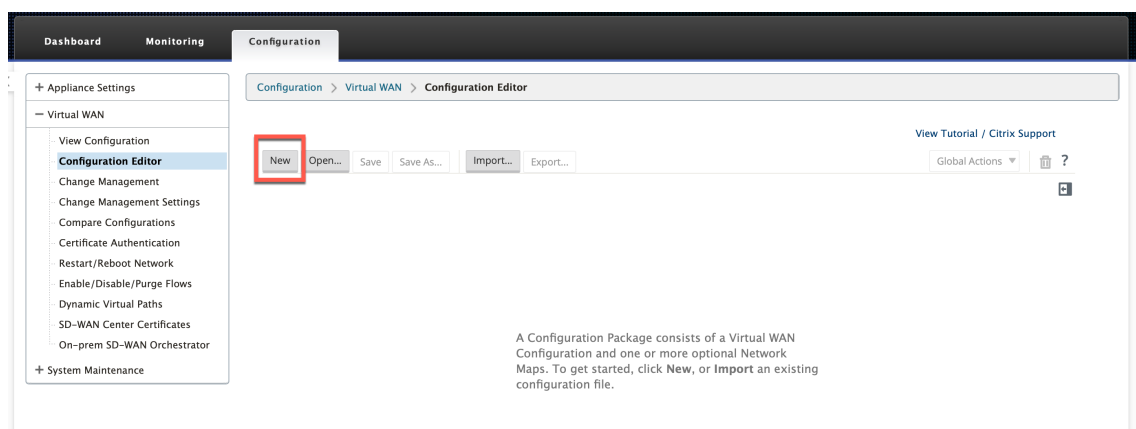
Remarque

Si **Basculer vers la console client** s'affiche, cela signifie que l'apppliance est déjà en mode MCN. Vous ne devez disposer que d'un seul MCN actif dans un réseau SD-WAN.

2. Accédez à **Configuration > Virtual WAN > Activer/Désactiver/Purger les flux**, puis cliquez sur **Activer** dans la section **Activer Citrix Virtual WAN Service**.



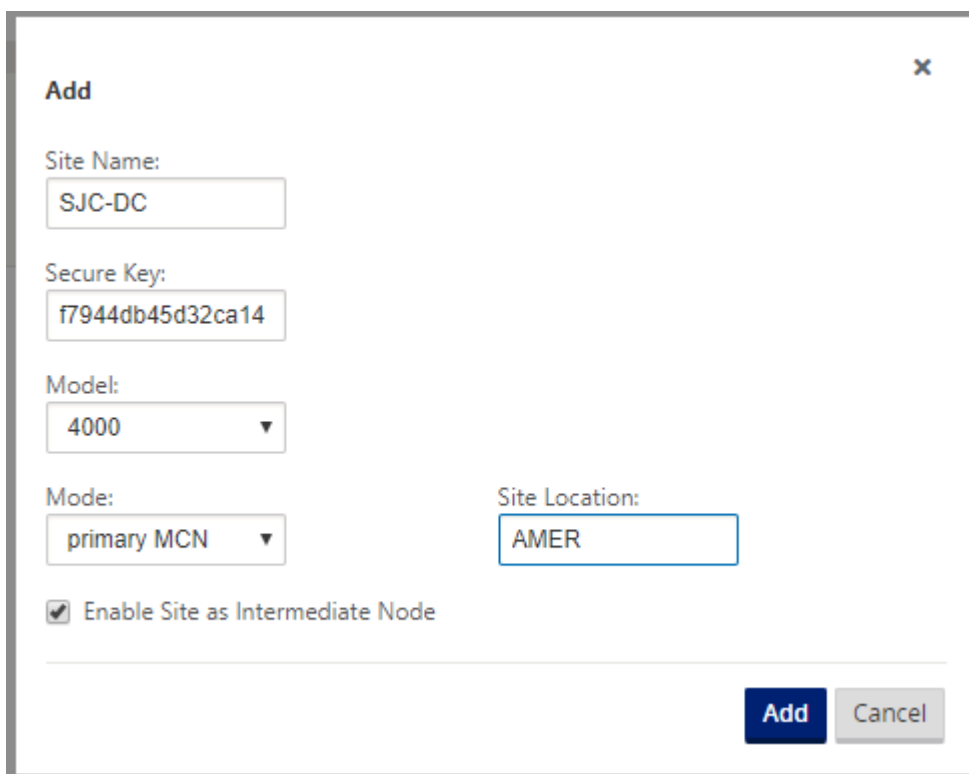
3. Démarrez la configuration en accédant à **Configuration > Virtual WAN > Configuration Editor**. Cliquez sur **Nouveau** pour commencer la configuration. Le fait de cliquer sur **Nouveau** crée un fichier de configuration initial dont le nom de fichier est **Untitled_1**. Vous pouvez renommer le fichier [ultérieurement] en utilisant le bouton **Enregistrer sous**.



Site du centre de données - configuration en mode virtuel en ligne

Créer un site de centre de données

1. Accédez à **Configuration > Virtual WAN > Configuration Editor > Sites**, puis cliquez sur **+ Site**.
2. Entrez le nom et l'emplacement du site. Choisissez le modèle d'appliance dans la liste déroulante **Modèle** et le **MCN principal** dans la liste déroulante **Mode**.
3. Cliquez sur **Ajouter**.



Add

Site Name:
SJC-DC

Secure Key:
f7944db45d32ca14

Model:
4000

Mode:
primary MCN

Site Location:
AMER

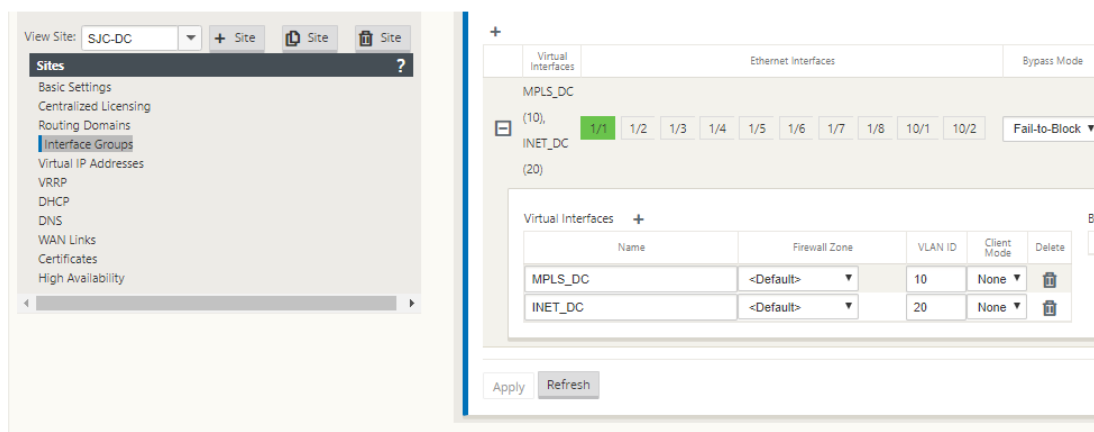
☒ Enable Site as Intermediate Node

Add **Cancel**

Configurer des groupes d'interfaces basés sur des interfaces Ethernet connectées

Dans la configuration en mode virtuel en ligne, une seule interface Ethernet est utilisée, c'est-à-dire l'interface connectant le routeur en amont, ce qui implique la stratégie de routage (Exemple-Interface 1/5). Le mode de contournement est défini sur Fail-to-Block (FTB) car une seule interface Ethernet/physique est utilisée par interface virtuelle. De plus, il n'y a pas de paires de ponts.

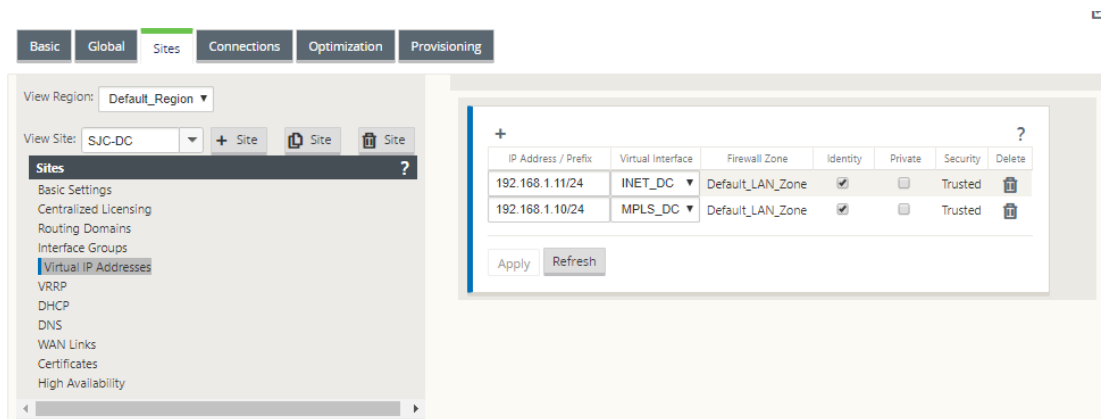
1. Dans l'**éditeur de configuration**, accédez à **Sites > [Nom du site] > Groupes d'interface**. Cliquez sur **+** pour ajouter des interfaces destinées à être utilisées.
2. Sélectionnez l'interface Ethernet qui est connectée au routeur en amont et cliquez sur **+** en regard de Interfaces virtuelles. Ajoutez les interfaces virtuelles pour les liens MPLS et INTERNET. Selon l'exemple de topologie, ajoutez les éléments suivants :
 - Interface virtuelle **MPLS** configurée sur **VLAN 10**
 - Interface virtuelle **INTERNET** configurée sur **VLAN 20**
3. Sélectionnez **Échec du blocage** dans la liste déroulante **Mode de contournement**. Cliquez sur **Apply**.



Créer une adresse IP virtuelle pour chaque interface virtuelle

Créez une adresse IP virtuelle (VIP) sur le sous-réseau approprié pour chaque lien WAN. Les VIP sont utilisés pour la communication entre deux appliances SD-WAN dans l'environnement Virtual WAN.

1. Dans l'**éditeur de configuration**, accédez à **Sites > [Nom du site] > Adresses IP virtuelles**. Cliquez sur **+** pour créer des VIP.
2. Entrez l'adresse IP/le préfixe et sélectionnez l'interface virtuelle correspondante pour MPLS et Internet.
3. Cliquez sur **Apply**.



Créer un lien Internet WAN

Créez une liaison WAN Internet basée sur le débit physique et non sur la vitesse de rafale.

1. Dans l'**éditeur de configuration**, accédez à **Sites > [Nom du site] > Liens WAN**, puis cliquez sur **+ Lien**. Entrez un nom et sélectionnez **Type d'accès** comme **Internet public**. Cliquez sur **Ajouter**.

2. Saisissez le tarif physique. Ne cochez pas la case **Détection automatique des adresses IP publiques**. Pour l'apppliance SD-WAN configurée en tant que MCN, la case à cocher **Détection automatique des adresses IP publiques** ne peut pas être activée.

WAN Link: SJC-DC-INET Section: Settings + Add Link Delete Link

Basic Settings

Link Name: SJC-DC-INET

Access Type: Public Internet WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 20000

☒ Set Permitted From Physical

Permitted Rate (kbps): 20000

WAN to LAN

Physical Rate (kbps): 20000

☒ Set Permitted From Physical

Permitted Rate (kbps): 20000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Advanced Settings

Eligibility

Metered/Standby Link

Provisioning

Apply Revert

3. Sélectionnez **Interfaces d'accès** dans la liste déroulante **Section** et cliquez sur le bouton **+** pour ajouter des détails d'interface spécifiques au lien Internet.
4. Entrez l'adresse IP virtuelle et l'adresse de la passerelle Internet WAN. L'ARP du proxy n'est pas vérifié pour moins de deux interfaces Ethernet.

5. Cliquez sur **Apply**.

WAN Link: SJC-DC-INET ▼

Section: Access Interfaces ▼

+ Add Link

Delete Link

+

?

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
SJC-DC-INET-AI-1	INET_DC ▼	192.168.1.11	192.168.1.1	Primary ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Apply

Refresh

Créer un lien MPLS

1. Dans la page **Sites [Nom du site] > > Liens WAN**, sélectionnez **Paramètres** dans la liste déroulante **Section** . Cliquez sur le **bouton+Lien** pour ajouter une liaison WAN pour MPLS.
2. Entrez le nom de la liaison WAN MPLS et sélectionnez **Type d'accès** en tant qu'**intranet privé**. Cliquez sur **Ajouter**.
3. Saisissez le tarif physique et d'autres détails. Cliquez sur **Apply**.

Basic Settings

LAN to WAN

Physical Rate (kbps):
100000

☒ Set Permitted From Physical

Permitted Rate (kbps):
100000

WAN to LAN

Physical Rate (kbps):
100000

☒ Set Permitted From Physical

Permitted Rate (kbps):
100000

Access Type:

Private Intranet

☐ Autodetect Public IP

Public IP Address:

Tracking IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
SJC-DC-MPLS-A...	MPLS_DC	192.168.1.10	192.168.1.9	Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

- Sélectionnez **Interfaces d'accès** dans la liste déroulante **Section** et cliquez sur le bouton **+** pour ajouter des détails d'interface spécifiques au lien MPLS.
- Entrez l'adresse IP virtuelle MPLS et l'adresse de la passerelle. L'ARP du proxy n'est pas vérifié pour moins de deux interfaces Ethernet.
- Cliquez sur **Apply**.

WAN Link: SJC-DC-MPLS

Section: Access Interfaces (IPv4)

+ Link

Link

Remplissez les itinéraires

Du côté du centre de données, ajoutez une route sur l’appliance SD-WAN sur la façon d’atteindre les sous-réseaux LAN (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc.) via l’une des interfaces physiques.

0/1/0.1 —192.168.1.1 sur VLAN 10

0/1/0.2 —192.168.2.1 sur VLAN 20

Dans cet exemple, l’interface 192.168.1.1 est utilisée.

Dans l’**éditeur de configuration**, accédez à **Connexions > Routes**, puis cliquez sur **+** pour ajouter les itinéraires.

Entrez l’**adresse IP réseau**, le **coût** et l’**adresse de la passerelle**. Cliquez sur **Ajouter**.

Edit?×

Network IP Address

10.10.11.0/24

Routing Domain

Default_RoutingI ▾

Cost

5

Service Type

Local ▾

Gateway IP Address

192.168.1.1

☒ Export Route

☐ Summary Route

☐ Eligibility Based On Path

Path:

<None> ▾

☐ Eligibility Based On Gateway

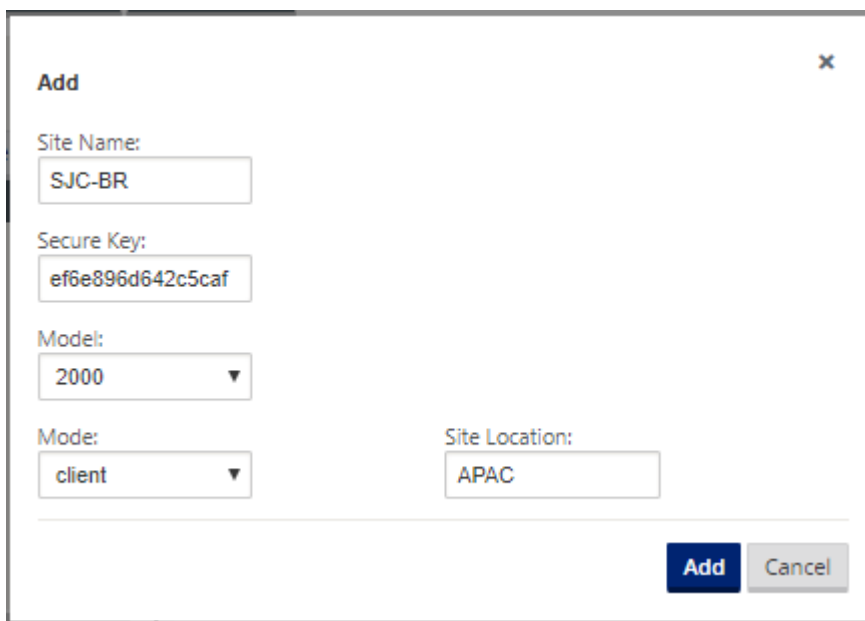
Apply

Cancel

Configuration du déploiement en ligne du site de succursale

Créer un site de succursale

1. Accédez à **Configuration Editor > Sites**, puis cliquez sur **+ Site**.
2. Entrez le nom et l'emplacement du site. Choisissez le modèle d'appliance dans la liste déroulante **Modèle** et **Client** dans la liste déroulante **Mode**.
3. Cliquez sur **Ajouter**.



Add

Site Name:
SJC-BR

Secure Key:
ef6e896d642c5caf

Model:
2000

Mode:
client

Site Location:
APAC

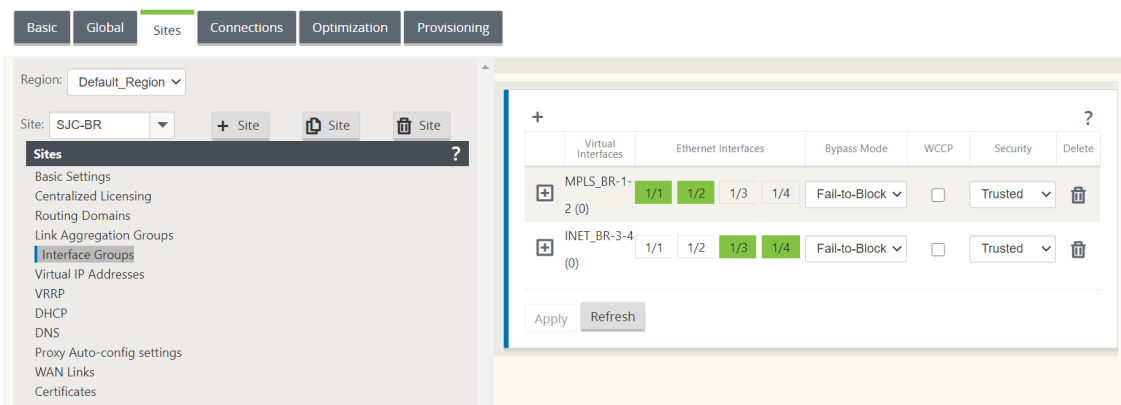
Add **Cancel**

Configurer des groupes d'interfaces basés sur des interfaces Ethernet connectées

1. Dans l'**éditeur de configuration**, accédez à **Sites > [Nom du site client] > Groupes d'interface**. Cliquez sur **+** pour ajouter des interfaces destinées à être utilisées. Pour la configuration en mode Inline, quatre interfaces Ethernet sont utilisées ; les paires d'interfaces 1/3, 1/4 et les paires d'interfaces 1/1 et 1/2.
2. Définissez le **mode de contournement** sur Fail-to-Wire, car deux interfaces Ethernet/physiques sont utilisées par interface virtuelle. Il y a deux paires de ponts.
3. Cliquez sur **+** en regard de **Virtual Interfaces** (Interfaces virtuelles) et remplissez les liens WAN en fonction du débit physique et non des vitesses de rafale à l'aide de liens Internet et MPLS.
 - Interface virtuelle **INTERNET** configurée sur la paire de ponts 1/3 et 1/4
 - Interface virtuelle **MPLS** configurée sur Bridge Pair 1/1 et 1/2.

4. Cliquez sur **+** en regard de **Paires de ponts** et créez la paire de ponts en sélectionnant les interfaces appropriées.

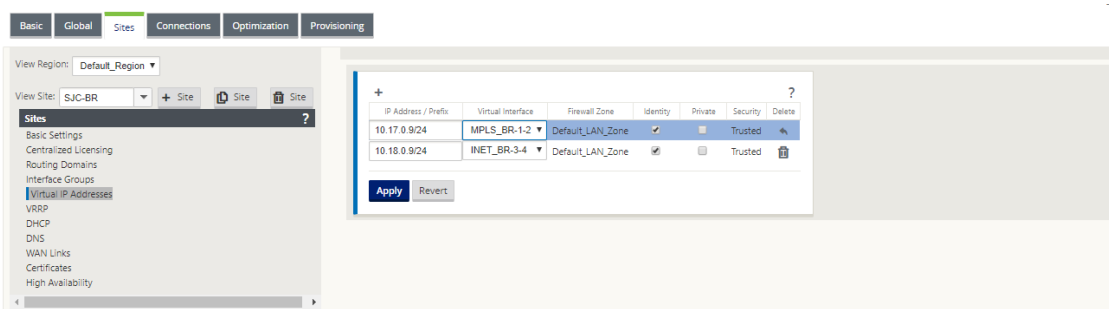
Reportez-vous au diagramme **Topologie de branche —topologie en mode en ligne** sous la section [Prérequis](#) et renseignez les groupes d'interface.



Créer une adresse IP virtuelle (VIP) pour chaque interface virtuelle

Créez une adresse IP virtuelle sur le sous-réseau approprié pour chaque liaison WAN. Les VIP sont utilisés pour la communication entre deux appliances SD-WAN dans l'environnement Virtual WAN.

1. Dans l'**éditeur de configuration**, accédez à **Sites > [Nom du site] > Adresses IP virtuelles**. Cliquez sur **+** pour créer des VIP.
2. Entrez l'adresse IP/le préfixe et sélectionnez l'interface virtuelle correspondante pour MPLS et Internet.
3. Cliquez sur **Apply**.



Créer un lien Internet WAN

Pour remplir les liens WAN en fonction du débit physique et non de la vitesse de rafale à l'aide d'un lien Internet

1. Accédez à **Liens WAN**, cliquez sur le **bouton+Lien** pour ajouter un lien WAN pour le lien Internet. Entrez un nom et sélectionnez **Type d'accès** comme **Internet public**. Cliquez sur **Ajouter**.
2. Renseignez les détails du lien Internet et activez la case à cocher **Détection automatique de l'adresse IP publique**.
3. Sélectionnez **Interfaces d'accès** dans la liste déroulante **Section** et cliquez sur le **signe +** pour ajouter des détails d'interface spécifiques au lien Internet.
4. Entrez l'adresse IP virtuelle et l'adresse de la passerelle Internet WAN. L'ARP du proxy n'est pas vérifié pour moins de deux interfaces Ethernet.

The screenshot displays the Citrix SD-WAN configuration interface. At the top, the 'WAN Link' is set to 'SJC-BR-INET' and the 'Section' is 'Settings'. There are buttons for '+ Add Link' and 'Delete Link'.

The main configuration area is titled 'Basic Settings'. It includes a note: 'Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.' Below this, the 'Link Name' is 'SJC-BR-INET'. The 'Access Type' is 'Public Internet' and the 'WAN Link Template' is '<None>'. There are two sections for 'LAN to WAN' and 'WAN to LAN' settings, each with 'Physical Rate (kbps)' and 'Permitted Rate (kbps)' set to 2000, and checkboxes for 'Set Permitted From Physical' (checked) and 'Auto Learn' (unchecked). A 'Tracking IP Address' field is present. The 'Autodetect Public IP' checkbox is checked, and a 'Public IP Address' field is shown.

At the bottom, there is a navigation bar with tabs: 'Basic', 'Global', 'Sites', 'Connections', 'Optimization', and 'Provisioning'. The 'Sites' tab is selected, showing a 'View Region' dropdown set to 'Default_Region'. Below this, there is a 'View Site' dropdown set to 'SJC-BR' and buttons for '+ Site', 'Site', and 'Site'. A list of sites is shown, including 'Basic Settings', 'Centralized Licensing', 'Routing Domains', 'Interface Groups', 'Virtual IP Addresses', 'VRRP', 'DHCP', 'DNS', 'WAN Links', 'Certificates', and 'High Availability'.

On the right, a table lists virtual interfaces:

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.17.0.9/24	MPLS_BR-1-2	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
10.18.0.9/24	INET_BR-3-4	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	

Buttons for 'Apply' and 'Revert' are at the bottom of the table.

Créer une liaison WAN MPLS

1. Accédez à **Liens WAN** et sélectionnez **Paramètres** dans la liste déroulante **Section** . Cliquez sur le **bouton+Lien** pour ajouter une liaison WAN pour le lien MPLS.
2. Entrez le nom de la liaison WAN MPLS et d'autres détails. Sélectionnez **Type d'accès** en tant qu'**intranet privé**.

WAN Link: **SJC-BR-MPLS** Section: **Settings** **+ Add Link** **Delete Link**

Basic Settings ?

Link Name: **SJC-BR-MPLS**

Access Type: **Private MPLS** WAN Link Template: **<None>**

LAN to WAN

Physical Rate (kbps): **10000**

☒ Set Permitted From Physical

Permitted Rate (kbps): **10000**

WAN to LAN

Physical Rate (kbps): **10000**

☒ Set Permitted From Physical

Permitted Rate (kbps): **10000**

MPLS Queues **+ Add** ?

Advanced Settings ?

Metered/Standby Link ?

Provisioning ?

Apply **Revert**

3. Sélectionnez **Interfaces d'accès** dans la liste déroulante **Section** et cliquez sur le **bouton+** pour ajouter des détails d'interface spécifiques au lien MPLS.
4. Entrez l'adresse IP virtuelle MPLS et l'adresse de la passerelle. L'ARP du proxy n'est pas vérifié pour moins de deux interfaces Ethernet.

WAN Link: SJC-BR-MPLS Section: Access Interfaces + Add Link Delete Link

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
SJC-BR-MPLS-AI-1	MPLS_BR-1-2	10.17.0.9	10.17.0.1	Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Apply Revert

Remplissez les itinéraires

Les itinéraires sont créés automatiquement en fonction de la configuration précédente. S'il existe d'autres sous-réseaux spécifiques à cette succursale distante, des routes spécifiques doivent être ajoutées pour identifier la passerelle pour diriger le trafic vers ces sous-réseaux back-end.

Créer des groupes Autopath

1. Dans l'**éditeur de configuration**, accédez à **Global > Autopath Groups**. Cliquez sur **+**.
2. Entrez un nom et cliquez sur **Appliquer**.
3. Configurez le groupe Autopath en fonction de vos besoins, puis cliquez sur **Apply**.

Global ?

- Network Settings
- Regions
- Centralized Licensing
- Routing Domains
- Applications
- Firewall Zones
- Firewall Policy Templates
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- Autopath Groups**
- Service Providers
- WAN-to-WAN Forwarding Groups
- WAN-to-WAN Forwarding Groups

+ Edit Delete

Name	Edit	Delete
Default_Group		
MPLS		

Apply Refresh

Edit

☒ Set as Default

IP DSCP Tagging: Any

Bad Loss Sensitive: Enable (Default)

Silence Period (ms): DEFAULT

Path Probation Period (ms): 10000 (Default)

☒ Instability Sensitive

Apply Cancel

4. Accédez à **Connexions > Liaisons WAN**. Sélectionnez le lien Internet **WAN** dans la liste déroulante **Liens WAN** et **Chemins virtuels** dans la liste déroulante **Section**.
5. Activez la case à cocher **Utiliser** et choisissez le groupe de chemins d'accès automatique nouvellement créé dans la case à cocher **Groupe de chemins automatiques** pour les liens WAN Intranet sur les sites respectifs (centre de données et succursale).

Aucun groupe de chemin automatique ne peut être marqué par défaut. Si cette option est cochée, cela entraînerait une erreur d'audit.

Virtual Path Service	Use	Tunnel Header Size (Bytes)	Active MTU Detect	UDP Port	UDP Hole Punching	Enable	Alt Port	Interval (min)	Autopath Group
SJC_DC-SJC-BR	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	4980	<input type="checkbox"/>	<input type="checkbox"/>		1440	<None>

Apply Revert

Après avoir ajouté manuellement les chemins virtuels des liens WAN avec le type d'accès en tant qu'**intranet privé**, les chemins virtuels sont renseignés sous **Chemins**.

Une fois toutes les étapes précédentes terminées, passez à la section [Préparation des packages de l'appliance SD-WAN](#).

Résolution des erreurs d'audit

Une fois la configuration des sites de centre de données et de succursale terminée, vous serez averti pour résoudre les erreurs d'audit sur les sites DC et BR. Réglez les erreurs d'audit (le cas échéant).

Créer un réseau SD-WAN

May 6, 2021

Pour créer un réseau de superposition SD-WAN sans avoir besoin de créer des tables de routage de superposition SD-WAN :

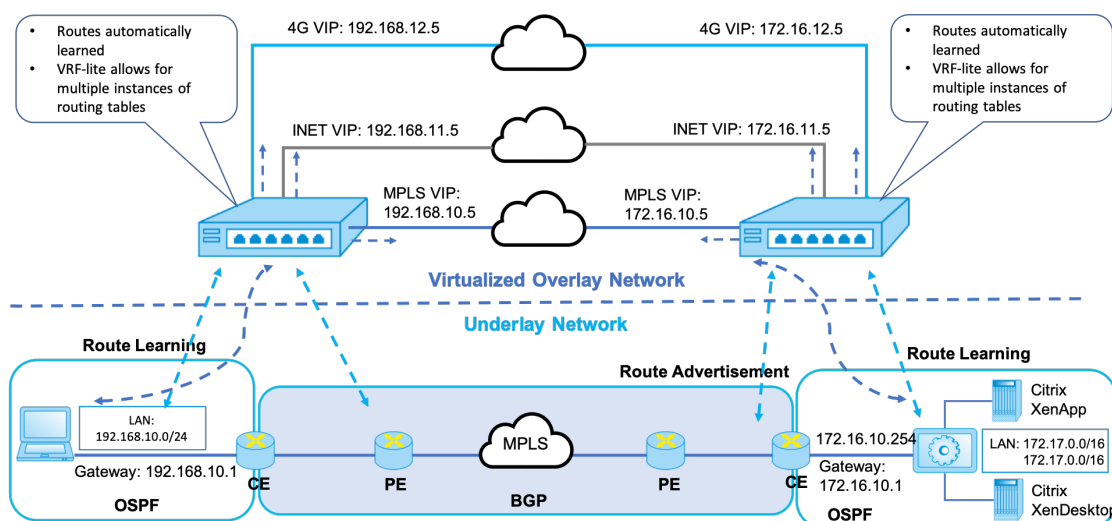
1. Créez un tunnel WAN Path sur chaque liaison WAN entre deux appliances SD-WAN.
2. Configurez Virtual IP pour représenter le point de terminaison de chaque liaison WAN. Vous pouvez établir des chemins WAN chiffrés via le réseau L3 actuel.
3. Agrégez les chemins WAN 2, 3 et 4 (liens physiques) en un seul chemin virtuel permettant aux paquets de traverser le WAN en utilisant le réseau de superposition SD-WAN au lieu de la sous-couche existante, ce qui est le moins intelligent et peu coûteux.

Composants de routage SD-WAN et topologie réseau

- Local —le sous-réseau réside sur ce site (annoncé dans l'environnement SD-WAN)
- Chemin d'accès virtuel : envoyé via Chemin d'accès virtualisé vers l'appliance de site sélectionnée

- Intranet —sites sans dispositif SD-WAN
- Internet —trafic lié à Internet
- Pass-through —trafic intact, dans une interface de pont hors de l'autre
- Route par défaut (0.0.0.0/0) définie - Utilisé pour le trafic pass-through non capturé par la table de routage de superposition SD-WAN, ou utilisé au niveau du MCN pour demander aux sites clients de transférer tout le trafic vers le nœud MCN pour le back-haul du trafic Internet.

SD-WAN overlay dynamic network routing



Optimisation WAN uniquement avec l'édition Premium (Enterprise)

May 6, 2021

Les appliances SD-WAN Premium (Enterprise) Edition contiennent des fonctionnalités complètes d'optimisation WAN en plus de la virtualisation WAN. Certains clients préfèrent implémenter la fonctionnalité d'optimisation WAN avant de migrer vers les services SD-WAN. Ce cas d'utilisation de déploiement fournit les étapes à suivre pour utiliser les appliances Premium Edition pour utiliser les services d'optimisation WAN.

Les éditions Citrix SD-WAN Product Platform incluent les appliances suivantes :

- SD-WAN : Dispositif SD-WAN Standard Edition
- Premium (Entreprise) : appliance SD-WAN Édition Premium
- WANOP : Appliance SD-WAN WANOP Edition

Pour intégrer des appliances Premium (Enterprise) Edition dans un réseau WANOP distribué existant, vous pouvez configurer l'appliance SD-WAN (physique ou virtuel) sur le site DC en tant que MCN. L'appliance SD-WAN gère toute la configuration du réseau. Un chemin virtuel est établi entre le site de la succursale et le MCN sur le site de DC. Ce chemin virtuel est utilisé uniquement pour l'envoi de trafic de contrôle entre les appliances. Au niveau de l'appliance de succursale, le trafic de données est traité en tant que service intranet. Le trafic intranet n'est pas encapsulé et traverse la liaison WAN existante pour atteindre le site DC. Une appliance WANOP sur le site de contrôleur de domaine doit se trouver dans le chemin de trafic afin d'optimiser le trafic de bout en bout.

Pour les sites clients qui ne disposent pas de matériel SD-WAN en tête de ligne, les appliances VPX d'une paire HA (deux VPX virtuels WAN) peuvent être utilisées comme MCN en mode monobras. Pour le mode monobras, des règles PBR sur le routeur tiers sont nécessaires pour rediriger le trafic vers l'appliance SD-WAN.

Ce document suppose que les appliances de site de contrôleur de domaine sont déployées en mode HA à des fins de redondance. Le mode HA n'est pas obligatoire pour ce déploiement.

Conditions préalables

- Une paire d'appliances WANOP et une paire d'appliances SD-WAN déployées en mode HA sur le site DC.
- Une appliance Édition Premium sur le site de la succursale.

Topologie réseau

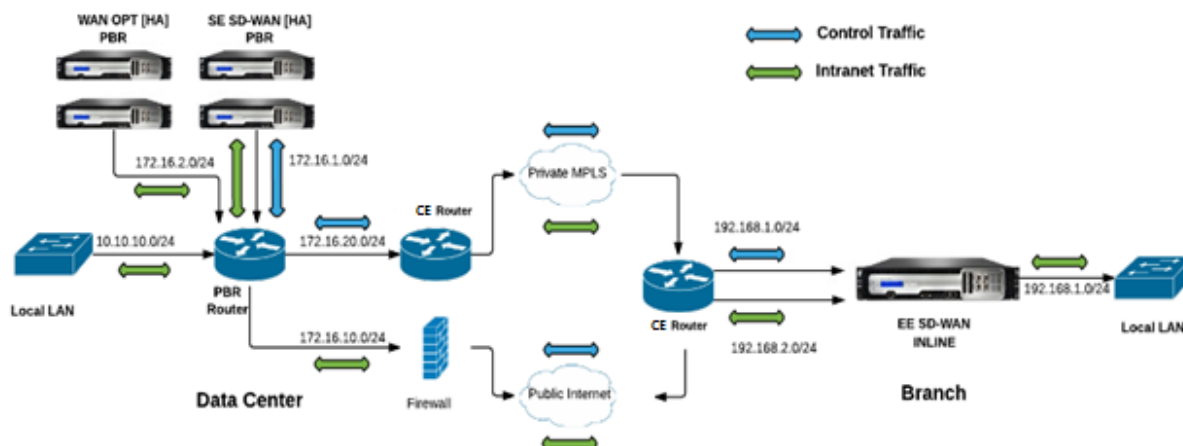
Appliances SD-WAN Standard Edition et WANOP dans le déploiement PBR :

Dans l'illustration ci-dessous, les appliances SD-WAN SE et WAN OP sur le site DC sont déployées en mode à un bras. L'appliance SD-WAN prend en charge le déploiement PBR tandis que l'appliance WANOP prend en charge à la fois PBR et WCCP. Le trafic de contrôle (trafic de chemin virtuel) reçu du WAN sur le site DC est redirigé vers l'appliance SD-WAN par le routeur PBR. Le trafic de données est redirigé vers l'appliance WAN Optimization par le routeur PBR.

Flux de trafic pour le réseau WAN vers le réseau local DC :

- Routeur CE (Customer Edge) -> Routeur PBR -> SD-WAN -> Routeur PBR -> LAN
- Routeur CE (Customer Edge) -> Routeur PBR -> WAN OPT -> Routeur PBR -> LAN

Le même flux de circulation est suivi dans le sens inverse.



SD-WAN Standard Edition en mode PBR et WANOP en déploiement en ligne :

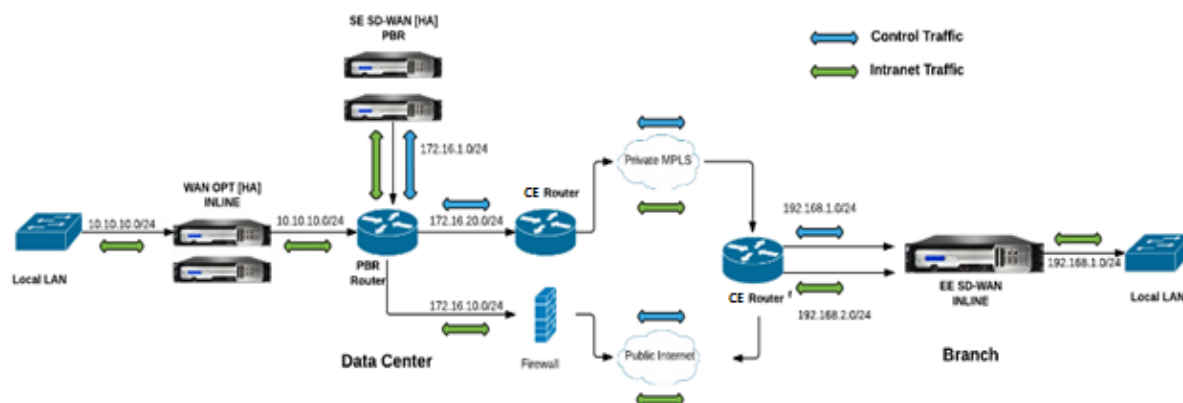
Dans l'illustration ci-dessous, l'appliance SD-WAN sur le site DC est déployée en mode à un bras tandis que l'appliance WANOP est déployée en mode Inline.

Le trafic de contrôle (trafic de chemin virtuel) reçu du WAN sur le site DC est redirigé vers l'appliance SD-WAN par le routeur PBR. Le trafic de données est transféré à l'appliance WAN Optimization (en ligne) par le routeur PBR.

Flux de trafic pour le réseau WAN vers le réseau local DC :

- Routeur CE (Customer Edge) -> Routeur PBR -> SD-WAN -> Routeur PBR -> LAN
- Routeur CE (Customer Edge) -> Routeur PBR -> WAN OPT -> LAN

Le même flux de circulation est suivi dans le sens inverse.



Étapes de configuration

1. Configurez l'appliance SD-WAN au DC [MCN] pour établir des chemins virtuels entre les sites DC et Branch.

Consultez [configuration du service de chemin d'accès virtuel entre MCN et clients](#).

2. Configurez le service Intranet sur le site DC.

- a) Sur le site MCN (DC), accédez à **Configuration > Réseau étendu virtuel > Éditeur de configuration > Connexions > Site (DC) > Services Intranet**. Cliquez sur le **[signe+]** pour ajouter un service Intranet.
- b) Sélectionnez une ou plusieurs liaisons WAN pour le **service Intranet**, puis cliquez sur **Appliquer**.
- c) Accédez à Itinéraires sous le même **site (DC)**, cliquez sur **[signe+]** Signer pour ajouter le réseau distant dont le coût est inférieur à 5, puis sélectionnez **Ajouter**.

Par exemple, - Entrez **192.168.1.0/24** dans le champ **Adresse IP réseau** avec le coût 4 et sélectionnez **Type de service** comme **Intranet**.

Remarque

Le coût de chaque site doit être inférieur à 5 pour que l'itinéraire intranet ait priorité.

3. Configurez le service Intranet sur le site Branch.

- a) Répétez les sous-étapes a à c de **l'étape 2** ci-dessus sur le site Branch.

Par exemple, - Entrez **172.16.1.0/24** dans le champ Adresse IP réseau avec le coût 4 et sélectionnez **Type de service** comme **Intranet**.

4. Exécutez **la gestion des modifications** pour télécharger et distribuer la configuration sur le site Branch.

Voyez, [Exportation du package de configuration et de la gestion des modifications](#)

Par défaut, le trafic est envoyé de Branch à DC via le chemin virtuel.

Remarque

Le routeur PBR doit être configuré pour rediriger le trafic conformément aux étapes de déploiement fournies.

Pour plus d'informations sur la configuration de l'optimisation WAN, reportez-vous à : [Activation de la configuration-optimisation du WAN](#).

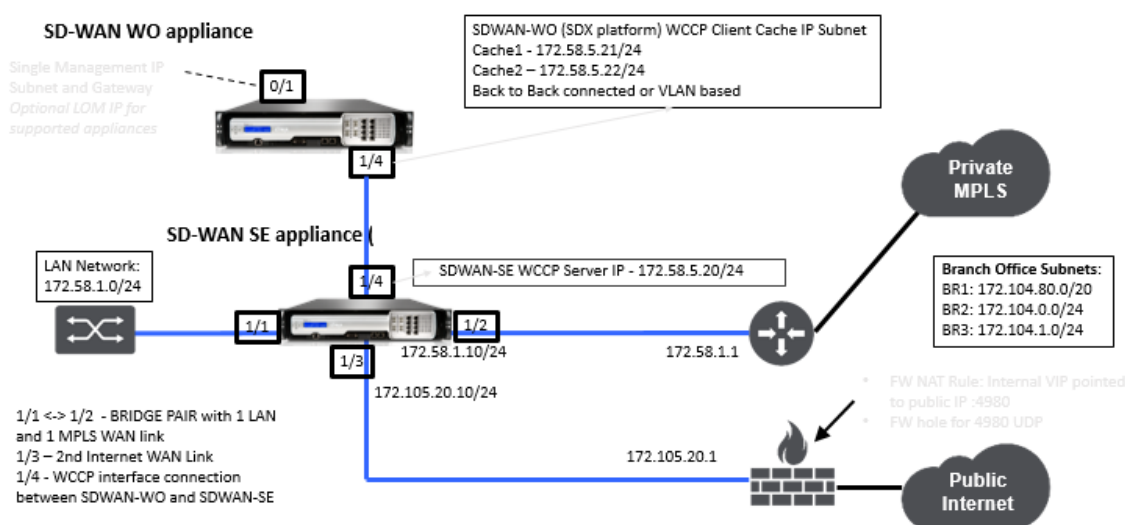
Mode deux boîtes

May 6, 2021

Le mode à deux boîtes est un déploiement basé sur un bras WCCP où l'apppliance SD-WAN SE agit comme un routeur WCCP et les appliances SDWAN-WANOP (4000/5000) agissent comme des clients WCCP et aident à établir la convergence WCCP. De cette façon, tous les paquets TCP orientés chemin virtuel/service Intranet atteignant l'apppliance SD-WAN SE sont redirigés vers l'apppliance SDWAN-WANOP pour optimiser les avantages en offrant à la fois des avantages SD-WAN SE et WANOP pour le trafic client.

Le mode Two Box n'est pris en charge que sur les modèles d'apppliance suivants :

- Appareils SD-WAN SE —4000, 4100 et 5100
- Appareils WANOP SD-WAN —4000, 4100, 5000 et 5100



Remarque

Les modes de déploiement haute disponibilité et WCCP ne sont pas accessibles lorsque le mode Two Box est activé. Toutefois, ces modes de déploiement sont disponibles pour l'utilisateur à administrer.

Important

- Bien que le déploiement WCCP hérité soit désactivé lorsque le mode à deux boîtes est activé, la convergence du groupe de services peut uniquement être vérifiée à partir de la page de surveillance WCCP. Il n'y a pas de page d'interface graphique séparée sous la section Surveillance pour le mode Two Box.
- Si le processus WCCP exécuté sur l'apppliance Standard Edition redémarre plusieurs fois dans un court laps de temps, par exemple, 3 fois par minute, le groupe de services s'arrête automatiquement. Dans un tel scénario, pour obtenir la convergence WCCP sur l'apppliance WANOP, réactivez la fonctionnalité WCCP dans l'interface graphique Web de l'apppliance WANOP.

- En cas de modification de la configuration WCCP ou de l'optimisation WAN liée à la configuration sur l'appliance Standard Edition, l'appliance WANOP externe redémarre. Par exemple, l'activation/désactivation de la case à cocher WCCP dans le groupe d'interface de l'éditeur de configuration suivi du processus de gestion des modifications redémarre également l'appliance WANOP.

Remarque

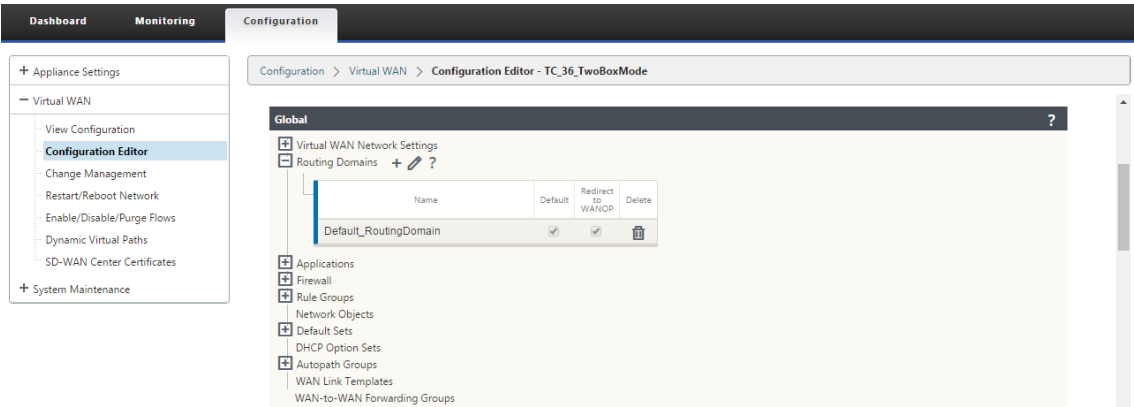
Notez également les points suivants à prendre en compte lors de l'implémentation du mode deux boîtes :

- Lorsqu'un domaine de routage est sélectionné pour être redirigé vers l'appliance WANOP à partir de l'éditeur de configuration, il doit être ajouté dans le groupe d'interface pour lequel WCCP est activé.
- Le trafic du même domaine de routage doit également être sélectionné sur le site partenaire. Par exemple, **MCN > Branch01** pour observer les avantages de l'optimisation WAN.
- Si un domaine de routage est sélectionné dans le groupe d'interfaces sur lequel WCCP est activé, un autre groupe d'interfaces contenant les interfaces pontées doit avoir le même domaine de routage configuré. Seulement si le domaine de routage est configuré pour le groupe d'interface WCCP, il ne suffit pas de transmettre le trafic de bout en bout qui coule avec les avantages d'optimisation WAN.

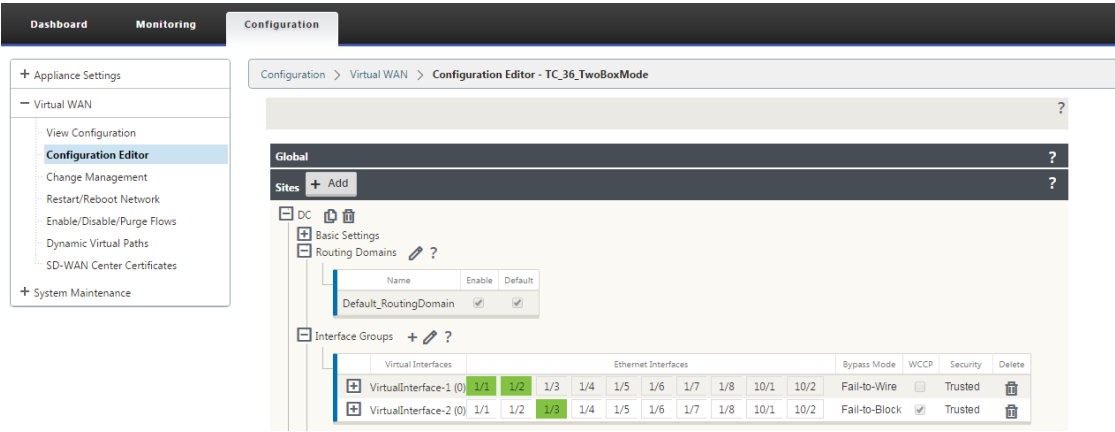
Citrix SD-WAN édition standard

Pour configurer la solution en mode deux boîtes dans l'appliance Standard Edition sur le site DC ou Branch :

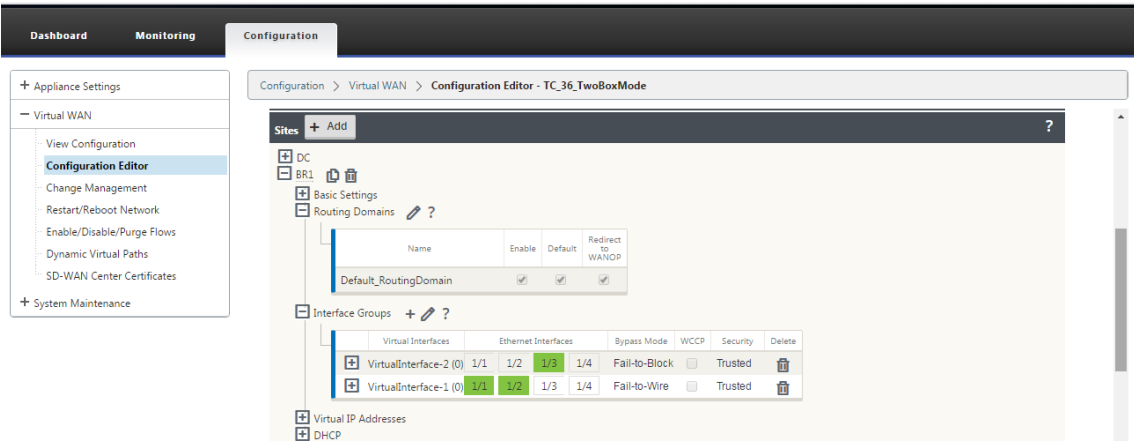
1. Dans l'interface de gestion Web SD-WAN SE, accédez à **Configuration > Réseau étendu virtuel > Éditeur de configuration** . Ouvrez un package de configuration existant ou créez un package.
2. Dans le package de configuration choisi, accédez à l'onglet **Avancé** pour afficher les détails de configuration.
3. Ouvrez les paramètres **globaux** et développez **Domaines de routage** pour afficher que la case **Rediriger vers WANOP** est activée.



4. Développez contrôleur de domaine pour activer **WCCP** pour l'**interface virtuelle** sous Paramètres **du groupe d'interface** qui indiquent l'interface réseau virtuelle pour laquelle l'appliance est activée.



5. Développez **Sites+ Ajouter** pour afficher les paramètres du domaine de routage Branch et du groupe d'interface. Sous le site Branch, la case **Rediriger vers WANOP** est activée pour les domaines de routage.



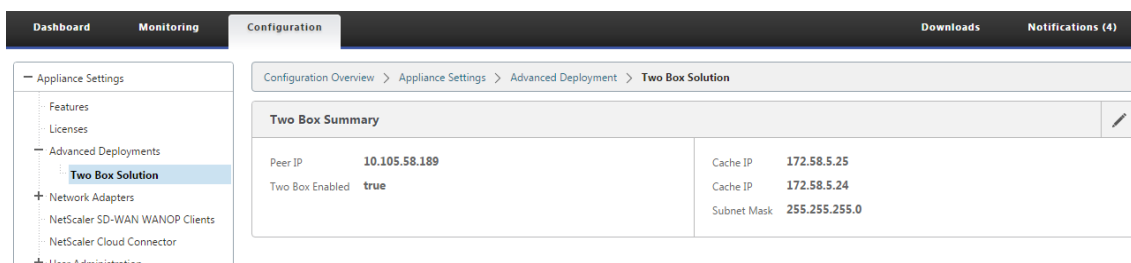
Remarque

L'écouteur WCCP ne doit être activé que pour les interfaces réseau virtuelles qui ont une seule interface Ethernet configurée. N'activez pas l'écouteur WCCP sur une paire BRIDGED. Il est destiné à être activé sur l'interface ONE-ARM entre les appliances SD-WAN SE et SD-WAN WANOP.

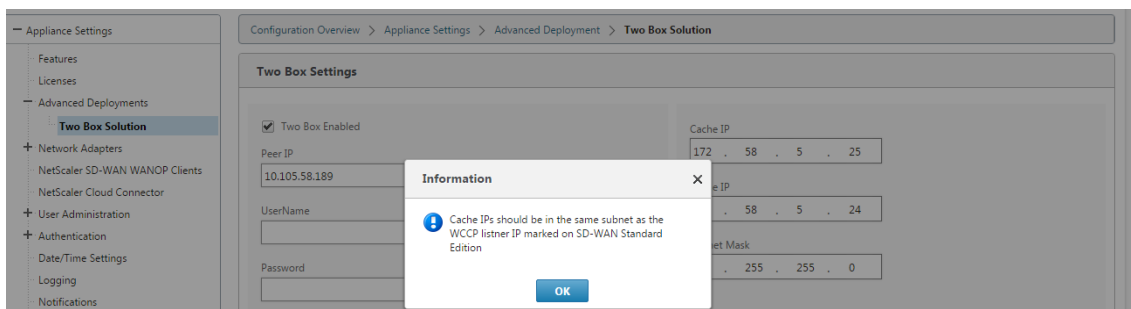
Configuration de Citrix SD-WAN WANOP

Pour configurer le mode de déploiement à deux boîtes dans l'interface graphique Web de l'appliance WANOP SD-WAN :

1. Dans l'interface de gestion Web WANOP SD-WAN, accédez à **Configuration > Paramètres de l'appliance > Déploiements avancés > Solution à deux boîtes**.



2. Cliquez sur l'icône **Modifier** pour modifier les deux paramètres du mode boîte. La boîte de dialogue d'informations sur **les adresses IP de cache** s'affiche. Cliquez sur **OK**.



3. Activez la **case à cocher Deux cases activées**.
4. Entrez l'**adresse IP homologue**. L'adresse IP homologue est l'adresse IP de l'appliance SD-WAN Standard Edition.
5. Entrez les informations d'identification de l'utilisateur et cliquez sur **Appliquer**.

Two Box Settings

☒ Two Box Enabled

Peer IP

UserName

Password

Cache IP

Cache IP

Subnet Mask

Apply

Cancel

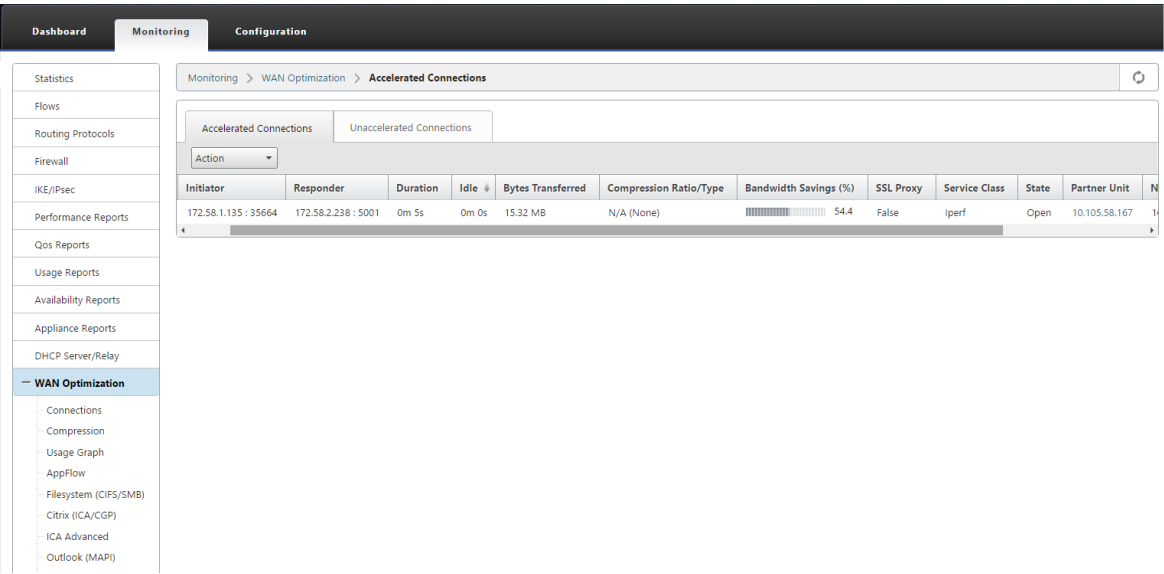
Configuration et facilité de gestion en deux modes boîte

Voici quelques-uns des deux points de configuration en mode boîte et de gérabilité à prendre en compte pour le déploiement :

- Les configurations WANOP SD-WAN mentionnées ci-dessous peuvent être configurées à partir de l'éditeur de configuration SD-WAN SE en tant que volet unifié
 - CLASSE DE SERVICE
 - CLASSIFICATEUR D'APPLICATIONS
 - CARACTÉRISTIQUES
 - RÉGLAGE DU SYSTÈME

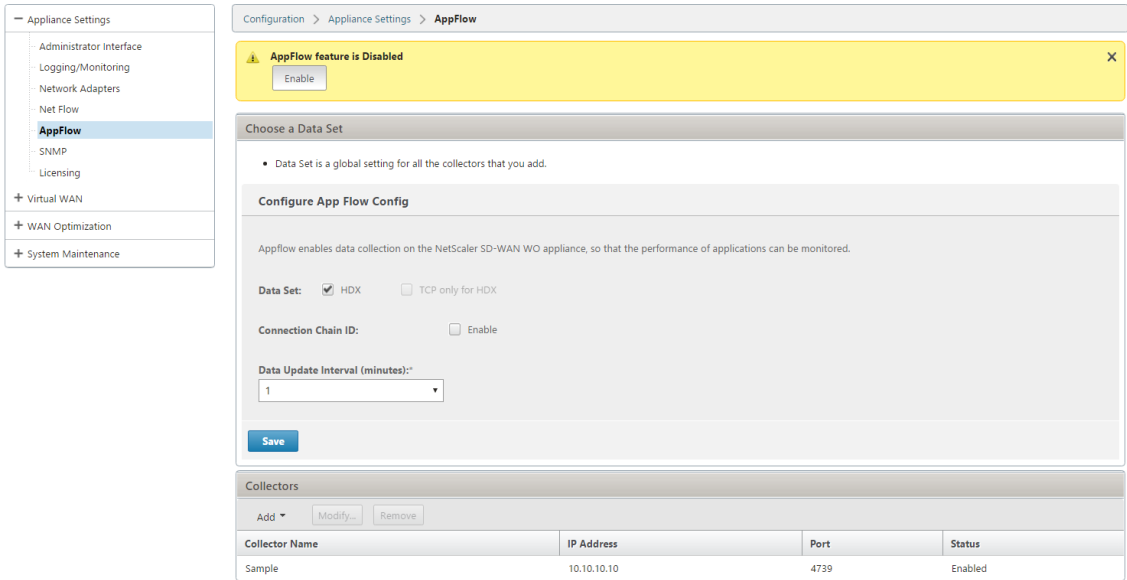
Surveillance

Vous pouvez surveiller le trafic WANOP SD-WAN directement à l'aide de la page Surveillance de l'interface utilisateur Web de l'appliance SD-WAN SE. Cela permet la surveillance d'un seul volet des appliances SDWAN-SE et SDWAN-WO lors du traitement du trafic de données. Vous pouvez afficher les détails de connexion, les détails du partenaire sécurisé, etc., sous le nœud d'optimisation WAN dans l'interface utilisateur SDWAN-SE.



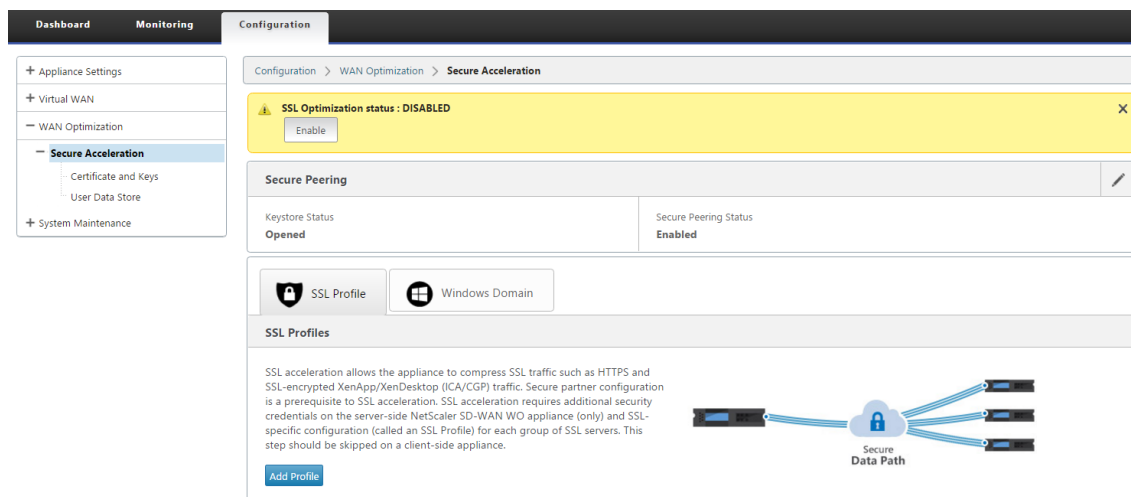
Configuration

Vous pouvez configurer APPFLOW directement à partir de la page **Configuration** SDWAN-SE sous le nœud **APPFLOW** . Cela permet à SDWAN-SE d’agir comme un seul volet pour la configuration d’ APPFLOW et d’autres attributs de configuration de traitement des données tels que la classe de service, les classificateurs d’applications. La configuration effectuée sur le SDWAN-SE reflète la configuration SDWAN-WO, en maintenant une prise en charge transparente des fonctionnalités APPFLOW.



Le WANOP SD-WAN déjà découvert par Citrix Application Delivery Management (ADM), s’il est utilisé en mode à deux boîtes, doit être isolé et non configuré à l’aide de Citrix ADM tant que ce mode n’est pas désactivé. En effet, la configuration de WANOP pour le traitement du trafic est gérée par l’appliance SD-WAN SE en mode Two Box.

Les optimisations avancées ou Secure Acceleration doivent être configurées directement sur l'appliance SDWAN-SE, comme nous le ferions sur l'appliance SDWAN-WO. Cela permet de maintenir un seul volet de configuration de configurations telles que la jointure de domaine ou l'accélération sécurisée/création de profil SSL pour les optimisations avancées ou le proxy SSL.



- Les licences doivent être gérées séparément pour chacune des appliances SD-WAN SE et SD-WAN WANOP.
- La mise à niveau logicielle doit être gérée séparément pour chacune des appliances SD-WAN SE et SD-WAN WANOP avec les packages logiciels respectifs. Par exemple, tar.gz pour SD-WAN SE et mise à niveau upg pour SD-WAN WANOP.
- L'intégration des chemins de données doit être configurée entre les appliances SD-WAN SE et WANOP externes via le mode de déploiement WCCP.
 - Au niveau du chemin de données, les fonctionnalités WCCP et Virtual WAN sont offertes par l'intégration de chemin de données entre WANOP et SE en externe en mode à un bras pour obtenir des avantages d'optimisation.

Configuration et surveillance unifiées

Lorsque vous activez le mode à deux boîtes avec les appliances SD-WAN SE et SDWAN-WANOP, vous pouvez afficher la configuration dans l'appliance SD-WAN SE de la même manière que vous pouvez afficher la configuration à deux boîtes avec l'appliance SD-WAN-EE.

1. Accédez à **Configuration > Réseau étendu virtuel > Optimisation du réseau étendu**
2. Nœud Appflow sous **Configuration > Paramètres de l'appliance**
3. Nœud d'optimisation WAN sous Configuration.

Ces informations sont redirigées à partir de l’appliance SD-WAN WANOP qui est en mode Deux boîtes avec l’appliance SD-WAN SE.

La configuration liée à WANOP, telle que SSL Acceleration et AppFlow, peut désormais être effectuée à partir de l’interface graphique Web SD-WAN SE.

Les statistiques relatives au trafic, telles que Connexions, Compression, CIFS/SMB, ICA Advanced, MAPI et partenaires, peuvent désormais être surveillées à partir de l’interface graphique Web SD-WAN SE sous **Monitoring > Optimisation WAN**, similaire à l’appliance SD-WAN Premium (Enterprise) edition.

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

- WAN Optimization

+ Secure Acceleration

+ System Maintenance

Configuration > WAN Optimization

SSL Optimization status : DISABLED

Enable

Secure Peering

Keystore Status

Opened

Secure Peering Status

Enabled

SSL Profile

Windows Domain

DashboardMonitoringConfiguration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Monitoring > Statistics

Statistics

Show: Paths (Summary) ☐ Enable Auto Refresh 5 seconds Refresh ☒ Show latest data.

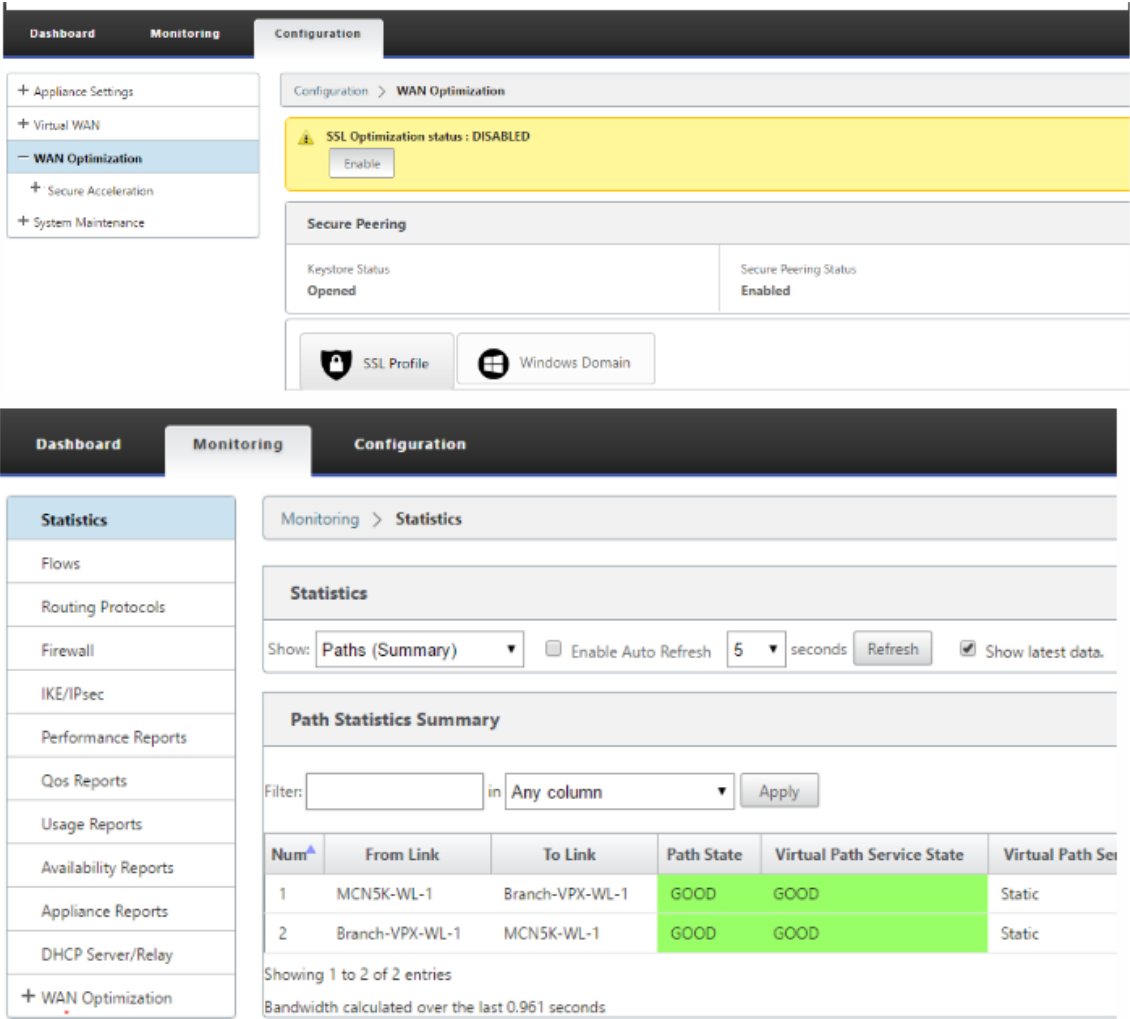
Path Statistics Summary

Filter: in Any column

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Ser
1	MCN5K-WL-1	Branch-VPX-WL-1	GOOD	GOOD	Static
2	Branch-VPX-WL-1	MCN5K-WL-1	GOOD	GOOD	Static

Showing 1 to 2 of 2 entries

Bandwidth calculated over the last 0.961 seconds



Changement d'adresse IP de gestion pour l'appliance WANOP SD-WAN en mode deux boîtes

Pour modifier l'adresse IP de gestion de l'appliance SDWAN-WANOP en mode Deux boîtes :

1. Exécutez la commande `clear_wo_sync` sur l'appliance SD-WAN SE. Il garantit que les informations d'adresse IP WANOP SD-WAN sont effacées pour la redirection de l'interface graphique.
2. Désactivez et activez la configuration du mode Deux boîtes sur l'appliance WANOP SD-WAN. La nouvelle adresse IP (IP modifiée) de l'appliance WANOP SD-WAN est envoyée à SD-WAN SE. La nouvelle adresse IP modifiée s'affiche dans les pages de redirection d'URL.

L'adresse IP de gestion est utilisée pour la configuration de l'adresse IP homologue.

Désactiver le mode deux boîtes sur l'appliance WANOP SD-WAN

Pour désactiver ou découpler les appliances WANOP SD-WAN et SD-WAN SE du mode Two Box :

1. Désactivez le mode Two Box de l'appliance WANOP SD-WAN.
2. Il est prévu de voir l'appliance SD-WAN WANOP deux pages en mode boîte dans l'interface graphique Web SD-WAN SE. Pour effacer ces pages, exécutez la commande : `clear_wo_sync`.

Haute disponibilité

November 1, 2021

Cette rubrique couvre les déploiements et les configurations de haute disponibilité (haute disponibilité) pris en charge par les appliances SD-WAN (Standard Edition et Premium (Enterprise) Edition)).

Les appliances Citrix SD-WAN peuvent être déployées en configuration haute disponibilité sous la forme d'une paire d'appliances dans des rôles actif/veille. Il existe trois modes de déploiement haute disponibilité :

- Haute disponibilité en ligne parallèle
- Haute disponibilité
- Haute disponibilité

Ces modes de déploiement haute disponibilité sont similaires au protocole VRRP (Virtual Router Redundancy Protocol) et utilisent un protocole SD-WAN propriétaire. Les nœuds clients (clients) et les nœuds de contrôle maître (MCN) au sein d'un réseau SD-WAN peuvent être déployés dans une configuration haute disponibilité. L'appliance principale et secondaire doit être les mêmes modèles de plate-forme.

Dans la configuration haute disponibilité, un dispositif SD-WAN sur le site est désigné comme dispositif actif. L'appliance de secours surveille l'appliance active. La configuration est mise en miroir sur les deux appliances. Si l'appliance de secours perd sa connectivité avec l'appliance active pendant une période définie, l'appliance de secours assume l'identité de l'appliance active et prend en charge la charge de trafic. Selon le mode de déploiement, ce basculement rapide a un impact minimal sur le trafic d'application passant par le réseau.

Modes de déploiement haute disponibilité

Mode à un bras :

En mode One-Arm, la paire d'appiances haute disponibilité se trouve en dehors du chemin de données. Le trafic d'application est redirigé vers la paire d'appiances avec le routage basé sur des stratégies (PBR). Le mode à bras unique est mis en œuvre lorsqu'un seul point d'insertion dans le réseau n'est pas réalisable ou pour faire face aux défis de la fail-to-wire. L'appliance de secours peut être ajoutée au même VLAN ou sous-réseau que l'appliance active et le routeur.

En mode One-Arm, il est recommandé que les appliances SD-WAN ne résident pas dans les sous-réseaux de données. Le trafic de chemin virtuel n'a pas à traverser le PBR et évite les boucles de route. L'appliance SD-WAN et le routeur doivent être connectés directement, soit via un port Ethernet, soit dans le même VLAN.

- **Surveillance IP SLA pour le recul :**

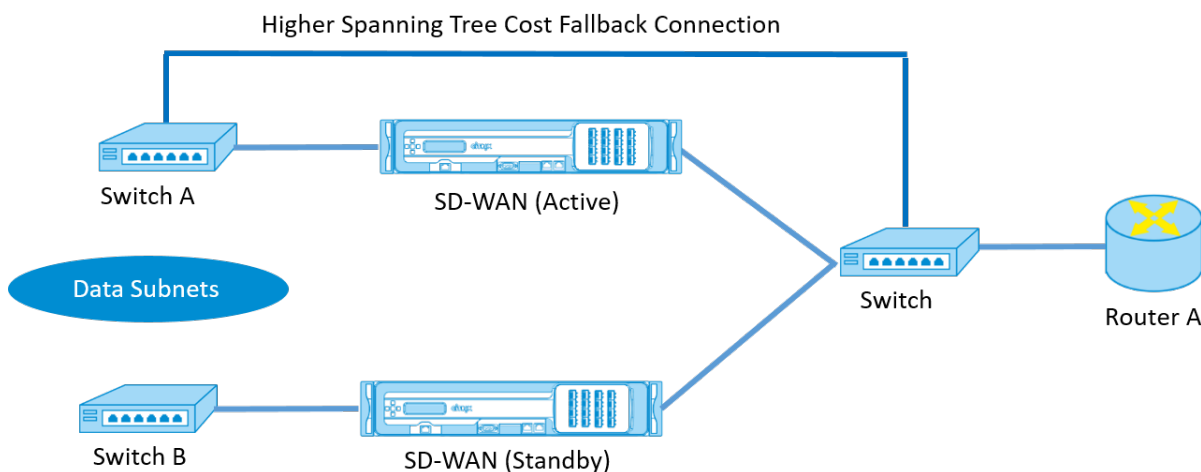
Le trafic actif circule même si le chemin virtuel est en panne, tant que l'une des appliances SD-WAN est active. L'appliance SD-WAN redirige le trafic vers le routeur en tant que trafic Intranet. Toutefois, si les deux appliances SD-WAN actif/de secours deviennent inactives, le routeur tente de rediriger le trafic vers les appliances. La surveillance SLA IP peut être configurée au niveau du routeur pour désactiver PBR, si l'appliance suivante n'est pas accessible. Il permet au routeur de revenir en arrière pour effectuer une recherche d'itinéraire et transférer les paquets de manière appropriée.

Mode haute disponibilité parallèle Inline :

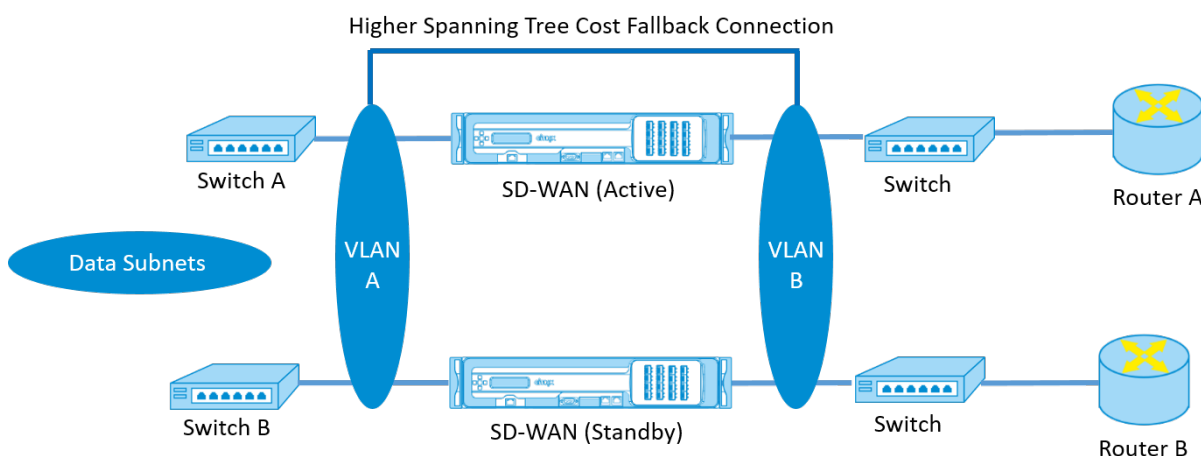
En mode haute disponibilité Parallel Inline, les appliances SD-WAN sont déployées les unes à côté des autres, en ligne avec le chemin de données. Un seul chemin d'accès à l'appliance active est utilisé. Il est important de noter que les groupes d'interface de contournement sont configurés pour être bloqués de façon à éviter les boucles de pontage lors d'un basculement.

L'état de haute disponibilité peut être surveillé via les groupes d'interfaces en ligne ou via une connexion directe entre les appliances. Le suivi externe peut être utilisé pour surveiller l'accessibilité de l'infrastructure réseau en amont ou en aval. Par exemple ; échec du port du commutateur pour diriger le changement d'état de haute disponibilité, si nécessaire.

Si les dispositifs SD-WAN actifs et de secours sont désactivés ou échoués, un chemin tertiaire peut être utilisé directement entre le commutateur et le routeur. Ce chemin doit avoir un coût de spanning tree plus élevé que les chemins SD-WAN afin qu'il ne soit pas utilisé dans des conditions normales. Le basculement en mode haute disponibilité en ligne parallèle dépend du temps de basculement configuré, le temps de basculement par défaut est de 1000 ms. Toutefois, un basculement a un impact sur le trafic de 3 à 5 secondes. Le retour au chemin tertiaire a un impact sur le trafic pendant la durée de la reconvergence Spanning Tree. S'il existe des connexions hors chemin vers d'autres liaisons WAN, les deux appliances doivent y être connectées.



Dans des scénarios plus complexes, où plusieurs routeurs peuvent utiliser VRRP, des VLAN non routables sont recommandés pour s'assurer que le commutateur côté LAN et les routeurs sont accessibles à la couche 2.



Mode Fail-to-wire :

En mode Fail-to-wire, les appliances SD-WAN sont intégrées dans le même chemin de données. Les groupes d'interface de contournement doivent être en mode Fail-to-Wire avec l'appliance de veille dans un état de transmission ou de contournement. Une connexion directe entre les deux appliances sur un port séparé doit être configurée et utilisée pour le groupe d'interfaces haute disponibilité.

Remarque

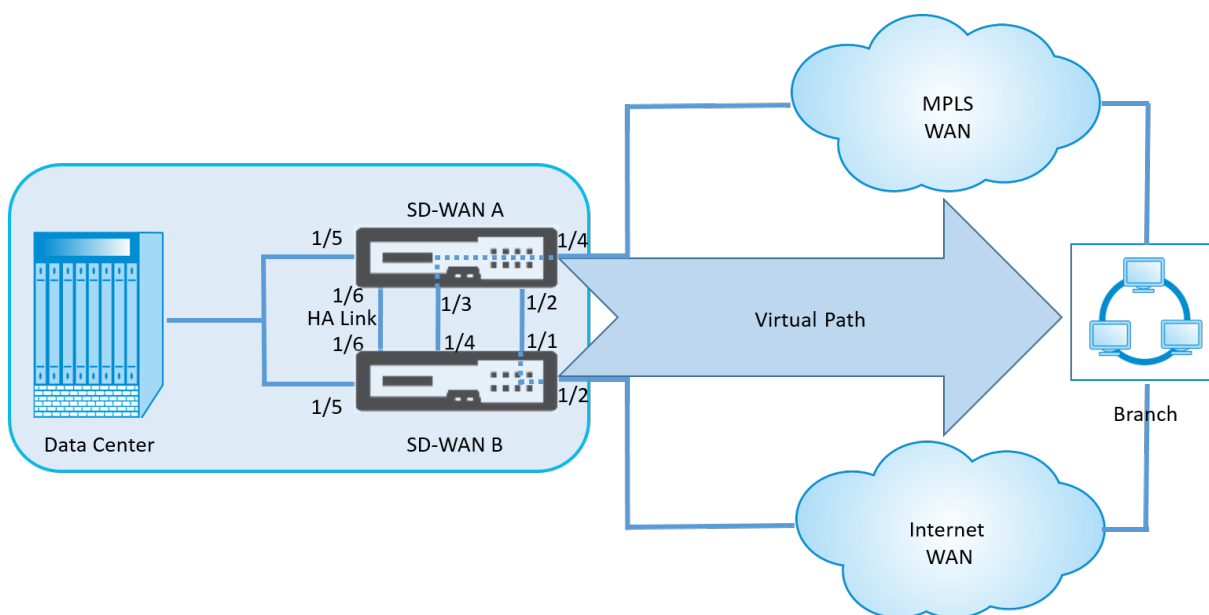
- Le basculement haute disponibilité en mode Fail-to-Wire prend environ 10 à 12 secondes en raison du délai de récupération des ports du mode Fail-to-Wire.
- Si la connexion à haute disponibilité entre les appliances échoue, les deux appliances passent à l'état Actif et provoquent une interruption de service. Pour atténuer l'interrup-

tion de service, affectez plusieurs connexions haute disponibilité afin qu'il n'y ait pas de point de défaillance unique.

- Il est impératif qu'en mode Fail-to-Wire haute disponibilité, un port séparé soit utilisé dans les paires matérielles pour le mécanisme d'échange de contrôle haute disponibilité afin de faciliter la convergence des états.

En raison d'un changement d'état physique lorsque les appliances SD-WAN passent d'Active à Standby, le basculement peut entraîner une perte partielle de connectivité en fonction de la durée de la négociation automatique sur les ports Ethernet.

L'illustration suivante illustre un exemple de déploiement Fail-to-Wire.



La configuration de haute disponibilité à un bras ou la configuration de haute disponibilité parallèle en ligne est recommandée pour les centres de données ou les sites qui transmettent un volume élevé de trafic afin de minimiser les interruptions pendant le basculement.

Si une perte de service minimale est acceptable lors d'un basculement, le mode de haute disponibilité Fail-to-Wire est une meilleure solution. Le mode de haute disponibilité Fail-to-Wire protège contre les défaillances de l'appliance et la haute disponibilité parallèle en ligne protège contre toutes les défaillances. Dans tous les scénarios, la haute disponibilité est précieuse pour préserver la continuité du réseau SD-WAN en cas de panne du système.

Configurer la haute disponibilité

Pour configurer la haute disponibilité :

1. Dans l'éditeur de configuration, accédez à **Sites > Nom du site > Haute disponibilité**. Sélectionnez **Activer la haute disponibilité**, puis cliquez sur **Appliquer**.

BasicGlobalSitesConnectionsOptimizationProvisioning

View Region: Default_Region

View Site: MCN-5100

+ Site

Site

Site

Sites

Basic Settings

Centralized Licensing

Routing Domains

Interface Groups

Virtual IP Addresses

VRRP

DHCP

WAN Links

Certificates

High Availability

☒ Enable High Availability

To enable HA and begin configuring HA settings, please click the Apply button.

Apply

Revert

☒ Enable High Availability

HA Appliance Name:MATRIZ-1

Failover Time (ms):1000

Shared Base MAC:AA:AA:AA:00:00:00

☐ Swap Primary/Secondary

☐ Primary Reclaim

☐ HA Fail-to-Wire Mode

HA IP Interfaces

+

	Virtual Interface	Control IP Addresses		
		Primary	Secondary	Delete
<div>+ </div>	LAN (100)	10.0.15.241	10.0.15.240	<div></div>
<div>+ </div>	INET (0)	10.213.16.35	10.213.16.34	<div></div>

2. Tapez les valeurs du paramètre suivant :

- **Nom de l’appliance haute disponibilité** : nom de l’appliance haute disponibilité (secondaire).
- **Temps de basculement** : le temps d’attente (en millisecondes) après la perte du contact avec l’appliance principale, avant que l’appliance de secours ne devienne active.
- **MAC de base partagée** : adresse MAC partagée pour les appliances de paires haute disponibilité. Lorsque un basculement se produit, le matériel secondaire possède les mêmes adresses MAC virtuelles que le matériel principal défaillant.
- **Échangez primaire/secondaire** : lorsque cette option est sélectionnée, si les deux appliances de la paire haute disponibilité sont simultanément, l’appliance secondaire devient l’appliance principale et a priorité.
- **Réclamation principale** : Lorsque cette option est sélectionnée, l’appliance principale

désignée reprend le contrôle lors du redémarrage après un événement de basculement.

- Mode **Fail-to-Wire haute disponibilité** : **sélectionnez cette option pour activer le mode** de déploiement haute disponibilité Fail-to-Wire.

Remarque

Pour les plates-formes basées sur l'hyperviseur et le cloud, choisissez l'option **Désactiver Shared Base MAC** pour désactiver l'adresse MAC virtuelle partagée.

Pour les plates-formes basées sur l'Hypervisor, assurez-vous que le mode promiscuous est activé sur les hyperviseurs pour permettre l'approvisionnement des paquets à partir d'une adresse MAC partagée haute disponibilité. Si le mode promiscuous n'est pas activé, vous pouvez activer l'option **Désactiver le MAC de base partagée**.

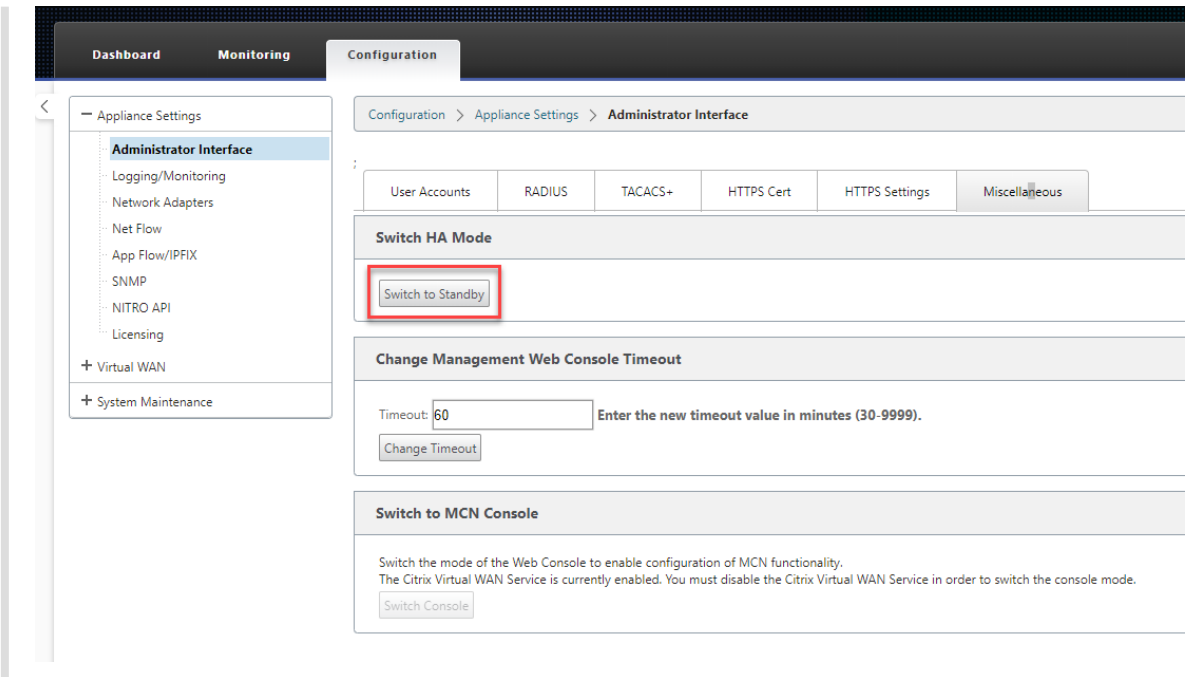
Cliquez sur **+** en regard de **Interfaces IP haute disponibilité pour configurer les groupes d'interfaces**. Tapez Valeurs pour les paramètres suivants :

- **Interface virtuelle** : Interface virtuelle à utiliser pour la communication entre les appliances de la paire haute disponibilité. Il surveille l'accessibilité de l'appliance Active. Pour le mode haute disponibilité à un bras, un seul groupe d'interfaces est requis.
- **Principal** : adresse IP virtuelle unique de l'appliance principale. L'appliance secondaire utilise l'adresse IP virtuelle principale pour communiquer avec l'appliance principale.
- **Secondaire** : adresse IP virtuelle unique de l'appliance secondaire. L'appliance principale utilise l'adresse IP virtuelle secondaire pour communiquer avec l'appliance secondaire.

Cliquez sur **+** à gauche de la nouvelle entrée **Interfaces IP haute disponibilité**. Dans le champ **Adresse IP de suivi** externe, tapez l'adresse IP du périphérique externe qui répond aux demandes ARP pour déterminer l'état de l'appliance principale, puis cliquez sur **Appliquer**.

Remarque :

Vous pouvez également déclencher manuellement un basculement HA à partir de l'appliance. Accédez à **Configuration > Paramètres du matériel > Interface administrateur > Divers**. Dans la section Basculer le mode HA, cliquez sur **Basculer en veille** ou **Passer en mode actif** en fonction de l'appliance HA.



Surveillance

Pour surveiller la configuration de haute disponibilité :

Connectez-vous à l'interface de gestion Web SD-WAN pour les appliances Active et Standby pour lesquelles la haute disponibilité est implémentée. Affichez l'état de la haute disponibilité sous l'onglet Tableau de **board** .

DashboardMonitoringConfiguration

System Status

Name:

BLR_DC-Appliance

Model:

4000

Appliance Mode:

MCN

Management IP Address:

10.105.58.172

Appliance Uptime:

3 days, 7 hours, 1 minutes, 43.0 seconds

Service Uptime:

3 days, 6 hours, 39 minutes, 51.0 seconds

Routing Domain Enabled:

Default_RoutingDomain

High Availability Status

Local Appliance:

Active

Peer Appliance:

Standby

Last Update Received:

0 seconds ago

DashboardMonitoringConfiguration

System Status

Name:

BLR_DC-BLR_DC_HA

Model:

4000

Appliance Mode:

MCN

Management IP Address:

10.105.58.142

Appliance Uptime:

1 weeks, 1 days, 12 hours, 41 minutes, 5.3 seconds

Service Uptime:

3 days, 6 hours, 50 minutes, 31.0 seconds

Routing Domain Enabled:

Default_RoutingDomain

High Availability Status

Local Appliance:

Standby

Peer Appliance:

Active

Last Update Received:

0 seconds ago

Pour plus d’informations sur la carte réseau des appliances haute disponibilité actives et de secours, accédez à **Configuration > Paramètres de l’appliance > Cartes réseau** > onglet **Ethernet** .

DashboardMonitoringConfiguration

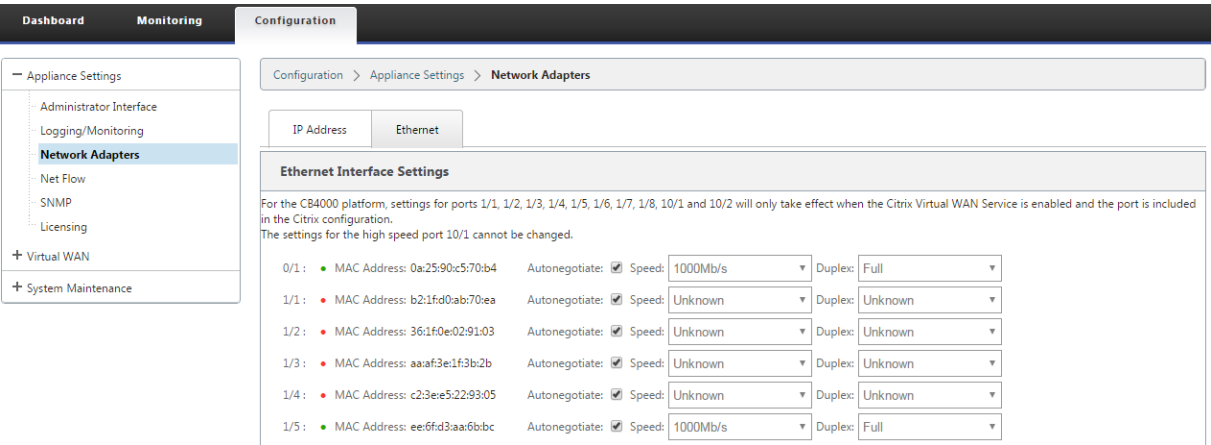
Configuration > Appliance Settings > Network Adapters

IP AddressEthernet

Ethernet Interface Settings

For the CB4000 platform, settings for ports 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 10/1 and 10/2 will only take effect when the Citrix Virtual WAN Service is in the Citrix configuration.
The settings for the high speed port 10/1 cannot be changed.

0/1 :	MAC Address: 0a:c4:7a:14:c9:d6	Autonegotiate:	<input checked="" type="checkbox"/>	Speed:	1000Mb/s	Duplex:	Full
1/1 :	MAC Address: 5a:4c:f8:f0:71:b2	Autonegotiate:	<input checked="" type="checkbox"/>	Speed:	Unknown	Duplex:	Unknown
1/2 :	MAC Address: d6:1e:72:d5:d1:18	Autonegotiate:	<input checked="" type="checkbox"/>	Speed:	1000Mb/s	Duplex:	Full
1/3 :	MAC Address: 66:4f:9d:c5:48:d2	Autonegotiate:	<input checked="" type="checkbox"/>	Speed:	Unknown	Duplex:	Unknown
1/4 :	MAC Address: 46:63:cb:5d:39:db	Autonegotiate:	<input checked="" type="checkbox"/>	Speed:	1000Mb/s	Duplex:	Full
1/5 :	MAC Address: 06:7b:ce:9a:c5:dd	Autonegotiate:	<input checked="" type="checkbox"/>	Speed:	1000Mb/s	Duplex:	Full



Résolution des problèmes

Effectuez les étapes de dépannage suivantes lors de la configuration de l’appliance SD-WAN en mode Haute disponibilité (HA) :

1. La principale raison du problème de diviser le cerveau est due à un problème de communication entre les appareils HA.
 - Vérifiez si un problème de connectivité (par exemple, les ports de l’appliance SD-WAN sont en haut ou en bas) entre les appliances SD-WAN.
 - Vous devez désactiver le service SD-WAN sur l’une des appliances SD-WAN pour s’assurer qu’une seule appliance SD-WAN est active.
2. Vous pouvez vérifier les journaux liés à la HA qui est connecté au fichier **SDWAN_common.log**.

REMARQUE

Tous les journaux liés à la HA sont consignés avec le mot clé **racp**.

3. Vous pouvez vérifier les événements liés au port dans le fichier **SDWAN_common.log** (par exemple, les ports activés HA sont en panne ou en haut).
4. Pour chaque changement d’état HA, un événement SD-WAN est enregistré. Donc, si les journaux sont reconduits, vous pouvez vérifier les journaux des événements pour obtenir les détails de l’événement.

Activer la haute disponibilité en mode Edge à l’aide d’un câble Y à fibre optique

September 26, 2023

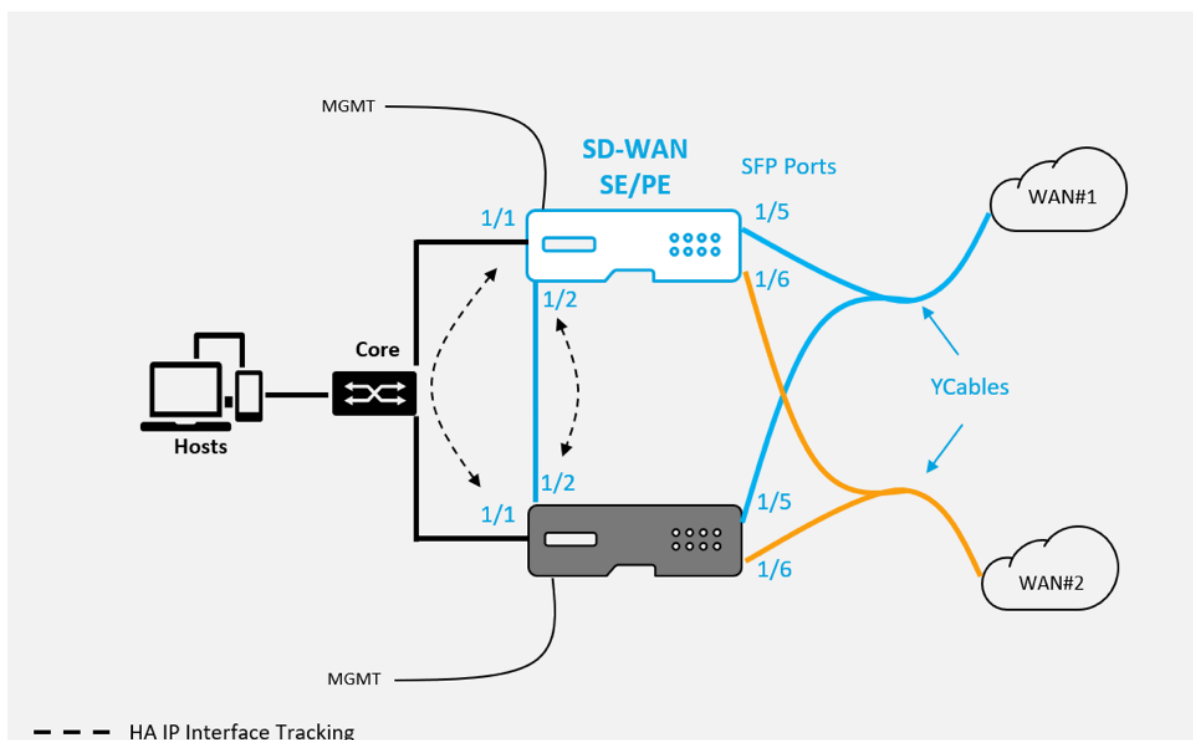
Remarque : dans la version 2 de 10.2, cette fonctionnalité s'applique uniquement à l'apppliance 1100 SE/PE.

La procédure suivante décrit les étapes à suivre pour activer la haute disponibilité (HA) sur les appliances 1100 SE/PE déployées en mode Edge où les transferts des fournisseurs de services de liaison WAN sont à fibre optique.

Les ports SFP (Small Form-Factor Pluggable) disponibles sur les appliances 1100 peuvent être utilisés avec les câbles en Y à fibre optique pour permettre une fonctionnalité de haute disponibilité pour le déploiement en mode Edge.

Sur l'apppliance 1100 SE/PE, l'extrémité divisée du câble séparateur se connecte aux ports fibre de deux appliances 1100 configurées en paire HA.

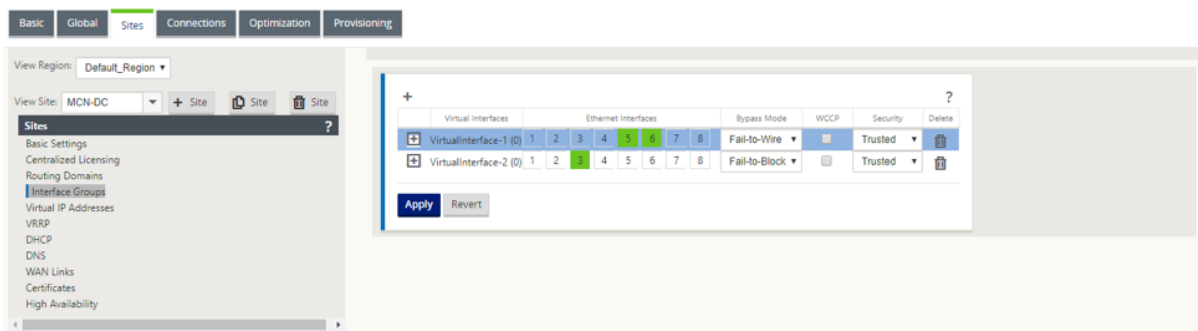
La fibre optique Y-Cable a trois extrémités. Une extrémité se connecte au transfert de fibre du fournisseur et les deux autres extrémités se connectent aux ports SFP configurés pour cette liaison WAN sur deux appliances 1100 SE/PE déployées en paire HA. Le câble séparateur est utilisé pour diviser un signal entrant en plusieurs signaux.



Conditions préalables :

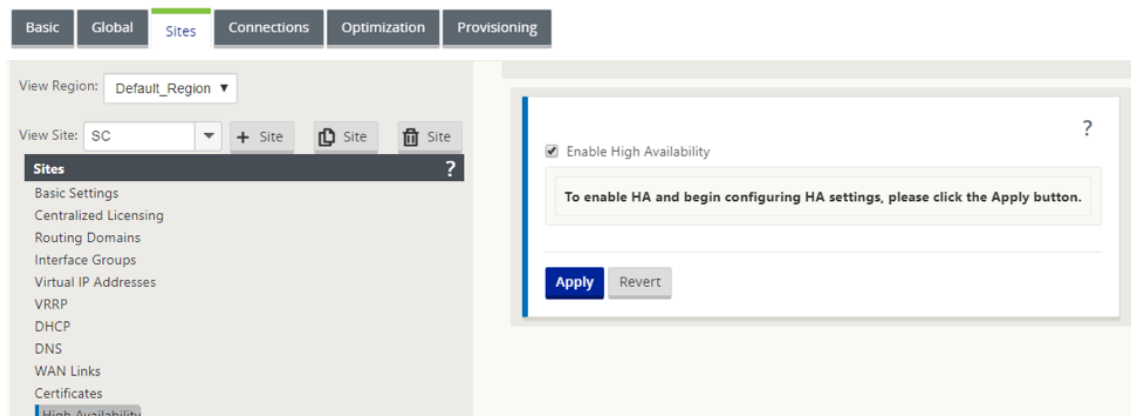
1. Sur l'apppliance 1100 SE/PE, les ports 1/5 et 1/6 sont des ports SFP. Connectez les extrémités du séparateur du câble Y à l'un de ces ports sur les deux appliances de la paire HA. Pour plus d'informations, reportez-vous à la section [1100 SE](#).
2. Ajoutez des ports SFP à la configuration de l'apppliance SD-WAN. La configuration des ports SFP équivaut à la configuration des ports d'interface réseau. Pour plus d'informations, reportez-

vous à la section [Comment configurer des groupes d'interface](#). L'ajout de ports 1/5 ou 1/6 à la configuration vous permet d'activer la fonction de prise en charge du câble Y.



Pour activer la haute disponibilité à l'aide du câble Y :

1. Dans l'interface graphique de l'appareil 1100 SE/PE, accédez à **Configuration > Réseau étendu virtuel > Éditeur de configuration > Sites**. Cliquez sur **Activer la haute disponibilité**.



2. Cliquez sur **Activer la prise en charge des câbles enY**.
3. Ajoutez des interfaces IP HA en utilisant toute autre interface en plus des interfaces connectées aux câbles Y (par exemple interface 1/1 LAN, ou 1/2 interfaces directement connectées). Lorsque la fonction de câble Y est activée, les ports SFP ne peuvent pas être utilisés pour les interfaces IP HA.

The screenshot displays the Citrix SD-WAN configuration interface. On the left, a sidebar shows the 'Sites' menu with 'High Availability' selected. The main panel shows the configuration for a site named 'SC'. The 'Enable High Availability' checkbox is checked. Below this, there are fields for 'HA Appliance Name' (set to 'New_HA_Appla...'), 'Failover Time (ms)' (set to '1000'), and 'Shared Base MAC' (set to 'AA:AA:AA:00:00:00'). There are also checkboxes for 'Swap Primary/Secondary', 'Primary Reclaim', 'HA Fail-to-Wire Mode', and 'Enable Y-Cable Support' (checked). A table titled 'HA IP Interfaces' shows a single entry for 'VirtualInterface-1 (0)' with 'Primary' IP '192.10.1.24' and 'Secondary' IP '192.10.1.25'. Below this is an 'External Tracking' section with a field for 'External Tracker IP Address' and a 'Delete' button. At the bottom, there are 'Apply' and 'Revert' buttons.

4. Appliquer, Stage et Activer la configuration.

Limitations :

- La configuration du mode Fail-to-Wire HA à l'aide du câble Y n'est pas prise en charge.
- Les SFP connectés au câble Y ne peuvent pas être utilisés comme suivi d'interface IP HA.
- La version 10.2.2 ou supérieure et 11.0 ou supérieure est requise pour prendre en charge ce déploiement.

Inscription sans contact

November 1, 2021

Remarque

Le service Zero Touch Deployment est pris en charge uniquement sur certaines appliances Citrix SD-WAN :

- SD-WAN 110 Édition Standard
- SD-WAN 210 Édition Standard
- SD-WAN 410 Édition Standard
- SD-WAN 2100 Édition Standard
- SD-WAN 1000 Standard Edition (nouvelle image requise)
- SD-WAN 1000 Édition Entreprise (Édition Premium) (réimage requise)

- SD-WAN 1100 Édition Standard
- SD-WAN 1100 Édition Premium (Entreprise)
- SD-WAN 2000 Standard Edition (réimage requise)
- SD-WAN 2000 Édition Entreprise (Édition Premium (réimage requise))
- SD-WAN 2100 Édition Entreprise (Édition Premium)
- Instance VPX AWS SD-WAN

Le service cloud de déploiement sans intervention est un service cloud géré et géré par Citrix qui permet de découvrir de nouvelles appliances dans le réseau Citrix SD-WAN, principalement axé sur la rationalisation du processus de déploiement de Citrix SD-WAN dans les succursales ou les bureaux de service cloud. Le service Cloud à déploiement zéro touche est accessible publiquement à partir de n'importe quel point d'un réseau via un accès Internet public. Le service cloud de déploiement sans intervention est accessible via le protocole SSL (Secure Socket Layer).

Le déploiement zéro touche Cloud Services communique en toute sécurité avec les services principaux Citrix hébergeant l'identification stockée des clients Citrix qui ont acheté des appareils compatibles Zero Touch (par exemple SD-WAN 410-SE, 2100-SE). Les services back-end sont en place pour authentifier toute demande de déploiement Zero Touch, validant correctement l'association entre le compte client et les numéros de série des appliances Citrix SD-WAN.

Architecture et flux de travail de haut niveau ZTD :

Site du centre de données :

Administrateur Citrix SD-WAN : utilisateur disposant des droits d'administration de l'environnement SD-WAN avec les responsabilités principales suivantes :

- Création de la configuration à l'aide de l'outil Citrix SD-WAN Center Network Configuration ou importation de la configuration à partir de l'appliance SD-WAN Master Control Node (MCN)
- Connexion Citrix Cloud pour lancer le service de déploiement sans intervention pour le déploiement de nouveaux nœuds de site.

Remarque

Si votre SD-WAN Center est connecté à Internet via un serveur proxy, vous devez configurer les paramètres du serveur proxy sur SD-WAN Center. Pour plus d'informations, consultez la section [Paramètres du serveur proxy pour le déploiement Zero Touch](#).

Administrateur réseau : utilisateur responsable de la gestion du réseau d'entreprise (DHCP, DNS, Internet, pare-feu, etc.)

- Si nécessaire, configurez les pare-feu pour la communication sortante vers le nom de domaine complet ***sdwanzt.citrixnetworkapi.net*** à partir de SD-WAN Center.

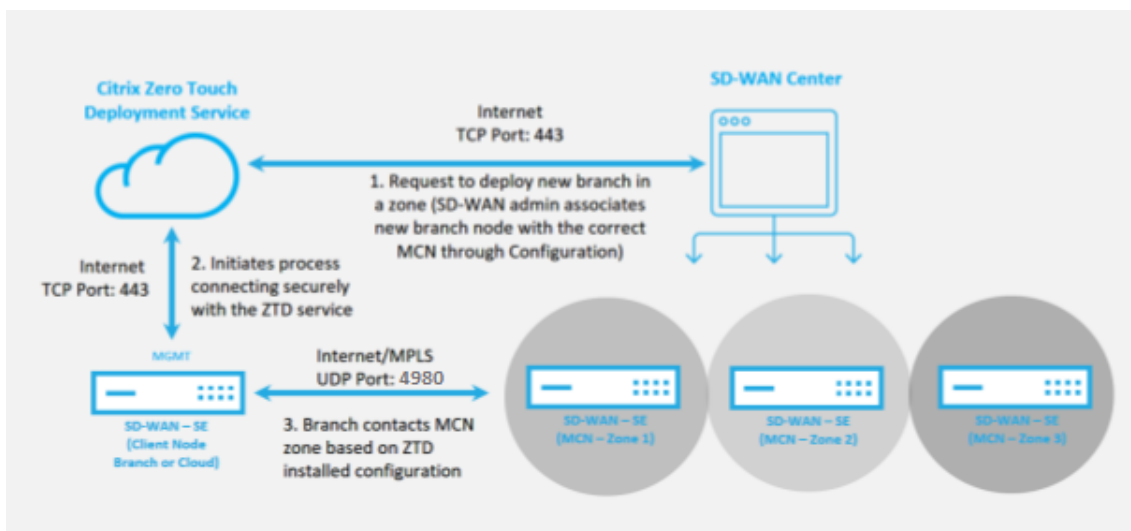
Site distant :

Installateur sur site — Un contact local ou un installateur engagé pour une activité sur site avec les principales responsabilités suivantes :

- Décompressez physiquement l'apppliance Citrix SD-WAN.
- Réimaginez les appliances non compatibles avec ZTD.
 - Requis pour : SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
 - Non requis pour : SD-WAN 410-SE, 2100-SE
- Câble d'alimentation de l'appareil.
- Câblez l'apppliance pour la connectivité Internet sur l'interface de gestion (par exemple, MGMT ou 0/1).
- Câblez l'apppliance pour la connectivité de liaison WAN sur les interfaces de données (par exemple APA.wan, APB.wan, APC.wan, 0/2, 0/3, 0/5, etc.).

Remarque

La disposition de l'interface est différente pour chaque modèle, donc référencer la documentation pour l'identification des ports de données et de gestion.

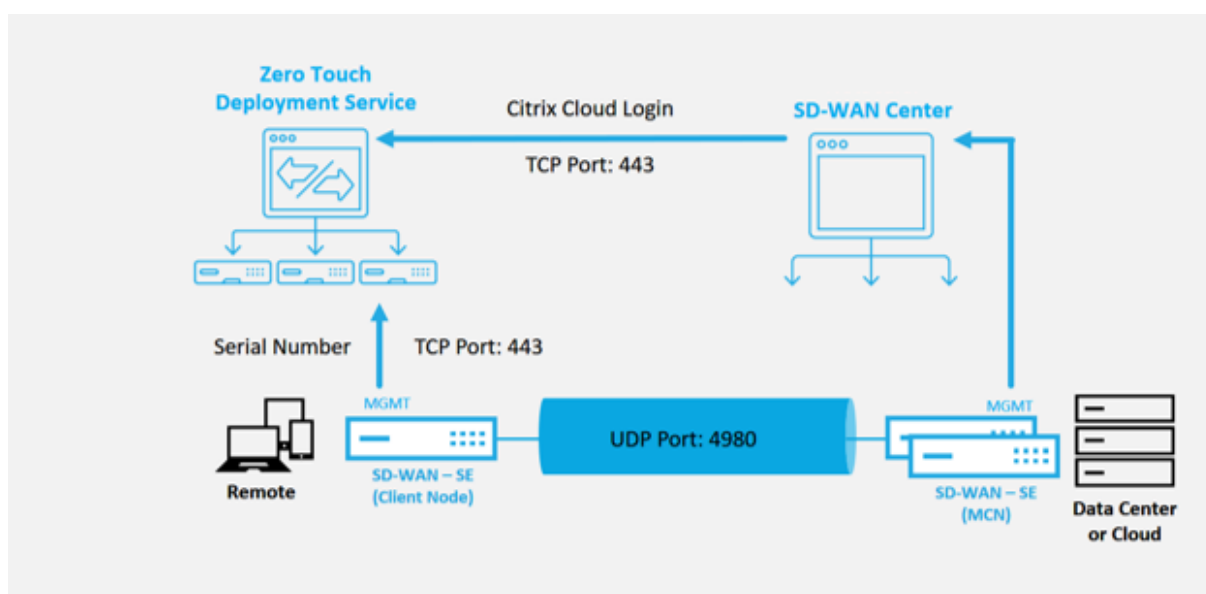


Les conditions préalables suivantes sont requises avant de démarrer un service de déploiement sans intervention :

- Exécution active du SD-WAN promu en MCN (Master Control Node).
- Exécution active de SD-WAN Center avec connectivité au MCN via Virtual Path.
- Informations d'identification de connexion Citrix Cloud créées sur <https://onboarding.cloud.com> (reportez-vous aux instructions ci-dessous sur la création du compte).

- Connectivité réseau de gestion (SD-WAN Center et appliance SD-WAN) à Internet sur le port 443, soit directement, soit via un serveur proxy.
- (Facultatif) Au moins une appliance SD-WAN en cours d'exécution active opérant dans une succursale en mode client avec une connectivité de chemin virtuel valide à MCN pour aider à valider la mise en place du chemin sur le réseau de sous-couche existant.

La dernière condition préalable n'est pas obligatoire, mais elle permet à l'administrateur SD-WAN de valider que le réseau sous-jacent permet d'établir des chemins virtuels lorsque le déploiement Zero Touch est terminé avec un site nouvellement ajouté. Cela permet principalement de vérifier que les stratégies de pare-feu et de routage appropriées sont en place pour le trafic NAT en conséquence ou confirmer que le port UDP 4980 peut pénétrer avec succès dans le réseau pour atteindre le MCN.



Présentation du service de déploiement Zero Touch :

Le service de déploiement sans intervention fonctionne en tandem avec le SD-WAN Center pour faciliter le déploiement des appliances SD-WAN des succursales. SD-WAN Center est configuré et utilisé comme outil de gestion central pour les appliances SD-WAN Standard et Enterprise (Premium) Edition. Pour utiliser le service de déploiement Zero Touch (ou le service cloud de déploiement sans intervention), un administrateur doit commencer par déployer le premier périphérique SD-WAN dans l'environnement, puis configurer et déployer le SD-WAN Center en tant que point central de gestion. Lorsque le SD-WAN Center, version 9.1 ou ultérieure, est installé avec une connectivité à Internet publique sur le port 443, SD-WAN Center lance automatiquement le service Cloud et installe les composants nécessaires pour déverrouiller les fonctionnalités de déploiement Zero Touch et rendre l'option Déploiement Zero Touch disponible dans l'interface graphique de SD-WAN Center. Le déploiement Zero Touch n'est pas disponible par défaut dans le logiciel SD-WAN Center. Ceci est spécialement conçu pour s'assurer que les composants préliminaires appropriés sur le réseau sous-jacent sont présents avant de permettre à un administrateur de lancer toute activité sur site.

impliquant un déploiement Zero Touch.

Une fois qu'un environnement SD-WAN fonctionnel est en cours d'exécution, l'enregistrement dans le service de déploiement sans intervention est effectué par la création d'une connexion à un compte Citrix Cloud. Avec SD-WAN Center capable de communiquer avec le service de déploiement zéro contact, l'interface graphique présente les options de déploiement zéro tactile sous l'onglet **Configuration**. La connexion au service Zero Touch authentifie l'ID client associé à l'environnement SD-WAN particulier et enregistre SD-WAN Center, en plus de déverrouiller le compte pour une authentification supplémentaire des déploiements d'appiances de déploiement zéro contact.

À l'aide de l'outil de configuration réseau de SD-WAN Center, l'administrateur SD-WAN devra ensuite utiliser les modèles ou la fonctionnalité de clonage de site pour créer la configuration SD-WAN afin d'ajouter de nouveaux sites. La nouvelle configuration est utilisée par SD-WAN Center pour lancer le déploiement du déploiement zéro contact pour les sites nouvellement ajoutés. Lorsque l'administrateur SD-WAN initie un site à déployer à l'aide du processus de déploiement sans intervention, vous avez la possibilité de pré-authentifier l'appliance à utiliser pour un déploiement sans intervention en prérenseignant le numéro de série et en initiant une communication par e-mail au programme d'installation sur site pour commencer sur site. activité.

Le programme d'installation sur site reçoit une communication électronique indiquant que le site est prêt pour le déploiement sans intervention et peut commencer la procédure d'installation de mise sous tension et de câblage de l'appliance pour l'attribution d'adresse IP DHCP et l'accès Internet sur le port MGMT. En outre, le câblage dans n'importe quel port LAN et WAN. Tout le reste est initié par le service de déploiement sans intervention et la progression est surveillée à l'aide de l'URL d'activation. Dans le cas où le nœud distant à installer est une instance de cloud, l'ouverture de l'URL d'activation déclenche le flux de travail pour installer automatiquement l'instance dans l'environnement de cloud désigné, aucune action n'est requise par un programme d'installation local.

Le service Cloud de déploiement Zero Touch automatise les actions suivantes :

Téléchargez et mettez à jour l'agent de déploiement zéro touche si de nouvelles fonctionnalités sont disponibles sur le dispositif de succursale.

- Authentifiez l'appliance de succursale en validant le numéro de série.
- Authentifiez que l'administrateur SD-WAN a accepté le site pour un déploiement sans contact à l'aide de SD-WAN Center.
- Extrayez le fichier de configuration spécifique à l'appliance ciblée à partir du SD-WAN Center.
- Poussez le fichier de configuration spécifique à l'appliance ciblée vers l'appliance de branche.
- Installez le fichier de configuration sur le dispositif de branche.
- Poussez tous les composants logiciels SD-WAN manquants ou les mises à jour requises vers l'appliance de succursale.

- Envoie un fichier de licence temporaire de 10 Mbps pour confirmer l'établissement du chemin virtuel vers le dispositif de succursale.
- Activez le service SD-WAN sur le dispositif de succursale.

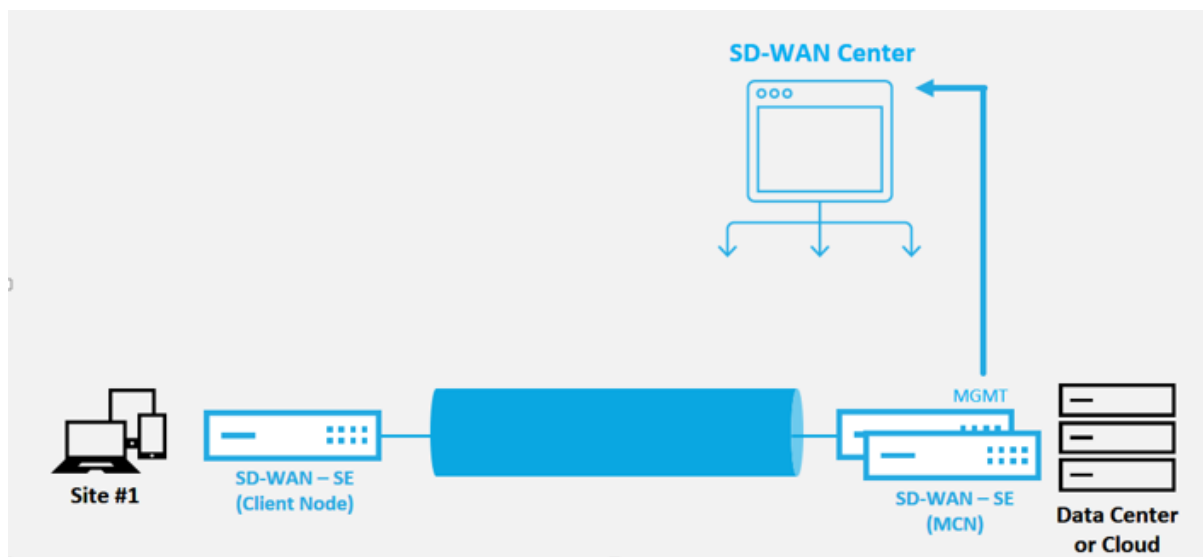
D'autres étapes sont requises pour l'administrateur SD-WAN pour installer un fichier de licence permanent sur l'appliance.

Remarque

Lors de l'exécution d'une configuration de branche qui possède déjà la même version du logiciel de l'appliance utilisée dans MCN, le processus de déploiement sans contact ne télécharge pas à nouveau le fichier logiciel de l'appliance. Cette modification s'applique aux appareils neufs expédiés en usine, aux appareils réinitialisés aux paramètres d'usine et à la réinitialisation de la configuration administrativement. Si la configuration est réinitialisée, cochez la case **Redémarrer après** la restauration pour lancer le processus de déploiement sans intervention.

Procédure de périphérique de déploiement Zero Touch

La procédure suivante détaille les étapes requises pour déployer un nouveau site à l'aide du service de déploiement Zero Touch. Avoir un MCN en cours d'exécution et un nœud client qui fonctionnent déjà avec une communication appropriée avec le SD-WAN Center, et ont établi des chemins virtuels confirmant la connectivité sur le réseau sous-jacent. Les étapes suivantes sont requises pour l'administrateur SD-WAN pour lancer le déploiement sans intervention :



Comment configurer le service de déploiement zéro tactile

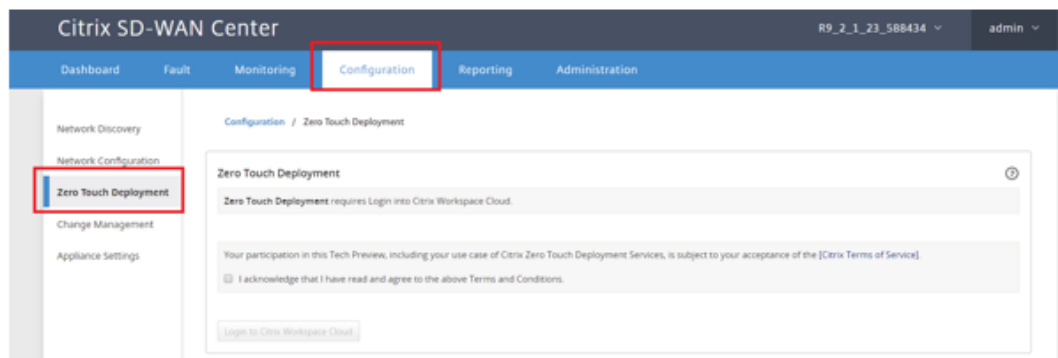
Le SD-WAN Center dispose de la fonctionnalité permettant d'accepter les demandes de connexion des appliances nouvellement connectées au réseau SD-WAN Enterprise. La demande est transmise à l'interface Web via le service de déploiement Zero Touch. Une fois l'appliance connectée au service, les packages de configuration et de mise à niveau logicielle sont téléchargés.

Workflow de configuration :

- Accédez au **SD-WAN Center** > **Créer une nouvelle configuration de site** ou Importez la configuration existante et enregistrez-la.
- Connectez-vous à Citrix Cloud pour activer le service de déploiement zéro touche. L'option de menu Déploiement Zero Touch s'affiche désormais dans l'interface de gestion Web de SD-WAN Center.
- Dans SD-WAN Center, accédez à **Configuration** > **Zero Touch Deployment** > **Deploy New Site**.
- Sélectionnez une appliance, cliquez sur **Activer**, puis sur **Déployer**.
- Le programme d'installation reçoit l'e-mail d'activation > Entrez le numéro de série > **Activer** > L'appliance est correctement déployée.

Pour configurer le service de déploiement sans intervention :

1. Installez SD-WAN Center avec les fonctionnalités de déploiement Zero Touch activées :
 - a) Installez SD-WAN Center avec l'adresse IP attribuée à DHCP.
 - b) Vérifiez que SD-WAN Center attribue une adresse IP de gestion appropriée et une adresse DNS réseau avec une connectivité à l'Internet public sur le réseau de gestion.
 - c) Mettez à niveau SD-WAN Center vers la dernière version du logiciel SD-WAN.
 - d) Avec une connectivité Internet appropriée, le SD-WAN Center lance le service cloud de déploiement sans contact et télécharge et installe automatiquement toutes les mises à jour de microprogramme spécifiques au déploiement sans contact. Si cette procédure Call Home échoue, l'option de déploiement Zero Touch suivante ne sera pas disponible dans l'interface graphique.



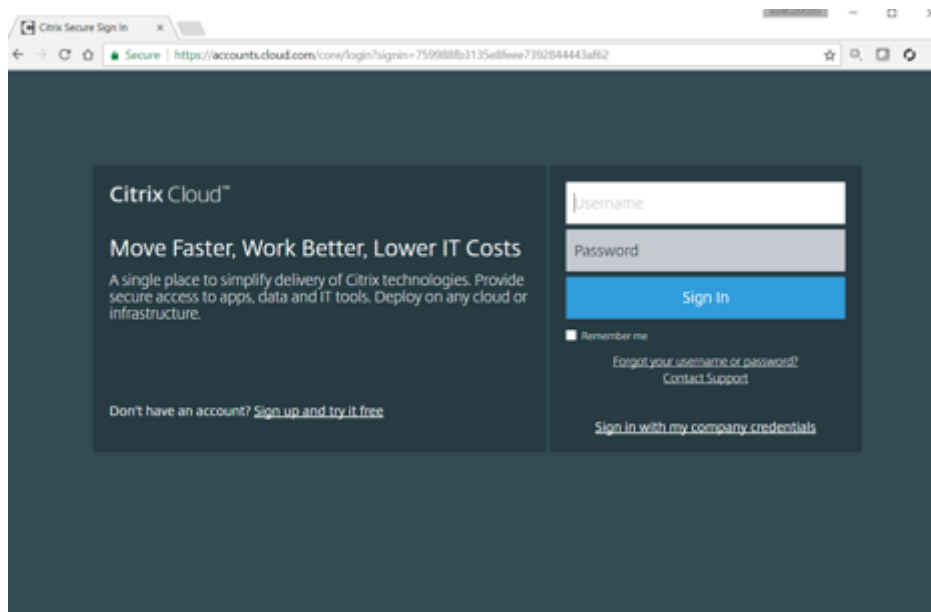
- e) Lisez les Termes et Conditions, puis sélectionnez **Je reconnais avoir lu et accepté les Termes et Conditions ci-dessus**.
- f) Cliquez sur le bouton **Connexion à Citrix Workspace Cloud** si un compte Citrix Cloud a déjà été créé.
- g) Connectez-vous au compte Citrix Cloud et à la réception du message suivant de connexion réussie, **VEUILLEZ NE PAS FERMER CETTE FENÊTRE, LE PROCESSUS NÉCESSITE ENVIRON 20 SECONDES SUPPLÉMENTAIRES POUR QUE L'INTERFACE GRAPHIQUE DE SD-WAN CENTER SOIT ACTUALISÉE**. La fenêtre doit se fermer d'elle-même lorsqu'elle est terminée.



- 2. Pour créer un compte Cloud Login, suivez la procédure ci-dessous : Ouvrez un navigateur Web sur <https://onboarding.cloud.com>
- 3. Cliquez sur le lien pour **Wait, j'ai un compte Citrix.com**.

A screenshot of the Citrix Cloud 'Sign Up' page. The page has a dark blue header with the 'Citrix Cloud' logo. Below the logo is a 'Sign Up' heading, and a red box highlights a link that says 'Wait, I have a Citrix.com account'. Below this is a form with fields for 'Business Email Address', 'First Name', 'Last Name', 'Company Name', 'Phone Number', 'Address', 'City', 'Country' (set to USA), 'State' (set to AA), and 'Zip or Postal Code'. There is a checkbox for 'I've read, understand and agree to the Terms of Service' and a blue 'Continue' button. A 'Contact Support' link is at the bottom.

4. Connectez-vous avec un compte Citrix existant.



5. Une fois connecté à la page Déploiement Zero Touch SD-WAN Center, vous pouvez remarquer qu'aucun site n'est disponible pour un déploiement sans contact pour les raisons suivantes :

- La configuration active n'a pas été sélectionnée dans le menu déroulant Configuration
- Tous les sites de la configuration active actuelle ont déjà été déployés
- La configuration n'a pas été construite à l'aide du SD-WAN Center, mais plutôt de l'Éditeur de configuration disponible sur le MCN
- Les sites n'ont pas été construits dans la configuration référençant les appliances compatibles zéro contact (par exemple 410-SE, 2100-SE, Cloud VPX)

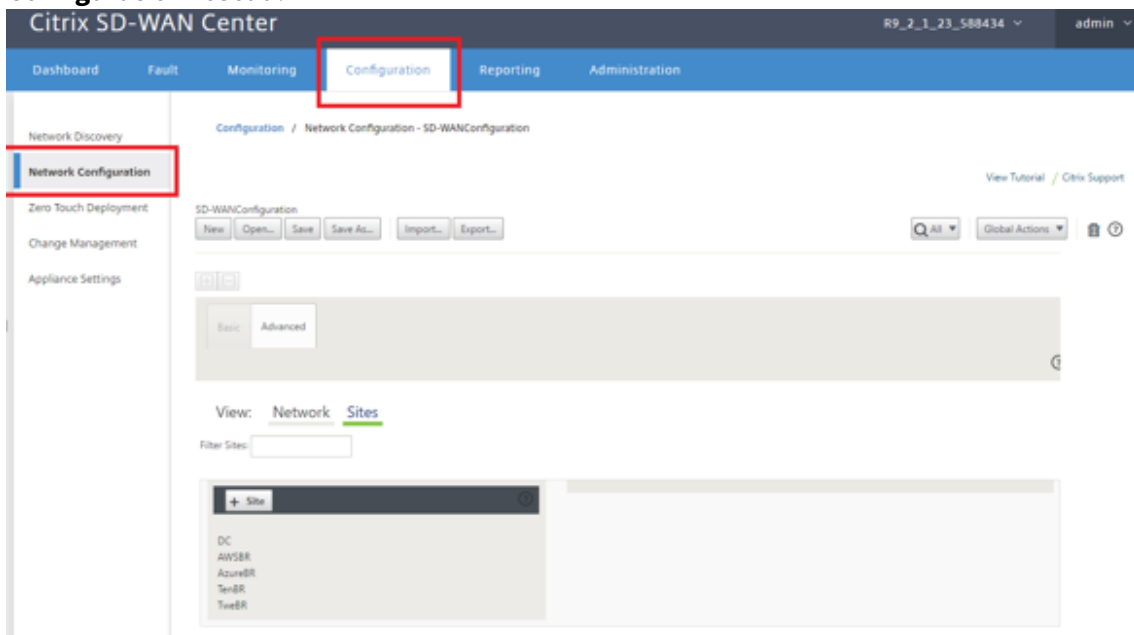
6. Mettez à jour la configuration pour ajouter un **nouveau site distant** avec une **appliance SD-WAN compatible ZTD** à l'aide de la configuration réseau SD-WAN Center.

Si la configuration SD-WAN n'a pas été créée à l'aide de la configuration réseau SD-WAN Center, importez la configuration active à partir du MCN et commencez à modifier la configuration à l'aide du SD-WAN Center. Pour la capacité de déploiement sans intervention, l'administrateur SD-WAN doit créer la configuration à l'aide du SD-WAN Center. La procédure suivante doit être utilisée pour ajouter un nouveau site ciblé pour le déploiement zéro tactile.

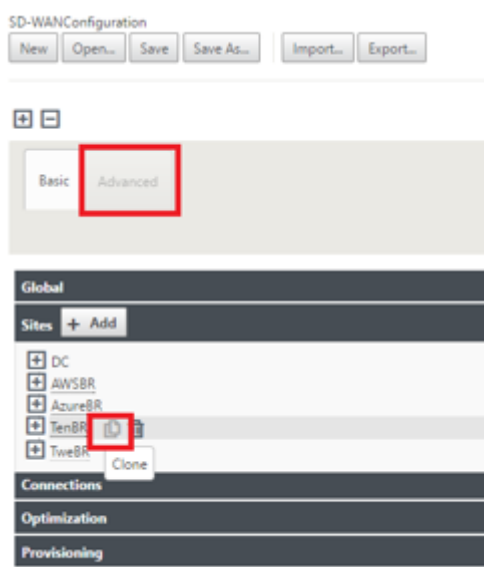
- a) Concevez le nouveau site pour le déploiement de l'appliance SD-WAN en décrivant d'abord les détails du nouveau site (c'est-à-dire le modèle d'appliance, l'utilisation des groupes d'interface, les adresses IP virtuelles, les liens WAN avec la bande passante et leurs passerelles respectives).

ou Gateway, éliminant ainsi la nécessité d'un routeur et d'un pare-feu de périphérie WAN et consolidant les besoins du réseau en matière de routage périphérique et de pare-feu sur la solution SD-WAN.

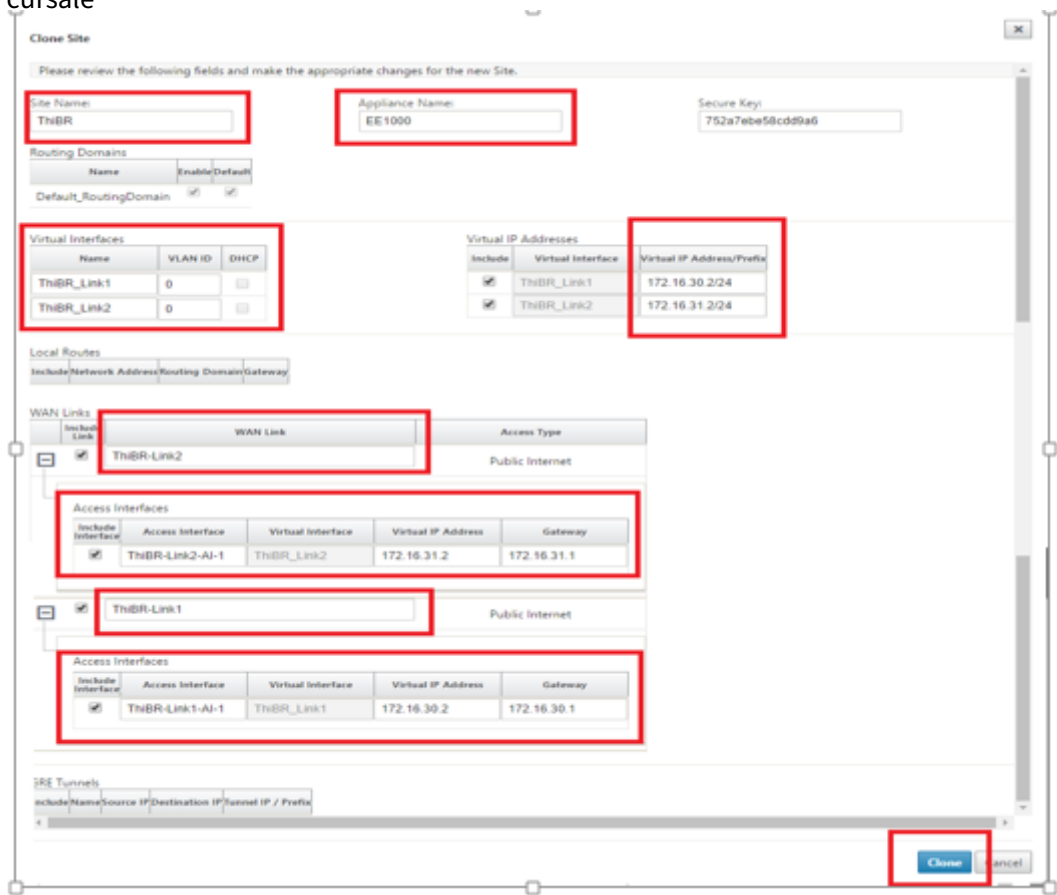
7. Ouvrez l'interface de gestion Web SD-WAN Center et accédez à la page **Configuration** > **Configuration réseau**.



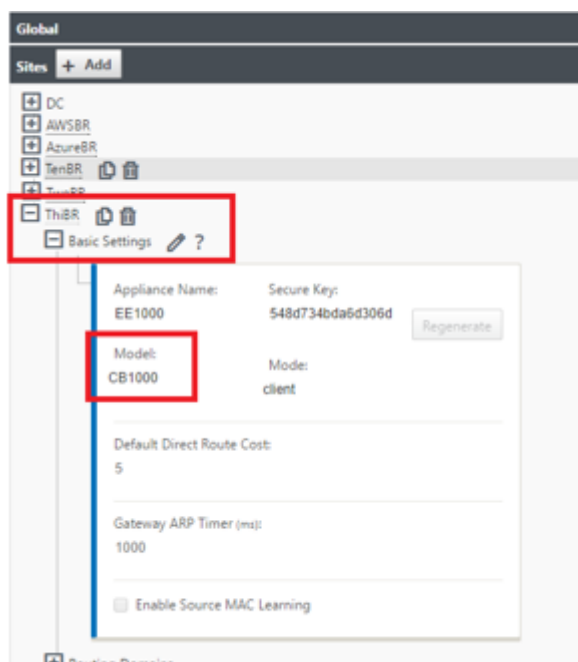
8. Assurez-vous qu'une configuration de travail est déjà en place ou importez-le à partir du MCN.
9. Accédez à l'onglet Avancé pour créer un site.
10. Ouvrez la vignette Sites pour afficher les sites actuellement configurés.
11. Vous avez rapidement créé la configuration du nouveau site à l'aide de la fonction de clonage de n'importe quel site existant.



12. Renseignez tous les champs obligatoires de la topologie conçue pour ce nouveau site de succursale

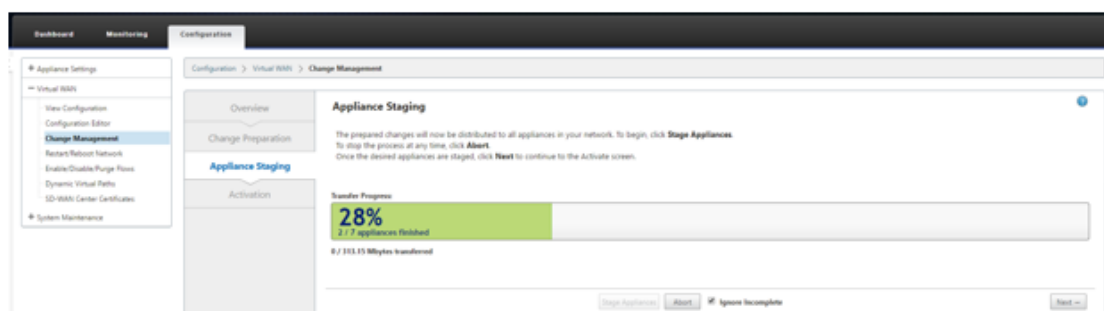


13. Après avoir cloné un nouveau site, accédez aux **paramètres de base** du site et vérifiez que le modèle de SD-WAN est correctement sélectionné pour prendre en charge le service Zero Touch.



Le modèle SD-WAN du site peut être mis à jour, mais sachez que les groupes d'interface doivent peut-être être redéfinis car l'appareil mis à jour peut avoir une nouvelle disposition d'interface que celle utilisée pour le clonage.

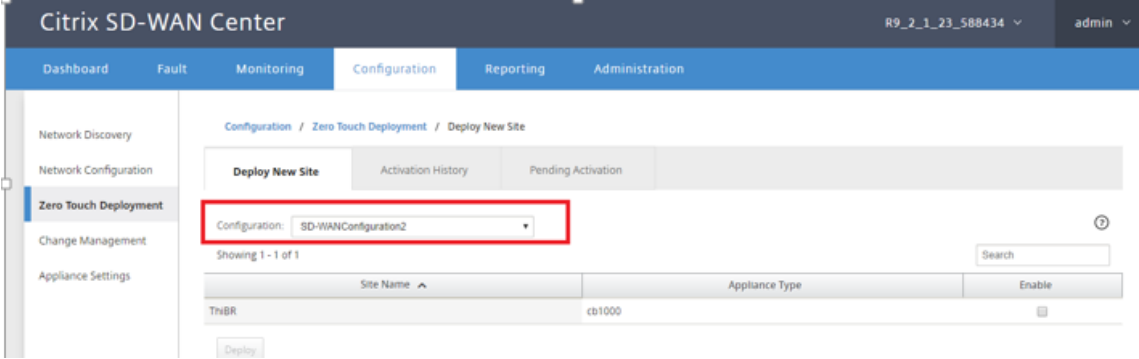
14. Enregistrez la nouvelle configuration sur SD-WAN Center et utilisez l'option d'exportation vers la **boîte de réception de la gestion des modifications** pour pousser la configuration à l'aide de la gestion des modifications.
15. Suivez la procédure de gestion des modifications pour préparer correctement la nouvelle configuration, ce qui permet aux périphériques SD-WAN existants de connaître le nouveau site à déployer sans intervention. Vous devez utiliser l'option « Ignorer incomplet » pour ignorer la tentative de transmission de la configuration vers le nouveau site qui doit encore passer par le flux de travail de déploiement sans intervention.



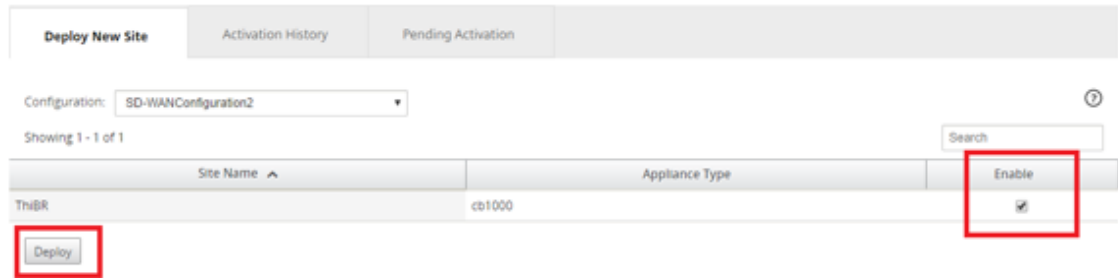
16. Revenez à la page SD-WAN Center Zero Touch Deployment et lorsque la nouvelle configuration active est en cours d'exécution, le nouveau site est disponible pour le déploiement.
17. Dans la page Déploiement sans intervention, sous l'onglet **Déployer un nouveau site**, sélectionnez

tionnez le fichier de configuration réseau en cours d'exécution

18. Une fois le fichier de configuration en cours d'exécution sélectionné, la liste de tous les sites de succursale avec des périphériques SD-WAN non déployés qui sont pris en charge pour zéro contact s'affiche.



19. Sélectionnez les sites de succursale que vous souhaitez configurer pour le service Zero Touch, cliquez sur **Activer**, puis **Déployer**.



20. Une fenêtre contextuelle Déployer un nouveau site s'affiche, dans laquelle l'administrateur peut fournir le numéro de série, l'adresse postale du site de la succursale, l'adresse e-mail du programme d'installation et d'autres notes, si nécessaire.

Deploy New Site

Site Name:
ThiBR

Serial Number:
XXXXXXXXXX

Street Address:
123 Street Dr

Installer Email:
ztdinstaller@outlook.com

Additional Notes:
Installer.
1) Cable all WAN and LAN interfaces to match the topology and configuration built in earlier steps.
2) Cable the management interface (MGMT, 0/1) in the

Deploy Cancel

Remarque

Le champ de saisie du numéro de série est facultatif et, selon qu'il est renseigné ou non, entraînera une modification de l'activité sur site dont le programme d'installation est responsable.

- Si le champ Numéro de série est renseigné —Le programme d'installation n'est pas tenu de saisir le numéro de série dans l'URL d'activation générée avec la commande de site de déploiement

- Si le champ Numéro de série est laissé noir —Le programme d'installation sera responsable de la saisie dans le champ numéro de série correct de l'appliance dans l'URL d'activation générée avec la commande de déploiement du site

21. Après avoir cliqué sur le bouton **Déployer**, un message s'affiche indiquant que “La configuration du site a été déployée.” Cette action déclenche SD-WAN Center, qui était précédemment enregistré auprès du service Cloud de déploiement zéro touche, pour partager la configuration de ce site particulier afin qu'il soit stocké dans le service Cloud de déploiement zéro touche.
22. Accédez à l'onglet Activation en attente pour confirmer que les informations du site de succursale ont été remplies avec succès et ont été placées dans un état d'activité d'installation en attente.

Pending Activation					
Showing 1 - 1 of 1					
Site Name	Serial No	Installer Email	Address	Status	Action
ThiBR	██████████	ztdinstaller@██████████.com	123 Street Dr	Connecting	
<div>Delete</div> <div>Modify</div>					

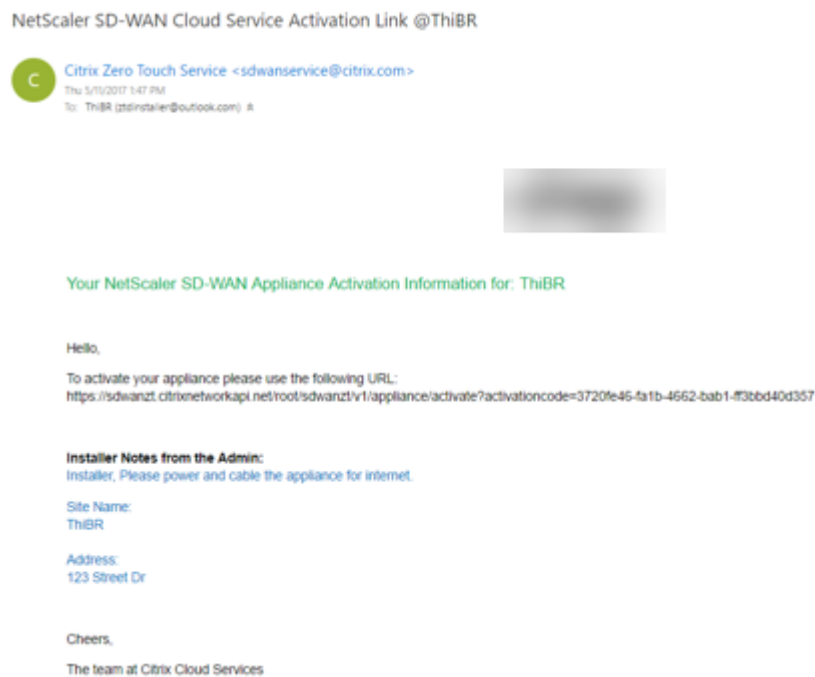
Remarque

Un déploiement zéro contact dans l'état Activation en attente peut éventuellement être choisi pour Supprimer ou Modifier, si les informations sont incorrectes. Si un site est supprimé de la page d'activation en attente, il devient disponible pour être déployé dans la page de l'onglet Déployer un nouveau site. Une fois que vous choisissez de supprimer le site de la succursale de En attente d'activation, le lien d'activation envoyé au programme d'installation devient invalide.

Si le champ Numéro de série n'a pas été renseigné par l'administrateur SD-WAN, le champ Status indique « En attente du programme d'installation » au lieu de « Connexion ».

23. La prochaine série d'activités est effectuée par l'installateur sur site.

- a) Le programme d'installation vérifie la boîte aux lettres de l'adresse de messagerie utilisée par l'administrateur SD-WAN lors du déploiement du site.



- b) Ouvrez l'URL d'activation du déploiement zéro contact dans une fenêtre de navigateur Internet (par exemple <https://sdwanzt.citrixnetworkapi.net>).
- c) Si l'administrateur SD-WAN n'a pas prérenseigné le numéro de série à l'étape du site de déploiement, le programme d'installation est chargé de localiser le numéro de série sur l'appliance physique et d'entrer le numéro de série manuellement dans l'URL d'activation, puis de cliquer sur le bouton **Activer**.



- d) Si l'administrateur préremplit les informations du numéro de série, l'URL d'activation aura déjà progressé à l'étape suivante.



e) Le programme d'installation doit être physiquement sur place pour effectuer les actions suivantes :

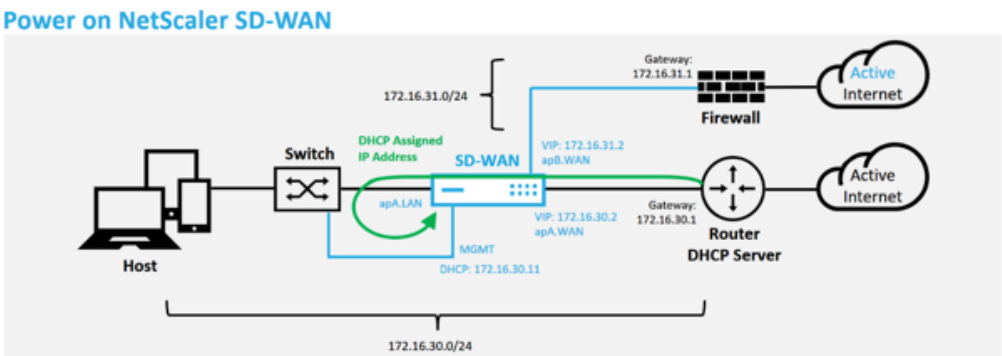
- Câblage de toutes les interfaces WAN et LAN pour qu'elles correspondent à la topologie et à la configuration construites lors des étapes précédentes.
- Câblage de l'interface de gestion (MGMT, 0/1) dans le segment du réseau qui fournit l'adresse IP DHCP et la connectivité à Internet avec la résolution DNS et FQDN vers adresse IP.
- Câble d'alimentation de l'appliance SD-WAN.
- Allumez l'interrupteur d'alimentation de l'appliance.

Remarque

La plupart des appareils s'allument automatiquement lorsque le câble d'alimentation est connecté. Il se peut que certaines appliances soient mises sous tension à l'aide de l'interrupteur d'alimentation situé à l'avant de l'appliance, d'autres peuvent avoir l'interrupteur d'alimentation à l'arrière de l'appliance. Certains interrupteurs d'alimentation nécessitent de maintenir le bouton d'alimentation jusqu'à ce que l'unité soit mise sous tension.

24. La série d'étapes suivante est automatisée à l'aide du service déploiement sans intervention, mais nécessite que les conditions préalables suivantes soient disponibles.

- Le dispositif de branche doit être mis sous tension
 - DHCP doit être disponible dans le réseau existant pour attribuer une adresse IP de gestion et DNS
 - Toute adresse IP attribuée par DHCP nécessite une connectivité à Internet avec la possibilité de résoudre les noms de domaine de domaine fqdns
 - L'attribution IP peut être configurée manuellement, tant que les autres conditions préalables sont remplies
- a) l'appliance obtient une adresse IP à partir du serveur DHCP des réseaux, dans cet exemple de topologie, elle est obtenue via les interfaces de données contournées d'un dispositif d'état par défaut d'usine.



- b) Lorsque l'apppliance obtient les adresses IP de gestion Web et DNS du serveur DHCP du réseau sous-jacent, elle lance le service de déploiement Zero Touch et télécharge toutes les mises à jour logicielles liées au déploiement zéro contact.
- c) Avec une connectivité réussie au service Cloud de déploiement zéro touche, le processus de déploiement effectue automatiquement les opérations suivantes :
- Télécharger le fichier de configuration qui est stocké précédemment par SD-WAN Center
 - Application de la configuration à l'apppliance locale
 - Télécharger et installer un fichier de licence temporaire de 10 Mo
 - Téléchargez et installez les mises à jour logicielles si nécessaire
 - Activer le service SD-WAN



- d) Une confirmation supplémentaire peut être effectuée dans l'interface de gestion Web SD-WAN Center, le menu Déploiement zéro tactile affiche les appliances activées avec succès dans l'onglet **Historique d'activation**.

Dashboard Fault Monitoring Configuration Reporting Administration

Configuration / Zero Touch Deployment / Activation History

Deploy New Site Activation History Pending Activation

Showing 1 - 1 of 1

Site Name	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
ThsBR	3F6PBQ307	ztdinstaller@outlook.com	123 Street Dr	Appliance Activated	May 11 22:18:03 2017 UTC	Activated	

- e) Il se peut que les chemins virtuels ne s'affichent pas immédiatement dans un état connecté, car le MCN peut ne pas approuver la configuration transmise par le service cloud de déploiement zéro touche, et signale une « incompatibilité de la version de configuration » dans le tableau de bord MCN.

The screenshot shows the MCN Configuration page with three main sections:

- System Status:**
 - Name: DC
 - Model: VPX
 - Appliance Mode: MCN
 - Serial Number: 1079975b-b067-ae77-1718-d7bdf0375a2b
 - Management IP Address: 172.16.10.51
 - Appliance Uptime: 3 weeks, 5 days, 22 hours, 45 minutes, 35.2 seconds
 - Service Uptime: 1 weeks, 2 days, 20 hours, 58 minutes, 57.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions:**
 - Software Version: 9.2.1.23.588434
 - Built On: Apr 21 2017 at 05:23:29
 - Hardware Version: VPX
 - OS Partition Version: 4.6
- Virtual Path Service Status:**
 - Virtual Path DC-AWSBR: Uptime: 1 hours, 12 minutes, 48.0 seconds.
 - Virtual Path 'DC-AzureBR' is currently dead.
 - Virtual Path 'DC-TierBR' is currently dead.
 - Virtual Path 'DC-ThiBR' is currently dead (Configuration version mismatch)** (highlighted with a red box)
 - Virtual Path 'DC-FouBR' is currently dead.

- f) La configuration est remise à la nouvelle appliance de succursale installée et son état est surveillé sur la page **MCN > Configuration > Réseau étendu virtuel > Gestion des modifications** (ce processus peut prendre plusieurs minutes).

The screenshot shows the MCN Configuration page with the Change Management process overview and a table of site appliances.

Change Process Overview:

- Step 1: Change Preparation** (MCN)
- Step 2: Appliance Staging** (MCN)
- Step 3: Activation** (Clients)

Configuration File Names: Active - 9d2-270-TenTwoThruAWSApure-DO-NOT-ALTER.cfg Staged - SD-WANConfiguration.zip

Site Appliance	Model	State	Currently Active	Currently Staged	Traffic Interruption	Download Package			
DC-VR	CR10K	Not Connected	9.2.1.23.588434	2019 on 5/11/17	9.2.1.23.588434	16d7 on 5/11/17	<1 min	198 ms	active / staged
AzureBR-Azure-001	CR10K	Not Connected	9.2.1.23.588434	2019 on 5/11/17	9.2.1.23.588434	16d7 on 5/11/17	<1 min	80 s	active / staged
FouBR-001	CR10K	Not Connected	Not Connected				Loc Chg Mgr		active / none
ThiBR-001	CR10K	Not Connected	Not Connected				Loc Chg Mgr		active / staged
ThiBR-002	CR10K	Not Connected	Not Connected				Loc Chg Mgr		active / staged
ThiBR-003	CR10K	Not Connected	Not Connected				Loc Chg Mgr		active / staged

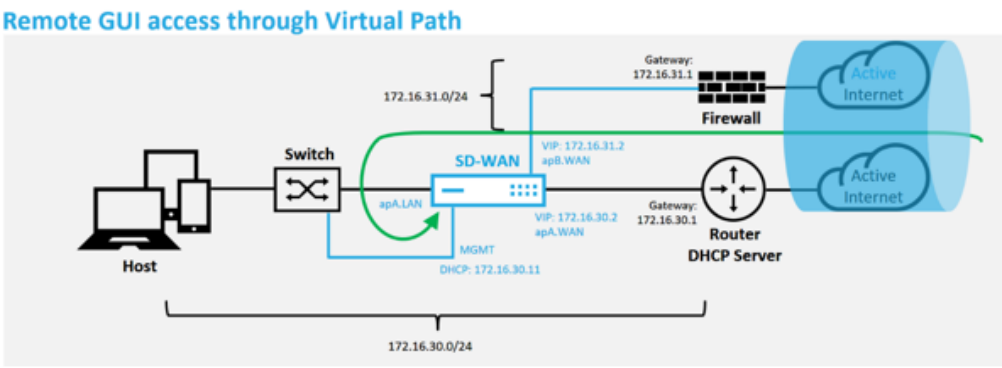
- g) L'administrateur SD-WAN peut surveiller la page de gestion Web MCN tête de ligne pour les chemins virtuels établis du site distant.

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path
13	DC-A5	ThiBR-Wifi	GOOD	GOOD	Static
14	DC-B4	ThiBR-4G	GOOD	GOOD	Static
15	ThiBR-4G	DC-B4	GOOD	GOOD	Static
16	ThiBR-Wifi	DC-A5	GOOD	GOOD	Static

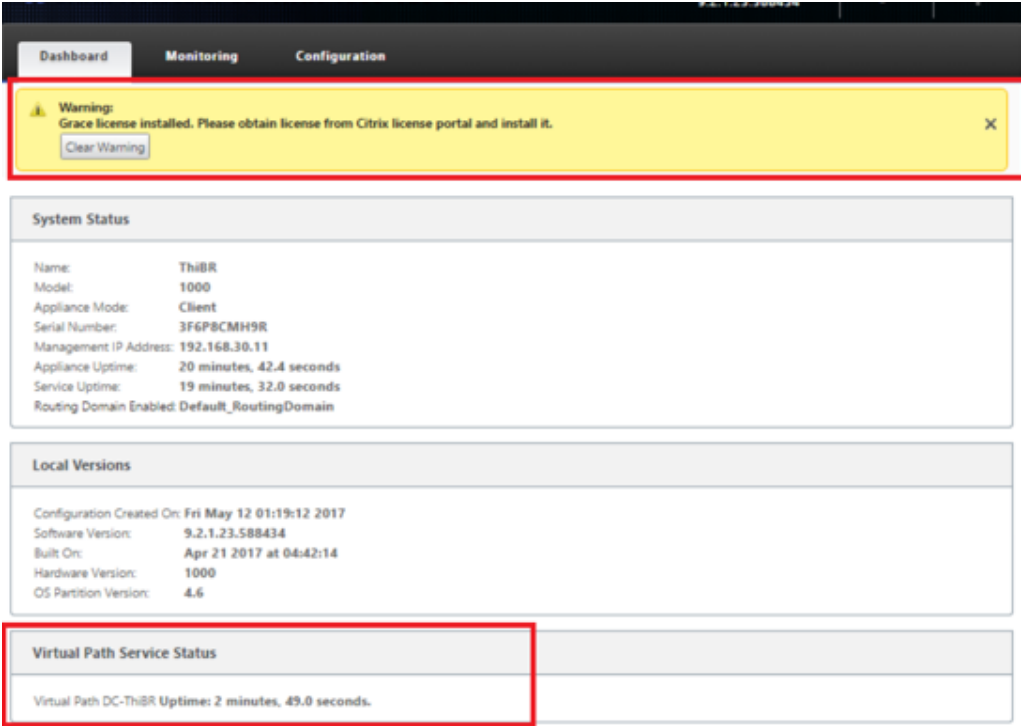
h) SD-WAN Center peut également être utilisé pour identifier l’adresse IP attribuée DHCP de l’appliance sur site à partir de la page **Configuration > Détection du réseau > Inventaire et état**.

Poll	State	Name	MGT IP Address	Model	Serial Number	Software	Registry Timestamp	Last Successful Poll	Latest Record	Download
<input checked="" type="checkbox"/>	Stats in Sync	DC	192.168.10.11	cbrpx	1079975b-b067-4e77-171b-d7bdf0375a2b	89_2_1_33_588434	1494551952	05/11/17 19:02	05/11/17 19:01	
<input checked="" type="checkbox"/>	Unknown	AWSBR	192.168.202.4							
<input checked="" type="checkbox"/>	Not Reachable	AzureBR	192.168.10.11							
<input checked="" type="checkbox"/>	Unknown	FouBR	192.168.10.11							
<input checked="" type="checkbox"/>	Not Reachable	TenBR	192.168.10.11							
<input checked="" type="checkbox"/>	Not Reachable	ThiBR	192.168.30.11							
<input checked="" type="checkbox"/>	Unknown	TweBR	192.168.30.11							

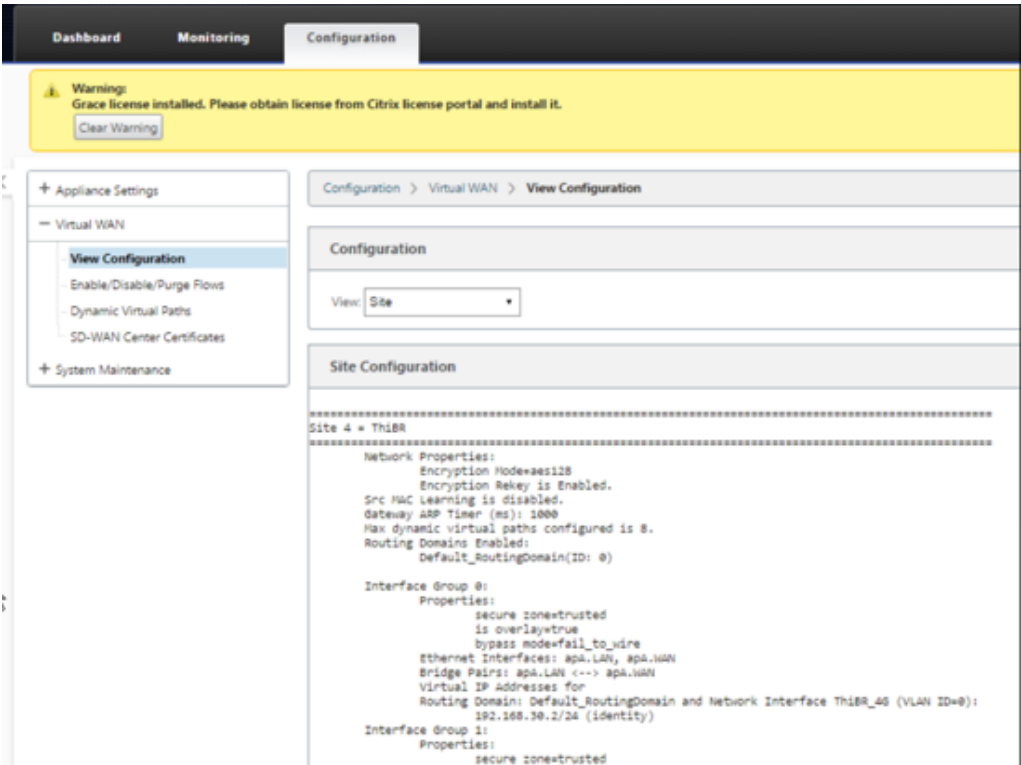
i) À ce stade, l’administrateur réseau SD-WAN peut obtenir un accès de gestion Web à l’appliance sur site à l’aide du réseau de superposition SD-WAN.



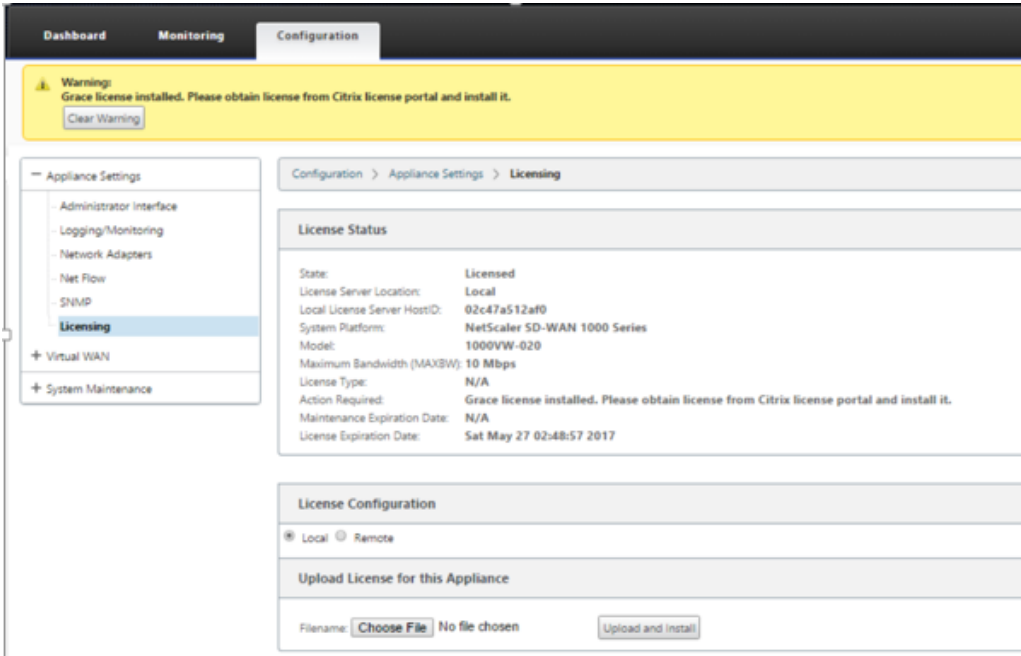
- j) L'accès de gestion Web à l'appliance de site distant indique que l'appliance a été installée avec une licence Grace temporaire à 10 Mbit/s, ce qui permet à l'état du service Virtual Path de déclarer actif.



- k) La configuration de l'appliance peut être validée à l'aide de la page **Configuration > Virtual WAN > Afficher la configuration**.



- l) Le fichier de licence de l’appliance peut être mis à jour vers une licence permanente à l’aide de la page **Configuration > Paramètres de l’appliance > Licences** .



Après le téléchargement et l’installation du fichier de licence permanent, la bannière d’avertissement Grace License disparaît et pendant le processus d’installation de la licence, aucune perte de connec-

tivité vers le site distant ne se produira (zéro pings est supprimé).

Installation locale sans intervention

May 6, 2021

Pour obtenir des instructions sur le déploiement d'une appliance SD-WAN avec le service Zero Touch, reportez-vous à la rubrique [Comment configurer le service de déploiement sans intervention](#).

AWS

May 6, 2021

Les sections suivantes décrivent comment déployer ZTD dans un environnement AWS.

Déploiement dans AWS :

Avec SD-WAN version 9.3, les capacités de déploiement sans intervention ont été étendues aux instances Cloud. La procédure de déploiement du processus de déploiement zéro contact quatre instances cloud diffère légèrement du déploiement de l'appliance pour le service zéro contact.

1. Mettez à jour la configuration pour ajouter un nouveau site distant avec un périphérique cloud SD-WAN compatible ZTD à l'aide de la configuration réseau SD-WAN Center.

Si la configuration SD-WAN n'a pas été créée à l'aide de la configuration réseau SD-WAN Center, importez la configuration active à partir du MCN et commencez à modifier la configuration à l'aide du SD-WAN Center. Pour la capacité de déploiement sans intervention, l'administrateur SD-WAN doit créer la configuration à l'aide du SD-WAN Center. La procédure suivante doit être utilisée pour ajouter un nouveau nœud de cloud destiné au déploiement sans intervention.

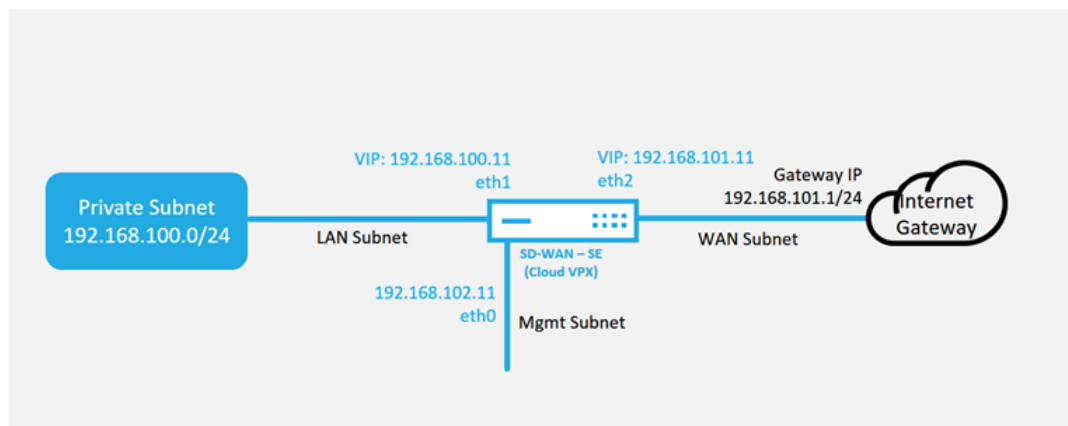
- a) Concevez le nouveau site pour le déploiement du cloud SD-WAN en décrivant d'abord les détails du nouveau site (taille VPX, utilisation des groupes d'interface, adresses IP virtuelles, lien(s) WAN avec bande passante et passerelles respectives).

Remarque

- Les instances SD-WAN déployées dans le cloud doivent être déployées en mode Edge/Gateway.
- Le modèle pour l'instance de cloud est limité à trois interfaces : Gestion, LAN et WAN (dans cet ordre).
- Les modèles de cloud disponibles pour SD-WAN VPX sont actuellement config-

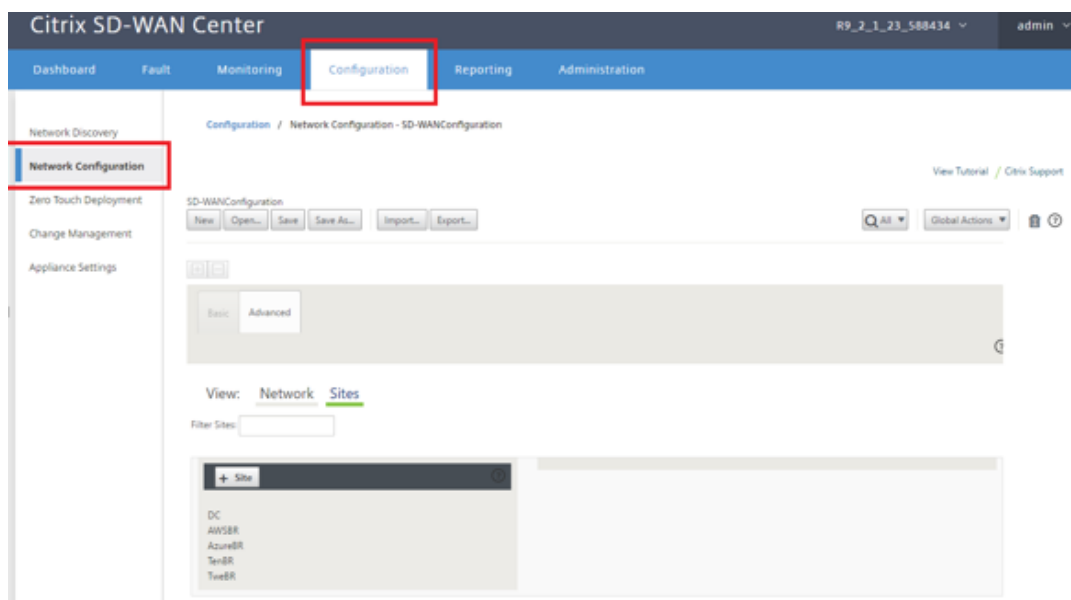
urés pour obtenir l'adresse IP #.#.#.#.11 des sous-réseaux disponibles dans le VPC.

Cloud Topology with NetScaler SD-WAN



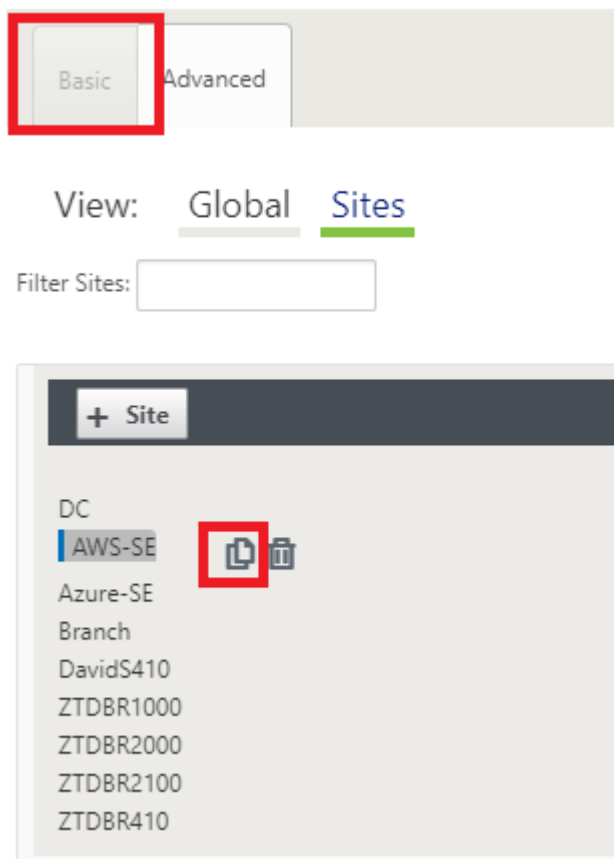
Il s'agit d'un exemple de déploiement d'un site cloud SD-WAN déployé, le périphérique Citrix SD-WAN est déployé en tant que périphérique desservant une seule liaison Internet WAN dans ce réseau cloud. Les sites distants pourront tirer parti de plusieurs liaisons WAN Internet distinctes qui se connectent à cette même passerelle Internet pour le cloud, offrant une résilience et une connectivité de bande passante agrégée à partir de n'importe quel site de déploiement SD-WAN vers l'infrastructure cloud. Cela fournit une connectivité rentable et hautement fiable au cloud.

- b) Ouvrez l'interface de gestion Web SD-WAN Center et accédez à la page **Configuration > Configuration réseau**.



- c) Assurez-vous qu'une configuration opérationnelle est déjà en place ou importez la configuration à partir du MCN.

- d) Accédez à l'onglet Basic pour créer un nouveau site.
- e) Ouvrez la vignette Sites pour afficher les sites actuellement configurés.
- f) Création rapide de la configuration pour le nouveau site cloud en utilisant la fonctionnalité de clone de n'importe quel site existant, ou création manuelle d'un nouveau site.



- g) Remplissez tous les champs requis à partir de la topologie conçue précédemment pour ce nouveau site cloud

Gardez à l'esprit que le modèle disponible pour les déploiements ZTD cloud est difficile à utiliser l'adresse IP #. #. #.11 pour les sous-réseaux Mgmt, LAN et WAN. Si la configuration n'est pas définie pour correspondre à l'adresse d'hôte IP .11 attendue pour chaque interface, le périphérique ne sera pas en mesure d'établir correctement l'ARP sur les passerelles de l'environnement cloud et la connectivité IP sur le chemin virtuel du MCN.

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name: ! Appliance Name: Secure Key:

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
E1Vlan0	0	<input type="checkbox"/>
E2Vlan0	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	E1Vlan0	192.168.100.11/2 !
<input checked="" type="checkbox"/>	E2Vlan0	192.168.101.11/2 !

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type
<input checked="" type="checkbox"/>	AWS-INET !	Public Internet

Access Interfaces

Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	AWS-INET-AI-1	E2Vlan0	192.168.101.11 !	192.168.101.1 !

h) Après le clonage d'un nouveau site, accédez aux **paramètres de base** du site et vérifiez que le modèle de SD-WAN est correctement sélectionné pour prendre en charge le service sans intervention.

Edit Site Settings

Appliance Name:

Model:

☐ Enable Site as Intermediate Node

☐ Enable Dynamic Virtual Paths

View: **Global** Site

Filter Sites:

+ Site

DC

- AWS-SE
- Azure-SE
- Branch
- DavidS410
- ZTDBR1000
- ZTDBR2000
- ZTDBR2100
- ZTDBR410

Appliance

AWS-SE-CBVPX

Model:

Interfaces

Ethernet Port 1

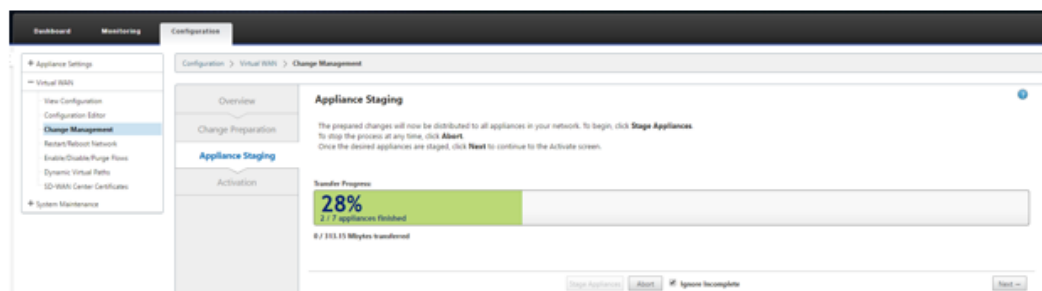
Ethernet Port 2

Model: Fail-to-Block, Trusted

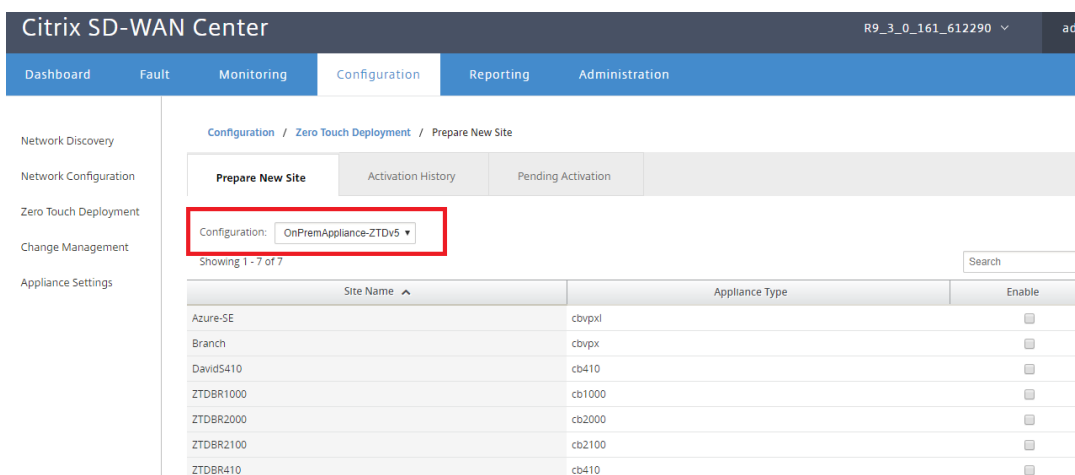
VLANs: 0 (192.168.101.11/24)

i) Enregistrez la nouvelle configuration sur SD-WAN Center et utilisez l'option d'exportation vers la **boîte de réception de la gestion des modifications** pour pousser la configuration à l'aide de la gestion des modifications.

- j) Suivez la procédure de gestion des modifications pour organiser correctement la nouvelle configuration, ce qui rend les périphériques SD-WAN existants conscients du nouveau site à déployer via zéro contact, vous devrez utiliser l'option *Ignorer incomplet pour ignorer* la tentative de pousser la configuration vers le nouveau site que doit encore passer par le flux de travail ZTD.



2. Revenez à la page SD-WAN Center Zero Touch Deployment et lorsque la nouvelle configuration active est en cours d'exécution, le nouveau site sera disponible pour le déploiement.
 - a) Dans la page Déploiement sans contact, sous l'onglet **Déployer un nouveau site**, sélectionnez le fichier de configuration réseau en cours d'exécution.
 - b) Une fois le fichier de configuration en cours d'exécution sélectionné, la liste de tous les sites de branche avec des périphériques Citrix SD-WAN non déployés qui sont pris en charge pour zéro contact s'affiche.



- c) Sélectionnez le site cloud cible que vous souhaitez déployer à l'aide du service Zero Touch, cliquez sur **Activer**, puis **Provisionner et déployer**.

Site Name ^	Appliance Type	Enable
AWS-SE	cbvpxl	<input checked="" type="checkbox"/>
Azure-SE	cbvpxl	<input type="checkbox"/>
Branch	cbvpx	<input type="checkbox"/>
DavidS410	cb410	<input type="checkbox"/>
ZTDBR1000	cb1000	<input type="checkbox"/>
ZTDBR2000	cb2000	<input type="checkbox"/>
ZTDBR2100	cb2100	<input type="checkbox"/>
ZTDBR410	cb410	<input type="checkbox"/>

Deploy

Provision and Deploy

- d) Une fenêtre contextuelle s’affiche, où l’administrateur Citrix SD-WAN peut lancer le déploiement pour Zero Touch.

Remplissez une adresse e-mail dans laquelle l’URL d’activation peut être remise, puis sélectionnez le **type de provision** pour le Cloud souhaité.

Provision and Deploy

Site Name:

AWS-SE

Installer Email:

ztdinstaller@outlook.com

Provision Type

AWS

Next

- e) Après avoir cliqué sur **Suivant**, sélectionnez la région appropriée, la taille de l’instance, remplissez correctement les champs Nom de clé SSH et ARN de rôle.

Provision and Deploy AWS

AWS Region

US West (Oregon)

AWS Instance Size

m4.2xlarge

SSH Key Name:

aws-ztd

Role ARN:

arn:aws:iam::*****:role/ZeroTouch

Back

Deploy

Remarque

Utilisez les liens d’aide pour obtenir des conseils sur la configuration de l’ARN de clé et de rôle SSH sur le compte Cloud. Assurez-vous également que la région de sélection correspond à ce qui est disponible sur le compte et que la taille de l’instance

sélectionnée correspond à VPX ou VPXL comme modèle sélectionné dans la configuration SD-WAN.

- f) Cliquez sur **Déployer**, déclenchant SD-WAN Center, précédemment enregistré auprès du service cloud ZTD, pour partager la configuration de ce site afin qu’il soit stocké temporairement dans le service cloud ZTD.
- g) Accédez à l’onglet **Activation en attente** pour confirmer que les informations du site ont bien été remplies et qu’elles ont été placées dans un état d’approvisionnement.

Configuration / Zero Touch Deployment / Pending Activation

Prepare New Site	Activation History	Pending Activation			
Showing 1 - 1 of 1					
<div>Search</div>					
Site Name ^	Serial No	Installer Email	Address	Status	Action
AWS-SE	2E20EFCF-1A26-42DC-86D0-5624FD27C37F	ztdinstaller@outlook.com	AWS - US West (Oregon)	Provisioning	<div></div>
<div>Delete</div>		<div>Modify</div>			

3. Lancez le processus de déploiement sans intervention en tant qu’administrateur Cloud.
- a) Le programme d’installation devra vérifier la boîte aux lettres de l’adresse de messagerie utilisée par l’administrateur SD-WAN lors du déploiement du site.

NetScaler SD-WAN Cloud Service Activation Link @AWS-SE

C

Citrix Zero Touch Service <sdwanservice@citrix.com>
Today, 11:01 AM
You

Reply all

Inbox

NetScaler SD-WAN Appliance Activation Information

To begin the process of activating your appliance, [click here](#) .
(Or paste this URL into your browser
`https://sdwanzt.citrixnetworkapi.net/root/sdwanz/v1/appliance/activate?activationcode=67940818-abb8-47f0-9f17-9a20a3955d57`)

Site Name

AWS-SE

Address

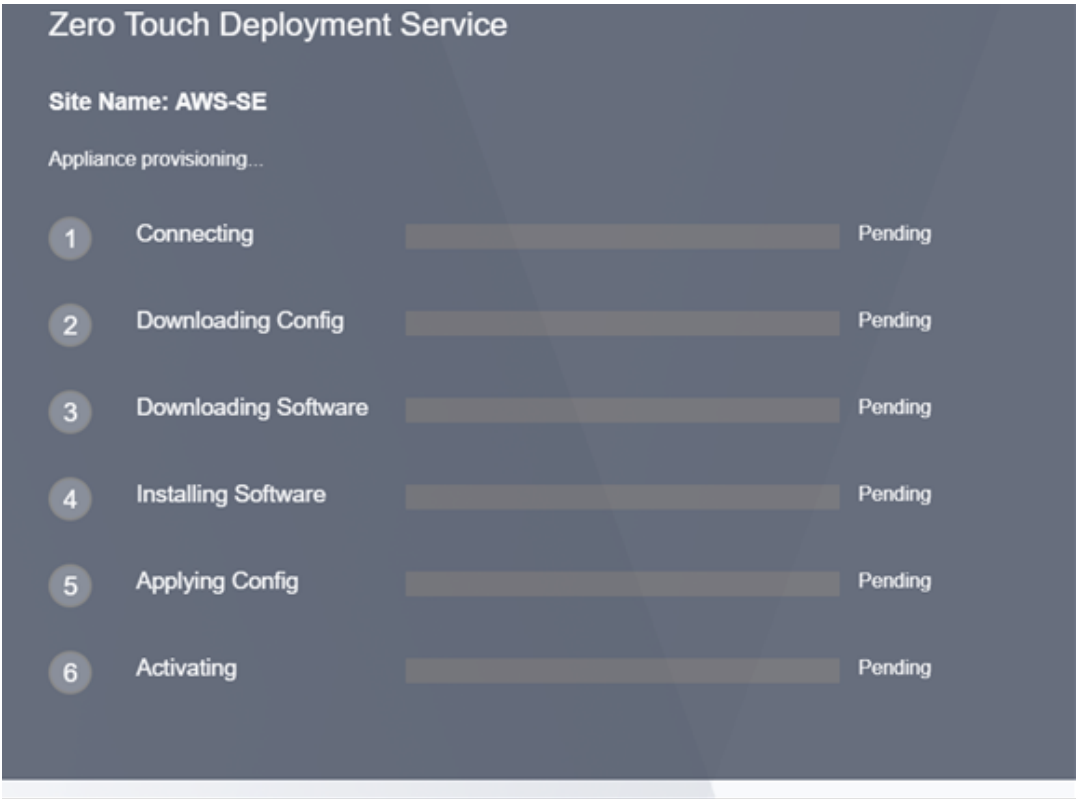
AWS - US West (Oregon)

Additional Notes

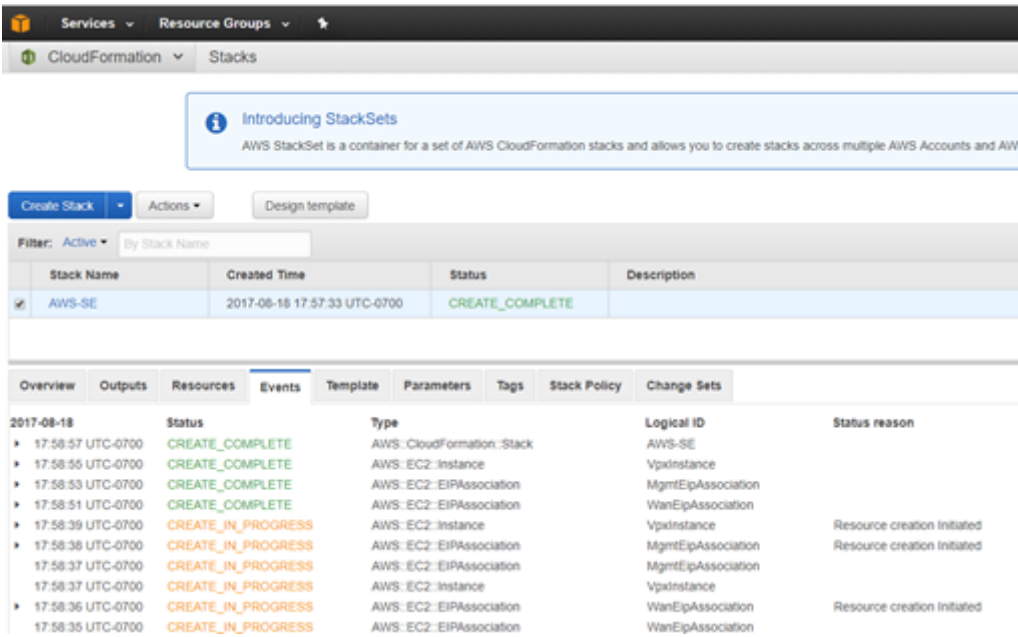
The NetScaler SD-WAN Team

*** This is an automatically generated email, please do not reply ***

- b) Ouvrez l'URL d'activation trouvée dans l'e-mail dans une fenêtre de navigateur Internet (exemple ;<https://sdwanzt.citrixnetworkapi.net>).
- c) Si la clé SSH et l'ARN de rôle sont correctement entrés, le service de déploiement sans intervention commencera immédiatement à provisionner l'instance SD-WAN, sinon des erreurs de connexion s'afficheront immédiatement.



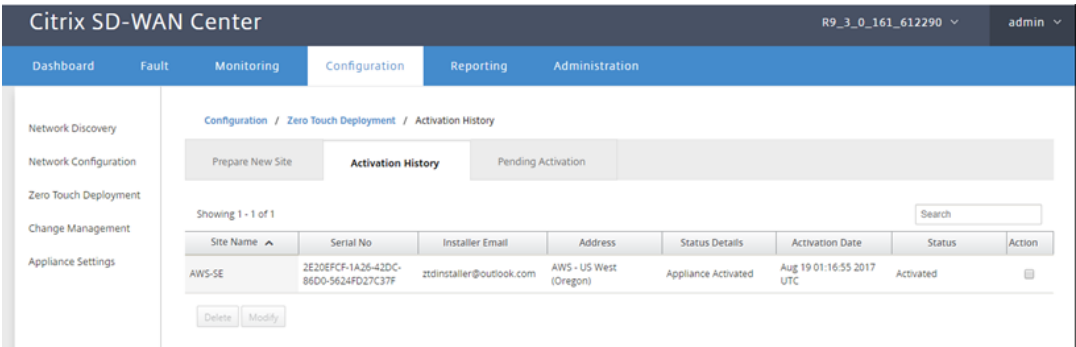
- d) Pour un dépannage supplémentaire sur la console AWS, le service Cloud Formation peut être utilisé pour détecter tous les événements qui se produisent au cours du processus de Provisioning.



- e) Autorisez le processus de provisionnement ~ 8-10 minutes et l'activation d'une autre ~ 3-5 minutes pour terminer complètement.
- f) Avec la connectivité réussie de l'instance de cloud SD-WAN au service de cloud ZTD, le service effectue automatiquement les opérations suivantes :
- Télécharger le fichier de configuration spécifique au site qui a été stocké précédemment par SD-WAN Center
 - Application de la configuration à l'instance locale
 - Télécharger et installer un fichier de licence temporaire de 10 Mo
 - Téléchargez et installez les mises à jour logicielles si nécessaire
 - Activer le service SD-WAN



g) Une confirmation supplémentaire peut être effectuée dans l’interface de gestion Web SD-WAN Center ; le menu Déploiement Zero Touch affiche les appliances activées avec succès dans l’onglet **Historique des activations** .



h) Les chemins virtuels peuvent ne pas s’afficher immédiatement dans un état connecté, car le MCN peut ne pas faire confiance à la configuration transmise à partir du service cloud ZTD et signale une *incompatibilité de version de configuration* dans le tableau de bord MCN.

DashboardMonitoringConfiguration

System Status

Name:DC

Model:VPX

Appliance Mode:MCN

Serial Number:b536a38c-5f48-b720-4f8d-b3f50b23f69f

Management IP Address:172.16.10.30

Appliance Uptime:1 weeks, 2 days, 3 hours, 50 minutes, 18.3 seconds

Service Uptime:1 weeks, 2 days, 3 hours, 42 minutes, 19.0 seconds

Routing Domain Enabled:Default_RoutingDomain

Local Versions

Software Version:9.3.0.161.612290

Built On:Aug 8 2017 at 14:45:01

Hardware Version:VPX

OS Partition Version:4.6

Virtual Path Service Status

Virtual Path DC-Branch:Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.

Virtual Path 'DC-DavidS410' is currently dead.

Virtual Path DC-ZTDBR1000:Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.

Virtual Path 'DC-ZTDBR2000' is currently dead.

Virtual Path 'DC-ZTDBR2100' is currently dead.

Virtual Path 'DC-ZTDBR410' is currently dead.

Virtual Path 'DC-AWS-SE' is currently dead (Configuration version mismatch)

Virtual Path 'DC-Azure-SE' is currently dead.

- i) La configuration sera automatiquement remise à la nouvelle appliance de succursale installée, dont l'état peut être suivi sur la page **MCN >Configuration> Réseauétendu virtuel>Gestion des modifications** (en fonction de la connectivité, cette peut prendre plusieurs minutes à terminer).

DashboardMonitoringConfiguration

+

Appliance Settings

-Virtual WAN

- View Configuration
- Configuration Editor
- Change Management
- Change Management Settings
- Restart/Reboot Network
- Enable/Disable/Purge Flows
- Dynamic Virtual Paths
- SD-WAN Center Certificates

+

System Maintenance

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Change Process Overview

The Change Management process allows a user to upload changes to the network, whether it t processes that ensure that configuration changes and software updates are applied in a reliable

Step 1

Change Preparation

Upload Files to MCN

■■■■■■■■■■→MCN

Step 2

Appliance

Transfer Files

■■■■■■■■■■MCN■■■■■■■■■■

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a pr

Configuration Filenames: Active - OnPremAppliance-ZTDv5.zip Stag

Search

Site-Appliance	Model	State	Currently Active		Current
			Software	Config	Software
DC-DC_SDWAN	CBVPX		9.3.0.161.612290	10:55 on 8/18/17	9.3.0.161.612290
AWS-SE-AWS-SE-CBVPX	CBVPXL	6%	9.3.0.161.612290		
Azure-SE-Azure-SE-CBVPX	CBVPXL	Not Connected			
Branch-Branch_SDWAN	CBVPX		9.3.0.161.612290	10:55 on 8/18/17	9.3.0.161.612290

j) L’administrateur SD-WAN peut surveiller la page de gestion Web MCN tête de ligne pour les chemins virtuels établis du site cloud nouvellement ajouté.

DashboardMonitoringConfiguration

Statistics

Flows

Routing Protocols

Firewall

IKL/Ipsec

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

Monitoring > Statistics

Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Start Show latest data.

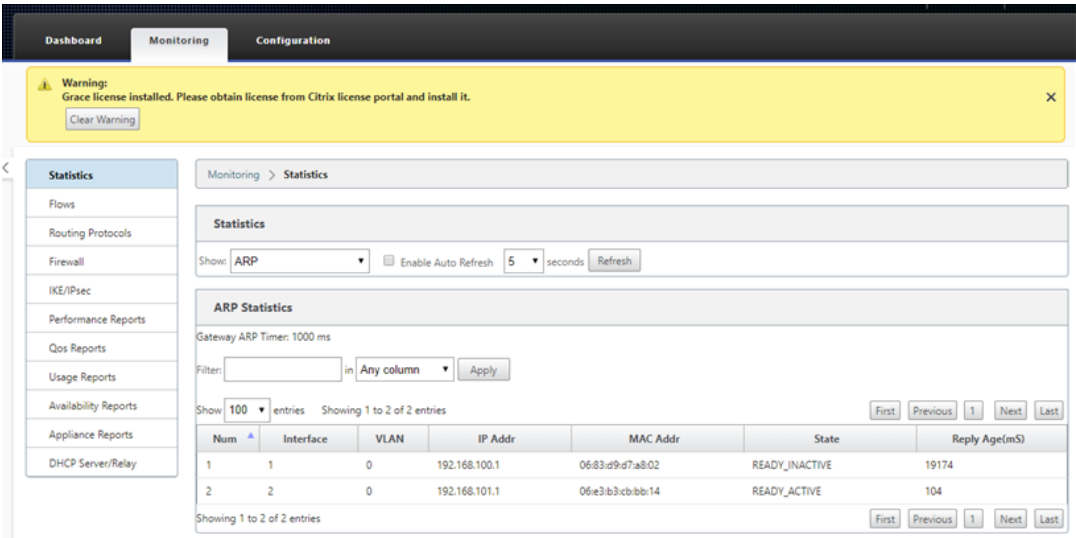
Path Statistics Summary

Filter: AWS in Any column Apply

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
27	DC-INET	AWS-INET	GOOD	GOOD	Static	26	2	0.00	16.20	NO
28	AWS-INET	DC-INET	GOOD	GOOD	Static	26	2	0.00	15.13	NO

Showing 1 to 2 of 2 entries (filtered from 30 total entries)
Bandwidth calculated over the last 0.956 seconds

k) Si un dépannage est nécessaire, ouvrez l’interface utilisateur des instances SD-WAN à l’ aide de l’adresse IP publique attribuée par l’environnement de cloud pendant le provi- sionnement, et utilisez la table ARP de la page **Surveillance > Statistiques** pour identifier les problèmes de connexion aux passerelles attendues ou utilisez le traceroute et les op- tions de capture de paquets dans les diagnostics.



Azure

May 6, 2021

La procédure de déploiement du processus de déploiement sans intervention pour les instances de cloud diffère légèrement du déploiement de l’appliance pour le service sans intervention.

Mettre à jour la configuration pour ajouter un nouveau site distant avec un périphérique cloud SD-WAN compatible ZTD à l’aide de la configuration réseau SD-WAN Center

Si la configuration SD-WAN n’a pas été créée à l’aide de la configuration réseau SD-WAN Center, importez la configuration active à partir du MCN et commencez à modifier la configuration à l’aide du SD-WAN Center. Pour la capacité de déploiement sans intervention, l’administrateur SD-WAN doit créer la configuration à l’aide du SD-WAN Center. La procédure suivante doit être utilisée pour ajouter un nouveau nœud de cloud destiné au déploiement sans intervention.

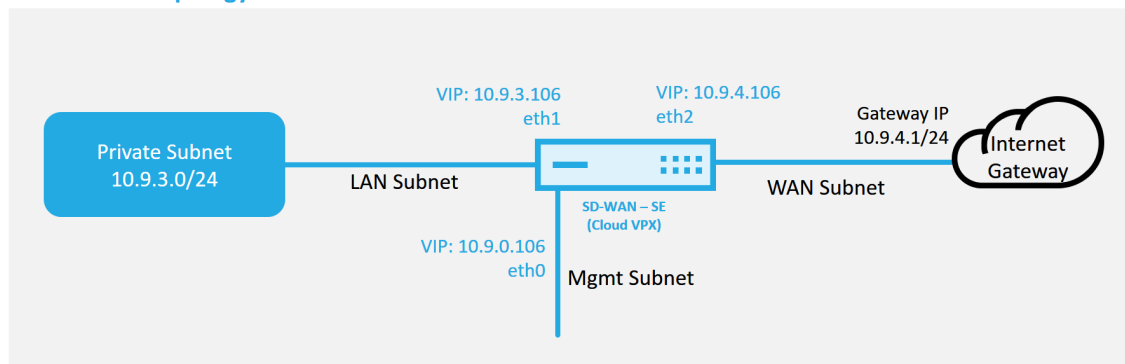
1. Concevez le nouveau site pour le déploiement du cloud SD-WAN en décrivant d’abord les détails du nouveau site (taille VPX, utilisation des groupes d’interface, adresses IP virtuelles, lien(s) WAN avec bande passante et passerelles respectives).

Remarque

- Les instances SD-WAN déployées dans le cloud doivent être déployées en mode Edge/-Gateway.
- Le modèle pour l’instance de cloud est limité à trois interfaces : Gestion, LAN et WAN (dans cet ordre).

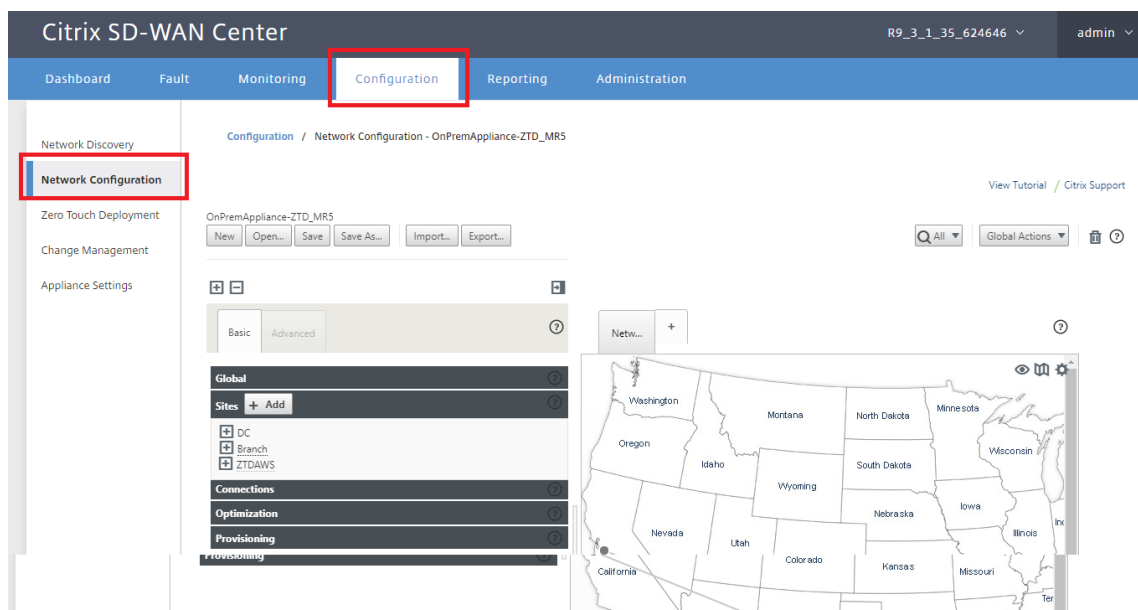
- Les modèles de cloud Azure disponibles pour SD-WAN VPX sont actuellement définis pour obtenir l'adresse IP 10.9.4.106 pour le réseau étendu, 10.9.3.106 IP pour le réseau local et 10.9.0.16 IP pour l'adresse de gestion. La configuration SD-WAN pour le nœud Azure ciblé pour Zero Touch doit correspondre à cette disposition.
- Le nom du site Azure dans la configuration doit être en minuscules sans caractères spéciaux (par exemple ztdazure).

Azure Cloud Topology with NetScaler SD-WAN

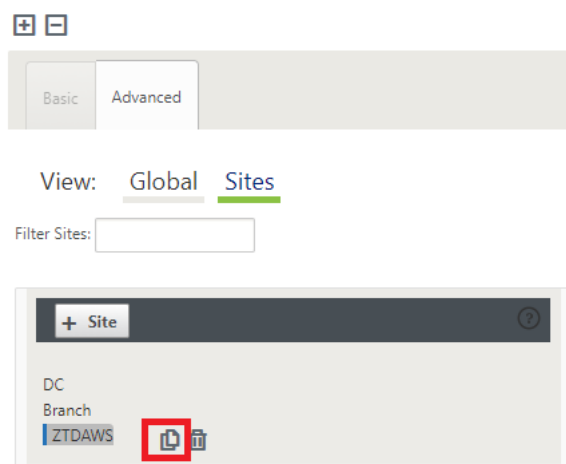


Il s'agit d'un exemple de déploiement d'un site cloud SD-WAN déployé, le périphérique Citrix SD-WAN est déployé en tant que périphérique desservant une seule liaison Internet WAN dans ce réseau cloud. Les sites distants pourront tirer parti de plusieurs liaisons WAN Internet distinctes qui se connectent à cette même passerelle Internet pour le cloud, offrant une résilience et une connectivité de bande passante agrégée à partir de n'importe quel site de déploiement SD-WAN vers l'infrastructure cloud. Cela fournit une connectivité rentable et hautement fiable au cloud.

2. Ouvrez l'interface de gestion Web SD-WAN Center et accédez à la page **Configuration > Configuration réseau**.



3. Assurez-vous qu'une configuration opérationnelle est déjà en place ou importez la configuration à partir du MCN.
4. Accédez à l'onglet Basic pour créer un nouveau site.
5. Ouvrez la vignette Sites pour afficher les sites actuellement configurés.
6. Création rapide de la configuration pour le nouveau site cloud en utilisant la fonctionnalité de clone de n'importe quel site existant, ou création manuelle d'un nouveau site.



7. Remplissez tous les champs requis à partir de la topologie conçue précédemment pour ce nouveau site cloud.

Gardez à l'esprit que le modèle disponible pour les déploiements ZTD cloud Azure est actuellement difficile pour obtenir l'adresse IP 10.9.4.106 pour le réseau étendu, 10.9.3.106 IP pour le réseau local et 10.9.0.16 IP pour l'adresse de gestion. Si la configuration n'est pas définie pour correspondre à l'adresse VIP attendue pour chaque interface, le périphérique ne sera pas en

mesure d'établir correctement ARP sur les passerelles de l'environnement cloud et la connectivité IP sur le chemin virtuel du MCN.

Il est d'importance que le nom du site soit conforme à ce que Azure attend. Le nom du site doit être en minuscules, au moins 6 caractères, sans caractères spéciaux, il doit confirmer à l'expression régulière suivante **^[a-z][a-z0-9-]{1,61}[a-z0-9]\$**.

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name:

Appliance Name:

Secure Key:

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
E1Vlan0	0	<input type="checkbox"/>
E2Vlan0	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	E1Vlan0	10.9.3.106/24
<input checked="" type="checkbox"/>	E2Vlan0	10.9.4.106/24

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type
<input checked="" type="checkbox"/>	Azure-INET	Public Internet

Access Interfaces

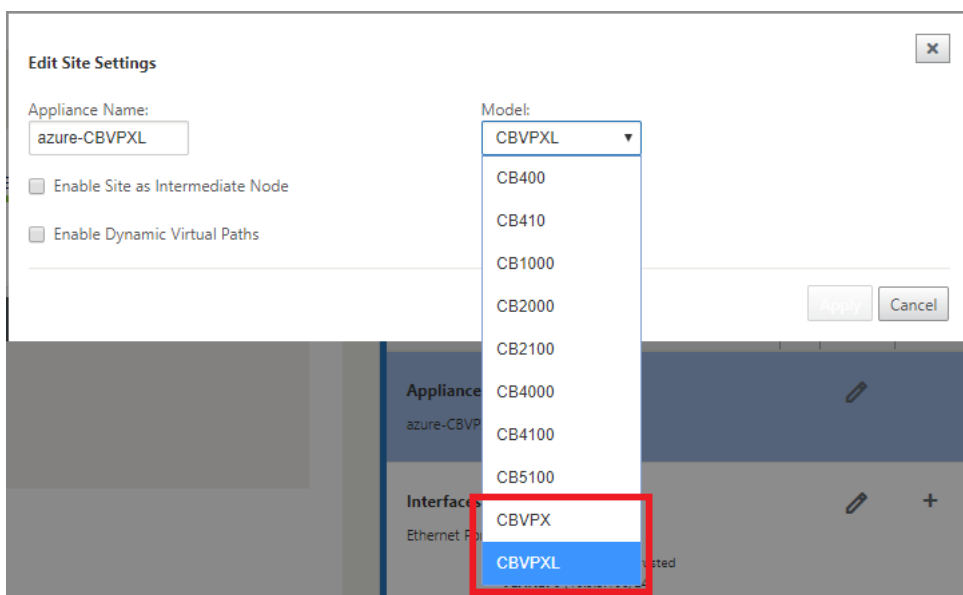
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	Azure-WL-1-AI-1	E2Vlan0	10.9.4.106	10.9.4.1

GRE Tunnels

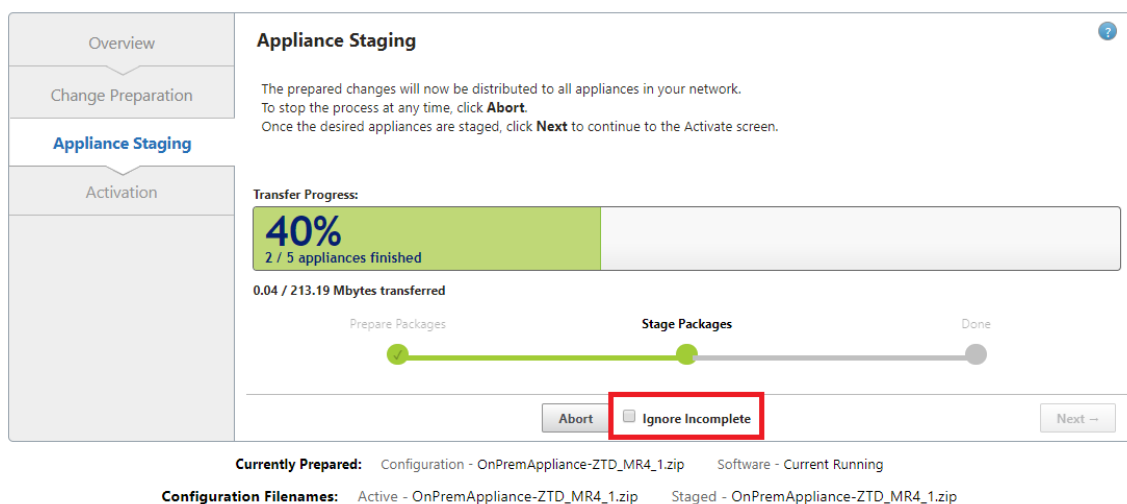
Include	Name	Source IP	Destination IP	Tunnel IP / Prefix
---------	------	-----------	----------------	--------------------

Clone Cancel

- Après le clonage d'un nouveau site, accédez aux **paramètres de base** du site et vérifiez que le modèle de SD-WAN est correctement sélectionné pour prendre en charge le service sans intervention.

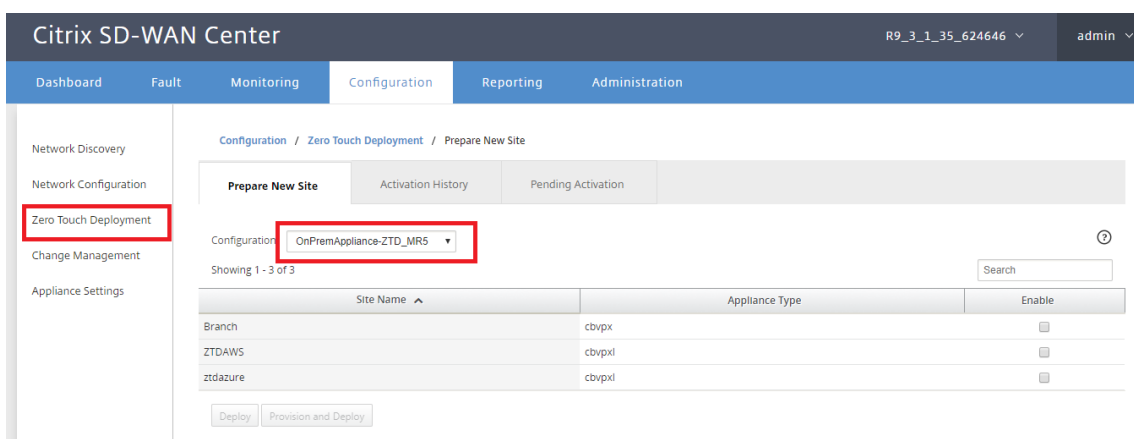


9. Enregistrez la nouvelle configuration sur SD-WAN Center et utilisez l'option d'exportation vers la **boîte de réception de la gestion des modifications** pour pousser la configuration à l'aide de la gestion des modifications.
10. Suivez la procédure de gestion des modifications pour organiser correctement la nouvelle configuration, ce qui rend les périphériques SD-WAN existants conscients du nouveau site à déployer via zéro contact, vous devrez utiliser l'option *Ignorer incomplet pour ignorer* la tentative de pousser la configuration vers le nouveau site que doit encore passer par le flux de travail ZTD.

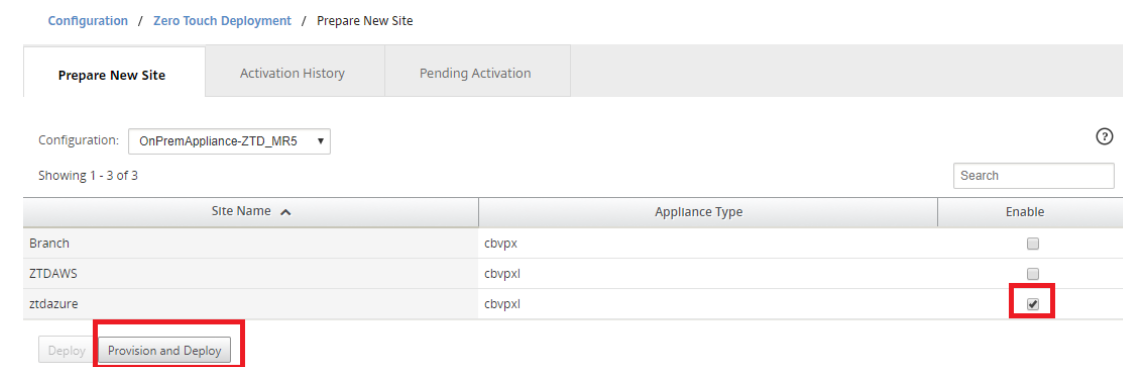


Accédez à la page Déploiement zéro tactile du SD-WAN Center, et lorsque la nouvelle configuration active est en cours d'exécution, le nouveau site sera disponible pour le provisionnement de SD-WAN Center et le déploiement d'Azure (Étape 1 sur 2)

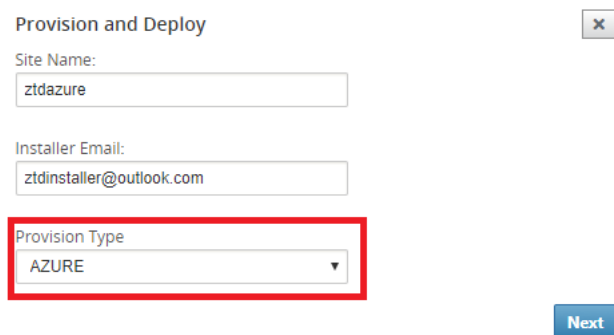
1. Dans la page déploiement sans intervention, connectez-vous avec vos informations d'identification de compte Citrix. Sous l'onglet **Déployer un nouveau site**, sélectionnez le fichier de configuration réseau en cours d'exécution.
2. Une fois le fichier de configuration en cours d'exécution sélectionné, la liste de tous les sites de branche avec des périphériques Citrix SD-WAN compatibles ZTD s'affiche.



3. Sélectionnez le site cloud cible que vous souhaitez déployer à l'aide du service Zero Touch, cliquez sur **Activer**, puis **Provisionner et déployer**.



4. Une fenêtre contextuelle s'affiche, où l'administrateur Citrix SD-WAN peut lancer le déploiement pour Zero Touch. Vérifiez que le nom du site est conforme aux exigences sur Azure (minuscules sans caractères spéciaux). Remplissez une adresse e-mail dans laquelle l'URL d'activation peut être remise, puis sélectionnez Azure comme **Type de provisionnement** pour le Cloud souhaité, avant de cliquer sur **Suivant**.



Provision and Deploy

Site Name:
ztdazure

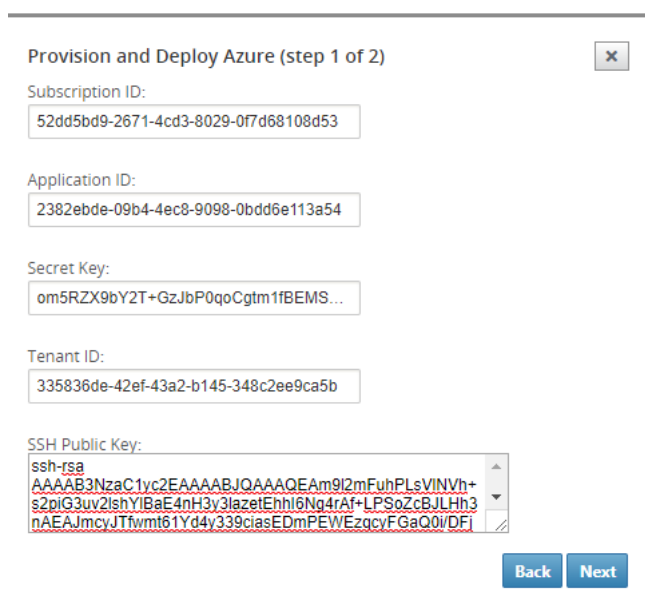
Installer Email:
ztdinstaller@outlook.com

Provision Type
AZURE

Next

5. Après avoir cliqué sur **Suivant**, la fenêtre Provisionner et déployer Azure (étape 1 of 2) nécessitera l'entrée de obtenu à partir du compte Azure.

Copiez et collez chaque champ requis après avoir obtenu les informations de votre compte Azure. Les étapes ci-dessous expliquent comment obtenir l'ID d'abonnement, l'ID d'application, la clé secrète et l'ID de locataire requis à partir de votre compte Azure, puis cliquez sur **Suivant**.



Provision and Deploy Azure (step 1 of 2)

Subscription ID:
52dd5bd9-2671-4cd3-8029-0f7d68108d53

Application ID:
2382ebde-09b4-4ec8-9098-0bdd6e113a54

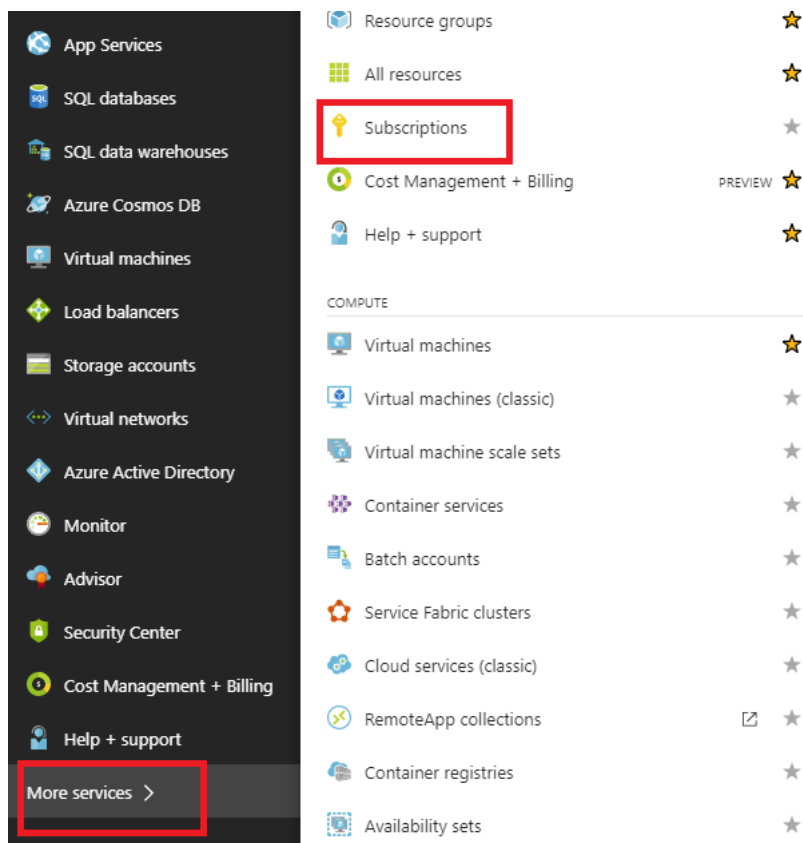
Secret Key:
om5RZX9bY2T+GzJbP0qoCgtm1fBEMS...

Tenant ID:
335836de-42ef-43a2-b145-348c2ee9ca5b

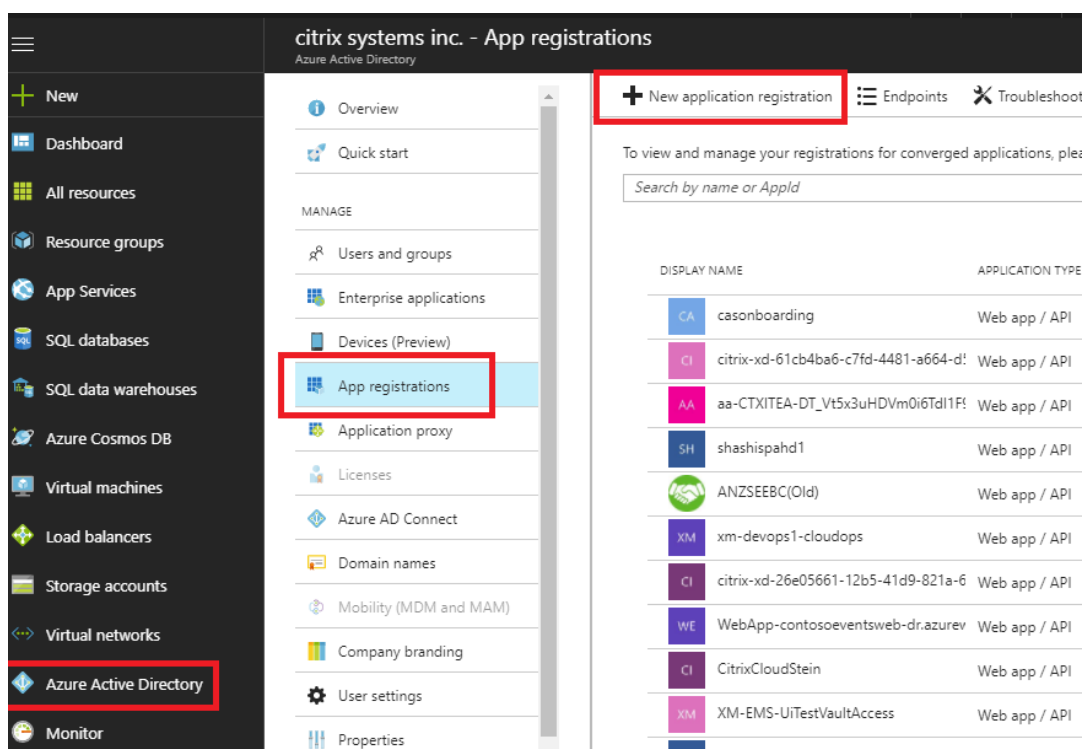
SSH Public Key:
ssh-rsa
AAAAB3NzaC1vc2EAAAABJQAAAAQEAml2mFuhPLsVINVh+s2piG3uv2lshYlBaE4nH3y3lazeEhhl6Ng4rAf+LPSoZcBJLHh3nAEAJmcyJTfwmt61Yd4y339ciasEDmPEWEzgcyFGaQ0i/DFI

Back Next

- a) Sur le compte Azure, nous pouvons identifier l'**ID d'abonnement** requis en accédant à « Plus de services » et en sélectionnant **Abonnements**.



- b) Pour identifier le ***ID d'application requis**, accédez à Azure Active Directory, Inscriptions d'application, puis cliquez sur **Nouvelle inscription d'application**.



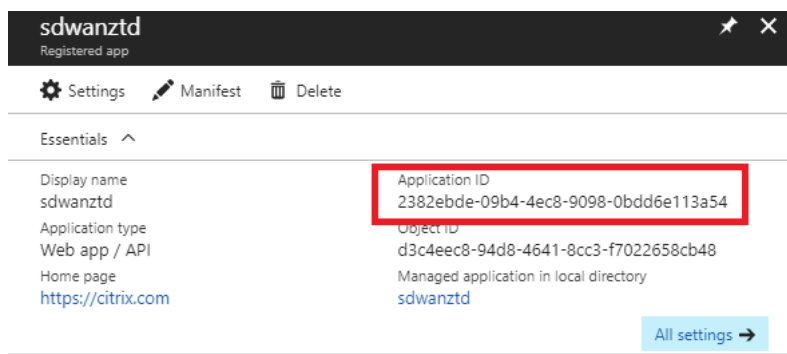
- c) Dans le menu Créer l'enregistrement de l'application, entrez un nom et une URL d'authentification (il peut s'agir de n'importe quelle URL, la seule condition requise est qu'elle soit valide), puis cliquez sur **Créer**.

The 'Create' dialog box is shown with the following fields:

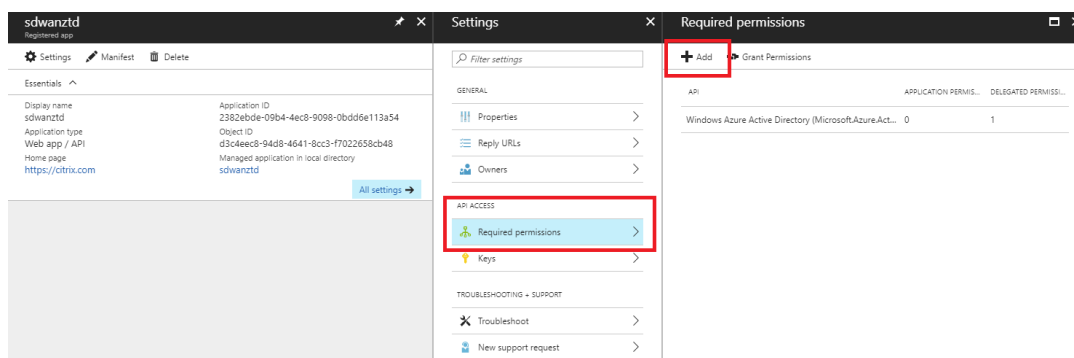
- Name**: sdwanztd (with a green checkmark)
- Application type**: Web app / API (dropdown menu)
- Sign-on URL**: https://citrix.com (with a green checkmark)

A blue 'Create' button is located at the bottom of the dialog.

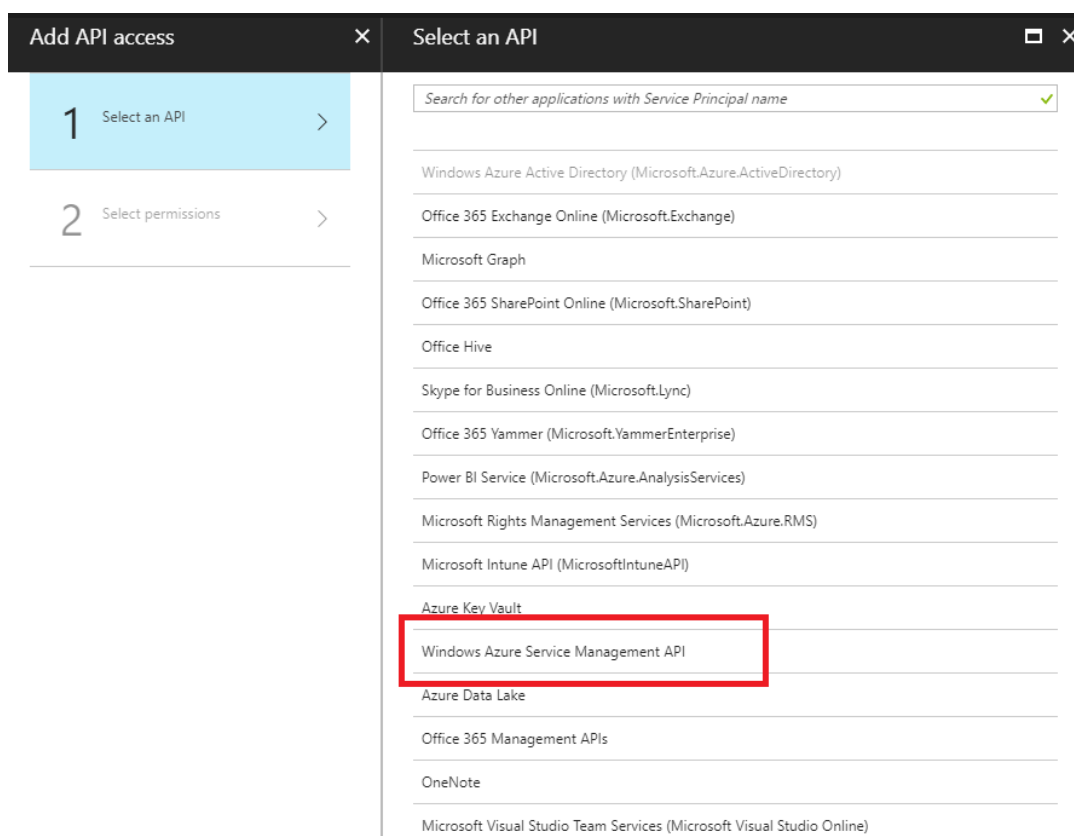
- d) Recherchez et ouvrez l'application enregistrée nouvellement créée, et notez l'ID de l'application.



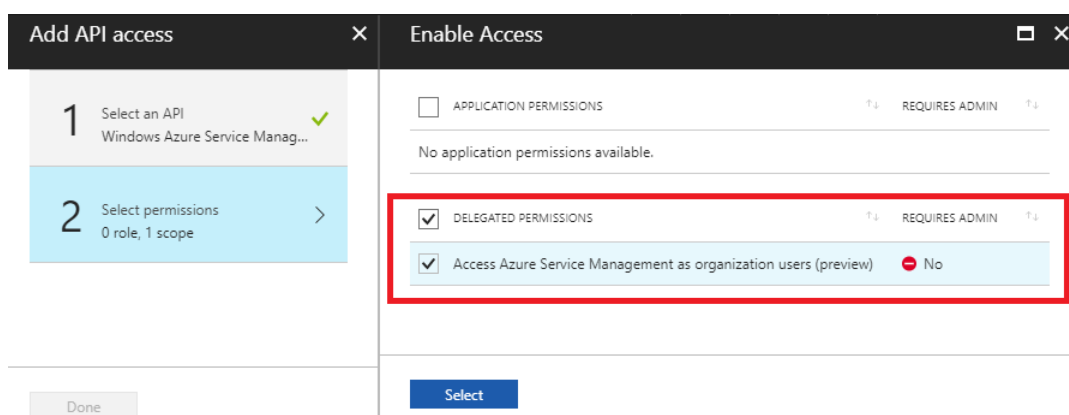
- e) Ouvrez à nouveau l'application d'enregistrement nouvellement créée, et pour identifier la *clé de sécurité* requise, sous Accès API, sélectionnez **Autorisations requises**, pour permettre à un tiers de provisionner et d'effectuer une instance. Sélectionnez ensuite **Ajouter**.



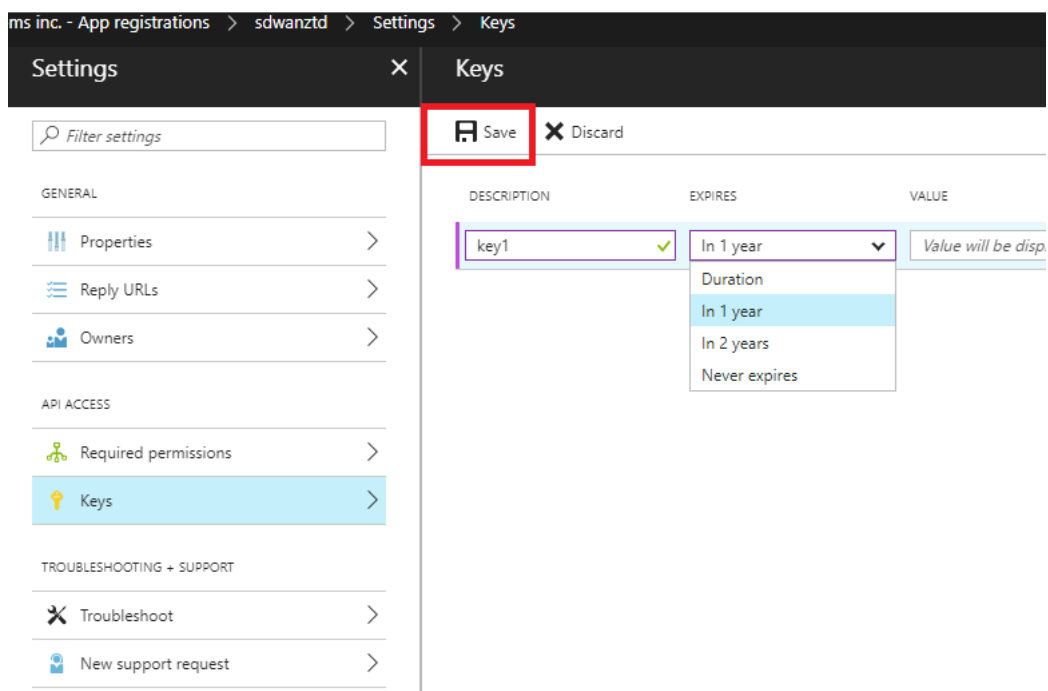
- f) Lors de l'ajout des autorisations requises, **sélectionnez une API**, puis mettez en surbrillance l'**API de gestion des services Windows Azure**.



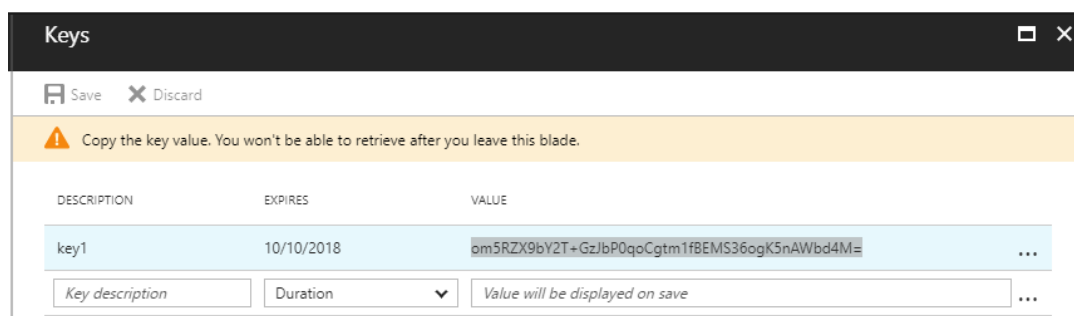
- g) Activez **les autorisations déléguées** pour provisionner les instances, puis cliquez sur **Sélectionner** et **Terminé**.



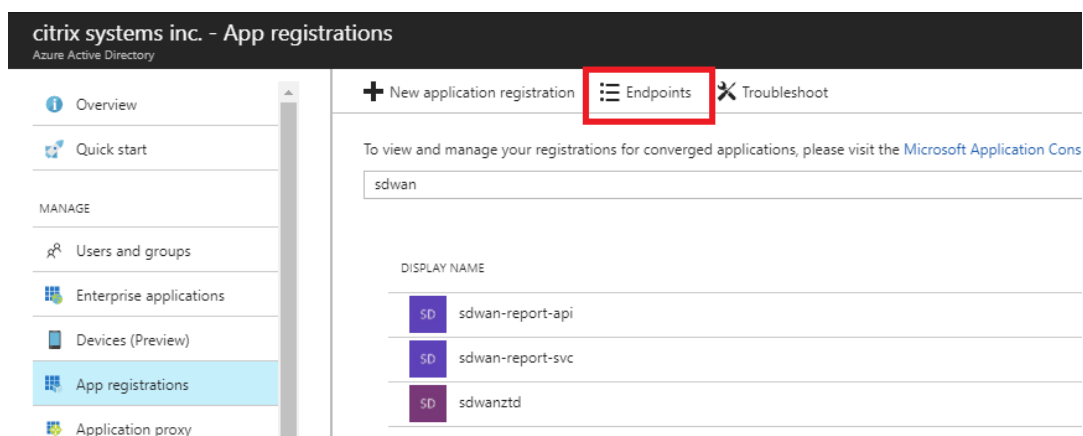
- h) Pour cette application enregistrée, sous Accès API, sélectionnez **Clés**, puis créez une **description de clé** secrète et la **durée** souhaitée pour que la clé soit valide. Ensuite, cliquez sur **Enregistrer** qui produira une **clé secrète** (la clé n'est requise que pour le processus de Provisioning, elle peut être supprimée une fois l'instance rendue disponible).



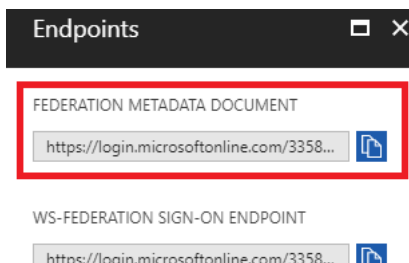
- i) Copiez et enregistrez la clé secrète (notez que vous ne pourrez pas la récupérer ultérieurement).



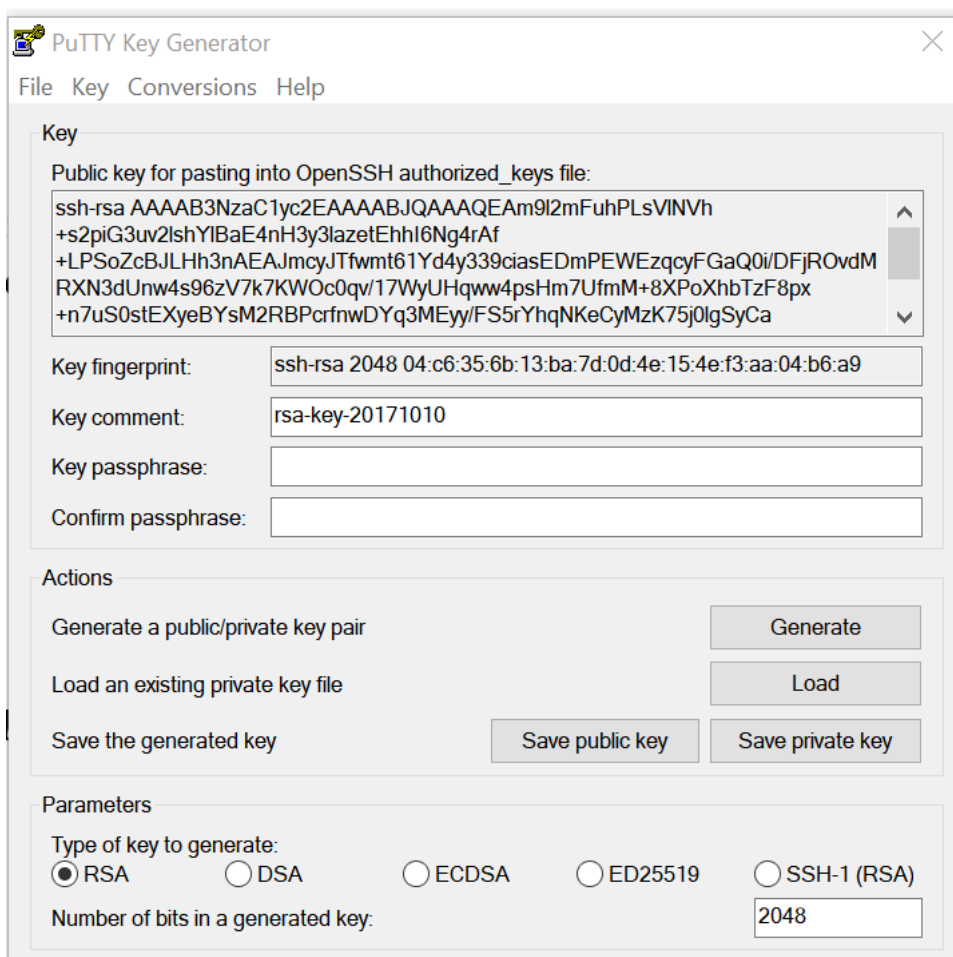
- j) Pour identifier l'**ID de locataire** requis, revenez au volet d'enregistrement de l'application, puis sélectionnez **Points de terminaison**.



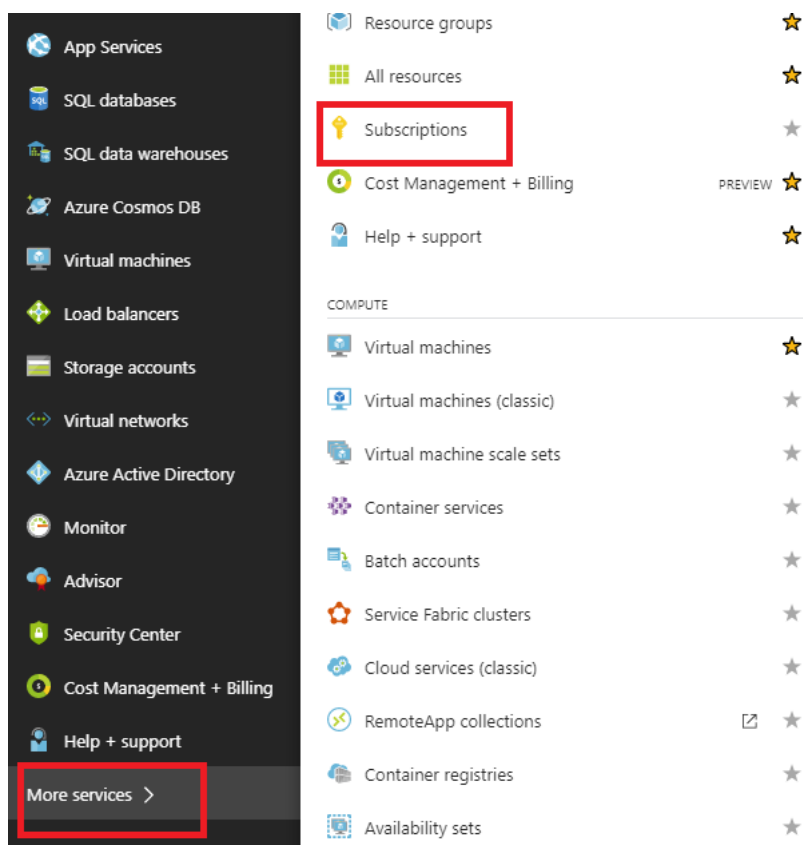
- k) Copiez le **document de métadonnées de fédération** pour identifier votre ID de locataire (notez que l'ID de locataire est une chaîne de 36 caractères située entre `leonline.com/` et le `/federation` dans l'URL).



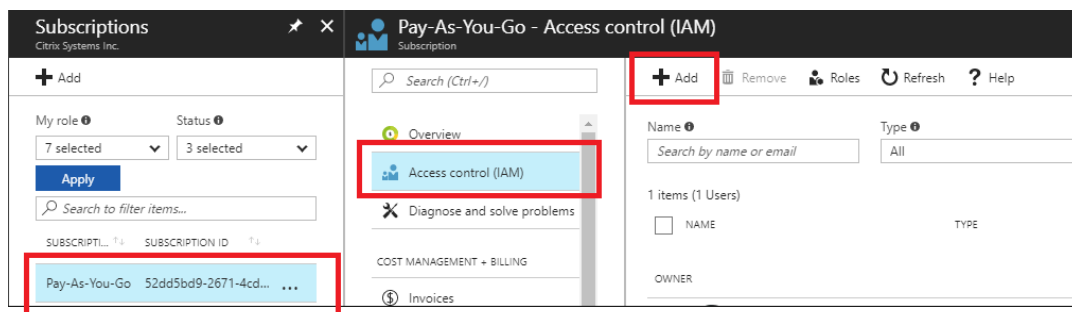
- l) Le dernier élément requis est la **clé publique SSH**. Cela peut être créé à l'aide de Putty Key Generator ou ssh-keygen et sera utilisé pour l'authentification, éliminant ainsi le besoin de mots de passe pour se connecter. La clé publique SSH peut être copiée (y compris le titre ssh-rsa et les chaînes rsa-key de fin). Cette clé publique sera partagée via l'entrée SD-WAN Center au service de déploiement Citrix Zero Touch.



- m) Des étapes supplémentaires sont nécessaires pour attribuer un rôle à l'application. Accédez à Plus de services, puis Abonnements.



n) Sélectionnez l'abonnement actif, puis **Contrôle d'accès (IAM)**, puis cliquez sur **Ajouter**.




o) Dans le volet Ajouter des autorisations, sélectionnez Rôle **Propriétaire**, attribuez l'accès à **l'utilisateur, au groupe ou à l'application Azure AD** et recherchez l'application enregistrée dans le **champ Sélectionner** pour autoriser le service de cloud de déploiement Zero Touch à créer et configurer l'instance sur Azure abonnement. Une fois l'application identifiée, sélectionnez-la et assurez-vous qu'elle est remplie en tant que membre Sélectionné avant de cliquer sur **Enregistrer**.

Add permissions ✕


Role ⓘ
Owner ▼

Assign access to ⓘ
Azure AD user, group, or application ▼

Select ⓘ
ztd ✓

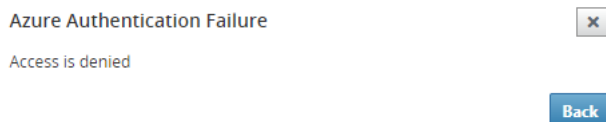
 **mbx_ztduser**
mbx_ztduser@citrite.net

Selected members:

 ztd [Remove](#)

[Save](#) [Discard](#)

- p) Après avoir collecté les entrées requises et les avoir entrées dans SD-WAN Center, cliquez sur **Suivant**. Si les entrées ne sont pas correctes, vous rencontrerez un échec d'authentification.



Mise en service et déploiement de SD-WAN Center Azure (Étape 2 sur 2)

1. Une fois l'authentification Azure réussie, remplissez les champs appropriés pour sélectionner la région Azure souhaitée et la taille d'instance appropriée, puis cliquez sur **Déployer**.

Provision and Deploy Azure (step 2 of 2)

Azure Region

West US

Azure Instance Size

Standard_D4_v2

WAN subnet address prefix:

10.9.4.0/24

LAN subnet address prefix:

10.9.3.0/24

Management subnet prefix:

10.9.0.0/24

Back

Deploy

2. La navigation vers l'onglet **Activation en attente** dans SD-WAN Center permet de suivre l'état actuel du déploiement.

Citrix SD-WAN Center

R9_3_1_35_624646

admin

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Network Discovery

Network Configuration

Zero Touch Deployment

Change Management

Appliance Settings

Configuration / Zero Touch Deployment / Pending Activation

Prepare New Site

Activation History

Pending Activation

Showing 1 - 1 of 1

Site Name	Serial No	Installer Email	Address	Status	Action
ztdazure	B0F20EC1-9DEE-4902-B072-D593536C6C02	ztdinstaller@outlook.com	AZURE - West US 2	Provisioning	

Delete

Modify

3. Un e-mail avec un code d'activation sera envoyé à l'adresse e-mail saisie à l'étape 1, obtenir l'e-mail et ouvrir l'**URL d'activation** pour déclencher le processus et vérifier l'état d'activation.

Focused

Other

Filter

NetScaler SD-WAN Team

NetScaler SD-WAN Cloud Service As

3:44 PM

NetScaler SD-WAN Appliance Activation Info...

NetScaler SD-WAN Cloud Service Activation Link @uswestazure

NT

NetScaler SD-WAN Team <sdwanservice@citrix.com>

Today, 3:44 PM

You

NetScaler SD-WAN Appliance Activation Information

To check the activation status, [click here](#)

(Or copy and paste this link into your Browser's address bar

https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate?activationcode=4f19b443-7e89-4b69-9872-0f7ebeeaa8ac2).

Site Name

uswestazure

Address

AZURE - West US

Additional Notes

The NetScaler SD-WAN Team

*** This is an automatically generated email, please do not reply ***

4. Un e-mail avec une URL d'activation sera remis à l'adresse e-mail saisie à l'étape 1. Obtenez l'e-mail et ouvrez l'**URL d'activation** pour déclencher le processus et vérifier l'état d'activation.



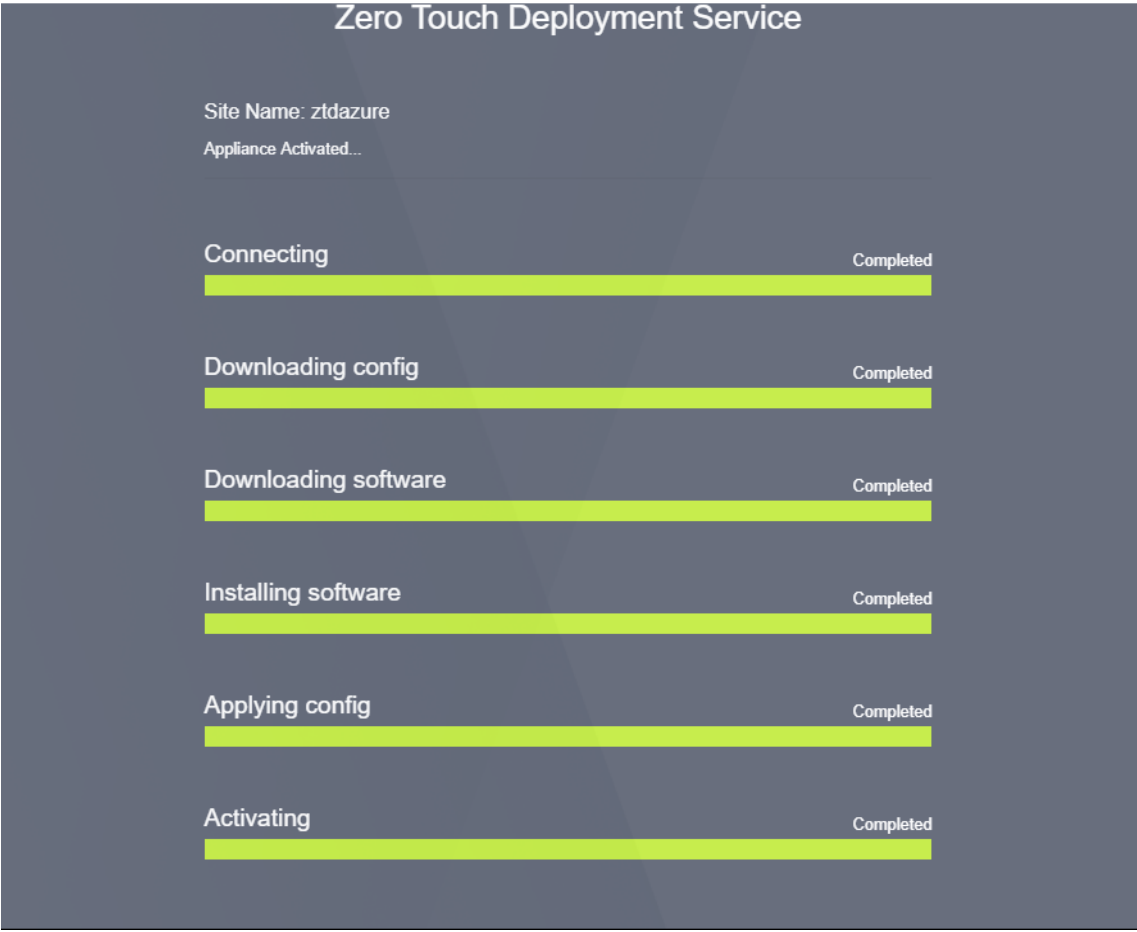
5. Il faudra quelques minutes pour que l'instance soit provisionnée par le SD-WAN Cloud Service. Vous pouvez surveiller l'activité sur le portail Azure, sous **Journal d'activité** pour le **groupe de ressources** créé automatiquement. Tous les problèmes ou erreurs liés au Provisioning seront renseignés ici, ainsi que répliqués vers SD-WAN Center dans l'état d'activation.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Purchase	Succeeded	Just now	Fri Oct 13 20...	Pay-As-You-Go	ztd
Write Deployments	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write NetworkSecurity	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write VirtualNetworks	Accepted	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write PublicIPaddress	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write NetworkInterface	Succeeded	4 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write StorageAccount	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write VirtualMachines	Succeeded	Just now	Fri Oct 13 20...	Pay-As-You-Go	
Validate	Started	6 min ago	Fri Oct 13 20...	Pay-As-You-Go	ztd
Update resource group	Started	6 min ago	Fri Oct 13 20...	Pay-As-You-Go	ztd

6. Dans le portail Azure, l'instance lancée avec succès sera disponible sous **Machines virtuelles**. Pour obtenir l'adresse IP publique attribuée, accédez à la vue d'ensemble de l'instance.

Public IP address: 32.247.213.21

7. Une fois que la machine virtuelle est en cours d'exécution, donnez-lui une minute avant que le service atteigne et commence le processus de téléchargement de la configuration, du logiciel et de la licence.



8. Une fois que chacune des étapes du service SD-WAN Cloud est automatiquement compliquée, connectez-vous à l'interface Web des instances SD-WAN à l'aide de l'adresse IP publique obtenue à partir du portail Azure.

DashboardMonitoringConfiguration

Warning: Grace license installed. Please obtain license from Citrix license portal and install it. Clear Warning

System Status

Name:ztdazure

Model:VPXL

Appliance Mode:Client

Serial Number:0000-0005-7786-4927-4958-4331-78

Management IP Address:10.9.0.106

Appliance Uptime:6 minutes, 52.3 seconds

Service Uptime:1 minutes, 58.0 seconds

Routing Domain Enabled:Default_RoutingDomain

Local Versions

Configuration Created On:Fri Oct 13 16:30:55 2017

Software Version:9.3.1.35.624646

Built On:Oct 2 2017 at 21:01:31

Hardware Version:VPXL

OS Partition Version:4.6

Virtual Path Service Status

Virtual Path DC-ztdazure Uptime: 1 minutes, 15.0 seconds.

9. La page Statistiques de surveillance Citrix SD-WAN identifie la connectivité réussie entre le MCN et l’instance SD-WAN dans Azure.

DashboardMonitoringConfiguration

Warning: Grace license installed. Please obtain license from Citrix license portal and install it. Clear Warning

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

Monitoring > Statistics

Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Refresh Show latest data.

Path Statistics Summary

Filter: in Any column Apply Show 100 entries

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	Azure-INET	DC-INET	GOOD	GOOD	Static	2	2	0.00	10.83	NO
2	DC-INET	Azure-INET	GOOD	GOOD	Static	2	2	0.00	17.60	NO

Showing 1 to 2 of 2 entries

Bandwidth calculated over the last 0.851 seconds

First Previous 1 Next Last

10. En outre, la tentative de provisionnement réussie (ou infructueuse) sera consignée dans la page Historique d’activation du SD-WAN Center.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

418

The screenshot shows the Citrix SD-WAN Center interface. The top navigation bar includes 'Dashboard', 'Fault', 'Monitoring', 'Configuration', 'Reporting', and 'Administration'. The 'Configuration' tab is active, and the sub-menu 'Zero Touch Deployment / Activation History' is selected. The left sidebar lists various configuration options. The main content area shows the 'Activation History' tab with a table of activation records.

Site Name	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
ztdazure	C736A440-0A37-4676-AF5D-CCD874220783	ztdinstaller@outlook.com	AZURE - West US	Appliance Activated	Oct 14 15:10:13 2017 UTC	Activated	

Déploiement d'une région

May 6, 2021

Les régions vous permettent de définir une hiérarchie de réseau avec gestion distribuée. Une région doit définir un nœud de contrôle régional (RCN) qui prendra en charge les fonctions exécutées par le nœud de contrôle réseau (MCN) pour sa région. Le MCN est le Controller de la région par défaut.

Les chemins virtuels statiques et dynamiques ne sont pas autorisés entre les régions. Les RCN gèrent le trafic entre les régions.

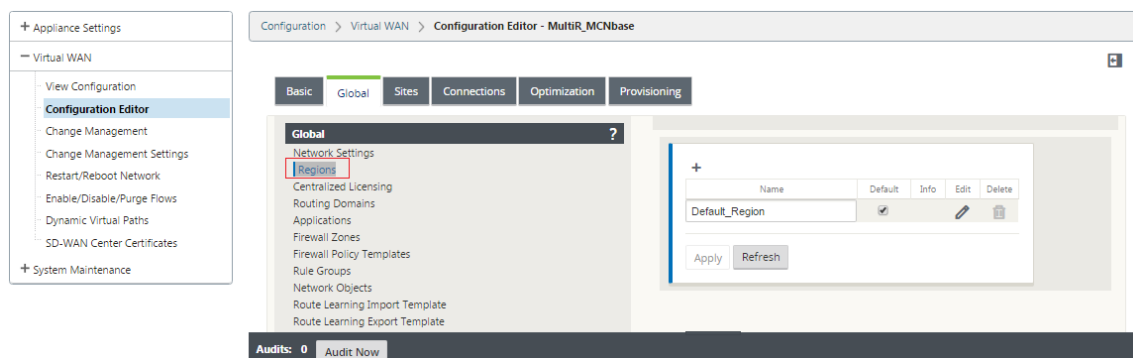
Un déploiement à une seule région dans un réseau SD-WAN peut prendre en charge des sites réseau inférieurs à 550.

Vous pouvez configurer une région par défaut dans l'éditeur de configuration de l'interface graphique de l'appliance SD-WAN. L'éditeur Basic est utile pour créer uniquement un petit réseau avec des nœuds MCN et Client SD-WAN. Pour configurer un réseau multi-régions avec MCN, RCN, Clients ou fonctionnalités avancées, utilisez d'autres options de configuration dans l'éditeur de configuration.

Pour configurer le déploiement d'une région unique :

1. Accédez à l'onglet **Global** dans l'Éditeur de configuration. Sélectionnez **Régions**. Les options de configuration de région par défaut s'affichent.

Vous pouvez modifier le nom et la description de la région par défaut en le modifiant.



2. Modifiez **Default_Region** pour modifier le nom et configurer les sous-réseaux.
3. Activez la correspondance VIP d'intervalle selon que vous souhaitez que la **correspondance VIP interne forcée** ou **Autoriser la correspondance VIP externe** .
 - VIP interne forcé : Lorsque cette option est activée, toutes les adresses IP virtuelles non privées de la région sont forcées de correspondre aux sous-réseaux configurés.
 - VIP externe autorisé - Lorsque cette option est activée, les adresses IP virtuelles non privées provenant d'autres régions sont autorisées à correspondre aux sous-réseaux configurés.
4. Cliquez sur + pour ajouter des sous-réseaux.

Edit

Name:

Default_Region

Description:

☐ Force Internal VIP Matching

☐ Allow External VIP Matching

Subnets +

Routing Domain	Network	Delete
Default_RoutingDomain ▼		

Apply

Cancel

5. Sélectionnez un **domaine de routage**, entrez l'adresse **réseau**. Cliquez sur **Apply**. L'adresse réseau est l'adresse IP et le masque du sous-réseau.

Déploiement multi-régions

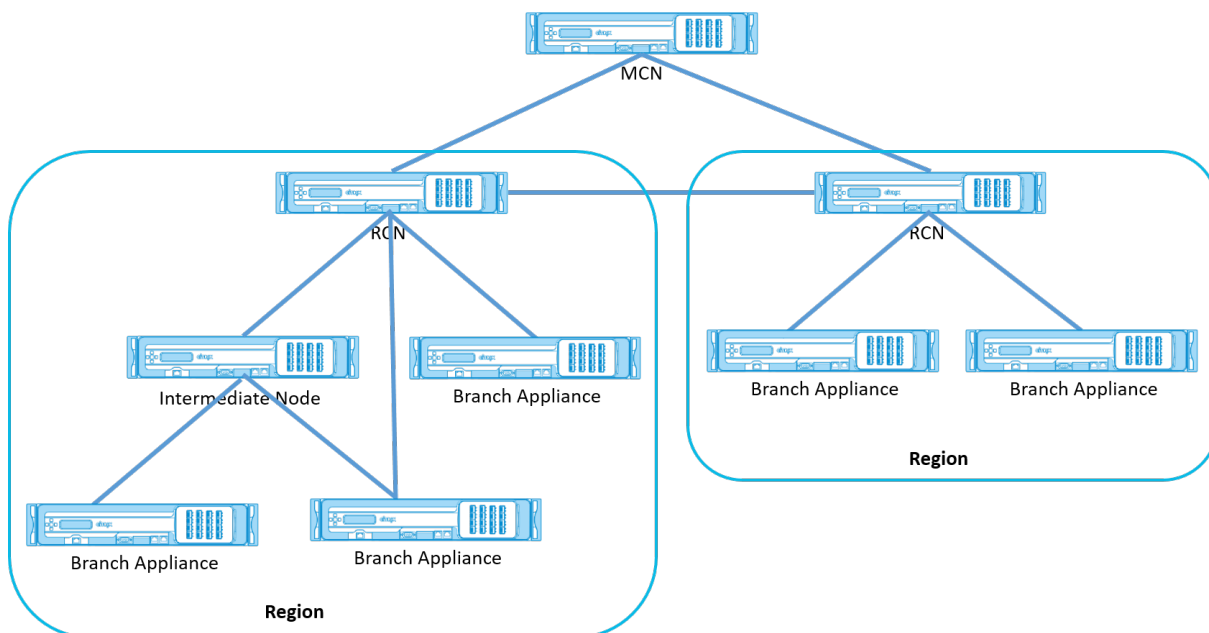
November 1, 2021

Une appliance SD-WAN configurée en tant que nœud de contrôle principal (MCN) prend en charge le déploiement multi-régions. Le MCN gère plusieurs nœuds de contrôle régionaux (RCN). Chaque RCN, à son tour, gère plusieurs sites clients. Le MCN peut également être utilisé pour gérer directement certains sites clients.

Avec MCN comme nœud de contrôle du réseau et RCN comme nœuds de contrôle des régions, SD-WAN peut gérer jusqu'à 6000 sites.

Le déploiement multi-régions vous permet de fragmenter un réseau en régions et de configurer un réseau hiérarchisé, tel que la branche (client) > RCN > MCN.

Un MCN avec une seule région peut être configuré avec un maximum de 1000 sites. Vous pouvez conserver les sites existants dans la région par défaut et ajouter de nouvelles régions avec des RCN et leurs sites pour un déploiement multi-régions.



Le tableau suivant fournit la liste des plates-formes prises en charge pour la configuration MCN/RCN principale et secondaire.

REMARQUE

- L'appliance Premium Edition (PE) est anciennement appelée Enterprise Edition (EE).
- Utilisez l'appliance Citrix SD-WAN 210 SE en tant que MCN uniquement dans les réseaux gérés par SD-WAN Orchestrator.

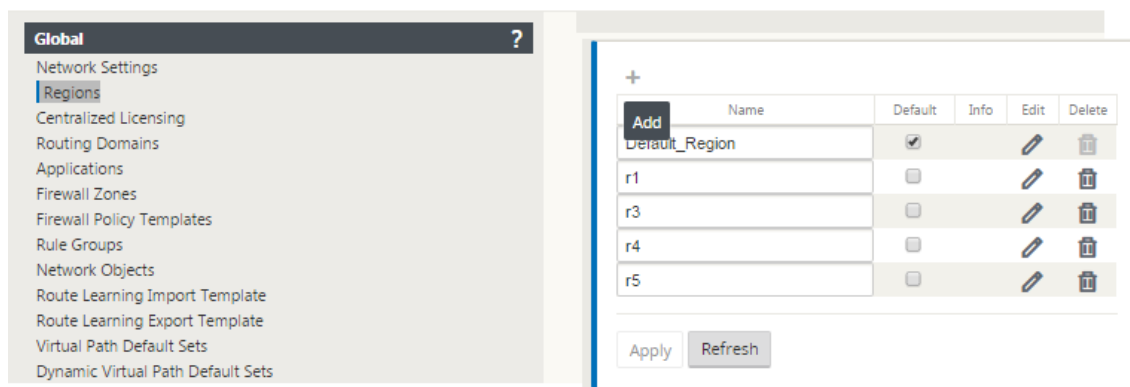
Édition Plateforme	MCN primaire/secondaire	RCN primaire/secondaire
110-SE	Non	Non
210-SE	Oui	Oui
400-SE	Oui	Non
410-SE	Oui	Non
1000-SE, 1000-PE	Oui	Non
1100-SE, 1100-PE	Oui	Oui
VPX-SE, VPXL-SE	Oui	Oui
2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE	Oui	Oui

Pour configurer un déploiement multi-régions pour un réseau SD-WAN :

1. Accédez à l'onglet **Global** dans l'Éditeur de configuration. Sélectionnez **Régions**. Les options de configuration de région par défaut s'affichent.

Vous pouvez modifier le nom et la description de la région par défaut en le modifiant.

2. Cliquez sur **+ Ajouter** pour ajouter une nouvelle région.



? x

Add

Name:

Description:

☐ Force Internal VIP Matching

☐ Allow External VIP Matching

Subnets **+**

Network	Delete

Add Cancel

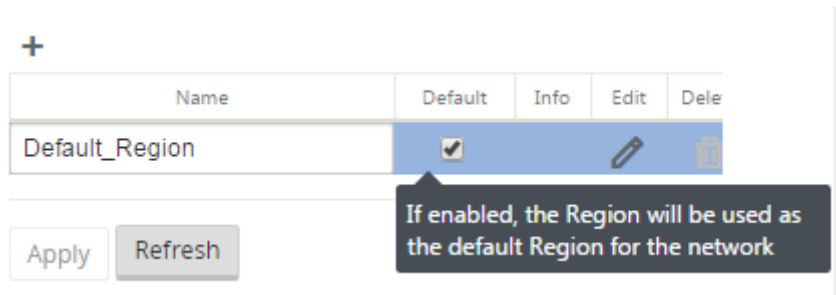
- Entrez un nom et une description pour la région.
- Activez la correspondance VIP interne selon que vous souhaitez effectuer une **correspondance VIP interne forcée** ou **autoriser une correspondance VIP externe** .
 - VIP interne forcé : Lorsque cette option est activée, toutes les adresses IP virtuelles non privées de la région sont forcées de correspondre aux sous-réseaux configurés.
 - Autorisé VIP externe - Lorsque cette option est activée, les adresses IP virtuelles non privées provenant d'autres régions sont autorisées à correspondre aux sous-réseaux configurés.
- Cliquez sur + pour ajouter des sous-réseaux. Choisissez un domaine de routage.

Subnets **+**

Routing Domain	Network	Delete
<Default>		
<Default>		
Default_RoutingDomain		
WCCP_RoutingDomain		

Add Cancel

- Entrez une adresse **réseau** . Cliquez sur **Ajouter**. L'adresse réseau est l'adresse IP et le masque du sous-réseau. La région nouvellement créée est ajoutée à la liste existante des régions.
 Vous pouvez cocher la case **par défaut** pour utiliser la région souhaitée comme valeur par défaut.



Remarque

Vous pouvez cloner MCN vers un site GEO ou client.

SD-WAN Center prend en charge le déploiement multi-régions. Pour plus d’informations, consultez la section [Déploiement et création de rapports multi-régions SD-WAN Center](#).

Vue récapitulative de gestion des modifications

Lorsque vous exécutez le processus de gestion des modifications pour les appliances configurées dans un déploiement multi-régions, le tableau récapitulatif de la gestion des modifications s’affiche dans l’interface graphique de l’appliance SD-WAN.

La colonne **Région** affiche la liste des régions actuellement configurées dans le réseau. Vous pouvez afficher le résumé de la gestion des modifications d’une région spécifique en le sélectionnant dans le tableau récapitulatif.

Récapitulatif de la région par défaut :

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - Default_Region Details

Show 25 entries

Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 min		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
BR1-BR1-CBVPXL	CBVPXL	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
AMER-1RCN-5100-AMER-1RCN-5100	CB5100	Not Needed	Not Connected				Loc Chg Mgt		none / staged

Previous 1 Next

Résumé de la région :

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - AMEA_r1 Details

Show25entries

Search

CustomizeRefresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
AMEA_r1_vpx01-AMEA_r1_vpx01	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx02-AMEA_r1_vpx02	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx03-AMEA_r1_vpx03	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx04-AMEA_r1_vpx04	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx05-AMEA_r1_vpx05	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx06-AMEA_r1_vpx06	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx07-AMEA_r1_vpx07	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx08-AMEA_r1_vpx08	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx13-AMEA_r1_vpx13	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx14-AMEA_r1_vpx14	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx15-AMEA_r1_vpx15	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx16-AMEA_r1_vpx16	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx17-AMEA_r1_vpx17	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx18-AMEA_r1_vpx18	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx19-AMEA_r1_vpx19	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx20-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx33-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx34-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx35-vpx35	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx36-vpx36	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx37-vpx37	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx38-vpx38	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx39-vpx39	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx40-vpx40	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx49-vpx49	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged

Previous12Next

Remarque

Dans certains cas, la valeur **Total Sites** affichée dans le tableau **Global Multi-Region Summary** est inférieure à la somme des colonnes restantes.

Par exemple, lorsqu'un nœud de branche n'est pas connecté, il est possible que la branche soit comptée deux fois ; une fois comme « Non connecté » et une fois comme « Préparation/Mise en scène ».

Guide de configuration des charges de travail Citrix Virtual Apps and Desktops

August 31, 2022

Citrix SD-WAN est une solution WAN Edge de nouvelle génération qui accélère la transformation numérique grâce à une connectivité et des performances flexibles, automatisées et sécurisées pour les applications SaaS, cloud et virtuelles, afin de garantir une expérience d'Workspace toujours active.

Citrix SD-WAN est le moyen recommandé et le meilleur moyen pour les organisations utilisant Citrix Virtual Apps and Desktops Service de se connecter aux charges de travail Citrix Virtual Apps and Desktops dans le Cloud. Pour plus d'informations, reportez-vous à la section [blog Citrix](#).

Ce document se concentre sur la configuration de Citrix SD-WAN pour la connectivité vers/depuis les charges de travail Citrix Virtual Apps and Desktops sur Azure.

Avantages

- Facile à configurer SD-WAN dans Citrix Virtual Apps and Desktops via un flux de travail guidé
- Connectivité toujours active et haute performance grâce à des technologies SD-WAN avancées
- Avantages pour toutes les connexions (VDA-DC, User-to-VDA, VDA-Cloud, User-to-Cloud)
- Réduit la latence par rapport au trafic de rétroacheminement vers le centre de données
- Gestion du trafic pour garantir la qualité de service (QoS)
 - QoS sur les flux de trafic HDX/ICA (AutoQoS HDX mult flux monoport)
 - QoS entre HDX et d'autres trafics
 - HDX QoS Équité entre les utilisateurs
 - QoS de bout en bout
- Le collage de liaison offre plus de bande passante pour des performances plus rapides
- Haute disponibilité avec basculement de lien transparent et redondance SD-WAN sur Azure
- Expérience VoIP optimisée (course de paquets pour une gigue réduite et une perte minimale de paquets, QoS, break-out local pour une latence réduite)
- Économies importantes et déploiement doit être plus rapide et plus facile par rapport à Azure ExpressRoute

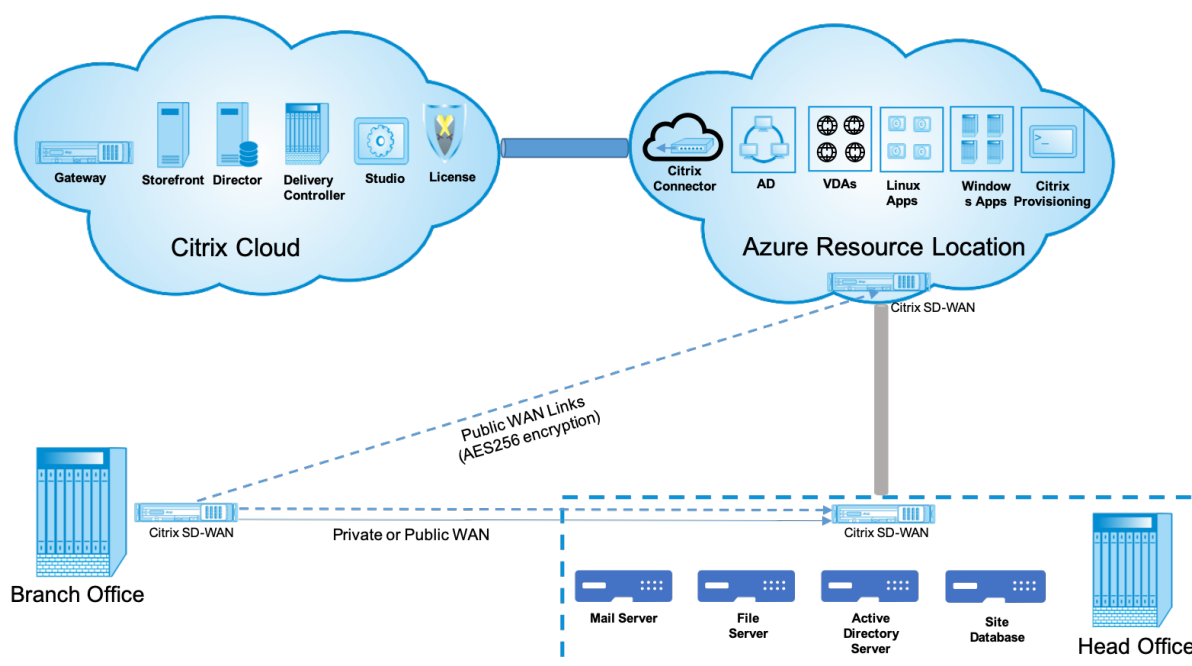
Conditions préalables

Adhérez aux conditions préalables suivantes pour évaluer et déployer les fonctionnalités des charges de travail Citrix Virtual Apps and Desktops :

- Vous devez disposer d'un réseau SD-WAN existant ou en créer un nouveau.
- Vous devez disposer d'un abonnement au service Citrix Virtual Apps and Desktops.
- Pour utiliser les fonctionnalités SD-WAN telles que l'AutoQoS HDX mult flux et la visibilité profonde, le service de localisation réseau (NLS) doit être configuré pour tous les sites SD-WAN de votre réseau.

- Vous devez disposer d'un serveur DNS et d'AD déployés là où les points de terminaison client sont présents (souvent co-situés dans votre environnement de datacenter) ou vous pouvez utiliser Azure Active Directory (AAD).
- Le serveur DNS doit être capable de résoudre les adresses IP internes (privées) et externes (publiques).
- Assurez-vous que le nom de domaine complet (sdwan-location.citrixnetworkapi.net) est ajouté à la liste autorisée dans le pare-feu. Il s'agit du nom de domaine complet pour le service de localisation réseau qui est essentiel pour l'envoi du trafic via le chemin virtuel SD-WAN. De plus, si vous êtes à l'aise avec la liste blanche des noms de domaine complet, il serait préférable d'ajouter *.citrixnetworkapi.net à la liste autorisée, car il s'agit du sous-domaine pour les autres services Citrix Cloud tels que le provisioning zéro touche.
- Inscrivez-vous sur sdwan.cloud.com pour utiliser l'orchestrateur SD-WAN pour gérer votre réseau SD-WAN. SD-WAN Orchestrator est une plate-forme de gestion multi-locataires basée sur Citrix Cloud pour Citrix SD-WAN.

Architecture de déploiement



Les entités suivantes sont requises pour le déploiement :

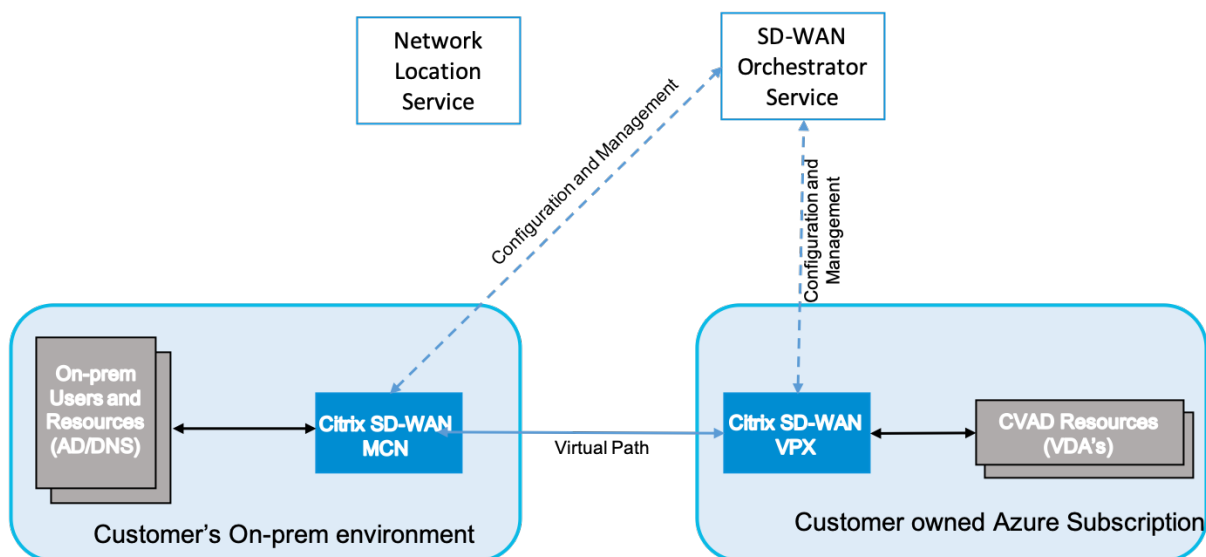
- Emplacement local hébergeant l'appliance SD-WAN qui peut être déployé en mode branche ou sous la forme d'un MCN (nœud de contrôle maître). Le mode branche ou MCN contient les machines clientes, Active Directory et DNS. Toutefois, vous pouvez également choisir d'utiliser le DNS et AD d'Azure. Dans la plupart des scénarios, l'emplacement local sert de centre de données et héberge le MCN.

- **Service cloud Citrix Virtual Apps and Desktops** —Citrix Virtual Apps and Desktops fournit des solutions de virtualisation qui permettent aux services informatiques de contrôler les machines virtuelles, les applications et la sécurité tout en fournissant un accès où que vous soyez pour n'importe quel appareil. Les utilisateurs peuvent utiliser des applications et des bureaux indépendamment du système d'exploitation et de l'interface de l'appareil.

À l'aide du service Citrix Virtual Apps and Desktops, vous pouvez fournir des applications et des bureaux virtuels sécurisés sur n'importe quel périphérique et laisser la plupart de l'installation, de la configuration, des mises à niveau et de la surveillance du produit à Citrix. Vous conservez un contrôle total sur les applications, les stratégies et les utilisateurs tout en offrant la meilleure expérience possible sur n'importe quel appareil.

- **Connecteur Citrix connector/cloud** - Vous connectez vos ressources au service via Citrix Cloud Connector, qui sert de canal de communication entre Citrix Cloud et vos emplacements de ressources. Cloud Connector permet d'administrer le cloud sans nécessiter de configuration de réseau ou d'infrastructure complexe telle que des VPN ou des tunnels IPsec. Les emplacements de ressources contiennent les machines et autres ressources qui mettent à disposition des applications et des postes de travail à vos abonnés.
- **SD-WAN Orchestrator** —Citrix SD-WAN Orchestrator est un service de gestion multi-locataire hébergé dans le cloud disponible pour les entreprises **Do It Yourself** et les partenaires Citrix. Les partenaires Citrix peuvent utiliser SD-WAN Orchestrator pour gérer plusieurs clients avec un seul panneau de verre et des contrôles d'accès basés sur les rôles appropriés.
- **Appliances SD-WAN virtuelles et physiques** : il s'exécute sous la forme de plusieurs instances dans le cloud (VM) et sur site dans le centre de données et dans les branches (appliances physiques ou machines virtuelles) pour fournir une connectivité entre ces emplacements et vers/depuis l'Internet public. L'instance SD-WAN dans Citrix Virtual Apps and Desktops est créée sous la forme d'un seul ou d'un ensemble d'appliances virtuelles (dans le cas d'un déploiement HA) en provisionnant ces instances via Azure Marketplace. Les appliances SD-WAN situées dans d'autres emplacements (DC et succursales) sont créées par le client. Toutes ces appliances SD-WAN sont gérées (en termes de configuration et de mise à niveau logicielle) par les administrateurs SD-WAN via SD-WAN Orchestrator.

Déploiement et configuration



Dans un déploiement commun, l'apppliance Citrix SD-WAN (H/W ou VPX) est déployée en tant que MCN dans son bureau DC/Large. Le contrôleur de domaine client héberge généralement des utilisateurs et des ressources sur site tels que les serveurs AD et DNS. Dans certains scénarios, le client peut utiliser les services Azure Active Directory (AADS) et DNS, qui sont tous deux pris en charge par l'intégration Citrix SD-WAN et CMD.

Dans l'abonnement Azure géré par le client, le client doit déployer l'apppliance virtuelle Citrix SD-WAN et les VDA. Les appliances SD-WAN sont gérées via SD-WAN Orchestrator. Une fois que l'apppliance SD-WAN est configurée, elle se connecte au réseau Citrix SD-WAN existant et d'autres tâches telles que la configuration, la visibilité et la gestion sont gérées via SD-WAN Orchestrator.

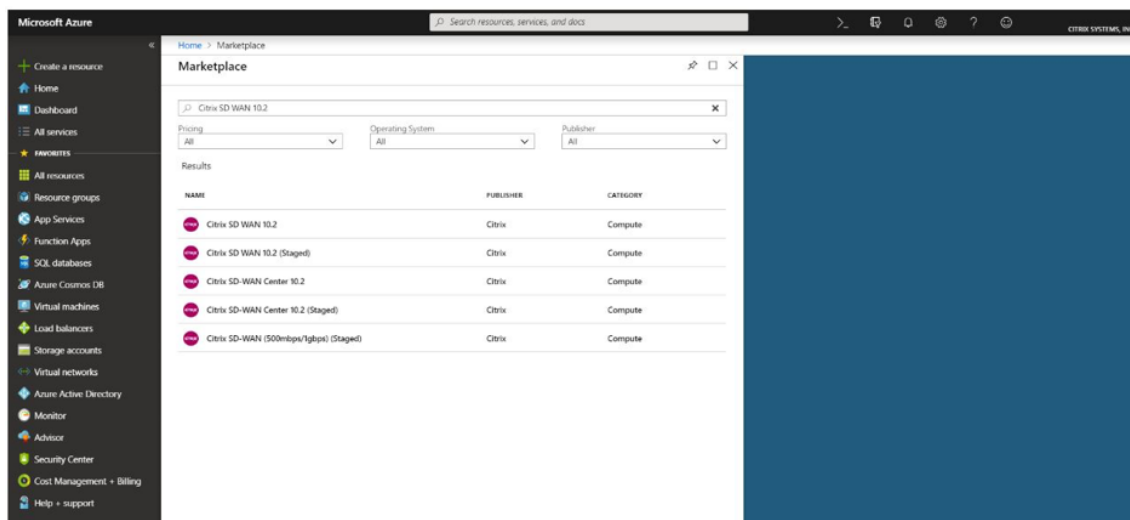
Le troisième composant de cette intégration est le **service de localisation réseau (NLS)** qui permet aux utilisateurs internes de contourner la passerelle et de se connecter directement aux VDA, réduisant ainsi la latence du trafic réseau interne. Vous pouvez configurer NLS manuellement ou via Citrix SD-WAN Orchestrator. Pour plus d'informations, reportez-vous à la section [NLS](#).

Configuration

La machine virtuelle Citrix SD-WAN est déployée dans une région spécifiée (selon les besoins du client) et peut être connectée à plusieurs succursales via MPLS, Internet ou 4G/LTE. Dans une infrastructure de réseau virtuel (VNET), la machine virtuelle SD-WAN Standard Edition (SE) est déployée en mode Gateway. Le VNET a des routes vers la Gateway Azure. L'instance SD-WAN a une route vers la Gateway Azure pour la connectivité Internet. Cette route doit être créée manuellement.

1. Depuis un navigateur Web, accédez à [portail Azure](#). Connectez-vous à un compte Microsoft Azure et recherchez Citrix SD-WAN Standard Edition.

2. Dans les résultats de recherche, choisissez la solution Citrix SD-WAN Standard Edition. Cliquez sur **Créer** après avoir passé en revue la description et vous assurer que la solution choisie est correcte.

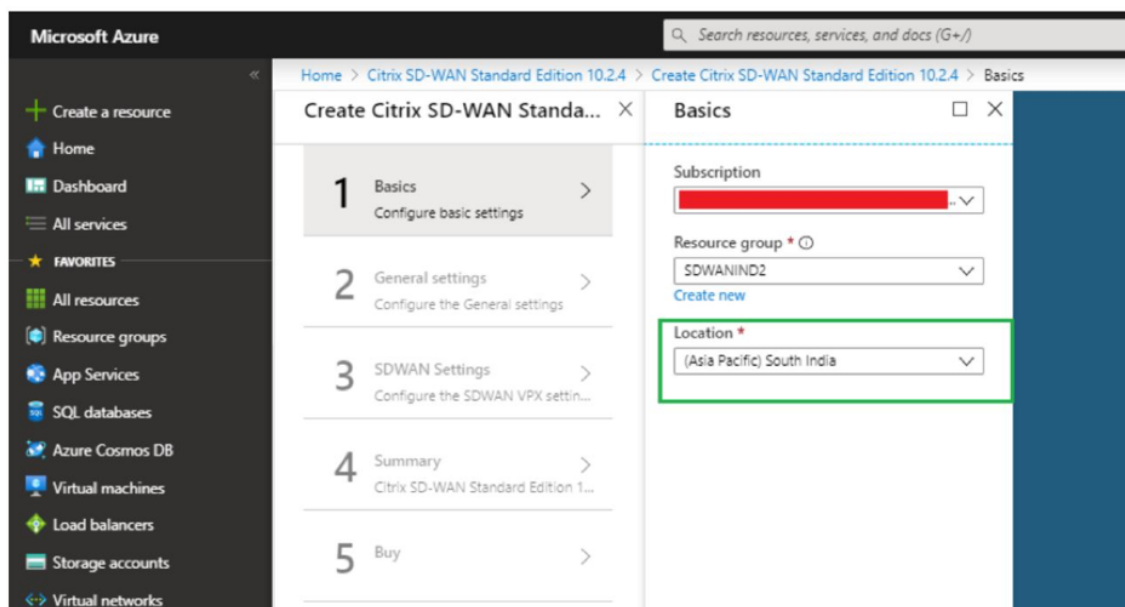


En cliquant sur **Créer**, un assistant vous invite avec les détails nécessaires pour créer la machine virtuelle.

3. Dans la page **Paramètres de base**, choisissez le groupe de ressources dans lequel vous souhaitez déployer la solution SD-WAN SE.

Un groupe de ressources est un conteneur qui contient des ressources associées pour une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous souhaitez gérer en tant que groupe. Vous pouvez décider de la façon dont vous souhaitez allouer des ressources aux groupes de ressources en fonction de votre déploiement.

Pour Citrix SD-WAN, il est recommandé que le groupe de ressources que vous choisissez soit vide. De même, sélectionnez la région Azure dans laquelle vous souhaitez déployer l'instance SD-WAN. La région doit être identique à la région dans laquelle vos ressources Citrix Virtual Apps and Desktops sont déployées.



4. Sous la page **Paramètres de l'administrateur**, indiquez un nom pour la machine virtuelle. Choisissez un nom d'utilisateur et un mot de passe fort. Le mot de passe doit être composé d'une lettre majuscule, d'un caractère spécial et doit comporter plus de neuf caractères. Cliquez sur **OK**.

Ce mot de passe est nécessaire pour vous connecter à l'interface de gestion de l'instance en tant qu'utilisateur invité. Pour obtenir l'accès administrateur à l'instance, utilisez admin comme nom d'utilisateur et le mot de passe créé lors du Provisioning de l'instance. Si vous utilisez le nom d'utilisateur créé lors du Provisioning de l'instance, vous obtenez un accès en lecture seule. Choisissez également le type de déploiement ici.

Si vous souhaitez déployer une seule instance, assurez-vous que vous choisissez désactivé dans l'option Mode Déploiement HA, sinon choisissez activé. Pour les réseaux de production, Citrix recommande toujours de déployer des instances en mode haute disponibilité car il protège votre réseau contre les défaillances de l'instance.

Create Citrix SD-WAN Standa... X

Administrator settings □ X

1 Basics Done ✓

2 Administrator settings > Configure deployment settings

3 SDWAN settings > Configure Netscaler SD-WAN a...

4 SDWAN Route settings > Configure the route settings

* Virtual Machine name ⓘ SDWSEA ✓

HA Deployment Mode ⓘ Enabled Disabled

* Username ⓘ ctsdwadmin ✓

* Password ⓘ ✓

* Confirm password ✓

5. Sous la page **Paramètres du SD-WAN**, choisissez l'instance dans laquelle vous souhaitez exécuter l'image. Choisissez le type d'instance suivant selon vos besoins :

- Type d'instance D3_V2 pour un débit unidirectionnel maximal de 200 Mbps avec connectivité directe à un maximum de 16 branches.
- Type d'instance D4_V2 pour un débit unidirectionnel maximal de 500 Mbps avec connectivité directe à un maximum de 16 branches.
- Type d'instance F8 standard pour un débit unidirectionnel maximal de 1 Gbit/s avec connectivité directe à un maximum de 64 branches.
- Type d'instance F16 standard pour un débit unidirectionnel maximal de 1 Gbit/s avec connectivité directe à un maximum de 128 branches.

Home > Marketplace > Citrix SD-WAN 10.2 > Create Citrix SD-WAN 10.2 > SDWAN Settings > Choose a size

SDWAN Settings

Virtual machine size ⓘ 1x Standard D3 v2

Virtual network ⓘ (new) vnet

Subnets ⓘ Configure subnets ⓘ

Choose a size

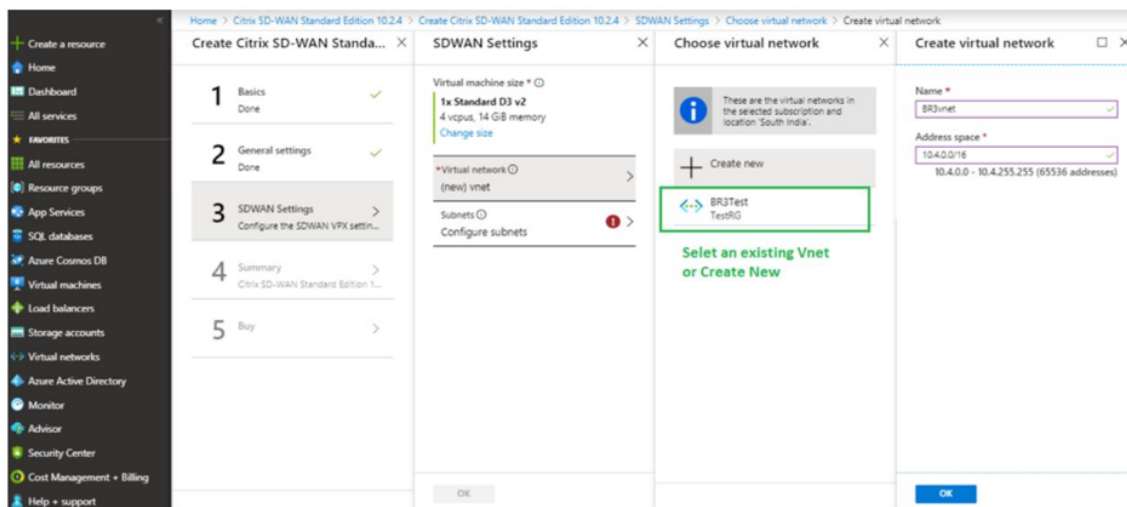
Search: [] Compute type: Current generation Disk type: All disk types vCPUs: 1 128

RECOMMENDED	SKU	TYPE	COMPUTE	vCPUS	GB RAM	DATA DISKS	MAX IOPS	LOCAL SSD	PREMIUM	ADDITIONAL	USD/MON
★	D3_V2	Standard	General purpose	4	14	16	16x500	200 GB	No		\$209.06
★	D4_V2	Standard	General purpose	8	28	32	32x500	400 GB	No		\$418.13
★	F8	Standard	Compute optim	8	16	32	32x500	128 GB	No		\$282.72
	F16	Standard	Compute optim	16	32	64	64x500	256 GB	No		\$565.44

Prices presented are estimates in your local currency that include Azure infrastructure applicable software costs, as well as any discounts for the subscription and location. Final charges will appear in your local currency in cost analysis and billing views. If you purchased Azure services through a reseller, contact your reseller for full pricing details. Recommended sizes are determined by the publisher of the selected image based on hardware and software requirements.

6. Créez un nouveau réseau virtuel (VNet) ou utilisez un réseau virtuel existant. Il s'agit de l'étape

la plus critique pour le déploiement, car cette étape choisit les sous-réseaux à affecter aux interfaces de la machine virtuelle SD-WAN VPX.



Le sous-réseau auxiliaire n'est nécessaire que lorsque vous déployez les instances en mode HA. Assurez-vous que l'instance SD-WAN est déployée sur le même réseau virtuel que vos ressources Citrix Virtual Apps and Desktops et qu'elle se trouve sur le même sous-réseau que l'interface LAN de l'appliance VPX SD-WAN.

SDWAN Settings

Virtual machine size * ⓘ
1x Standard D3 v2
4 vcpus, 14 GiB memory
[Change size](#)

*Virtual network ⓘ
(new) BR3vnet

Subnets ⓘ
Configure subnets ⓘ

OK

Subnets

Manangement subnet name *
snet-mgmt ✓

Manangement subnet address prefix *
10.4.0.0/24 ✓

LAN subnet name *
snet-lan ✓

LAN subnet address prefix *
10.4.1.0/24 ✓

WAN subnet name *
snet-wan ✓

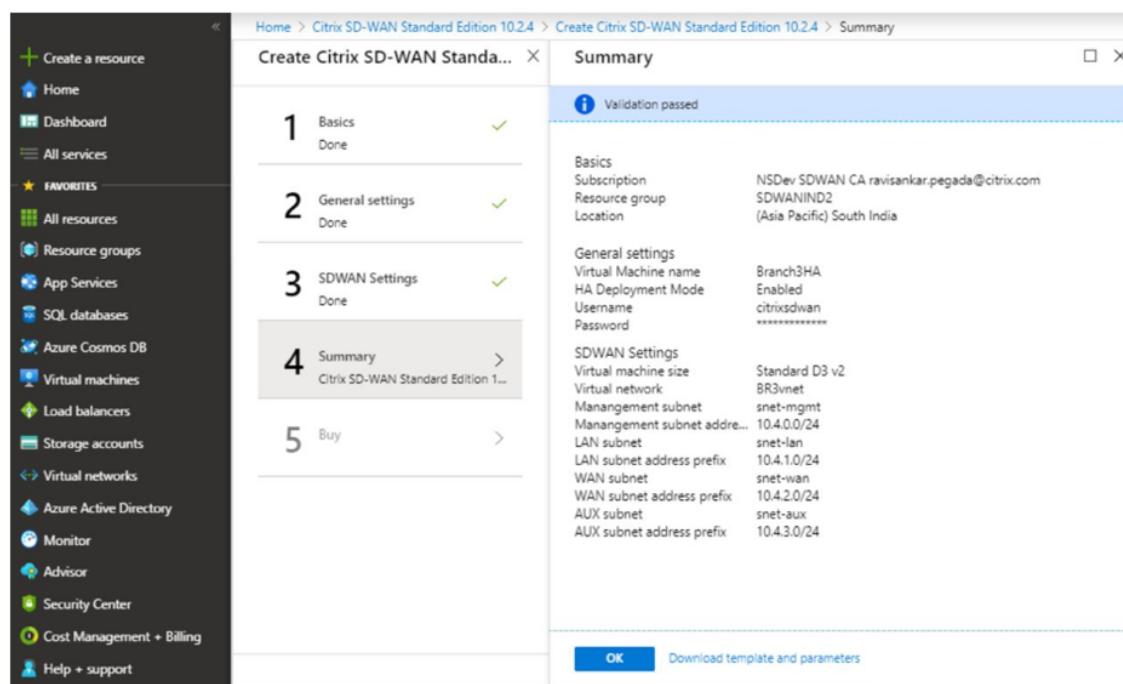
WAN subnet address prefix *
10.4.2.0/24 ✓

AUX subnet name *
snet-aux ✓

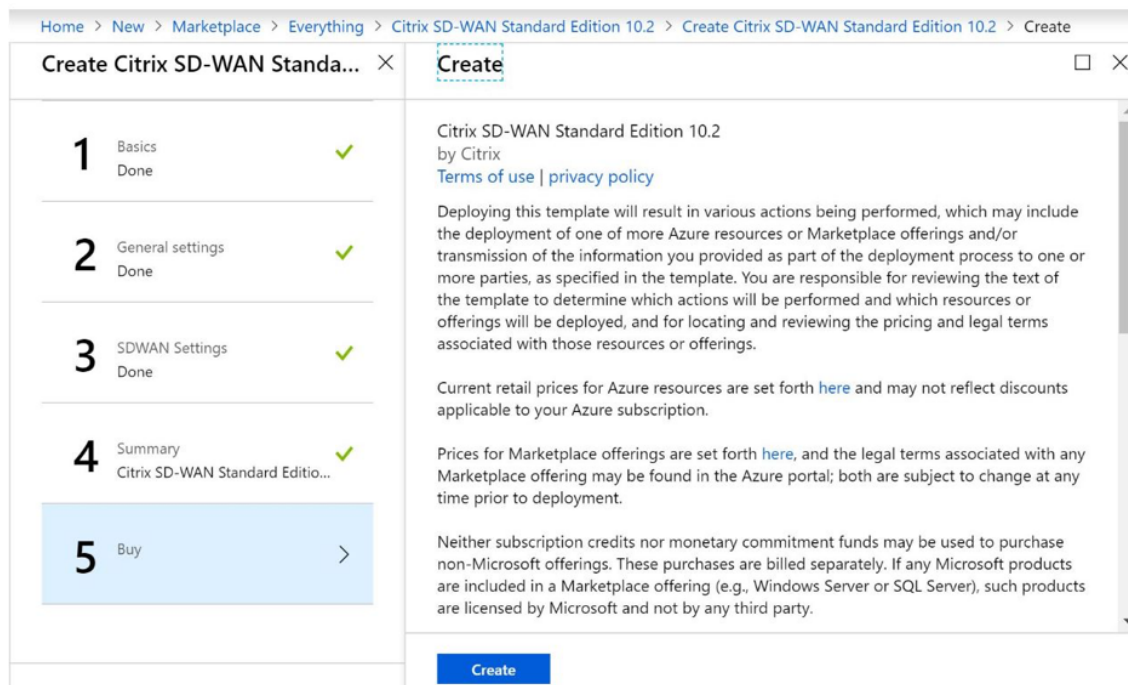
AUX subnet address prefix *
10.4.3.0/24 ✓

OK

7. Vérifiez la configuration dans la page **Résumé** et cliquez sur **OK**.



8. Sur la page **Acheter**, cliquez sur **Créer** pour démarrer le processus de provisioning pour les instances. Le provisionnement de l'instance peut prendre environ 10 minutes. Vous recevez une notification dans le portail de gestion Azure suggérant le succès ou l'échec de la création d'instance.



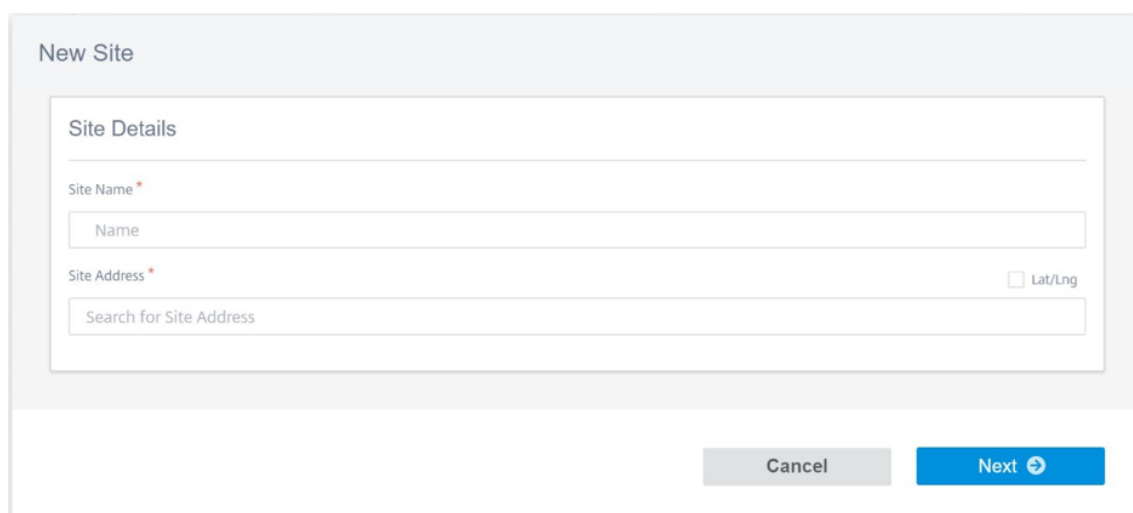
Une fois l'instance créée avec succès, récupère l'adresse IP publique attribuée à l'interface de gestion de l'instance SD-WAN. Elle se trouve dans la section Mise en réseau du groupe de

ressources dans lequel l'instance a été provisionnée. Une fois récupéré, vous pouvez l'utiliser pour vous connecter à l'instance.

Remarque

Pour l'accès administrateur, le nom d'utilisateur est **admin** et le mot de passe est celui que vous avez défini lors de la création de l'instance.

9. Une fois le site configuré, connectez-vous au SD-WAN Orchestrator pour le configurer. Comme mentionné dans les pré-requis, vous devez avoir le droit de SD-WAN Orchestrator pour configurer le site. Si vous ne l'avez pas encore, référez-vous [Intégration de Citrix SD-WAN Orchestrator](#).
10. Si vous disposez déjà d'un réseau SD-WAN, procédez à la création de la configuration pour le site que vous avez provisionné dans Azure. Sinon, vous devez créer un MCN. Pour plus d'informations, reportez-vous à la section [Configuration réseau](#).
11. Une fois que vous avez accès à SD-WAN Orchestrator et que vous avez déjà configuré un MCN, connectez-vous à l'orchestrateur SD-WAN et cliquez sur le **site +Nouveau** pour commencer à configurer l'appliance SD-WAN VPX (que vous avez provisionné dans Azure).

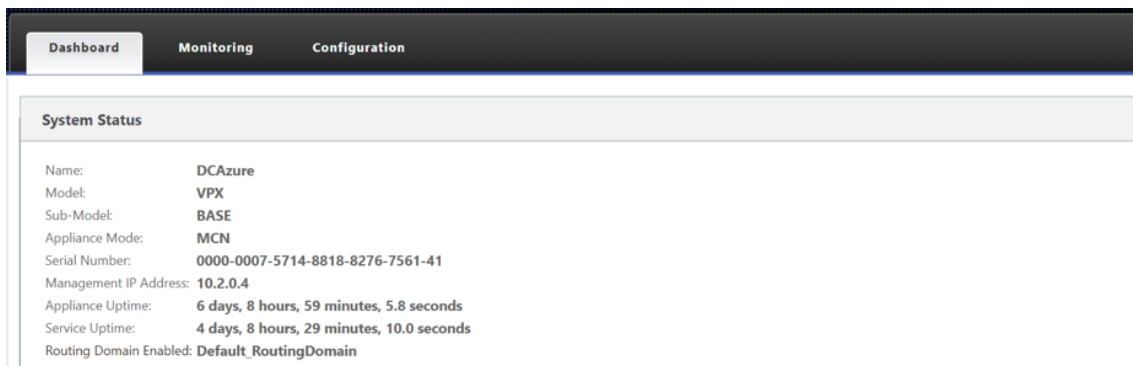


12. Indiquez un nom de site unique et entrez l'adresse en fonction de la région dans laquelle vous Provisionnez l'image. Pour configurer l'instance dans Azure, reportez-vous à la section [Paramètres de base](#).

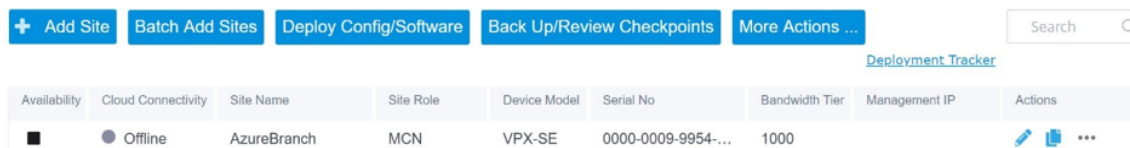
Remarque

Pour récupérer le numéro de série de l'instance dans Azure, connectez-vous à l'instance via l'IP de gestion publique. Vous pouvez voir le numéro de série sur l'écran du tableau de bord. Si vous configurez des instances dans HA, les deux numéros de série doivent être capturés. En outre, lors de la configuration de l'instance, assurez-vous que les interfaces sont choisies comme **approuvées**.

13. Pour récupérer les adresses IP associées aux interfaces LAN et WAN sur Azure. Accédez au **portail Azure > Groupes de ressources > Groupe de ressources** où le SD-WAN est **provisionné > VM SD-WAN > Mise en réseau**.



14. Une fois que vous avez terminé avec la configuration de l'instance. Cliquez sur **Déployer Config/Logiciel** en accédant à **Configuration > Configuration réseau Accueil**.



15. S'il n'y a aucun problème et que la configuration est précise, vous devez disposer des chemins virtuels entre l'instance dans Azure et votre MCN une fois le déploiement de configuration exécuté.

Configuration Citrix Virtual Apps and Desktops

Comme indiqué dans la [Déploiement et configuration](#) section, l'AD/DNS est présent dans l'emplacement local agissant comme contrôleur de domaine et dans un déploiement avec SD-WAN qu'il présente derrière le SD-WAN qui se trouve sur le réseau LAN. C'est l'IP de votre AD/DNS que vous devez configurer ici. Dans le cas où vous utilisez Azure Active Directory Service/DNS, configurez **168.63.129.16** comme adresse IP DNS.

Si vous utilisez un AD/DNS local, vérifiez si vous pouvez effectuer un ping sur l'IP de votre DNS à partir de votre appliance SD-WAN. Pour ce faire, accédez à **Dépannage > Diagnostics**. Cochez la case **Ping** et lancez un ping depuis l'interface LAN et l'interface par défaut de l'appliance SD-WAN vers l'adresse IP de votre AD/DNS.

The screenshot shows the Citrix Cloud SD-WAN Orchestrator interface. The top navigation bar includes the Citrix Cloud logo and SD-WAN Orchestrator. Below this, the customer is identified as 'cloudDNATest' and the site as 'All Sites'. The left sidebar contains navigation links: Dashboard, Reports, Configuration, Troubleshooting (with sub-links for Audit Logs, Device Logs, and Diagnostics), and Administration. The main content area is titled 'Network Troubleshooting : Diagnostics'. It features a form with the following elements:

- Test type selection: ☒ Ping, ☐ Traceroute, ☐ Packet Capture, ☐ Bandwidth Test.
- Source Site: A dropdown menu showing 'cDNTestCMD'.
- PING: A section header for the test configuration.
- IP Address: An empty text input field.
- Interface: A dropdown menu showing 'Default'.
- Gateway IP (Optional): A dropdown menu showing 'Default'.
- Routing Domain: A dropdown menu showing 'Default_RoutingDomain'.
- Packet Size (KB): A text input field showing '70'.

Si le ping réussit, cela signifie que votre AD/DNS peut être atteint avec succès, sinon cela signifie qu'il y a un problème de routage dans votre réseau qui empêche l'accès à votre AD/DNS. Si possible, essayez d'héberger votre appliance AD et SD-WAN sur le même segment LAN.

En cas de problème, contactez votre administrateur réseau. Sans terminer cette étape avec succès, l'étape de création du catalogue ne réussira pas et vous obtenez un message d'erreur comme **IP DNS global non configuré**.

Remarque

Assurez-vous que le DNS est capable de résoudre les adresses IP internes et externes.

Service de localisation du réseau

Avec le service de **localisation réseau** dans Citrix Cloud, vous pouvez optimiser le trafic interne vers les applications et les postes de travail que vous mettez à disposition des espaces de travail des abonnés pour accélérer les sessions HDX. Les utilisateurs des réseaux internes et externes doivent se connecter aux VDA via une Gateway externe. Bien que cela soit attendu pour les utilisateurs externes, les utilisateurs internes connaissent des connexions plus lentes aux ressources virtuelles. Le service d'**emplacement réseau** permet aux utilisateurs internes de contourner la Gateway et de se connecter directement aux VDA, réduisant ainsi la latence du trafic réseau interne.

Configuration

Pour configurer le service d'**emplacement réseau**, utilisez l'une des méthodes suivantes :

- **Citrix SD-WAN Orchestrator** : Pour plus d'informations sur la configuration de NLS à l'aide de Citrix SD-WAN Orchestrator, reportez-vous à la section [Service de localisation du réseau](#).
- **Module PowerShell de service d'emplacement réseau fourni par Citrix** : Pour plus d'informations sur la configuration de NLS à l'aide du module PowerShell, reportez-vous à la section [Module PowerShell et configuration](#).

Les emplacements réseau partagent les plages IP publiques des réseaux à partir desquels vos utilisateurs internes se connectent. Lorsque les abonnés lancent des sessions Virtual Apps and Desktops à partir de leur Workspace, Citrix Cloud détecte si les abonnés sont internes ou externes au réseau de l'entreprise en fonction de l'adresse IP publique du réseau à partir duquel ils se connectent.

Si un abonné se connecte à partir du réseau interne, Citrix Cloud achemine la connexion directement vers le VDA, en contournant Citrix Gateway. Si un abonné se connecte en externe, Citrix Cloud achemine l'abonné via Citrix Gateway comme prévu, puis redirige l'abonné vers le VDA dans le réseau interne.

REMARQUE

L'IP publique qui doit être configurée dans le service d'emplacement réseau doit être l'IP publique affectée aux liaisons WAN.

Système de noms de domaine

November 1, 2021

Le système de noms de domaine (DNS) traduit les noms de domaine lisibles par l'homme en adresses IP lisibles par machine, et vice versa. Citrix SD-WAN fournit les fonctionnalités DNS suivantes :

- Proxy DNS
- Transfert transparent DNS

Vous pouvez configurer un proxy DNS ou un transfert transparent DNS à l'aide des types de service DNS suivants :

- **Service DNS statique** : Permet de configurer les adresses IP du serveur DNS IPv4 statiques. Vous pouvez créer Interne, FAI, google ou tout autre service DNS open source. Le service DNS statique peut être configuré au niveau global et au niveau du site.

- **Service DNS dynamique** : permet de configurer les adresses IP du serveur DNS IPv4 dynamique. Le service DNS dynamique peut être configuré uniquement au niveau du site. Un seul service DNS dynamique est autorisé par site.
- **Service DNS Staticv6** : Permet de configurer les adresses IP statiques du serveur DNS IPv6. Vous pouvez créer Interne, FAI, google ou tout autre service DNS open source. Le service DNS Staticv6 peut être configuré au niveau global et au niveau du site.
- **Service DNS Dynamicv6** : Permet de configurer les adresses IP du serveur DNS IPv6 dynamique. Le service DNS Dynamicv6 peut être configuré uniquement au niveau du site. Un seul service DNS dynamique est autorisé par site.

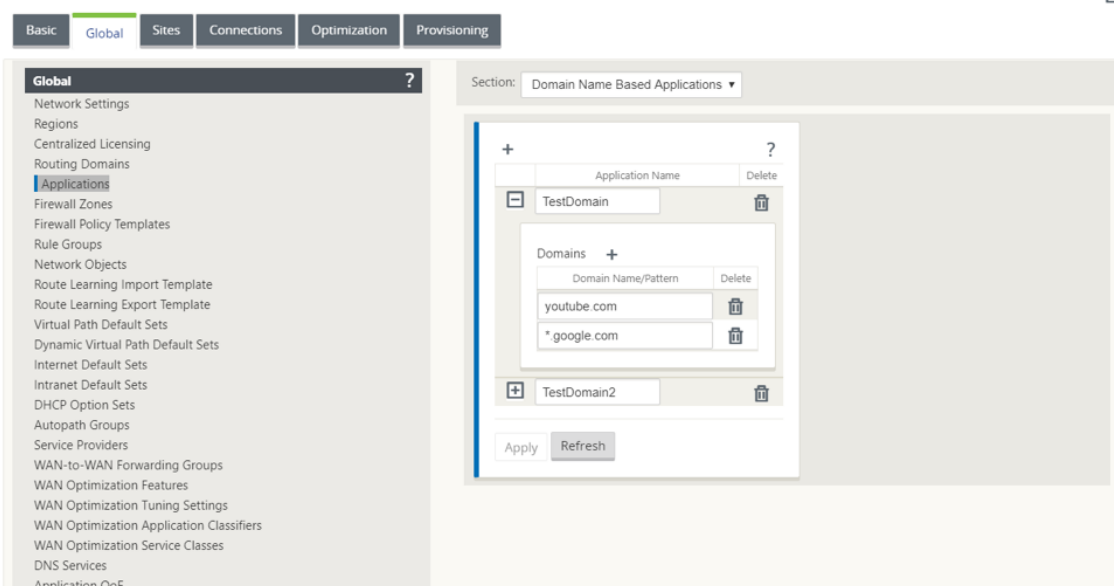
Proxy DNS

Vous pouvez configurer un proxy avec plusieurs redirecteurs qui aide à diriger les demandes DNS en fonction des noms de domaine d'application. Le transfert DNS fonctionne pour les demandes reçues via les connexions UDP.

Pour configurer SD-WAN en tant que proxy DNS :

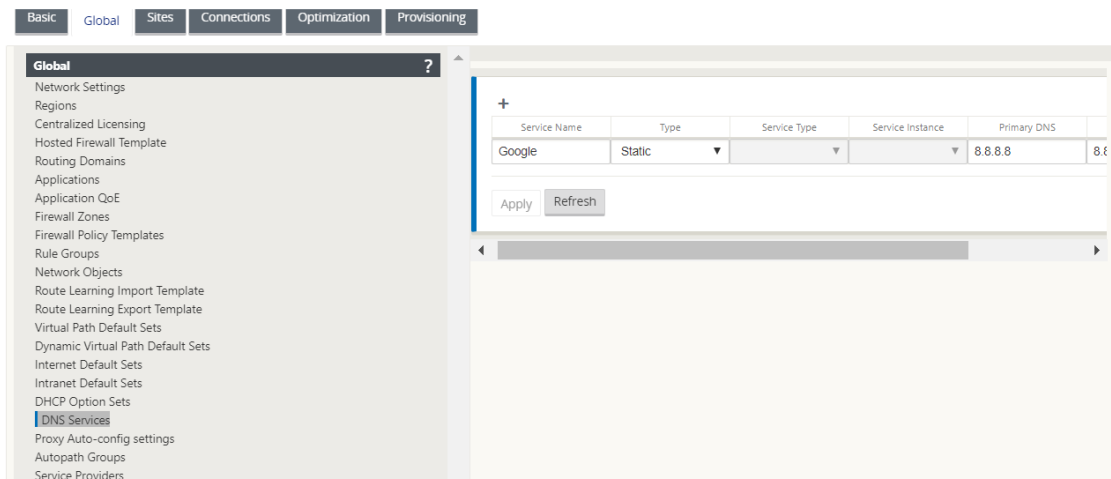
1. Définissez les applications basées sur un nom de domaine. Dans l'éditeur de configuration, accédez à **Global > Applications > Applications basées sur un nom de domaine**.

Entrez le nom de l'application et les noms de domaine ou modèles requis. Vous pouvez regrouper plusieurs noms de domaine en tant qu'application. Vous pouvez entrer le nom de domaine complet ou utiliser des caractères génériques au début. Par exemple - *.google.com



2. Définissez les services DNS requis. Vous pouvez définir un service DNS statique ou dynamique.

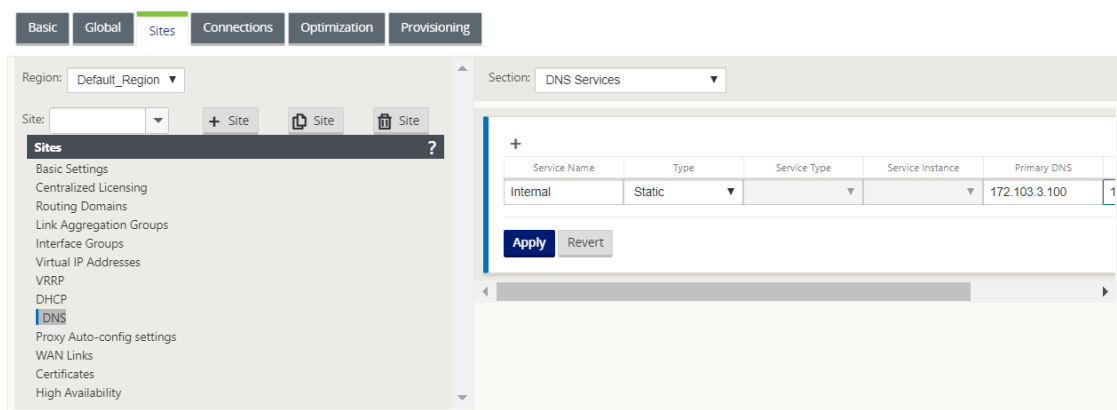
Pour configurer un service DNS statique, accédez à **Global > Service DNS**, sélectionnez **Type** en tant que **statique** (pour les adresses IPv4) ou **Staticv6** (pour les adresses IPv6). Entrez le **nom du service** et une paire d'adresses IP du serveur DNS principal et secondaire.



Remarque

Si vous avez configuré la stratégie d'intégration Office 365, un service DNS Quad9 est créé automatiquement. Pour plus d'informations, consultez la section [Optimisation d'Office 365](#).

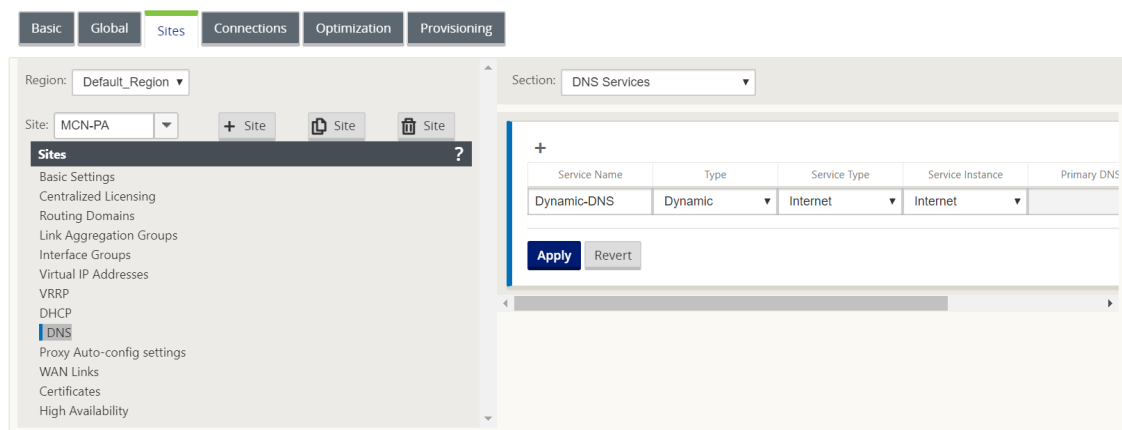
Vous pouvez également définir les services DNS statiques au niveau du site. La configuration du service DNS au niveau du site remplace la configuration globale. Pour configurer le service DNS statique spécifique au site, accédez à **Sites > DNS > Services DNS** et sélectionnez **Type** en tant que **statique** (pour les adresses IPv4) ou **Staticv6** (pour les adresses IPv6).



Pour configurer un service DNS dynamique, accédez à **Sites > DNS > Services DNS** et sélectionnez **Type** en tant que **dynamique** (pour les adresses IPv4) ou **Dynamicv6** (pour les adresses IPv6). Entrez le **nom du service** et sélectionnez **Internet** pour **Type de service** et **Instance de service**.

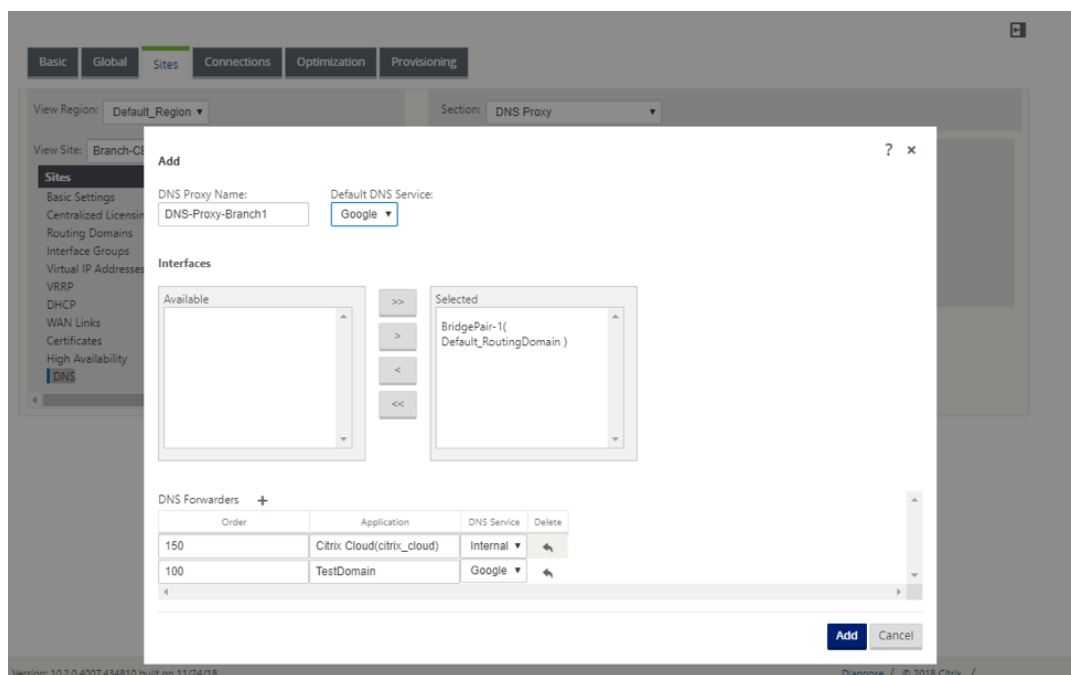
Remarque

Le service DNS dynamique peut être configuré uniquement au niveau du site. Un seul service DNS dynamique est autorisé par site.



3. Configurez le proxy DNS pour le site. Accédez à **Sites > DNS > DNS Proxy DNS**. Cliquez sur **+**. Entrez des valeurs pour les paramètres suivants :

- **Nom du proxy DNS** : nom du proxy DNS.
- **ServiceDNS par défaut IPv4 : ServiceDNS** par défaut IPv4 vers lequel les demandes DNS sont transférées, si aucune des applications ne correspond à la recherche de redirection DNS.
- **ServiceDNS par défaut IPv6 : ServiceDNS** par défaut IPv6 vers lequel les demandes DNS sont transférées, si aucune des applications ne correspond à la recherche de redirection DNS.
- **Interfaces** : Interfaces sur lesquelles les requêtes DNS sont interceptées. Seules les interfaces approuvées sont autorisées.
- **Redirecteurs DNS** : liste des redirecteurs DNS.
 - **Ordre** : priorité du transitaire.
 - **Application** : Applications pour lesquelles les demandes DNS doivent être transmises au service DNS sélectionné.
 - **ServiceDNS IPv4 : ServiceDNS** IPv4 vers lequel les demandes DNS sont transférées pour l'application spécifiée.
 - **ServiceDNS IPv6 : ServiceDNS** IPv6 vers lequel les demandes DNS sont transférées pour l'application spécifiée.



Remarque

Le proxy DNS n'est pas configurable sur les appliances SD-WAN suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

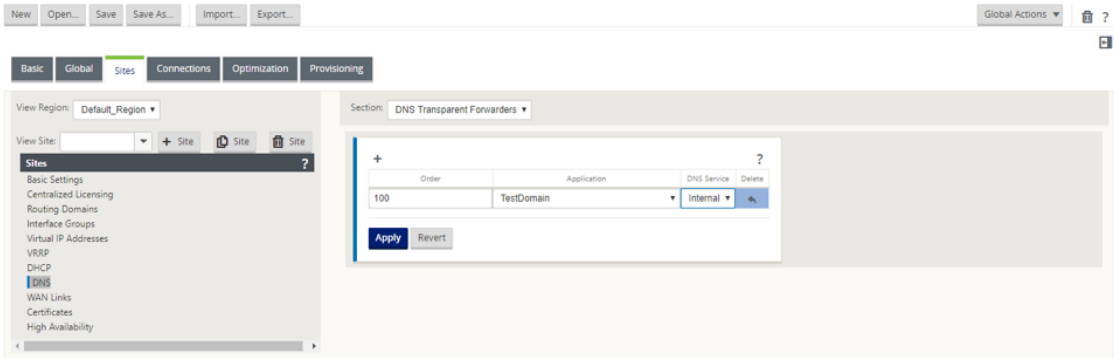
Redirecteur DNS transparent

Citrix SD-WAN peut être configuré en tant que redirecteur DNS transparent. Dans ce mode, SD-WAN peut intercepter les requêtes DNS qui ne sont pas destinées à son adresse IP et les transférer au service DNS spécifié. Seules les requêtes DNS provenant du service local sur les interfaces approuvées sont interceptées. Si les requêtes DNS correspondent à des applications de la liste de redirection DNS, elles sont transférées au service DNS configuré. Le transfert DNS est pris en charge uniquement pour les demandes arrivant via des connexions UDP.

Pour configurer le SD-WAN en tant que transitaire transparent DNS :

1. Accédez à **Sites > DNS > Redirecteurs transparents DNS**. Cliquez sur **+**.
2. Entrez des valeurs pour les paramètres suivants :
 - **Ordre** : priorité du transitaire.
 - **Application** : Applications pour lesquelles les demandes DNS doivent être transmises au service DNS sélectionné.

- **ServiceDNS IPv4 : Service**DNS IPv4 vers lequel les demandes DNS sont transférées pour l’application spécifiée.
- **ServiceDNS IPv6 : Service**DNS IPv6 vers lequel les demandes DNS sont transférées pour l’application spécifiée.



De même, continuez à ajouter d’autres redirecteurs transparents DNS si nécessaire.

3. Cliquez sur **Apply**.

Surveillance

Pour afficher les statistiques du proxy et les statistiques du redirecteur transparent, accédez à **Surveillance > DNS**.

Vous pouvez afficher le nom de l’application, le nom du service DNS, l’état du service DNS et le nombre d’accès au service DNS.

Statistiques de proxy

Dashboard	Monitoring	Configuration
Statistics	Monitoring > DNS	
Flows		
Routing Protocols		
Firewall		
IKE/IPsec		
ICMP		
Performance Reports		
Qos Reports		
Usage Reports		
Availability Reports		
Appliance Reports		
DHCP Server/Relay		
VRRP		
PPPoE		
DNS		

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
DNS_Proxy1	office365_optimize	Quad9	YES	2
DNS_Proxy1	office365_allow	Quad9	YES	8
DNS_Proxy1	office365_default	Quad9	YES	6
DNS_Proxy1	Any	Google	YES	17

Showing 1 to 4 of 4 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
office365_allow	Quad9	YES	0
office365_default	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 3 of 3 entries

Statistiques sur les redirecteurs transparents

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
No Proxy Stats at this time.				
Showing 0 to 0 of 0 entries				

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
SocialMedia	Google	YES	5
OnlineShopping	Google	YES	2
office365_optimize	Quad9	YES	1
office365_default	Quad9	YES	11
office365_allow	Quad9	YES	8

Showing 1 to 5 of 5 entries

Serveur DHCP et relais DHCP

November 16, 2022

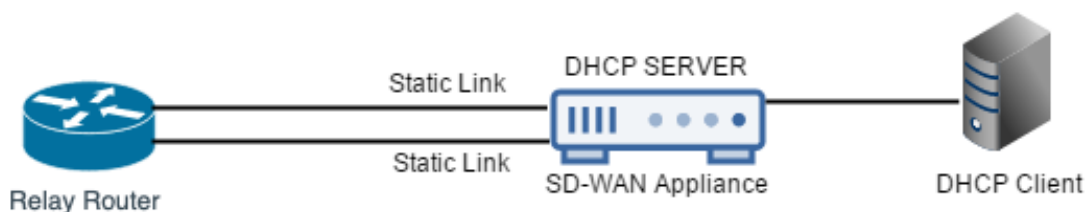
Citrix SD-WAN permet d'utiliser des appliances Standard ou Premium Edition en tant que serveurs DHCP ou agents relais DHCP. La fonctionnalité serveur DHCP permet aux périphériques du même réseau que l'interface LAN/WAN de l'appliance SD-WAN d'obtenir leur configuration IP à partir de l'appliance SD-WAN. La fonction de relais DHCP permet à vos appliances SD-WAN de transférer des paquets DHCP entre le client DHCP et le serveur.

Voici les avantages de l'utilisation du serveur DHCP et des fonctions de relais DHCP :

- Réduire la quantité d'équipement sur le site du client.
- Remplacez le routeur sur le site client (déploiement facile des services de routeur Edge).
- Simplifiez le réseau du site client.
- Configuration du routeur sans commandes CLI.
- Réduisez la configuration manuelle sur les sites clients simples.

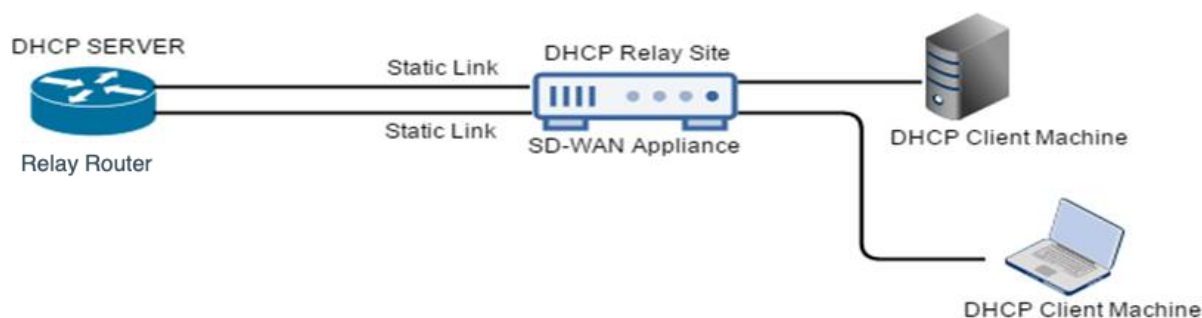
Serveur DHCP

Les appliances Citrix SD-WAN peuvent être configurées en tant que serveur DHCP. Il peut attribuer et gérer des adresses IP à partir de pools d'adresses spécifiés dans le réseau aux clients DHCP. Le serveur DHCP peut être configuré pour attribuer plus de paramètres tels que l'adresse IP du serveur DNS (Domain Name System) et le routeur par défaut. Le serveur DHCP accepte les demandes d'attribution d'adresse et les renouvellements. Le serveur DHCP accepte également les diffusions à partir de segments LAN connectés localement ou de requêtes DHCP transmises par d'autres agents relais DHCP au sein du réseau.



Relais DHCP

Un agent de relais DHCP est un hôte ou un routeur qui transfère des paquets DHCP entre les clients et les serveurs. Les administrateurs réseau peuvent utiliser le service de relais DHCP des appliances SD-WAN pour relayer les demandes et les réponses entre les clients DHCP locaux et un serveur DHCP distant. Il permet aux hôtes locaux d'acquies des adresses IP dynamiques à partir du serveur DHCP distant. L'agent relais reçoit des messages DHCP et génère un nouveau message DHCP à envoyer sur une autre interface.



Configuration du serveur DHCP et du relais DHCP

November 1, 2021

Configurer le serveur DHCP et le relais DHCP à l'aide de l'éditeur de configuration

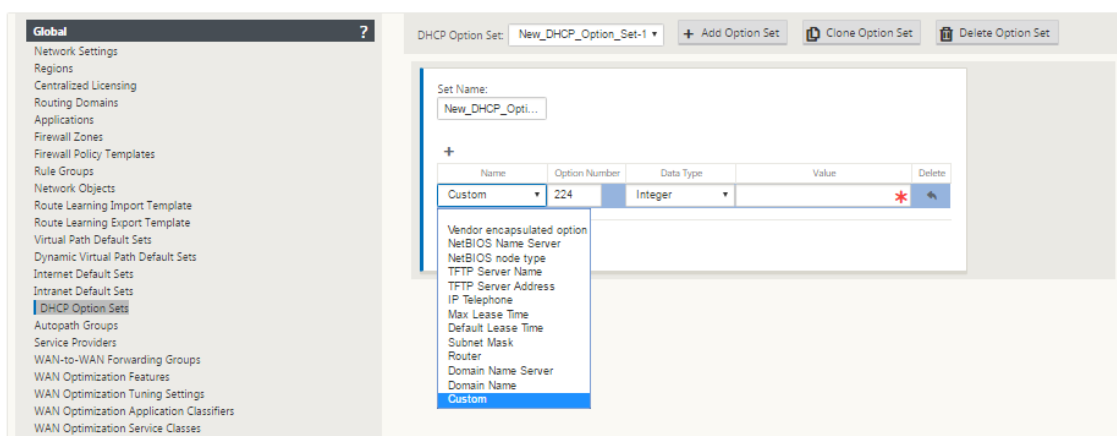
Vous pouvez configurer les paramètres du serveur DHCP et du relais DHCP pour les appliances de votre réseau à l'aide de l'éditeur de configuration. La configuration est poussée vers les appliances du réseau SD-WAN via le processus de gestion des modifications.

Pour configurer un site en tant que serveur DHCP à l'aide de l'éditeur de configuration :

1. Accédez à **Configuration Editor > Sites > [Nom du site] > DHCP > Sous-réseaux de serveur**. Cliquez sur **+**.
2. Sélectionnez un domaine de routage configuré, si plusieurs domaines sont présents.
3. Sélectionnez l'**interface virtuelle** à utiliser pour recevoir les demandes DHCP. Le sous-réseau IP utilisé par le serveur DHCP pour fournir les adresses pour est renseigné automatiquement.
4. Entrez le **nom de domaine**, le **DNS principal** et le **DNS secondaire**. Le serveur DHCP transmet ces informations aux clients.
5. Cliquez sur **Activer** pour activer le sous-réseau.
6. Configurez les pools d'adresses IP dynamiques qui seront utilisés pour allouer des adresses IP aux clients. Spécifiez l'adresse IP de début et de fin de la plage, puis sélectionnez le **jeu d'options**.

Remarque

Les jeux d'options DHCP sont des groupes de paramètres DHCP qui peuvent être appliqués à des plages d'adresses IP individuelles. Pour créer des jeux d'options DHCP, accédez à **Global > Jeux d'options DHCP**. Sélectionnez les options DHCP requises et spécifiez une valeur pour celle-ci.



7. Configurez des hôtes individuels qui nécessitent une adresse IP fixe basée sur l'adresse MAC. Également connue sous le nom d'adresse IP de réserve. Sélectionnez l'**adresse IP fixe**, l'**adresse MAC** et le **jeu d'options**.

Ranges +				
Range Start IP	Range End IP	Gateway IP	Option Set	Delete
10.200.247.200	10.200.247.205	10.200.247.1	New DHCP Option Set	

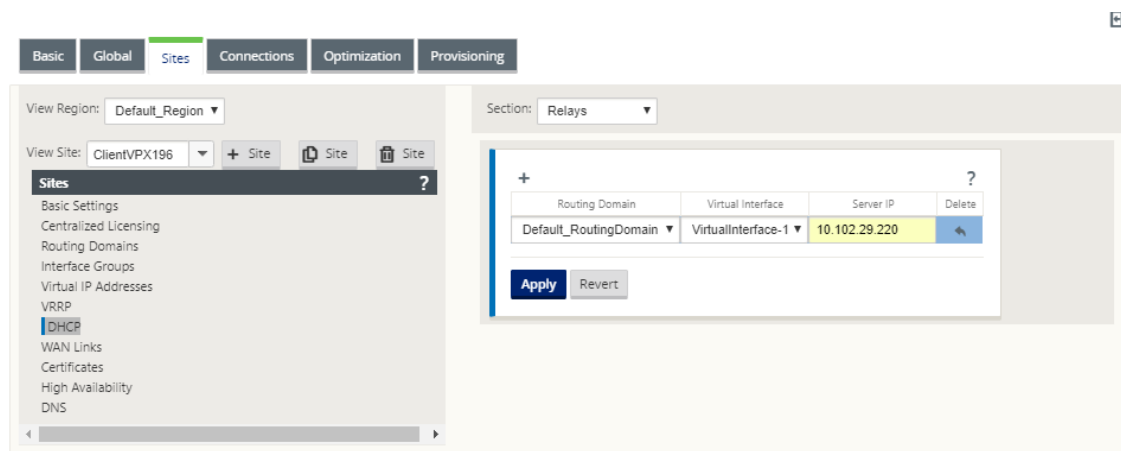
Hosts +			
Fixed IP Address	MAC Address	Option Set	Delete
10.200.247.206	1a:0a:45:14:e1:52	<None>	

Remarque

Pour les adresses IP fixes, l'**IP de passerelle** est définie en configurant l'option **Routeur** dans le **jeu d'options DHCP**.

Pour configurer un site en tant que relais DHCP à l'aide de l'éditeur de configuration :

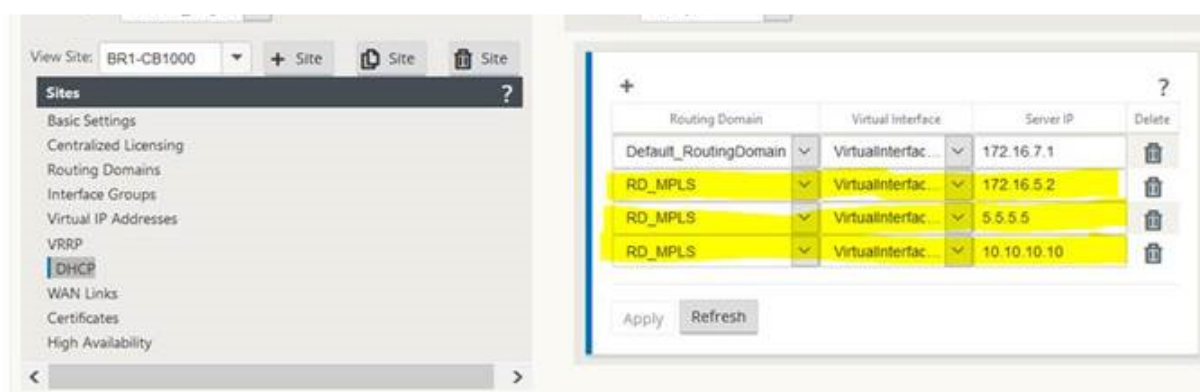
1. Accédez à **Configuration Editor > Sites**[Nom du site] > **DHCP > Relais**. Cliquez sur **+**.
2. Sélectionnez un domaine de routage configuré, si plusieurs domaines sont présents.
3. Sélectionnez une interface virtuelle qui communique avec un serveur DHCP distant.
4. Entrez l'adresse IP du serveur DHCP que le relais utilisera pour transférer la demande et la réponse des clients.



Vous pouvez configurer un relais DHCP unique à l'aide d'une interface réseau virtuelle commune et le pointer vers plusieurs serveurs DHCP.

Remarque :

Un agent relais est déclenché par interface virtuelle et un total de 16 serveurs DHCP peuvent être configurés par agent relais. Un maximum de 16 agents relais peuvent être configurés sur un site.



Pour afficher la liste des clients à partir de la base de données du serveur DHCP, dans l'interface de gestion Web, accédez à **Moniteur > Serveur/Relais DHCP**.



Configuration d'une appliance SD-WAN en tant que serveur DHCP ou relais DHCP à l'aide des paramètres de l'appliance

Vous pouvez configurer manuellement une appliance SD-WAN individuelle en tant que serveur DHCP ou en tant que réexécution DHCP à partir de la page des paramètres de l'appliance.

Pour activer le serveur DHCP sur un dispositif SD-WAN :

1. Accédez à **Configuration > Paramètres du matériel > Adaptateurs réseau**. Dans la page **Adaptateurs réseau**, recherchez le volet **Serveur DHCP de l'interface de gestion**.
2. Cliquez sur **Activer le serveur DHCP** pour démarrer le serveur, puis entrez l'**heure de location** (en minutes), le **nom de domaine** et définissez la **plage d'adresses IP** en saisissant une **adresse IP de début** et une **adresse IP de fin**.

Remarque

Le pool d'adresses IP du serveur doit se trouver dans le réseau de gestion.

Management Interface DHCP Server

If you plan to use the DHCP Server or DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead to duplicate IP addresses on the defined management network.

When HA switches from the Active to the Standby Citrix Appliance, the DHCP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working.

The Management Interface DHCP Server will use the current Management Interface IP settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server IP range, defined by Start and End IP Address, must be valid in the Management Interface subnet.

DHCP Server Status: stopped

Enable DHCP Server: ☒

Lease Time (minutes):

Domain Name:

Start IP Address:

End IP Address:

[Change Settings](#)

3. Cliquez sur **Modifier les paramètres** pour terminer la configuration du serveur DHCP.

Remarque

Si vous envisagez d'utiliser le serveur DHCP sur une appliance SD-WAN configurée pour la haute disponibilité (HA), ne configurez pas le service sur le matériel actif et de secours. Cela conduit à dupliquer les adresses IP sur le réseau de gestion défini.

4. Cliquez sur **Afficher le client** pour afficher les clients DHCP actuels, puis cliquez sur **Effacer les clients** pour libérer les baux du client DHCP

Pour activer le service de relais DHCP sur une appliance SD-WAN :

1. Accédez à **Configuration > Paramètres du matériel > Adaptateurs réseau**. Dans la page **Adaptateurs réseau**, recherchez le volet **Relais DHCP de l'interface de gestion**.
2. Cochez la case **Activer le relais DHCP** pour activer le service. Entrez l'**adresse IP du serveur DHCP** et cliquez sur **Modifier les paramètres** pour commencer à utiliser votre appliance en tant qu'agent relais DHCP.

Remarque

Si vous envisagez d'utiliser le service de relais DHCP sur une appliance configurée pour la haute disponibilité (HA), ne configurez pas le service sur les appliances actives et de secours. Cela conduit à dupliquer les adresses IP sur le réseau de gestion défini.

Management Interface DHCP Relay

Enable DHCP Relay: ☒

DHCP Server IP Address:

[Change Settings](#)

Apprentissage des adresses IP de liaison WAN via le client DHCP

June 8, 2022

Les appliances Citrix SD-WAN prennent en charge l'apprentissage des adresses IP WAN Link via les clients DHCP. Cette fonctionnalité réduit la quantité de configuration manuelle requise pour déployer des appliances SD-WAN et réduit les coûts des FAI en éliminant le besoin d'acheter des adresses IP statiques. Les appliances SD-WAN peuvent obtenir des adresses IP dynamiques pour les liaisons WAN sur des interfaces non fiables. Cela élimine le besoin d'un routeur WAN intermédiaire pour effectuer cette fonction.

Remarque

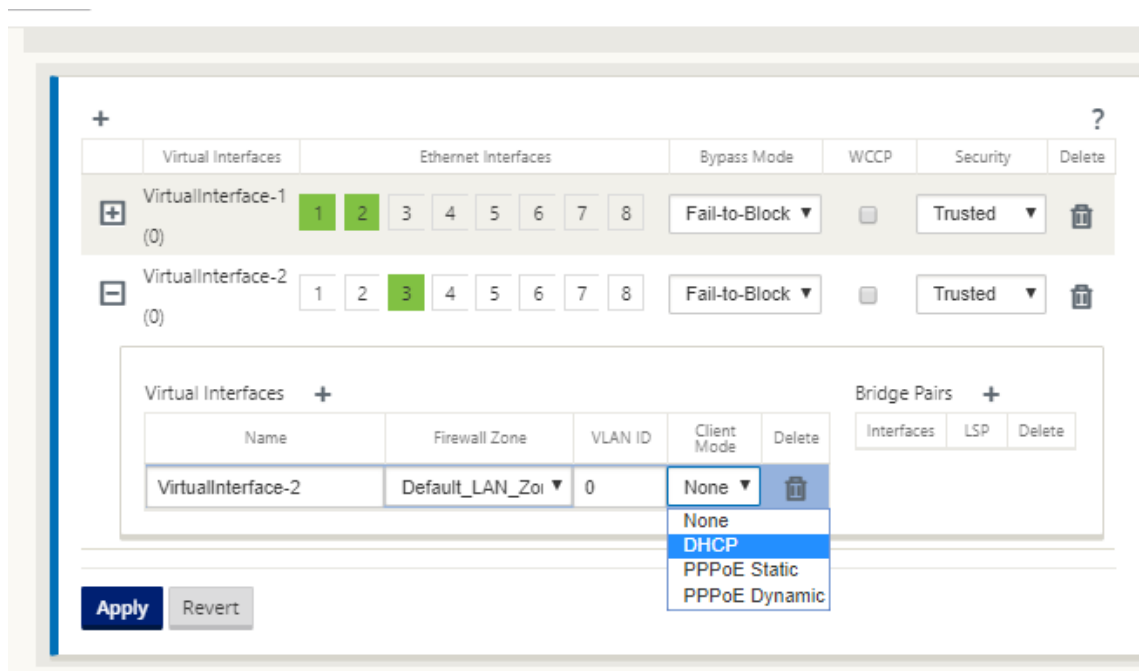
- Le client DHCP ne peut être configuré que pour les interfaces non pontées non fiables configurées en tant que nœuds client.
- Le client DHCP et le port de données peuvent être activés sur MCN/RCN uniquement si l'adresse IP publique est configurée.
- Le déploiement à bras unique ou PBR (Policy Based Routing) n'est pas pris en charge sur le site avec la configuration du client DHCP.
- Les événements DHCP sont enregistrés uniquement du point de vue du client et aucun journal du serveur DHCP n'est généré.

Pour configurer DHCP pour une interface virtuelle non approuvée en mode échec à bloc :

1. Dans l'**éditeur de configuration**, accédez à **Sites** > [Nom du site] > **Groupes d'interfaces** > **Interfaces virtuelles**.

Remarque

L'interface physique du groupe d'interfaces doit être une paire non pontée sur une seule interface.

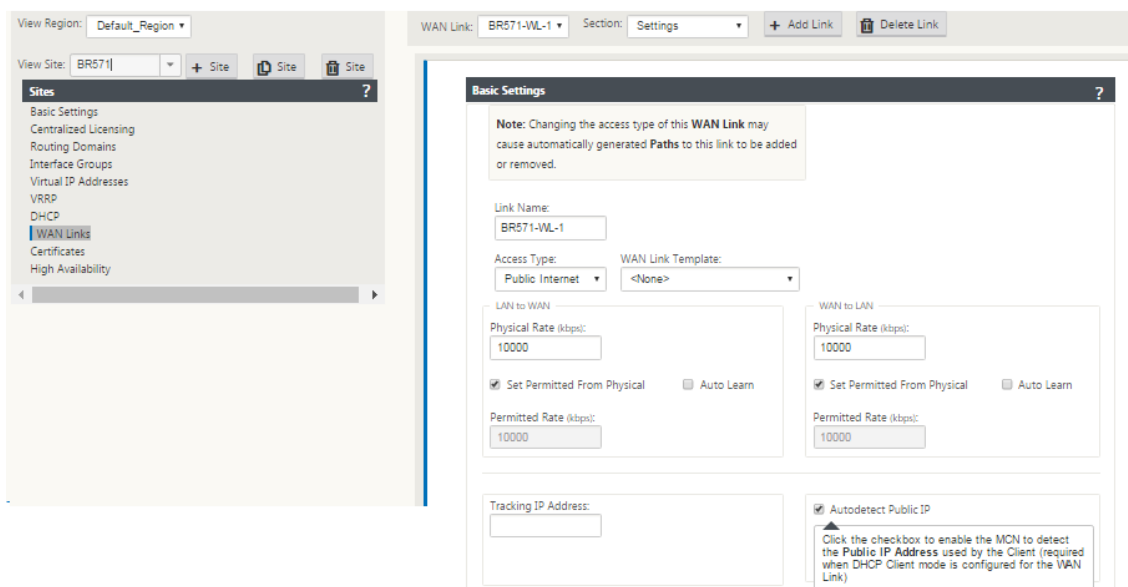


2. Sélectionnez l'une des options suivantes en tant que **mode client** :

- DHCP IPv4 uniquement
- IPv6 DHCP uniquement
- DHCP IPv4 IPv6

Si SLAAC et DHCP IPv6 ou DHCP IPv4 IPv6 sont activés, DHCPv6 fonctionne en mode sans état.

1. Accédez à **Liens WAN** > **[Nom du lien WAN]** > **Paramètres** > **Paramètres de base**.
2. Activez la case à cocher **Autodetect Public IP** pour activer le MCN pour détecter l'adresse IP publique utilisée par le client. Ceci est requis lorsque le mode Client DHCP est configuré pour la liaison WAN.

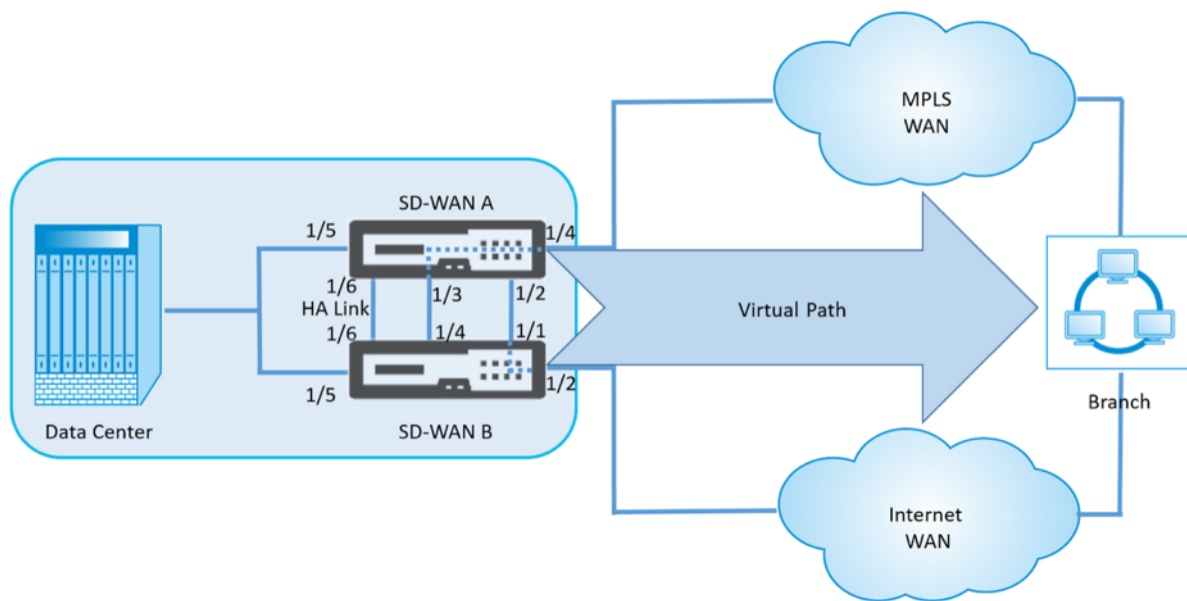


Prise en charge DHCP sur le port Fail-to-Wire

Auparavant, le client DHCP n'était pris en charge que sur le port Fail-to-Block. Avec la version 11.2.0, la capacité du client DHCP est étendue sur le port Fail-to-Wire pour le site de la succursale avec des déploiements de haute disponibilité (HA) série. Cette amélioration :

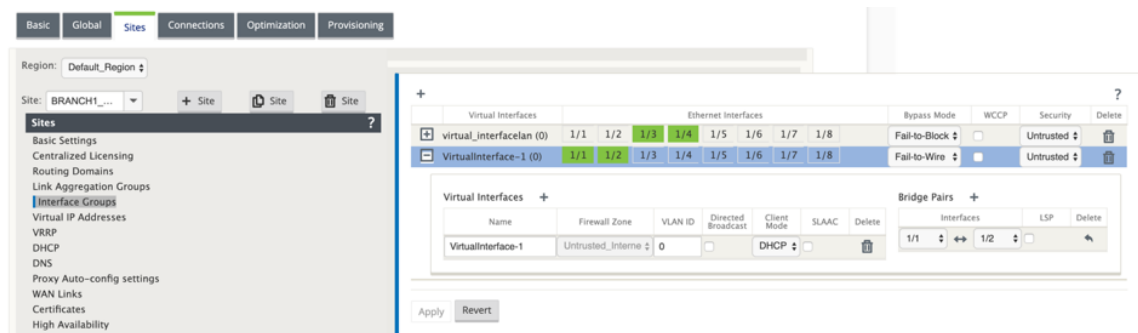
- Autorise la configuration du client DHCP sur un groupe d'interface non approuvé qui a des déploiements de paire de pont à fil et d'HA série.
- Permet de sélectionner les interfaces DHCP dans le cadre des **liaisons WAN Intranet privé**.

Le client DHCP est désormais pris en charge sur le lien intranet privé.

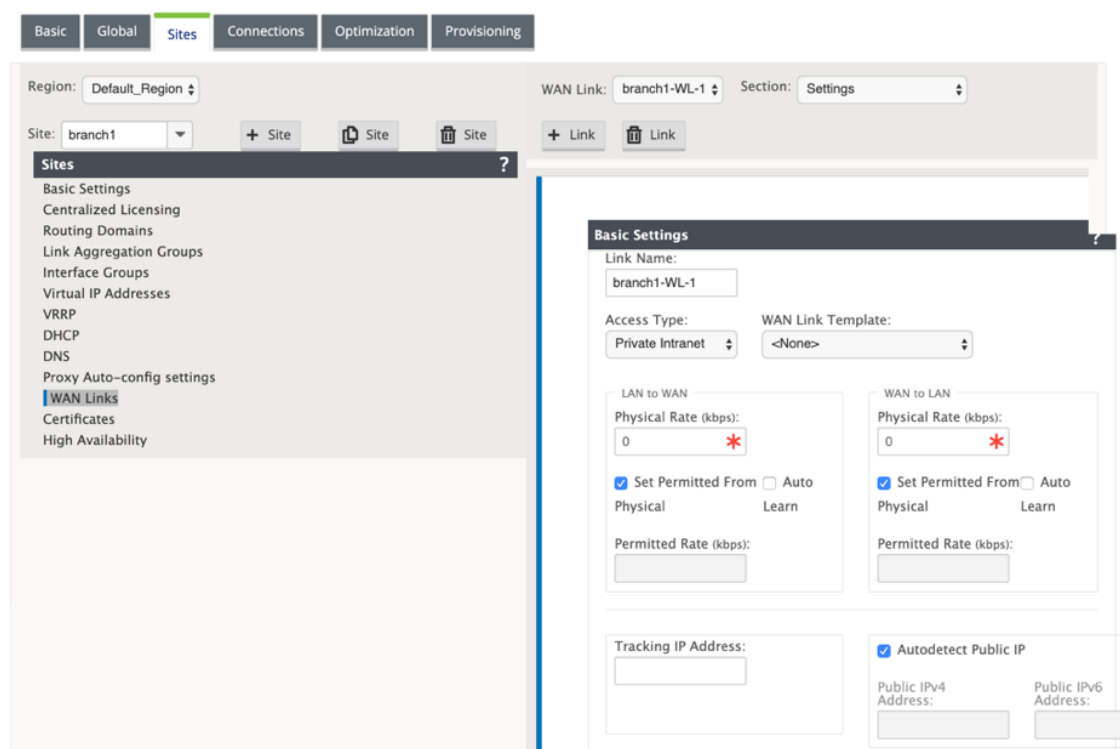


Pour configurer DHCP pour une interface virtuelle non approuvée en mode Fail-to-Wire :

1. Dans l'**éditeur de configuration**, accédez à **Sites > [Nom du site] > Groupes d'interfaces > Interfaces virtuelles**.



2. Sélectionnez l'une des options suivantes en tant que **mode client**, puis ajoutez des **paires de pont** :
 - DHCP IPv4 uniquement
 - IPv6 DHCP uniquement
 - DHCP IPv4 IPv6
3. Accédez à **Liens WAN** cliquez sur **+** sélectionnez **Nom du lien WAN** dans la liste déroulante > sélectionnez **Paramètres** dans le champ **Section> Paramètres de base**.
4. Activez la case à cocher **Autodetect Public IP** pour activer le MCN pour détecter l'adresse IP publique utilisée par le client. Ceci est requis lorsque le mode Client DHCP est configuré pour la liaison WAN.



Remarque

Une interface LAN ne doit pas être connectée à la paire Fail-to-Wire car les paquets peuvent être reliés entre les interfaces.

Surveillance des liens WAN du client DHCP

L'adresse IP virtuelle d'exécution, le masque de sous-réseau et les paramètres de passerelle sont consignés et archivés dans un fichier journal appelé *SDWANVW_ip_learned.log*. Les événements sont générés lorsque les adresses IP virtuelles dynamiques sont apprises, libérées ou arrivées à expiration, et en cas de problème de communication avec la passerelle ou le serveur DHCP appris. Ou lorsque des adresses IP en double sont détectées dans le fichier journal archivé. Si des adresses IP dupliquées sont détectées sur un site, les adresses IP virtuelles dynamiques sont libérées et renouvelées jusqu'à ce que toutes les interfaces virtuelles du site obtiennent des adresses IP virtuelles uniques.

Pour surveiller les liens WAN du client DHCP :

1. Dans la page **Enable/Disable/Purge Flows** de l'appliance SD-WAN, le tableau Liens WAN client DHCP fournit l'état des adresses IP apprises.
2. Vous pouvez demander le renouvellement de l'adresse IP, qui actualise la durée du bail. Vous pouvez également choisir de **Release Renew**, qui émet une nouvelle adresse IP ou la même adresse IP avec un nouveau bail.

DHCP Client WAN Links									
Ethernet Interface	Virtual Interface	WAN Link	IP Address / Prefix	Gateway IP Address	Lease Duration Seconds	Remaining Seconds	Expiration Date	Action	
X2	VLAN349	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

Journaux DHCP

Citrix SD-WAN vous permet de générer des journaux de serveur DHCP pour les adresses IP. Chaque fois que des adresses IP sont attribuées à des points de terminaison, les journaux sont générés. Les journaux contiennent des détails tels que l’horodatage de l’attribution de l’adresse IP et la durée du bail, l’adresse MAC, l’ID client, etc. L’ID client **none** indique qu’il n’est pas présent dans la requête DHCP.

Pour générer et afficher les journaux DHCP, accédez à **Configuration > Journalisation/surveillance**. Sélectionnez l’option **SDWAN_dhcp.log** dans la liste déroulante et cliquez sur **Afficher le journal**.

```
Feb 4 11:58:30 BR1-Primary dhcpd: Internet Systems Consortium DHCP Server 4.3.2
Feb 4 11:58:30 BR1-Primary dhcpd: Copyright 2004-2015 Internet Systems Consortium.
Feb 4 11:58:30 BR1-Primary dhcpd: All rights reserved.
Feb 4 11:58:30 BR1-Primary dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Feb 4 11:58:30 BR1-Primary dhcpd: wrote 0 deleted host decls to leases file.
Feb 4 11:58:30 BR1-Primary dhcpd: wrote 0 new dynamic host decls to leases file.
Feb 4 11:58:30 BR1-Primary dhcpd: wrote 1 leases to leases file.
Feb 4 11:58:30 BR1-Primary dhcpd: Listening on LPF/vni-1/36:00:00:52:9f:cc/172.58.3.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Sending on LPF/vni-1/36:00:00:52:9f:cc/172.58.3.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb 4 11:58:30 BR1-Primary dhcpd: Listening on LPF/vni-0/de:82:2f:9e:4c:3d/172.58.30.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Sending on LPF/vni-0/de:82:2f:9e:4c:3d/172.58.30.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPDISCOVER from 02:63:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPOFFER on 172.58.30.151 to 02:63:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPREQUEST for 172.58.30.151 from 02:63:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPACK on 172.58.30.151 to 02:63:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: Lease time Start : 4 1970/01/01 00:00:00; Lease time end : 4 1970/01/01 00:00:00; for IP : MAC-Address : 02:63:f0:de:19:3f; Client-Id : <none>
```

Remarque

Ces journaux sont générés uniquement lorsque Citrix SD-WAN agit en tant que serveur DHCP.

Personnalisation des fichiers PAC dynamique

May 6, 2021

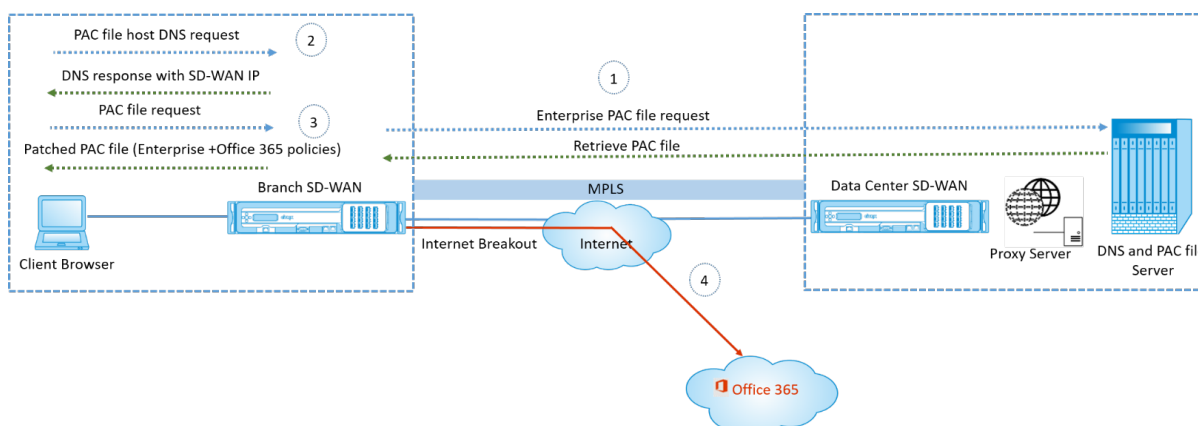
Avec l’adoption croissante des applications SaaS stratégiques et de la main-d’œuvre distribuée, il devient extrêmement crucial de réduire la latence et la congestion. La latence et la congestion sont inhérentes aux méthodes traditionnelles de réacheminement du trafic via le datacenter. Citrix SD-WAN permet de router le trafic Internet via le réseau local pour des applications SaaS telles qu’Office 365. Pour plus d’informations, reportez-vous à la section [Optimisation d’Office 365](#).

Si des proxy Web explicites sont configurés sur le déploiement de l'entreprise, tout le trafic est dirigé vers le proxy Web, ce qui rend difficile la classification et la rupture directe d'Internet. La solution consiste à exclure le trafic d'application SaaS de l'obtention d'un proxy en personnalisant le fichier PAC (Proxy Auto-Config) d'entreprise.

Citrix SD-WAN 11.0 permet de contourner le proxy et de router le trafic des applications Office 365 à travers le réseau local en générant et en servant dynamiquement un fichier PAC personnalisé. Le fichier PAC est une fonction JavaScript qui définit si les requêtes de navigateur Web vont directement à la destination ou à un serveur proxy Web.

Fonctionnement de la personnalisation des fichiers PAC

Idéalement, le fichier PAC hôte réseau d'entreprise sur le serveur Web interne, ces paramètres proxy sont distribués via la stratégie de groupe. Le navigateur client demande des fichiers PAC à partir du serveur Web d'entreprise. L'appliance Citrix SD-WAN sert les fichiers PAC personnalisés pour les sites sur lesquels la sortie Office 365 est activée.



1. Citrix SD-WAN demande et récupère périodiquement la dernière copie du fichier PAC d'entreprise à partir du serveur Web d'entreprise. L'appliance Citrix SD-WAN met à jour les URL Office 365 dans le fichier PAC d'entreprise. Le fichier PAC d'entreprise devrait avoir un espace réservé (balise spécifique SD-WAN) dans lequel les URL Office 365 sont corrigées de manière transparente.
2. Le navigateur client déclenche une requête DNS pour l'hôte de fichier PAC d'entreprise. Citrix SD-WAN intercepte la demande de nom de domaine complet du fichier de configuration proxy et répond avec le VIP Citrix SD-WAN.
3. Le navigateur Client demande le fichier PAC. L'appliance Citrix SD-WAN sert localement le fichier PAC corrigé. Le fichier PAC inclut la configuration du proxy d'entreprise et les stratégies d'exclusion d'URL Office 365.
4. Lors de la réception d'une demande d'application Office 365, l'appliance Citrix SD-WAN effectue une panne Internet directe.

Conditions préalables

1. Les entreprises devraient avoir un fichier PAC hébergé.
2. Le fichier PAC doit avoir un espace réservé *SDWAN_TAG* ou une occurrence de la fonction *find-proxyforurl* pour appliquer des correctifs aux URL Office 365.
3. L'URL du fichier PAC doit être basée sur le domaine et non sur IP.
4. Le fichier PAC n'est servi que sur les VIP d'identité de confiance.
5. L'apppliance Citrix SD-WAN doit pouvoir télécharger le fichier PAC d'entreprise via son interface de gestion.

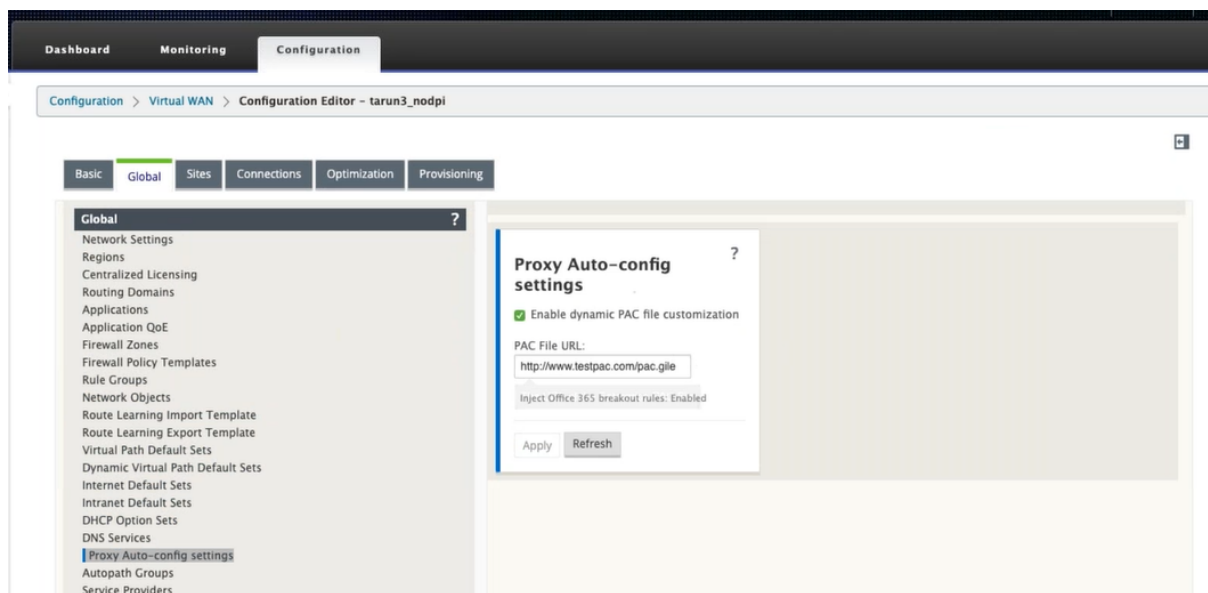
Configurer la personnalisation des fichiers PAC

Vous pouvez activer la personnalisation des fichiers PAC globalement ou au niveau du site.

Remarque

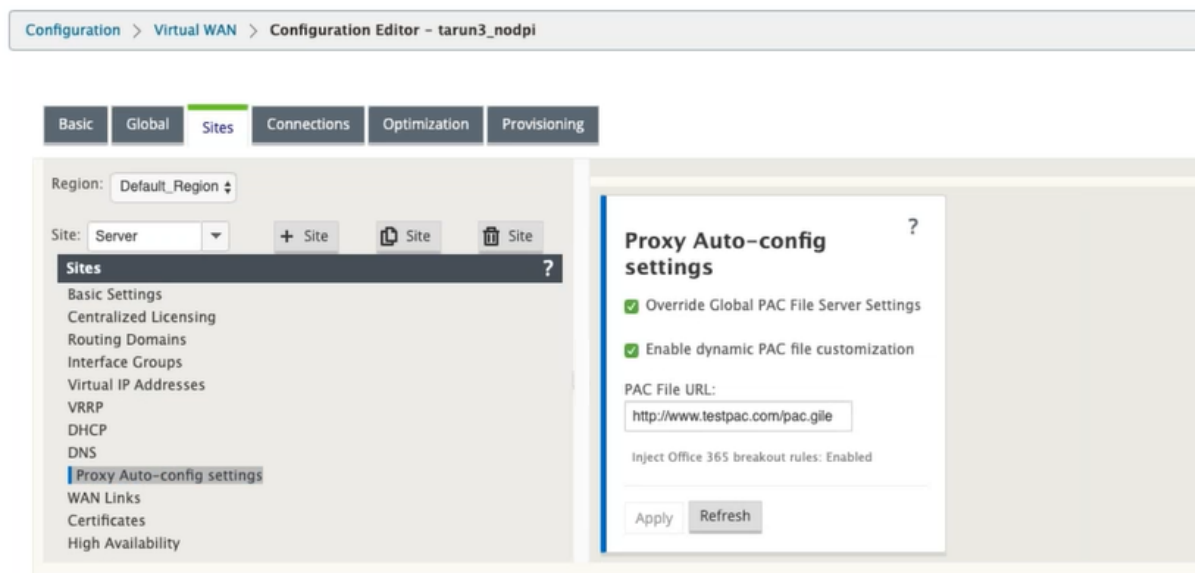
L'option de découplage Office 365 doit être activée pour la personnalisation dynamique des fichiers PAC. Pour plus d'informations sur la façon d'activer le découplage Office 365, reportez-vous à la section [Optimisation d'Office 365](#).

Pour configurer globalement la personnalisation des fichiers PAC dynamique pour tous les sites, dans l'éditeur de configuration, accédez à **Global > Paramètres de configuration automatique du proxy**.



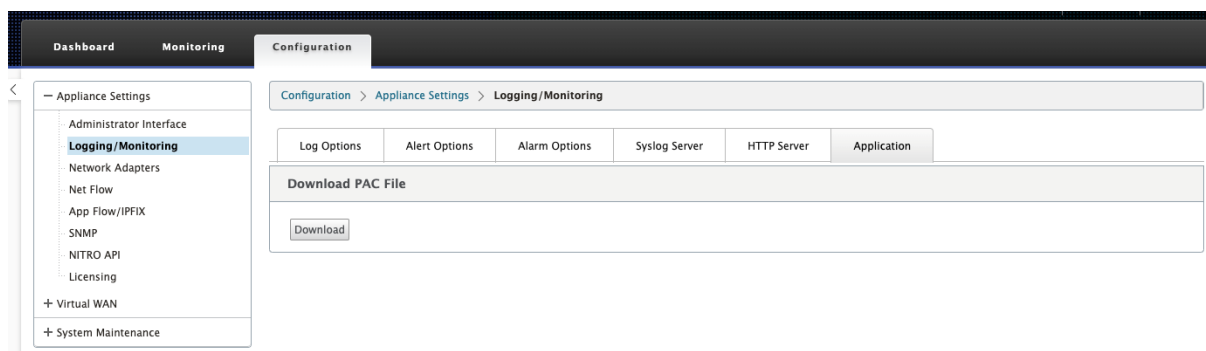
Sélectionnez **Activer la personnalisation des fichiers PAC dynamiques**. Dans le champ **URL du fichier PAC**, entrez l'URL du serveur de fichiers PAC d'entreprise. Les règles de présentation d'Office 365 sont appliquées dynamiquement au fichier PAC d'entreprise.

Pour configurer la personnalisation du fichier PAC dynamique pour un site, accédez à **Sites** > [Site] > **Paramètres de configuration automatique du proxy**. Vous pouvez également choisir de remplacer les paramètres du serveur de fichiers PAC global et spécifier une URL différente du serveur de fichiers PAC.

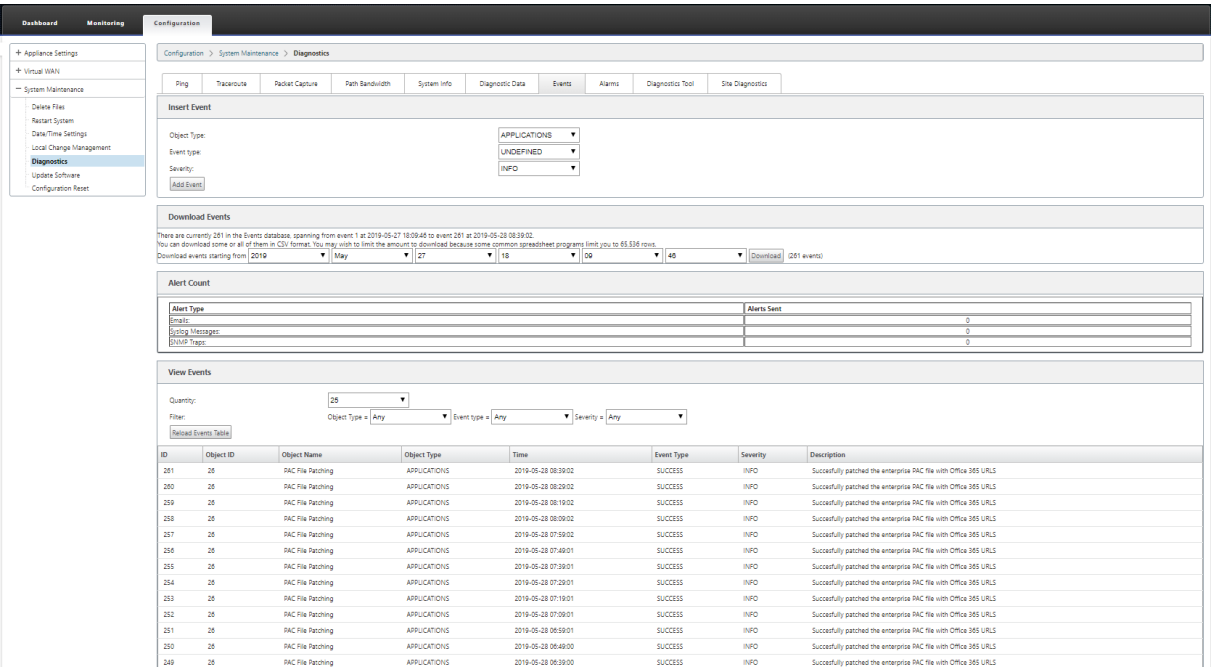


Résolution des problèmes

Vous pouvez télécharger le fichier PAC personnalisé à partir de l'appliance Citrix SD-WAN pour le débogage. Accédez à **Configuration** > **Paramètres de l'appliance** > **Logging/Monitoring** > **Application**, puis cliquez sur **Télécharger**.



Vous pouvez également afficher l'état de l'application des correctifs du fichier PAC dans la section **Événements**, accédez à **Configuration** > **Maintenance du système** > **Diagnostics**, puis cliquez sur l'onglet **Événements**.



Limitations

- Les demandes de serveur de fichiers HTTPS PAC ne sont pas prises en charge.
- Plusieurs fichiers PAC dans un réseau ne sont pas pris en charge, y compris les fichiers PAC pour les domaines de routage ou les zones de sécurité.
- La génération d’un fichier PAC sur Citrix SD-WAN à partir de zéro n’est pas prise en charge.
- WPAD via DHCP n’est pas pris en charge.

tunnel GRE

May 6, 2021

La fonctionnalité de tunnel GRE vous permet de configurer les appliances Citrix SD-WAN pour qu’elles terminent les tunnels GRE sur le réseau local ou intranet. Si vous ne souhaitez pas configurer le site en tant que nœud de terminaison de tunnel GRE, vous pouvez ignorer cette étape et passer à la section, [Configuration des liens WAN pour le site MCN](#).

Pour configurer un tunnel GRE :

En continuant dans la vue **Sites** du nouveau site MCN, cliquez sur **+** à gauche de l’étiquette **Tunnels GRE** . La table **Tunnels GRE** pour le nouveau site s’ouvre. Pour plus d’informations, consultez les rubriques du GRE.

[Configuration des tunnels GRE sur le site MCN.](#)

[Configuration des tunnels GRE pour le site de succursale.](#)

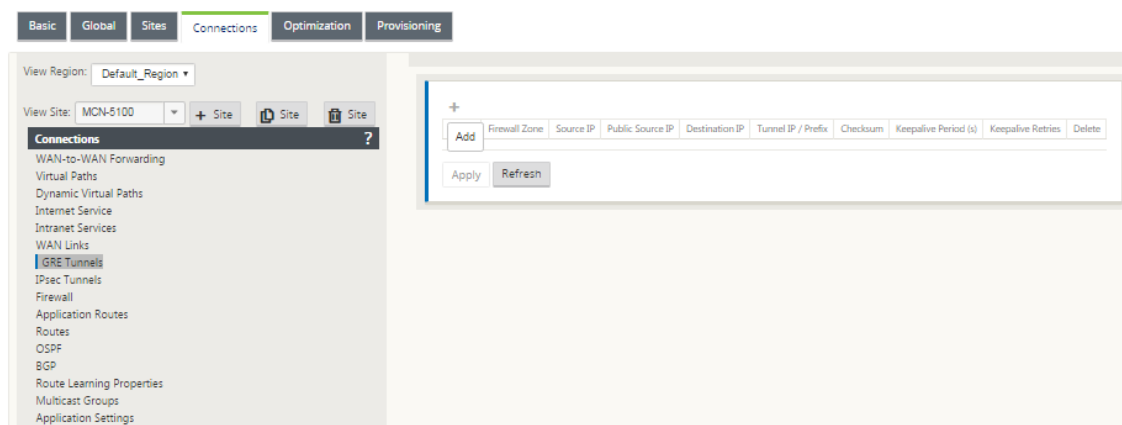
Configurer les tunnels GRE pour le site MCN (facultatif)

November 1, 2021

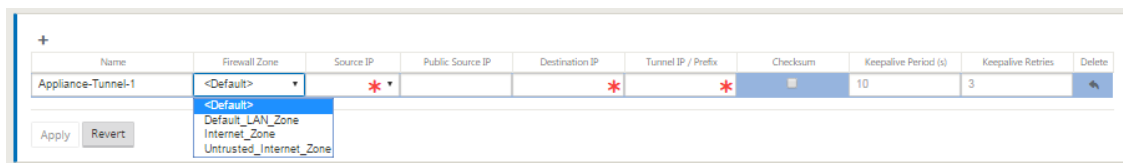
La fonctionnalité de tunnel GRE vous permet de configurer les appliances Citrix SD-WAN pour qu'elles terminent les tunnels GRE sur le réseau local ou intranet. Si vous ne souhaitez pas configurer ce site en tant que nœud de terminaison de tunnel GRE, vous pouvez ignorer cette étape et passer à la section [Configuration des liens WAN pour le site MCN](#).

Pour configurer un tunnel GRE, procédez comme suit :

1. Dans l'onglet Connexions du nouveau site MCN, cliquez sur **Tunnels GRE**. Ceci ouvre la table **Tunnels GRE** pour le nouveau site.



2. Cliquez sur **+** à droite des tunnels **GRE**. Cela ajoute une nouvelle entrée de tunnel GRE vide à la table et l'ouvre pour modification.



3. Configurez les paramètres du tunnel GRE.

Saisissez ce qui suit :

- **Type de service** - Choisissez le type de service Intranet ou LAN dans la liste déroulante.
- **Nom** :

- Si le type de service est Intranet, choisissez dans la liste des services intranet configurés dans le menu déroulant.
- Si le type de service est LAN, entrez un nom pour le nouveau tunnel GRE ou acceptez la valeur par défaut.
- Par défaut utilise un format de nommage **Appliance-Tunnel-** <number> - Où < number> est le nombre de tunnels GRE configurés pour ce site, incrémenté d'un.

• **Type de service Intranet - Pour un type** de service Intranet, choisissez **Default** ou **ZS-calier** dans la liste déroulante.

• **Zone de pare-feu** - Sélectionnez la zone de fichier pour le tunnel GRE à vous.

• **IP source** : sélectionnez une adresse IP source pour le tunnel dans le menu déroulant de ce champ. Les options de menu correspondent à la liste des interfaces virtuelles configurées pour ce site. Configurez au moins une interface virtuelle avant de pouvoir configurer un tunnel GRE. Pour obtenir des instructions, consultez [Configuration des groupes d'interface virtuelle pour le site MCN](#) et [Configuration des adresses IP virtuelles pour le site MCN](#).

- **IP source publique** : entrez l'adresse IP à utiliser comme adresse source pour les paquets dans le tunnel GRE. L'adresse IP source est le point de départ du tunnel GRE.
- Adresse **IP de destination** : saisissez l'adresse IP à utiliser comme destination de l'hôte. L'adresse IP de destination est le point d'arrivée du tunnel GRE.
- **Tunnel IP/Prefix** — Entrez l'adresse IP et le préfixe utilisés pour l'interface du tunnel GRE.
- **Somme de contrôle** — Activez la **case Somme** de contrôle pour activer la somme de contrôle pour l'en-tête GRE du tunnel.
- **Période Keepalive** — Entrez l'intervalle de temps d'attente (en secondes) entre les messages keepalive. S'il est configuré sur 0, aucun paquet keepalive n'est envoyé, mais le tunnel reste en place. La valeur par défaut est 10.
- **Retentatives Keepalive** — Saisissez le nombre de tentatives keepalive que l'appliance Virtual WAN doit tenter avant de faire descendre le tunnel. La valeur par défaut est 3.

4. Cliquez sur **Apply**. Cela soumet vos paramètres et ajoute le nouveau tunnel GRE à la table.

+									
Name	Firewall Zone	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	Default_LAN_Zo	192.113.59.5	192.113.59.8	10.199.81.237	10.199.100.2/23	<input checked="" type="checkbox"/>	10	3	
<div> <div>Apply</div> <div>Revert</div> </div>									

5. Pour configurer d'autres tunnels GRE, cliquez sur **+** à droite des **tunnels GRE**, puis suivez les étapes précédentes.

L'étape suivante consiste à configurer les [liens WAN pour le site MCN](#).

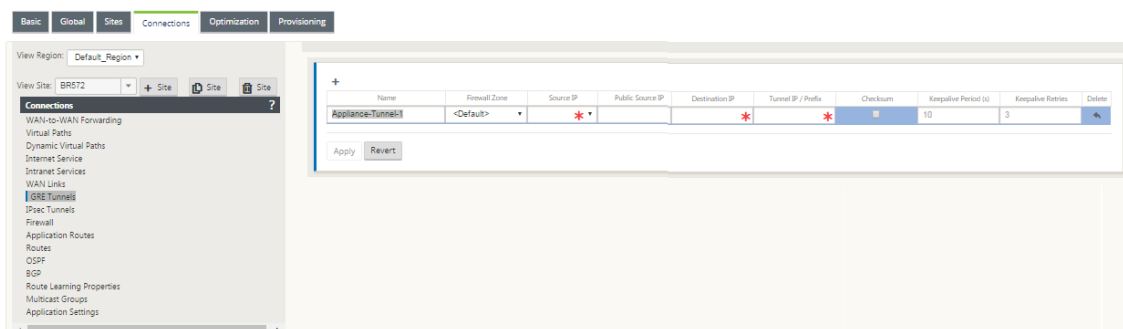
Configurer les tunnels GRE pour un site de succursale

November 1, 2021

La fonctionnalité de tunnel GRE vous permet de configurer les appliances Citrix SD-WAN pour qu'elles terminent les tunnels GRE sur le réseau local ou intranet. Si vous ne souhaitez pas configurer ce site de branche en tant que nœud de terminaison de tunnel GRE LAN, vous pouvez ignorer cette étape et passer à la section [Configuration des liens WAN pour le site de succursale](#).

Pour configurer un tunnel GRE LAN pour le site de succursale :

1. En continuant dans la vue des connexions du nouveau site de succursale, cliquez sur **Tunnels GRE**. La vue **Tunnels GRE** du nouveau site s'ouvre.
2. Cliquez sur **+** à droite des **tunnels GRE**. Cela ajoute une nouvelle entrée de tunnel GRE vide à la table et l'ouvre pour modification.



3. Configurez les paramètres du tunnel GRE. Saisissez ce qui suit :

- **Type de service** - Choisissez le type de service Intranet ou LAN dans la liste déroulante.
- **Nom** :
 - Si le type de service est Intranet, choisissez dans la liste des services intranet configurés dans le menu déroulant.
 - Si le type de service est LAN, entrez un nom pour le nouveau tunnel GRE ou acceptez la valeur par défaut.
 - Par défaut utilise un format de nommage **Appliance-Tunnel- <number>** - Où < nombre > est le nombre de tunnels GRE configurés pour ce site, incrémenté d'un.
- **Type de service Intranet - Pour un type** de service Intranet, choisissez **Default** ou **ZS-calculer** dans la liste déroulante.
- **Zone de pare-feu** : sélectionnez une zone de pare-feu pour le tunnel GRE.

- **IP source** : sélectionnez une adresse IP source pour le tunnel dans le menu déroulant de ce champ. Les options de menu sont la liste des adresses IP virtuelles que vous avez configurées pour ce site. Configurez au moins une interface virtuelle et une adresse IP virtuelle avant de pouvoir configurer un tunnel GRE LAN. Pour obtenir des instructions, reportez-vous aux sections [Configuration des groupes d'interface virtuelle pour le site de succursale](#) et [Configuration des adresses IP virtuelles pour le site de succursale](#).
 - **IP source publique** - Entrez l'adresse IP à utiliser comme adresse source pour les paquets dans le tunnel GRE. L'adresse IP source est le point de départ du tunnel GRE.
 - **Adresse IP de destination** : saisissez l'adresse IP à utiliser comme destination de l'hôte. L'adresse IP de destination est le point d'arrivée du tunnel GRE.
 - **Tunnel IP/Prefix** — Entrez l'adresse IP et le préfixe utilisés pour l'interface du tunnel GRE.
 - **Somme de contrôle** — Activez la **case Somme** de contrôle pour activer la somme de contrôle pour l'en-tête GRE du tunnel.
 - **Périodes Keepalive** : entrez l'intervalle de temps d'attente (en secondes) entre les messages keepalive. S'il est configuré sur 0, aucun paquet keepalive n'est envoyé, mais le tunnel reste en place. La valeur par défaut est 10.
 - **Retentatives Keepalive** — Saisissez le nombre de tentatives keepalive que l'appliance Virtual WAN doit tenter avant de faire descendre le tunnel. La valeur par défaut est 3.
4. Cliquez sur **Apply**. Cela soumet vos paramètres et ajoute la nouvelle entrée GRE Tunnel à la table.

Name	Firewall Zone	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	Default_LAN_Zo	192.113.59.5	192.113.59.6	10.199.81.237	10.199.108.2/20	<input checked="" type="checkbox"/>	10	3	

Apply Revert

5. Pour configurer d'autres tunnels GRE, cliquez sur **+** à droite de l'étiquette **Tunnels GRE**, puis suivez les étapes précédentes.

L'étape suivante consiste à configurer les [liens WAN pour le site de la succursale](#).

Gestion entrante et des sauvegardes

February 8, 2022

Gestion intrabande

Citrix SD-WAN vous permet de gérer l'appliance SD-WAN de deux façons : la gestion out-of-band et la gestion in-band. La gestion hors bande vous permet de créer une adresse IP de gestion à l'aide d'un port réservé à la gestion, qui transporte uniquement le trafic de gestion. La gestion in-band vous permet d'utiliser les ports de données SD-WAN pour la gestion. Il transporte à la fois le trafic de données et de gestion, sans avoir à configurer un chemin de gestion supplémentaire.

La gestion in-band permet aux adresses IP virtuelles de se connecter à des services de gestion tels que l'interface utilisateur Web et SSH. Vous pouvez activer la gestion In-band sur plusieurs interfaces de confiance qui sont activées pour être utilisées pour les services IP. Vous pouvez accéder à l'interface utilisateur Web et SSH à l'aide de l'adresse IP de gestion et des adresses IP virtuelles in-band.

À partir de la version 11.4.2 de Citrix SD-WAN, il est obligatoire de configurer la gestion in-band sur l'appliance SD-WAN, afin d'établir la connectivité au service Citrix SD-WAN Orchestrator via un port de gestion in-band. Dans le cas contraire, l'appliance perd la connectivité au service Citrix SD-WAN Orchestrator lorsque le port de gestion n'est pas connecté et que l'adresse IP intrabande n'est pas non plus configurée.

Remarque

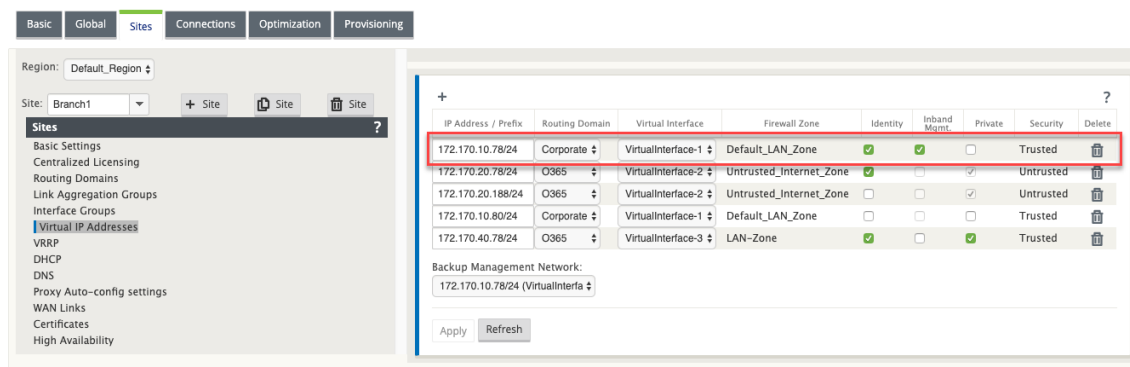
- Citrix SD-WAN Center ne prend pas en charge la connectivité à l'appliance haute disponibilité via la gestion in-band.
- Vous pouvez configurer le **type de service** comme **n'importe quel** à l'aide de l'Éditeur de configuration MCN. Le service Citrix SD-WAN Orchestrator n'autorise pas la configuration du **type de service** comme **n'importe quel** pour les stratégies NAT de destination.
- Évitez de désactiver le service lorsque la seule connectivité de gestion est HA in-band. Vous pouvez vous verrouiller de l'appliance si vous désactivez le service.

Pour activer la gestion in-band sur une adresse IP virtuelle :

1. Dans l'éditeur de configuration, accédez à **Sites > Adresses IP virtuelles**.
2. Sélectionnez **Inband Mgmt** pour les adresses IP virtuelles pour lesquelles vous souhaitez activer la gestion intrabande.

Remarque :

Assurez-vous que le type de sécurité de l'interface est **approuvé** et que **l'identité** est activée.



3. Cliquez sur **Appliquer**

Pour obtenir une procédure détaillée sur la configuration de l'adresse IP virtuelle, consultez [Comment configurer une adresse IP virtuelle](#).

À partir de la version 11.3.1 de Citrix SD-WAN, la gestion in-band prend en charge les paires d'appiances haute disponibilité. La communication entre les appliances principale et secondaire se fait via les interfaces virtuelles à l'aide de NAT.

Les ports suivants permettent la communication avec les services de gestion sur les appliances HA :

- HTTPS
 - 443 - Se connecte à la HA active
 - 444 - Redirige vers la HA primaire
 - 445 - Redirige vers la HA secondaire
- SSH
 - 22 - Se connecte à la HA active
 - 23 - Redirige vers l'HA primaire
 - 24 - Redirige vers l'AP secondaire
- SNMP
 - 161 - Se connecte à la HA actif
 - 162 - Redirige vers la HA primaire
 - 163 - Redirige vers la HA secondaire

Utilisez les stratégies NAT de destination pour créer des adresses IP qui permettent la connectivité à HA in-band sans avoir besoin d'entrer dans un port.

Par exemple, les adresses IP in-band suivantes sont utilisées pour accéder aux appliances :

- Appareil actif - 1.0.1.2
- Appareil principal - 1.0.1.10
- Appareil secondaire - 1.0.1.11

Créez deux nouvelles adresses IP virtuelles qui se trouvent dans le même réseau que celui de l’adresse IP virtuelle de gestion in-band. Dans cet exemple, 1.0.1.2/24 correspond aux adresses IP virtuelles de gestion in-band et 1.0.1.2/24 est sélectionné comme réseau de sauvegarde. 1.0.1.10 et 1.0.1.11 sont les nouvelles adresses IP virtuelles créées. 1.0.1.10 est utilisé pour accéder au matériel principal et 1.0.1.11 est utilisé pour accéder à l’appliance secondaire.

BasicGlobal**Sites**ConnectionsOptimizationProvisioning

Region: Default_Region

Site: DC+ Site Site Site

Sites

Basic SettingsCentralized LicensingRouting DomainsLink Aggregation GroupsInterface Groups**Virtual IP Addresses**VRRPDHCPDNSProxy Auto-config settingsNDP Router AdvertisementPrefix Delegation GroupWAN LinksCertificatesHigh Availability

Section: IPv4

+ ?

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Inband Mgmt.	Private	Security	Delete
1.0.0.2/24	E1Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
1.0.1.2/24	E2Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
6.0.0.1/24	E3Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
1.0.1.11/24	E2Vlan0	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
1.0.1.10/24	E2Vlan0	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Backup Management Network: 1.0.1.2/24 (E2Vlan0)DNS Proxy Name:

ApplyRefresh

Créez des stratégies NAT de destination. Les six stratégies DNAT redirigent les ports de base pour les services vers le port HA intrabande approprié. Après avoir appliqué la configuration, vous pouvez accéder directement aux appliances principales et secondaires à l’aide des adresses IP internes.

BasicGlobal**Sites**Connections**Optimization**Provisioning

Region: Default_Region

Site: DC+ Site Site Site

Connections

WAN-to-WAN ForwardingVirtual PathsDynamic Virtual PathsInternet ServiceIntranet ServicesWAN LinksGRE TunnelsIPsec Tunnels**Firewall**Application RoutesRoutesOSPFBGPRoute Learning PropertiesInter Routing Domain ServicesMulticast GroupsApplications

Section: Destination NAT Policies

+ ?

Priority	Direction	Service	Inside IP Address	Inside Port	Outside IP Address	Outside Port	Edit	Delete	Clone
100	Inbound	Any	1.0.1.10/32	443	1.0.1.2	444			
200	Inbound	Any	1.0.1.11/32	443	1.0.1.2	445			
300	Inbound	Any	1.0.1.10/32	22	1.0.1.2	23			
400	Inbound	Any	1.0.1.11/32	22	1.0.1.2	24			
500	Inbound	Any	1.0.1.10/32	161	1.0.1.2	162			
600	Inbound	Any	1.0.1.11/32	161	1.0.1.2	163			

ApplyRefresh

Surveillance de la gestion intrabande

Dans l’exemple précédent, nous avons activé la gestion in-band sur l’IP virtuelle 172.170.10.78. Vous pouvez utiliser cette adresse IP pour accéder à l’interface utilisateur Web et SSH.

Dans l’interface utilisateur Web, accédez à **Surveillance > Pare-feu**. Vous pouvez voir SSH et l’inter- face utilisateur Web accessibles à l’aide de l’IP virtuelle sur les ports 22 et 443 respectivement dans

la colonne **Adresse IP de destination** .

← → ↻ ⚠ Not secure | Http://172.170.10.78/ | bin/vwmon.cgi

Monitoring | Configuration

Monitoring > Firewall

Firewall Statistics

Statistics

Maximum entries to display: 50

Filtering

Routing Domain: Any

Application: Any

Family: Any

IP Protocol: Any

Source Zone: Any

Destination Zone: Any

Source Service Type: Any

Source Service Instance: Any

Source IP:

Source Port:

Destination Service Type: Any

Destination Service Instance: Any

Destination IP: 172.170.10.78

Destination Port:

Refresh

Show latest data

Show Drops

Clear Connections

Help

Connections

Routing Domain	Application	Family	IP Protocol	Source				Destination				State	Is NAT	Sent			Received					
				IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type			Service Name	Zone	Packets	Bytes	PPS	Packets	Bytes	PPS	
Corporate	Secure Shell(ssh)	Encrypted	TCP	172.170.10.135	54257	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	22	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	78	6824	0.364	0.295	53	7429	0.247
Corporate	Hypertext Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54288	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	129	10130	5.692	3.319	234	338238	9.583
Corporate	Hypertext Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54299	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	565	28811	23.147	9.443	1087	1594099	44.533
Corporate	Hypertext Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54300	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	90	9201	3.691	3.019	157	212744	6.439
Corporate	Hypertext Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54301	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	111	7987	4.554	2.621	202	291743	8.287
Corporate	Hypertext Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54302	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.419	0.434	4	309	0.280
Corporate	Hypertext Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54303	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.422	0.437	4	309	0.282
Corporate	Hypertext Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54289	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	355	20266	13.558	16.681	1066	1392449	25.435

Remarque

La gestion intrabande n’est pas prise en charge sur les appliances SD-WAN suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

Provisioning intrabande

La nécessité de déployer des appliances SD-WAN dans des environnements plus simples, comme la maison ou les petites succursales, a considérablement augmenté. La configuration d’un accès de gestion distinct pour des déploiements plus simples est une surcharge supplémentaire. Le déploiement sans contact et la fonction de gestion in-band permettent le provisionnement et la gestion de la configuration via des ports de données désignés. Le déploiement sans contact est désormais pris en charge sur les ports de données désignés et il n’est pas nécessaire d’utiliser un port de gestion distinct pour le déploiement zéro contact. Citrix SD-WAN permet également de basculer le trafic de gestion en toute transparence vers le port de gestion lorsque le port de données tombe en panne et vice versa.

Une appliance expédiée en usine, qui prend en charge le Provisioning in-band, peut être provisionnée en connectant simplement le port de données ou de gestion à Internet. Les appliances prenant en charge le Provisioning in-band disposent de ports spécifiques pour le réseau local et le réseau étendu. L’appliance en état de réinitialisation d’usine a une configuration par défaut qui permet d’établir une connexion avec le service de déploiement zéro contact. Le port LAN agit en tant que serveur DHCP et attribue une IP dynamique au port WAN qui agit en tant que client DHCP. Les liaisons WAN surveillent

le service DNS Quad 9 pour déterminer la connectivité WAN.

Remarque

Le Provisioning en bande s'applique uniquement aux plates-formes SD-WAN 110 SE et SD-WAN VPX.

Une fois l'adresse IP obtenue et une connexion établie avec le service de déploiement zéro contact, les packages de configuration sont téléchargés et installés sur l'appliance. Pour plus d'informations sur le déploiement sans intervention via SD-WAN Center, consultez la section [Déploiement Zero Touch](#). Pour plus d'informations sur le déploiement sans intervention via SD-WAN Orchestrator, reportez-vous à la section [Déploiement sans intervention](#).

Remarque : pour le provisionnement jour 0 des appliances SD-WAN via les ports de données, la version logicielle de l'appliance doit être SD-WAN 11.1.0 ou supérieure.

La configuration par défaut d'une appliance en état de réinitialisation d'usine comprend les configurations suivantes :

- Serveur DHCP sur port LAN
- Client DHCP sur port WAN
- Configuration QUAD9 pour DNS
- L'IP LAN par défaut est 192.168.0.1
- Licence Grace de 35 jours.

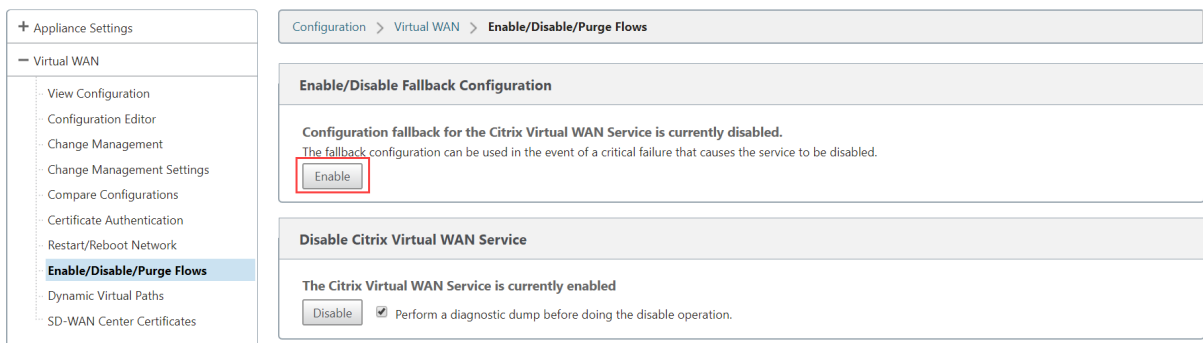
Une fois l'appliance provisionnée, la configuration par défaut est désactivée et remplacée par la configuration reçue du service de déploiement zéro touche. Si une licence d'appliance ou une licence de grâce expire, la configuration par défaut est activée afin de garantir que l'appliance reste connectée au service de déploiement zéro touche et qu'elle reçoit les licences gérées via un déploiement zéro contact.

Configuration par défaut/de secours

La configuration de secours garantit que l'appliance reste connectée au service de déploiement zéro contact en cas de défaillance de liaison, de non-correspondance de configuration ou de non-correspondance logicielle. La configuration de secours est activée par défaut sur les appliances disposant d'un profil de configuration par défaut. Vous pouvez également modifier la configuration de secours en fonction de vos paramètres réseau LAN existants.

Remarque : Après le provisionnement initial de l'appliance, vérifiez que la configuration de secours est activée pour la connectivité du service de déploiement zéro contact.

Si la configuration de retour arrière est désactivée, vous pouvez l'activer en accédant à **Configuration > Paramètres de l'appliance > Config par défaut/de secours** > cliquez sur **Activer**.



Le tableau suivant fournit les détails des ports WAN et LAN prédésignés pour la configuration de secours sur différentes plates-formes :

Plateforme	Ports WAN	Ports LAN
110	12	1/1
110-LTE	1/2, LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)

À partir de Citrix SD-WAN version 11.3.1, les paramètres du port WAN sont configurables. Les ports WAN peuvent être configurés en tant que liens WAN indépendants à l'aide du client DHCP et surveiller le service DNS Quad9 pour déterminer la connectivité WAN. Vous pouvez configurer les IP WAN ou IP statiques pour les ports WAN en l'absence de DHCP pour utiliser la gestion in-band pour le provisionnement initial.

Remarque

Vous pouvez uniquement configurer les ports Ethernet avec les IP statiques. Les IP statiques ne sont pas configurables avec les ports LTE-1 et LTE-E1. Bien que vous puissiez ajouter les ports LTE-1 et LTE-E1 en tant que WAN, les champs de configuration restent non modifiables.

Lorsque vous ajoutez un port WAN, il est ajouté dans la section **Paramètres WAN (Port : 2)** avec la case **Mode DHCP** activée par défaut. Si la case à cocher **Mode DHCP** est activée, les champs de texte **Adresse IP**, **Adresse IP de passerelle** et **ID VLAN** sont grisés. Désactivez la case à cocher **Mode DHCP** si vous souhaitez configurer l'adresse IP statique.

WAN Settings (Ports: 2)					
Port	DHCP Mode	IP Address	Gateway IP Address	VLAN ID	Wan Tracking IP Address
2	<input type="checkbox"/>	11.11.11.10/24	11.11.11.11	50	
4	<input checked="" type="checkbox"/>				9.9.9.9
5	<input checked="" type="checkbox"/>				9.9.9.9

Par défaut, le champ **Adresse IP de suivi WAN** est automatiquement rempli avec le 9.9.9.9. Vous pouvez modifier l'adresse au besoin.

Remarque

Si vous activez la case à cocher **Serveurs DNS dynamiques**, assurez-vous d'ajouter/configurer au moins un port WAN avec le **mode DHCP** sélectionné.

Pour personnaliser la configuration de secours selon votre réseau LAN :

1. Accédez à **Configuration > Paramètres de l'apppliance > Config par défaut/secours**.
2. Modifiez les valeurs des paramètres LAN suivants en fonction des exigences de votre réseau. Il s'agit de la configuration minimale requise pour établir une connexion avec le service de déploiement zéro touche.
 - **ID VLAN** : ID VLAN auquel le port LAN doit être groupé.
 - **Adresse IP : Adresse** IP virtuelle affectée au port LAN.
 - **DHCP activé** : active le port LAN en tant que serveur DHCP. Le serveur DHCP attribue des adresses IP dynamiques aux clients sur le port LAN.
 - **Début DHCP et fin DHCP** : Plage d'adresses IP que DHCP utilise pour attribuer dynamiquement une adresse IP aux clients sur le port LAN.
 - **Serveur DNS** : adresse IP du serveur DNS principal.
 - **Serveur DNS Alt** : Adresse IP du serveur DNS secondaire.
 - **Accès Internet** : Autoriser l'accès Internet à tous les clients LAN sans autre filtrage.

Fallback Configuration

The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.

WAN Settings (Ports: 1)

WAN settings are currently not configurable. WAN ports are configured as independent WAN Links using DHCP client and monitor the Quad9 DNS service to determine WAN connectivity.

LAN Settings (Ports: 2)

VLAN ID:

0

IP Address:

192.168.0.1/24

DHCP Enabled:

☐

DHCP Start:

192.168.0.50

DHCP End:

192.168.0.250

DNS Server:

9.9.9.9

Alt DNS Server:

149.112.112.112

Internet Access:

☐ ?

Port Settings

Port Name	Mode
1	<input checked="" type="radio"/> WAN <input type="radio"/> LAN <input type="radio"/> Disabled
2	<input type="radio"/> WAN <input checked="" type="radio"/> LAN <input type="radio"/> Disabled
3	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled
4	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled
5	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled
6	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled
7	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled
8	<input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled

Unassigned Port Bypass Mode: Fail-to-Block ▼

Apply

3. Configurez le mode pour chaque port. Le port peut être un port LAN ou un port WAN ou peut être désactivé. Les ports affichés dépendent du modèle de l’appliance. En outre, définissez le mode de contournement de port sur **Fail-to-block** ou **Fail-to-Wire**.
- Pour réinitialiser la configuration de secours à la configuration par défaut à tout moment, cliquez sur **Réinitialiser**.

Remarque

La configuration de secours n’est pas prise en charge sur les appliances SD-WAN suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

Port de gestion ou de données configurable

La gestion in-band permet aux ports de données de transporter à la fois les données et le trafic de gestion, éliminant ainsi le besoin d'un port de gestion dédié. Cela laisse le port de gestion inutilisé sur les appliances bas de gamme, qui ont déjà une faible densité de port. Citrix SD-WAN vous permet de configurer le port de gestion pour qu'il fonctionne en tant que port de données ou port de gestion.

Remarque

Vous pouvez convertir le port de gestion en port de données uniquement sur les plates-formes suivantes :

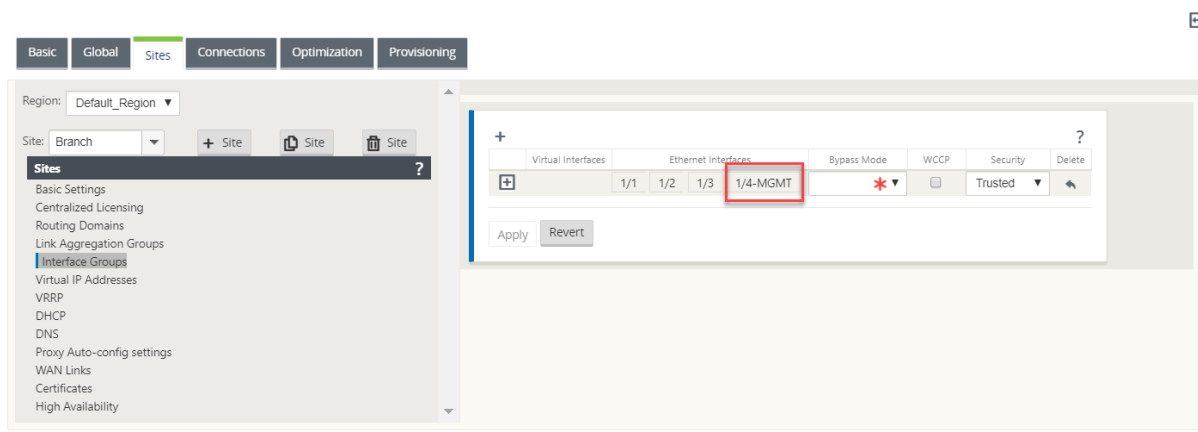
- Citrix SD-WAN 110 SE/LTE
- Citrix SD-WAN 210 SE/LTE

Dans l'éditeur de configuration, utilisez le port de gestion dans votre configuration. Une fois la configuration activée, le port de gestion est converti en port de données.

Remarque

Vous pouvez configurer un port de gestion uniquement lorsque la gestion intrabande est activée sur d'autres interfaces approuvées de l'appliance.

Pour configurer une interface de gestion, dans l'éditeur de configuration, accédez à **Sites**, sélectionnez un site et cliquez sur **Groupes d'interface**. L'interface MGMT est disponible pour être configurée. Pour plus d'informations sur la configuration des groupes d'interfaces, consultez la rubrique [Procédure de configuration des groupes d'interfaces](#).



Pour reconfigurer le port de gestion afin d'exécuter la fonctionnalité de gestion, supprimez la configuration. Créez une configuration sans utiliser le port de gestion et activez-la.

Réseau de gestion des sauvegardes

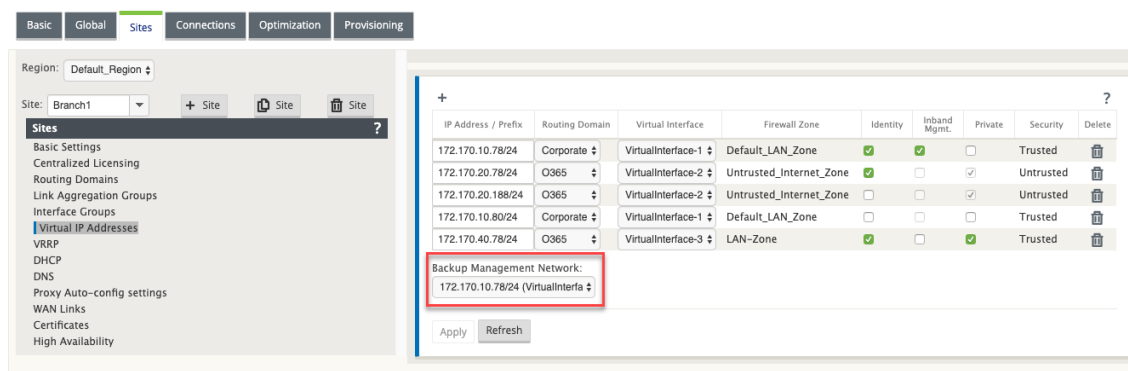
Vous pouvez configurer une adresse IP virtuelle en tant que réseau de gestion de sauvegarde. Il est utilisé comme adresse IP de gestion si le port de gestion n'est pas configuré avec une Gateway par défaut.

Remarque

Si un site possède un service Internet configuré avec un seul domaine de routage, une interface de confiance dont l'identité est activée est sélectionnée comme réseau de gestion de sauvegarde par défaut.

Pour sélectionner une adresse IP virtuelle en tant que réseau de gestion de sauvegarde :

1. Dans l'éditeur de configuration, accédez à **Sites > Adresses IP virtuelles**.
2. Sélectionnez une adresse IP virtuelle en tant que réseau de gestion de sauvegarde.



3. Sélectionnez le proxy DNS vers lequel toutes les demandes DNS sur le plan de gestion in-band et de sauvegarde sont transférées.

Remarque

Le proxy DNS peut être sélectionné uniquement lorsque la gestion In-band et Backup Management Network sont activés pour une adresse IP virtuelle.

4. Cliquez sur **Apply**.

Pour obtenir une procédure détaillée sur la configuration de l'adresse IP virtuelle, consultez [Comment configurer l'adresse IP virtuelle](#)

Surveillance de la gestion des sauvegardes

Dans l'exemple précédent, nous avons sélectionné 172.170.10.78 IP virtuelle comme réseau de gestion de sauvegarde. Si l'adresse IP de gestion n'est pas configurée avec une Gateway par défaut, vous pouvez utiliser cette adresse IP pour accéder à l'interface utilisateur Web et SSH.

Dans l’interface utilisateur Web, accédez à **Surveillance > Pare-feu**. Vous pouvez voir cette adresse IP virtuelle comme adresse IP source pour l’accès SSH et l’accès à l’interface utilisateur Web.

Monitoring > Firewall

Firewall Statistics

Statistics:

Connections

Maximum entries to display:

50

Filtering:

Routing Domain:

Any

Application:

Any

Family:

Any

IP Protocol:

Any

Source Zone:

Any

Destination Zone:

Any

Source Service Type:

Any

Source Service Instance:

Any

Source IP:

172.170.10.78

Source Port:

Destination Service Type:

Any

Destination Service Instance:

Any

Destination IP:

Destination Port:

Refresh

Show latest data

Show Drops

Clear Connections

Help

Connections

Routing Domain	Application	Family	IP Protocol	Source				Destination				State	Is NAT	Sent			Received				
				IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	Packets	Bytes	PPS	Packets	Bytes	PPS		
Corporate	Transmission Control Protocol(tcp)	Network Service	TCP	172.170.10.78	49818	IPHost	-	Default_LAN_Zone	18.210.2.11	443	Internet	Branch1-Internet	Untrusted_Internet_Zone	SYN_SENT	Yes	1	60	-	0	0	-
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58939	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	NEW	Yes	2	148	-	0	0	-
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43012	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	168	0.070	2	297	0.070
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36558	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	148	0.011	2	277	0.011
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.78	60624	IPHost	-	Default_LAN_Zone	18.235.40.8	443	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	9	1271	0.176	7	4069	0.137
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	60585	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	1	128	0.003
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58010	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.020	1	80	0.020
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36684	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	1	161	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	33173	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	1	80	0.003
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53914	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	1	128	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53708	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	128	0.013	2	144	0.013
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43704	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	1	128	0.003

Accès Internet

May 6, 2021

Le service Internet est utilisé pour le trafic entre un site d'utilisateur final et des sites sur Internet public. Le trafic de service Internet n'est pas encapsulé par SD-WAN et n'a pas les mêmes capacités que le trafic fourni par le service Virtual Path. Cependant, il est important de classer et de prendre en compte ce trafic sur le SD-WAN. Le trafic identifié comme un service Internet permet de gérer activement la bande passante des liaisons WAN en limitant le trafic Internet par rapport au trafic acheminé par le chemin virtuel et intranet selon la configuration établie par l'administrateur. En plus des capacités de Provisioning de bande passante, le SD-WAN offre la possibilité supplémentaire d'équilibrer la charge du trafic acheminé sur le service Internet à l'aide de plusieurs liaisons WAN Internet ou, éventuellement, d'utiliser les liaisons Internet WAN dans une configuration principale ou secondaire.

Le contrôle du trafic Internet à l'aide du service Internet sur les appliances SD-WAN peut être configuré dans les modes de déploiement suivants :

- Routage d'Internet direct à la succursale avec pare-feu intégré
- Réacheminement direct par Internet à la succursale vers Secure Web Gateway
- Réacheminement d'Internet vers le MCN DataCenter

Internet Traffic Control

Direct Internet Breakout at Branch with Integrated Firewall



Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



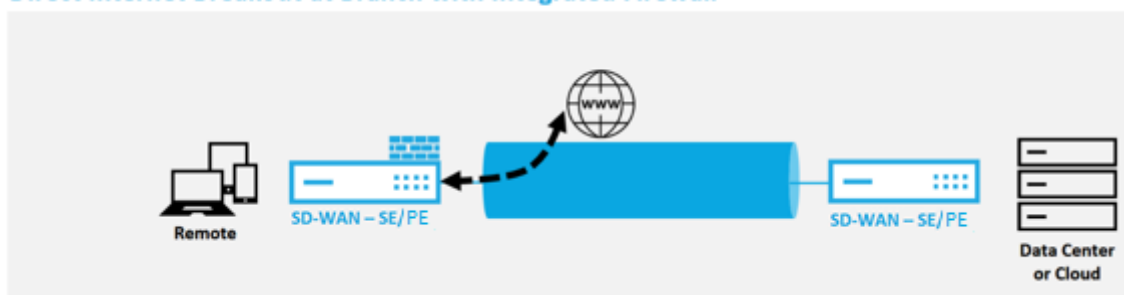
Backhaul Internet to Data Center MCN



Routage d'Internet direct à la succursale avec pare-feu intégré

May 6, 2021

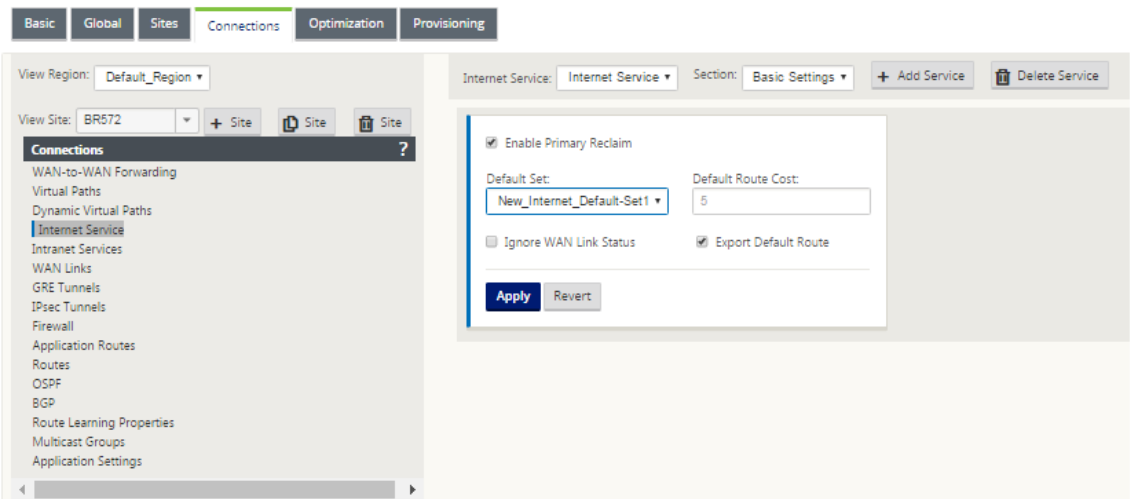
Direct Internet Breakout at Branch with Integrated Firewall



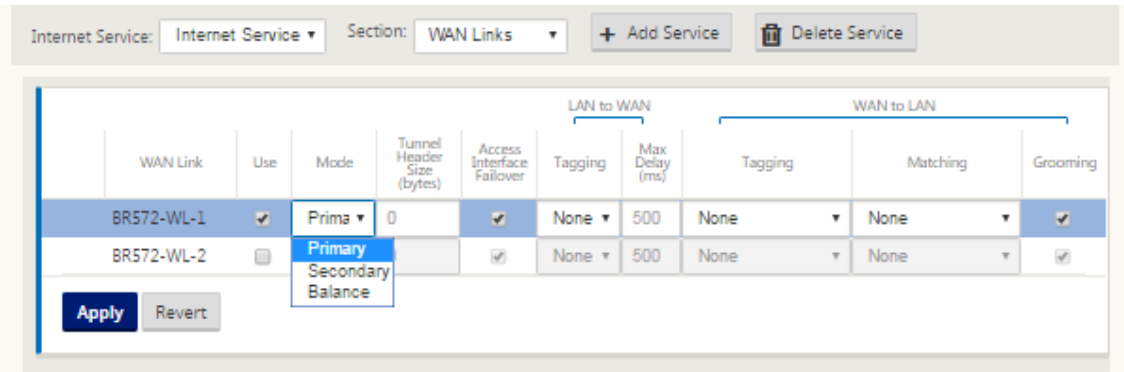
Procédez comme suit pour activer le service Internet pour n'importe quel site (nœud client ou MCN) :

1. Dans l'**Éditeur de configuration**, accédez à la vignette **Connexions**. Cliquez sur l'icône Ajouter (+) pour ajouter un service Internet pour ce site. Un seul service Internet peut être créé par site.
2. Dans les **paramètres de base** du service Internet, il existe plusieurs options sur la façon dont vous souhaitez que le service Internet se comporte en cas d'indisponibilité des liaisons WAN. Un jeu par défaut Internet peut être défini dans la vignette Global avec un jeu de règles qui peut être

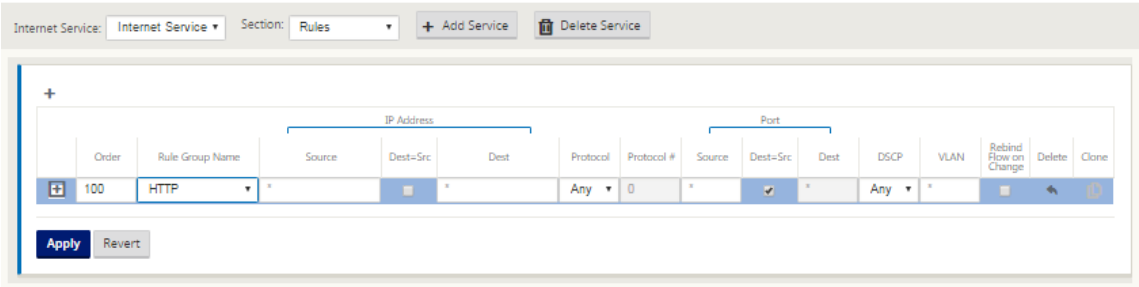
appliqué à n’importe quel nœud de la configuration sur lequel le service Internet est activé, ce qui donne un contrôle central pour la gestion du service Internet sans avoir à configurer chaque nœud séparément.



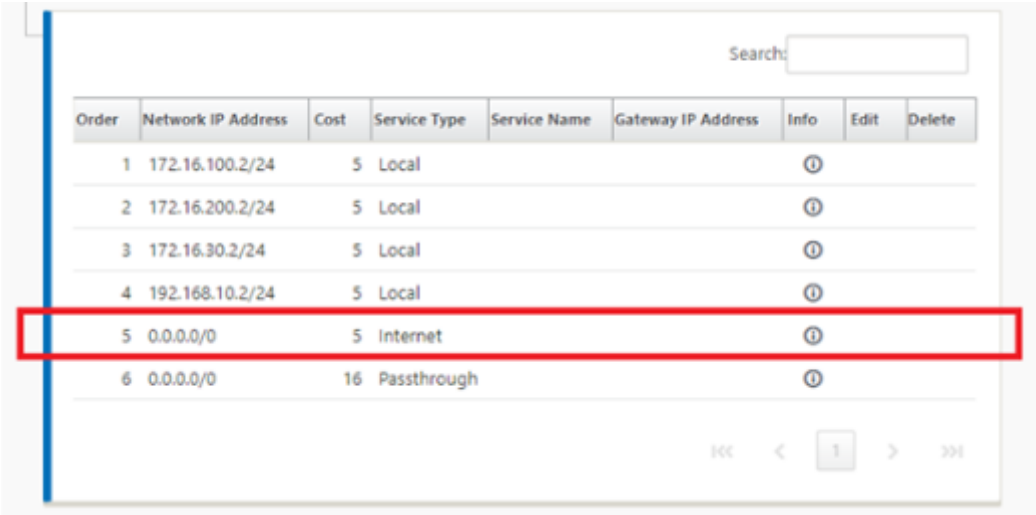
3. Dans le nœud Liens WAN du service Internet, les liens WAN créés dans la vignette Site sont disponibles pour sélectionner la liaison WAN que vous souhaitez utiliser pour le trafic Internet. En plus des autres options, les Modes disponibles sont Primaire, Secondaire et Équilibré, permettant à l’administrateur d’utiliser les liaisons WAN disponibles simultanément ou dans un rôle actif/passif.



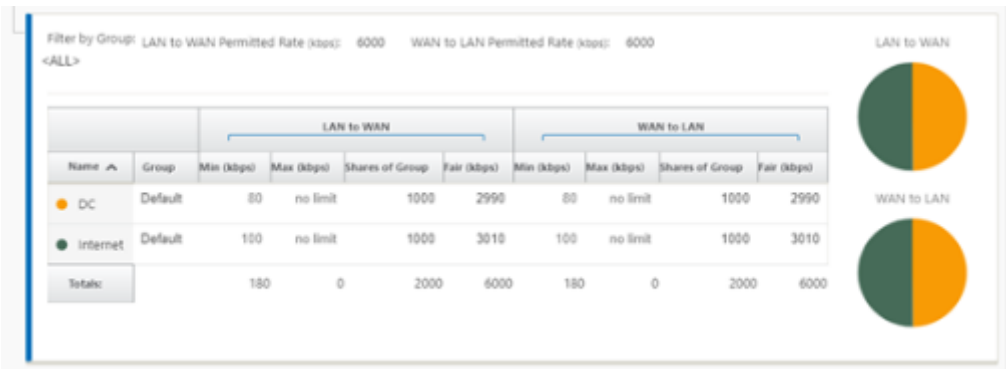
4. Des règles spécifiques aux nœuds de site sont disponibles, ce qui permet de personnaliser chaque site de manière unique en remplaçant tous les paramètres généraux configurés dans le jeu par défaut global. Les modes incluent la livraison souhaitée sur une liaison WAN spécifique ou en tant que service de remplacement permettant de passer ou de rejeter le trafic filtré.



Au fur et à mesure qu'un service Internet est créé pour un nœud, la table Routage pour ce nœud particulier est automatiquement mise à jour avec un itinéraire 0.0.0.0/0 pour le type de service égal à Internet et un coût d'itinéraire de 5, sinon l'itinéraire par défaut avec le coût 16 avec Passthrough comme type de service serait mis en place, et le trafic Internet serait être remis au réseau de sous-couche pour acheminer.



Avec le service Internet activé pour un nœud de site, la vignette Provisioning est disponible pour permettre la distribution bidirectionnelle (LAN vers WAN /WAN vers LAN) de la bande passante pour une liaison WAN entre les différents services utilisant la liaison WAN. La section Services permet aux utilisateurs d'affiner davantage l'allocation de bande passante. En outre, le partage équitable peut être activé, ce qui permet à tous les services de recevoir leur bande passante minimale réservée avant l'adoption d'une distribution équitable.



Le service Internet peut être utilisé dans les différents modes de déploiement pris en charge par Citrix SD-WAN.

- Mode de déploiement en ligne (Superposition SD-WAN)

Citrix SD-WAN peut être déployé en tant que solution de superposition sur n'importe quel réseau. En tant que solution de superposition, le SD-WAN est généralement déployé derrière des routeurs et/ou des pare-feu existants. Si le SD-WAN est déployé derrière un pare-feu réseau, l'interface peut être configurée comme fiable et le trafic Internet peut être distribué au pare-feu en tant que Gateway Internet.

- Mode Edge ou passerelle

Citrix SD-WAN peut être déployé en tant que périphérique périphérique, en remplaçant les routeurs et/ou les périphériques de pare-feu existants. La fonctionnalité de pare-feu intégrée permet au SD-WAN de protéger le réseau contre la connectivité Internet directe. Dans ce mode, l'interface connectée à la liaison Internet publique est configurée comme non fiable, ce qui oblige le chiffrement à être activé, et les fonctionnalités de pare-feu et NAT dynamique sont activées pour sécuriser le réseau.

Accès direct à Internet avec Secure Web Gateway

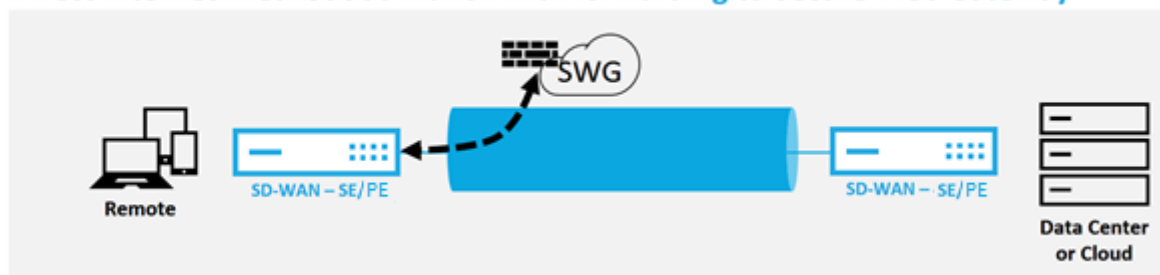
November 1, 2021

Pour sécuriser le trafic et appliquer des stratégies, les entreprises utilisent souvent des liens MPLS pour acheminer le trafic des succursales vers le centre de données de l'entreprise. Le centre de données applique des stratégies de sécurité, filtre le trafic via les appliances de sécurité pour détecter les logiciels malveillants et achemine le trafic via un fournisseur de services Internet. Une telle liaison terrestre sur des liaisons MPLS privées est coûteuse. Cela entraîne également une latence importante, ce qui crée une mauvaise expérience utilisateur sur le site de la succursale. Il existe également un risque que les utilisateurs contournent vos contrôles de sécurité.

Une alternative au réacheminement consiste à ajouter des dispositifs de sécurité à la succursale. Toutefois, le coût et la complexité augmentent à mesure que vous installez plusieurs appliances afin de maintenir des stratégies cohérentes sur l'ensemble des sites. Plus important encore, si vous avez de nombreuses succursales, la gestion des coûts devient impraticable.

Une autre solution consiste à renforcer la sécurité sans augmenter les coûts, la complexité ou la latence, en acheminant tout le trafic Internet des succursales à l'aide de Citrix SD-WAN vers le service Secure Web Gateway. Un service Secure Web Gateway tiers permet la création de stratégies de sécurité granulaires et centralisées que tous les réseaux connectés peuvent utiliser. Les stratégies sont appliquées de manière cohérente, que l'utilisateur se trouve dans le centre de données ou dans un site de succursale. Les solutions Secure Web Gateway étant basées sur le cloud, vous n'avez pas besoin d'ajouter des appliances de sécurité plus coûteuses au réseau.

Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



Citrix SD-WAN prend en charge les solutions Secure Web Gateway tierces suivantes :

- [Zscaler](#)
- [Point de force](#)
- [Palo Alto](#)
- [Citrix Secure Internet Access](#)

Backhauling d'Internet

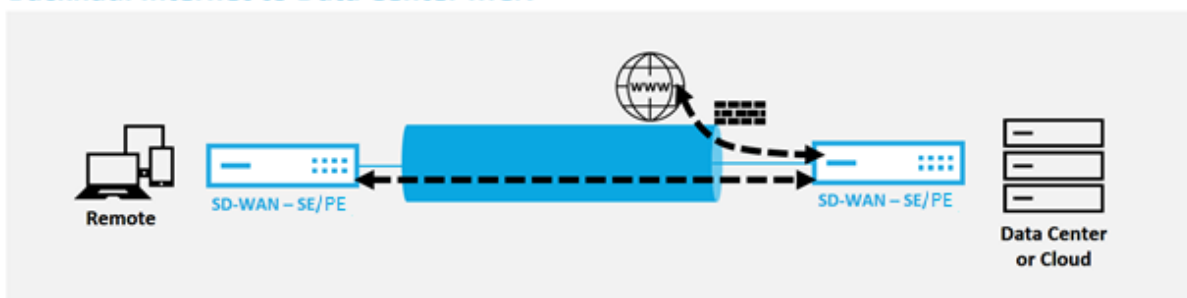
May 6, 2021

La solution Citrix SD-WAN peut rediriger le trafic Internet vers le site MCN ou d'autres sites de succursale. Le backhaul indique que le trafic destiné à Internet est renvoyé par un autre site prédéfini qui peut accéder à Internet. Il est utile pour les réseaux qui n'autorisent pas l'accès à Internet directement en raison de problèmes de sécurité ou de la topologie des réseaux sous-jacents. Par exemple, un site distant ne dispose pas d'un pare-feu externe où le pare-feu SD-WAN intégré ne répond pas aux exigences de sécurité de ce site. Dans certains environnements, la rétroacheminement de tout le trafic Internet des sites distants via la zone démilitarisée du centre de données pourrait être la meilleure approche pour fournir un accès Internet aux utilisateurs des bureaux distants. Toutefois, cette approche

a ses limites à connaître et notamment la taille appropriée des liaisons WAN sous-couche.

- Le backhaul du trafic Internet ajoute une latence à la connectivité Internet et est variable en fonction de la distance du site de la succursale pour le datacenter.
- Le backhaul du trafic Internet consomme de la bande passante sur le chemin virtuel et est pris en compte dans le dimensionnement des liaisons WAN.
- Le backhaul du trafic Internet peut surallouer la liaison WAN Internet au centre de données.

Backhaul Internet to Data Center MCN



Tous les périphériques Citrix SD-WAN peuvent mettre fin à jusqu'à huit liaisons WAN Internet distinctes en un seul appareil. Les capacités de débit sous licence pour les liaisons WAN agrégées sont répertoriées par appliance respective sur la fiche technique Citrix SD-WAN.

La solution Citrix SD-WAN prend en charge le backhaul du trafic Internet avec la configuration suivante.

1. Activez le service Internet sur le nœud de site MCN ou toute autre note de site où le service Internet est souhaité.

Remarque

Activez les itinéraires de service Internet et d'exportation si tous les autres sites font partie du groupe de transfert WAN vers WAN.

2. Sur les nœuds de branche où le trafic Internet est rétroacheminé, ajoutez manuellement une route 0.0.0.0/0 pour diriger tout le trafic par défaut vers le service Virtual Path. Le saut suivant est désigné comme le MCN, ou site intermédiaire.

?

✕

Add Route

Network IP Address

Cost

Service Type

Gateway IP Address

0.0.0.0/0

5

Virtual Path

Next Hop Site:

DC

☐ Eligibility Based On Path

Path:

<None>

Add

Cancel

3. Vérifiez que la table de routage du site de la succursale n’a pas d’autres routes moins coûteuses qui pourraient diriger le trafic autre que la route de retour souhaitée.

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	172.16.100.2/24	5	Local			ⓘ		
2	172.16.30.2/24	5	Local			ⓘ		
3	192.168.10.2/24	5	Local			ⓘ		
4	0.0.0.0/0	5	Virtual Path	DC		ⓘ	✎	✕
5	0.0.0.0/0	16	Passthrough			ⓘ		

100 < 1 > 100

Mode épingle à cheveux

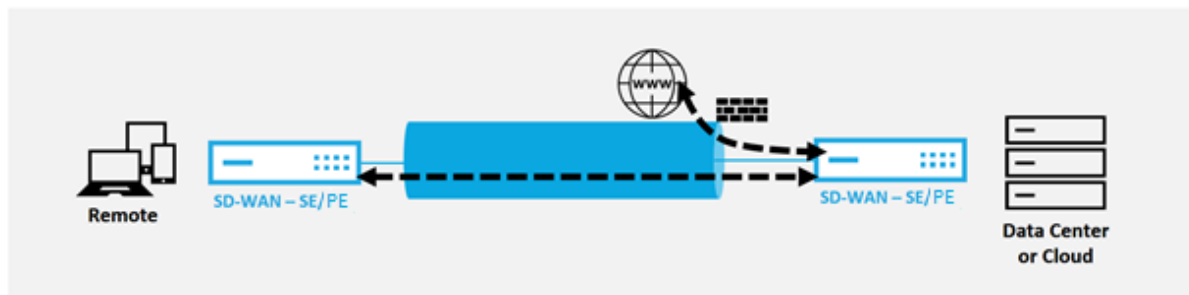
May 6, 2021

Avec le déploiement en épingle à cheveux, vous pouvez implémenter l’utilisation d’un site Hub distant pour l’accès à Internet via le backhaul ou l’épingle à cheveux lorsque les services Internet locaux ne sont pas disponibles ou que le trafic est plus lent. Vous pouvez appliquer un routage à large bande passante entre les sites clients en autorisant le backhauling à partir de sites spécifiques.

Le but d’un déploiement en épingle à cheveux d’un site non-WAN vers un site de transfert WAN est de fournir un processus de déploiement plus efficace et une implémentation technique plus rational-

isée. Vous pouvez utiliser un site concentrateur distant pour accéder à Internet en cas de besoin et acheminer les flux via le chemin virtuel vers le réseau SD-WAN.

Backhaul Internet to Data Center MCN



Par exemple, considérez un administrateur disposant de plusieurs sites SD-WAN A et B. Le site A présente un mauvais service Internet. Le site B dispose d'un service Internet utilisable, avec lequel vous souhaitez rediriger le trafic du site A vers le site B uniquement. Vous pouvez essayer d'y parvenir sans la complexité des coûts d'itinéraire pondérés stratégiquement et de la propagation vers des sites qui ne devraient pas recevoir le trafic.

En outre, la table de routage n'est pas partagée sur tous les sites dans un déploiement en épingle à cheveux. Par exemple, si le trafic est épinglé entre le site A et le site B via le site C, seul le site C est au courant des itinéraires du site A et du site B. Le site A et le site B ne partagent pas la table de routage de l'autre contrairement au transfert WAN à WAN.

Lorsque le trafic est en épingle à cheveux entre le site A et le site B via le site C, les routes statiques doivent être ajoutées dans le site A et le site B indiquant que le prochain saut pour les deux sites est le site C.

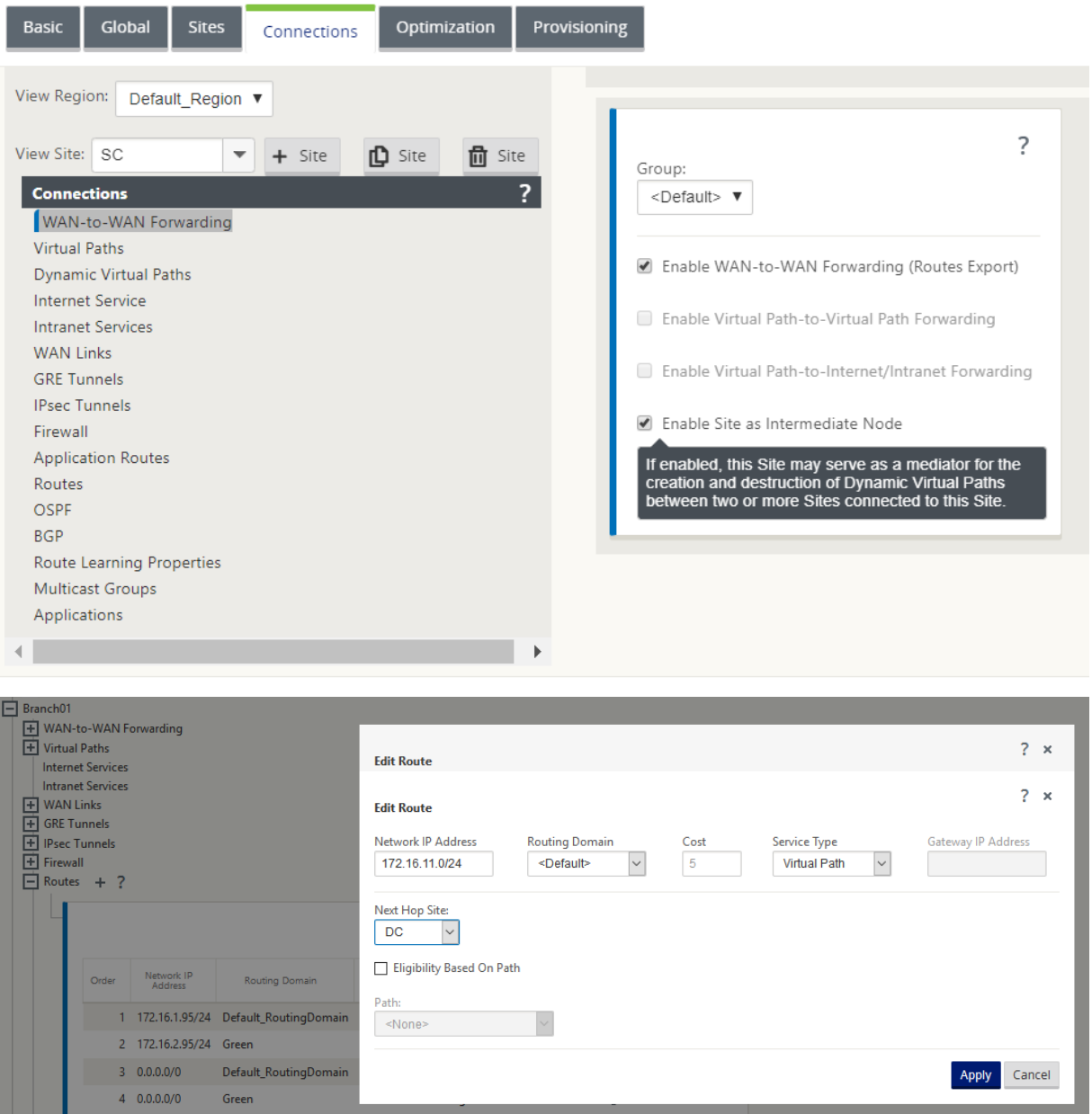
Le transfert WAN-to-WAN et le déploiement Hairpin présentent certaines différences, à savoir :

1. Les chemins virtuels dynamiques ne sont pas configurés. Toujours, le site intermédiaire voit tout le trafic entre les deux sites.
2. Ne participe pas aux groupes Wan to WAN Forwarding.

Le transfert Wan to WAN et le déploiement Hairpin s'excluent mutuellement. Un seul d'entre eux peut être configuré à un moment donné dans le temps.

Les appliances Citrix SD-WAN SE/PE et VPX (virtuelles) prennent en charge le déploiement en épingle à cheveux. Vous pouvez maintenant configurer un itinéraire 0.0.0.0/0 vers le trafic en épingle à cheveux entre deux emplacements sans affecter d'emplacements supplémentaires. Si l'épinglage est utilisé pour le trafic intranet, des itinéraires Intranet spécifiques sont ajoutés au site client pour transférer le trafic intranet via le chemin virtuel vers le site épingle à cheveux. Il n'est plus nécessaire d'activer le transfert WAN vers WAN pour accomplir la fonctionnalité d'épingle à cheveux.

Vous pouvez configurer le déploiement en épingle à cheveux via l’interface de gestion Web Citrix SD-WAN à partir de l’éditeur de configuration.



Pare-feu hébergés

May 6, 2021

Actuellement, Citrix SD-WAN prend en charge les pare-feu hébergés suivants :

- Réseaux Palo Alto

- [Check Point](#)

Intégration du pare-feu Palo Alto Networks sur la plate-forme SD-WAN 1100

May 6, 2021

Citrix SD-WAN prend en charge l'hébergement du pare-feu Palo Alto Networks Next Generation Virtual Machine (VM) -Series sur la plate-forme SD-WAN 1100. Les modèles de machines virtuelles pris en charge sont les suivants :

- VM 50
- VM 100

Le pare-feu de la série de machines virtuelles Palo Alto Network s'exécute comme une machine virtuelle sur la plate-forme SD-WAN 1100. La machine virtuelle pare-feu est intégrée en mode **Virtual Wire** avec deux interfaces virtuelles de données qui lui sont connectées. Le trafic requis peut être redirigé vers la machine virtuelle du pare-feu en configurant des stratégies sur SD-WAN.

Avantages

Voici les principaux objectifs ou avantages de l'intégration de Palo Alto Networks sur la plateforme SD-WAN 1100 :

- Consolidation des périphériques de succursale : une appliance unique qui effectue à la fois le SD-WAN et la sécurité avancée
- Sécurité des succursales avec pare-feu NGFW sur site (Next Generation Firewall) pour protéger le trafic LAN à LAN, LAN à Internet et Internet-to-LAN

Étapes de configuration

Les configurations suivantes sont nécessaires pour intégrer la machine virtuelle Palo Alto Networks sur SD-WAN :

- Provisionner la machine virtuelle du pare-feu
- Activer la redirection du trafic vers la machine virtuelle de sécurité

Remarque La

machine virtuelle Pare-feu doit d'abord être provisionnée avant d'activer la redirection du trafic.

Provisionnement de la machine virtuelle du réseau Palo Alto

Il existe deux façons de provisionner la machine virtuelle du pare-feu :

- Provisionnement via SD-WAN Center
- Provisionnement via l'interface graphique de l'appliance SD-WAN

Provisioning de machines virtuelles par le biais de SD-WAN Center

Conditions préalables

- Ajoutez le stockage secondaire à SD-WAN Center pour stocker les fichiers image de la machine virtuelle du pare-feu. Pour plus d'informations, reportez-vous à la section [Configuration système requise et installation](#).
- Réservez le stockage à partir de la partition secondaire pour les fichiers image de la machine virtuelle du pare-feu. Pour configurer la limite de stockage, accédez à **Administration > Maintenance du stockage**.
 - Sélectionnez la quantité de stockage requise dans la liste.
 - Cliquez sur **Appliquer**.

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Nitro API

User/Authentication Settings

Global Settings

Database Maintenance

Storage Maintenance

Diagnostics

Administration / Storage Maintenance

Region: Default_Region

Storage Systems

Host	File System	Type	Size (MB)	Available (MB)	Active	Migrate Data
Local*	/dev/xvda2	ext3	7288	3471		
Local	/dev/xvdb	ext3	14910	12921		

Apply

Note: Software image storage reserved will be reduced while calculating the secondary partition Size(MB) and Available(MB)

Software Image Storage Reservation

Note: User can modify the storage reservation only if the SD-WAN Center has secondary partition mounted and it should operate in headend mode

Amount of storage to reserve from secondary partition storage(Active) is 10GB

Apply

Thresholds

SD-WAN Center Database Storage and Auto Cleanup settings are misconfigured, SD-WAN Center will reach auto cleanup threshold before the configured 6 months.

Stop stats polling when storage usage exceeds 55% of active storage size

☐ Notify user when storage usage exceeds 10% of active storage size

Apply

Remarque

Le stockage est réservé à partir de la partition secondaire qui est active si la condition est remplie.

Procédez comme suit pour Provisioning la machine virtuelle de pare-feu via la plate-forme SD-WAN Center :

1. Dans l’interface graphique Citrix SD-WAN Center, accédez à **Configuration** > sélectionnez **Pare-feu hébergé** .

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Nitro API

Network Discovery

Network Configuration

Zero Touch Deployment

Change Management

Appliance Settings

Mobile Broadband

Licensing

Hosted Firewall

Cloud Connectivity

Security

Configuration / Hosted Firewall

Hosted Firewall Sites

Software Images

Provision

Start

Shutdown

Deprovision

Refresh

Select Region: Default_Region

<input type="checkbox"/>	SITE NAME	MGT IP ADDRESS	REGION NAME	VENDOR	MODEL	ADMIN STATE	OPERATION STATUS	HOSTED SITE

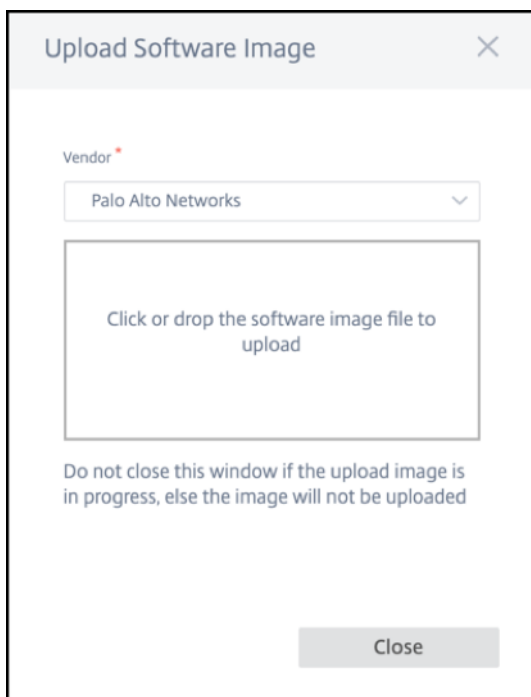
Vous pouvez sélectionner la **Région** dans la liste déroulante pour afficher les détails du site provisionné pour cette région sélectionnée.

2. Téléchargez l’image du logiciel.

Remarque

Assurez-vous que vous disposez de suffisamment d'espace disque pour télécharger l'image logicielle.

Accédez à **Configuration > Pare-feu hébergé > Images logicielles** et sélectionnez le nom du fournisseur Palo Alto Networks dans la liste déroulante. Cliquez ou déposez le fichier image du logiciel dans la zone à télécharger.



Une barre d'état apparaît avec le processus de téléchargement en cours. Ne cliquez pas sur **Actualiser** ou n'effectuez aucune autre action jusqu'à ce que le fichier image affiche 100 % téléchargé.

- **Actualiser** : cliquez sur l'option **Actualiser** pour obtenir les derniers détails du fichier image.
- **Supprimer** : cliquez sur l'option **Supprimer** pour supprimer tout fichier image existant.

Remarque

- Pour provisionner la machine virtuelle de pare-feu sur la partie sites d'une région autre que par défaut, téléchargez le fichier image sur chacun du nœud collecteur.
- La suppression de l'image de machine virtuelle Palo Alto de SDWAN Center supprime l'image du stockage SDWAN Center, et PAS de l'appliance.

3. Pour le provisioning, revenez à l'onglet **Sites de pare-feu hébergés** et cliquez sur **Provisioning**.

Provision Virtual Machine
✕

Vendor *

Palo Alto Networks

Vendor Virtual Machine Model *

VM50

Software Image *

PA-VM-KVM-9.0.1.qcow2

Please ensure to upload this image in the collector, for non-default region sites provisioning

Region *

Region1

Sites for Firewall Hosting *

DC () ✕

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Management Server Secondary IP Address/Domain Name

Enter Management Server Secondary IP Address or domain name

Virtual Machine Authentication Key

Enter the virtual authentication key to be used in the Management server

Authentication Code

Enter the authentication code to be used for licensing

Start Provision

Cancel

- **Fournisseur** : sélectionnez le nom **du fournisseur** en tant que **Palo Alto Networks** dans la liste déroulante.
- **Modèle de machine virtuelle fournisseur** : sélectionnez le numéro de modèle de machine virtuelle dans la liste.
- **Image logicielle** : sélectionnez le fichier Image à provisionner.
- **Région** : Sélectionnez la région dans la liste.
- **Sites pour l'hébergement de pare-feu** : sélectionnez des sites pour la liste d'héberge-

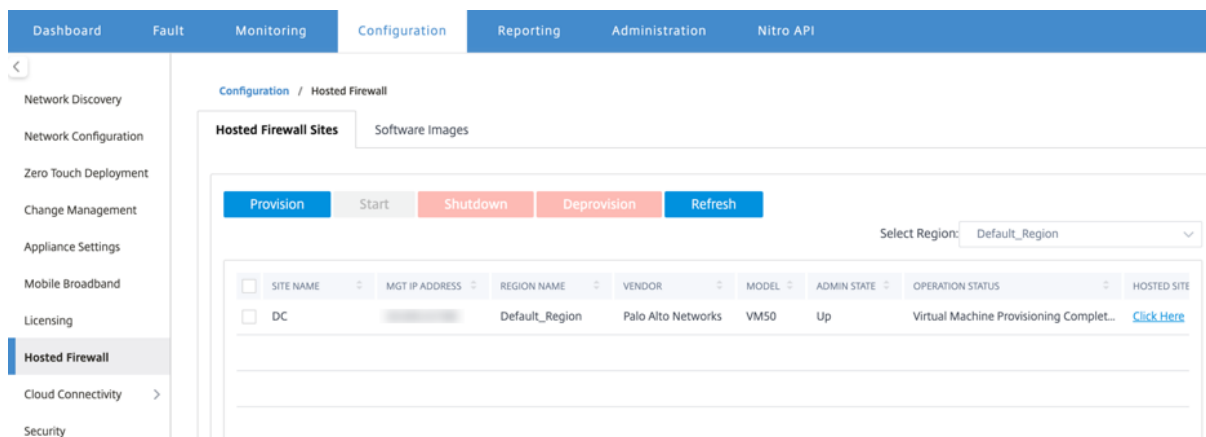
ment de pare-feu. Vous devez sélectionner les sites principaux et secondaires si les sites sont en mode haute disponibilité.

- **Adresse IP principale/Nom de domaine du serveur Management Server** : entrez l'adresse IP principale de gestion ou le nom de domaine complet (facultatif).
- **Adresse IP secondaire du serveur de gestion** : entrez l'adresse IP secondaire du serveur de gestion ou le nom de domaine complet (facultatif).
- **Clé d'authentification de machine virtuelle** : entrez la clé d'authentification virtuelle à utiliser dans le serveur de gestion.
- **Code d'authentification** : Entrez le code d'authentification virtuel à utiliser pour les licences.

4. Cliquez sur **Démarrer la mise en service**.

5. Cliquez sur **Actualiser** pour obtenir le dernier état. Une fois la machine virtuelle Palo Alto Networks démarre complètement, elle se penchera sur l'interface utilisateur SD-WAN Center.

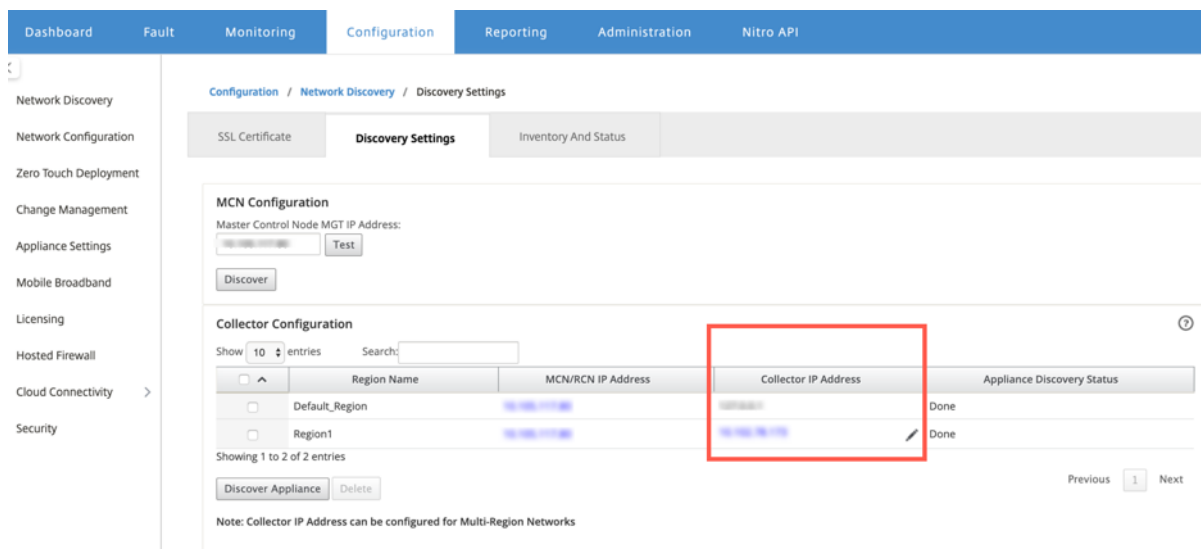
Vous pouvez **démarrer, arrêter et désapprovisionner** la machine virtuelle si nécessaire.



- **Nom du site** : affiche le nom du site.
- **IP de gestion** : affiche l'adresse IP de gestion du site.
- **Nom de la région** : affiche le nom de la région.
- **Vendeur** : Affiche le nom du fournisseur (Palo Alto Networks).
- **Modèle** : affiche le numéro de modèle (VM50/VM100).
- **État d'administration** : état de la machine virtuelle du fournisseur (haut/bas).
- **Statut de l'opération** : affiche le message d'état opérationnel.
- **Site hébergé** : Utilisez le lien **Cliquez ici** pour accéder à l'interface graphique de la machine virtuelle Palo Alto Networks.

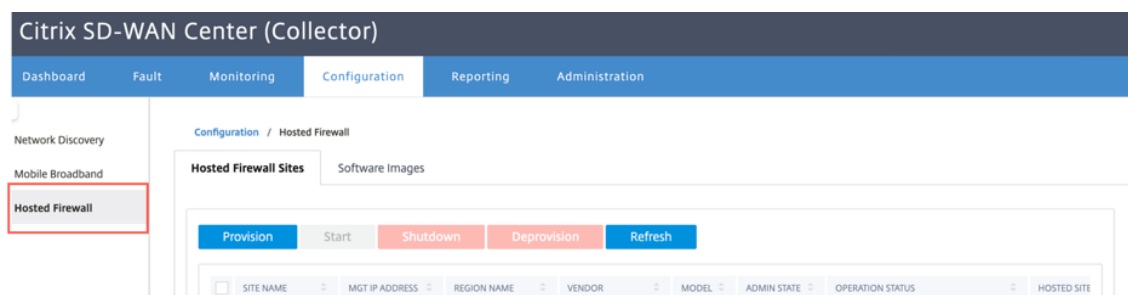
Pour provisionner les sites de région autres que ceux par défaut, vous devez télécharger l'image logicielle sur le collecteur SD-WAN Center. Vous pouvez provisionner les réseaux Palo Alto à la fois depuis l'interface graphique de tête de ligne SD-WAN Center ou SD-WAN Center Collector.

Pour obtenir l'adresse IP du collecteur SD-WAN Center, accédez à **Configuration > Découverte réseau** > sélectionnez l'onglet **Paramètres de découverte**.



Pour provisionner les réseaux Palo Alto de SD-WAN Collector :

1. Dans l'interface graphique SD-WAN Collector, accédez à **Configuration > Pare-feu hébergé**.



2. Accédez à l'onglet **Images logicielles** pour télécharger l'image logicielle.
3. Cliquez sur **Provisionner** sous l'onglet **Sites pare-feu hébergés**
4. Fournissez les détails suivants et cliquez sur **Démarrer le provisionnement**.

Vendor *

Palo Alto Networks

Vendor Virtual Machine Model *

VM50

Software Image *

PA-VM-KVM-8.1.3.qcow2

Please ensure to upload this image in the collector, for non-default region sites provisioning

Sites for Firewall Hosting *

BRANCH-PA (10.10.10.10) X

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Management Server Secondary IP Address/Domain Name

Enter Management Server Secondary IP Address or domain name

Virtual Machine Authentication Key

Enter the virtual authentication key to be used in the Management server

Authentication Code

Enter the authentication code to be used for licensing

Start Provision Cancel

- **Fournisseur** : sélectionnez le nom **du fournisseur** en tant que **Palo Alto Networks** dans la liste déroulante.
- **Modèle de machine virtuelle fournisseur** : sélectionnez le numéro de modèle de machine virtuelle dans la liste.
- **Image logicielle** : sélectionnez le fichier Image à provisionner.
- **Région** : Sélectionnez la région dans la liste.
- **Sites pour l'hébergement de pare-feu** : sélectionnez des sites pour la liste d'hébergement de pare-feu. Vous devez sélectionner les sites principaux et secondaires si les sites sont en mode haute disponibilité.
- **Adresse IP principale/Nom de domaine du serveur Management Server** : entrez l'adresse IP principale de gestion ou le nom de domaine complet (facultatif).
- **Adresse IP secondaire du serveur de gestion** : entrez l'adresse IP secondaire du serveur

de gestion ou le nom de domaine complet (facultatif).

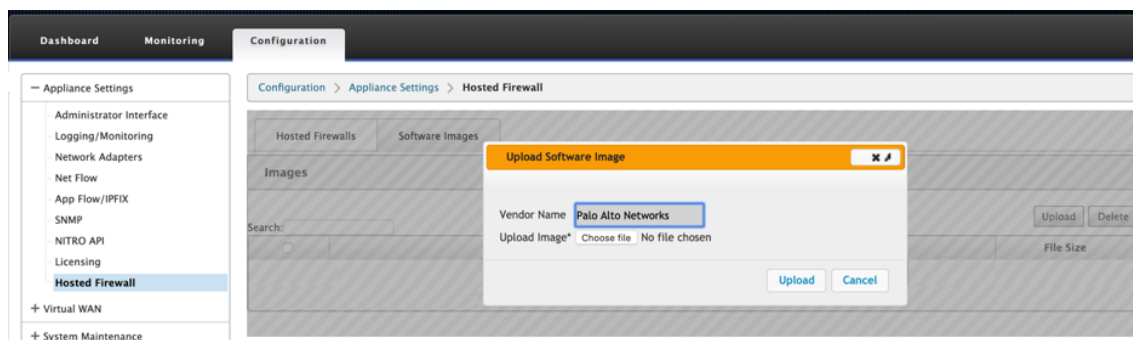
- **Clé d'authentification de machine virtuelle** : entrez la clé d'authentification virtuelle à utiliser dans le serveur de gestion.
- **Code d'authentification** : Entrez le code d'authentification virtuel à utiliser pour les licences.

5. Cliquez sur **Démarrer la mise en service**.

Provisioning de machines virtuelles par pare-feu via l'interface graphique du dispositif SD-WAN

Sur la plate-forme SD-WAN, provisionnez et démarrez la machine virtuelle hébergée. Effectuez les étapes suivantes pour le Provisioning :

1. Dans l'interface graphique Citrix SD-WAN, accédez à **Configuration** > Développez **Paramètres de l'appliance** > sélectionnez **Pare-feu hébergé**.
2. Téléchargez l'image du logiciel :
 - Sélectionnez l'onglet **Images logicielles**. Sélectionnez le nom du fournisseur en tant que **Palo Alto Networks**.
 - Choisissez le fichier image du logiciel.
 - Cliquez sur **Upload**.

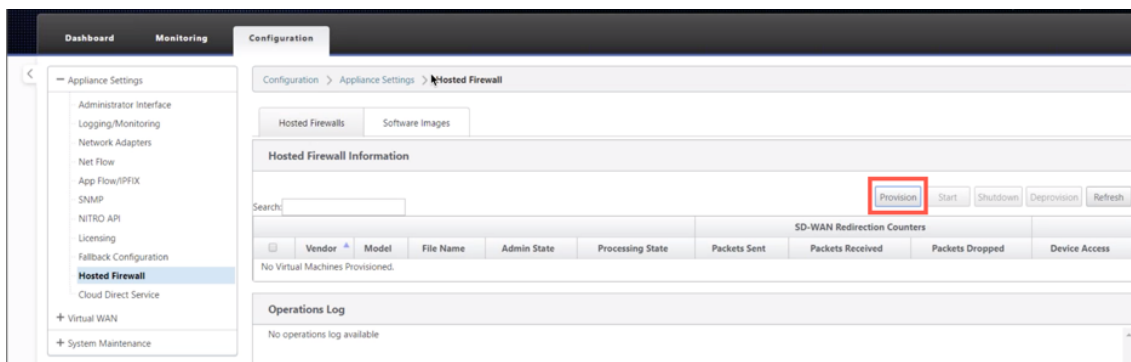


Remarque

Un maximum de deux images logicielles peut être téléchargé. Le téléchargement de l'image de la machine virtuelle Palo Alto Networks peut prendre plus de temps en fonction de la disponibilité de la bande passante.

Vous pouvez voir une barre d'état pour suivre le processus de téléchargement. Le détail du fichier reflète, une fois l'image téléchargée avec succès. L'image utilisée pour le Provisioning ne peut pas être supprimée. N'effectuez aucune action ou revenez à une autre page jusqu'à ce que le fichier image affiche 100% téléchargée.

3. Pour le provisioning, sélectionnez l'onglet **Pare-feu hébergés** et cliquez sur le bouton **Provisioning**.

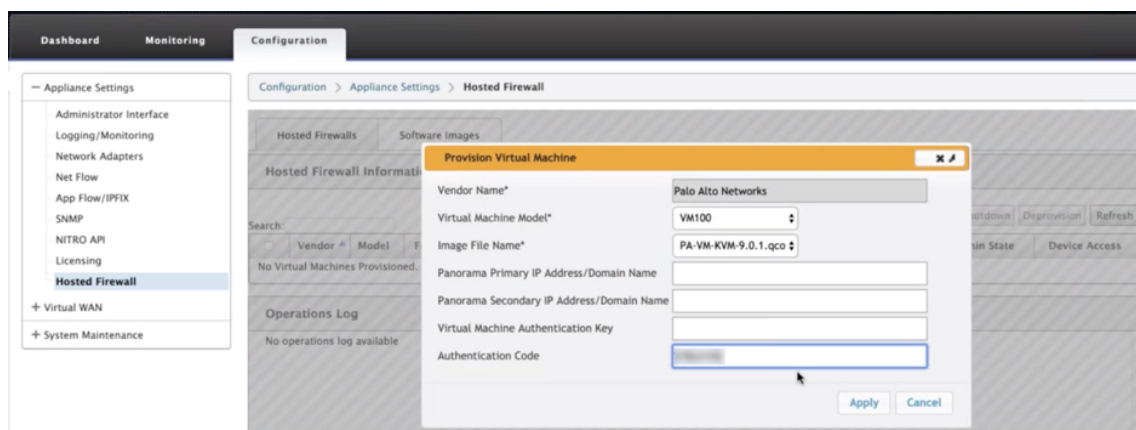


4. Fournissez les détails suivants pour le Provisioning.

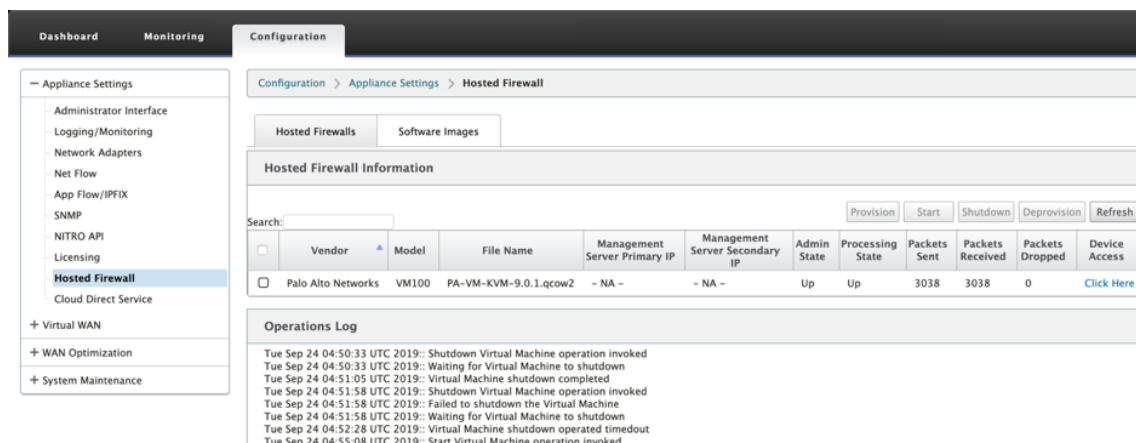
- **Nom du fournisseur** : sélectionnez le fournisseur comme **Palo Alto Networks**.
- **Modèle de machine virtuelle** : sélectionnez le numéro de modèle de machine virtuelle dans la liste.
- **Nom du fichier image** : Sélectionnez le fichier image.
- **Adresse IP principale/Nom de domaine Panorama** : Indiquez l'adresse IP principale Panorama ou le nom de domaine complet (Facultatif).
- **Adresse IP secondaire Panorama** : Indiquez l'adresse IP secondaire Panorama ou le nom de domaine complet (facultatif).
- **Clé d'authentification de la machine virtuelle** : fournissez la clé d'authentification de la machine virtuelle (facultatif).

La clé d'authentification de machine virtuelle est nécessaire pour l'enregistrement automatique de la machine virtuelle Palo Alto Networks sur le Panorama.

- **Code d'authentification** : Entrez le code d'authentification (code de licence de machine virtuelle) (facultatif).
- Cliquez sur **Appliquer**.



5. Cliquez sur **Actualiser** pour obtenir le dernier état. Une fois la machine virtuelle Palo Alto Networks démarre complètement, elle réfléchira sur l'interface utilisateur SD-WAN avec le détail du journal des opérations.



- **État d'administration** : indique si la machine virtuelle est en service ou en panne.
- **État de traitement** : état de traitement du datapath de la machine virtuelle.
- **Paquet envoyé** : Paquets envoyés depuis SD-WAN vers la machine virtuelle de sécurité.
- **Paquet reçu** : Paquets reçus par SD-WAN de la machine virtuelle de sécurité.
- **Paquet abandonné** : Paquets abandonnés par SD-WAN (par exemple, lorsque la machine virtuelle de sécurité est en panne).
- **Accès au périphérique** : cliquez sur le lien pour obtenir l'accès GUI à la machine virtuelle de sécurité.

Vous pouvez **démarrer**, **arrêter** et **désapprovisionner** la machine virtuelle si nécessaire. Utilisez l'option **Cliquez ici** pour accéder à l'interface graphique de la machine virtuelle Palo Alto Networks ou utilisez votre adresse IP de gestion avec le port 4100 (adresse IP de gestion : 4100).

Remarque

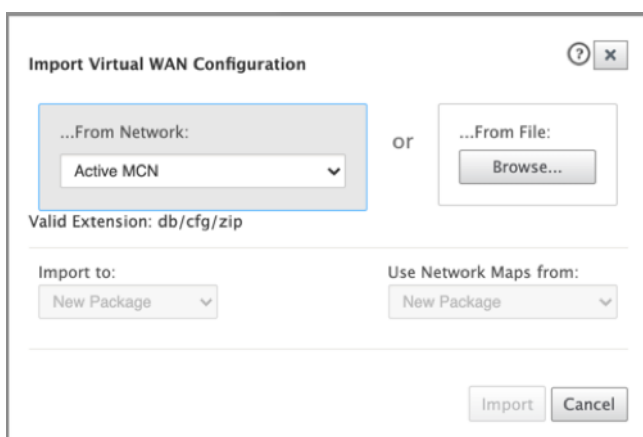
Utilisez toujours le mode navigation privée pour accéder à l'interface graphique de Palo Alto Networks.

Redirection du trafic

La configuration de la redirection du trafic peut être effectuée à la fois via l'Éditeur de configuration sur MCN ou l'Éditeur de configuration sur SD-WAN Center.

Pour naviguer dans l'Éditeur de configuration sur SD-WAN Center :

1. Ouvrez l'interface utilisateur du centre Citrix SD-WAN, accédez à **Configuration > Importation de configuration réseau**. Importez la configuration WAN virtuel à partir du MCN actif et cliquez sur **Importer**.



Les étapes restantes sont similaires comme suit : la configuration de redirection du trafic via MCN.

Pour naviguer dans l'Éditeur de configuration sur MCN :

1. Définissez le **type de correspondance de connexion** sur **Symétrique** sous **Global > Paramètres réseau**.

The screenshot displays the Citrix SD-WAN configuration interface. On the left is a navigation pane under the 'Global' tab, listing various settings categories. The main panel is divided into two sections: 'Global Security Settings' and 'Global Firewall Settings'.

Global Security Settings:

- Note:** Changing the Network Encryption Mode may cause Site Secure Keys to be truncated or regenerated if they do not meet the requirements of the new mode.
- Network Encryption Mode:** AES 128-Bit
- ☒ Enable Encryption Key Rotation
- ☐ Enable Extended Packet Encryption Header
- ☐ Enable Extended Packet Authentication Trailer
- Extended Packet Authentication Trailer Type:** 32-Bit Checksum
- ☐ Enable FIPS Mode
- ☐ Enable Appliance Authentication
- Network Secure Key:** 72d050ce5ca54c... Regenerate

Global Firewall Settings:

- Global Policy Template:** New_Firewall_...
- Default Firewall Action:** Allow
- ☒ Default Connection State Tracking
- Connection Match Type:** Symmetric (highlighted with a red box)
- Denied Timeout (s):** 30
- TCP Initial Timeout (s):** 120
- TCP Idle Timeout (s):** 7440
- TCP Closing Timeout (s):** 60
- TCP Time Wait Timeout (s):** 120
- TCP Closed Timeout (s):** 10
- UDP Initial Timeout (s):** 30
- UDP Idle Timeout (s):** 300
- ICMP Initial Timeout (s):** 30
- ICMP Idle Timeout (s):** 60
- Generic Initial Timeout (s):** 30
- Generic Idle Timeout (s):** 300

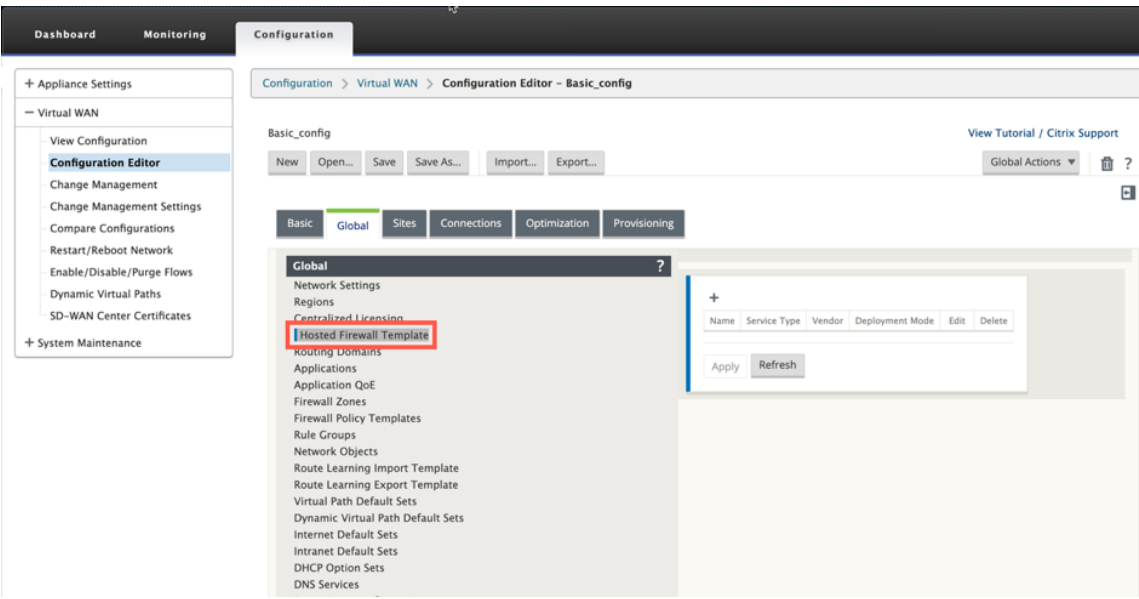
Global On-Demand Bandwidth Limit Setting:

- Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%): 120

At the bottom, there are 'Apply' and 'Revert' buttons.

Par défaut, les stratégies de pare-feu SD-WAN sont spécifiques à la direction. Le type de correspondance symétrique correspond aux connexions à l'aide de critères de correspondance spécifiés et applique une action de stratégie dans les deux directions.

- Ouvrez l'**interface utilisateur Citrix SD-WAN**, accédez à **Configuration** développez **Virtual WAN** sélectionnez **Éditeur de configuration** > sélectionnez **Modèle de pare-feu hébergé** sous la section **Global**.



3. Cliquez sur + et fournissez les informations requises disponibles dans la capture d’écran suivante pour ajouter le modèle de **pare-feu hébergé** et cliquez sur **Ajouter**.

Édit

Name:

PaloAlto-NGFW

Model:

VM50

Primary Management Server IP/FQDN:

Vendor

Palo Alto Networks

Deployment Mode:

Virtual Wire

Secondary Management Server IP/FQDN:

Service Redirection Interfaces

Name	Input Interface	Output Interface	VLAN ID	Delete
INTERNET-OUT	Interface-1	Interface-2	0	
INTERNET-IN	Interface-2	Interface-1	0	

Apply

Cancel

Le **modèle de pare-feu hébergé** vous permet de configurer la redirection du trafic vers la **machine virtuelle Pare-feu** hébergée sur l’appliance SD-WAN. Voici les entrées nécessaires à la configuration du modèle :

- **Nom** : Nom du modèle de pare-feu hébergé.
- **Fournisseur** : nom du fournisseur du pare-feu.
- **Mode de déploiement** : le champ **Mode de déploiement** est automatiquement renseigné et grisé. Pour le fournisseur **Palo Alto Networks**, le mode de déploiement est **Virtual Wire**.

- **Modèle :** **Modèle** de machine virtuelle du pare-feu hébergé. Vous pouvez sélectionner le numéro de modèle de la machine virtuelle en tant que VM 50/VM 100 pour le fournisseur Palo Alto Networks.
- **Serveur d'administration principal IP/FQDN :** **nom** de domaine de domaine complet du serveur d'administration principal de Panorama.
- **Serveur d'administration secondaire IP/FQDN :** Serveur d'administration secondaire IP/FQDN de Panorama.
- **Interfaces de redirection de service :** **Interfaces** logiques utilisées pour la redirection du trafic entre le SD-WAN et le pare-feu hébergé.

Interface-1, Interface-2 fait référence aux deux premières interfaces du pare-feu hébergé. Si des VLAN sont utilisés pour la redirection du trafic, les mêmes VLAN doivent être configurés sur le pare-feu hébergé. Les VLAN configurés pour la redirection du trafic sont internes au SD-WAN et au pare-feu hébergé.

Remarque

L'interface d'entrée de

redirection doit être sélectionnée à partir de la direction de l'initiateur de connexion, l'interface de redirection est automatiquement choisie pour le trafic de réponse. Par exemple, si le trafic Internet sortant est redirigé vers le pare-feu hébergé sur Interface-1, le trafic de réponse est automatiquement redirigé vers le pare-feu hébergé sur Interface-2. Il n'y a pas besoin d'Interface-2 dans l'exemple ci-dessus, s'il n'y a pas de trafic entrant Internet.

Seules deux interfaces physiques sont affectées pour héberger le pare-feu Palo Alto Networks. Si le trafic provenant de plusieurs zones doit être redirigé vers le pare-feu hébergé, plusieurs sous-interfaces peuvent être créées à l'aide de VLAN internes et associées à différentes zones de pare-feu sur le pare-feu hébergé.

Grâce aux stratégies de pare-feu SD-WAN ou au niveau du site, vous pouvez rediriger tout le trafic vers la machine virtuelle Palo Alto Networks.

Remarque

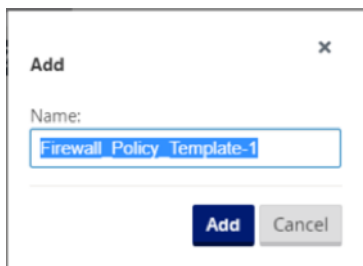
Les stratégies de pare-feu

SD-WAN sont créées automatiquement pour **autoriser** le trafic vers/depuis les serveurs de gestion de pare-feu hébergés. Cela évite la redirection du trafic de gestion qui provient (ou) du pare-feu hébergé.

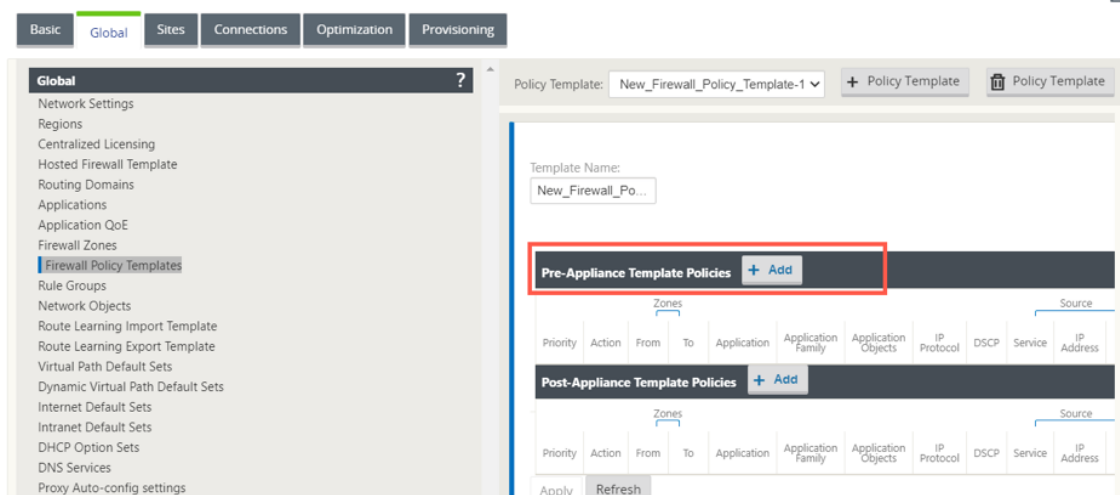
La redirection du trafic vers la machine virtuelle du pare-feu peut être effectuée à l'aide des stratégies de pare-feu SD-WAN. Il existe deux méthodes pour créer des stratégies de pare-feu SD-WAN - soit par le biais de modèles de stratégie de pare-feu dans la section **Global** ou au niveau du site.

Méthode - 1

1. Depuis l'interface graphique Citrix SD-WAN, accédez à **Configuration** développez **Réseau étendu virtuel > Éditeur de configuration**. Accédez à l'onglet **Global** et sélectionnez **Modèles de stratégie de pare-feu**. Cliquez sur **+ Modèle de stratégie**. Indiquez un nom au modèle de stratégie et cliquez sur **Ajouter**.



2. Cliquez sur **+ Ajouter** en regard de **Stratégies de modèle de pré-appliance**.



3. Modifiez le **type de stratégie** par **Pare-feu hébergé**. Le champ **Action** est automatiquement rempli sur **Redirection**. Sélectionnez le **modèle de pare-feu hébergé** et l'**interface de redirection de service** dans la liste déroulante. Remplissez les autres critères de correspondance selon les besoins.

Priority: Policy Type: **Hosted Firewall** ▼

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: **IP Protocol** ▼ IP Protocol: **Any** ▼ DSCP: **Any** ▼ ☐ Match Established

Application Objects: **Any** ▼

Source Service Type: **Any** ▼ Source Service Name: **Any** ▼ Source IP: Source Port:

Dest Service Type: **Any** ▼ Dest Service Name: **Any** ▼ Dest IP: Dest Port:

Actions

Action: **Redirect** ▼ ☒ Allow Fragments Connection State Tracking: **No Tracking** ▼

Hosted Firewall Template: **PaloAlto-NGFW** ▼ Service Redirection Interface: **INTERNET-OUT** ▼

4. Accédez à **Connexions > Pare-feu**, puis sélectionnez la stratégie de pare-feu (que vous avez créée) dans le champ Nom. Cliquez sur **Appliquer**.

Basic Global Sites **Connections** Optimization Provisioning

Region: **Default_Region** ▼

Site: **BR1100** ▼ **+ Site** **Site** **Site**

Connections ?

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall**
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups

Section: **Settings** ▼

Policy Templates + ?

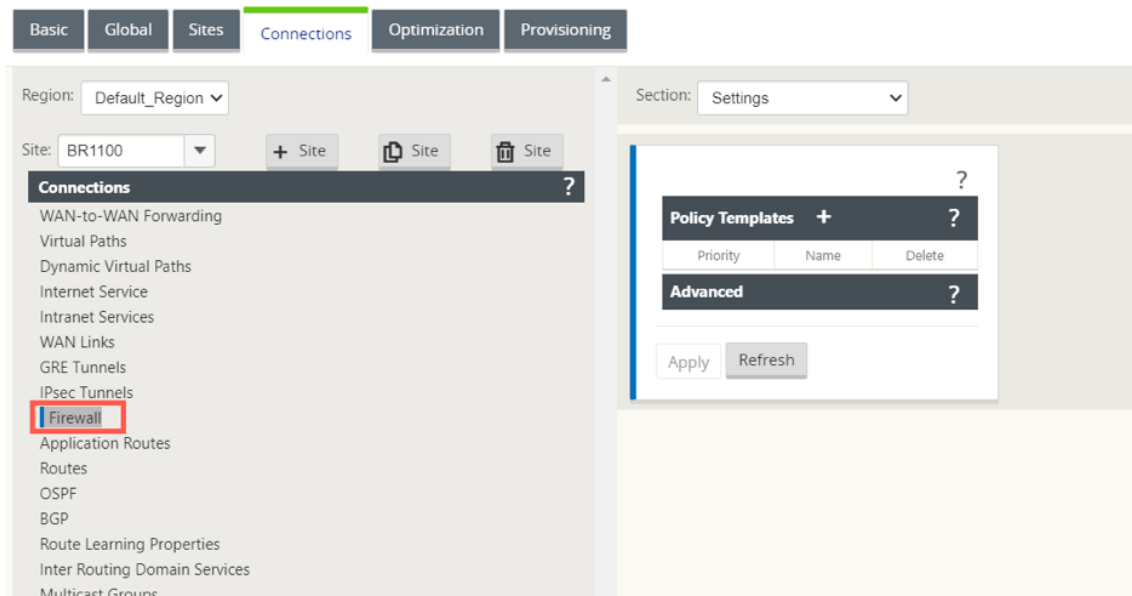
Priority	Name	Delete
100	New_Firewall_P... ▼	

Advanced ?

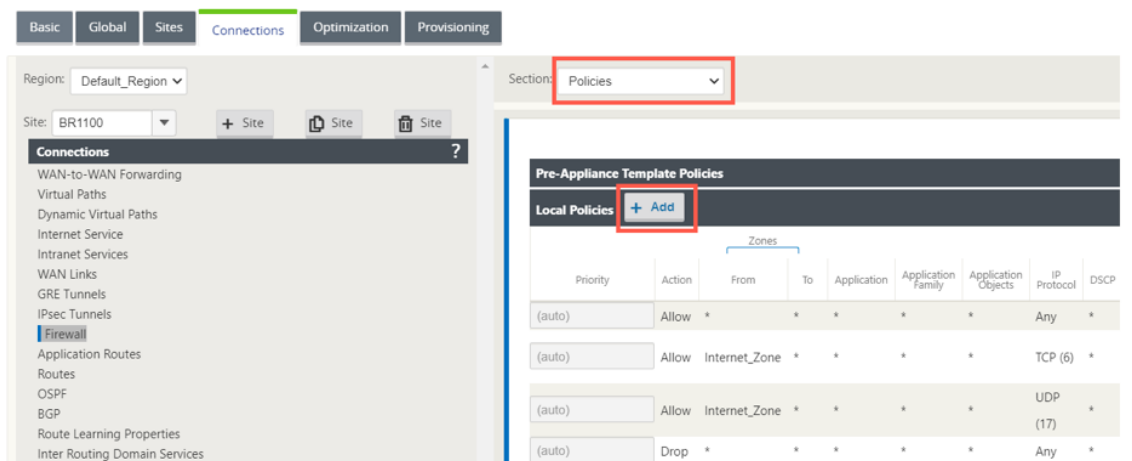
Apply **Revert**

Méthode - 2

1. Pour rediriger tout le trafic, sous l'**Éditeur de configuration > Réseau étendu virtuel**, accédez à l'onglet **Connexion** et sélectionnez **Pare-feu**.



2. Sélectionnez **Stratégies** dans la liste déroulante **Section** et cliquez sur **+Ajouter** pour créer une stratégie de pare-feu.



3. Modifiez le **type de stratégie** par **Pare-feu hébergé**. Le champ **Action** est automatiquement rempli sur Redirection. Sélectionnez le **modèle de pare-feu hébergé** et l'**interface de redirection de service** dans la liste déroulante. Cliquez sur **Ajouter**.

Priority: Policy Type: **Hosted Firewall** ▼

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: **IP Protocol** ▼ IP Protocol: **Any** ▼ DSCP: **Any** ▼ ☐ Match Established

Application Objects: **Any** ▼

Source Service Type: **Any** ▼ Source Service Name: **Any** ▼ Source IP: Source Port:

Dest Service Type: **Any** ▼ Dest Service Name: **Any** ▼ Dest IP: Dest Port:

Actions

Action: **Redirect** ▼ ☒ Allow Fragments Connection State Tracking: **No Tracking** ▼

Hosted Firewall Template: **PaloAlto-NGFW** ▼ Service Redirection Interface: **INTERNET-OUT** ▼

Alors que toute la configuration réseau est en mode opérationnel, vous pouvez surveiller la connexion sous **Surveillance > Pare-feu** > dans la liste **Statistiques**, sélectionnez **Stratégies de filtrage**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Firewall

Firewall Statistics

Statistics: Filter Policies

Maximum entries to display: 50

Filtering: Application: Any Family: Any IP Protocol: Any

Filter Policy Action: Any Source Service Type: Any Source Service Name: Any Source IP: *

Destination Service Type: Any Destination Service Name: Any Destination IP: *

Source Port: * Destination Port: * Source Zone: Any Destination Zone: Any DSCP: Any

Refresh

Show latest data.

Help

Filter Policies

Default Policy=Allow(Not Tracked) Packets=42 Bytes=3528

Match In Progress Packets=0 Bytes=0

ID	Application	Family	IP Protocol	DSCP	Service Type	Service Name	IP Address	Port or ICMP Type	Zone	Service Type	Service Name	IP Address	Port or ICMP Code	Zone	Action	Conn Match Type	Track Connection	Allow Fragments
1	*	*	*	*	*	-	*	NA	*	Internet	-	*	NA	*	Redirect	Symmetric	No	Yes
2	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
3	*	*	*	*	*	-	*	NA	*	Virtual Path	-	*	NA	*	Redirect	Symmetric	No	Yes
4	*	*	*	*	Virtual Path	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
5	*	*	*	*	* IPHost	-	*	NA	*	*	-	*	NA	*	Allow	Symmetric	No	Yes
6	*	*	TCP	*	Internet	-	*	*	Internet_Zone	*		172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes
7	*	*	UDP	*	Internet	-	*	*	Internet_Zone	*		172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes
8	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Drop	Symmetric	No	Yes

Filter Policies Displayed: 8

Filter Policies In Use: 8/1000

Vous pouvez vérifier le mappage entre la configuration que vous avez effectuée sur le modèle de chaîne de service SD-WAN et la configuration du réseau Palo Alto à l'aide de l'interface utilisateur des réseaux Palo Alto.

paloalto

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Commit

Config

Search

Interfaces

Zones

VLANs

Virtual Wires

Virtual Routers

IPSec Tunnels

GRE Tunnels

DHCP

DNS Proxy

GlobalProtect

Portals

Gateways

MDM

Device Block List

Clientless Apps

Clientless App Groups

QoS

LLDP

Network Profiles

GlobalProtect IPSec Crypt

IKE Gateways

IPSec Crypto

IKE Crypto

Interface Mgmt

Zone Protection

QoS Profile

LLDP Profile

BFD Profile

Ethernet

VLAN

Loopback

Tunnel

26 items

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual Wire	Security Zone	Features	Comment
ethernet1/1	Virtual Wire		none	none	none	Untagged	VWIRE-INET	LAN		
ethernet1/1.10	Virtual Wire		none	none	none	10	VWIRE-INTRANET	LAN		
ethernet1/2	Virtual Wire		none	none	none	Untagged	VWIRE-INET	Internet		
ethernet1/2.10	Virtual Wire		none	none	none	10	VWIRE-INTRANET	Intranet		
ethernet1/3			none	none	none	Untagged	none	none		
ethernet1/4			none	none	none	Untagged	none	none		
ethernet1/5			none	none	none	Untagged	none	none		
ethernet1/6			none	none	none	Untagged	none	none		
ethernet1/7			none	none	none	Untagged	none	none		
ethernet1/8			none	none	none	Untagged	none	none		
ethernet1/9			none	none	none	Untagged	none	none		
ethernet1/10			none	none	none	Untagged	none	none		
ethernet1/11			none	none	none	Untagged	none	none		
ethernet1/12			none	none	none	Untagged	none	none		
ethernet1/13			none	none	none	Untagged	none	none		
ethernet1/14			none	none	none	Untagged	none	none		
ethernet1/15			none	none	none	Untagged	none	none		
ethernet1/16			none	none	none	Untagged	none	none		

REMARQUE

La machine virtuelle Palo Alto Networks ne peut pas être provisionnée si **Cloud Direct** ou **SD-WAN WANOP (PE)** est déjà provisionné sur l'appliance 1100.

Cas d'utilisation — Pare-feu hébergé sur SD-WAN 1100

Voici quelques-uns des scénarios de cas d'utilisation implémentés à l'aide de l'appliance Citrix SD-WAN 1100 :

Cas d'utilisation 1 : Rediriger tout le trafic vers le pare-feu hébergé

Ce cas d'utilisation s'applique aux cas d'utilisation de petites succursales où tout le trafic est traité par le pare-feu de nouvelle génération hébergé. Les exigences en matière de bande passante doivent être prises en considération, car le débit de trafic redirigé est limité à 100 Mbps.

Pour ce faire, créez une règle de pare-feu pour correspondre à tout trafic et avec **Action** en tant que **redirection**, comme illustré dans la capture d'écran suivante :

Priority:
100

Policy Type:
Hosted Firewall

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type:
IP Protocol

IP Protocol:
Any

DSCP:
Any

☐ Match Established

Application Objects:
Any

Source Service Type:
Any

Source Service Name:
Any

Source IP:
*

Source Port:
*

Dest Service Type:
Any

Dest Service Name:

Dest IP:
*

Dest Port:
*

Actions

Action:
Redirect

☒ Allow Fragments

Connection State Tracking:
No Tracking

Hosted Firewall Template:
PA-Template

Service Redirection Interface
PA-Intf

Cas d'utilisation 2 : Rediriger uniquement le trafic Internet vers le pare-feu hébergé

Ce cas d'utilisation s'applique à tous les sites de succursale où le trafic lié à Internet n'excède pas le débit de trafic redirigé pris en charge. Dans ce cas, le trafic entre la branche et le centre de données est traité par les appliances/services de sécurité déployés dans les centres de données.

Pour ce faire, créez une règle de pare-feu pour correspondre à n'importe quel trafic et avec **Action** comme **Redirection** comme illustré dans la capture d'écran suivante :

Priority: 100

Policy Type: Hosted Firewall

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

☐ Match Established

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Internet

Dest Service Name: Any

Dest IP: *

Dest Port: *

Actions

Action: Redirect

☒ Allow Fragments

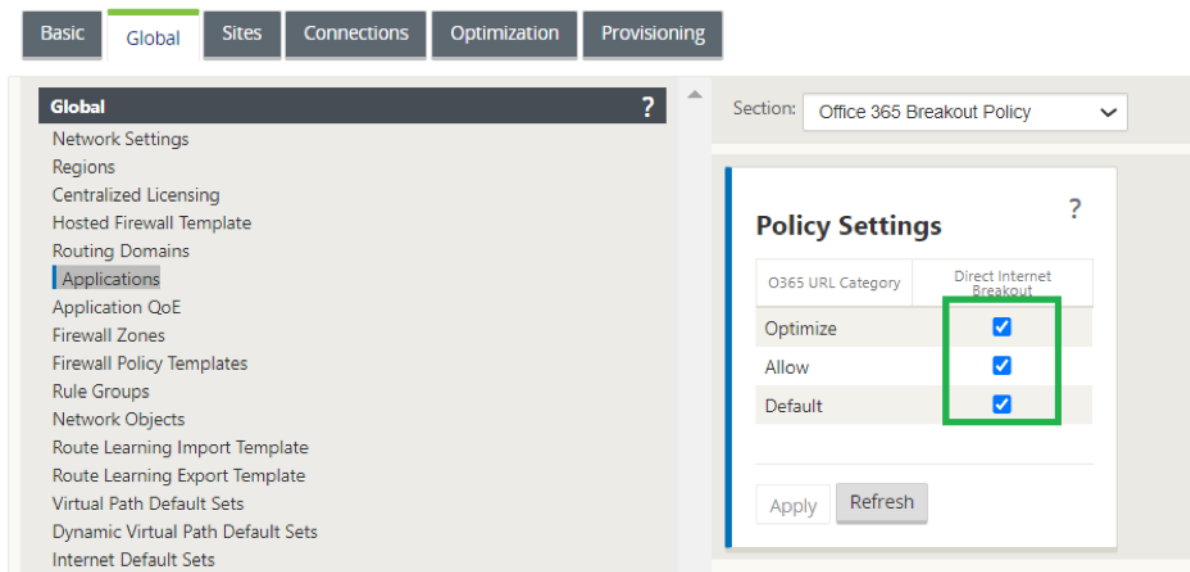
Connection State Tracking: No Tracking

Hosted Firewall Template: PA-Template

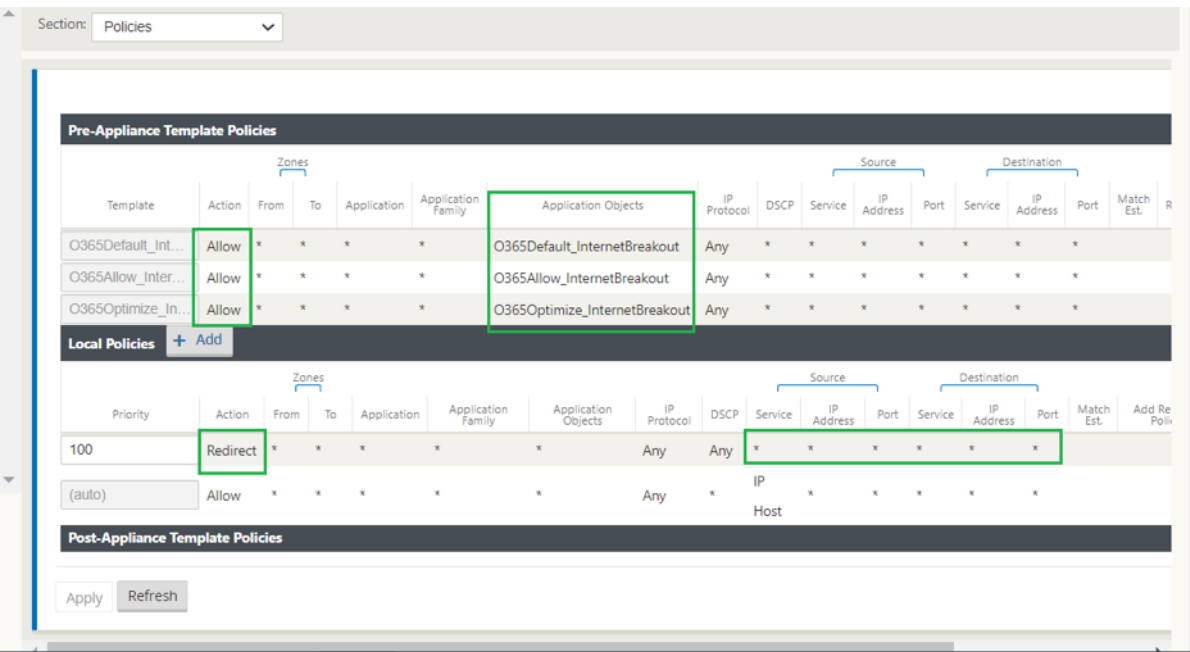
Service Redirection Interface: PA-Intf

Cas d'utilisation 3 : connexion Internet directe pour les applications Internet SaaS fiables et redirection tout le trafic restant vers la machine virtuelle hébergée

Dans ce cas d'utilisation, une règle de pare-feu est ajoutée pour effectuer une ventilation Internet directe pour les applications SaaS approuvées telles que Office 365. Activez d'abord la stratégie de rupture Office 365 comme indiqué dans la capture d'écran suivante :



Cela ajoute automatiquement des **stratégies de modèle de pré-appliance** pour autoriser le trafic Office 365, comme indiqué dans la capture d'écran suivante. Ajoutez maintenant une règle de pare-feu pour rediriger tout le trafic restant vers le pare-feu hébergé comme mentionné ci-dessous.



Remarque

La configuration du pare-feu hébergé est indépendante de la configuration Citrix SD-WAN. Ainsi, le pare-feu hébergé peut être configuré conformément aux exigences de sécurité de l'entreprise.

Intégration du pare-feu Check Point sur la plate-forme SD-WAN 1100

November 1, 2021

Citrix SD-WAN prend en charge l'hébergement de **Check Point Quantum Edge** sur la plate-forme SD-WAN 1100.

Le **Check Point Quantum Edge** s'exécute en tant que machine virtuelle sur la plate-forme SD-WAN 1100. La machine virtuelle pare-feu est intégrée en mode Bridge avec deux interfaces virtuelles de données qui lui sont connectées. Le trafic requis peut être redirigé vers la machine virtuelle du pare-feu en configurant des stratégies sur SD-WAN.

Remarque

À partir de Citrix SD-WAN 11.3.1, la VM Check Point version 80.20 et supérieure est prise en charge pour le provisionnement de machines virtuelles sur de nouveaux sites.

Avantages

Les principaux objectifs ou avantages de l'intégration de Check Point sur la plate-forme SD-WAN 1100 sont les suivants :

- Consolidation des périphériques de succursale : une appliance unique qui effectue à la fois le SD-WAN et la sécurité avancée
- Sécurité des succursales avec pare-feu NGFW sur site (Next Generation Firewall) pour protéger le trafic LAN à LAN, LAN à Internet et Internet-to-LAN

Étapes de configuration

Les configurations suivantes sont nécessaires pour intégrer la machine virtuelle du pare-feu Check Point sur le SD-WAN :

- Provisionner la machine virtuelle du pare-feu
- Activer la redirection du trafic vers la machine virtuelle de sécurité

Remarque La

machine virtuelle Pare-feu doit d'abord être provisionnée avant d'activer la redirection du trafic.

Provisioning Check Point Firewall machine virtuelle

Il existe deux façons de provisionner la machine virtuelle du pare-feu :

- Provisionnement via SD-WAN Center
- Provisionnement via l'interface graphique de l'appliance SD-WAN

Provisioning de machines virtuelles par le biais de SD-WAN Center

Conditions préalables

- Ajoutez le stockage secondaire à SD-WAN Center pour stocker les fichiers image de la machine virtuelle du pare-feu. Pour plus d'informations, consultez [Configuration système requise et installation](#).
- Réservez le stockage à partir de la partition secondaire pour les fichiers image de la machine virtuelle du pare-feu. Pour configurer la limite de stockage, accédez à **Administration > Maintenance du stockage**.
 - Sélectionnez la quantité de stockage requise dans la liste.
 - Cliquez sur **Apply**.

Administration / Storage Maintenance

Region: Default_Region

Host	File System	Type	Size (MB)	Available (MB)	Active/Migrate Data
Local*	/dev/xvda2	ext3	7288	3471	
Local	/dev/xvdb	ext3	14910	12921	

Apply

Note: Software image storage reserved will be reduced while calculating the secondary partition Size(MB) and Available(MB)

Software Image Storage Reservation

Note: User can modify the storage reservation only if the SD-WAN Center has secondary partition mounted and it should operate in headend mode

Amount of storage to reserve from secondary partition storage(Active) is: **10GB**

Apply

Thresholds

SD-WAN Center Database Storage and Auto Cleanup settings are misconfigured, SD-WAN Center will reach auto cleanup threshold before the configured 6 months.

Stop stats polling when storage usage exceeds **55%** of active storage size

☐ Notify user when storage usage exceeds **10%** of active storage size

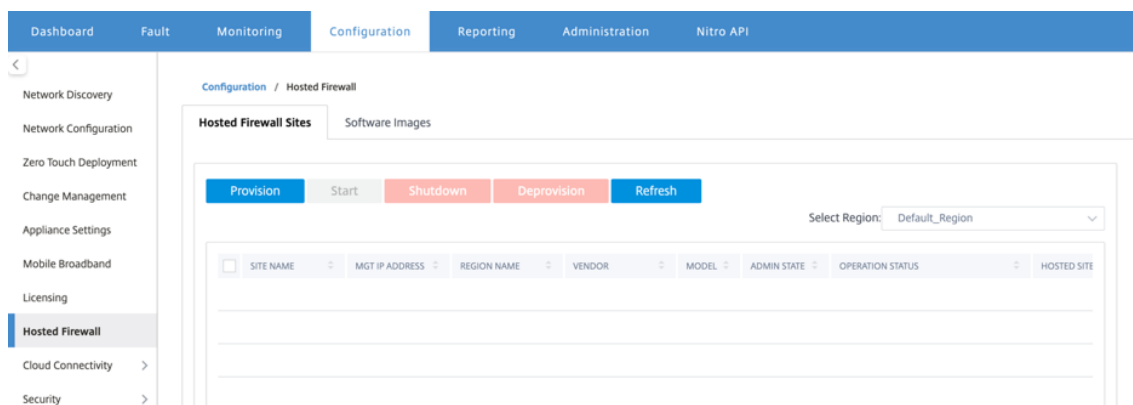
Apply

Remarque

Le stockage est réservé à partir de la partition secondaire qui est active si la condition est remplie.

Procédez comme suit pour Provisioning la machine virtuelle de pare-feu via la plate-forme SD-WAN Center :

1. Dans l'interface graphique Citrix SD-WAN Center, accédez à **Configuration** > sélectionnez **Pare-feu hébergé**.



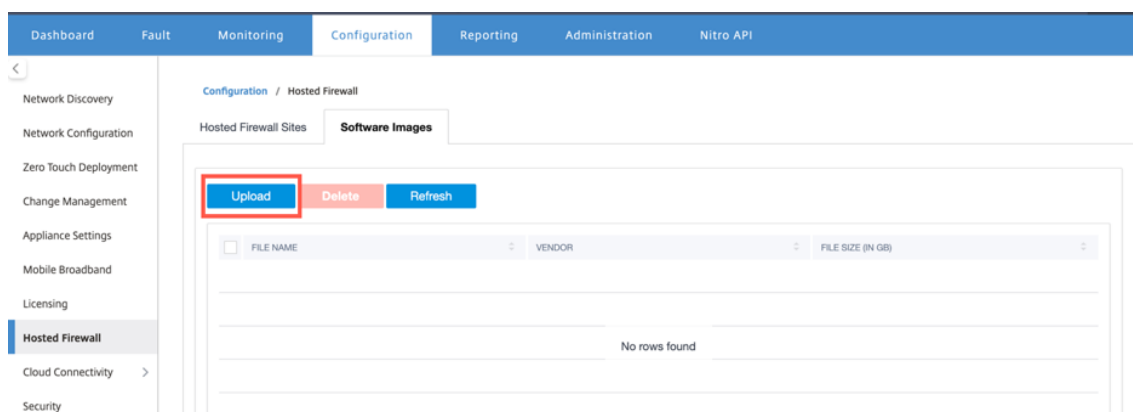
Vous pouvez sélectionner la **Région** dans la liste déroulante pour afficher les détails du site provisionné pour cette région sélectionnée.

2. Téléchargez l'image du logiciel.

Remarque

Assurez-vous que vous disposez de suffisamment d'espace disque pour télécharger l'image logicielle.

Accédez à **Configuration** > **Pare-feu hébergé** > **Images logicielles** et cliquez sur **Télécharger**.



3. Sélectionnez le nom du fournisseur en tant que **point de contrôle** dans la liste déroulante. Cliquez ou déposez le fichier image du logiciel dans la zone à télécharger.



Une barre d'état apparaît avec le processus de téléchargement en cours. Ne cliquez pas sur **Actualiser** ou n'effectuez aucune autre action jusqu'à ce que le fichier image affiche 100 % téléchargé.

- **Actualiser** : cliquez sur l'option **Actualiser** pour obtenir les derniers détails du fichier image.
- **Supprimer** : cliquez sur l'option **Supprimer** pour supprimer tout fichier image existant.

Remarque

Pour provisionner la machine virtuelle de pare-feu sur la partie sites d'une région autre que par défaut, téléchargez le fichier image sur chacun des nœuds du collecteur.

4. Pour le provisionnement, revenez à l'onglet **Sites de pare-feu hébergés** et cliquez sur **Provisionner**.

Provision Virtual Machine

Vendor *

Check Point

Vendor Virtual Machine Model *

EDGE

Region *

Region where the sites available

Software Image *

Choose the Image to provision

Please ensure to upload this image in the collector for non-default region sites provisioning

Sites for Firewall Hosting *

Sites to host the firewall

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Virtual Machine SIC Key

Enter the SIC key

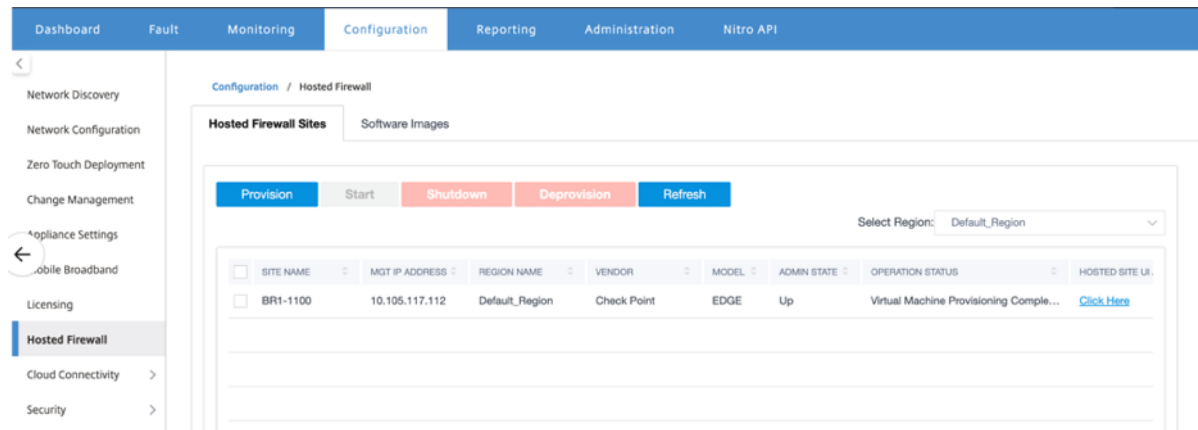
Start Provision Cancel

- **Fournisseur** : sélectionnez le nom du fournisseur en tant que **point de contrôle** dans la liste déroulante.
- **Modèle de machine virtuelle fournisseur** : Le champ de modèle de machine virtuelle est automatiquement rempli en tant que Edge.
- **Région** : Sélectionnez la région dans la liste.
- **Image logicielle** : sélectionnez le fichier Image à provisionner.
- **Sites pour l'hébergement de pare-feu** : sélectionnez des sites pour la liste d'hébergement de pare-feu. Vous devez sélectionner les sites principaux et secondaires si les sites sont en mode haute disponibilité.
- **Adresse IP principale/Nom de domaine du serveur Management Server** : entrez l'adresse IP principale de gestion ou le nom de domaine complet (facultatif).
- **Clé SIC de machine virtuelle** : **entrez la clé SIC**(Secure Internal Communication) de la machine virtuelle. SIC crée des connexions fiables entre les composants **Check Point**.

5. Cliquez sur **Démarrer la mise en service**.

6. Cliquez sur **Actualiser** pour obtenir le dernier état. Une fois que la machine virtuelle Check Point est complètement démarrée, elle se reflète sur l'interface utilisateur SD-WAN Center.

Vous pouvez **démarrer**, **arrêter** et **désapprovisionner** la machine virtuelle si nécessaire.

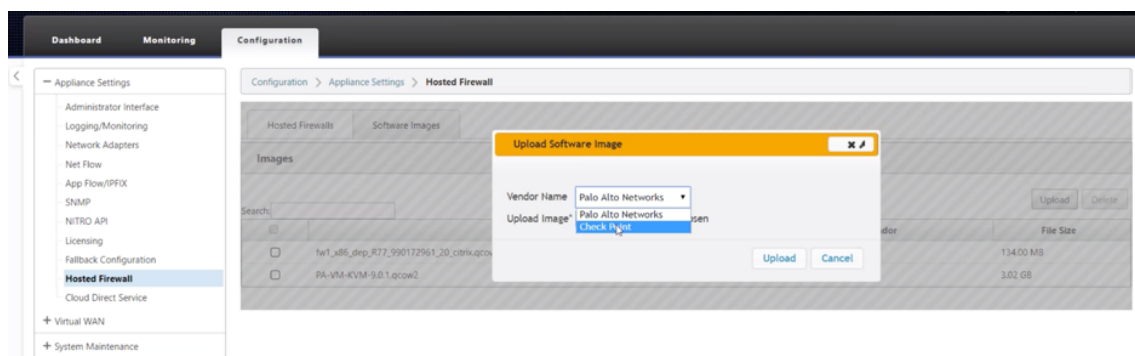


- **Nom du site** : affiche le nom du site.
- **IP de gestion** : affiche l'adresse IP de gestion du site.
- **Nom de la région** : affiche le nom de la région.
- **Fournisseur** : affiche le nom du fournisseur (Point de contrôle).
- **Modèle** : Affiche le modèle - **Edge**.
- **État d'administration** : état de la machine virtuelle du fournisseur (haut/bas).
- **État de l'opération** : affiche le dernier message d'état de l'opération.
- **Accès à l'interface utilisateur du site hébergé** : utilisez le lien **Cliquez ici** pour accéder à l'interface graphique de la machine virtuelle Check Point.

Provisioning de machines virtuelles par pare-feu via l'interface graphique du dispositif SD-WAN

Sur la plate-forme SD-WAN, provisionnez et démarrez la machine virtuelle hébergée. Effectuez les étapes suivantes pour le Provisioning :

1. Dans l'interface graphique Citrix SD-WAN, accédez à **Configuration > Paramètres de l'appliance** sélectionnez **Pare-feu hébergé**.
2. Téléchargez l'image du logiciel :
 - Sélectionnez l'onglet **Images logicielles** . Sélectionnez le **nom du fournisseur** comme point de contrôle.
 - Choisissez le fichier image du logiciel.
 - Cliquez sur **Charger**.

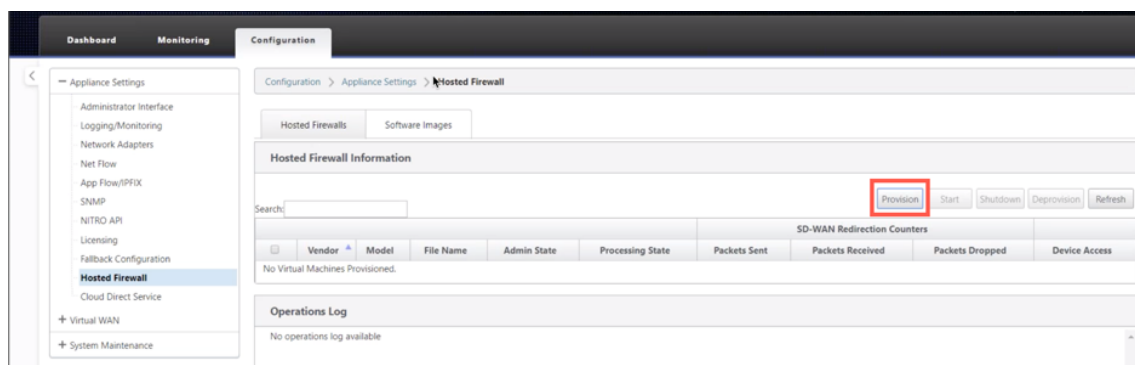


Remarque

Un maximum de deux images peut être téléchargé. Le téléchargement de l'image de la machine virtuelle Check Point peut prendre plus de temps en fonction de la disponibilité de la bande passante.

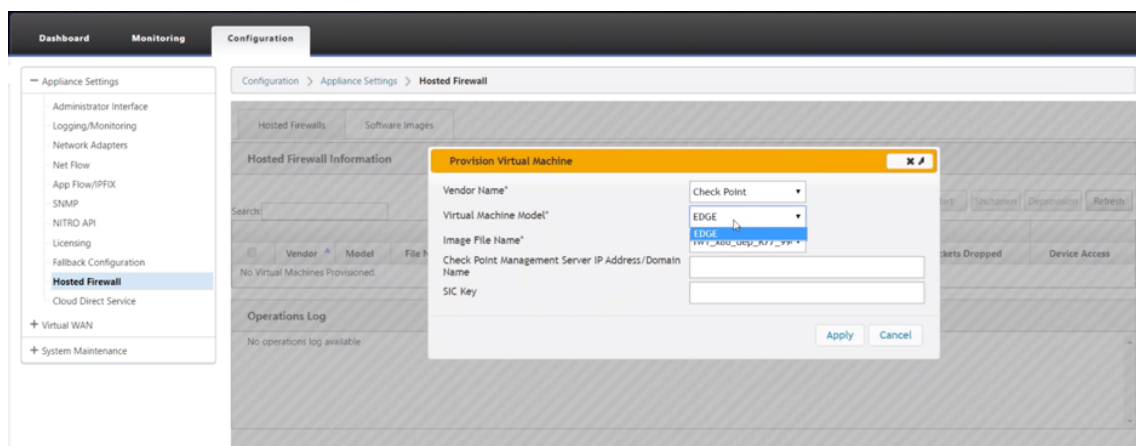
Vous pouvez voir une barre d'état pour suivre le processus de téléchargement. Le détail du fichier reflète, une fois que l'image est téléchargée avec succès. L'image utilisée pour le Provisioning ne peut pas être supprimée. N'effectuez aucune action ou revenez à une autre page jusqu'à ce que le fichier image affiche 100% téléchargée.

3. Pour le provisioning, sélectionnez l'onglet **Pare-feu hébergé** > cliquez sur le bouton **Provisioning**.

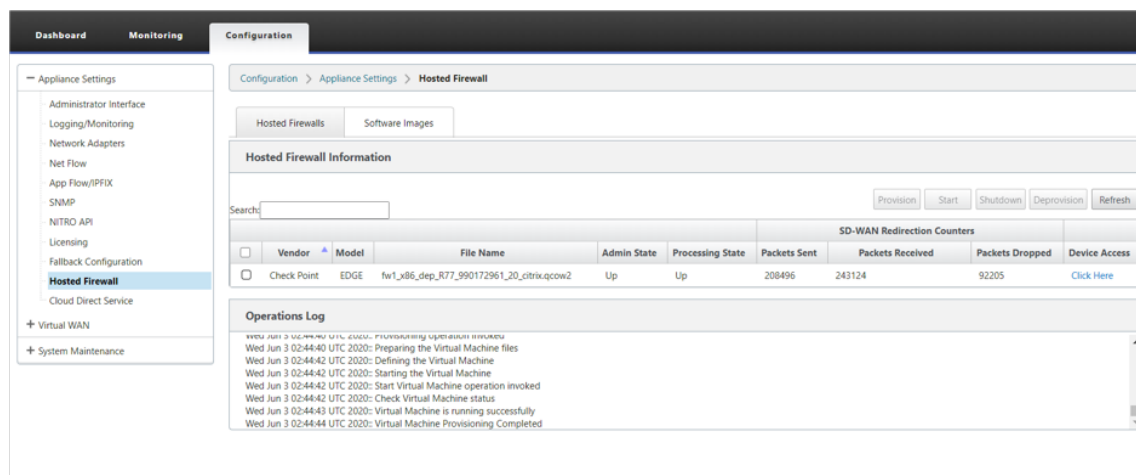


4. Fournissez les détails suivants pour le Provisioning.

- **Nom du fournisseur** : sélectionnez le **nom du fournisseur** comme point de contrôle.
- **Modèle de machine virtuelle** : le **modèle** de machine virtuelle est automatiquement rempli en tant que **Edge**.
- **Nom du fichier image** : le nom du fichier image est automatiquement renseigné.
- **Adresse IP/Domaine du serveur Check Point Management** : Fournissez l'adresse IP/-domaine du serveur de gestion de point de contrôle.
- **Clé SIC** : Fournir la clé SIC (facultatif). SIC crée des connexions fiables entre les composants **Check Point**. Cliquez sur **Apply**.



5. Cliquez sur **Actualiser** pour obtenir le dernier état. Une fois que la machine virtuelle Check Point est complètement démarrée, elle refléchet sur l'interface utilisateur SD-WAN avec les détails du journal des opérations.



- **État d'administration** : indique si la machine virtuelle est en service ou en panne.
- **État de traitement** : état de traitement du chemin de données de la machine virtuelle.
- **Paquet envoyé** : paquets envoyés depuis le SD-WAN vers la machine virtuelle de sécurité.
- **Paquet reçu** : paquets reçus par SD-WAN depuis la machine virtuelle de sécurité.
- **Paquet abandonné** : Paquets supprimés par le SD-WAN (par exemple, lorsque la machine virtuelle de sécurité est en panne).
- **Accès aux périphériques** : cliquez sur le lien pour obtenir l'accès de l'interface graphique à la machine virtuelle de sécurité.

Vous pouvez **démarrer**, **arrêter** et **désapprovisionner** la machine virtuelle si nécessaire. Utilisez l'option **Cliquez ici** pour accéder à l'interface graphique de la machine virtuelle Check Point ou utiliser votre adresse IP de gestion avec le port 4100 (IP de gestion : 4100).

Remarque

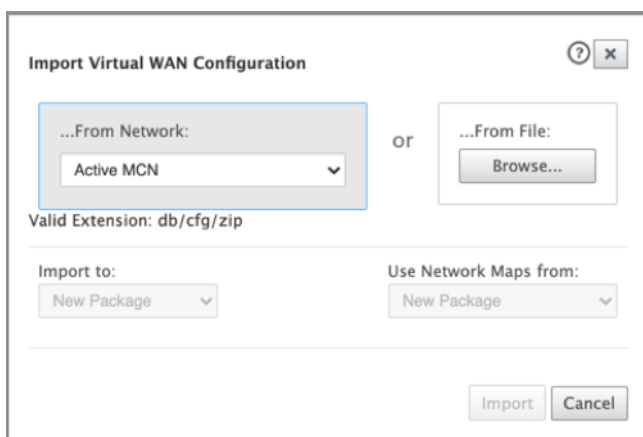
Utilisez toujours le mode navigation privée pour accéder à l'interface graphique du point de contrôle.

Rediriger le trafic vers Edge

La configuration de la redirection du trafic peut être effectuée à la fois via l'Éditeur de configuration sur MCN ou l'Éditeur de configuration sur SD-WAN Center.

Pour naviguer dans l'Éditeur de configuration sur SD-WAN Center :

1. Ouvrez l'interface utilisateur du centre Citrix SD-WAN, accédez à **Configuration > Importation de configuration réseau**. Importez la configuration WAN virtuel à partir du MCN actif et cliquez sur **Importer**.



Les étapes restantes sont similaires comme suit : la configuration de redirection du trafic via MCN.

Pour naviguer dans l'Éditeur de configuration sur MCN :

1. Définissez le **type de correspondance de connexion** sur **Symétrique** sous **Global > Paramètres réseau**.

The screenshot displays the Citrix SD-WAN Configuration Editor interface. On the left is a navigation pane under the 'Global' tab, listing various settings categories. The main panel is divided into two sections: 'Global Security Settings' and 'Global Firewall Settings'.

Global Security Settings:

- Note:** Changing the Network Encryption Mode may cause Site Secure Keys to be truncated or regenerated if they do not meet the requirements of the new mode.
- Network Encryption Mode:** AES 128-Bit
- ☒ Enable Encryption Key Rotation
- ☐ Enable Extended Packet Encryption Header
- ☐ Enable Extended Packet Authentication Trailer
- Extended Packet Authentication Trailer Type:** 32-Bit Checksum
- ☐ Enable FIPS Mode
- ☐ Enable Appliance Authentication
- Network Secure Key:** 72d050ce5ca54c... Regenerate

Global Firewall Settings:

- Global Policy Template:** New_Firewall_...
- Default Firewall Action:** Allow
- ☒ Default Connection State Tracking
- Connection Match Type:** Symmetric (highlighted with a red box)
- Denied Timeout (s):** 30
- TCP Initial Timeout (s):** 120
- TCP Idle Timeout (s):** 7440
- TCP Closing Timeout (s):** 60
- TCP Time Wait Timeout (s):** 120
- TCP Closed Timeout (s):** 10
- UDP Initial Timeout (s):** 30
- UDP Idle Timeout (s):** 300
- ICMP Initial Timeout (s):** 30
- ICMP Idle Timeout (s):** 60
- Generic Initial Timeout (s):** 30
- Generic Idle Timeout (s):** 300

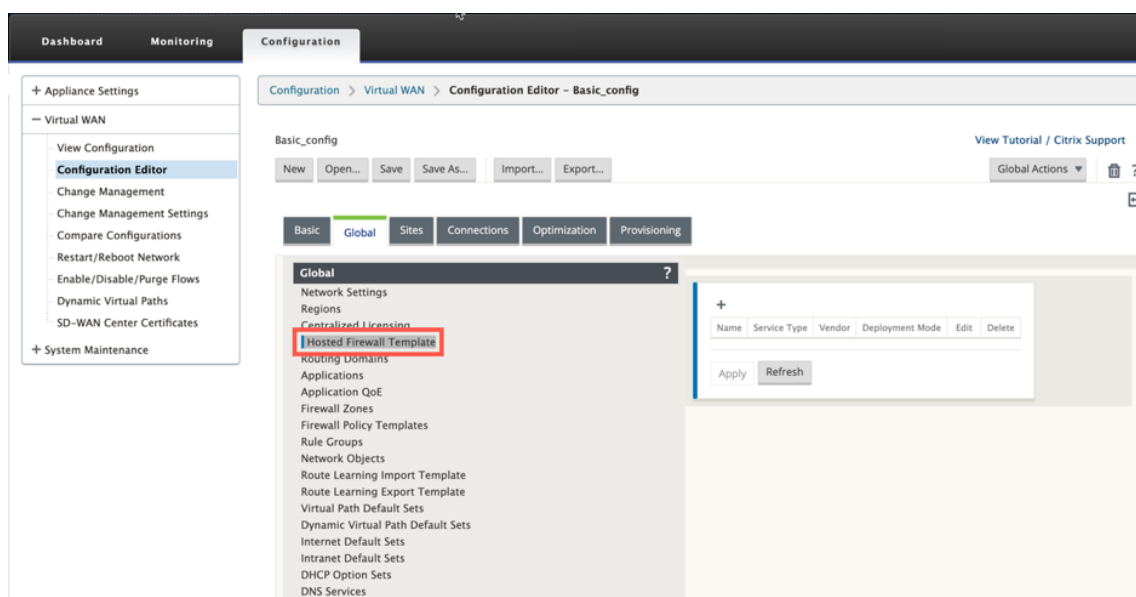
Global On-Demand Bandwidth Limit Setting:

- Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%): 120

At the bottom, there are 'Apply' and 'Revert' buttons.

Par défaut, les stratégies de pare-feu SD-WAN sont spécifiques à la direction. Le type de correspondance symétrique correspond aux connexions à l'aide de critères de correspondance spécifiés et applique une action de stratégie dans les deux directions.

- Ouvrez l'interface utilisateur Citrix SD-WAN, accédez à **Configuration > développez Virtual WAN** **sélectionnez **Configuration Editor** ** sélectionnez **Hosted Firewall Template (Modèle de pare-feu hébergé)** dans la section **Global**.



3. Cliquez sur **+** et fournissez les informations requises disponibles dans la capture d'écran suivante pour ajouter le **modèle de pare-feu hébergé**. Cliquez sur **Ajouter**.

Edit

Name:

Vendor:

Model:

Deployment Mode:

Primary Management Server IP/FQDN:

Secondary Management Server IP/FQDN:

Service Redirection Interfaces

Name	Input Interface	Output Interface	VLAN ID	Delete
INTERNET-OUT	Interface-1	Interface-2	0	
INTERNET-IN	Interface-2	Interface-1	0	

Le **modèle de pare-feu hébergé** vous permet de configurer la redirection du trafic vers la **machine virtuelle de pare-feu** hébergée sur la plate-forme SD-WAN. Voici les entrées nécessaires à la configuration du modèle :

- **Nom** : nom du modèle de pare-feu hébergé.
- **Fournisseur** : Nom du fournisseur du pare-feu —Point de contrôle.
- **Mode de déploiement** : le champ **Mode de déploiement** est automatiquement renseigné et grisé. Pour le fournisseur du **point de contrôle**, le mode de déploiement est **Bridge**.

- **Modèle : Modèle** de machine virtuelle du pare-feu hébergé. Une fois que vous avez sélectionné le fournisseur comme **Point de contrôle**, le champ modèle est automatiquement rempli avec **Edge**.
- **Serveur d'administration principal IP/FQDN : nom** de domaine de domaine complet du serveur d'administration principal.
- **Serveur d'administration secondaire IP/FQDN : nom** de domaine complet du serveur d'administration secondaire.
- **Interfaces de redirection de service** : il s'agit d'interfaces logiques utilisées pour la redirection du trafic entre le SD-WAN et le pare-feu hébergé.

Remarque

L'interface d'entrée de redirection doit être sélectionnée dans la direction de l'initiateur de connexion, l'interface de sortie est automatiquement choisie pour le trafic de réponse. Par exemple, si le trafic Internet sortant est redirigé vers le pare-feu hébergé sur Interface-1, le trafic de réponse est automatiquement redirigé vers le pare-feu hébergé sur Interface-2. En outre, il n'y a pas besoin d'Interface-2 s'il n'y a pas de trafic entrant Internet.

Seules deux interfaces de données sont affectées à la machine virtuelle Check Point.

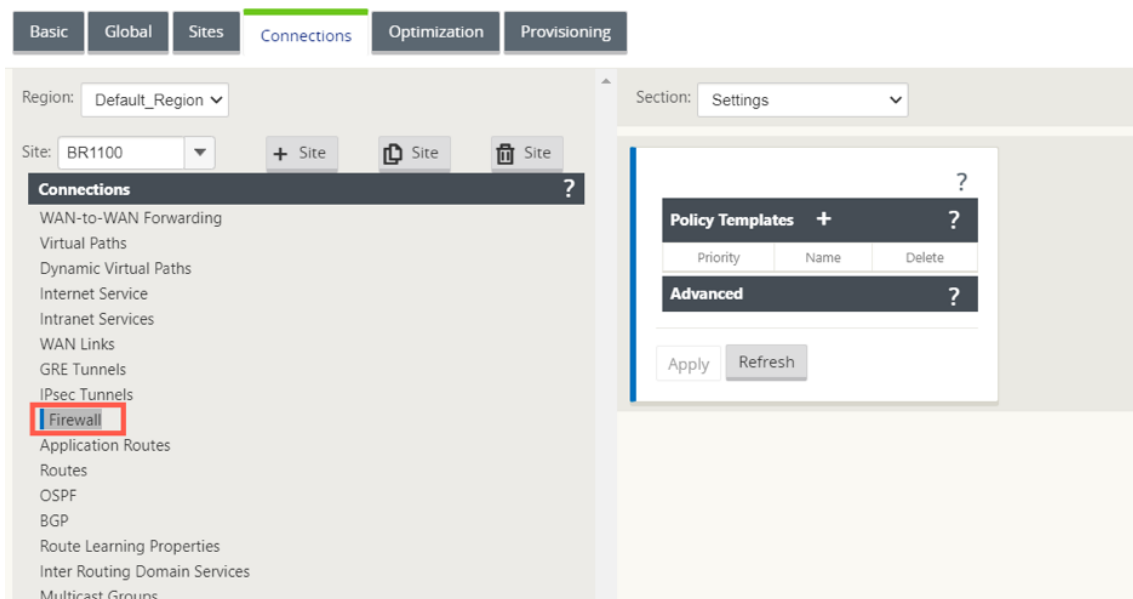
Remarque

Les stratégies de pare-feu SD-WAN sont automatiquement créées pour **Autoriser** le trafic depuis/vers les serveurs de gestion de pare-feu hébergés. Cela évite la redirection du trafic de gestion qui provient (ou) du pare-feu hébergé.

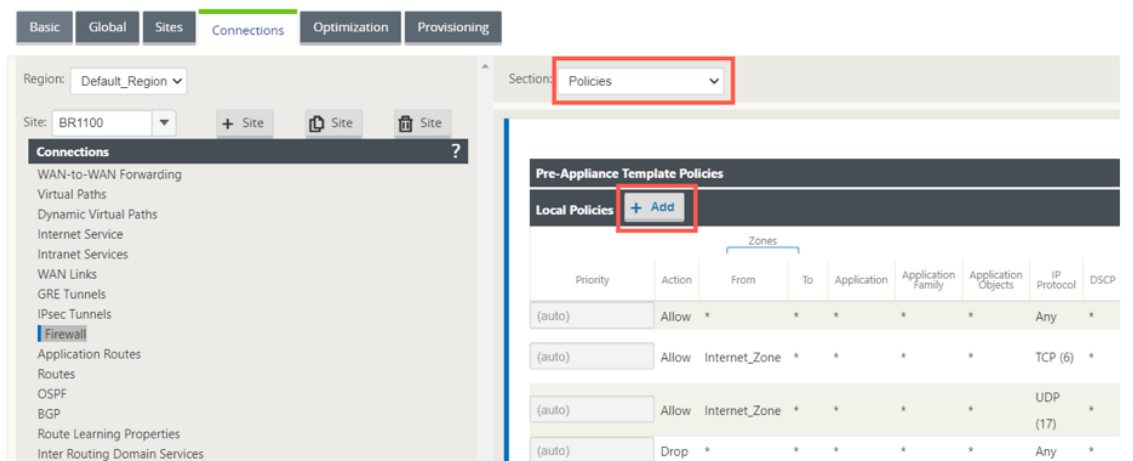
La redirection du trafic vers la machine virtuelle du pare-feu peut être effectuée à l'aide de stratégies de pare-feu SD-WAN. Il existe deux méthodes pour créer les stratégies de pare-feu SD-WAN : via des modèles de stratégie de pare-feu dans la section **Global** ou au niveau du site.

Méthode - 1

1. Depuis l'interface graphique Citrix SD-WAN, accédez à **Configuration** développez **Réseau étendu virtuel > Éditeur de configuration**. Sélectionnez **Pare-feu** sous **Connexions**.



2. Sélectionnez **Stratégies** dans la liste déroulante **Section**, puis cliquez sur **+Ajouter** pour créer une stratégie de pare-feu.



3. Modifiez le **type de stratégie** par **Pare-feu hébergé**. Le champ **Action** est automatiquement rempli sur Redirection. Sélectionnez le **modèle de pare-feu hébergé** et l'**interface de redirection de service** dans la liste déroulante. Cliquez sur **Ajouter**.

Priority: 400

Policy Type: **Hosted Firewall**

Match Criteria

From Zones	Zone	Enable
<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Default_LAN_Zone	<input type="checkbox"/>
<input type="checkbox"/>	Inter_Routing_Domain_Zone	<input type="checkbox"/>
<input type="checkbox"/>	Internet_Zone	<input type="checkbox"/>

To Zones	Zone	Enable
<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Default_LAN_Zone	<input type="checkbox"/>
<input type="checkbox"/>	Inter_Routing_Domain_Zone	<input type="checkbox"/>
<input type="checkbox"/>	Internet_Zone	<input type="checkbox"/>

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

☐ Match Established

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: Any

Dest IP: *

Dest Port: *

Actions

Action: **Redirect**

☒ Allow Fragments

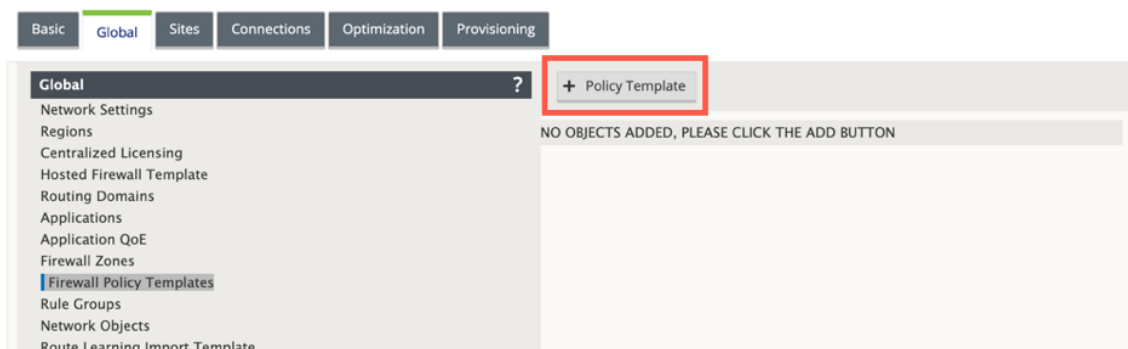
Connection State Tracking: No Tracking

Hosted Firewall Template: CheckPoint-NGFW

Service Redirection Interface: INTERNET-OUT

Méthode - 2

1. Accédez à l'onglet **Global** et sélectionnez **Modèles de stratégie de pare-feu**. Cliquez sur **+ Modèle de stratégie**.



2. Indiquez un nom au modèle de stratégie et cliquez sur **Ajouter**.

Add

Name:

New_Firewall_Policy_Template-1

Add **Cancel**

3. Cliquez sur **+ Ajouter** en regard de **Stratégies de modèle de pré-appliance**.

Basic Global Sites Connections Optimization Provisioning

Global

- Network Settings
- Regions
- Centralized Licensing
- Hosted Firewall Template
- Routing Domains
- Applications
- Application QoS
- Firewall Zones
- Firewall Policy Templates**
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- DNS Services
- Proxy Auto-config settings

Policy Template: New_Firewall_Policy_Template-1 **+ Policy Template** **Policy Template**

Template Name: New_Firewall_Po...

Pre-Appliance Template Policies **+ Add**

Priority	Action	From	To	Application	Application Family	Application Objects	IP Protocol	DSCP	Service	IP Address																						
Post-Appliance Template Policies + Add																																
<table border="1"> <thead> <tr> <th>Priority</th> <th>Action</th> <th>From</th> <th>To</th> <th>Application</th> <th>Application Family</th> <th>Application Objects</th> <th>IP Protocol</th> <th>DSCP</th> <th>Service</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td colspan="11"> <div>Apply Refresh</div> </td> </tr> </tbody> </table>											Priority	Action	From	To	Application	Application Family	Application Objects	IP Protocol	DSCP	Service	IP Address	<div>Apply Refresh</div>										
Priority	Action	From	To	Application	Application Family	Application Objects	IP Protocol	DSCP	Service	IP Address																						
<div>Apply Refresh</div>																																

4. Modifiez le **type de stratégie** par **Pare-feu hébergé**. Le champ **Action** est automatiquement renseigné pour **rediriger**. Sélectionnez le **modèle de pare-feu hébergé** et l'**interface de redirection de service** dans la liste déroulante. Cliquez sur **Ajouter**.

Priority: Policy Type: **Hosted Firewall**

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: **IP Protocol** IP Protocol: **Any** DSCP: **Any** ☐ Match Established

Application Objects: **Any**

Source Service Type: **Any** Source Service Name: **Any** Source IP: Source Port:

Dest Service Type: **Any** Dest Service Name: **Any** Dest IP: Dest Port:

Actions

Action: **Redirect** ☒ Allow Fragments Connection State Tracking: **No Tracking**

Hosted Firewall Template: **CheckPoint-NGFW** Service Redirection Interface: **INTERNET-OUT**

5. Accédez à **Connexions > Pare-feu**, puis sélectionnez la stratégie de pare-feu (que vous avez créée) dans le champ Nom. Cliquez sur **Apply**.

Basic Global Sites **Connections** Optimization Provisioning

Region: **Default_Region** Section: **Settings**

Site: **BR1100** **+ Site** **Site** **Site**

Connections

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall**
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups

Policy Templates

Priority	Name	Delete
100	New_Firewall_P...	

Advanced

Apply **Revert**

Alors que toute la configuration réseau est en mode opérationnel, vous pouvez surveiller la connexion sous **Surveillance > Pare-feu >** dans la liste **Statistiques**, sélectionnez **Stratégies de filtrage**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Firewall

Firewall Statistics

Statistics:

Filter Policies

Maximum entries to display:

50

Filtering:

Application: Any

Family: Any

IP Protocol: Any

Filter Policy Action: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Destination Service Type: Any

Destination Service Name: Any

Destination IP: *

Source Port: *

Destination Port: *

Source Zone: Any

Destination Zone: Any

DSCP: Any

Refresh

Show latest data.

Help

Filter Policies

Default Policy - Allow(Not Tracked) Packets - 42 Bytes - 3528

Match In Progress Packets - 0 Bytes - 0

ID	Application	Family	IP Protocol	DSCP	Source				Zone	Destination				Action	Conn Match Type	Track Connection	Allow Fragments	
					Service Type	Service Name	IP Address	Port or ICMP Type		Service Type	Service Name	IP Address	Port or ICMP Code					
1	*	*	*	*	*	-	*	NA	*	Internet	-	*	NA	*	Redirect	Symmetric	No	Yes
2	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
3	*	*	*	*	*	-	*	NA	*	Virtual Path	-	*	NA	*	Redirect	Symmetric	No	Yes
4	*	*	*	*	Virtual Path	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
5	*	*	*	*	*	-	*	NA	*	*	-	*	NA	*	Allow	Symmetric	No	Yes
6	*	*	TCP	*	Internet	-	*	*	Internet_Zone	*	-	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes
7	*	*	UDP	*	Internet	-	*	*	Internet_Zone	*	-	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes
8	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Drop	Symmetric	No	Yes

Filter Policies Displayed: 8

Filter Policies In Use: 8/1000

Groupes d'agrégation de liens

November 1, 2021

La fonctionnalité de groupes d'agrégation de liens (LAG) vous permet de regrouper deux ports ou plus de votre appliance SD-WAN afin qu'ils fonctionnent ensemble comme un seul port. Cela garantit une disponibilité accrue, une redondance de liaison et des performances améliorées.

Auparavant, seul le mode Active-Backup était pris en charge dans LAG. À partir de la version 11.3 de Citrix SD-WAN, les négociations basées sur le protocole LACP (Link Aggregation Control Protocol) 802.3AD sont prises en charge. Le LACP est un protocole standard et fournit plus de fonctionnalités pour les LAG.

En mode de sauvegarde active, à tout moment, un seul port est actif et les autres ports sont en mode sauvegarde. Les supports actifs et de sauvegarde s'appuient sur le package Data Plane Development Kit (DPDK) pour la fonctionnalité LAG.

Avec le LACP, vous pouvez envoyer le trafic à travers tous les ports simultanément. En tant qu'avantage, vous obtenez plus de bande passante avec le mécanisme de redondance des liens. L'implémentation LACP prend en charge le mode **Active-Active**. Maintenant, avec le mode Active-Sauvegarde, vous avez également la possibilité de sélectionner le mode actif-actif LACP complet à partir de l'interface utilisateur SD-WAN.

La fonctionnalité LAG est disponible uniquement sur les plates-formes prises en charge par DPDK suivantes :

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 4100 et 5100 SE
- Citrix SD-WAN 6100 SE
- Citrix SD-WAN 2100 SE

La fonctionnalité LAG LACP n'est pas disponible sur les plates-formes suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

Remarque

La fonctionnalité LAG n'est pas prise en charge sur les plates-formes VPX/VPXL.

Limitations

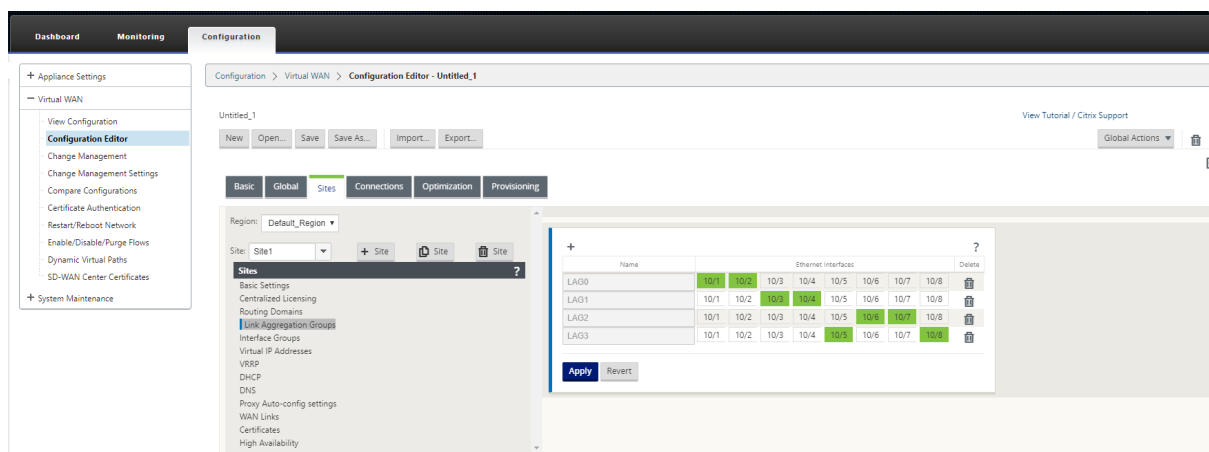
- Vous pouvez créer un maximum de quatre LAG avec un maximum de quatre ports regroupés dans chaque LAG sur les appliances Citrix SD-WAN.
- Les options de priorité de port et de priorité système ne sont pas prises en charge par l'implémentation LACP.

Avec la version 11.3, dans le SD-WAN avec l'implémentation LACP, les ports sont toujours en mode actif. Cela signifie que le SD-WAN peut toujours commencer la négociation.

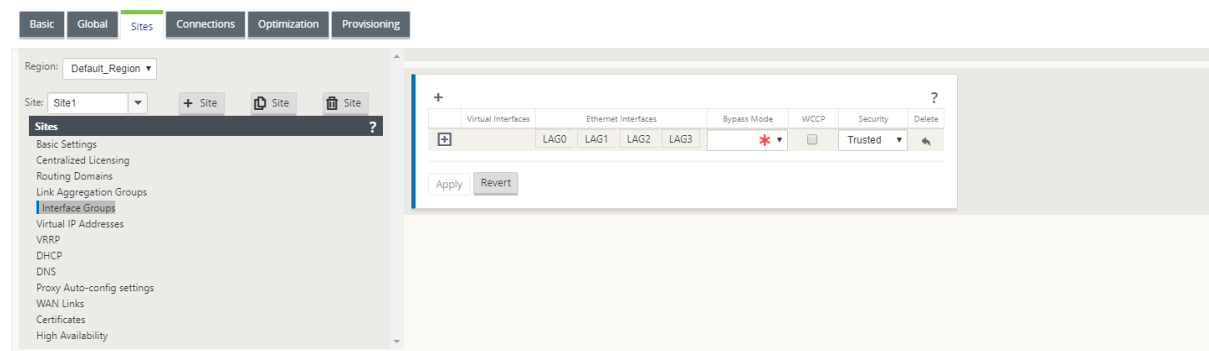
Remarque

Pour les appliances Citrix SD-WAN 210 et 410, vous ne pouvez créer qu'un seul LAG avec un maximum de trois ports regroupés.

Pour configurer des groupes d'agrégation de liens, dans l'**éditeur de configuration**, accédez à **Sites > Groupes d'agrégation de liens**. Vous pouvez afficher tous les ports physiques et les interfaces Ethernet disponibles. Cliquez sur **+** pour créer un LAG.



Sélectionnez les ports membres, puis cliquez sur **Appliquer**. Une fois les ports ajoutés au LAG, vous ne pouvez voir que les LAG dans le **groupe d'interface** au lieu des ports membres.



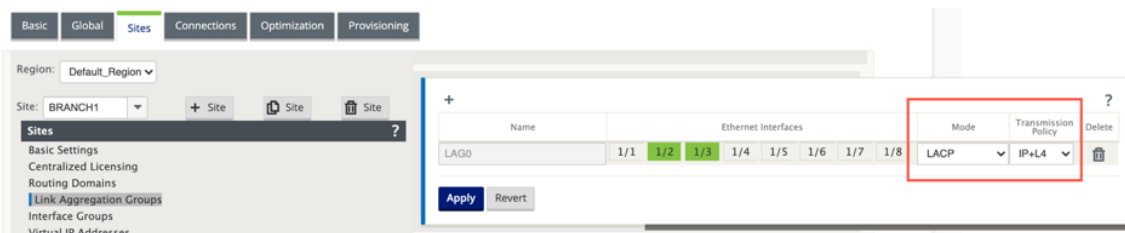
De même, si vous voulez configurer les LAG avec le mode LACP :

1. Cliquez sur **+** pour créer un LAG et sélectionnez les ports d'interface Ethernet.
2. Sélectionnez le mode de configuration comme **LACP** dans la liste déroulante.
3. Sélectionnez la **stratégie de transmission** dans la liste déroulante.

REMARQUE

Si le mode est sélectionné en tant que **sauvegarde active**, le champ **Stratégie de transmission** est désactivé.

4. Cliquez sur **Apply**.



Étant donné que les groupes LAG possèdent de nombreux ports, la **stratégie de transmission** permet de sélectionner le port pouvant être utilisé pour envoyer du trafic. Le champ de stratégie de transmission ne peut être activé que si le mode Agrégation est **Active-actif**. Deux stratégies de transmission sont définies : MAC+IP et IP+L4.

- **MAC+IP** : La sélection de liens pour un paquet donné est basée sur les paramètres des couches 2 et 3. Ainsi, les adresses MAC et IP source et destination prennent ces paramètres et les hachent. Selon le hachage, il sélectionne le port.
- **IP+L4** : La stratégie IP+L4 est basée sur les ports IP source et destination ainsi que les ports et le protocole de couche 4. La stratégie IP+L4 notifie quel paquet passe par quel port. Les paquets avec les mêmes paramètres seront toujours envoyés sur l'un des liens. Cela signifie que le même flux ou un seul flux (même source et destination Mac et IP) passe toujours par les mêmes ports et ne se distribue pas entre les autres ports. En tant qu'avantage, les paquets hors service ne peuvent pas atteindre l'appareil de destination

Vous pouvez créer des interfaces virtuelles à l'aide de LAG et ces interfaces sont ensuite utilisées pour configurer les liaisons LAN/WAN et HA.

Remarque

La fonctionnalité **LSP (Link State Propagation)** n'est pas prise en charge si les LAG sont utilisés comme interfaces Ethernet dans les groupes d'interface.

Surveillance et dépannage

Pour afficher les statistiques ou l'état du lien, accédez à **Surveillance > Statistiques**. Sélectionnez **Ethernet** dans la liste déroulante **Afficher**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Statistics

Statistics

Show: Ethernet ☐ Enable Auto Refresh 5 seconds Refresh

Ethernet Statistics

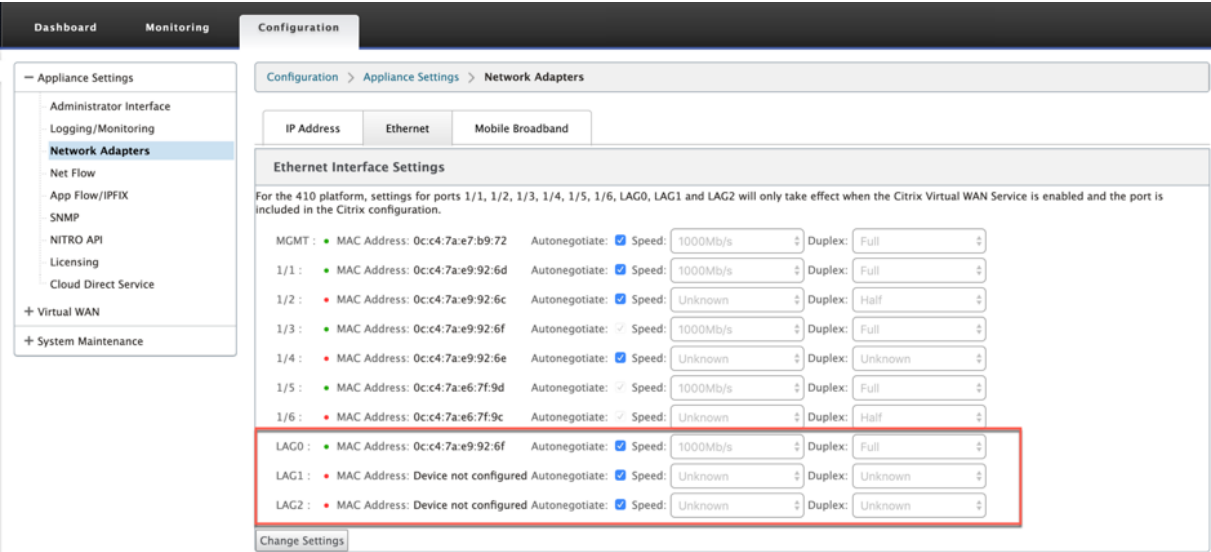
Filter: in Any column Apply

Show 100 entries Showing 1 to 3 of 3 entries

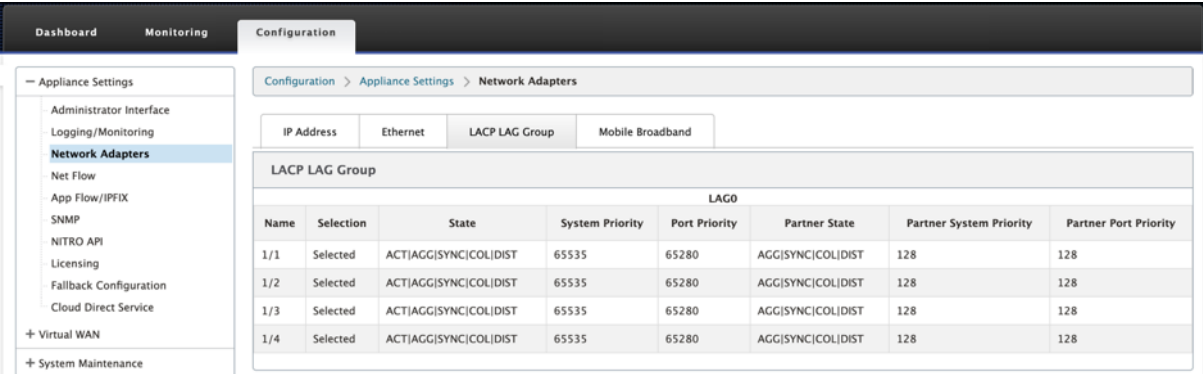
Port	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
LAG0	UP	228799	20119310	210823	16480420	0
1/4	UP	976632	86479280	951719	79790814	0
1/1	UP	0	0	10134	718152	0

Showing 1 to 3 of 3 entries

Pour afficher les ports LAG actifs et de secours, accédez à **Configuration > Paramètres de l'appliance > Cartes réseau > Ethernet**.



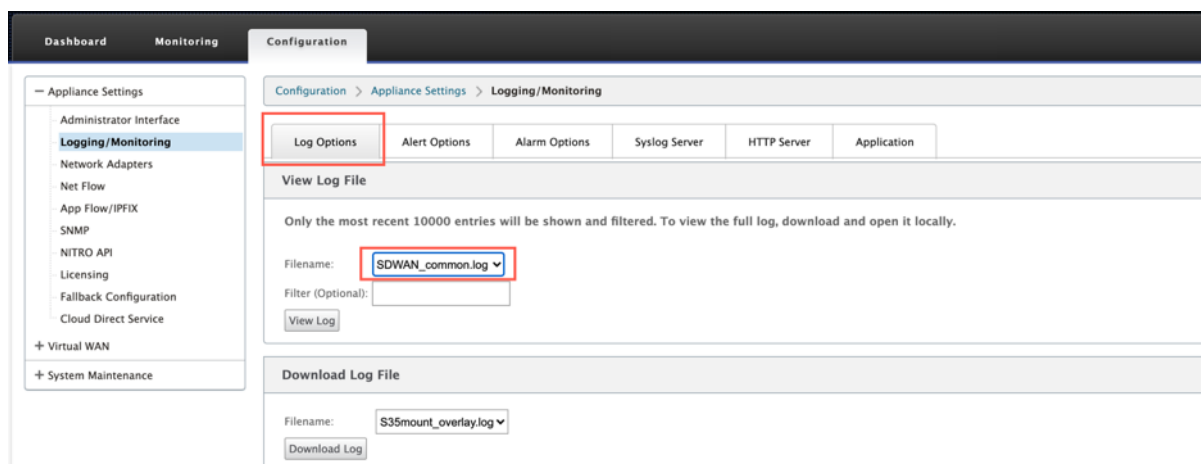
Sélectionnez l'onglet **Groupe de LAG LACP** pour afficher les différents détails relatifs au groupe LAG LACP.



Remarque

Vous ne pouvez pas modifier les paramètres des ports membres individuels, les modifications de configuration apportées au LAG sont automatiquement répercutées sur les ports membres.

Vous pouvez télécharger les fichiers journaux pour un dépannage ultérieur. Accédez à **Configuration > Logging/Surveillance** et sélectionnez **SDWAN_common.log** dans l'onglet **Options du journal**.



Propagation de l'état de liaison

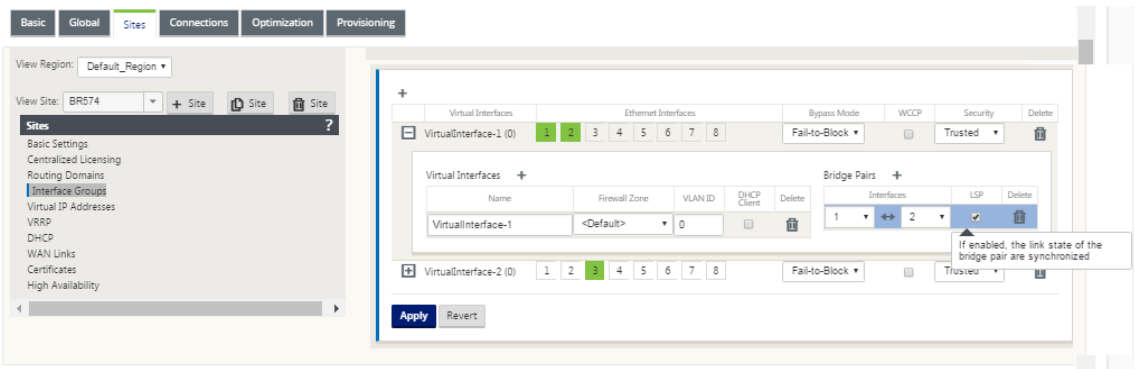
May 6, 2021

La fonctionnalité LSP (Link State Propagation) permet aux administrateurs réseau de garder synchronisé l'état de liaison d'une paire de contournement, ce qui permet aux périphériques attachés de l'autre côté du lien d'afficher lorsque les liens sont inactifs. Lorsqu'un port d'une paire de dérivation devient inactif, la liaison couplée est désactivée administrativement. Si votre architecture réseau inclut un réseau de basculement parallèle, cela force le trafic à effectuer la transition vers ce réseau. Une fois le lien perturbé restauré, son lien correspondant devient automatiquement actif.

Comment configurer la propagation de l'état de lien

Pour configurer la propagation de l'état des liens :

1. Accédez à l'**Éditeur de configuration** > **Sites** > **[Nom du site]** > **Groupes d'interface** .
2. Développez **Interfaces virtuelles** et, sous **Paires de ponts**, cochez la case **LSP** pour activer la **propagation de l'état de liaison** pour une paire de ponts. Cliquez sur **Appliquer** pour enregistrer les paramètres.



Surveillance des statistiques des liens

Pour surveiller les statistiques de liaison :

1. Dans la page **Moniteur > Statistiques**, choisissez **Ethernet dans le menu déroulant Afficher** pour afficher l'état de la paire de ports de contournement avec laquelle la propagation de l'état des liens est activée. Observez que la liaison latérale LAN est en panne et que plus tard, la liaison latérale WAN de la paire de dérivation est désactivée administrativement.

Statistics

Show: Ethernet ☐ Enable Auto Refresh 5 seconds Refresh

Ethernet Statistics

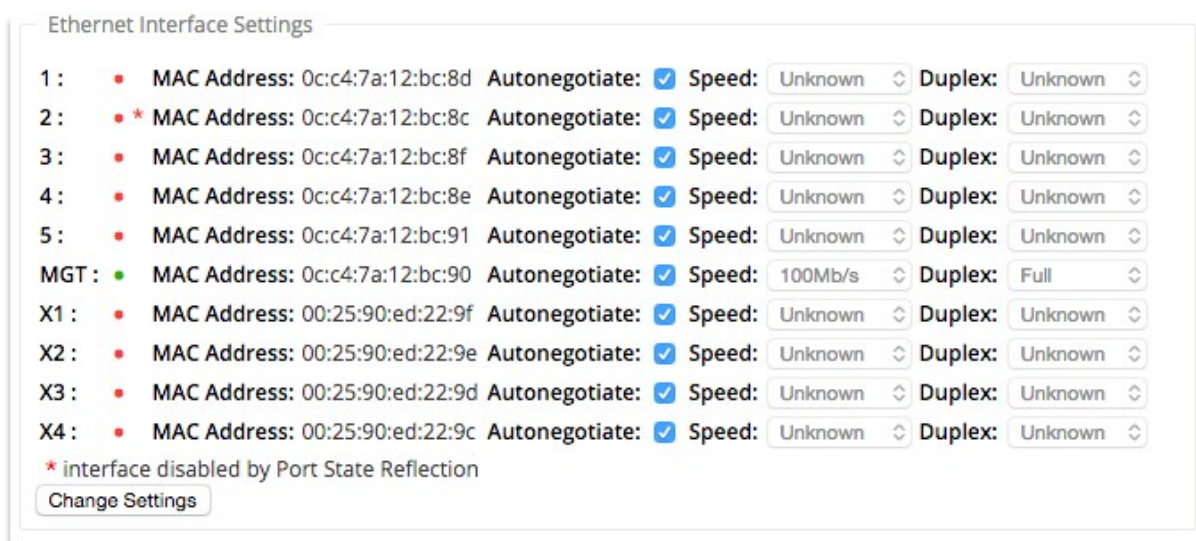
Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries

Port	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
1	DOWN	132885	8755483	212584	15332801	0
2	DISABLED	17984552	1531084459	18189043	1584612144	3258

Showing 1 to 2 of 2 entries

2. Accédez à **Configuration > Paramètres de l'apppliance > Cartes réseau > onglet Ethernet** . Les ports qui sont administrativement en panne sont indiqués par un astérisque rouge (*) dans la liste **Paramètres de l'interface Ethernet** .



Mesure et liens WAN de secours

May 6, 2021

Citrix SD-WAN prend en charge l'activation des liaisons mesurées, qui peuvent être configurées de telle sorte que le trafic utilisateur ne soit transmis que sur une liaison WAN Internet spécifique lorsque toutes les autres liaisons WAN disponibles sont désactivées.

Les liens mesurés conservent la bande passante sur les liens facturés en fonction de l'utilisation. Avec les liens mesurés, vous pouvez configurer les liens en tant que lien Dernier recours, ce qui exclut l'utilisation du lien jusqu'à ce que tous les autres liens non mesurés soient en panne ou dégradés. Définir le dernier recours est généralement activé lorsqu'il y a trois liaisons WAN vers un site (c'est-à-dire MPLS, Internet à large bande, 4G/LTE) et que l'une des liaisons WAN est 4G/LTE et peut être trop coûteuse pour permettre l'utilisation d'une entreprise, sauf si cela est nécessaire. Le comptage n'est pas activé par défaut et peut être activé sur un lien WAN de n'importe quel type d'accès (Internet public/MPLS privé/Intranet privé). Si la mesure est activée, vous pouvez éventuellement configurer les éléments suivants :

- Capuchon de données
- Cycle de facturation (hebdomadaire/mensuel)
- Date de début
- Mode veille
- Priority
- Intervalle de pulsation active : intervalle auquel un message de pulsation est envoyé par une appliance à son homologue à l'autre extrémité du chemin virtuel lorsqu'il n'y a pas eu de trafic (utilisateur/contrôle) sur le chemin pendant au moins un intervalle de pulsation cardiaque

Avec un lien de mesure local, le tableau de bord d'une appliance affiche une table de **mesure de liaison WAN** en bas avec des informations de mesure.

L'utilisation de la bande passante sur une liaison comptée locale est suivie par rapport au plafond de données configuré. Lorsque l'utilisation dépasse 50 %, 75 % ou 90 % de la limite de données configurée, l'appliance génère un événement pour alerter l'utilisateur et une bannière d'avertissement s'affiche en haut du tableau de bord de l'appliance. Cet événement d'alerte d'utilisation peut également être affiché dans SD-WAN Center. Un chemin mesuré peut être formé avec 1 ou 2 liaisons mesurées. Si un chemin est formé entre deux liens mesurés, l'intervalle de pulsation actif utilisé sur le chemin mesuré est le plus grand des deux intervalles de pulsation actifs configurés sur les liens.

Un chemin d'accès mesuré est un chemin d'accès non de secours et est toujours éligible au trafic utilisateur. Lorsqu'il y a au moins un chemin non mesuré qui est dans l'état GOOD, un chemin mesuré transporte la quantité réduite de trafic de contrôle et est évité lorsque le plan de transfert recherche un chemin pour un paquet en double.

Mode veille

Le mode veille d'une liaison WAN est désactivé par défaut. Pour activer le mode veille, vous devez spécifier dans lequel opère l'un des deux modes suivants le lien veille

- **À la demande** : liaison de secours qui devient active lorsque l'une des conditions est remplie.

Lorsque la bande passante disponible dans le chemin virtuel est inférieure à la limite de bande passante à la demande configurée ET que l'utilisation est suffisante. L'utilisation suffisante est définie comme étant supérieure à 95 % (ON_DEMAND_USAGE_THRESHOLD_PCT) de la bande passante disponible actuelle, ou la différence entre la bande passante disponible actuelle et l'utilisation actuelle est inférieure à 250 kbps (ON_DEMAND_THRESHOLD_GAP_KBPS) les deux paramètres peuvent être modifiés à l'aide de t2_variables lorsque tous les paramètres sont morts ou désactivés.

- **Last-resort** - une liaison de secours qui ne devient active que lorsque toutes les liaisons non secours et les liaisons de secours à la demande sont mortes ou désactivées.
- La priorité de secours indique l'ordre dans lequel un lien de secours devient actif, s'il existe plusieurs liens de secours :
 - un lien de secours de priorité 1 devient actif en premier alors qu'un lien de secours de priorité 3 devient actif en dernier
 - Plusieurs liens de secours peuvent être assignés la même priorité

Lors de la configuration d'une liaison de secours, vous pouvez spécifier la priorité de secours et deux intervalles de pulsation :

- **Intervalle de pulsation active** - Intervalle de pulsation utilisée lorsque le chemin de secours est actif (par défaut 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- **Intervalle de pulsation de secours - Intervalle** de pulsation utilisé lorsque le chemin de secours est inactif (par défaut 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/désactivé)

Un chemin de secours est formé avec 1 ou 2 liens de secours.

- **On-Demand** - Un chemin d'attente à la demande est formé entre :
 - une liaison non secours et une liaison de secours à la demande
 - 2 liens de secours à la demande
- **Last-Resort** - Un sentier d'attente de dernière station est formé entre :
 - une liaison non en attente et une liaison en attente de dernier recours
 - une liaison de secours à la demande et une liaison de secours de dernier recours
 - 2 liens de secours de dernier recours

Les intervalles de pulsation utilisés sur un chemin de secours sont déterminés comme suit :

- Si le rythme cardiaque de secours est désactivé sur au moins 1 des 2 liens, le rythme cardiaque est désactivé sur le chemin de secours lorsqu'il est inactif.
- Si le rythme cardiaque de secours n'est pas désactivé sur l'un ou l'autre des liens, la plus grande des deux valeurs est utilisée lorsque le chemin d'attente est en attente.
- Si l'intervalle de pulsation active est configuré sur les deux liens, la plus grande des deux valeurs est utilisée lorsque le chemin de secours est actif.

Messages de rythme cardiaque (garder vivant) :

- Sur un chemin non en veille, les messages de pulsation sont envoyés uniquement lorsqu'il n'y a pas eu de trafic (contrôle ou utilisateur) pendant au moins un intervalle de pulsation. L'intervalle de pulsation varie en fonction de l'état du chemin. Pour les chemins **non en veille et non mesurés** :
 - 50 ms lorsque l'état du chemin est GOOD
 - 25 ms lorsque l'état du chemin est BAD

Sur un chemin de secours, l'intervalle de pulsation utilisé dépend de l'état d'activité et de l'état du chemin :

- Bien qu'inactif, si le rythme cardiaque n'est pas désactivé, les messages de pulsation sont envoyés régulièrement à l'intervalle de pulsation de secours configuré, car aucun autre trafic n'est autorisé.
- l'intervalle de pulsation actif configuré est utilisé lorsque l'état du chemin est GOOD.
- 1/2 l'intervalle de pulsation actif configuré est utilisé lorsque l'état du chemin est BAD.

- Lorsqu'ils sont actifs, comme les chemins non en veille, les messages de pulsation sont envoyés uniquement lorsqu'il n'y a pas eu de trafic (contrôle ou utilisateur) pendant au moins l'intervalle de pulsation actif configuré.
- l'intervalle de pulsation de secours configuré est utilisé lorsque l'état du chemin est GOOD.
- 1/2 l'intervalle de pulsation de secours configuré est utilisé lorsque l'état du chemin est BAD.

Lorsqu'ils sont inactifs, les chemins de secours ne sont pas éligibles pour le trafic utilisateur. Les seuls messages de protocole de contrôle envoyés sur les chemins de secours inactifs sont les messages de pulsation, qui sont destinés à la détection des défaillances de connectivité et à la collecte de mesures de qualité. Lorsque les chemins de secours sont actifs, ils sont éligibles au trafic utilisateur avec un coût de temps supplémentaire. Ceci est fait de sorte que les chemins non en veille, si disponibles, soient favorisés lors de la sélection du chemin de transfert.

L'état du chemin d'accès d'un chemin de secours avec un rythme cardiaque désactivé, alors qu'il est inactif, est supposé être GOOD et il est affiché comme étant GOOD dans le tableau Statistiques du chemin sous **Surveillance**. Lorsqu'il devient actif, contrairement à un chemin non en attente qui commence en état DEAD jusqu'à ce qu'il entende de son homologue Virtual Path, il démarre dans l'état GOOD. Si la connectivité avec le pair Virtual Path n'est pas détectée, le chemin passe BAD, puis DEAD. Si la connectivité avec le pair Virtual Path est rétablie, le chemin passe BAD, puis GOOD à nouveau.

Si un tel chemin de secours devient DEAD et devient inactif, l'état du chemin ne change pas immédiatement à (supposé) GOOD. Au lieu de cela, il est conservé à l'état DEAD pour le temps de sorte qu'il ne peut pas être utilisé immédiatement. Ceci permet d'éviter que l'activité oscille entre un groupe de chemins de priorité inférieure avec des chemins DEAD supposés bons et un groupe de chemins de priorité supérieure avec des chemins réellement GOOD. Cette période d'attente (NO_HB_PATH_ON_HOLD_PERIOD_MS) est définie sur 5 min et peut être modifiée via `t2_variables`.

Si la découverte MTU de chemin est activée sur un chemin virtuel, la MTU du chemin de secours n'est pas utilisée pour calculer la MTU du chemin virtuel pendant que le chemin est en veille. Lorsque le chemin de secours devient actif, le MTU du chemin virtuel est recalculé en tenant compte de la MTU du chemin de secours. (La MTU du chemin virtuel est la plus petite MTU de chemin parmi tous les chemins actifs du chemin virtuel).

Les événements et les messages de journal sont générés lorsqu'un chemin de secours passe entre veille et actif.

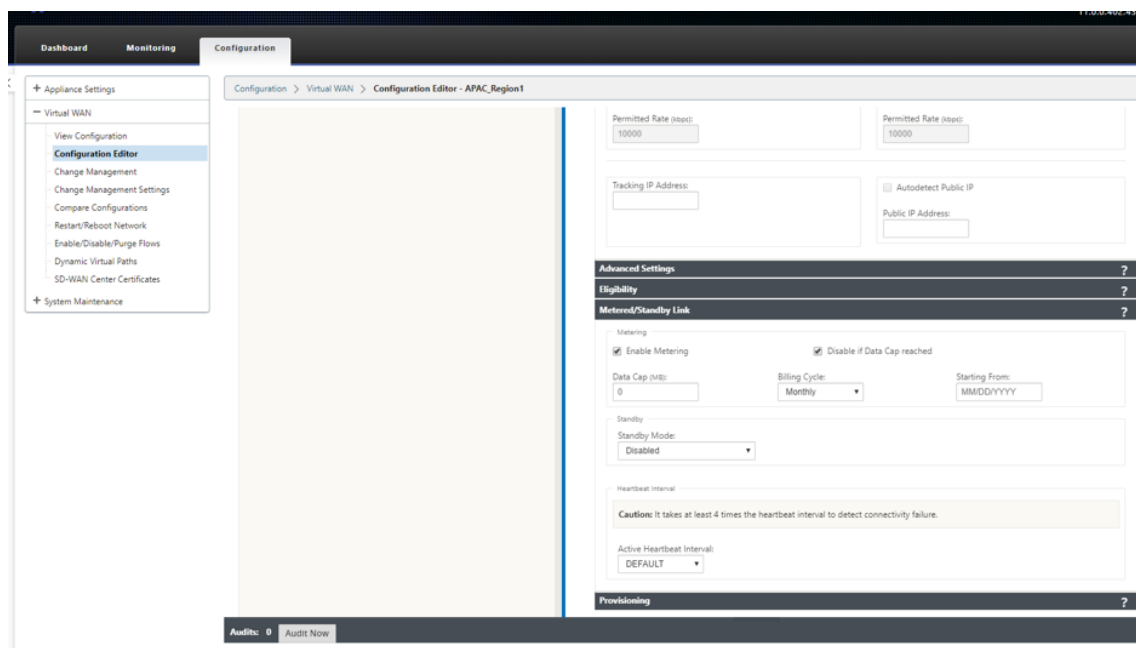
Prérequis pour la configuration :

- Un lien de compteur peut être de n'importe quel type d'accès.
- Tous les liens d'un site peuvent être configurés avec la mesure activée.
- Un lien de secours peut être de type Internet public ou Intranet privé. Une liaison WAN de type d'accès MPLS privé ne peut pas être configurée en tant que liaison de secours.

- Au moins un lien non en veille doit être configuré par site. Un maximum de 3 liens de secours par site est pris en charge.
- Les services Internet/Intranet peuvent ne pas être configurés sur les liens de secours à la demande. Les liens de secours à la demande prennent uniquement en charge le service Virtual Path.
- Le service Internet peut être configuré sur une liaison de secours de dernier recours, mais seul le mode d'équilibrage de charge est pris en charge.
- Le service Intranet peut être configuré sur une liaison de secours de dernier recours, mais seul le mode secondaire est pris en charge et la récupération principale doit être activée.

Pour configurer des liens mesurés :

1. Dans l'interface de gestion Web SD-WAN, accédez à **Configuration > Réseau étendu virtuel** sélectionnez **Éditeur de configuration** ajouter ou sélectionner **Sites** dans la liste déroulante > sélectionnez **Liens WAN** Cliquez sur l'onglet **Lien compteur/veille** pour le développer.



2. Cochez la case **Activer la mesure**. Vous pouvez fournir des valeurs pour la limite de données, la date de début du cycle de facturation, l'utilisation approximative déjà utilisée et l'intervalle de pulsation actif.

Metering

☒ Enable Metering ☒ Disable if Data Cap reached

Data Cap (MB): Billing Cycle: Starting From:

Standby

Standby Mode:

Heartbeat Interval

Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.

Active Heartbeat Interval:

3. Désactiver le lien si la limite de données est atteinte :

- Si la case à cocher **Désactiver le lien si la limite de données est atteinte** est activée, le lien mesuré et tous ses chemins d'accès associés seront désactivés jusqu'au prochain cycle de facturation, si l'utilisation des données atteint la limite de données.
- Par défaut, la case à cocher **Désactiver le lien si la limite de données a atteint** l'état est désactivée, où elle conserve le mode actuel ou l'état défini pour que le lien mesuré soit poursuivi une fois la limite de données atteinte jusqu'au prochain cycle de facturation.

4. Si le lien mesuré est configuré, vous pouvez fournir les données approximatives déjà utilisées en Mo pour le lien mesuré.

Pour suivre l'utilisation appropriée du lien mesuré, vous devez entrer l'utilisation approximative sur le lien mesuré si le lien a déjà été utilisé pendant quelques jours dans le cycle de facturation en cours. Cette utilisation approximative est seulement pour le premier cycle. L'utilisation totale depuis la date de début jusqu'à la date actuelle est calculée et affichée dans le tableau de bord.

Metered/Standby Link ?

Metering

☒ Enable Metering ☒ Disable Link if Data Cap reached

Data Cap (MB): **Approximate Data Already Used (MB):** Billing Cycle: Starting From:

Standby

Standby Mode:

Après avoir effectué la mise à jour de configuration, vous pouvez afficher les détails d'utilisation dans

le tableau de bord.

WAN Link Name:	DC-WL-1
Total Usage:	999.35 MBs of 500 MBs
Data Usage:	0.00 MBs
Control Usage:	999.35 MBs
Usage(in %):	199
Billing Cycle:	MONTHLY
Starting From:	05/06/2020
Days Elapsed:	8 days of 31 days

Pour configurer les liens de secours :

1. Par défaut, le mode veille d'une liaison WAN est désactivé. Pour configurer le lien WAN en mode veille, sélectionnez l'un des modes de veille (Last-Resort/On-Demand) dans la liste déroulante.

The screenshot shows a configuration window for a WAN link. At the top, under the 'Standby' section, there are two dropdown menus: 'Standby Mode' set to 'Last-Resort' and 'Priority' set to '1'. Below this is the 'Heartbeat Interval' section, which contains a yellow caution box stating: 'Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.' Underneath the caution box are two more dropdown menus: 'Active Heartbeat Interval' set to '1 second' and 'Standby Heartbeat Interval' set to '1 second'. At the bottom of the configuration area is a 'Provisioning' button with a question mark icon. Below the entire configuration area are 'Apply' and 'Revert' buttons.

2. Une fois qu'un mode veille est sélectionné, sélectionnez la priorité de secours, l'intervalle de pulsation actif et l'intervalle de pulsation de secours, selon le cas. Cliquez sur **Appliquer** pour valider la configuration.
3. Si une liaison de secours à la demande est configurée, la limite globale de bande passante à la demande par défaut (120 %) est appliquée au chemin d'accès virtuel. Indique la bande passante WAN-to-LAN maximale autorisée pour le chemin virtuel. Elle est exprimée en pourcentage de la bande passante totale fournie par tous les liens non en veille dans le chemin virtuel. Tant que la bande passante disponible dans le chemin d'accès virtuel est inférieure à la limite et si l'utilisation est suffisante, l'apppliance tente d'activer les chemins à la demande pour compléter la bande passante.
4. Pour afficher ou modifier la limite globale de bande passante à la demande par défaut, ouvrez les sections **Global** > Paramètres **réseau WAN virtuel**.

Global Security Settings

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode:

AES 128-Bit

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type:

32-Bit Checksum

☐ Enable FIPS Mode

Network Secure Key:

*

Regenerate

Global Firewall Settings

Global Policy Template:

<None>

Default Firewall Action:

Allow

☐ Default Connection State Tracking

Denied Timeout (s):

30

TCP Initial Timeout (s):

120

TCP Idle Timeout (s):

7440

TCP Closing Timeout (s):

60

TCP Time Wait Timeout (s):

120

TCP Closed Timeout (s):

10

UDP Initial Timeout (s):

30

UDP Idle Timeout (s):

300

ICMP Initial Timeout (s):

30

ICMP Idle Timeout (s):

60

Generic Initial Timeout (s):

30

Generic Idle Timeout (s):

300

Global On-Demand Bandwidth Limit Setting

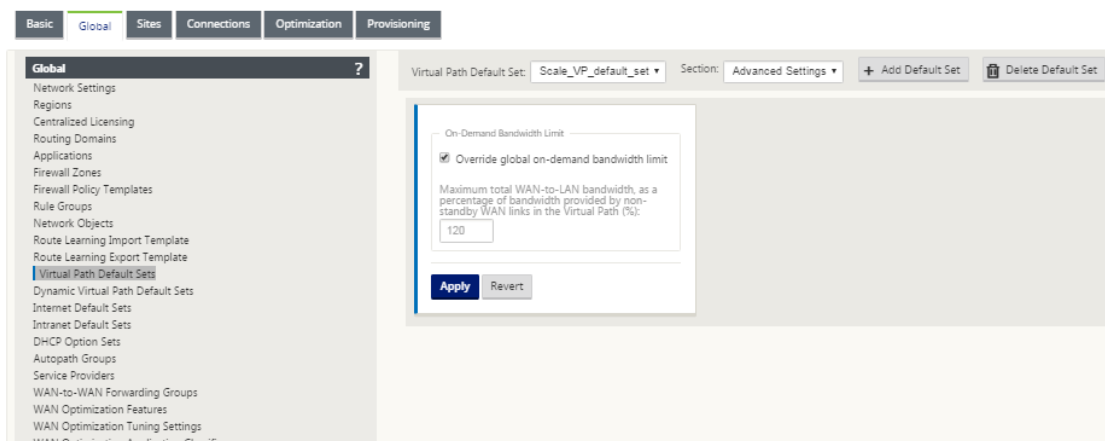
Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%):

120

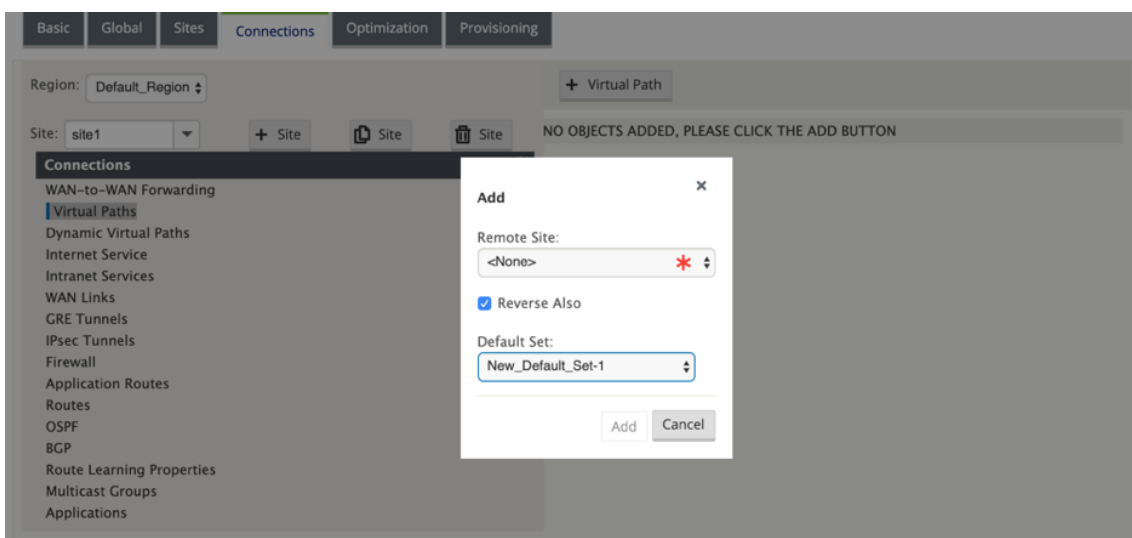
Apply

Refresh

5. Si vous souhaitez appliquer une limite de bande passante à la demande spécifique à un chemin virtuel et conserver le paramètre par défaut global inchangé, un jeu par défaut de chemin virtuel doit être créé et la limite de bande passante à la demande dans les paramètres avancés peut être modifiée.



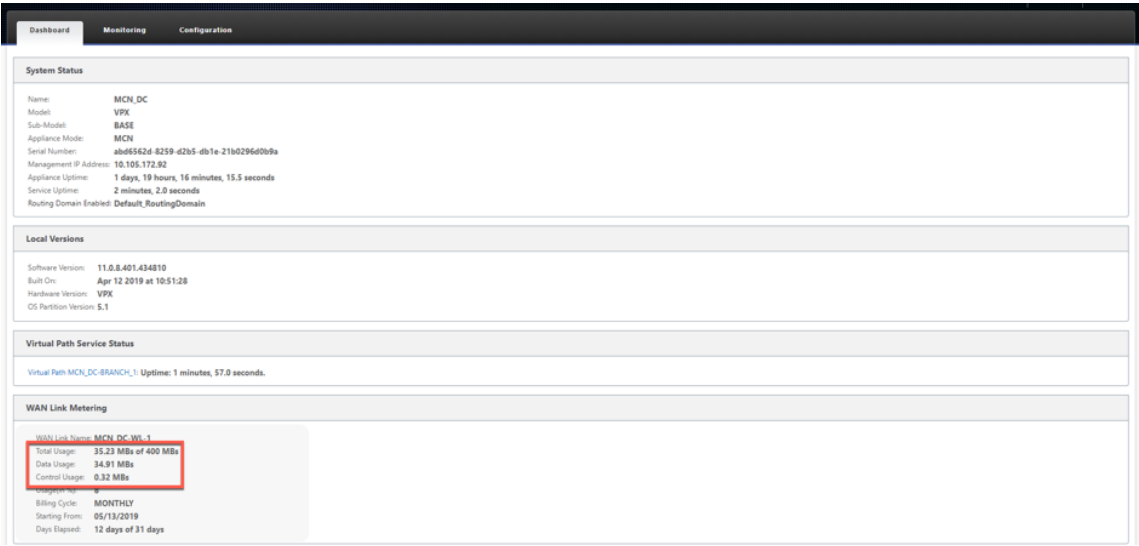
6. Pour appliquer les paramètres d'un chemin virtuel spécifique, accédez à la section **Connexions** > **Chemins virtuels** et cliquez sur **+ Chemin virtuel**.



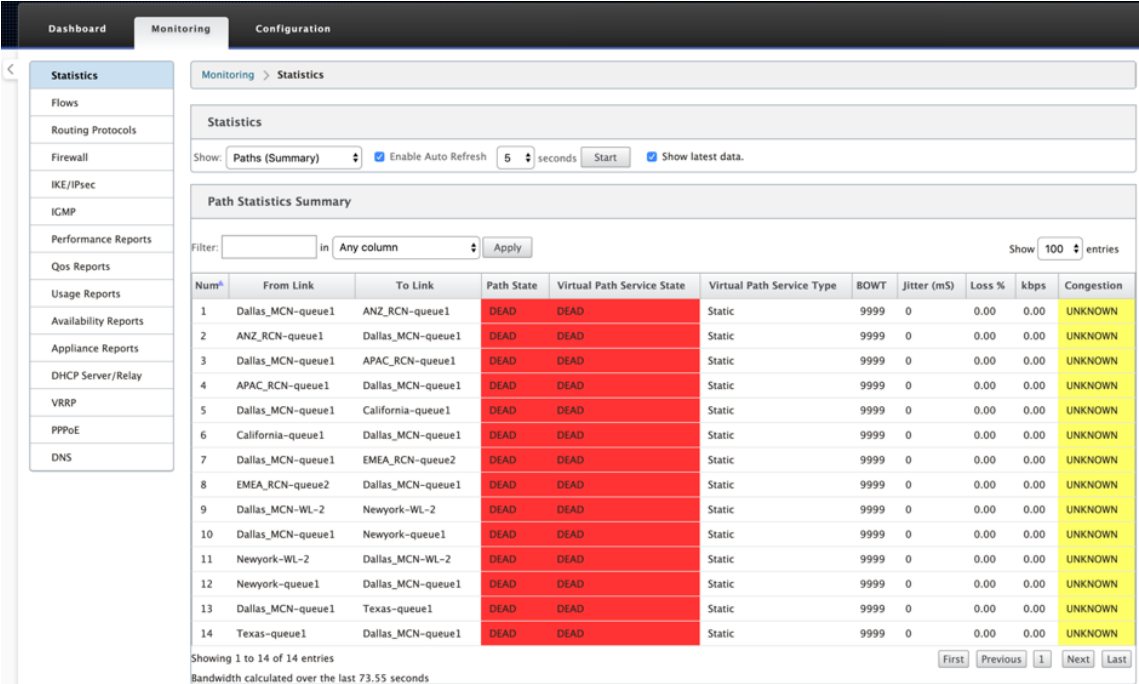
Surveiller les liaisons WAN mesurées et de secours

- La page Tableau de bord fournit les informations de **mesure de liaison WAN** suivantes avec les valeurs d'utilisation :
 - Nom du lien WAN** : Affiche le nom du lien WAN.
 - Utilisation totale** : Affiche l'utilisation totale du trafic (utilisation des données+ utilisation du contrôle).
 - Utilisation des données** : affiche l'utilisation par trafic utilisateur.
 - Contrôle de l'utilisation** : affiche l'utilisation par contrôle du trafic.
 - Utilisation (en%)** : affiche la valeur du plafond des données utilisées en pourcentage (utilisation totale/plafond de données) x 100.
 - Cycle defacturation** : Fréquence de facturation (hebdomadaire/mensuelle)

- **À partir de** : Date de début du cycle de facturation
- **Jours écoulés** : Temps écoulé (en jours, heures, minutes et secondes)



- Lorsque les statistiques de chemin (**Surveillance > Statistiques > Chemins**) sont affichées, les liens mesurés et les liens de secours sont marqués comme indiqué dans la capture d’écran.



- Si l’appliance dispose d’un chemin virtuel comportant une liaison de secours à la demande locale ou distante, lorsque les statistiques d’utilisation des liaisons WAN sont affichées, un tableau supplémentaire indiquant la bande passante à la demande s’affiche au bas de la page (**Surveillance > Statistiques > Utilisation des liaisons WAN**).

Local WAN-to-LAN On Demand WAN Link Usages

Filter: in Any column Apply

Show entries Showing 0 to 0 of 0 entries First Previous Next Last

Adaptive Bandwidth Detection										
WAN Link	WAN Link Mode	Standby Priority	Configured	Minimum Acceptable BW Kbps	Maximum Allowed BW Kbps	Current Allowed BW Kbps	Virtual Path Name	Virtual Path On Demand Bandwidth Limit Kbps	Virtual Path Available Bandwidth Kbps	In Use
No data available in table										

Showing 0 to 0 of 0 entries First Previous Next Last

Bandwidth calculated over the last 5.078 seconds

- Lorsque l'utilisation sur un lien mesuré dépasse 50 % de la limite de données configurée, une bannière d'avertissement s'affiche en haut du tableau de bord. En outre, si l'utilisation dépasse 75 % de la limite de données configurée, les informations de mesure numérique vers le bas du tableau de bord sont mises en surbrillance.

The data usage on the following Metered Wanlinks have reached the threshold:
• BR1-WL1-New : 75%.

System Status

Name: BR1

Model: VPX

Sub-Model: BASE

Appliance Mode: Client

Serial Number: 9a4f580b-7527-8dee-fbec-9824a89142e6

Management IP Address: 10.105.184.72

Appliance Uptime: 10 hours, 7 minutes, 34.6 seconds

Service Uptime: 9 hours, 17 minutes, 53.0 seconds

Routing Domain Enabled: Default, RoutingDomain

Local Versions

Configuration Created On: Thu Apr 18 20:08:57 2019

Software Version: 11.5.13.401.434810

Built On: Apr 18 2019 at 19:35:14

Hardware Version: VPX

OS Partition Version: 5.1

Virtual Path Service Status

Virtual Path DC-BR1 Uptime: 9 hours, 17 minutes, 43.0 seconds.

WAN Link Metering

WAN Link Name: BR1-WL1-New

Total Usage: 329.58 MBs of 400 MBs

Data Usage: 258.09 MBs

Control Usage: 71.48 MBs

UsageIn %: 82

Billing Cycle: MONTHLY

Starting From: 07/17/2019

Days Elapsed: 3 days of 31 days

Un événement d'utilisation de liaison WAN est également généré au niveau de l'apppliance lorsque l'utilisation dépasse 50 %, 75 % et 90 % du plafond de données configuré.

17654	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:22:58	USAGE_3	WARNING	Total usage 1.84 Gbytes used (91% of limit 2.00 Gbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17653	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:17:58	USAGE_2	WARNING	Total usage 1.52 Gbytes used (75% of limit 2.00 Gbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17652	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:09:58	USAGE_1	WARNING	Total usage 1.00 Gbytes used (50% of limit 2.00 Gbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017

- Lorsqu'un chemin de secours passe entre l'état de veille et l'état actif, un événement est généré par l'apppliance.

24640	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become standby
24639	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become standby
24638	1	RL-TB-CL2-WL-1->RL-TB-MCN-WL-2	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-2 state has changed from BAD to GOOD because notified by peer.
24637	2	RL-TB-MCN-WL-2->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24636	2	RL-TB-MCN-RL-TB-CL2	VIRTUAL PATH	2017-05-26 10:18:27	GOOD	NOTICE	The state of Virtual Path RL-TB-MCN-RL-TB-CL2 has changed from BAD to GOOD
24635	0	RL-TB-CL2-WL-1->RL-TB-MCN-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-1 state has changed from BAD to GOOD because notified by peer.
24634	0	RL-TB-MCN-WL-1->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24633	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become active
24632	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become active

2. Les intervalles de pulsation actifs et de secours configurés pour chaque chemin peuvent être affichés dans **Configuration > Réseau étendu virtuel > Afficher la configuration > Chemins d'accès**.

Dashboard

Monitoring

Configuration

+ Appliance Settings

- Virtual WAN

View Configuration

Configuration Editor

Change Management

Change Management Settings

Compare Configurations

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

+ System Maintenance

Configuration > Virtual WAN > View Configuration

Configuration

View: Paths

Path Configuration

Paths on virtual path 3 'Dallas_MCN-ANZ_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	ANZ_RCN-queue1	192.168.1.10	192.168.90.10	-	-	4980	4980	
0	ANZ_RCN-queue1	Dallas_MCN-queue1	192.168.90.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	ANZ_RCN-queue1	YES	YES	YES	0	n/a	n/a
ANZ_RCN-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 8 'Dallas_MCN-APAC_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	APAC_RCN-queue1	192.168.1.10	192.168.80.10	-	-	4980	4980	
0	APAC_RCN-queue1	Dallas_MCN-queue1	192.168.80.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	APAC_RCN-queue1	YES	YES	YES	0	n/a	n/a
APAC_RCN-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 9 'Dallas_MCN-California':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	California-queue1	192.168.1.10	192.168.50.10	-	-	4980	4980	
0	California-queue1	Dallas_MCN-queue1	192.168.50.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	California-queue1	YES	YES	YES	0	n/a	n/a
California-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 12 'Dallas_MCN-EMEA_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	EMEA_RCN-queue2	192.168.1.10	17.1.1.10	-	-	4980	4980	
0	EMEA_RCN-queue2	Dallas_MCN-queue1	17.1.1.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	EMEA_RCN-queue2	YES	YES	YES	0	n/a	n/a
EMEA_RCN-queue2	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 13 'Dallas_MCN-Newyork':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
1	Dallas_MCN-queue1	Newyork-queue1	192.168.1.10	192.168.70.10	-	-	4980	4980	
0	Dallas_MCN-WL-2	Newyork-WL-2	192.168.10.10	192.168.60.10	-	-	4980	4980	
0	Newyork-WL-2	Dallas_MCN-WL-2	192.168.60.10	192.168.10.10	-	-	4980	4980	
1	Newyork-queue1	Dallas_MCN-queue1	192.168.70.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	Newyork-queue1	YES	YES	YES	0	n/a	n/a
Dallas_MCN-WL-2	Newyork-WL-2	YES	YES	YES	0	n/a	n/a
Newyork-WL-2	Dallas_MCN-WL-2	YES	YES	YES	0	n/a	n/a
Newyork-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 14 'Dallas_MCN-Texas':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	Texas-queue1	192.168.1.10	192.168.40.10	-	-	4980	4980	
0	Texas-queue1	Dallas_MCN-queue1	192.168.40.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	Texas-queue1	YES	YES	YES	0	n/a	n/a
Texas-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Optimisation d'Office 365

November 1, 2021

Les fonctionnalités d'**optimisation Office 365** respectent les [principes de connectivité réseau de Microsoft Office 365](#), afin d'optimiser Office 365. Office 365 est fourni en tant que service via plusieurs points de terminaison de service (portes d'entrée) situés dans le monde entier. Pour obtenir une expérience utilisateur optimale pour le trafic Office 365, Microsoft recommande de rediriger le trafic Office365 directement vers Internet à partir d'environnements de succursales. Évitez les pratiques telles que le retour vers un proxy central. Le trafic Office 365, tel qu'Outlook, Word, sont sensibles à la latence et le trafic de retour introduit plus de latence, ce qui entraîne une mauvaise expérience utilisateur. Citrix SD-WAN vous permet de configurer des stratégies pour ventiler le trafic Office 365 vers Internet.

Le trafic Office 365 est dirigé vers le point de terminaison de service Office 365 le plus proche, qui existe à la périphérie de l'infrastructure Microsoft Office 365 dans le monde entier. Une fois que le trafic atteint une porte d'entrée, il passe sur le réseau de Microsoft et atteint la destination réelle. Il réduit la latence au fur et à mesure que le temps aller-retour entre le réseau client et le point de terminaison Office 365 diminue.

Points de terminaison Office 365

Les points de terminaison Office 365 sont un ensemble d'adresses réseau et de sous-réseaux. Les points de terminaison Office 365 sont classés en catégories **Optimiser**, **Autoriser** et **Par défaut**. Citrix SD-WAN 11.4.0 fournit une classification plus granulaire des catégories **Optimiser** et **Autoriser**, permettant de réserver sélectivement pour améliorer les performances du trafic Office 365 sensible au réseau. La direction du trafic sensible au réseau vers le SD-WAN dans le cloud (Cloud Direct ou un VPX SD-WAN sur Azure), ou d'un périphérique SD-WAN domestique vers un SD-WAN situé à proximité avec une connectivité Internet plus fiable, permet une qualité de service de qualité de service et une résilience de connexion supérieure par rapport à la simple direction du trafic vers le plus proche Porte d'entrée Office 365, au prix d'une augmentation de la latence. Une solution SD-WAN réservée avec QoS réduit les abandons et les déconnexions VoIP, réduit la gigue et améliore les scores d'opinion moyenne de qualité médiatique pour Microsoft Teams :

- **Optimisation** : ces terminaux fournissent une connectivité à tous les services et fonctionnalités Office 365 et sont sensibles à la disponibilité, aux performances et à la latence. Il représente plus de 75 % de la bande passante, des connexions et du volume de données Office 365. Tous les points de terminaison Optimizer sont hébergés dans les centres de données Microsoft. Les demandes de service à ces points de terminaison doivent sortir de la branche vers Internet et ne doivent pas passer par le centre de données.

La catégorie **Optimiser** est classée dans les sous-catégories suivantes :

- 1 - Teams Realtime
- 2 - Exchange Online
- 3 - SharePoint Optimize

Pour plus d'informations sur les considérations relatives à la mise à [niveau](#), consultez [Considérations importantes](#)

- **Autoriser** : ces points de terminaison fournissent uniquement la connectivité aux services et fonctionnalités Office 365 spécifiques, et ne sont pas sensibles aux performances du réseau et à la latence. La représentation de la bande passante et du nombre de connexions Office 365 est également plus faible. Ces points de terminaison sont hébergés dans les centres de données Microsoft. Les demandes de service à ces points de terminaison peuvent s'échapper de la branche vers Internet ou passer par le centre de données.

La catégorie **Autoriser** est classée dans les sous-catégories suivantes :

- 1 - Teams TCP Fallback
- 2 - Exchange Mail
- 3 - SharePoint Allow
- 4 - Office365 Common

Pour plus d'informations sur les considérations relatives à la mise à [niveau](#), consultez [Considérations importantes](#)

Remarque

La sous-catégorie **Teams Realtime** utilise le protocole de transport en temps réel UDP pour gérer le trafic Microsoft Teams, tandis que la sous-catégorie **Teams TCP Fallback** utilise le protocole de couche de transport TCP. Comme le trafic multimédia est fortement sensible à la latence, vous pouvez préférer ce trafic pour emprunter le chemin le plus direct possible et utiliser UDP au lieu de TCP comme protocole de couche de transport (transport le plus préféré pour les médias interactifs en temps réel en termes de qualité). Bien que UDP soit un protocole privilégié pour le trafic multimédia Teams, certains ports doivent être autorisés dans le pare-feu. Si les ports ne sont pas autorisés, le trafic Teams utilise TCP comme solution de secours, et l'activation de l'optimisation pour Teams TCP Fallback garantit une meilleure livraison de l'application Teams dans ce scénario. Pour plus d'informations, consultez [Flux d'appels Microsoft Teams](#).

- **Par défaut** : ces points de terminaison fournissent des services Office 365 qui ne nécessitent aucune optimisation et peuvent être traités comme du trafic Internet normal. Certains de ces points de terminaison peuvent ne pas être hébergés dans les centres de données Microsoft. Le trafic de cette catégorie n'est pas sensible aux variations de latence. Par conséquent, la rupture directe de ce type de trafic ne provoque aucune amélioration des performances par rapport à la panne Internet. En outre, le trafic dans cette catégorie peut ne pas toujours être du trafic Office

365. Par conséquent, il est recommandé de désactiver cette option lors de l'activation de la répartition Office 365 dans votre réseau.

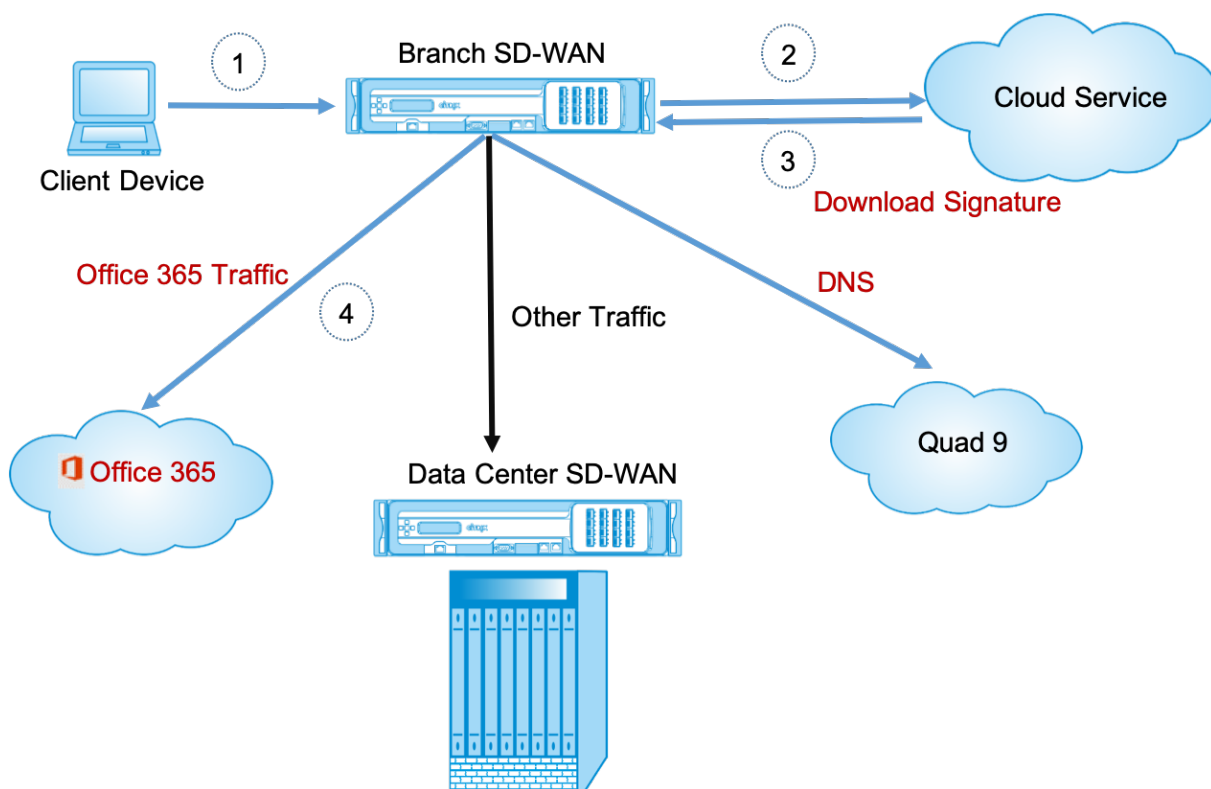
Fonctionnement de l'optimisation Office 365

Les signatures de point de terminaison Microsoft sont mises à jour au maximum une fois par jour. L'agent de l'appliance interroge quotidiennement le service Citrix (sdwan-app-routing.citrixnetworkapi.net) pour obtenir le dernier ensemble de signatures de point de terminaison. L'appliance SD-WAN interroge le service Citrix (sdwan-app-routing.citrixnetworkapi.net), une fois par jour, lorsque l'appliance est activée. Si de nouvelles signatures sont disponibles, l'appliance les télécharge et les stocke dans la base de données. Les signatures sont essentiellement une liste d'URL et d'adresses IP utilisées pour détecter le trafic Office 365 en fonction des stratégies de direction du trafic qui peuvent être configurées.

Remarque

À l'exception de la catégorie Office 365 par défaut, la détection et la classification des premiers paquets du trafic Office 365 sont effectuées par défaut, que la fonctionnalité de répartition d'Office 365 soit activée ou non.

Lorsqu'une demande pour l'application Office 365 arrive, le classificateur d'applications effectue une première recherche de base de données de classificateur de paquets, identifie et marque le trafic Office 365. Une fois que le trafic Office 365 est classé, la route d'application créée automatiquement et les stratégies de pare-feu prennent effet et répartit le trafic directement vers Internet. Les requêtes DNS Office 365 sont transférées à des services DNS spécifiques tels que Quad9. Pour plus d'informations, consultez la section [Système de noms de domaine](#).



Les signatures sont téléchargées depuis Cloud Service (sdwan-app-routing.citrixnetworkapi.net).

Configurer la ventilation Office 365

La stratégie de répartition Office 365 vous permet de spécifier la catégorie de trafic Office 365 que vous pouvez extraire directement de la succursale. En activant le découpage Office 365 et la compilation de la configuration, un objet DNS, un objet d'application, un itinéraire d'application et un modèle de stratégie de pare-feu sont automatiquement créés et appliqués aux sites de succursales avec le service Internet.

Conditions préalables

Assurez-vous que vous disposez des éléments suivants :

1. Pour effectuer une panne Office 365, un service Internet doit être configuré sur l'apppliance. Pour plus d'informations sur la configuration du service Internet, consultez [Accès Internet](#).
2. Assurez-vous que l'interface de gestion est connectée à Internet.

Vous pouvez utiliser l'interface Web Citrix SD-WAN pour configurer les paramètres de l'interface de gestion.

3. Assurez-vous que le DNS de gestion est configuré. Pour configurer le DNS de l'interface de gestion, accédez à **Configuration > Paramètres du matériel > Carte réseau**. Sous la section **Paramètres DNS**, fournissez les détails du serveur DNS principal et secondaire, puis cliquez sur **Modifier les paramètres**.

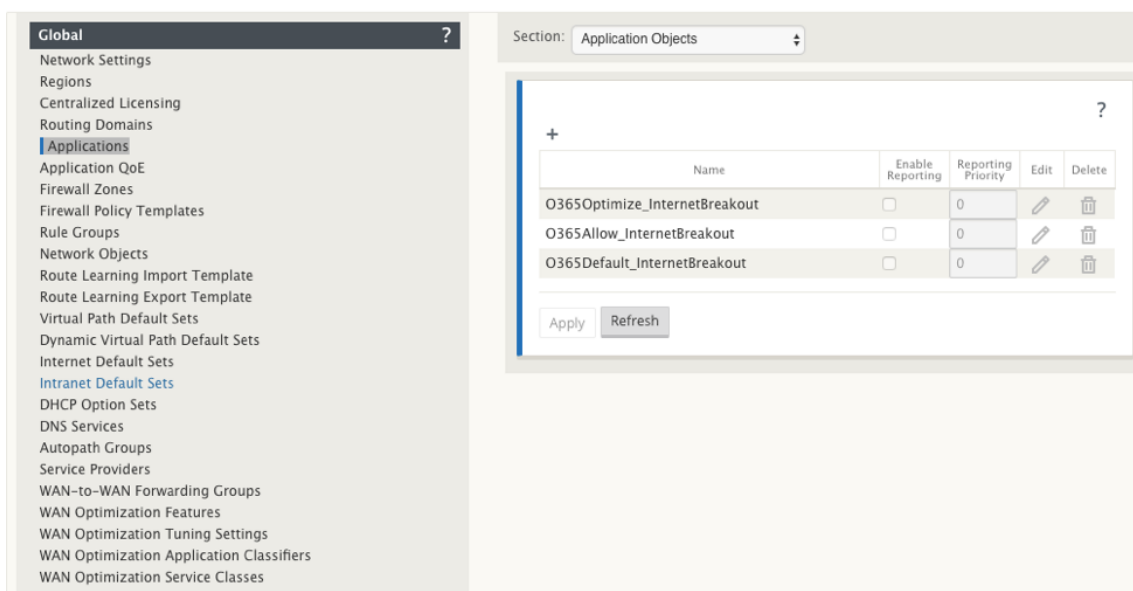
The screenshot shows the 'Configuration > Appliance Settings > Network Adapters' page. The 'Management Interface IP' section is expanded, showing 'DHCP' (disabled) and 'Manual' settings. The 'Manual' section has input fields for IP Address (10.105.147.52), Subnet Mask (255.255.255.0), and Gateway IP Address (10.105.147.1). Below this, the 'DNS Settings' section is highlighted with a red box. It contains input fields for 'Primary DNS' and 'Secondary DNS', and 'Change Settings' and 'Clear Settings' buttons.

Le paramètre de **stratégie de répartition Office 365** est disponible dans les paramètres globaux, sélectionnez la catégorie Office 365 requise pour la répartition Internet et cliquez sur **Appliquer**.

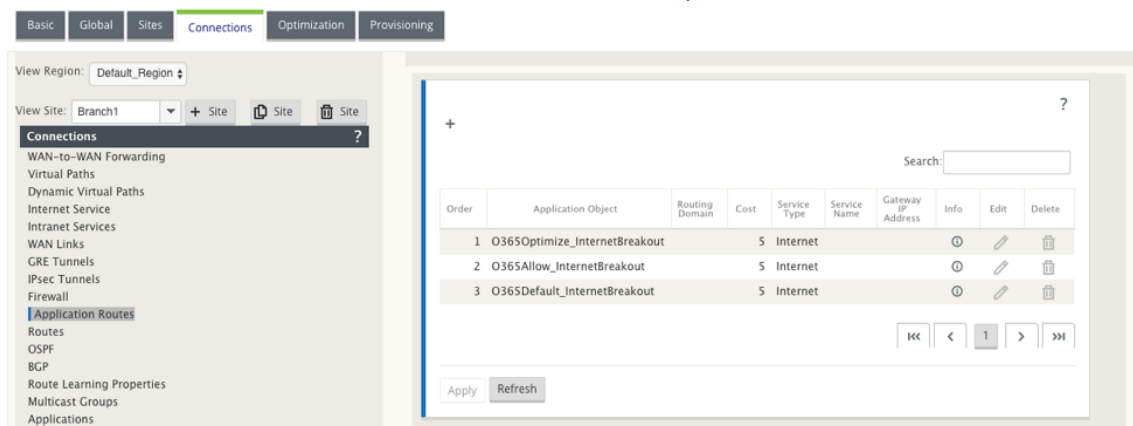
The screenshot shows the 'Global' settings page. The 'Policy Settings' section is highlighted with a blue box. It contains a table with columns 'O365 URL Category' and 'Direct Internet Breakout From Branch'. The table has three rows: 'Optimize' (checked), 'Allow' (checked), and 'Default' (unchecked). Below the table are 'Apply' and 'Revert' buttons.

Après avoir configuré les paramètres de stratégie Office 365 décomposer et compiler la configuration. Les paramètres suivants sont renseignés automatiquement.

- **Objet DNS** : l'objet DNS spécifie le type de trafic à transférer vers le service DNS configuré par l'utilisateur. Les requêtes DNS sont entendues sur toutes les interfaces approuvées, et les redirections DNS sont inclus pour diriger les requêtes DNS Office 365 vers le service Quad9. Cette règle de redirection prend la priorité la plus élevée. Pour plus d'informations, consultez la section **Service de noms de domaine**.
- **Objet Application** - Un objet application avec la catégorie ou la sous-catégorie Office 365 sélectionnée par l'utilisateur est créé. Si vous avez sélectionné la catégorie **Par défaut** et les sous-catégories **Optimiser** et **Autoriser**, les objets d'application correspondants sont créés comme illustré dans la capture d'écran suivante :



- **Route de l'application** : un itinéraire d'application est créé pour chacun des objets d'application Office 365 avec le type de service Internet. Pour plus d'informations sur les considérations relatives à la mise à [niveau](#), consultez [Considérations importantes](#)



- **Modèle de stratégie de pré-appliance de pare-feu** : un modèle de stratégie globale de pré-appliance est créé pour chaque catégorie Office 365 configurée. Ce modèle est appliqué à tous les sites de succursale disposant d'un service Internet. La stratégie de pré-appliance prend la priorité sur les modèles de stratégie locale et post-appliance. Pour plus d'informations sur les considérations relatives à la mise à [niveau](#), consultez [Considérations importantes](#)

Section: Policies

Pre-Appliance Template Policies

Template	Routing Domain	Action	Zones		Application	Application Family	Application Objects	IP Protocol	DSCP	Source			Destination			Match Est.	Reverse Also	Info
			From	To						Service	IP Address	Port	Service	IP Address	Port			
O365Optimize_In...	*	Allow	*	*	*	*	O365Optimize_InternetBreakout	Any	*	*	*	*	*	*	*	*		
O365Allow_Inter...	*	Allow	*	*	*	*	O365Allow_InternetBreakout	Any	*	*	*	*	*	*	*	*		
O365Default_Int...	*	Allow	*	*	*	*	O365Default_InternetBreakout	Any	*	*	*	*	*	*	*	*		

Transparent Transparent pour Office 365

La branche se décompose pour Office 365 commence par une requête DNS. La requête DNS passant par les domaines Office 365 doit être orientée localement. Si la panne Internet Office 365 est activée, les routes DNS internes sont déterminées et la liste transparente des redirecteurs est renseignée automatiquement. Les demandes DNS Office 365 sont transférées au service DNS open source Quad 9 par défaut. Le service DNS Quad 9 est sécurisé, évolutif et a une présence multi-pop. Vous pouvez modifier le service DNS si nécessaire.

Des redirecteurs transparents pour les applications Office 365 sont créés dans toutes les succursales où le service Internet et le service Office 365 sont activés.

Si vous utilisez un autre proxy DNS ou si le SD-WAN est configuré en tant que proxy DNS, la liste des redirecteurs est automatiquement remplie avec des redirecteurs pour les applications Office 365.

BasicGlobalSitesConnectionsOptimizationProvisioning

View Region: Default_Region

View Site: Branch-CB2K + Site Site Site

Sites ?

- Basic Settings
- Centralized Licensing
- Routing Domains
- Interface Groups
- Virtual IP Addresses
- VRRP
- DHCP
- WAN Links
- Certificates
- High Availability
- DNS

Section: DNS Transparent Forwarders

Order	Application	DNS Service	Delete
100	Office 365 Optimize(offic...	Quad9	
200	Office 365 Allow(office36...	Quad9	
300	Office 365 Default(office...	Quad9	

Apply Refresh

Considérations importantes pour la mise à niveau

Optimiser et autoriser les catégories

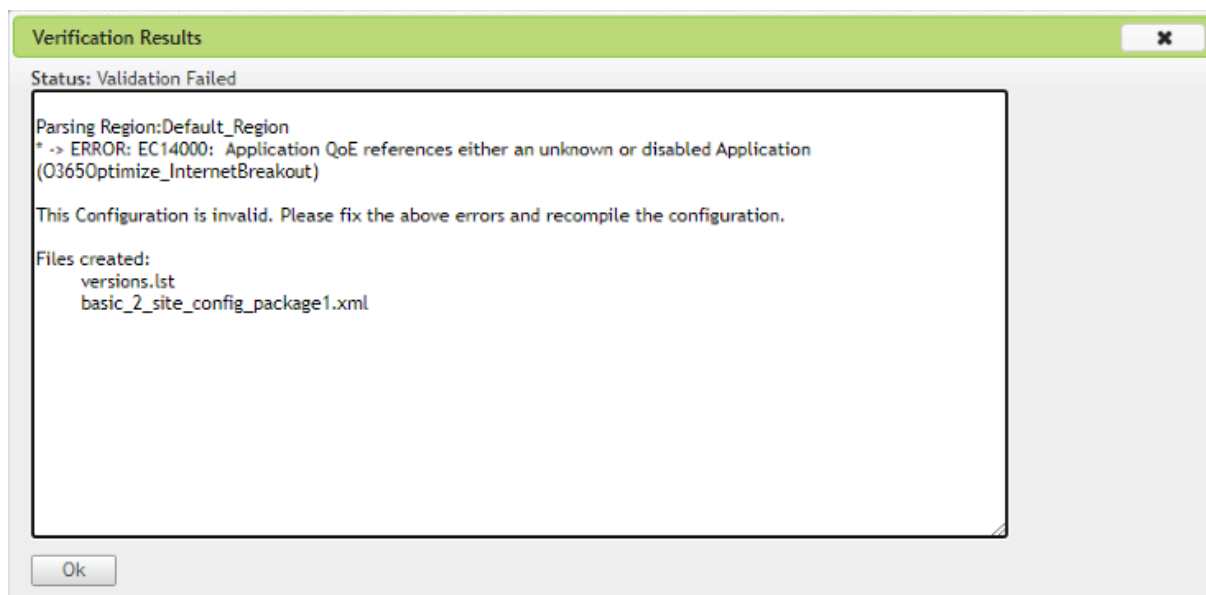
Si vous avez activé la stratégie de répartition Internet pour les catégories **Optimiser** et **Autoriser** Office 365, Citrix SD-WAN active automatiquement la stratégie de déclassement Internet pour les sous-catégories correspondantes lors de la mise à niveau vers Citrix SD-WAN 11.4.0.

Lorsque vous rétrogradez vers une version logicielle antérieure à Citrix SD-WAN 11.4.0, vous devez activer manuellement la répartition Internet pour la catégorie **Optimiser** ou **Autoriser** Office 365, que vous ayez activé les sous-catégories correspondantes dans la version 11.4.0 de Citrix SD-WAN ou pas.

Objets d'application Office 365

Si vous avez créé des règles/routes à l'aide des objets d'application générés automatiquement **O365Optimize_InternetBreakout** et **O365allow_InternetBreakout**, assurez-vous de supprimer les règles/routes avant la mise à niveau vers Citrix SD-WAN 11.4.0. Après la mise à niveau, vous pouvez créer des règles/itinéraires à l'aide des nouveaux objets d'application correspondants.

Si vous procédez à la mise à niveau Citrix SD-WAN 11.4.0 sans supprimer les règles/itinéraires, une erreur s'affiche et, par conséquent, la mise à niveau échoue. Dans l'exemple ci-dessous, un utilisateur a configuré un profil Application QoE et voit une erreur lors de la tentative de mise à niveau vers Citrix SD-WAN 11.4.0 sans supprimer les règles/routes :



Si vous avez créé des règles de proxy DNS ou des règles de transfert transparent DNS à l'aide des applications **Office 365 Optimisation** et **Office 365 Autoriser**, assurez-vous de supprimer les règles avant de procéder à la mise à niveau vers Citrix SD-WAN 11.4.0. Après la mise à niveau, vous pouvez à nouveau créer les règles en utilisant les nouvelles applications correspondantes.

Remarque

Cette activité ne s'applique pas aux règles DNS créées automatiquement. Elle s'applique uniquement aux règles DNS que vous avez créées.

Vous pouvez surveiller les statistiques de l'application Office 365 dans les rapports de statistiques SD-WAN suivants :

- | Connections | | Source | | | | | | | | | | Destination | | | | | | | | | | Related | | | | | | | | | |
|-----------------------|---|--------|-------------|-------------|-------|--------------|-------------------|------------------|---------------|------|--------------|------------------|---------------|-------------|---------|-------|-------|----------|--------|---------|---------------|-----------------|-------|---|---|---|--|--|--|--|--|
| Routing Domain | Application * | Family | IP Protocol | IP Address | Port | Service Type | Service Name | Zone | IP Address | Port | Service Type | Service Name | Zone | State | In MB/s | Sent | | Received | | Age (s) | Last Activity | Related Objects | | | | | | | | | |
| | | | | | | | | | | | | | | | | Bytes | Pkts | Bytes | Pkts | | | | | | | | | | | | |
| Default_RoutingDomain | Windows LiveUpdateSvc | WinV | TCP | 172.17.0.10 | 5682 | Local | VirusProtection-1 | Default_LAN_Zone | 52.121.251.30 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 1886 | 0071 | 0.071 | 13 | 6764 | 0.226 | 21 | 3900 | View Flow Rule NAT2 (Doc) | | | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 5682 | Local | VirusProtection-1 | Default_LAN_Zone | 52.126.244.40 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 54 | 7076 | 0.737 | 0.072 | 54 | 1330 | 0.064 | 1431 | 2880 | View Flow Rule NAT2 (Doc) | | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 60302 | Local | VirusProtection-1 | Default_LAN_Zone | 13.67.6.171 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 1385 | 82355 | 3.411 | 22.480 | 68935 | 614 | 16.274 | 20 | 4402 | View Flow Rule NAT2 (Doc) | | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 45040 | Local | VirusProtection-1 | Default_LAN_Zone | 13.67.6.171 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 63 | 2500 | 0.251 | 0.796 | 72 | 1414 | 0.267 | 6489 | 21 | 3262 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 60862 | Local | VirusProtection-1 | Default_LAN_Zone | 13.67.6.171 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 391 | 13193 | 0.805 | 24.401 | 42 | 35662 | 0.853 | 6.606 | 42 | 1417 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 60201 | Local | VirusProtection-1 | Default_LAN_Zone | 60.168.102.43 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 22 | 4258 | 0.075 | 0.116 | 17 | 1064 | 0.058 | 3.038 | 42 | 1008 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 56279 | Local | VirusProtection-1 | Default_LAN_Zone | 52.126.284.40 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 28 | 8489 | 0.317 | 0.769 | 23 | 10399 | 0.260 | 0.808 | 48 | 2836 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 56279 | Local | VirusProtection-1 | Default_LAN_Zone | 52.126.284.40 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 68 | 7984 | 0.341 | 0.717 | 72 | 1966 | 0.821 | 1.385 | 48 | 2919 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 60201 | Local | VirusProtection-1 | Default_LAN_Zone | 52.108.61.41 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 21 | 4378 | 0.492 | 1.539 | 13 | 1008 | 0.859 | 1.740 | 23 | 1363 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Office 365 ConsumerEAS(anonymous) | WinV | TCP | 172.17.0.10 | 56262 | Local | VirusProtection-1 | Default_LAN_Zone | 45.129.132.43 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 88 | 15423 | 0.217 | 0.745 | 29 | 24058 | 0.175 | 1.167 | 166 | 8262 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | MicrosoftConnect | WinV | TCP | 172.17.0.10 | 80207 | Local | VirusProtection-1 | Default_LAN_Zone | 13.67.6.103 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 27 | 7121 | 0.034 | 0.198 | 42 | 14963 | 0.141 | 0.279 | 20 | 887 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | MicrosoftConnect | WinV | TCP | 172.17.0.10 | 45040 | Local | VirusProtection-1 | Default_LAN_Zone | 52.223.308.40 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 24 | 3618 | 0.064 | 0.115 | 19 | 963 | 0.078 | 0.216 | 20 | 877 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | MicrosoftConnect | WinV | TCP | 172.17.0.10 | 60301 | Local | VirusProtection-1 | Default_LAN_Zone | 23.94.143.93 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 14 | 196 | 0.083 | 0.064 | 3 | 969 | 0.019 | 0.036 | 20 | 4015 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Microsoft Skype for Business (Anonymous) Local Only (Office 365) (Unauthenticated) | WinV | TCP | 172.17.0.10 | 56277 | Local | VirusProtection-1 | Default_LAN_Zone | 13.67.6.123 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 21 | 2336 | 0.284 | 0.224 | 12 | 1347 | 0.299 | 1.481 | 74 | 7883 | View Flow Rule NAT2 (Doc) | | | | | |
| Default_RoutingDomain | Microsoft Skype for Business (Anonymous) Remote Only (Office 365) (Unauthenticated) | WinV | TCP | 172.17.0.10 | 60201 | Local | VirusProtection-1 | Default_LAN_Zone | 52.174.644.40 | 443 | Internet | Winsock-Internet | Internet_Zone | ESTABLISHED | Yes | 16 | 5435 | 0.367 | 0.835 | 11 | 1060 | 0.211 | 0.475 | | | | | | | | |

- © 1999–2024 Cloud Software Group, Inc. All rights reserved. 552

Flows Data														
LAN to WAN Flows														
Details	Routing Domain	Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Hit Count	Service Type	Service Name	Age (mS)	Packets	Bytes	PPS	Application
+	Optimize	172.147.100.146	52.98.65.178	57930	443	TCP	4	INTERNET	-	120979	3	156	0.000	outlook
+	Optimize	172.147.100.146	13.107.18.11	57931	443	TCP	15	INTERNET	-	26513	14	1683	0.018	outlook
+	Optimize	172.147.100.146	13.107.42.11	57891	443	TCP	20	INTERNET	-	8418	19	1903	0.036	outlook
+	Optimize	172.147.100.146	40.100.136.146	57926	443	TCP	14	INTERNET	-	730	13	2118	0.036	outlook
+	Optimize	172.147.100.146	40.97.229.82	57918	443	TCP	15	INTERNET	-	1229	14	2178	0.036	outlook
+	Optimize	172.147.100.146	52.98.65.178	57929	443	TCP	4	INTERNET	-	121224	3	156	0.000	outlook
+	Optimize	172.147.100.146	34.203.255.247	51236	443	TCP	5	INTERNET	-	599759	4	164	0.000	okta
+	Optimize	172.147.100.146	34.203.255.247	51237	443	TCP	4	INTERNET	-	592420	3	123	0.000	okta
+	Optimize	172.147.100.146	13.107.6.156	51298	443	TCP	29	INTERNET	-	42061	28	11416	0.018	office365_common
+	Optimize	172.147.100.146	20.190.140.51	57935	443	TCP	16	INTERNET	-	24735	15	4184	0.018	office365_common
+	Optimize	172.147.100.146	13.67.50.225	57897	443	TCP	3	INTERNET	-	2250	2	81	0.047	office365_common
+	Optimize	172.147.100.146	13.67.50.225	51228	443	TCP	4	INTERNET	-	603355	3	123	0.000	office365_common
+	Optimize	172.147.100.146	13.107.6.156	51255	443	TCP	249	INTERNET	-	377061	248	85307	0.000	office365_common
+	Optimize	172.147.100.146	52.109.124.84	57939	443	TCP	20	INTERNET	-	22933	19	4679	0.018	office365_common
+	Optimize	172.147.100.146	13.67.50.225	51346	443	TCP	3	INTERNET	-	5900	2	81	0.044	office365_common

• Statistiques DNS

Dashboard	Monitoring	Configuration
Statistics	Monitoring > DNS	
Flows		
Routing Protocols		
Firewall		
IKE/IPsec		
IGMP		
Performance Reports		
QoS Reports		
Usage Reports		
Availability Reports		
Appliance Reports		
DHCP Server/Relay		
VRRP		
PPPoE		
DNS		
DNS Statistics		
Refresh		
Proxy Statistics		
Search:		
Proxy Name	Application Name	DNS Service Name
DNS_Proxy1	office365_optimize	Quad9
DNS_Proxy1	office365_allow	Quad9
DNS_Proxy1	office365_default	Quad9
DNS_Proxy1	Any	Google
Showing 1 to 4 of 4 entries		
Transparent Forwarder Statistics		
Search:		
Application Name	DNS Service Name	DNS Service Active
office365_allow	Quad9	YES
office365_default	Quad9	YES
office365_optimize	Quad9	YES
Showing 1 to 3 of 3 entries		

• Statistiques des itinéraires d’application

Monitoring > Statistics
Statistics
Show: Application Routes Enable Auto Refresh 5 seconds Stop Clear Counters on Refresh Processing...
Application Route Statistics
Maximum allowed routes: 64000
Application Routes for routing domain : Default_RoutingDomain
Filter: in Any column Apply
Show 100 entries Showing 1 to 3 of 3 entries
First Previous 1 Next Last
Num Application Object Gateway IP Address Service Firewall Zone Reachable Site Type Cost Hit Count Eligible Eligibility Type Eligibility Value
0 O365Optimize_InternetBreakout * Internet Internet_Zone YES Branch1 Static 5 1792 YES N/A N/A
2 O365Allow_InternetBreakout * Internet Internet_Zone YES Branch1 Static 5 1395 YES N/A N/A
1 O365Default_InternetBreakout * Internet Internet_Zone YES Branch1 Static 5 0 YES N/A N/A
Showing 1 to 3 of 3 entries
First Previous 1 Next Last

Vous pouvez également afficher les statistiques des applications Office 365 dans le rapport Application SD-WAN Center.

Routing Domain: Any

ApplicationsHDXApp QoEMOSServicesClassesSitesVirtual PathsPathsWAN LinksMPLS QueuesEthernetGREIPsecEvents

Report Type: Top ApplicationsSelect Site:

Show Bandwidth/Data in KbpsKBFilters: +

10 / pageShowing 1 - 10 of 12Search

Application Name	Aggregate Data	Aggregate Outgoing Data	Aggregate Incoming Data	Average Bandwidth	Average Outgoing Bandwidth	Average Incoming Bandwidth
Office 365 Common	644.22	445.29	198.93	28.63	19.79	8.84
Microsoft Office 365	440.82	21.42	419.40	19.59	0.95	18.64
Microsoft Outlook (Office 365)	264.79	31.72	233.07	11.77	1.41	10.36
Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)	215.94	178.94	37.00	9.60	7.95	1.64
Microsoft SharePoint Online (Office 365)	28.48	6.09	22.39	1.27	0.27	0.99
Google Generic	24.09	3.63	20.46	3.21	0.48	2.73
Microsoft	13.29	4.01	9.28	0.59	0.18	0.41
Domain Name Service	6.30	6.30	0.00	0.42	0.42	0.00

Résolution des problèmes

Vous pouvez consulter l’erreur de service dans la section **Événements** de l’appliance SD-WAN.

Pour vérifier les erreurs, accédez à **Configuration > Maintenance du système > Diagnostics**, cliquez sur l’onglet **Événements**.

DashboardMonitoringConfiguration

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

Insert Event

Object Type: USER EVENT

Event type: UNDEFINED

Severity: DEBUG

Add Event

S’il y a un problème lors de la connexion au service Citrix (sdwan-app-routing.citrixnetworkapi.net), le message d’erreur se reflète sous la table **Afficher les événements**.

View Events

Quantity: 25

Filter: Object Type = APPLICATIONSEvent type = FAILURESeverity = ERROR

Reload Events Table

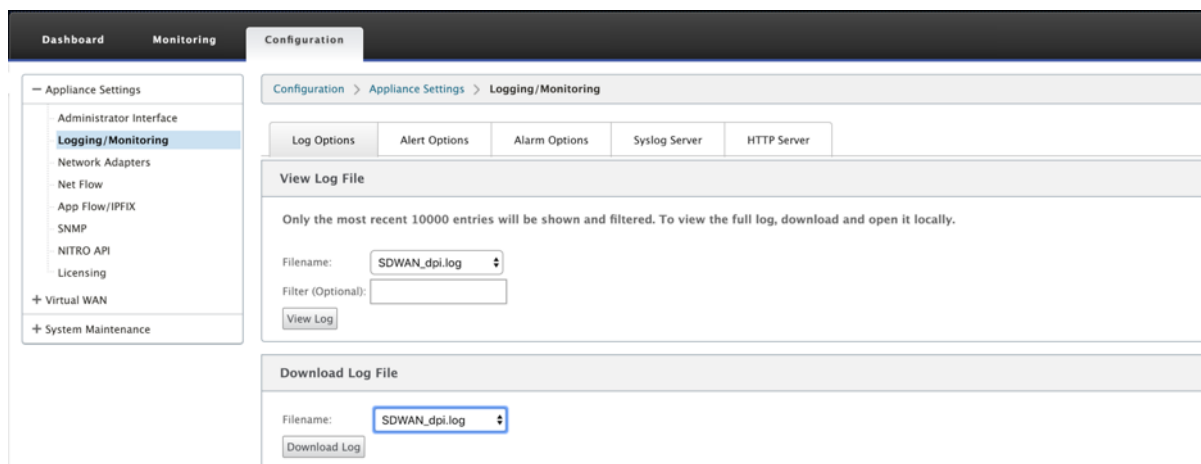
ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API

Times are in UTC

Les erreurs de connectivité sont également enregistrées dans **SDWAN_DPI.log**. Pour afficher le journal, accédez à **Configuration > Paramètres du matériel > Journalisation/surveillance > Options**

du journal. Sélectionnez le **fichier SDWAN_dpi.log** dans la liste déroulante, puis cliquez sur **Afficher le journal**.

Vous pouvez également télécharger le fichier journal. Pour télécharger le fichier journal, sélectionnez le fichier journal requis dans la liste déroulante sous la section **Télécharger le fichier journal**, puis cliquez sur **Télécharger le journal**.



Limitations

- Si la stratégie de répartition Office 365 est configurée, l'inspection approfondie des paquets n'est pas effectuée sur les connexions destinées à la catégorie configurée d'adresses IP.
- La stratégie de pare-feu créée automatiquement et les routes d'application ne sont pas modifiables.
- La stratégie de pare-feu créée automatiquement a la priorité la plus faible et n'est pas modifiable.
- Le coût de l'itinéraire pour l'itinéraire d'application créé automatiquement est de cinq. Vous pouvez le remplacer par un itinéraire à moindre coût.

Service de balises Office 365

Microsoft fournit le service de balise Office 365 pour mesurer l'accessibilité d'Office 365 via les liens WAN. Le service de balise est essentiellement une URL - sdwan.measure.office.com/apc/trans.png, qui est analysée à intervalles réguliers. Le sondage est effectué sur chaque appliance pour chaque liaison WAN activée par Internet. Avec chaque sonde, une requête HTTP est envoyée au service de balises et une réponse HTTP est attendue. La réponse HTTP confirme la disponibilité et la disponibilité du service Office 365.

Citrix SD-WAN vous permet non seulement d'effectuer un sondage de balises, mais également de déterminer la latence nécessaire pour atteindre les points de terminaison Office 365 via chaque li-

aison WAN. La latence est le temps aller-retour nécessaire pour envoyer une demande et obtenir une réponse du service de balises Office 365 via une liaison WAN. Cela permet aux administrateurs réseau d'afficher le rapport de latence du service de balises et de choisir manuellement le meilleur lien Internet pour la distribution directe d'Office 365. Le sondage de balise est activé uniquement via Citrix SD-WAN Orchestrator. Par défaut, le sondage de balise est activé sur toutes les liaisons WAN activées par Internet lorsque la sortie d'Office 365 est activée via Citrix SD-WAN Orchestrator.

Remarque

L'exploration de balises Office 365 n'est pas activée sur les liens mesurés.

Vous pouvez choisir de désactiver l'exploration de balises Office 365 et d'afficher les rapports de latence sur SD-WAN Orchestrator. Pour plus d'informations, consultez la section [Optimisation d'Office 365](#).

Pour désactiver le service de balise Office 365, dans SD-WAN Orchestrator, au niveau du réseau, accédez à **Configuration > Routage > Stratégies de routage > Paramètres d'optimisation réseau O365** et **désactivez Activer le service Beacon**.

Network Configuration : Routing Policies

Cost Ranges: Custom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)

Application Group Match Criteria

Match Type: Application Group Application Group *

Scope: Global Route Site / Group Specific Route

Traffic Steering: Internet Breakout

Delivery Service: Internet Breakout

O365 Network Optimization Settings

[Review Office 365 Network Connectivity Principles](#)

☐ Optimize: (Enable optimization for highly latency sensitive O365 services eg: Exchange, Sharepoint, Skype for Business, Teams etc)

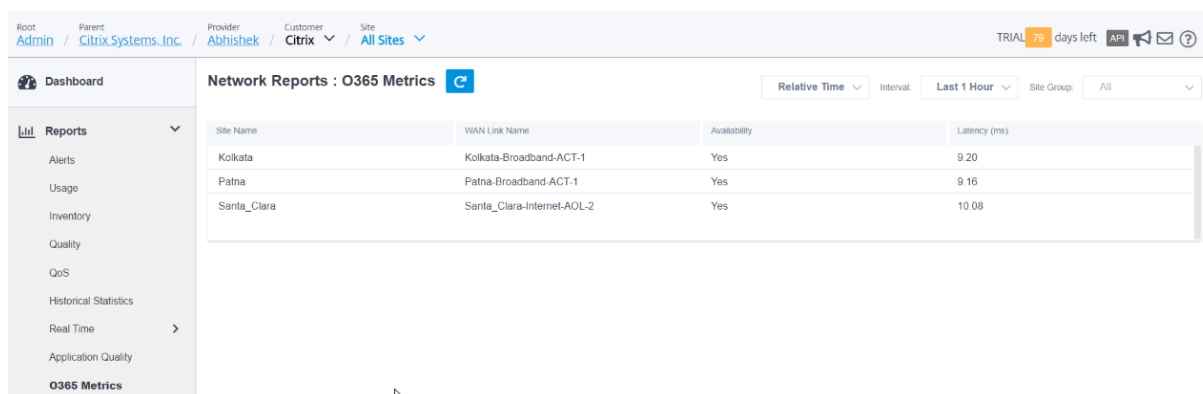
☐ Allow: (Enable optimization for less latency sensitive O365 services eg: "https://protection.outlook.com", "https://accounts.accesscontrol.windows.net")

☐ Default: (No optimization required for O365 services in this category eg: "https://odc.officeapps.live.com", "https://appexin.stb.s-man.com")

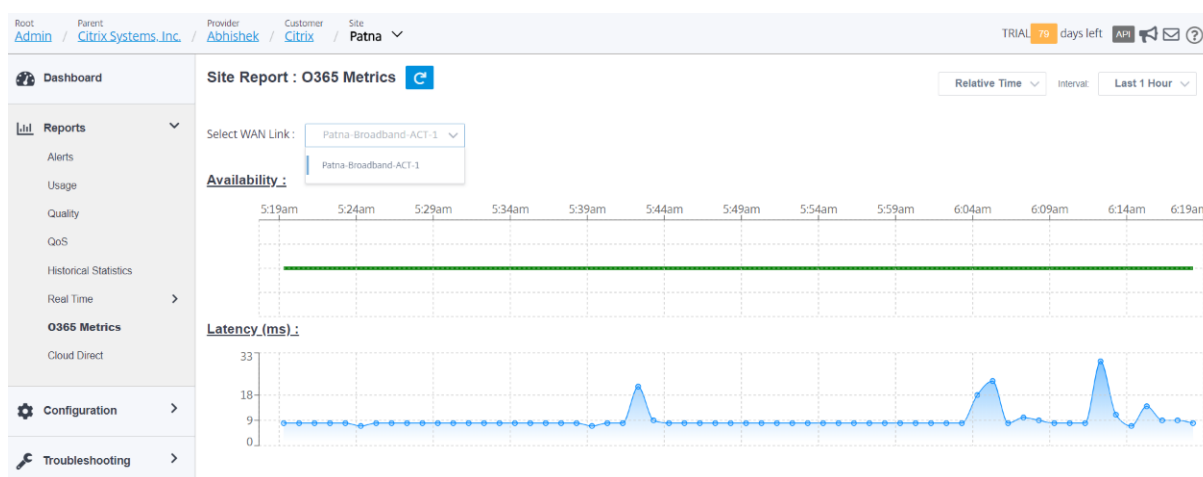
☒ Enable Beacon Service

Cancel Save

Pour afficher les rapports de disponibilité et de latence de sondage des indicateurs, dans Citrix SD-WAN Orchestrator, au niveau du réseau, accédez à **Rapports > Metrics O365**.



Pour afficher un rapport détaillé au niveau du site sur le service de balise, dans SD-WAN Orchestrator, accédez au niveau du site à **Rapports > Metrics O365**.



Optimisation des services Citrix Cloud et Gateway

August 31, 2022

Grâce à l'amélioration des fonctionnalités d'**optimisation du service Citrix Cloud and Gateway**, vous pouvez détecter et acheminer le trafic destiné à Citrix Cloud et Gateway Service. Vous pouvez créer des stratégies pour rompre le trafic vers Internet directement ou, pour l'envoyer via un itinéraire de backhaul via un chemin virtuel. En l'absence de cette fonctionnalité, lorsque l'itinéraire par défaut est un chemin virtuel, le service de passerelle reprend le centre de données du client, puis se rendra sur Internet en ajoutant une latence inutile. En outre, vous bénéficiez désormais d'une visibilité sur le service Citrix Gateway et le trafic Citrix Cloud et vous pouvez créer des stratégies QoS pour le hiérarchiser sur le chemin virtuel.

La fonctionnalité de sortie Citrix Cloud and Gateway Service est activée par défaut dans le logiciel Citrix SD-WAN version 11.2.1 et ultérieure.

Pour la version logicielle Citrix SD-WAN inférieure à la version 11.3.0, la première détection de paquets et la classification du trafic Citrix Cloud and Gateway Service sont effectuées uniquement si la fonctionnalité d'introduction Citrix Cloud and Gateway Service n'est pas désactivée.

Pour le logiciel Citrix SD-WAN version 11.3.0 et ultérieure, la première détection de paquets et la classification du trafic Citrix Cloud and Gateway Service sont effectuées, que la fonctionnalité de dépister Citrix Cloud and Gateway Service soit activée ou non.

Remarque

- Vous pouvez configurer l'optimisation Citrix Cloud et Gateway Service uniquement via Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section [Optimisation des Gateway Service](#).
- L'**optimisation du trafic Citrix SD-WAN Orchestrator** est introduite à partir du logiciel Citrix SD-WAN version 11.2.3 ou supérieure. L'objectif est de fournir une classification plus granulaire, et donc d'identifier séparément le trafic Citrix SD-WAN Orchestrator et le trafic d'autres services dépendants provenant de Citrix Cloud, et de fournir une option de dépannage Internet. Par conséquent, les clients peuvent désormais choisir d'optimiser uniquement le trafic Citrix SD-WAN Orchestrator.
- À partir de Citrix SD-WAN 11.4.3, les signatures de trafic du service Citrix SD-WAN Orchestrator sont mises en package avec la version du logiciel de l'appliance et chargées sur l'appliance pendant le processus de préparation de la gestion des modifications à partir du service Citrix SD-WAN Orchestrator. Cette étape permet de surmonter toutes les limitations susceptibles d'empêcher l'appliance de télécharger les signatures à partir du service Citrix SD-WAN Orchestrator après l'installation initiale ou la mise à niveau logicielle.

Catégories Citrix Cloud et Gateway Service

Voici les catégories de trafic utilisées à des fins de classification et d'optimisation :

- **Citrix Cloud** : permet de détecter et d'acheminer le trafic destiné à l'interface utilisateur Web et aux API Citrix Cloud.
 - Citrix SD-WAN Orchestrator et services critiques dépendants :
 - * **Citrix SD-WAN Orchestrator** : permet une sortie directe sur Internet du rythme cardiaque et d'autres trafic requis pour établir et maintenir la connectivité entre l'appliance Citrix SD-WAN et Citrix SD-WAN Orchestrator.
 - * **Citrix Cloud Download Service** : permet de télécharger directement sur Internet le logiciel, la configuration, les scripts, etc. sur l'appliance Citrix SD-WAN.

- **Service Citrix Gateway** : permet de détecter et d’acheminer le trafic (contrôle et données) destiné au service Citrix Gateway.
- **Données client du service de passerelle** : permet la diffusion directe sur Internet des tunnels de données ICA entre les clients et le service Citrix Gateway. Il nécessite une bande passante élevée et une faible latence.
- **Données du serveur de service de passerelle** : permet la diffusion directe sur Internet des tunnels de données ICA entre Virtual Delivery Agents (VDA) et Citrix Gateway Service. Elle nécessite une bande passante élevée et une faible latence et n’est pertinente que dans les emplacements de ressources VDA (connexions VDA à Citrix Gateway Service).
- **Trafic de contrôle de service de passerelle** : permet la diffusion directe du trafic de contrôle sur Internet. Aucune considération QoS spécifique.
- **Trafic proxy Web du service de passerelle** : Active la répartition directe du trafic de proxy Web par Internet. Il nécessite une bande passante élevée, mais les exigences de latence peuvent varier.

Surveillance

Vous pouvez surveiller les statistiques du service de passerelle dans les rapports de statistiques SD-WAN suivants :

- Statistiques de pare-feu

Connections																										
Application				Source				Destination				Sent				Received										
Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	In NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	Age (Sec)	Last Activity (Sec)	Related Objects	Clear Connection	
Citrix Cloud Web UI and AffinityCloudWebUIApp	Custom Application	TCP	10.23.1.5	1216	Local	VP-1-LAN-1	Default_LAN_Zone	52.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	825	0.270	0.254	6	4081	0.231	1.216	26	21849	[See File][See File](Post-Route NAT)	Clear
Domain Name Service(DNS)	Network Service	UDP	10.23.1.5	51545	Local	VP-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	70	0.009	0.002	1	188	0.009	0.061	26	21518	See File(Post-Route NAT)	Clear
Domain Name Service(DNS)	Network Service	UDP	10.23.1.5	59926	Local	VP-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	75	0.003	0.000	1	230	0.003	0.061	30	30268	[See File][See File](Post-Route NAT)	Clear
Citrix Cloud Web UI and AffinityCloudWebUIApp	Custom Application	TCP	10.23.1.5	1214	Local	VP-1-LAN-1	Default_LAN_Zone	52.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	825	0.246	0.232	6	4081	0.211	1.149	28	28317	[See File][See File](Post-Route NAT)	Clear
Domain Name Service(DNS)	Network Service	UDP	10.23.1.5	62851	Local	VP-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	71	0.005	0.000	1	148	0.005	0.042	28	28423	[See File][See File](Post-Route NAT)	Clear
Citrix Gateway service Client DataSyncClientData	Web	UDP	10.23.1.5	51546	Local	VP-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	13	2132	0.587	0.661	13	4514	0.509	1.413	26	18831	See File(Post-Route NAT)	Clear
Citrix Gateway service Client DataSyncClientData	Web	TCP	10.23.1.5	1223	Local	VP-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	166	18005	8.875	7.701	247	137819	13.206	58.990	19	4	See File(Post-Route NAT)	Clear
Citrix Cloud Web UI and AffinityCloudWebUIApp	Custom Application	TCP	10.23.1.5	1125	Local	VP-1-LAN-1	Default_LAN_Zone	52.177.88.75	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	45	21131	0.541	0.530	43	21389	0.135	0.536	319	32242	[See File][See File](Post-Route NAT)	Clear
Connections Displayed: 8																										
Connections in Use: 46/138000																										

Connections																										
Application				Source				Destination				Sent				Received										
Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	In NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	Age (Sec)	Last Activity (Sec)	Related Objects	Clear Connection	
Citrix Cloud Download Service(CitrixCloudDownloadSvc)	Web	TCP	172.16.30.30	40082	Local	VP-1-LAN-1	Default_LAN_Zone	54.236.77.239	80	Internet	BRANCH1_KVMNTP-Internet	Internet_Zone	SYN_SENT	Yes	3	380	0.834	0.400	0	0	0.000	0.000	4	157	See File(Post-Route NAT)	Clear
Citrix SD-WAN Orchestrator(CitrixOrchestrator)	Web	TCP	172.16.30.30	34934	Local	VP-1-LAN-1	Default_LAN_Zone	18.213.26.194	443	Internet	BRANCH1_KVMNTP-Internet	Internet_Zone	CLOSED	Yes	11	1384	1.903	1.611	12	6668	2.076	9.251	6	3678	See File(Post-Route NAT)	Clear
Domain Name Service(DNS)	Network Service	UDP	172.16.30.30	43158	Local	VP-1-LAN-1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMNTP-BRANCH1_KVMNTP	Any	ESTABLISHED	No	2	512	0.400	0.202	2	156	0.400	0.261	4	4149	[See File]	Clear
Domain Name Service(DNS)	Network Service	UDP	172.16.30.30	45885	Local	VP-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMNTP-Internet	Internet_Zone	ESTABLISHED	Yes	2	574	0.274	0.191	2	388	0.274	0.426	7	6743	[See File][See File](Post-Route NAT)	Clear
Domain Name Service(DNS)	Network Service	UDP	172.16.30.30	39958	Local	VP-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMNTP-Internet	Internet_Zone	ESTABLISHED	Yes	2	384	0.537	0.352	2	388	0.537	0.790	4	3843	[See File][See File](Post-Route NAT)	Clear
Google ConnectivityManager	Web	TCP	172.16.30.30	56534	Local	VP-1-LAN-1	Default_LAN_Zone	172.217.31.206	80	Virtual Path	MCN_KVMNTP-BRANCH1_KVMNTP	Any	CLOSED	No	6	394	1.526	0.801	1	796	1.271	1.819	4	3718	[See File]	Clear
Connections Displayed: 6																										
Connections in Use: 6/138000																										

- Flux

Monitoring > Flows

Select Flows

Flow Type: LAN to WAN, WAN to LAN, Internet Load Balancing Table, TCP Termination Table

Max Flows to Display: 50

Filter (Optional): Internet

Default

Flows Data

Both LAN to WAN and WAN to LAN Flows

1	172.16.70.5	40.112.143.211	LAN to WAN	49027	443	TCP	default	10	INTERNET	-	LOCAL	6421	9	940	1.362	1.770	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	ngs_client_data
2	172.16.70.4	9.9.9	LAN to WAN	54577	53	UDP	default	2	INTERNET	-	LOCAL	8646	1	74	0.116	0.000	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A
3	172.16.70.5	52.188.75.17	LAN to WAN	63914	443	TCP	default	2	INTERNET	-	LOCAL	3398198	1	160	0.000	0.000	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	https
4	172.16.70.4	40.112.143.211	LAN to WAN	50231	443	TCP	default	9	INTERNET	-	LOCAL	1079	8	906	7.106	6.438	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	ngs_client_data
5	172.16.70.4	40.112.143.211	LAN to WAN	50231	443	TCP	default	9	INTERNET	-	LOCAL	6461	8	906	1.240	1.123	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	ngs_client_data
6	172.16.70.5	40.112.143.211	LAN to WAN	49930	443	TCP	default	9	INTERNET	-	LOCAL	3761	8	906	2.137	1.936	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	ngs_client_data
7	172.16.70.5	40.112.143.211	LAN to WAN	62117	443	TCP	default	645	INTERNET	-	LOCAL	3690642	644	37916	0.112	0.033	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	ngs_client_data
8	172.16.70.4	40.112.143.211	LAN to WAN	64080	443	TCP	default	846	INTERNET	-	LOCAL	4062	845	40258	0.303	0.141	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	ngs_client_data
9	172.16.70.4	13.91.161.240	LAN to WAN	63394	443	TCP	default	3615	INTERNET	-	LOCAL	3399157	3614	1071236	0.762	1.752	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	ngs_server_data
10	9.9.9	172.16.70.5	WAN to LAN	52	53	UDP	default	1	INTERNET	-	LOCAL	3753	1	212	0.267	0.452	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A
11	40.112.143.211	172.16.70.4	WAN to LAN	443	50231	TCP	default	12	INTERNET	-	LOCAL	3752	12	5269	0.100	11.066	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A
12	40.112.143.211	172.16.70.4	WAN to LAN	443	50231	TCP	default	12	INTERNET	-	LOCAL	8521	12	5269	1.889	4.913	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A
13	40.112.143.211	172.16.70.5	WAN to LAN	443	49930	TCP	default	12	INTERNET	-	LOCAL	1108	12	5269	10.478	36.806	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A
14	40.112.143.211	172.16.70.5	WAN to LAN	443	49930	TCP	default	12	INTERNET	-	LOCAL	9038	12	5269	1.316	4.624	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A
15	40.112.143.211	172.16.70.5	WAN to LAN	443	64080	TCP	default	412	INTERNET	-	LOCAL	861	412	34405	0.209	0.122	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A
16	40.112.143.211	172.16.70.4	WAN to LAN	443	62433	TCP	default	327	INTERNET	-	LOCAL	3690409	327	28300	0.000	0.000	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A

Real LAN to WAN flows displayed: 16 out of 70
Total WAN to LAN flows displayed: 13 out of 69

• Statistiques DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
Default	office365_optimize	Quad9	YES	0
Default	citrix_cloud_web_ui_api	Quad9	YES	4
Default	ngs_client_data	Quad9	YES	14
Default	ngs_server_data	Quad9	YES	0
Default	ngs_control_traffic	Quad9	YES	2286
Default	ngs_web_proxy	Quad9	YES	0
Default	Any	azureDNS	YES	51490

Showing 1 to 7 of 7 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_web_ui_api	Quad9	YES	0
ngs_client_data	Quad9	YES	0
ngs_control_traffic	Quad9	YES	0
ngs_server_data	Quad9	YES	0
ngs_web_proxy	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 6 of 6 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_download_svc	Quad9	YES	1
citrix_sdwan_orchestrator	Quad9	YES	1

Showing 1 to 2 of 2 entries

- Statistiques des itinéraires d'application

Monitoring > Statistics

Statistics

Show: Application Routes ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 6 of 6 entries

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	7	YES	N/A	N/A
1	NGS_WebProxy_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A
2	NGS_ServerData_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	44	YES	N/A	N/A
3	NGS_ControlTraffic_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	72	YES	N/A	N/A
4	NGS_ClientData_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A
5	CitrixCloud_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A

Showing 1 to 6 of 6 entries

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries

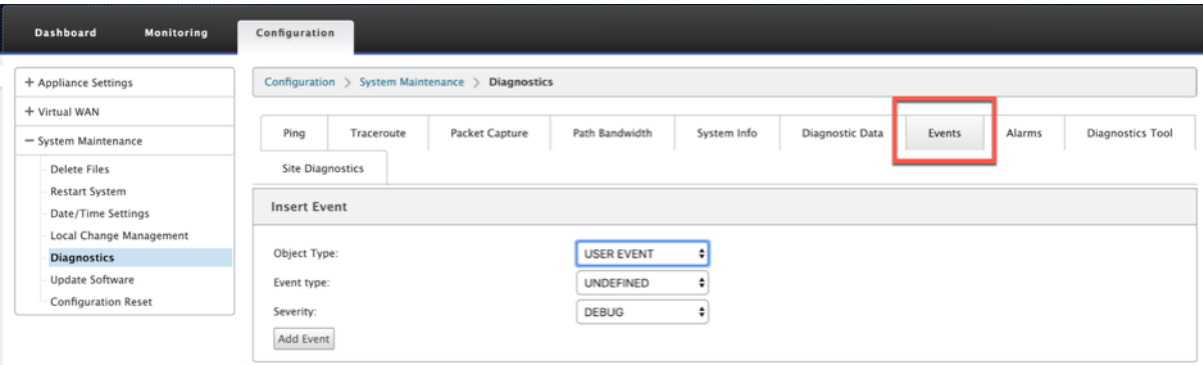
Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	CitrixSdwanOrchestrator_Breakout	*	Internet	Internet_Zone	YES	BRANCH1_KVMVPK	Static	50	35	YES	N/A	N/A
1	CitrixCloudDownloadSvc_Breakout	*	Internet	Internet_Zone	YES	BRANCH1_KVMVPK	Static	50	8	YES	N/A	N/A

Showing 1 to 2 of 2 entries

Résolution des problèmes

Vous pouvez consulter l'erreur de service dans la section **Événements** de l'appliance SD-WAN.

Pour vérifier les erreurs, accédez à **Configuration > Maintenance du système > Diagnostics**, cliquez sur l'onglet **Événements**.



S'il y a un problème lors de la connexion au service Citrix (sdwan-app-routing.citrixnetworkapi.net), le message d'erreur se reflète sous la table **Afficher les événements**.

View Events

Quantity: 25

Filter: Object Type = APPLICATIONS Event type = FAILURE Severity = ERROR

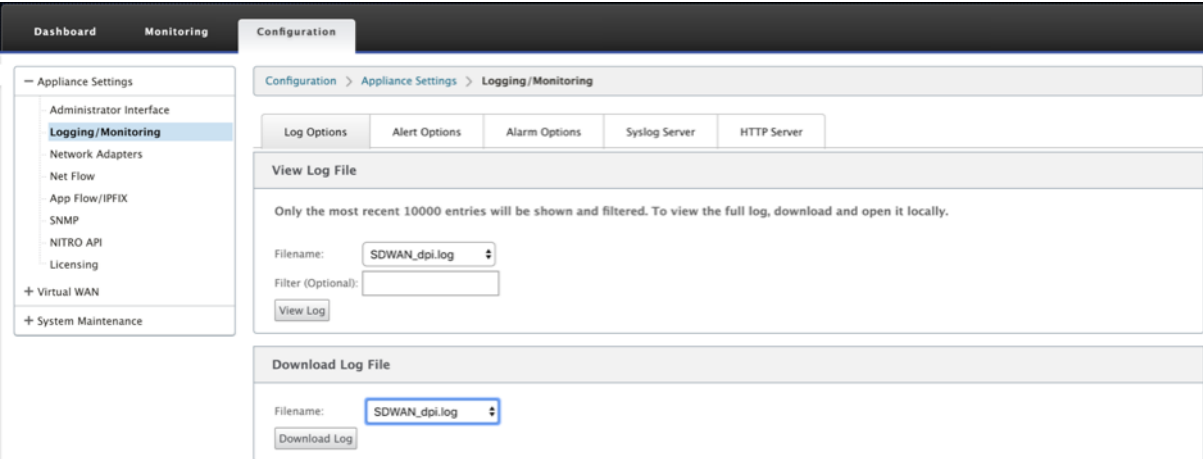
Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API

Times are in UTC

Les erreurs de connectivité sont également enregistrées dans **SDWAN_DPI.log**. Pour afficher le journal, accédez à **Configuration > Paramètres du matériel > Journalisation/surveillance > Options du journal**. Sélectionnez le fichier SDWAN_dpi.log dans la liste déroulante et cliquez sur **Afficher le journal**.

Vous pouvez également télécharger le fichier journal. Pour télécharger le fichier journal, sélectionnez le fichier journal requis dans la liste déroulante sous la section **Télécharger le fichier journal**, puis cliquez sur **Télécharger le journal**.



Citrix SD-WAN Orchestrator pour la configuration locale sur l'appliance Citrix SD-WAN

November 16, 2022

Citrix SD-WAN Orchestrator for On-premise est la version logicielle locale du service Citrix SD-WAN Orchestrator. Citrix SD-WAN Orchestrator for On-premise fournit une plate-forme de gestion en verre unique permettant aux partenaires Citrix de gérer plusieurs clients de manière centralisée, avec des contrôles d'accès basés sur les rôles appropriés.

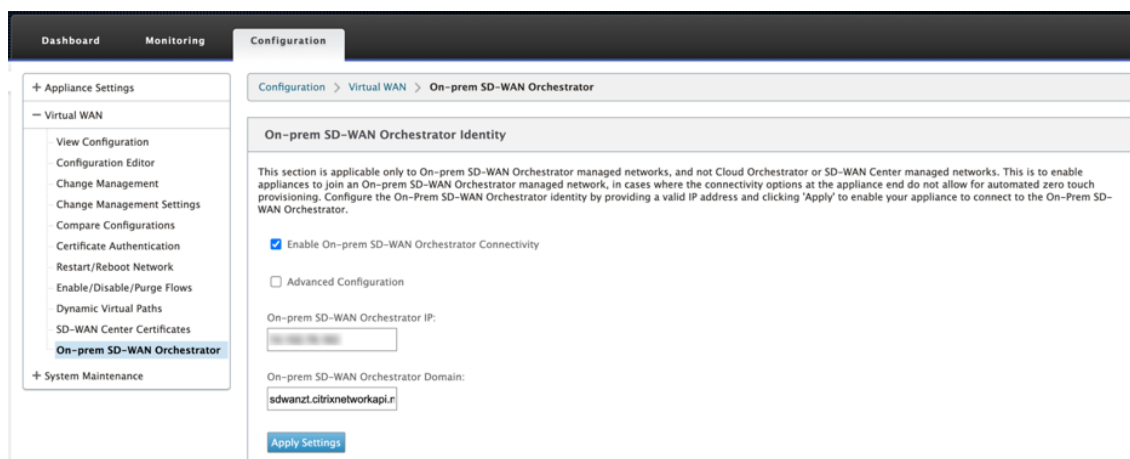
Vous pouvez établir une connexion entre votre appliance Citrix SD-WAN et Citrix SD-WAN Orchestrator for On-premise en activant la connectivité Orchestrator et en spécifiant l'identité Citrix SD-WAN Orchestrator for On-premise.

Remarque

- Le déploiement sans intervention de Cloud Orchestrator ne fonctionne pas si la **configuration SD-WAN Orchestrator sur site sur l'appliance SD-WAN** est configurée sur les appliances SD-WAN.
- Citrix SD-WAN Orchestrator for On-premise sur l'appliance SD-WAN est perdu si la configuration de Citrix SD-WAN Orchestrator for On-premise sur l'appliance SD-WAN configurée dans Citrix SD-WAN version 11.3.0 est rétrogradée vers la version 10.2.7. La rétrogradation de la version 11.3.0 vers la version 10.2.7 n'est pas prise en charge. La solution consiste à reconfigurer Citrix SD-WAN Orchestrator pour l'identité locale après la mise à niveau.
- Après avoir rétrogradé l'appliance SD-WAN de la version 11.3.0 à la version logicielle 11.1.1/11.2.0/10.2.7, vous devez appliquer à nouveau les paramètres d'identité sur l'interface utilisateur de l'appliance Citrix SD-WAN. En cas de problème lié à la configuration Citrix SD-WAN Orchestrator pour la configuration locale ou à la connectivité de l'appliance SD-WAN, désactivez Citrix SD-WAN Orchestrator pour la connectivité locale, puis activez à nouveau Citrix SD-WAN Orchestrator pour la connectivité locale.

Pour activer Citrix SD-WAN Orchestrator pour la connectivité locale, procédez comme suit :

1. Dans l'interface utilisateur de l'appliance SD-WAN, accédez à **Configuration > Virtual WAN > On-prem SD-WAN Orchestrator**.
2. **Activez la case à cocher Activer la connectivité SD-WAN Orchestrator** sur site.



3. Entrez l'adresse IP Citrix SD-WAN Orchestrator pour l'adresse IP locale ou le domaine, ou les deux (adresse IP et domaine) pour la configuration.

Si le client configure uniquement le domaine, il doit s'assurer d'ajouter l'enregistrement DNS dans son serveur DNS local et configurer l'adresse IP du serveur DNS sur les appliances SD-WAN. Pour configurer, accédez à **Configuration > Cartes réseau > Adresse IP**.

Par exemple, si Citrix SD-WAN Orchestrator pour domaine local est configuré en tant que **citrix.com**, vous devez créer un enregistrement DNS dans le serveur DNS pour le nom de domaine complet ci-dessous et Citrix SD-WAN Orchestrator pour adresse IP locale :

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

En configuration avancée :

Par exemple : si le domaine local Orchestrator est configuré en tant que **citrix.com**, le domaine du service de gestion des téléchargements est configuré en tant que **download.citrix.com** et le domaine du service de gestion des statistiques est configuré en tant que **statistiques.citrix.com**. Vous devez ensuite créer un enregistrement DNS sur le serveur DNS pour le nom de domaine complet ci-dessous et l'adresse IP correspondante :

- download.citrix.com
- sdwanzt.citrix.com
- statistiques.citrix.com

The screenshot displays the Citrix SD-WAN 11.4 Configuration interface. The left sidebar shows the navigation menu with 'On-prem SD-WAN Orchestrator' selected. The main content area is titled 'Configuration > Virtual WAN > On-prem SD-WAN Orchestrator'. It contains two main sections: 'On-prem SD-WAN Orchestrator Identity' and 'Authentication Type'.

On-prem SD-WAN Orchestrator Identity

This section is applicable only to On-prem SD-WAN Orchestrator managed networks, and not Cloud Orchestrator or SD-WAN Center managed networks. This is to enable appliances to join an On-prem SD-WAN Orchestrator managed network, in cases where the connectivity options at the appliance end do not allow for automated zero touch provisioning. Configure the On-Prem SD-WAN Orchestrator identity by providing a valid IP address and clicking 'Apply' to enable your appliance to connect to the On-Prem SD-WAN Orchestrator.

☒ Enable On-prem SD-WAN Orchestrator Connectivity

☒ Advanced Configuration

On-prem SD-WAN Orchestrator IP:

Download Management Service IP:

Statistics Management Service IP:

On-prem SD-WAN Orchestrator Domain:

Download Management Service Domain:

Statistics Management Service Domain:

Authentication Type

No Authentication : No Authentication between On-prem SD-WAN Orchestrator and SD-WAN Appliance. Customer can use this option if they have already secure network. For eg: MPLS

One-way Authentication : SD-WAN Appliance will authenticate On-prem SD-WAN Orchestrator. On-prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance.

Two-way Authentication : On-prem SD-WAN Orchestrator and SD-WAN Appliance authenticates each other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.

Authentication Type:

Orchestrator sur site peut prendre en charge des services en cours d'exécution tels que le téléchargement, les statistiques sur l'instance de serveur indépendant, afin de permettre une meilleure évolutivité pour les grands réseaux. Vous pouvez sélectionner la **configuration avancée** et configurer le service de **gestion des téléchargements et le service de gestion des statistiques**.

Activez la case à cocher **Configuration avancée** et fournissez les détails suivants :

- **Download Management Service IP/domaine** : Fournissez l'adresse/domaine IP qui aide à télécharger le logiciel SD-WAN et les aspects de téléchargement de configuration à une instance de serveur indépendante, afin de permettre une meilleure évolutivité pour les grands réseaux.
 - **Service de gestion statistique IP/domaine** : Fournissez l'adresse/domaine IP qui aide à télécharger la collecte et la gestion des statistiques SD-WAN des périphériques vers une instance de serveur indépendante, afin de permettre une meilleure évolutivité pour les grands réseaux.
4. Sélectionnez le **type d'authentification**. Voici les types d'authentification pris en charge entre l'appliance SD-WAN et Citrix SD-WAN Orchestrator pour la connectivité locale :
- **Aucune authentification** : aucune authentification entre le SD-WAN Orchestrator local et l'appliance SD-WAN, et il n'est pas nécessaire d'utiliser le certificat de l'**appliance SD-WAN** ou du **certificat SD-WAN Orchestrator sursite**. Mais vous pouvez utiliser cette option si vous disposez d'un réseau sécurisé tel que MPLS.

- **Authentification unidirectionnelle** : lorsque vous sélectionnez le type **d'authentification unidirectionnelle**, vous devez télécharger le certificat sur site Orchestrator. Téléchargez le certificat local Orchestrator à partir d'Orchestrator sur site, puis cliquez sur **Télécharger**. L'apppliance SD-WAN approuve Orchestrator sur site à l'aide des certificats téléchargés.
- **Authentification bidirectionnelle** : les certificats Orchestrator sur site et Appliance doivent être échangés les uns avec les autres. Pour **l'authentification bidirectionnelle**, vous devez régénérer, télécharger et charger le certificat de l'apppliance SD-WAN sur Orchestrator on=local. L'apppliance SD-WAN et Orchestrator sur site se confient mutuellement à l'aide des certificats échangés.

Remarque

Il est recommandé d'utiliser uniquement l'authentification unidirectionnelle ou l'authentification bidirectionnelle. Dans le cas de No Authentication, assurez-vous que le DNS est protégé contre les attaques DNS.

Si le **type d'authentification local d'** Orchestrator est désactivé, l'apppliance peut se connecter à Orchestrator sur site via **Aucune authentification ou Authentification unidirectionnelle ou Authentification bidirectionnelle**.

Si le **type d'authentification** sur site Orchestrator est activé, l'apppliance peut uniquement se connecter à Orchestrator sur site via **l'authentification bidirectionnelle**.

Lors de la désactivation du **type d'authentification** dans Orchestrator local de l'état d'activation, les appliances existantes en mode Authentification unidirectionnelle passent à l'état déconnecté. Les clients doivent modifier le type d'authentification de l'apppliance en Authentification bidirectionnelle et charger le certificat de l'apppliance SD-WAN sur l'Orchestrator sur site pour qu'il soit connecté.

Remarque

- Les certificats générés sont des certificats auto-signés X509.
- Le client doit régénérer les certificats si le certificat est expiré ou compromis.
- La validité du certificat est de 10 ans.
- Vous pouvez afficher les détails du certificat tels que l'empreinte digitale, la date de début et la date de fin
- Le client doit s'assurer que les certificats sont régénérés et échangés entre Orchestrator sur site et l'apppliance SD-WAN afin d'éviter toute perte de connectivité de l'apppliance avec Orchestrator sur site.

Authentication Type

No Authentication : No Authentication between On-prem SD-WAN Orchestrator and SD-WAN Appliance. Customer can use this option if they have already secure network. For eg: MPLS

One-way Authentication : SD-WAN Appliance will authenticate On-prem SD-WAN Orchestrator. On-prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance.

Two-way Authentication : On-prem SD-WAN Orchestrator and SD-WAN Appliance authenticates each other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.

Authentication Type Two-way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Filename: Choose file No file chosen Upload

[Certificate Details](#)

Certificate Fingerprint: 75:38:C2:32:AC:07:6E:26:6C:D9:C6:08:73:A2:73:8D:81:91:5A:4C

Start Date: Jul 22 11:26:32 2020 GMT

End Date: Jul 20 11:26:32 2030 GMT

SD-WAN Appliance Certificate

[Certificate Details](#)

Certificate Fingerprint: FC:36:3C:E5:EF:C2:F8:ED:48:20:0C:28:6C:5D:8A:82:55:CE:04:DD

Start Date: Jul 21 06:07:08 2020 GMT

End Date: Jul 19 06:07:08 2030 GMT

Regenerate Download

5. Cliquez sur **Appliquer les paramètres**.

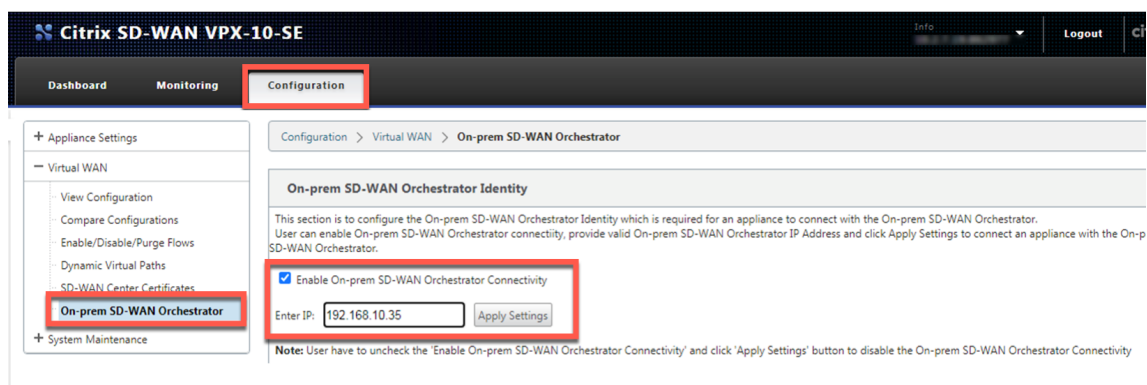
Pour désactiver Citrix SD-WAN Orchestrator pour la connectivité locale, **désactivez l'option Activer la connectivité locale de Citrix SD-WAN Orchestrator** et cliquez sur **Appliquer les paramètres**. Pour convertir un réseau géré local Orchestrator en réseau géré Cloud Orchestrator ou MCN, vous devez désactiver Citrix SD-WAN Orchestrator pour la connectivité locale et effectuer la réinitialisation de la configuration. Pour réinitialiser la configuration, accédez à **Configuration > Maintenance système > Réinitialisation de configuration**.

Déployez des appliances Citrix SD-WAN exécutées sur les versions logicielles 10.2.7, 11.1.1 ou 11.2.0 avec Citrix SD-WAN Orchestrator for On-premise

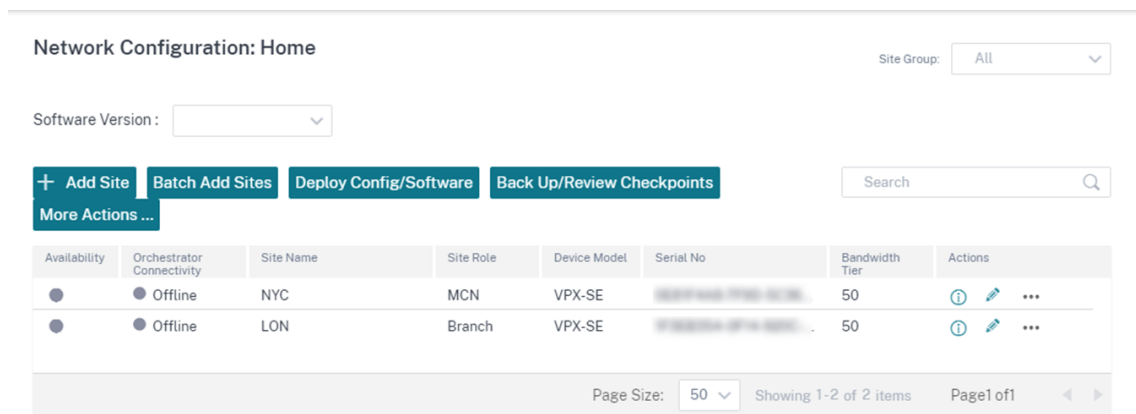
REMARQUE

Pour déployer des appliances Citrix SD-WAN avec les versions logicielles 10.2.7, 11.1.1 ou 11.2.0, vous avez besoin de Citrix SD-WAN Orchestrator for On-premise version 11.1 ou ultérieure.

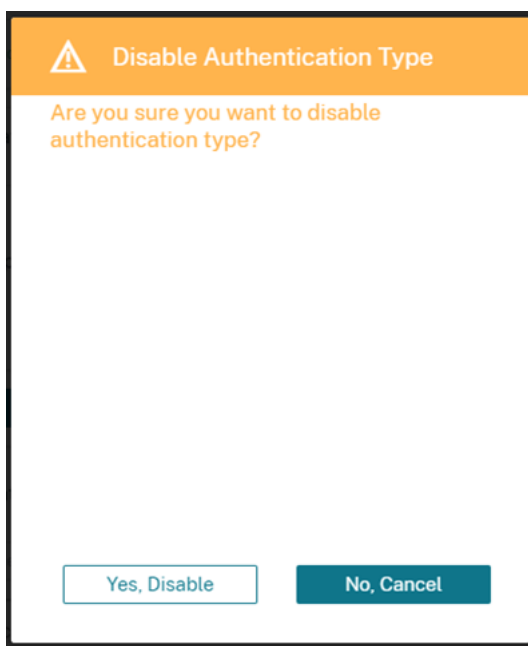
- Pour chaque appliance Citrix SD-WAN avec la version logicielle 10.2.7, 11.1.1 ou 11.2.0, connectez-vous à l'interface Web de l'appliance et effectuez les opérations suivantes :
 - Accédez à **Configuration > Virtual WAN > On-prem SD-WAN Orchestrator** et **activez la case à cocher Activer la connectivité SD-WAN Orchestrator** sur site.
 - Entrez l'adresse IP de Citrix SD-WAN Orchestrator for On-premise.
 - Cliquez sur **Appliquer les paramètres**.





2. Connectez-vous à Citrix SD-WAN Orchestrator pour l'interface utilisateur locale. Créez un site et créez la configuration. Entrez le numéro de série de chaque appliance Citrix SD-WAN dans sa configuration de site respective. Enregistrez la configuration.



3. Accédez à **Administration > Authentification des certificats** et activez le bouton à bascule **Type d'authentification sur OFF**. Cliquez sur **Oui, Désactiver** pour approuver la fenêtre contextuelle **Type d'authentification désactivé**.




Network Administration: Certificate Authentication

 Disabled authentication type successfully. 

☒ Authentication Type



On-prem Orchestrator Certificate

Certificate Details:


Certificate Fingerprint: 

Start Date: July 13 05:57:34 2021 GMT

End Date: July 11 05:57:34 2031 GMT


 

Appliance Certificate

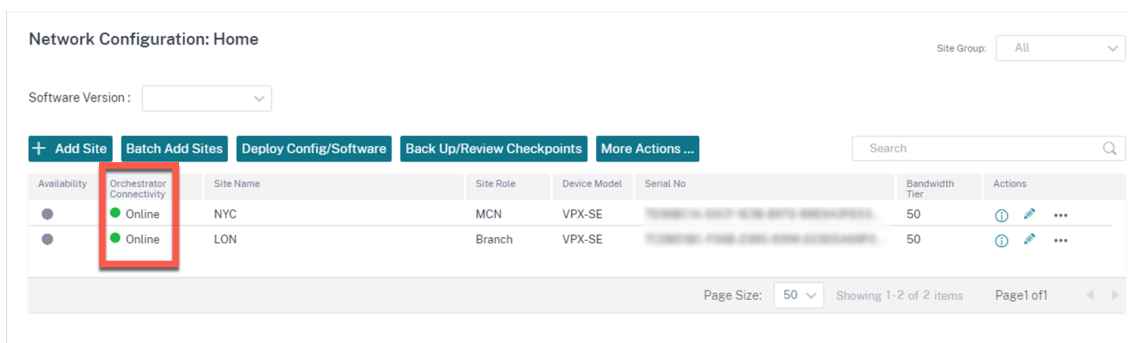
Select an appliance 

Click here to select the file or drag and drop the selected file.

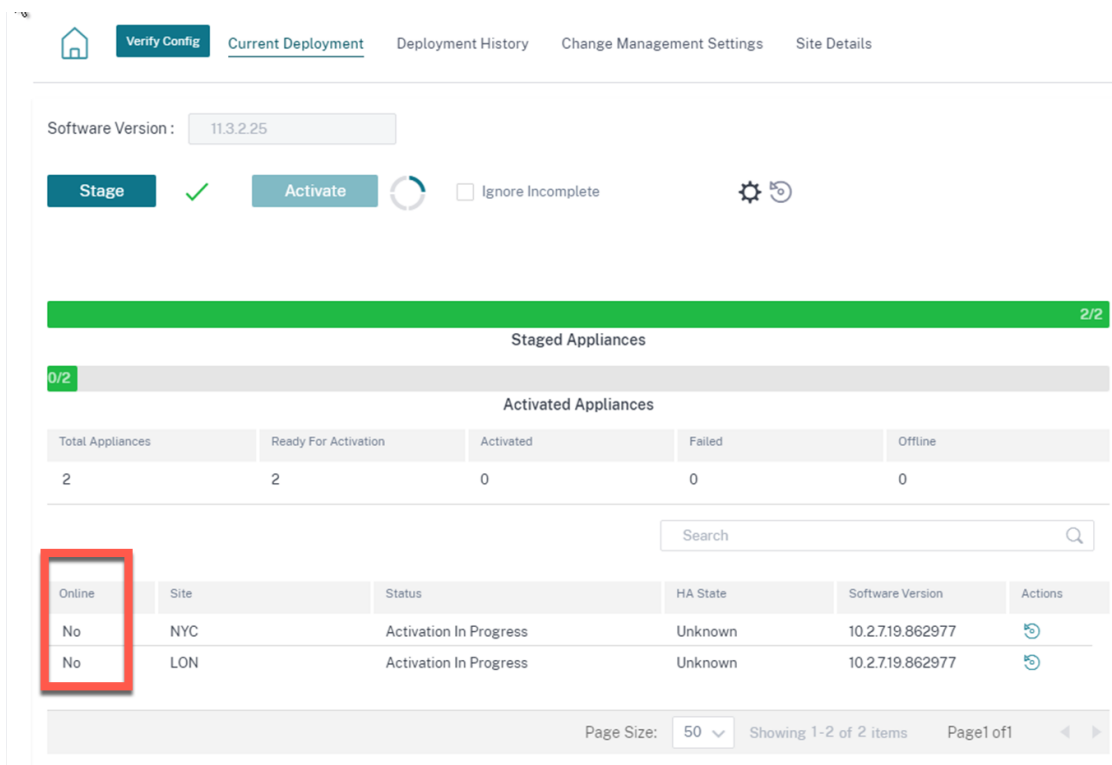
Allowed file type is .pem



4. Dans la page d'**accueil Configuration > Network Config**, les appliances SD-WAN apparaissent comme étant **en ligne** dans la colonne **Cloud Connectivity** . Cela est dû au fait que l'authentification des certificats est désactivée sur Citrix SD-WAN Orchestrator for On-premise et que les appliances SD-WAN sont activées pour Citrix SD-WAN Orchestrator pour la connectivité locale avec l'adresse IP appropriée. Comptez quelques minutes pour que les appareils soient signalés comme étant en ligne.



5. Sélectionnez une version de logiciel publiée (11.3.0 ou supérieure) et cliquez sur **Deploy Config/Software**. Pour plus d'informations sur la sélection de la version du logiciel publiée, consultez la section [Logiciels](#). **Mettre en scène** et **activer** les sites. Après l'activation, les solutions matérielles-logicielles affichent **Non** dans la colonne **En ligne**.



6. Accédez à **Administration > Paramètres ZTD > ZTD non cloud**. Cliquez sur **+Site** et ajoutez un site. Entrez l'adresse IP de gestion et les informations d'identification de connexion de chaque appliance. Cliquez sur **+** pour ajouter d'autres sites. Cliquez sur **Ajouter**.

Network Administration: ZTD Settings

Non-Cloud ZTD Cloud Brokered ZTD (Preview)



- Non-Cloud ZTD Settings helps to configure On-prem SD-WAN Orchestrator Information on SD-WAN Appliances running 11.3.0 and above releases.
- Multiple sites can also be added by importing a .csv file with all the site details.
[Click here](#) to download a sample .csv file.

Add Sites

Site Name	Management IP	Username	Freshly Provisioned	Password	New Password	
NYC	192.168.10.200	admin	<input type="checkbox"/>	*****		—
LON	192.168.10.201	admin	<input type="checkbox"/>	*****	New password	+

Add Cancel

7. Cliquez sur **Actualiser** pour surveiller l'état de la configuration. Lorsque le site est correctement configuré, la colonne **État de la configuration** affiche **Le site a été configuré avec succès**.

Non-Cloud ZTD Settings			
+ Site	Import	Delete All	Refresh
Site Name	Management IP	Configuration Status	Actions
NYC	192.168.10.200	Site is configured successfully	
LON	192.168.10.201	Site is configured successfully	

Page Size: 50 Showing 1-2 of 2 items Page 1 of 1

8. Accédez à la page d'**accueil Configuration > Network Config**. Les sites correctement configurés s'affichent comme étant **en ligne** dans la colonne **Connectivité d'Orchestrator**.

Network Configuration: Home

Site Group: All

Software Version: 11.3.2.25

+ Add Site Batch Add Sites Deploy Config/Software Back Up/Review Checkpoints More Actions ...

Availability	Orchestrator Connectivity	Site Name	Site Role	Device Model	Serial No	Bandwidth Tier	Actions
●	● Online	NYC	MCN	VPX-SE	7D36BC1A-55CF-1E3B-B972-88E9A3FE53...	50	
●	● Online	LON	Branch	VPX-SE	7CDBD1BC-F56B-2385-9399-E03D5A69F0...	50	

Page Size: 50 Showing 1-2 of 2 items Page 1 of 1

9. Suivez la même procédure pour ajouter des sites supplémentaires. L'exécution des étapes précédentes n'a aucune incidence sur les déploiements de sites existants.

Sessions PPPoE

May 6, 2021

Le protocole PPPoE (Point-to-Point Protocol over Ethernet) connecte plusieurs utilisateurs d'ordinateurs sur un réseau local Ethernet à un site distant par l'intermédiaire d'appliances locales communes, par exemple, Citrix SD-WAN. PPPoE permet aux utilisateurs de partager une ligne d'abonné numérique (DSL), un modem câble ou une connexion sans fil commune à Internet. PPPoE combine le protocole PPP (Point-to-Point Protocol), couramment utilisé dans les connexions commutées, avec le protocole Ethernet, qui prend en charge plusieurs utilisateurs dans un réseau local. Les informations de protocole PPP sont encapsulées dans une trame Ethernet.

Les appliances Citrix SD-WAN utilisent PPPoE pour fournir un support aux fournisseurs de services Internet (FAI) pour avoir des connexions continues et continues DSL et modem câble, contrairement aux connexions à distance. PPPoE fournit à chaque session de site utilisateur distant pour apprendre les adresses réseau de l'autre via un échange initial appelé « découverte ». Une fois qu'une session est établie entre un utilisateur individuel et le site distant, par exemple un fournisseur d'accès Internet, la session peut être surveillée. Les entreprises utilisent un accès Internet partagé via des lignes DSL via Ethernet et PPPoE.

Citrix SD-WAN agissent en tant que client PPPoE. Il s'authentifie auprès du serveur PPPoE et obtient une adresse IP dynamique, ou utilise une adresse IP statique pour établir des connexions PPPoE.

Les éléments suivants sont nécessaires pour établir des sessions PPPoE réussies :

- Configurez l'interface réseau virtuelle (VNI).
- Informations d'identification uniques pour créer une session PPPoE.
- Configurer la liaison WAN. Chaque VNI ne peut avoir qu'une seule liaison WAN configurée.
- Configurez l'adresse IP virtuelle. Chaque session obtient une adresse IP unique, dynamique ou statique en fonction de la configuration fournie.
- Déployez l'appliance en mode pont pour utiliser PPPoE avec une adresse IP statique et configurez l'interface comme étant « approuvée ».
- L'IP statique est préférable pour avoir une configuration pour forcer l'IP proposée par le serveur ; si elle est différente de l'IP statique configurée, sinon une erreur peut se produire.
- Déployez l'appliance en tant que périphérique Edge pour utiliser PPPoE avec IP dynamique et configurez l'interface comme « non fiable ».
- Les protocoles d'authentification pris en charge sont, PAP, CHAP, EAP-MD5, EAP-SRP.
- Le nombre maximal de sessions multiples dépend du nombre de VNI configurés.
- Créez plusieurs VNI pour prendre en charge plusieurs sessions PPPoE par groupe d'interface.

Note :

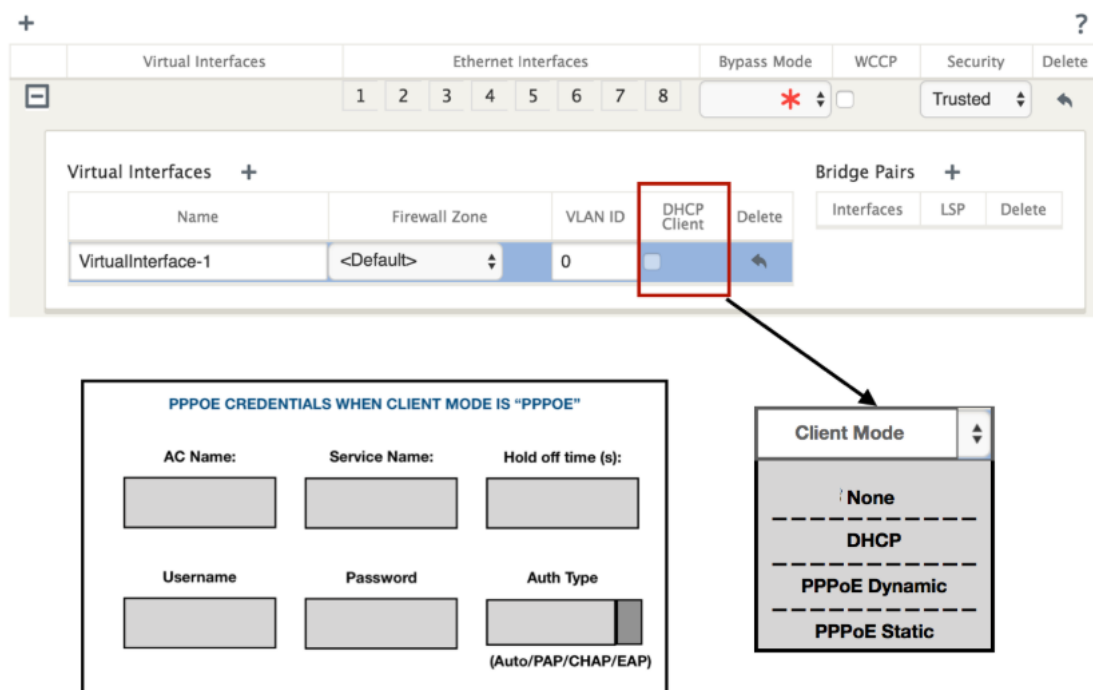
Plusieurs VNI sont autorisés à créer avec la même balise VLAN 802.1Q.

Limites pour la configuration PPPoE :

- Le balisage VLAN 802.1q n'est pas pris en charge.
- L'authentification EAP-TLS n'est pas prise en charge.
- Compression d'adresse/de contrôle.
- Compression dégonflée.
- Négociation de compression de champ de protocole.
- Protocole de contrôle de compression.
- Compresser BSD Compresser.
- Protocoles IPv6 et IPX.
- PPP Multi Link.
- Compression d'en-tête TCP/IP de style Van Jacobson.
- Option de compression d'ID de connexion dans la compression d'en-tête TCP/IP de style Van Jacobson.
- PPPoE n'est pas pris en charge sur les interfaces LTE

Dans la version 11.3.1 de Citrix SD-WAN, un en-tête PPPoE supplémentaire de 8 octets est envisagé pour ajuster la taille maximale du segment (MSS) de TCP. L'en-tête PPPoE supplémentaire de 8 octets ajuste le MSS dans les paquets de synchronisation en fonction du MTU.

Pour faciliter la configuration PPPoE, l'option **Client DHCP** est remplacée par une nouvelle option appelée le **Mode Client** dans l'interface de gestion Web SD-WAN sous Configuration des **sites** .



Le tableau suivant décrit les options de configuration PPPoE en mode client disponibles sur une appliance MCN et SD-WAN de succursale, respectivement.

MCN

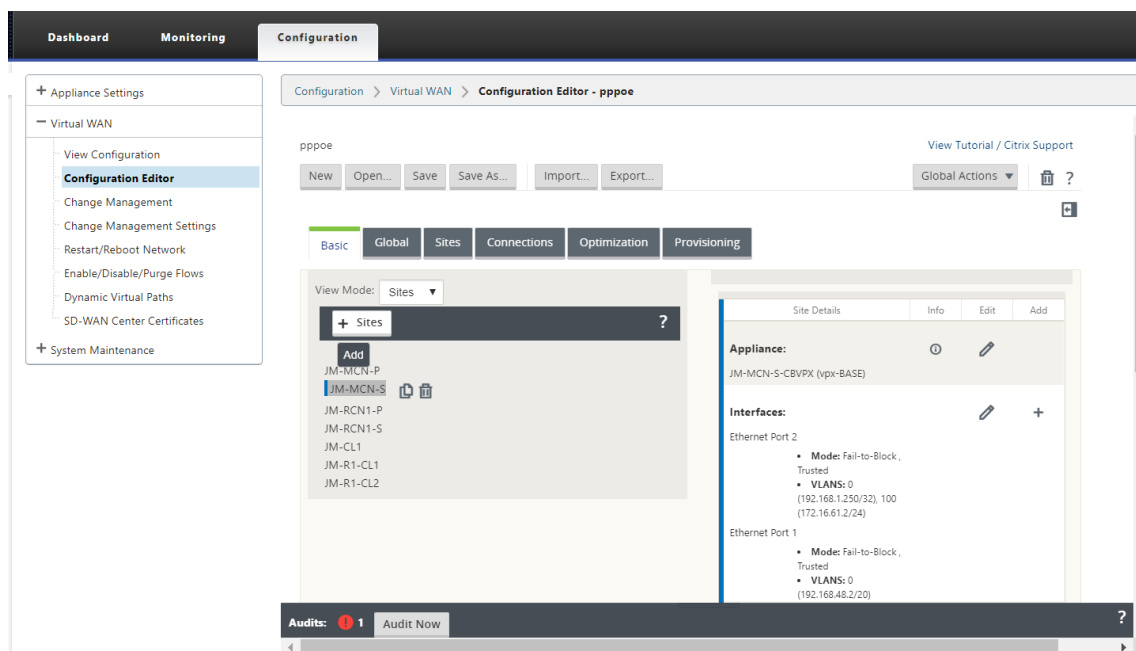
- Aucune
- PPPoE statique

Branch

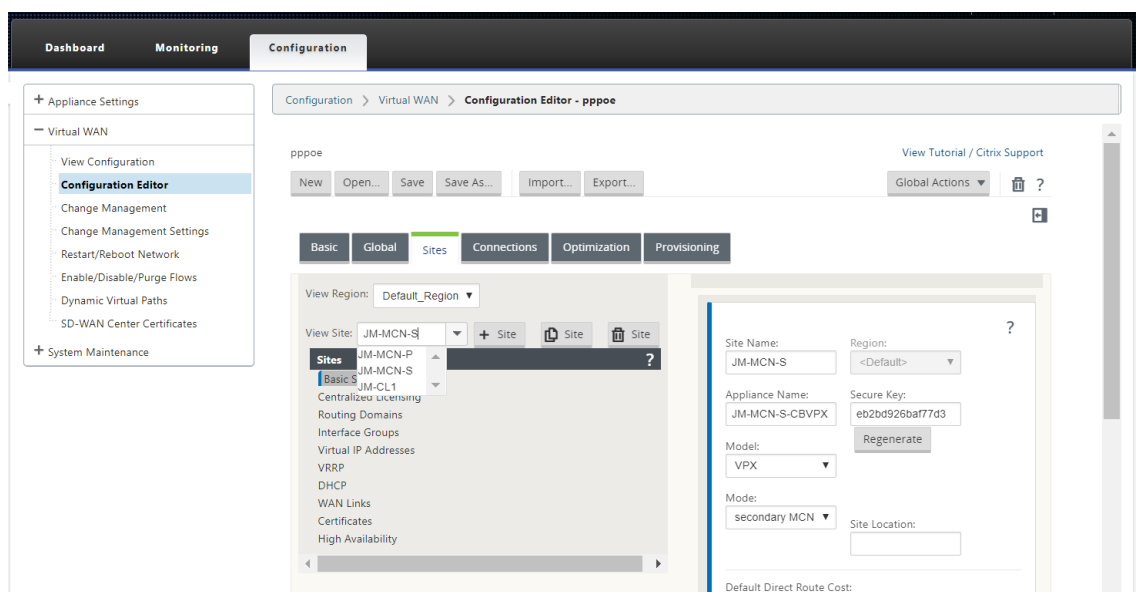
- Aucune
- PPPoE statique
- PPPoE Dynamique
- DHCP

Configurer l'appliance MCN

1. Dans l'interface graphique de l'appliance SD-WAN MCN, accédez à **Configuration > Réseau étendu virtuel > Éditeur de configuration**. Ajouter un site sous l'onglet **Basic**. Pour plus d'informations, reportez-vous à la configuration du nœud de branche à [configurer MCN](#).



2. Une fois le nouveau site créé, ouvrez l'onglet **Sites**. Sélectionnez le site nouvellement créé dans la liste déroulante **Voir le site**.

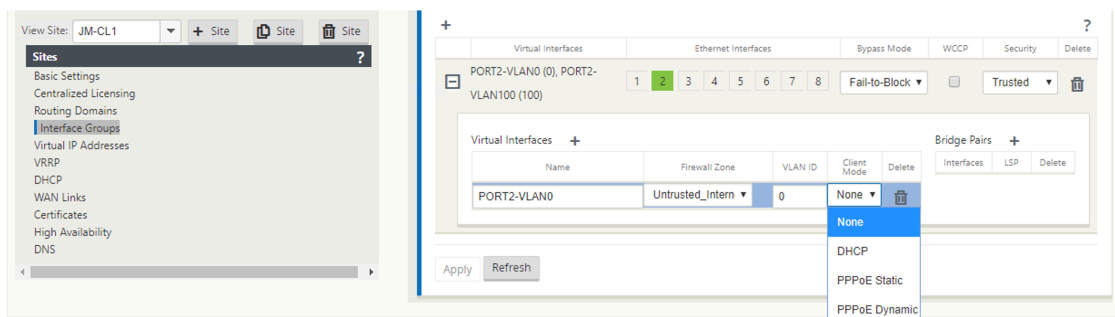


3. Sélectionnez **Groupes d'interface** pour le site MCN. Procédez comme suit :

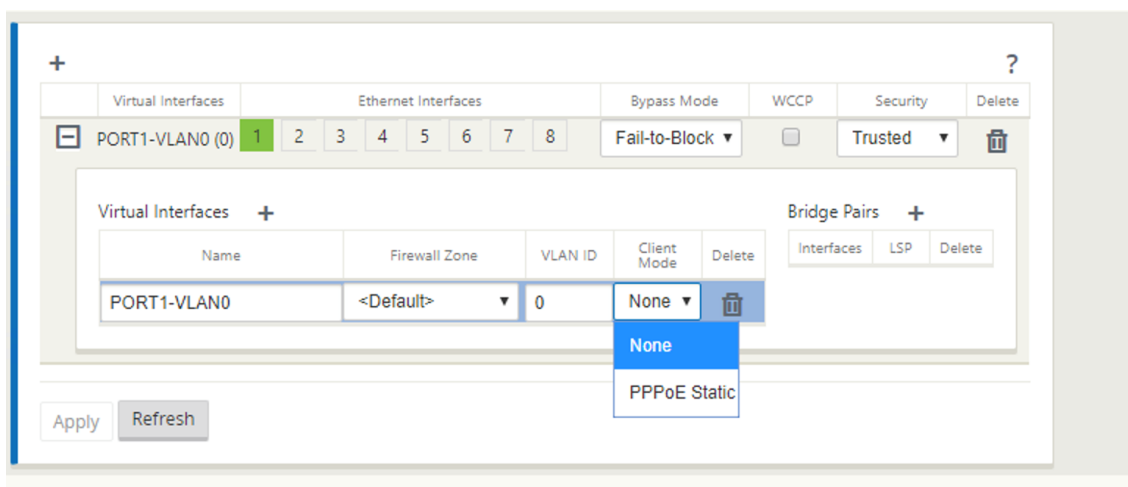
- Ajouter des interfaces virtuelles.
- Configurer les interfaces Ethernet.
- Configurez le mode de contournement.
- Choisissez **WCCP**, si nécessaire.
- Choisissez Sécurité —Approuvé/Non approuvé.

Pour l'interface virtuelle :

- Configurez le nom, la zone de pare-feu, l'ID VALN et le mode client.
- Un VNI configuré avec plusieurs interfaces ne peut avoir qu'une seule interface utilisée pour la connectivité PPPoE.
- Si un VNI configuré avec plusieurs interfaces et une connectivité PPPoE est remplacé par une interface différente, la page du moniteur peut être utilisée pour arrêter la session existante et démarrer une nouvelle session, puis une nouvelle session peut être établie sur la nouvelle interface.



4. Sélectionnez **PPPoE Static** ou **Aucun** en fonction de votre configuration réseau requise pour l'option Mode client sur l'appliance MCN. Les autres options suivantes s'affichent.



Configurez les paramètres PPPoE suivants et cliquez sur **Appliquer**.

- Accès au champ Nom du concentrateur (AC).
- Nom du service.
- Temps de reconnexion de retenue (la valeur par défaut est de se reconnecter immédiatement, « 0 »)
- Type d'authentification - (AUTO/PAP/CHAP/EAP).
 - Lorsque l'option Auth est définie sur Auto, l'appliance SD-WAN respecte la demande de protocole d'authentification prise en charge reçue du serveur.

- Lorsque l'option Auth est définie sur PAP/CHAP/EAP, seuls les protocoles d'authentification spécifiques sont respectés. Si PAP est dans la configuration et que le serveur envoie une demande d'authentification avec CHAP, la demande de connexion est rejetée. Si le serveur ne négocie pas avec PAP, un échec d'authentification se produit.
- CHAP inclut : CHAP, Microsoft CHAP et Microsoft CHAPV2.
- EAP prend en charge EAP-MD5.
- Nom d'utilisateur et mot de passe

La figure suivante affiche les options de mode client PPPoE pour une appliance SD-WAN de succursale. Si PPPoE Dynamic est sélectionné, le VNI doit être « Non approuvé. »

Configurer les liens WAN

1. Dans l'interface graphique SD-WAN, accédez à **Sites > Liens WAN**. Une seule création de liaison WAN est autorisée par VNI statique ou dynamique PPPoE. La configuration de la liaison WAN varie en fonction de la sélection VNI du Mode Client.
2. Si le VNI est configuré avec le mode client dynamique PPPoE :
 - Les champs Adresse IP et Adresse IP de la passerelle deviennent inactifs.
 - Le mode chemin virtuel est défini sur « Principal. »
 - L'ARP proxy ne peut pas être configuré.

Par défaut, la liaison d'adresses MAC de passerelle est sélectionnée.

WAN Link: RL-MCN-S-WL-1 Section: Access Interfaces + Add Link Delete Link

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
RL-MCN-S-WL-1...	PORT2-VLAN0			Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Apply Refresh

3. Si le VNI est configuré avec le mode client statique PPPoE, configurez l'adresse IP.

WAN Link: RL-MCN-S-WL-1 Section: Access Interfaces + Add Link Delete Link

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
RL-MCN-S-WL-1...	PORT2-VLAN0	192.168.1.250		Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Apply Refresh

Note :

Si le serveur n'honore pas l'adresse IP statique configurée et offre une adresse IP différente, une erreur se produit. La session PPPoE tente de rétablir la connexion périodiquement, jusqu'à ce que le serveur accepte l'adresse IP configurée.

Surveiller les sessions PPPoE

Vous pouvez surveiller les sessions PPPoE en accédant à la page **Surveillance > PPPoE** dans l’interface graphique SD-WAN.

La page PPPoE fournit des informations d’état des VNI configurés avec le mode client statique ou dynamique PPPoE. Il vous permet de démarrer ou d’arrêter manuellement les sessions à des fins de dépannage.

- Si le VNI est prêt, les colonnes **IP et IP de la passerelle** affichent les valeurs actuelles de la session. Il indique qu’il s’agit de valeurs récemment reçues.
- Si le VNI est arrêté ou est en état d’échec, les valeurs sont les dernières valeurs reçues.
- Le pointeur de la souris sur la colonne IP de la passerelle affiche l’adresse MAC du concentrateur d’accès PPPoE à partir duquel la session et l’adresse IP sont reçues.
- Passez la souris sur la valeur « état » affiche un message, ce qui est plus utile pour un état « Échec ».

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

Monitoring > PPPoE

Refresh

Virtual Interface	IP Address	Gateway IP	Session ID	State	Action
PORT2-VLAN0	192.168.1.22	192.168.1.254	18	Ready	Stop
abcd	0.0.0.0	0.0.0.0	0	Failed	Start
newVIF	0.0.0.0	0.0.0.0	0	Stopped	Start

La colonne **État** affiche l’état de la session PPPoE à l’aide de trois codes couleur : vert, rouge, jaune et valeurs. Le tableau suivant décrit les états et les descriptions. Vous pouvez survoler les états pour obtenir des descriptions.

Type de session PPPoE	Couleur	Description
Configuré	Jaune	Un VNI est configuré avec PPPoE. C’est un état initial.
Composition du numéro en cours	Jaune	Après avoir configuré un VNI, l’état de session PPPoE passe à l’état de numérotation en démarrant la découverte PPPoE. Les informations sur les paquets sont capturées.

Type de session PPPoE	Couleur	Description
La	Jaune	VNI est déplacé de l'état Découverte à l'état Session. En attente de réception IP, si dynamique ou en attente d'accusé de réception du serveur pour l'adresse IP annoncée, si statique.
Prêt	vert	Les paquets IP sont reçus et le VNI et la liaison WAN associée sont prêts à l'emploi.
Échec	rouge	La session PPP/PPPoE est terminée. La raison de l'échec peut être due à une configuration incorrecte ou à une erreur fatale. La session tente de se reconnecter après 30 secondes.
Arrêté	jaune	La session PPP/PPPoE est arrêtée manuellement.
Terminer	jaune	Etat intermédiaire se terminant en raison d'une raison. Cet état démarre automatiquement après une certaine durée (5 secondes pour une erreur normale ou 30 secondes pour une erreur fatale).
Désactivé	jaune	Le service SD-WAN est désactivé.

Dépannage des échecs de session PPPoE

Sur la page Surveillance, en cas de problème lors de l'établissement d'une session PPPoE :

- Le fait de passer le curseur de la souris sur l'état Échec indique la raison de l'échec récent.
- Pour établir une nouvelle session ou pour dépanner une session PPPoE active, utilisez la page Monitoring > PPPoE et redémarrez la session.
- Si une session PPPoE est arrêtée manuellement, elle ne peut pas être démarrée tant qu'elle n'a pas été démarrée manuellement et qu'une modification de configuration n'est pas activée ou

que le service ait été redémarré.

Une session PPPoE peut échouer pour les raisons suivantes :

- Lorsque SD-WAN ne parvient pas à s'authentifier auprès de l'homologue en raison d'un nom d'utilisateur/mot de passe incorrect dans la configuration.
- La négociation PPP échoue - la négociation n'atteint pas le point où au moins un protocole réseau est en cours d'exécution.
- Problème de mémoire système ou de ressource système.
- Configuration invalide/incorrecte (nom AC ou nom de service incorrect).
- Impossible d'ouvrir le port série en raison d'une erreur du système d'exploitation.
- Aucune réponse reçue pour les paquets d'écho (le lien est incorrect ou le serveur ne répond pas).
- Il y avait plusieurs sessions de composition infructueuses en une minute.

Après 10 échecs consécutifs, la raison de l'échec est observée.

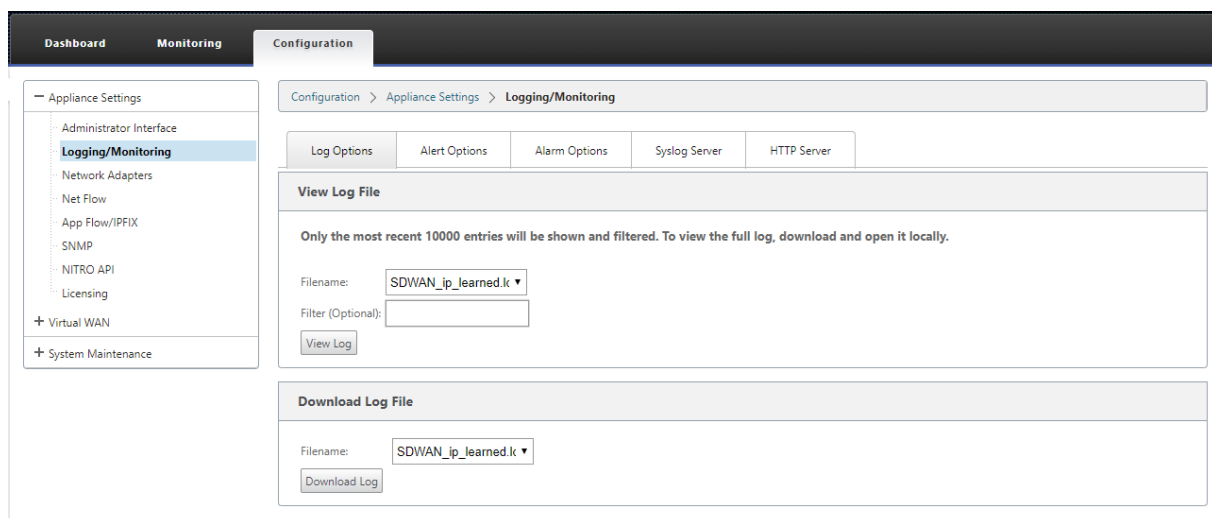
- Si l'échec est normal, il redémarre immédiatement.
- Si l'échec est une erreur, le redémarrage revient pendant 10 secondes.
- Si l'échec est fatal, le redémarrage revient pendant 30 secondes avant de redémarrer.

Les paquets de requête d'écho LCP sont générés à partir de SD-WAN toutes les 60 secondes et l'échec de réception de 5 réponses d'écho est considéré comme un échec de liaison et il rétablit la session.

Fichier journal PPPoE

Le fichier *SDWAN_IP_Learned.log* contient des journaux liés à PPPoE.

Pour afficher ou télécharger le fichier *SDWAN_IP_Learned.log* à partir de l'interface graphique SD-WAN, accédez à **Paramètres de l'appliance > Logging/Monitoring > Options du journal** . Affichez ou téléchargez le fichier *SDWAN_IP_Learned.log* .



Qualité du service

November 16, 2022

Le réseau entre les bureaux et le datacenter ou le cloud doit transporter une multitude d'applications et de données, y compris la vidéo de haute qualité ou la voix en temps réel. Les applications sensibles à la bande passante étendent les capacités et les ressources du réseau. Citrix SD-WAN fournit des services réseau garantis, sécurisés, mesurables et prévisibles. Ceci est réalisé en gérant le délai, la gigue, la bande passante et la perte de paquets sur le réseau.

La solution Citrix SD-WAN comprend un moteur de qualité de service (QoS) des applications sophistiquées qui accède au trafic des applications et priorise les applications critiques. Il comprend également les exigences relatives à la qualité du réseau WAN et choisit un chemin réseau basé sur les caractéristiques de qualité en temps réel.

Les rubriques des sections suivantes traitent des classes QoS, des règles IP, des règles QoS d'application et d'autres composants requis pour définir la QoS d'application.

Classes

November 1, 2021

La configuration Citrix SD-WAN fournit un ensemble par défaut de stratégies QoS basées sur l'application et l'IP/port qui sont appliquées à tout le trafic passant par des chemins virtuels. Ces paramètres peuvent être personnalisés en fonction des besoins de déploiement.

Les classes sont utiles pour hiérarchiser le trafic. Les stratégies QoS basées sur les applications et IP/port classent le trafic et le placent dans les classes appropriées spécifiées dans la configuration.

Pour plus d'informations sur la QoS des applications et la QoS basée sur l'adresse IP/port, consultez [les sections Règles par nom d'application](#) et [Règles par adresse IP et numéro de port](#) respectivement.

Le SD-WAN fournit 17 classes (ID : 0—16). Voici la configuration par défaut de toutes les 17 classes.

Virtual Path Default Set: New_Default_Set-1 Section: Classes + Add Default Set 🗑 Delete Default Set

ID	Name	Type	Initial				Sustained		Reset
			Period	Rate	%/Kbps	Share %	Rate	Share %	
0	HDX_priority_tag_0	Realtime	0	30	%	0	30	0	↕
1	HDX_priority_tag_1	Interactive	0	0	%	20	0	20	↕
2	HDX_priority_tag_2	Interactive	0	0	%	6	0	6	↕
3	HDX_priority_tag_3	Interactive	0	0	%	2	0	2	↕
4	class_4	Bulk		0	%	0	0	0	↕
5	class_5	Bulk		0	%	0	0	0	↕
6	class_6	Bulk		0	%	0	0	0	↕
7	class_7	Bulk		0	%	0	0	0	↕
8	class_8	Bulk		0	%	0	0	0	↕
9	class_9	Bulk		0	%	0	0	0	↕
10	realtime_class	Realtime	0	30	%	0	30	0	↕
11	interactive_high_class	Interactive	0	0	%	20	0	20	↕
12	interactive_medium_class	Interactive	0	0	%	13	0	13	↕
13	interactive_low_class	Interactive	0	0	%	6	0	6	↕
14	interactive_very_low_class	Interactive	0	0	%	3	0	3	↕
15	bulk_background_class	Bulk		0	%	0	0	100	↕
16	bulk_unused_class	Bulk		0	%	0	0	0	↕

Apply Revert

Voici les différents types de classes :

- **Temps réel** : Utilisé pour une faible latence, une faible bande passante et un trafic sensible au temps. Les applications en temps réel sont sensibles au temps, mais n'ont pas vraiment besoin d'une bande passante élevée (par exemple la voix sur IP). Les applications en temps réel sont sensibles à la latence et à la gigue, mais peuvent tolérer une certaine perte.
- **Interactif** : Utilisé pour le trafic interactif avec des exigences de latence faible à moyenne et des exigences de bande passante faible à moyenne. L'interaction se fait généralement entre un client et un serveur. La communication peut ne pas nécessiter de bande passante élevée, mais elle est sensible à la perte et à la latence.
- **Vrac** : Utilisé pour le trafic à bande passante élevée et les applications pouvant tolérer une latence élevée. Les applications qui gèrent le transfert de fichiers et qui ont besoin d'une bande

passante élevée sont classées comme classe groupée. Ces applications impliquent peu d'interaction humaine et sont principalement traitées par les systèmes eux-mêmes.

Partage de bande passante entre les classes

La bande passante est partagée entre les classes comme suit :

- **Temps réel** : Les classes de trafic en temps réel sont garanties pour avoir une faible latence et la bande passante est limitée à la part de classe lorsqu'il y a du trafic concurrentiel.
- **Interactif** : le trafic qui frappe les classes interactives obtient la bande passante restante après avoir servi le trafic en temps réel et la bande passante disponible est juste partagée entre les classes interactives.
- **Vrac** : Vrac est le meilleur effort. La bande passante restante après avoir servi le trafic interactif et en temps réel est donnée aux classes en vrac sur une base équitable. Le trafic en vrac peut mourir de faim si le trafic interactif et en temps réel utilise toute la bande passante disponible.

Remarque

Toute classe peut utiliser toute la bande passante disponible lorsqu'il n'y a pas de contention.

L'exemple suivant explique la distribution de la bande passante basée sur la configuration de la classe :

Considérez qu'il existe une bande passante agrégée de 10 Mbit/s sur le chemin virtuel. Si la configuration de la classe est

- Temps réel : 30%
- Interactif élevé : 40%
- Moyen interactif : 20%
- Interactive Faible : 10%
- Vrac : 100%

Le résultat de la distribution de la bande passante est

- Le trafic en temps réel obtient 30 % de 10 Mbit/s (3 Mbps) en fonction des besoins. S'il nécessite moins de 10 %, le reste de la bande passante est mis à la disposition des autres classes.
- Les classes interactives partagent la bande passante restante sur la base d'un partage équitable (4 Mbps : 2 Mbps : 1 Mbps).
- Tout ce qui reste lorsque le trafic interactif en temps réel n'utilise pas entièrement ses parts est attribué à la classe Bulk.

Pour personnaliser les classes :

1. Si des ensembles par défaut de chemin virtuel sont utilisés, les classes peuvent être modifiées sous **Global > Jeux par défaut de chemin virtuel**.

Remarque

Vous pouvez également modifier les classes au niveau du chemin virtuel (**Connexions -> Chemins virtuels -> Classes**)

2. Cliquez sur **Ajouter un jeu par défaut**, entrez un nom pour le jeu par défaut, puis cliquez sur **Ajouter**. Dans le champ **Section**, sélectionnez **Classes**.
3. Dans le champ **Nom**, laissez le nom par défaut ou entrez le nom de votre choix.
4. Dans le champ **Type**, sélectionnez le type de classe (Temps réel, Interactif ou Bulk).
5. Pour les classes en temps réel, vous pouvez spécifier les attributs suivants :
 - **Période initiale** : Période en millisecondes pour appliquer un taux initial avant de passer à un taux soutenu.
 - **Taux initial** : Taux maximal ou pourcentage auquel les paquets quittent la file d'attente pendant la période initiale.
 - **Taux soutenu** : Taux maximal ou pourcentage auquel les paquets quittent la file d'attente après la période initiale.
6. Pour les classes interactives, vous pouvez spécifier les attributs suivants :
 - **Période initiale** : Période de temps, en millisecondes, pendant laquelle appliquer le pourcentage initial de la bande passante disponible avant de passer au pourcentage soutenu. Typiquement, 20 ms
 - **% de partage initial** : Part maximale de bande passante de chemin virtuel restant après avoir servi en temps réel pendant la période initiale.
 - **Pourcentage de partage soutenu** : Part maximale de bande passante de chemin virtuel restant après avoir servi le trafic en temps réel après la période initiale.
7. Pour les classes en vrac, vous pouvez spécifier uniquement le **pourcentage de partage soutenu**, qui détermine la bande passante du chemin virtuel restant à utiliser pour une classe de masse après avoir servi le trafic interactif et en temps réel.
8. Cliquez sur **Apply**.

Remarque

Enregistrez la configuration, exportez la boîte de réception de gestion des modifications et lancez le processus de gestion des modifications.

Règles par adresse IP et numéro de port

May 6, 2021

Les règles par adresse IP et numéro de port vous aident à créer des règles pour votre réseau et à prendre certaines décisions de qualité de service (QoS) basées sur les règles. Vous pouvez créer des règles personnalisées pour votre réseau. Par exemple, vous pouvez créer une règle comme —Si l'adresse IP source est 172.186.30.74 et que l'adresse IP de destination est 172.186.10.89, définissez le **mode Transmission** comme Chemin persistant et **LAN à WAN Class** sur 10 (realtime_class) ».

À l'aide de l'éditeur de configuration, vous pouvez créer des règles pour le flux de trafic et les associer à des applications et des classes. Vous pouvez spécifier des critères pour filtrer le trafic d'un flux et appliquer un comportement général, un comportement LAN vers WAN, un comportement WAN vers LAN et des règles d'inspection de paquets.

Vous pouvez créer des règles localement au niveau du site ou au niveau global. Si plusieurs sites nécessitent la même règle, vous pouvez créer un modèle pour les règles globalement sous **Global > Jeux de chemins virtuels par défaut > Règles**. Le modèle peut ensuite être attaché aux sites où les règles doivent être appliquées. Même si un site est associé au modèle de règle créé globalement, vous pouvez créer des règles spécifiques au site. Dans de tels cas, les règles spécifiques au site ont priorité et remplacent le modèle de règle créé globalement.

Créer des règles par adresse IP et numéro de port

1. Dans l'Éditeur de configuration SD-WAN, accédez à **Global > Jeux par défaut de chemin virtuel**.

Remarque

Vous pouvez créer des règles au niveau du site en accédant à **Sites > Connexions > Chemins virtuels > Règles**.

2. Cliquez sur **Ajouter un jeu par défaut**, entrez un nom pour le jeu par défaut, puis cliquez sur **Ajouter**. Dans le champ **Section**, sélectionnez **Règles** et cliquez sur **+**.
3. Dans le champ **Ordre**, entrez la valeur de l'ordre à définir quand la règle est appliquée par rapport à d'autres règles.
4. Dans le champ **Nom du groupe de règles**, sélectionnez un groupe de règles. Les statistiques des règles avec le même groupe de règles sont regroupées et peuvent être visualisées ensemble. Pour afficher les groupes de règles, accédez à **Surveillance > Statistiques** et, dans le champ **Afficher**, sélectionnez **Groupes de règles**.

Vous pouvez également ajouter des applications personnalisées. Pour plus d'informations, reportez-vous à la section [Ajouter des groupes de règles et activer MOS](#).

5. Dans le champ **Domaine de routage**, choisissez l'un des domaines de routage configurés.
6. Vous pouvez définir des critères de correspondance de règles pour filtrer les services en fonction des paramètres répertoriés comme suit. Après le filtrage, les paramètres de règle sont appliqués aux services correspondant à ces critères.

- **Adresse IP source** : adresse IP source et masque de sous-réseau pour correspondre au trafic.
- **Adresse IP de destination** : adresse IP de destination et masque de sous-réseau pour correspondre au trafic.

Remarque

Si la **case à cocher Dest=Src** est activée, l'adresse IP source sera également utilisée pour l'adresse IP de destination.

- **Protocole** : Protocole à comparer avec le trafic.
- **Port source** : numéro de port source ou plage de ports à comparer avec le trafic.
- **Port de destination** : numéro de port de destination ou plage de ports à comparer avec le trafic.

Remarque

Si la **case à cocher Dest=Src** est activée, le port source sera également utilisé pour le port de destination.

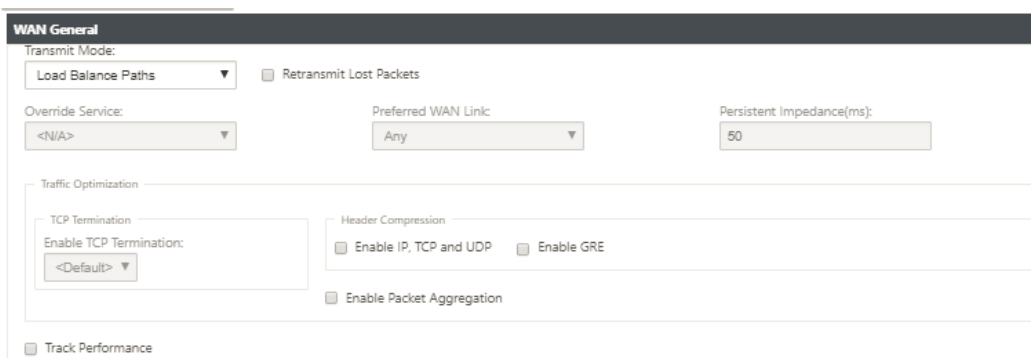
- **DSCP** : balise **DSCP** dans l'en-tête IP pour correspondre au trafic.
 - **VLAN : ID VLAN** à comparer avec le trafic.
7. Cliquez sur l'icône Ajouter (+) en regard de la nouvelle règle.
 8. Cliquez sur **Initialiser les propriétés à l'aide du protocole** pour initialiser les propriétés de la règle en appliquant les valeurs par défaut de la règle et les paramètres recommandés pour le protocole. Cette opération remplit les paramètres de règle par défaut. Vous pouvez également personnaliser les paramètres manuellement, comme indiqué dans les étapes suivantes.
 9. Cliquez sur la vignette **WAN General** pour configurer les propriétés suivantes.
 - **Mode de transmission** : Sélectionnez l'un des modes de transmission suivants.
 - **Chemin d'équilibrage** de charge : le trafic du flux sera réparti entre plusieurs chemins pour le service. Le trafic est envoyé par le meilleur chemin jusqu'à ce que ce chemin soit utilisé. Les paquets restants sont envoyés par le meilleur chemin suivant.

- **Chemin persistant** : le trafic du flux reste sur le même chemin jusqu'à ce que le chemin d'accès ne soit plus disponible.
- **Dupliquer le chemin** : le trafic du flux est dupliqué sur plusieurs chemins, ce qui augmente la fiabilité.
- **Service de remplacement** : le trafic pour le flux remplace un service différent. Dans le champ Remplacer le service, sélectionnez le type de service auquel le service remplace. Par exemple, un service de chemin d'accès virtuel peut remplacer un service intranet, Internet ou pass-through.
- **Retransmettre les paquets perdus** : envoie le trafic correspondant à cette règle à l'appliance distante via un service fiable et retransmet les paquets perdus.
- **Activer la terminaison TCP** : Activer la terminaison TCP du trafic pour ce flux. Le temps aller-retour pour l'accusé de réception des paquets est réduit, ce qui améliore le débit.
- **Liaison WAN préférée** : Liaison WAN que les flux doivent utiliser en premier.
- **Impédance persistante** : durée minimale en millisecondes pendant laquelle le trafic restera dans le même chemin, jusqu'au temps d'attente pendant lequel le chemin est plus long que la valeur configurée.
- **Activer IP, TCP et UDP** : Compresser les en-têtes dans les paquets IP, TCP et UDP.

REMARQUE Les

paquets IPv6 ne prennent pas en charge la compression d'en-tête.

- **Activer GRE** : Compresser les en-têtes dans les paquets GRE.
- **Activer l'agrégation de paquets** : Agrégez les petits paquets en paquets plus volumineux.
- **Performances de suivi** : enregistre les attributs de performance de cette règle dans une base de données de session (par exemple, perte, gigue, latence et bande passante).



WAN General

Transmit Mode:
 Load Balance Paths ☐ Retransmit Lost Packets

Override Service: Preferred WAN Link: Persistent Impedance(ms):

Traffic Optimization

TCP Termination
 Enable TCP Termination:

Header Compression
☐ Enable IP, TCP and UDP ☐ Enable GRE

☐ Enable Packet Aggregation

☐ Track Performance

10. Cliquez sur la vignette **LAN to WAN** pour configurer le comportement LAN to WAN pour cette règle.

- **Classe** : sélectionnez une classe à laquelle associer cette règle.

Remarque

Vous pouvez également personnaliser des classes avant d'appliquer des règles. Pour plus d'informations, reportez-vous à la section [Comment personnaliser les classes](#).

- **Grande taille de paquet** : Les paquets inférieurs ou égaux à cette taille reçoivent les valeurs **Limite de dépôt** et **Profondeur de dépôt** spécifiées dans les champs à droite du champ **Classe**.

LAN to WAN

General

Class: <Default>

Drop Limit (ms): 50

Drop Depth (bytes): 128000

Large Packet Size (bytes): 0

Large Packets

Drop Limit (ms): 0

Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0

Disable Depth (bytes): 128000

Reassign

Reassign Class: Disabled <Default>

Drop Limit (ms): 50

Drop Depth (bytes): 128000

Reassign Size (bytes): 2000

Large Packet Size (bytes): 0

Reassign

Drop Limit (ms): 50

Drop Depth (bytes): 128000

Reassign Size (bytes): 2000

Large Packet Size (bytes): 0

Reassign

Drop Limit (ms): 0

Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0

Disable Depth (bytes): 128000

Les paquets supérieurs à cette taille reçoivent les valeurs spécifiées dans les champs **Limite de dépôt** et **Profondeur de dépôt** par défaut de la section **Grands paquets** de l'écran.

LAN to WAN

General

Class: <Default>

Drop Limit (ms): 50

Drop Depth (bytes): 128000

Large Packet Size (bytes): 0

Large Packets

Drop Limit (ms): 0

Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0

Disable Depth (bytes): 128000

Reassign

Reassign Class: Disabled <Default>

Drop Limit (ms): 50

Drop Depth (bytes): 128000

Reassign Size (bytes): 2000

Large Packet Size (bytes): 0

Reassign

Drop Limit (ms): 50

Drop Depth (bytes): 128000

Reassign Size (bytes): 2000

Large Packet Size (bytes): 0

Reassign

Drop Limit (ms): 0

Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0

Disable Depth (bytes): 128000

- **Limite de dépôt** : durée après laquelle les paquets en attente dans le planificateur de classe sont supprimés. Ne s'applique pas à une classe en vrac.
- **Profondeur de dépôt** : seuil de profondeur de file d'attente après lequel les paquets sont supprimés.

- **Activer RED** : Random Early Detection (RED) assure un partage équitable des ressources de classe en rejetant les paquets en cas de congestion.
- **Réaffecter la taille** : longueur du paquet qui, lorsqu'elle est dépassée, entraîne la réaffectation du paquet à la classe spécifiée dans le champ Réaffecter la classe.
- **Réaffecter la classe** : Classe utilisée lorsque la longueur du paquet dépasse la longueur du paquet spécifiée dans le champ Réaffecter la taille.
- **Limite de désactivation** : durée pendant laquelle la duplication peut être désactivée pour empêcher les paquets dupliqués de consommer de la bande passante.
- **Désactiver la profondeur** : profondeur de la file d'attente du planificateur de classe, auquel moment les paquets dupliqués ne seront pas générés.
- **Classe ACK autonome TCP** : classe haute priorité à laquelle les accusés de réception autonomes TCP sont mappés lors des transferts de fichiers volumineux.

LAN to WAN

General

Class: 3 (citrix_class_3) Drop Limit (ms): 60

Large Packet Size (bytes): 0

☒ Enable RED

Large Packets

Drop Limit (ms): 50 Drop Depth (bytes): 128000

Duplicate Packets

Disable Limit (ms): 0 Disable Depth (bytes): 128000

Reassign

Reassign Class: 1 (citrix_class_1) Drop Limit (ms): 50

Reassign Size (bytes): 2000 Large Packet Size (bytes): 0

☒ Enable RED

Large Packets

Drop Limit (ms): 1 Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0 Disable Depth (bytes): 128000

TCP Standalone ACK

TCP Standalone ACK Class: Disabled <Default> Drop Limit (ms): 50

Large Packet Size (bytes): 0

☒ Enable RED

Large Packets

Drop Limit (ms): 0 Drop Depth (bytes): 0

11. Cliquez sur la vignette **WAN to LAN** pour configurer le comportement WAN to LAN pour cette règle.

- **Activer le reséquençage des paquets** : séquence les paquets dans l'ordre correct à la destination.

- **Temps de conservation** : intervalle de temps pendant lequel les paquets sont conservés pour le reséquençage, après quoi les paquets sont envoyés au réseau local.
- **Rejeter les paquets de reséquençage tardif** : Ignorez les paquets désorganisés arrivés après que les paquets nécessaires au reséquençage aient été envoyés au réseau local.
- **Balise DSCP : baliseDSCP** appliquée aux paquets qui correspondent à cette règle, avant de les envoyer au réseau local.

The screenshot shows the 'WAN to LAN' configuration window. Under the 'Packet Resequencing' section, there are two checked checkboxes: 'Enable Packet Resequencing' and 'Discard Late Resequencing Packets'. To the right, there is a 'Hold Time (ms):' label and an empty text input field. Below this, there is a 'DSCP Tag:' label and a dropdown menu currently showing 'af12'.

12. Cliquez sur la **vignette Inspection des paquets profonde** et sélectionnez **Activer la détection FTP passive** pour permettre à la règle de détecter le port utilisé pour le transfert de données FTP et d'appliquer automatiquement les paramètres de la règle au port détecté.
13. Cliquez sur **Appliquer**.

Remarque

Enregistrez la configuration, exportez-la dans la boîte de réception de gestion des modifications et lancez le processus de gestion des modifications.

Vérifier les règles

Dans l'Éditeur de configuration, accédez à **Surveillance > Flux**. Sélectionnez le champ **Type de flux** situé dans la section **Sélectionner des flux** en haut de la page **Flux**. En regard du champ **Type de flux**, une ligne de cases à cocher permet de sélectionner les informations de flux que vous souhaitez afficher. Vérifiez si les informations de flux sont conformes aux règles configurées.

Exemple :

La règle « Si l'adresse IP source est 172.186.30.74 et que l'adresse IP de destination est 172.186.10.89, définissez le **mode de transmission en** tant que chemin persistant » affiche les **données de flux** suivantes.

Select Flows

Flow Type:
☒ LAN to WAN
☒ WAN to LAN
☐ Internet Load Balancing Table
☐ TCP Termination Table
Max Rows to Display (Per Flow Type): 50
Filter (Optional):

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

Details	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IP	IP DSCP	HT Count	Service Type	Service Name	LAN GW IP	Age (ms)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
	172.166.30.74	172.166.10.89	LAN to WAN	55502	5003	TCP	default	88311	Virtual Path	DC-Client-1	LOCAL	0	88251	126639068	7558028	86763.328	3446.461	0.000	1	N/A	9	BULK	DC-WL-1->Client-1-WL-1	N/A	Persistent	iperf
	172.166.10.89	172.166.30.74	WAN to LAN	5003	55502	TCP	default	45207	Virtual Path	DC-Client-1	LOCAL	1	45207	2385488	3871.667	1634.405	1765.480	0.000	69	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Total LAN to WAN flows displayed: 1 out of 1
Total WAN to LAN flows displayed: 1 out of 1

Dans l’Éditeur de configuration, accédez à **Surveillance > Statistiques** et vérifiez les règles configurées.

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Statistics

Statistics

Show: Rules

☒ Enable Auto Refresh

5 seconds

Stop

Rule Statistics

Filter:

in Any column

Apply

Show 100 entries

Showing 1 to 100 of 275 entries

Num	Site	Service	IP Address		IP Proto	Port		VLAN ID	IP DSCP	LAN to WAN		WAN to LAN							
			Src	Dst		Src	Dst			Bytes	Packets	Bytes	Packets	Jitter (ms)	Packets Lost	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	
0	DC	DC-Client-1	*	*	TCP	5003	*	*	*	0	0	0	0						
1	DC	DC-Client-1	*	*	TCP	*	5003	*	*	426121168	285604	0	0						
2	DC	DC-Client-1	*	*	TCP	5060-5061	*	*	ef	0	0	0	0						
3	DC	DC-Client-1	*	*	TCP	*	5060-5061	*	ef	0	0	0	0						
4	DC	DC-Client-1	*	*	UDP	5060-5061	*	*	ef	0	0	0	0						
5	DC	DC-Client-1	*	*	UDP	*	5060-5061	*	ef	0	0	0	0						

Règles par nom d’application

May 6, 2021

La fonction de classification des applications permet à l’appliance Citrix SD-WAN d’analyser le trafic entrant et de les classer comme appartenant à une application ou à une famille d’applications particulière. Cette classification nous permet d’améliorer la qualité de service des familles d’applications ou d’applications individuelles en créant et en appliquant des règles d’application.

Vous pouvez filtrer les flux de trafic en fonction des types de correspondance d’application, de famille d’applications ou d’objet d’application et leur appliquer des règles d’application. Les règles d’application sont similaires aux règles IP (Internet Protocol). Pour plus d’informations sur les règles de propriété intellectuelle, voir Règles [par adresse IP et numéro de port](#).

Pour chaque règle d’application, vous pouvez spécifier le mode de transmission. Voici les modes de transmission disponibles :

- **Chemin d'équilibrage de charge** : le trafic d'application pour le flux est équilibré sur plusieurs chemins. Le trafic est envoyé par le meilleur chemin jusqu'à ce que ce chemin soit utilisé. Les paquets restants sont envoyés par le meilleur chemin suivant.
- **Chemin persistant** : le trafic d'application reste sur le même chemin jusqu'à ce que le chemin d'accès ne soit plus disponible.
- **Dupliquer le chemin** : le trafic d'application est dupliqué sur plusieurs chemins, ce qui augmente la fiabilité.

Les règles d'application sont associées aux classes. Pour plus d'informations sur les classes, reportez-vous à la section [Personnalisation des classes](#).

Par défaut, les cinq règles d'application prédéfinies suivantes sont disponibles pour les applications Citrix ICA :

Règle	Classe	Mode de transmission	Activer l'ajout							Redéfinir la séquence de la durée			Rejeter les paquets de la séquence tardif	Limite de charge (ms)	Profondeur de chute (octets)	Activer RED	Désactiver la limite (ms)	Désactiver la profondeur (octets)
			Retransmettre		Activer		durée		Rejeter									
			les paquets perdus	ga- tion de pa- quets	le resé- que- nce de pa- quets	de pen- sion (ms)	pa- quets	de	pa- quets	de								
HDX_Priority_0	Chemin (HDX_priority_tag_0)	True	False	True	250	Vrai	350	30000	Vrai	0	128000							
	équilibrage de charge																	
HDX_Priority_1	Chemin (HDX_priority_tag_1)	True	False	True	250	Vrai	350	30000	Vrai	0	128000							
	équilibrage de charge																	

Redéfinir la séquence de la Rejeter les paquets de séquence tardif												
Activer l'option de retransmission												
Mode de transmission												
Règle	Classe	Mode de transmission	les paquets perdus	ga- tion de pa- quets	le resé- que- nce de pa- quets	durée de pen- sion (ms)	Rejeter les paquets de séquence tardif	Limite de charge (ms)	Profondeur de chute (octets)	Activer RED	Désactiver la limite (ms)	Désactiver la profondeur (octets)
HDX_Priority_2	12	Chemin d'équili- brage de charge (HDX_priority_tag_2)	True	False	True	250	Vrai	350	30000	Vrai	0	128000
HDX_Priority_3	13	Chemin d'équili- brage de charge (HDX_priority_tag_3)	True	False	True	250	Vrai	350	30000	Vrai	0	128000
HDX	11	Chemin d'équili- brage de charge (interactive_high_class)	True	False	True	250	Vrai	350	30000	Vrai	0	128000

Comment les règles d'application sont-elles appliquées ?

Dans le réseau SD-WAN, lorsque les paquets entrants atteignent l'apppliance SD-WAN, les quelques paquets initiaux ne subissent pas la classification PPP. À ce stade, les attributs de règle IP tels que Class, TCP terminaison sont appliqués aux paquets. Après la classification PPP, les attributs de règle d'application tels que Classe, mode de transmission remplacent les attributs de règle IP.

Les règles IP ont plus d'attributs que les règles d'application. La règle d'application remplace seulement quelques attributs de règle IP, le reste des attributs de règle IP reste traité sur les paquets.

Par exemple, considérez que vous avez spécifié une règle d'application pour une application de messagerie Web telle que Google Mail qui utilise le protocole SMTP. Le jeu de règles IP pour le protocole SMTP est appliqué initialement avant la classification DPI. Après avoir analysé les paquets et les avoir classés comme appartenant à l'application Google Mail, la règle d'application spécifiée pour l'application Google Mail est appliquée.

Création de règles d'application

Pour créer des règles d'application :

1. Dans l'Éditeur de configuration SD-WAN, accédez à **Global > Jeux par défaut de chemin virtuel**.
2. Cliquez sur **Ajouter un jeu par défaut**, entrez un nom pour le jeu par défaut, puis cliquez sur **Ajouter**. Dans le champ **Section**, sélectionnez **Application QoS** et cliquez sur **+**.

Remarque

Vous pouvez également créer des règles d'application en accédant à **Connexions > Chemins virtuels > QoS de l'application** ou **Global > Jeu par défaut de chemin virtuel dynamique > QoS de l'application**.

? x

Add

Order: 100

Match Type: Application Object ▼

Application Objects: Any ▼

Rule Group Name: ALTHHTTP ▼

Source IP Address: 10.102.29.3/32

Destination IP Address: * ☐ Src = Dest

Source Port: *

Destination Port: * ☐ Src = Dest

WAN General

Transmit Mode: Load Balance Paths ▼

☐ Retransmit Lost Packets

Persistent Impedance(ms): 50

LAN to WAN

Class: 10 (realtime_class) ▼

Drop Limit (ms): 50

Drop Depth (bytes): 128000

☒ Enable RED

Duplicate Packets

Disable Limit (ms): 0

Disable Depth (bytes): 128000

WAN to LAN

☐ Enable Packet Resequencing

Resequencing Hold Time (ms):

☒ Discard Late Resequenced Packets

DSCP Tag: Any ▼

Add

Cancel

3. Dans le champ **Ordre**, tapez la valeur de l'ordre à définir quand la règle est appliquée par rapport à d'autres règles.
4. Dans le champ **Type de correspondance**, choisissez l'un des types de correspondance suivants :
 - **Application** : si ce type de correspondance est sélectionné, spécifiez l'application utilisée comme critère de correspondance pour ce filtre.
 - **Famille d'applications** : si ce type de correspondance est sélectionné, sélectionnez une famille d'applications utilisée comme critère de correspondance pour ce filtre.
 - **Objet Application** : si ce type de correspondance est sélectionné, sélectionnez un objet d'application utilisé comme critère de correspondance pour ce filtre.

Pour plus d'informations sur l'application, la famille d'applications et l'objet d'application, reportez-vous à la section [Classification des applications](#).

5. Dans le champ **Nom du groupe de règles**, sélectionnez un groupe de règles. Les statistiques des règles avec le même groupe de règles sont regroupées et peuvent être visualisées ensemble.
Pour afficher les groupes de règles, accédez à **Surveillance > Statistiques** et, dans le champ

Afficher, sélectionnez **Groupes de règles**.

Vous pouvez également ajouter des groupes de règles personnalisés. Pour de plus amples informations, consultez [Ajouter des applications personnalisées et activer MOS](#).

6. Spécifiez les critères de correspondance de règle d'application suivants pour filtrer le trafic d'application. Après le filtrage, les paramètres de règle sont appliqués aux services correspondant à ces critères.
 - **Adresse IP source** : adresse IP source et masque de sous-réseau pour correspondre au trafic.
 - **Adresse IP de destination** : adresse IP de destination et masque de sous-réseau pour correspondre au trafic.
 - **Port source** : numéro de port source ou plage de ports à comparer avec le trafic.
 - **Port de destination** : numéro de port de destination ou plage de ports à comparer avec le trafic.

Remarque

Choisissez **Src = Dest**, si l'adresse de protocole Internet source et de destination sont identiques.

7. Configurez les paramètres WAN généraux suivants :

- Dans le champ **Mode de transmission**, choisissez l'un des modes de transmission suivants :
 - **Chemin d'équilibrage de charge** : le trafic d'application pour le flux est équilibré sur plusieurs chemins. Le trafic est envoyé par le meilleur chemin jusqu'à ce que ce chemin soit complètement utilisé. Les paquets restants sont envoyés par le meilleur chemin suivant.
 - **Chemin persistant** : le trafic d'application reste sur le même chemin jusqu'à ce que le chemin d'accès ne soit plus disponible.

Dans le champ **Impédance persistante**, spécifiez la durée minimale en millisecondes pendant laquelle le trafic resterait dans le même chemin, jusqu'à ce que le temps d'attente sur le chemin soit plus long que la valeur configurée.
 - **Dupliquer le chemin** : le trafic d'application est dupliqué sur plusieurs chemins, ce qui augmente la fiabilité.
- Cochez **Retransmettre les paquets perdus** pour envoyer le trafic correspondant à cette règle à l'appliance distante via un service fiable et retransmettre les paquets perdus.

8. Configurez les paramètres LAN vers WAN :

- **Classe** : sélectionnez une classe à laquelle associer cette règle.

Vous pouvez également personnaliser les classes avant d'appliquer des règles. Pour plus d'informations, reportez-vous à la section [Personnaliser les classes](#).

- **Limite de dépôt** : durée après laquelle les paquets en attente dans le planificateur de classe sont supprimés. Ne s'applique pas à une classe en vrac.
- **Profondeur de dépôt** : Seuil de profondeur de file d'attente après lequel les paquets sont supprimés.
- **Activer RED** : Random Early Detection (RED) assure un partage équitable des ressources de classe en rejetant les paquets en cas de congestion.
- **Désactiver la limite** : Durée pendant laquelle la duplication peut être désactivée pour empêcher les paquets dupliqués de consommer de la bande passante.
- **Désactiver la profondeur** : profondeur de la file d'attente du planificateur de classe, auquel moment les paquets dupliqués ne seront pas générés.

9. Configurez le comportement WAN à LAN suivant pour cette règle :

- **Activer le reséquence des paquets** : séquence les paquets dans l'ordre correct à la destination.
- **Durée de suspension du reséquence** : intervalle de temps pendant lequel les paquets sont conservés pour le reséquence, après quoi les paquets sont envoyés au réseau local.
- **Rejeter les paquets de reséquence tardif** : Ignorez les paquets désorganisés arrivés après que les paquets nécessaires au reséquence aient été envoyés au réseau local.

10. Cliquez sur **Appliquer**.

Pour confirmer si des règles d'application sont appliquées au flux de trafic, accédez à **Surveillance > Flux**.

Notez l'identifiant de la règle de l'application et vérifiez si le type de classe et le mode de transmission correspondent à votre configuration de règle.

Flows Data

Both LAN to WAN and WAN to LAN Flows

Toggle Columns

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPF	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IFsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
172.166.30.74	172.166.10.89	LAN to WAN	35118	5001	UDP	default	4961	Virtual Path	DC-Clients-1	LOCAL	0	4959	7428582	292.687	3507.585	126.441	0.000	48	0	11	INTERACTIVE	DC-WL-1->Clients-1-WL-1	N/A	Duplicate

Total LAN to WAN flows displayed: 1 out of 1
Total WAN to LAN flows displayed: 0 out of 0

Vous pouvez surveiller la QoS de l'application, par exemple pas de paquets ou d'octets téléchargés, téléchargés ou supprimés sur chaque site, en accédant à **Surveillance > Statistiques > QoS de l'application**.

Le paramètre **Num** indique l'id de la règle de l'application. Vérifiez l'identifiant de la règle d'application obtenu à partir du flux.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

Monitoring > Statistics

Statistics

Show: Application QoS Enable Auto Refresh 5 seconds Refresh

Application QoS Statistics

Filter: in Any column Apply

Show: 100 entries Showing 1 to 12 of 12 entries

Num	Site	Service	IP Address		Port		Application Object	Application	Family	LAN to WAN		WAN to LAN		Dropped		Last Hit (DHHMM ago)
			Src	Dst	Src	Dst				Bytes	Packets	Bytes	Packets	Bytes	Packets	
0	DC	DC-Client-1	x	x	x	x	x	iperf	x	26325792	32262	0	0	267616	192	00:00
1	DC	DC-Client-1	x	x	x	x	x	ica_priority_0	x	0	0	0	0	0	0	0
2	DC	DC-Client-1	x	x	x	x	x	ica_priority_1	x	0	0	0	0	0	0	0
3	DC	DC-Client-1	x	x	x	x	x	ica_priority_2	x	0	0	0	0	0	0	0
4	DC	DC-Client-1	x	x	x	x	x	ica_priority_3	x	0	0	0	0	0	0	0
5	DC	DC-Client-1	x	x	x	x	x	ica	x	0	0	0	0	0	0	0
6	Client-1	DC-Client-1	x	x	x	x	x	iperf	x	0	0	4710	5	1484	1	00:38

Showing 1 to 12 of 12 entries

First Previous 1 Next Last

Création d'applications personnalisées

Vous pouvez utiliser des objets d'application pour définir des applications personnalisées en fonction des types de correspondance suivants :

- Protocole IP
- Nom de l'application
- Famille d'applications

Le classificateur DPI analyse les paquets entrants et les classe comme applications en fonction des critères de correspondance spécifiés. Vous pouvez utiliser ces applications personnalisées classées dans la QoS, le pare-feu et le routage des applications.

Conseil

Vous pouvez spécifier un ou plusieurs types de correspondance.

Vous pouvez afficher les rapports des applications personnalisées classées dans SD-WAN Center. Pour plus d'informations, reportez-vous à la section [Rapport d'application](#).

Pour créer des applications personnalisées :

1. Dans l'Éditeur de configuration, accédez à **Global > Applications > Applications personnalisées** et cliquez sur **+** .

2. Définissez les paramètres suivants :

- **Nom** : Nom de l'application personnalisée
- **Activer les rapports** : Permet d'afficher des rapports d'application personnalisés dans SD-WAN Center. Pour plus d'informations, veuillez consulter la section [Rapport d'application](#).
- **Priorité** : priorité de l'application personnalisée. Lorsque les paquets entrants correspondent à deux définitions d'application personnalisées ou plus, la définition d'application personnalisée avec la priorité la plus élevée est appliquée.

3. Cliquez sur + dans la section **Critères de correspondance de l'application**.

4. Sélectionnez l'un des types de correspondance suivants :

- **Protocole IP** : spécifiez le protocole, l'adresse IP réseau, le numéro de port et la balise DSCP.
- **Application** : spécifiez le nom de l'application, l'adresse IP réseau, le numéro de port et la balise DSCP.
- **Famille d'applications** : sélectionnez une famille d'applications et spécifiez l'adresse IP réseau, le numéro de port et la balise DSCP.

5. Cliquez sur + pour ajouter d'autres critères de correspondance d'application.

6. Cliquez sur **Appliquer**.

Ajouter des groupes de règles et activer MOS

May 6, 2021

Une application particulière du réseau peut être définie par le groupe de règles qui lui est appliqué. L'éditeur de configuration SD-WAN fournit une liste par défaut des groupes de règles. Vous pouvez également créer des groupes de règles personnalisés et marquer des règles IP individuelles ou des règles QoS d'application sur des applications.

Pour plus d'informations sur les règles, consultez [Règles par adresse IP et numéro de port](#) et [Règles par nom d'application](#).

Les statistiques des règles avec le même groupe de règles sont regroupées et peuvent être consultées ensemble.

Pour afficher des statistiques basées sur des groupes de règles, accédez à **Surveillance > Statistiques**, dans le **champ Afficher**, sélectionnez **Groupes de règles**.

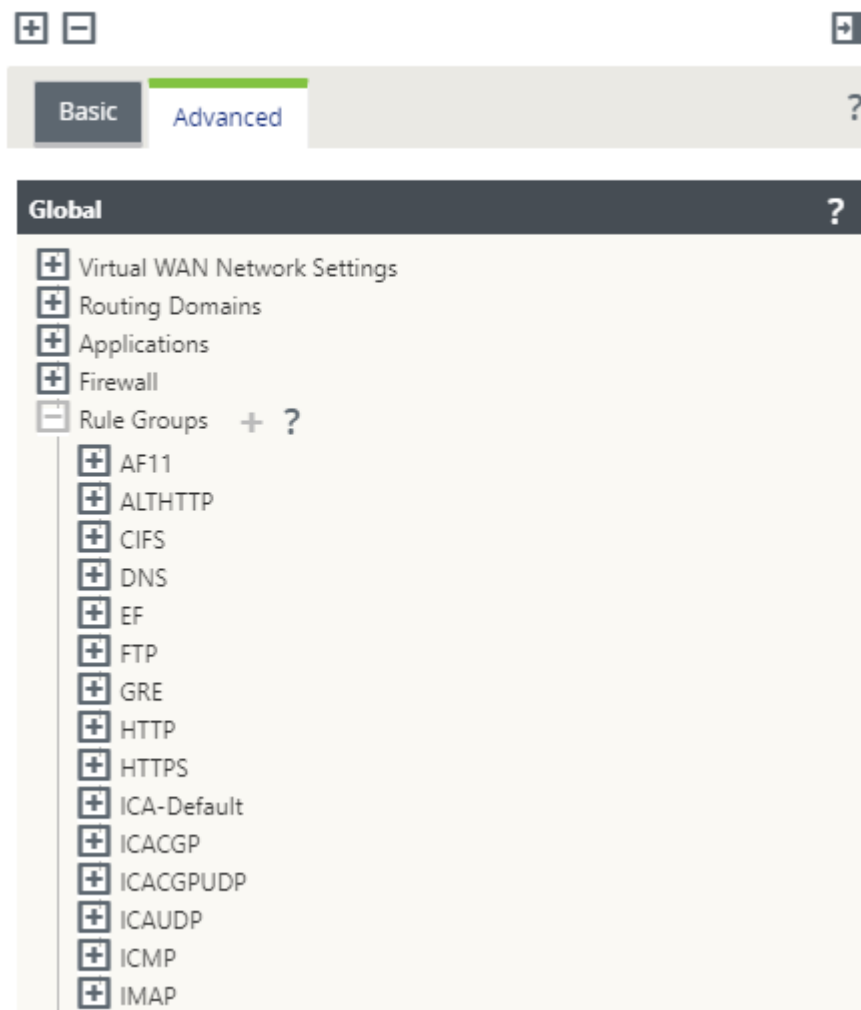
Le score d'opinion moyen (MOS) est une mesure numérique de la qualité de l'expérience qu'une application offre aux utilisateurs finaux. Il est principalement utilisé pour les applications VoIP. Dans SD-WAN, MOS est également utilisé pour évaluer la qualité des applications non-VoIP en jugeant le trafic comme s'il s'agissait d'un appel VoIP.

Le score moyen de MoS est calculé avec un intervalle d'échantillonnage de 1 minute. Le score de MO calculé par d'autres outils tiers peut varier en fonction de l'intervalle d'échantillonnage utilisé.

SD-WAN Center affiche le MOS pour le trafic existant qui passe par le chemin virtuel. Pour plus d'informations sur l'affichage de MOS dans SD-WAN Center, reportez-vous à la section [MOS pour applications](#).

Pour ajouter un groupe de règles personnalisé :

1. Dans l'Éditeur de configuration, accédez à **Global > Groupes de règles**. La liste par défaut des groupes de règles s'affiche.
2. Cliquez sur l'icône Ajouter (+).
3. Entrez le nom de l'application.
4. Cliquez sur l'icône d'édition et sélectionnez **Activer le MOS**.



5. Cliquez sur **Appliquer**.

Remarque

- Vous pouvez également activer l'estimation MOS pour les applications par défaut, en sélectionnant **Activer MOS**.
- Activez l'option Track Performance sous Règles pour estimer MOS pour les applications et l'afficher dans SD-WAN Center. Pour plus d'informations, reportez-vous à la section [MOS pour applications](#).

Classification des demandes

November 16, 2022

Les appliances Citrix SD-WAN effectuent une inspection approfondie des paquets (DPI) pour identifier et classer les applications à l'aide des techniques suivantes :

- Classification de la bibliothèque DPI
- Classification ICA (Independent Computing Architecture) propriétaire Citrix
- API fournisseur d'applications (par exemple, API REST Microsoft pour Office 365)
- Classification d'application basée sur un nom de domaine

Classification de la bibliothèque DPI

La bibliothèque Deep Packet Inspection (DPI) reconnaît des milliers d'applications commerciales. Il permet la découverte et la classification en temps réel des applications. À l'aide de la technologie DPI, l'appliance SD-WAN analyse les paquets entrants et classe le trafic comme appartenant à une application ou à une famille d'applications particulière. La classification des applications pour chaque connexion prend quelques paquets.

Pour activer la classification des bibliothèques PPP, dans l'**Éditeur de configuration**, accédez à **Global > Applications > Paramètres PPP** et **activez la case à cocher Activer l'inspection approfondie des paquets**.

Classification ICA

Les appliances Citrix SD-WAN peuvent également identifier et classer le trafic Citrix HDX pour les applications et les bureaux virtuels. Citrix SD-WAN reconnaît les variantes suivantes du protocole ICA :

- ICA
- ICA-CGP
- ICA à flux unique (SSI)
- ICA multiflux (MSI)
- ICA sur TCP
- L'ICA sur l'UDP/EDT
- ICA sur les ports non standard (y compris ICA multi-ports)
- Transport adaptatif HDX
- ICA sur WebSocket (utilisé par le récepteur HTML5)

Remarque

La classification du trafic ICA livré via SSL/TLS ou DTLS n'est pas prise en charge par SD-WAN Standard Edition, mais est prise en charge par SD-WAN Premium Edition et SD-WAN WANOP Edition.

La classification du trafic réseau se fait au cours des connexions initiales ou de l'établissement du

flux. Par conséquent, les connexions préexistantes ne sont pas classées comme ICA. La classification des connexions est également perdue lorsque la table de connexion est effacée manuellement.

Le trafic Framehawk et l'Audio-over-UDP/RTP ne sont pas classés comme des applications HDX. Ils sont signalés comme « UDP » ou « protocole inconnu ».

Depuis la version 10 version 1, l'apppliance SD-WAN peut différencier chaque flux de données ICA dans l'ICA multi-flux, même dans une configuration monoport. Chaque flux ICA est classé comme une application distincte avec sa propre classe QoS par défaut pour la hiérarchisation.

- Pour que la fonctionnalité ICA Multi-Stream fonctionne correctement, vous devez disposer du SD-WAN Standard Edition 10.1 ou supérieure ou du SD-WAN Premium Edition.
- Pour que les rapports utilisateur HDX soient affichés sur SDWAN-Center, vous devez disposer du SD-WAN Standard Edition ou Premium Edition 11.0 ou supérieur.

Configuration logicielle minimale requise pour le canal virtuel d'information HDX :

- Une version actuelle de Citrix Virtual Apps and Desktops (anciennement XenApp et XenDesktop), puisque la fonctionnalité requise a été introduite dans XenApp et XenDesktop 7.17 et n'est pas incluse dans la version de service à long terme 7.15.
- Version de l'application Citrix Workspace (ou de son prédécesseur, Citrix Receiver) prenant en charge l'ICA multi-flux et le canal virtuel d'informations HDX Insights, CTXNSAP. Recherchez **HDX Insight avec NSAP VC** et ICA multiport/multi-flux dans la [matrice des fonctionnalités de l'application Citrix Workspace](#). Consultez les versions actuellement prises en charge sur [HDX Insights](#).
- À partir de la version 11.2, la duplication des paquets est désormais activée par défaut pour le trafic HDX en temps réel lorsque l'ICA multflux est en cours d'utilisation.

Une fois classée, l'application ICA peut être utilisée dans les règles d'application et pour afficher des statistiques de demande semblables à celles d'autres applications classifiées.

Il existe cinq règles d'application par défaut pour les applications ICA, une pour chacune des balises de priorité suivantes :

- Architecture informatique indépendante (Citrix) (ICA)
- ICA en temps réel (ica_priority_0)
- ICA Interactive (ica_priority_1)
- Transfert en bloc ICA (ica_priority_2)
- Contexte ICA (ica_priority_3)

Pour plus d'informations, consultez la section [Règles par nom d'application](#)

Si vous exécutez une combinaison de logiciels qui ne prennent pas en charge l'ICA Multi-Stream sur

un seul port, alors pour effectuer la QoS, vous devez configurer plusieurs ports, un pour chaque flux ICA.

Pour classer HDX sur des ports non standard comme configurés dans la stratégie de serveur XA/XD, vous devez ajouter ces ports dans les configurations de ports ICA. En outre, pour faire correspondre le trafic sur ces ports à des règles IP valides, vous devez mettre à jour les règles IP ICA.

Dans la liste IP et ports ICA, vous pouvez spécifier les ports non standard utilisés dans la stratégie XA/XD pour traiter la classification HDX. L'adresse IP est utilisée pour restreindre davantage les ports à une destination spécifique. Utilisez '*' pour le port destiné à n'importe quelle adresse IP. L'adresse IP avec une combinaison de port SSL est également utilisée pour indiquer que le trafic est probablement ICA même si le trafic n'est pas finalement classé comme ICA. Cette indication est utilisée pour envoyer des enregistrements AppFlow L4 pour prendre en charge les rapports multi-sauts dans Citrix Application Delivery Management.

Pour activer la classification basée sur ICA, dans l'**Éditeur de configuration**, accédez à **Global > Applications > Paramètres DPI** et **activez la case à cocher Activer l'inspection approfondie des paquets pour les applications Citrix ICA**.

Classification basée sur l'API du fournisseur d'applications

Citrix SD-WAN prend en charge la classification basée sur l'API du fournisseur d'applications suivante :

- Office 365. Pour plus d'informations, consultez la section [Optimisation d'Office 365](#).
- Service Citrix Cloud et Citrix Gateway. Pour plus d'informations, consultez la section [Gateway Service Optimization](#).

Classification d'application basée sur un nom de domaine

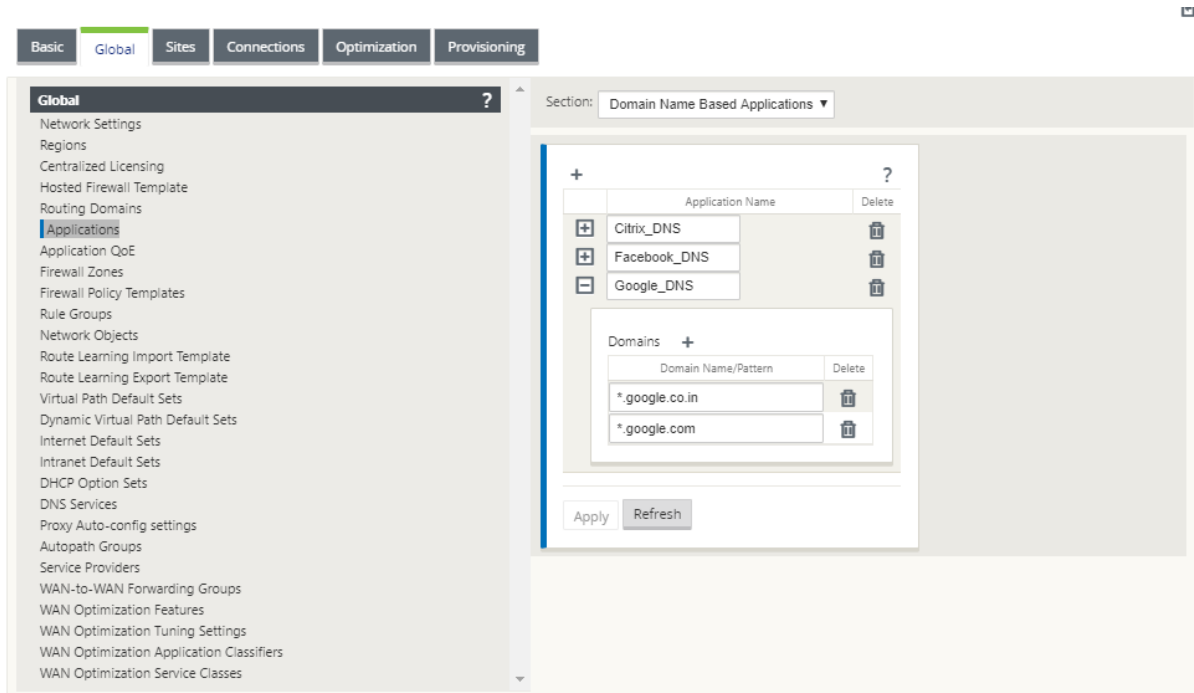
Le moteur de classification DPI est amélioré pour classer les applications en fonction du nom de domaine et des modèles. Une fois que le redirecteur DNS a intercepté et analysé les demandes DNS, le moteur DPI utilise le classificateur IP pour effectuer la première classification des paquets. D'autres bibliothèques DPI et la classification ICA sont effectuées et l'ID d'application basé sur le nom de domaine est ajouté.

La fonctionnalité d'application basée sur un nom de domaine vous permet de regrouper plusieurs noms de domaine et de les traiter comme une seule application. Faciliter l'application du pare-feu, de la direction des applications, de la qualité de service et d'autres règles. Un maximum de 64 applications basées sur des noms de domaine peuvent être configurées.

Pour définir des applications basées sur un nom de domaine, dans l'éditeur de configuration, accédez à **Global > Applications > Applications basées sur un nom de domaine**. Entrez un nom d'applica-

tion et ajoutez les noms de domaine ou les modèles requis. Vous pouvez entrer le nom de domaine complet ou utiliser des caractères génériques au début. Les formats de noms de domaine suivants sont autorisés :

- exemple.com
- *.exemple.com



Les applications basées sur un nom de domaine classifié sont utilisées pour configurer les éléments suivants :

- [Proxy DNS](#)
- [Transparent DNS](#)
- Objets d'application
- [Itinéraires d'application](#)
- [Stratégie de pare-feu](#)
- [Règles QoS d'application](#)
- [QoS des applications](#)

Remarque

À partir de la version 11.4.2, les applications basées sur le nom de domaine prennent en charge les ports et le protocole configurables dans le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez [Domaines et applications](#).

Limitations

- S'il n'y a pas de requête/réponse DNS correspondant à une application basée sur un nom de domaine, le moteur DPI ne classe pas l'application basée sur un nom de domaine et n'applique donc pas les règles d'application correspondant à l'application basée sur un nom de domaine.
- Si un objet Application est créé de telle sorte que la plage de ports inclut le port 80 et/ou le port 443, avec un type de correspondance d'adresse IP spécifique qui correspond à une application basée sur un nom de domaine, le moteur DPI ne classe pas l'application basée sur un nom de domaine.
- Si des proxys Web explicites sont configurés, vous devez ajouter tous les modèles de noms de domaine au fichier PAC, pour vous assurer que la réponse DNS ne renvoie pas toujours la même adresse IP.
- Les classifications d'applications basées sur un nom de domaine sont réinitialisées lors de la mise à niveau de Le reclassement se fait en fonction des techniques de classification antérieures à la version 11.0.2, telles que la classification de la bibliothèque DPI, la classification ICA et la classification basée sur les API d'application fournisseur.
- Les signatures d'application apprises (adresses IP de destination) par classification d'application basée sur un nom de domaine sont réinitialisées lors de la mise à jour de configuration.
- Seules les requêtes DNS standard et leurs réponses sont traitées.
- Les enregistrements AAAA ou IPv6 ne sont pas pris en charge.
- Les enregistrements de réponse DNS répartis sur plusieurs paquets ne sont pas traités. Seules les réponses DNS dans un seul paquet sont traitées.
- DNS sur TCP n'est pas pris en charge.
- Seuls les domaines de premier niveau sont pris en charge en tant que modèles de noms de domaine.

Classement du trafic chiffré

L'apppliance Citrix SD-WAN détecte et signale le trafic chiffré, dans le cadre des rapports d'application, selon les deux méthodes suivantes :

- Pour le trafic HTTPS, le moteur DPI inspecte le certificat SSL pour lire le nom commun, qui porte le nom du service (par exemple - Facebook, Twitter). Selon l'architecture de l'application, un seul certificat peut être utilisé pour plusieurs types de services (par exemple, e-mail, news, etc.). Si différents services utilisent des certificats différents, le moteur DPI serait en mesure de différencier les services.
- Pour les applications qui utilisent leur propre protocole de cryptage, le moteur DPI recherche des modèles binaires dans les flux. Par exemple, dans le cas de Skype, le moteur DPI recherche un modèle binaire à l'intérieur du certificat et détermine l'application.

Pour configurer les paramètres de classification des applications :

1. Dans l'**éditeur de configuration**, cliquez sur **Global > Applications > Paramètres**.

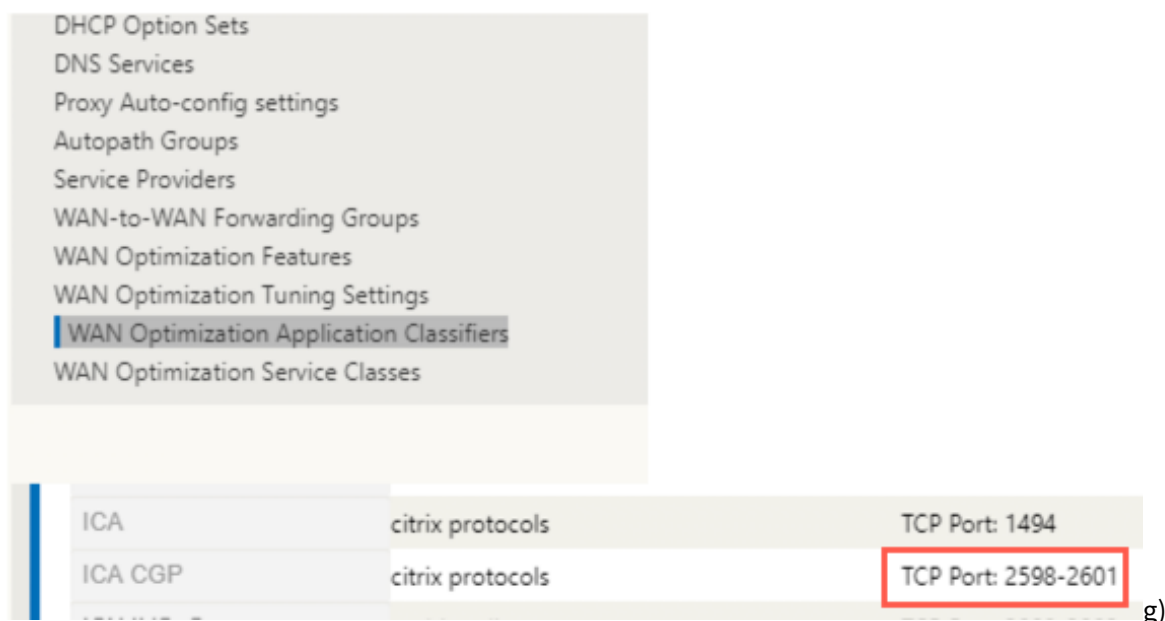
The screenshot shows the 'Settings' page in the Citrix SD-WAN configuration interface. The page has a blue sidebar on the left and a main content area. At the top right of the main area is a question mark icon. The 'Settings' title is in large bold font. Below it are two checked checkboxes: 'Enable Deep Packet Inspection' and 'Enable Deep Packet Inspection for Citrix ICA Applications'. A section titled 'Citrix ICA Deep Packet Inspection Settings' contains two more checked checkboxes: 'Enable HDX User Reporting' and 'Enable Multi-Stream ICA'. Below these is a section titled 'DPI ICA IP and Port List' which contains five rows of input fields. Each row has a label for the IP address (DPI ICA IP-1 through DPI ICA IP-5) and a label for the port (DPI ICA Port-1 through DPI ICA Port-5). The first three rows have pre-filled port values: 2599, 2600, and 2601 respectively. The last two rows have empty input fields.

DPI ICA IP and Port List	
DPI ICA IP-1:	DPI ICA Port-1: 2599
DPI ICA IP-2:	DPI ICA Port-2: 2600
DPI ICA IP-3:	DPI ICA Port-3: 2601
DPI ICA IP-4:	DPI ICA Port-4:
DPI ICA IP-5:	DPI ICA Port-5 :

Remarque

Si vous ajoutez un port ICA supplémentaire pour le déploiement multiport, ces ports doivent être ajoutés dans les classificateurs d'applications d'optimisation Wan. Sinon, le

trafic sur les trois ports supplémentaires ne sera pas transféré à WANOP. Seul le port 2598 par défaut est transféré si ICA est configuré pour optimiser.



2. Sélectionnez **Activer l'inspection approfondie des paquets**. Cela permet de classer les applications sur l'apppliance. Vous pouvez, afficher et surveiller les statistiques d'application sur SD-WAN Center. Pour plus d'informations, consultez la section [Rapport d'application](#).

Remarque

Par défaut, l'**option Enable Deep Packet Inspection** collecte des statistiques pour les données classifiées.

3. Sélectionnez **Activer l'inspection approfondie des paquets pour les applications Citrix ICA**. Cela permet de classer les applications Citrix ICA et de collecter des statistiques sur les utilisateurs, les sessions et le nombre de flux. Sans cette option activée, une partie de la saveur du trafic HDX peut encore être classée et QoE calculée, mais les statistiques sur SD-WAN Center ne sont pas disponibles. Vous pouvez, afficher et surveiller les statistiques des applications ICA sur SD-WAN Center. Cette option est activée par défaut. Pour plus d'informations, consultez la section [Rapports HDX](#).
4. Sélectionnez **Activer HDX User Reporting** pour générer des rapports utilisateur nouvellement ajoutés (HDX Summary, HDX User Sessions et **HDX Apps**). Ces rapports sont disponibles dans SD-WAN Center. Cela ne s'applique pas au rapport **HDX Site Stats**. Cette option est disponible au niveau global et au niveau du site similaire pour activer l'option DPI. Pour **activer le rapport utilisateur HDX** au niveau du site, dans l'**éditeur de configuration**, cliquez sur **Connexions > Applications**.

Section: DPI Settings

☐ Use Global Application Settings

☒ Enable Deep Packet Inspection

☒ Enable Deep Packet Inspection for Citrix ICA Applications

Citrix ICA Deep Packet Inspection Settings

☐ Enable HDX User Reporting

☐ Enable Multi-Stream ICA

DPI ICA IP and Port List

DPI ICA IP-1:	DPI ICA Port-1:
<input type="text"/>	<input type="text"/>
DPI ICA IP-2:	DPI ICA Port-2:
<input type="text"/>	<input type="text"/>
DPI ICA IP-3:	DPI ICA Port-3:
<input type="text"/>	<input type="text"/>
DPI ICA IP-4:	DPI ICA Port-4:
<input type="text"/>	<input type="text"/>
DPI ICA IP-5:	DPI ICA Port-5:
<input type="text"/>	<input type="text"/>

Apply Revert

5. Dans le **port ICA DPI**, spécifiez les ports non standard utilisés dans la stratégie XA/XD à traiter pour la classification HDX. N'incluez pas les numéros de port standard 2598 ou 1494 dans cette liste, car ils sont déjà inclus en interne.
6. Dans **IP ICA DPI**, spécifiez l'adresse IP à utiliser pour restreindre davantage les ports à la destination spécifique.

Remarque

Utilisez '*' pour le port destiné à n'importe quelle adresse IP.

7. Cliquez sur **Appliquer**

Vous pouvez configurer individuellement les paramètres de classification des applications sur chaque site. Cliquez sur **Connexions**, sélectionnez un site et cliquez sur **Paramètres des applications**. Vous pouvez également choisir d'utiliser les paramètres globaux de l'application.

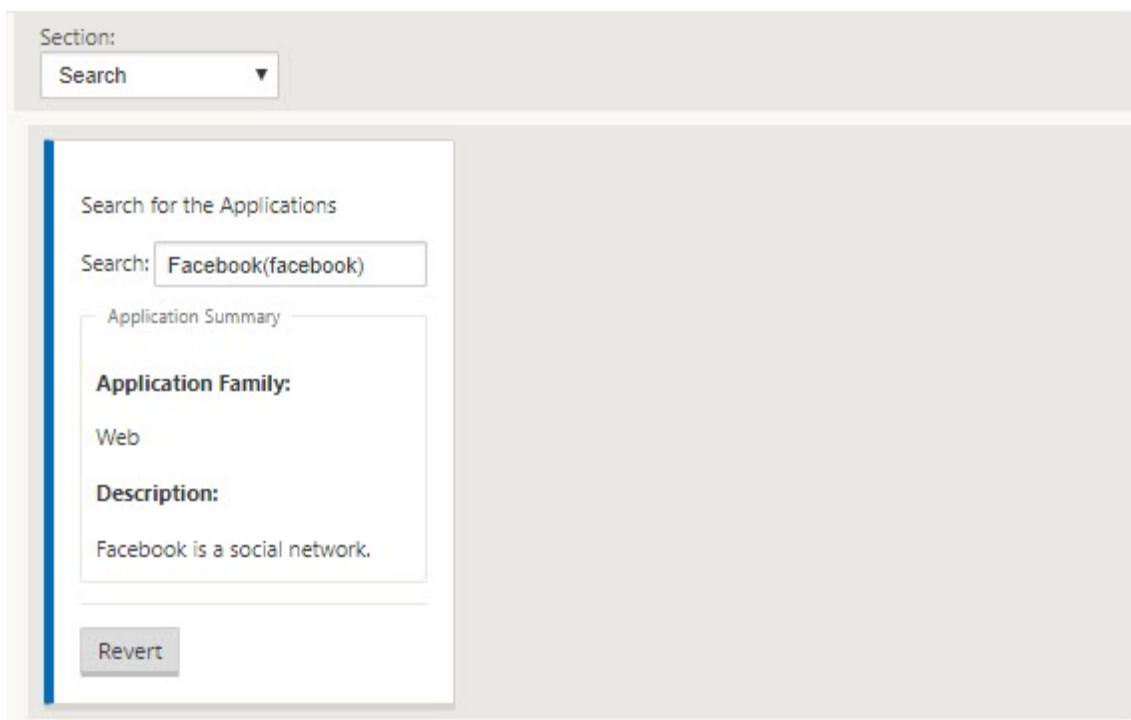
Rechercher des applications

Vous pouvez rechercher une application pour déterminer le nom de famille de l'application. Une brève description de la demande est également fournie.

Pour rechercher une application :

1. Dans l'Éditeur de configuration, cliquez sur **Global > Applications > Rechercher**.
2. Dans le champ Rechercher, tapez le nom de l'application et cliquez sur Entrée.

Une brève description de l'application et du nom de la famille de l'application s'affiche.



Les fonctionnalités suivantes utilisent l'application comme type de correspondance :

- [Stratégie de pare-feu](#)
- [Règles QoS d'application](#)
- [QoE des applications](#)

Remarque

Pour plus d'informations sur les applications que l'appliance SD-WAN peut identifier à l'aide de l'inspection approfondie des paquets, consultez [Bibliothèque de signatures d'application](#).

Objets d'application

Les objets d'application vous permettent de regrouper différents types de critères de correspondance en un seul objet qui peut être utilisé dans les stratégies de pare-feu et la direction d'application. Le protocole IP, l'application et la famille d'applications sont les types de correspondance disponibles.

Les fonctionnalités suivantes utilisent l'objet d'application comme type de correspondance :

- [Itinéraires d'application](#)
- [Stratégie de pare-feu](#)
- [Règles QoS d'application](#)
- [QoE des applications](#)

Pour créer un objet d'application :

1. Dans l'éditeur de configuration, cliquez sur **Global > Applications > Objets d'application**.
2. Cliquez sur **Ajouter** et, dans le champ **Nom**, saisissez un nom pour l'objet.

Add ? x

Name: Priority: ☒ Enable Reporting

Application Match Criteria +

Match Type	Application Family	Application	Protocol	Network IP Address 1	Port 1
Application ▼		Salesforce(salesforce)	Any ▼	192.168.3.4/3	*
Application ▼		Onjira.com (JIRA)(jira)	Any ▼	192.168.4.4/3	*

Add **Cancel**

3. Sélectionnez **Activer la création de rapports** pour activer l'affichage des rapports d'application personnalisés dans Citrix SD-WAN Center. Pour plus d'informations, voir [Rapport d'application](#).
4. Dans le champ **Priorité**, entrez la priorité de l'objet application. Lorsque les paquets entrants correspondent à deux définitions d'objet d'application ou plus, l'objet d'application ayant la priorité la plus élevée est appliqué.
5. Cliquez sur **+** dans la section **Critères de correspondance des demandes**.
6. Sélectionnez l'un des types de correspondance suivants :
 - **Protocole IP** : spécifiez le protocole, l'adresse IP réseau, le numéro de port et la balise DSCP.
 - **Application** : spécifiez le nom de l'application, l'adresse IP réseau, le numéro de port et la balise DSCP.
 - **Famille d'applications** : sélectionnez une famille d'applications et spécifiez l'adresse IP du réseau, le numéro de port et la balise DSCP.
7. Cliquez sur **+** pour ajouter d'autres critères de correspondance d'application.
8. Cliquez sur **Ajouter**.

Utilisation de la classification des applications avec un pare-feu

La classification du trafic en tant qu'applications, familles d'applications ou noms de domaine vous permet d'utiliser l'application, les familles d'applications et les objets d'application comme types de correspondance pour filtrer le trafic et appliquer la stratégie et les règles de pare-feu. Elle s'applique à toutes les politiques pré, postales et locales. Pour plus d'informations sur le pare-feu, consultez la section [Pare-feu avec état et prise en charge NAT](#).

Edit Firewall Policy ? x

Priority: 100

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action: Allow Log Interval (s): 0 Log Start Log End Connection State Tracking: Use Site Setting

Match Type: IP Protocol Application Application Family Application Objects

Application Objects: Any Application: Application Family:

DSCP: Any Allow Fragments Reverse Also Match Established

Source Service Type: Any Source Service Name: Any Source IP: Source Port:

Dest Service Type: Any Dest Service Name: Any Dest IP: Dest Port:

Apply Cancel

Affichage de la classification des applications

Après avoir activé la classification de l'application, vous pouvez afficher le nom de l'application et les détails de la famille d'applications dans les rapports suivants :

- Statistiques de connexion au pare-feu
- Informations sur les flux
- Statistiques relatives aux applications

Statistiques de connexion au pare-feu

Dans l'éditeur de configuration, accédez à **Surveillance > Pare-feu**. Sous la section **Connexions**, les colonnes **Application** et **Famille** répertorient les applications et la famille associée.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics: Connections 50
Maximum entries to display: 50
Filtering: Application: Any Family: Any
IP Protocol: Any Source Zone: Any Destination Zone: Any
Source Service Type: Any Source Service Instance: Any Source IP: Source Port:
Destination Service Type: Any Destination Service Instance: Any Destination IP: Destination Port:
Refresh Clear Connections Help

Connections

Application	Family	IP Protocol	Source				Destination				Sent							
			IP Address	Port	Service Type	Service Name	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	
GoToMeeting Online Meeting(gotomeeting)	Audio/Video	TCP	172.16.30.30	54612	Local	Site1_VL1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	4	259	0.716	0.371
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	47397	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	1	60	0.262	0.126
Network Time Protocol(ntp)	Network Service	UDP	172.16.30.30	48743	Local	Site1_VL1	Default_LAN_Zone	91.189.94.4	123	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	NEW	No	1	76	0.264	0.160
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	41348	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	118	0.476	0.225
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44961	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	114	0.513	0.234
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44119	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	1	60	0.263	0.126
Google Generic(google_gen)	Web	TCP	172.16.30.30	45706	Local	Site1_VL1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	394	1.017	0.534
BING	Custom Application	TCP	172.16.30.30	45464	Local	Site1_VL1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	31	1348	6.428	2.236
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	59856	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	116	0.410	0.190
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	49607	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	122	0.354	0.173
Mozilla.com - Mozilla.org(mozilla)	Web	TCP	172.16.30.30	46324	Local	Site1_VL1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	395	1.551	0.817
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	52889	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	112	0.332	0.149
Microsoft(microsoft)	Web	TCP	172.16.30.30	51194	Local	Site1_VL1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	397	1.433	0.758

Connections Displayed: 13
Connections in Use: 13/128000

Si vous n'activez pas la classification des applications, les colonnes **Application** et **Famille** n'affichent aucune donnée.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics: Connections 50
Maximum entries to display: 50
Filtering: Application: Any Family: Any
IP Protocol: Any Source Zone: Any Destination Zone: Any
Source Service Type: Any Source Service Instance: Any Source IP: Source Port:
Destination Service Type: Any Destination Service Instance: Any Destination IP: Destination Port:
Refresh Clear Connections Help

Connections

Application	Family	IP Protocol	Source				Destination				Sent				Received							
			IP Address	Port	Service Type	Service Name	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	
*	*	TCP	172.16.30.30	54632	Local	Site1_VL1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	4	259	0.909	0.471	3	217	0.682	0.395
*	*	UDP	172.16.30.30	41664	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	112	0.383	0.171	2	156	0.383	0.239
*	*	UDP	172.16.30.30	36817	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	122	0.408	0.199	2	196	0.408	0.320
*	*	TCP	172.16.30.30	45726	Local	Site1_VL1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	394	1.207	0.634	4	744	0.804	1.197
*	*	TCP	172.16.30.30	45484	Local	Site1_VL1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	26	1136	6.780	2.370	53	63972	13.820	133.449
*	*	UDP	172.16.30.30	53904	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	118	0.589	0.278	2	272	0.589	0.641
*	*	UDP	172.16.30.30	49809	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	116	0.513	0.238	2	354	0.513	0.727
*	*	TCP	172.16.30.30	51214	Local	Site1_VL1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	397	1.796	0.951	4	361	1.197	0.864
*	*	TCP	172.16.30.30	46344	Local	Site1_VL1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	395	1.904	1.003	4	387	1.269	0.982
*	*	UDP	172.16.30.30	52627	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	114	0.622	0.283	2	210	0.622	0.522

Connections Displayed: 10
Connections in Use: 10/128000

Informations sur les flux

Dans l'Éditeur de configuration, accédez à **Surveillance > Flux**. Sous la section **Données de flux**, la colonne **Application** répertorie les détails de l'application.

Monitoring > Flows

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 60

Filter (Optional): [Help](#)

[Refresh](#)

Flows Data

Both LAN to WAN and WAN to LAN Flows

IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6979	2	112	0.287	0.128	0.131	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4967	2	118	0.403	0.190	0.184	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	28	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4963	27	1176	4.950	1.725	2.257	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	bing
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4811	2	114	0.416	0.190	0.190	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	5	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5715	4	259	0.644	0.334	0.294	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	gotomeeting
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6717	2	122	0.298	0.145	0.136	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6692	6	394	0.876	0.460	0.399	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	google_gen
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4016	6	395	1.254	0.660	0.572	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	mozilla
P default	3	INTERNET	-	LOCAL	5711	2	116	0.350	0.162	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4775	6	397	1.222	0.647	0.557	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	microsoft
P default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6883	2	156	0.288	0.180	0.131	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
P default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4936	2	272	0.403	0.439	0.184	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
P default	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4969	53	64273	9.730	94.396	4.437	0.000	94	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	bing
P cs4	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4804	2	210	0.416	0.350	0.190	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A

Total LAN to WAN flows displayed: 10 out of 10
Total WAN to LAN flows displayed: 10 out of 10

Statistiques relatives aux applications

Dans l'Éditeur de configuration, accédez à **Surveillance > Statistiques**. Sous la section **Statistiques d'application**, la colonne **Application** répertorie les détails de l'application.

DashboardMonitoringConfiguration

Statistics

Monitoring > Statistics

Statistics

Show Applications ☐ Enable Auto Refresh 5 seconds Refresh ☒ Show latest data.

Applications Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 35 of 35 entries

Application	Family	Bytes Received	Bytes Sent	Total Bytes
Adobe	Web	122923	45896	168819
Akamai Technologies CDN	Web	40935	87002	127937
Amazon Ad System	Web	25405	8439	33844
Amazon Generic Services	Web	44130	11405	55535
Amazon Web Services/Cloudfront CDN	Web	17147	3804	20951
Bing.com (formerly MSN Search)	Web	914343	74913	989256
BoldChat Live Chat	Web	224358	97936	322294
Clicktale	Web	323870	69287	393157

Résolution des problèmes

Après avoir activé la classification des applications, vous pouvez afficher les rapports sous la section **Surveillance** et vous assurer qu'ils affichent les détails de l'application. Pour plus d'informations, consultez la section [Affichage de la classification des applications](#).

S'il y a un comportement inattendu, collectez le bundle de diagnostics STS pendant que le problème est observé et partagez-le avec l'équipe de support Citrix.

Le pack STS peut être créé et téléchargé à l'aide **de Configuration > Maintenance du système > Diagnostics > Informations de diagnostic**.

Équité QoS (RED)

May 6, 2021

La fonctionnalité d'équité QoS améliore l'équité des flux de chemins virtuels multiples en utilisant les classes QoS et la détection précoce aléatoire (RED). Un chemin virtuel peut être affecté à l'une des 16 classes différentes. Une classe peut être l'un des trois types de base :

- Les classes en temps réel servent des flux de trafic qui exigent un service rapide jusqu'à une certaine limite de bande passante. Une faible latence est préférable au débit agrégé.
- Les classes interactives ont une priorité inférieure à celle du temps réel, mais ont une priorité absolue sur le trafic en vrac.
- Les classes en vrac obtiennent ce qui reste des classes en temps réel et interactives, car la latence est moins importante pour le trafic en vrac.

Les utilisateurs spécifient différentes exigences de bande passante pour différentes classes, ce qui permet au planificateur de chemin virtuel d'arbitrer les demandes de bande passante concurrentes provenant de plusieurs classes du même type. Le planificateur utilise l'algorithme HFSC (Hierarchical Fair Service Curve) pour assurer l'équité entre les classes.

HFSC offre des cours dans l'ordre de premier entré, premier sorti (FIFO). Avant de planifier des paquets, Citrix SD-WAN examine la quantité de trafic en attente pour la classe de paquets. Lorsque le trafic excessif est en attente, les paquets sont abandonnés au lieu d'être placés dans la file d'attente (dépose de queue).

Pourquoi TCP provoque-t-il une file d'attente ?

TCP ne peut pas contrôler la vitesse à laquelle le réseau peut transmettre des données. Pour contrôler la bande passante, TCP implémente le concept d'une fenêtre de bande passante, qui est la quantité de trafic non reconnu qu'il autorise dans le réseau. Il commence d'abord par une petite fenêtre et double la taille de cette fenêtre chaque fois que des accusés de réception sont reçus. C'est ce qu'on appelle la phase de démarrage lent ou de croissance exponentielle.

TCP identifie la congestion réseau en détectant les paquets supprimés. Si la pile TCP envoie une rafale de paquets qui introduisent un délai de 250 ms, TCP ne détecte pas la congestion si aucun des paquets

n'est rejeté, de sorte qu'il continue d'augmenter la taille de la fenêtre. Il pourrait continuer à le faire jusqu'à ce que le temps d'attente atteigne 600 à 800 ms.

Lorsque TCP n'est pas en mode de démarrage lent, il réduit la bande passante de moitié lorsque la perte de paquets est détectée, et augmente la bande passante autorisée d'un paquet pour chaque accusé de réception reçu. TCP alterne donc entre la pression ascendante sur la bande passante et la marche arrière. Malheureusement, si le temps d'attente atteint 800 ms par la perte de paquets de temps est détectée, la réduction de la bande passante provoque un retard de transmission.

Incidence sur l'équité de la qualité de service

Lorsque le délai de transmission TCP se produit, fournir n'importe quel type de garantie d'équité dans une classe de chemin virtuel est difficile. Le planificateur de chemin virtuel doit appliquer un comportement de dépose pour éviter de contenir d'énormes quantités de trafic. La nature des connexions TCP est telle qu'un petit nombre de flux de trafic pour remplir le chemin virtuel, ce qui rend difficile pour une nouvelle connexion TCP d'atteindre une part équitable de la bande passante. Le partage de la bande passante nécessite de s'assurer que la bande passante est disponible pour les nouveaux paquets à transmettre.

Détection précoce aléatoire

La détection précoce aléatoire (RED) empêche les files d'attente de trafic de se remplir et provoque des actions de largage. Il empêche la mise en file d'attente inutile par le planificateur de chemin virtuel, sans affecter le débit qu'une connexion TCP peut atteindre.

Comment utiliser RED

1. Démarrez une session TCP pour créer le chemin virtuel. Vérifiez qu'avec RED activé, le temps d'attente de cette classe reste à environ 50 ms dans l'état stable.
2. Démarrez une deuxième session TCP et vérifiez que les deux sessions TCP partagent uniformément la bande passante du chemin virtuel. Vérifiez que le temps d'attente de la classe reste à l'état stationnaire.
3. Vérifiez que l'Éditeur de configuration peut être utilisé pour activer et désactiver RED et qu'il affiche la valeur correcte pour le paramètre.
4. Vérifiez que la page Afficher la configuration dans l'interface graphique SD-WAN indique si RED est activé pour une règle.

Comment activer RED

1. Accédez à l'**éditeur de configuration** > **Connexions** > **Chemins virtuels**[> **Sélectionner un chemin virtuel**]>**Règles**> Sélectionner une règle, par exemple ;(**VOIP**) .
2. Développez le volet **LAN vers WAN** . Sous la section **LAN to WAN**, cochez la case **Activer RED** pour l'activer pour les règles basées sur TCP.

The screenshot shows the 'Rules' configuration page in Citrix SD-WAN. At the top, 'Virtual Path to Site' is set to 'NSSDWANVPX_MCN-NSSDWAN1kBranch' and 'Section' is 'Rules'. Below this is a table of rules. The first rule, 'IPERF', is selected. The 'LAN to WAN' section is expanded, showing various configuration options. The 'Enable RED' checkbox is checked and highlighted with a red box.

Order	Rule Group Name	IP Address			Protocol	Protocol #	Port			DSC
		Source	Dest=Src	Dest			Source	Dest=Src	Dest	
100	IPERF	10.102.29.3/5	<input checked="" type="checkbox"/>	*	Any	0	*	<input checked="" type="checkbox"/>	*	Any

Initialize Properties Using Protocol

WAN General

LAN to WAN

General

Class: <Default>

Drop Limit (ms): 50

Drop Depth: 128000

Large Packet Size (bytes): 0

☒ Enable RED

Large Packets

Drop Limit (ms): 0

Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0

Disable Depth (bytes): 128000

Files d'attente MPLS

May 6, 2021

Cette fonctionnalité simplifie la création de configurations SD-WAN lors de l'ajout d'une liaison WAN MPLS (Multiprotocol Layer Switching). Auparavant, chaque file d'attente MPLS nécessitait la création d'une liaison WAN. Chaque liaison WAN nécessitait une adresse IP virtuelle (VIP) unique pour créer la liaison WAN et une balise DSCP (Differentiated Services Code Point) unique correspondant au schéma de mise en file d'attente du fournisseur. Après avoir défini une liaison WAN pour chaque file d'attente MPLS, le service Intranet à mapper à une file d'attente spécifique est défini.

Actuellement, une nouvelle définition de liaison WAN spécifique à MPLS (c'est-à-dire Type d'accès) est disponible. Lorsqu'un nouveau type d'accès MPLS privé est sélectionné, vous pouvez définir les files d'attente MPLS associées au lien WAN. Cela permet un seul VIP avec plusieurs balises DSCP qui

correspondent à l'implémentation de mise en file d'attente du fournisseur pour MPLS WAN Link. Cela mappe le service Intranet à plusieurs files d'attente MPLS sur un seul lien WAN MPLS.

Permet aux fournisseurs MPLS d'identifier le trafic en fonction des marques DSCP afin que la classe de service puisse être appliquée par le fournisseur.

Remarque

Si vous disposez de configurations MPLS existantes et que vous souhaitez implémenter le type d'accès MPLS privé, contactez le support technique Citrix pour obtenir de l'aide.

Configurer les liens WAN MPLS privés

1. Définissez le type d'accès à la liaison WAN en tant que MPLS privé.
2. Définissez les files d'attente MPLS correspondant aux files d'attente MPLS du fournisseur de services.
3. Activez la liaison WAN pour le service de chemin d'accès virtuel (activé par défaut pour les liaisons WAN MPLS privées).
4. À partir du chemin d'accès virtuel sur une liaison WAN, affectez un groupe Autopath.

Remarque

Si le groupe de chemin automatique est affecté à partir du niveau de liaison WAN, SD-WAN crée automatiquement des chemins entre les files d'attente MCN et MPLS client en fonction des balises DSCP correspondantes. Si le groupe de chemin automatique est affecté à partir du niveau de file d'attente MPLS, SD-WAN crée automatiquement des chemins, que les balises DSCP correspondent ou non.

5. Assurez-vous que le même groupe de chemin automatique est configuré au niveau du MCN et du client.
6. Vérifiez que les chemins d'accès pour la liaison WAN sont générés automatiquement.
7. Affectez le service Intranet à une file d'attente spécifique, si nécessaire.

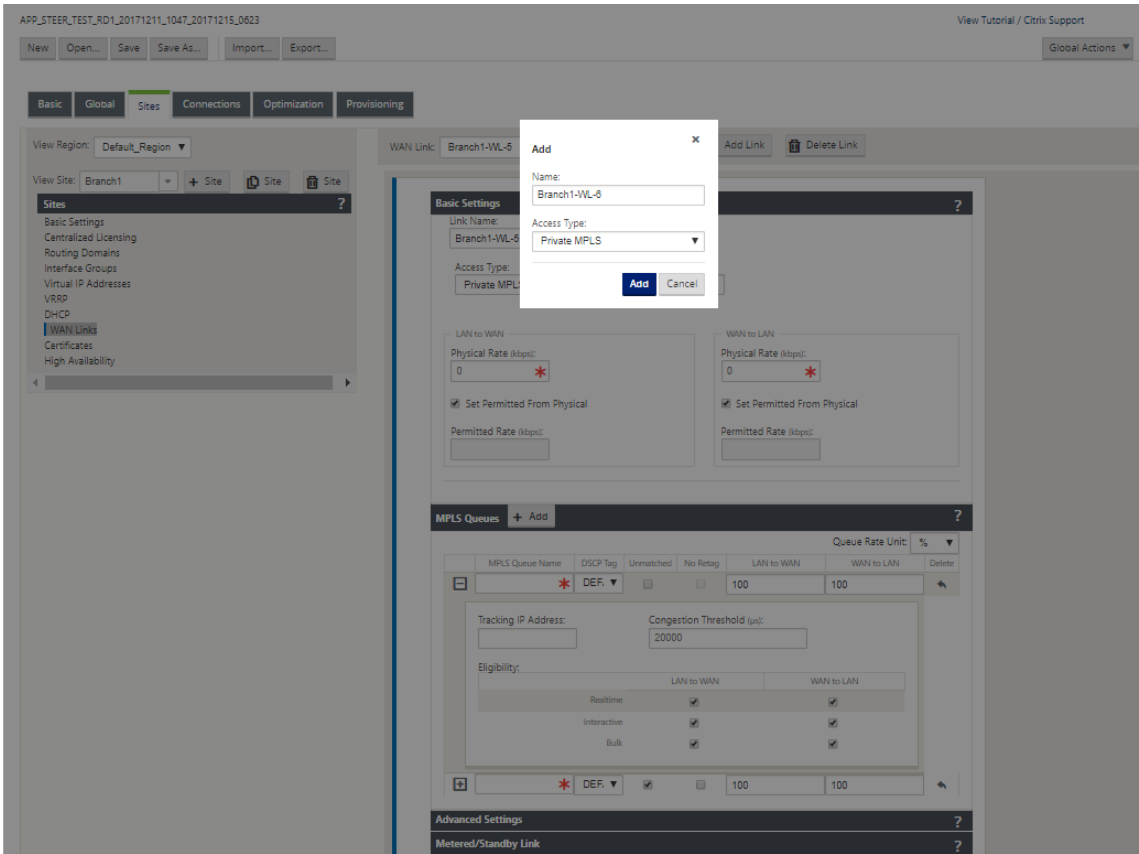
Remarque

La configuration SD-WAN peut ne pas avoir de mappage un-à-un pour les files d'attente basées sur le fournisseur. Ceci est basé sur des scénarios de déploiement spécifiques. Vous ne pouvez pas créer de groupes Autopath entre différents types d'accès privé. Par exemple, vous ne pouvez pas créer de groupes Autopath entre un type d'accès Internet privé et un type d'accès MPLS privé.

Comment ajouter un lien WAN MPLS privé

Pour configurer un nouveau type d'accès de liaison WAN pour MPLS privés :

1. Dans l'Éditeur de configuration, accédez à **Sites > [Nom du site] > Liens WAN**. Cliquez sur **Ajouter un lien**. Entrez le nom du lien WAN et sélectionnez **MPLS privé** comme type d'accès.



2. Sous les **paramètres de base**, il existe désormais un nouvel onglet **Files d'attente MPLS**. Cliquez sur + Ajouter pour ajouter des files d'attente MPLS spécifiques. Celles-ci doivent correspondre aux files d'attente définies par le fournisseur de services.

Champ	Description
Nom de la file d'attente MPLS	Nom de la file d'attente MPLS
Balise DSCP	Paramètre de balise DSCP du fournisseur de services pour la file d'attente.
Incomparable	Lorsque cette option est activée, toutes les trames arrivant qui ne correspondent pas aux balises définies dans le fichier de configuration sont mappées à cette file d'attente et la bande passante définie pour cette file d'attente.

Champ	Description
Taux autorisé LAN vers WAN (kbit/s)	Quantité de bande passante que les périphériques SD-WAN sont autorisés à utiliser pour le téléchargement, qui ne peut pas dépasser le taux de téléchargement physique défini de la liaison WAN.
Taux autorisé WAN à WAN (kbps)	Quantité de bande passante que les périphériques SD-WAN sont autorisés à utiliser pour le téléchargement, qui ne peut pas dépasser le taux de téléchargement physique défini de la liaison WAN.

Développez la définition de la file d'attente MPLS (en cliquant sur +) et d'autres options apparaissent. Ces options sont les suivantes :

Champ	Description
Suivi de l'adresse IP	Adresse de suivi WAN Link
Seuil de congestion	Durée définie pour la congestion (en microsecondes) après laquelle la file d'attente MPLS limite la transmission des paquets pour éviter plus de congestion. Lorsque la congestion dépasse le seuil défini, le SD-WAN désapprouve le taux d'envoi.
Éligibilité	L'éligibilité de la file d'attente MPLS pour traiter des classes de trafic spécifiques. Lorsque l'éligibilité est désactivée pour une classe de trafic spécifique, il est peu probable que cette classe de trafic passe par la file d'attente MPLS, sauf si les conditions réseau l'exigent.

Configurez les files d'attente MPLS qui correspondent aux définitions de file d'attente de liaison WAN Service Provider existantes.

Remarque

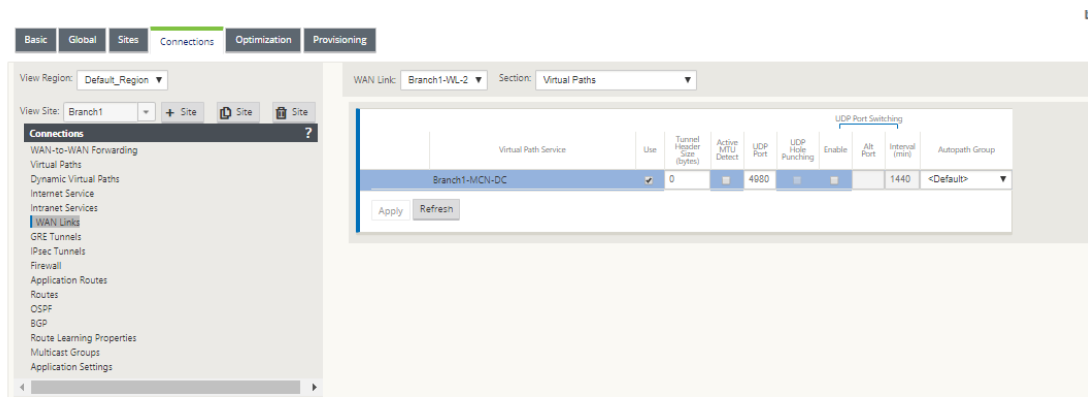
Les liaisons WAN MPLS existantes qui sont configurées avant SD-WAN 9.1 ne sont pas affectées.

Définition des propriétés de liaison WAN pour MPLS privé

Une fois que la liaison WAN MPLS privée avec ses files d'attente MPLS est définie, vous devez affecter un groupe de ath automatique pour la liaison WAN sous une définition de chemin virtuel spécifique.

Pour affecter un groupe de ath automatique :

1. [Allez dans **Connexions** > Site Name[] > **Liens WAN** > Nomdu lien WANMPLS[] > **Chemins virtuels** > Nomdu cheminvirtuel[] > **Sitelocal** > **Liens WAN** et cliquez sur **Modifier()**.]
2. Cliquez sur le menu déroulant **Groupe de ath automatique** et choisissez parmi les groupes disponibles. Par défaut, les files d'attente MPLS héritent du groupe de chemin automatique affecté à la liaison WAN MPLS. Vous pouvez choisir de définir les files d'attente MPLS individuelles pour Hériter le groupe de chemin automatique choisi ou choisir un substitut dans le menu déroulant Groupe de chemin automatique pour chaque file d'attente MPLS.



Remarque

S'il n'y a pas de mappage individuel, basé sur la balise DSCP, entre les files d'attente du site local et du site distant, vous devez mapper les files d'attente MPLS à des groupes de chemin automatique spécifiques. Hériter un groupe de chemins automatiques à partir de la liaison WAN MPLS génère automatiquement des chemins entre les files d'attente avec des balises DSCP correspondantes.

Attribuer un groupe de ath automatique au lien Path-WAN virtuel

Le groupe Autopath défini est le même pour l'apppliance MCN et Client. Cela permet au système de construire automatiquement les chemins. Sur le site MCN, vous pouvez également développer la liaison WAN associée au chemin virtuel.

Afficher le taux et la congestion autorisés pour les liaisons WAN

L’interface Web SD-WAN vous permet désormais d’afficher le taux autorisé pour les utilisations des liaisons WAN et WAN et de savoir si un lien WAN, un chemin ou un chemin virtuel est encombré. Dans les versions précédentes, ces informations n’étaient disponibles que dans les fichiers journaux SD-WAN et via l’interface de ligne de commande. Ces options sont désormais disponibles dans l’interface Web pour faciliter le débogage.

Voir le tarif autorisé

Le taux autorisé correspond à la quantité de bande passante qu’une liaison WAN, un service de chemin virtuel, un service intranet ou un service Internet particulier est autorisée à utiliser à un moment donné. Le taux autorisé pour une liaison WAN est statique et est défini explicitement dans la configuration SD-WAN. Le tarif autorisé pour un service de chemin virtuel, un service intranet ou un service Internet fluctuera au fil du temps, en réponse à la congestion, à la demande des utilisateurs et au partage équitable, mais sera toujours supérieur ou égal à la bande passante minimale réservée pour le service.

Surveiller la liaison WAN

Accédez à **Moniteur Statistiques**, puis sélectionnez **Connexion WAN** dans la liste déroulante **Afficher**

Monitoring > Statistics

Statistics

Show: WAN Link ☒ Enable Auto Refresh 5 seconds ☒ Show latest data. Processing...

WAN Link Statistics

Filter: in Any column

Show 100 entries Showing 1 to 6 of 6 entries

First Previous 1 Next Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
Client-1-WL-1	N/A	172.186.10.75	N/A	N/A	N/A	N/A
Client-1-WL-2	N/A	172.186.20.75	N/A	N/A	N/A	N/A
Client-2-WL-1	N/A	172.186.70.50	N/A	N/A	N/A	N/A
Client-2-WL-2	N/A	172.186.80.50	N/A	N/A	N/A	N/A
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	DISABLED	N/A	N/A
DC-WL-2	DC-WL-2-AI-1	172.186.40.85	N/A	DISABLED	N/A	N/A

Showing 1 to 6 of 6 entries

First Previous 1 Next Last

Virtual Path Service Data Rates

Filter: in Any column

Show 100 entries Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved
DC-WL-1	Recv	2618687	195069.42	289	26.16	37.81	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

623

Accédez à **Moniteur > Statistiques**, puis sélectionnez **Utilisation du lien WAN** dans la liste déroulante **Afficher**.

Statistics

Show

WAN Link Usage

Enable Auto Refresh

5

seconds

Stop

Show latest data

Processing...

WAN Link Usage Statistics

Local WAN Links

Filter

on

Any column

Apply

Show

100

entries

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

WAN Link	Direction	Packets	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
DC-WG-1	Send	2551632	238	17.69	28.34	100000	N/A
DC-WG-1	Recv	2630429	240	21.97	35.59	99000	NO
q1	Send	2359231	312	20.94	35.77	50000	N/A
q1	Recv	2366461	308	18.36	29.74	49000	NO
q2	Send	119194	306	16.52	26.77	50000	N/A
q2	Recv	128796	321	19.66	32.21	49000	NO

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

Usage and Permitted Rates

Filter

on

Any column

Apply

Show

100

entries

Showing 1 to 14 of 14 entries

First

Previous

1

Next

Last

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
DC-WG-1	DC-Client-1	Recv	1673996	124885.42	118	10.8	16.99	24425.95	NO
DC-WG-1	DC-Client-2	Recv	956409	71427.76	138	12.12	19.07	24490	NO
DC-WG-1	DC-Client-1	Send	1623616	108311624	134	10.34	16.27	24990	N/A
DC-WG-1	DC-Client-2	Send	930096	64771056	132	9.47	14.9	24990	N/A
DC-WG-1	Internet-Intranet	Send	0	0	0	0	0	50000	N/A
DC-WG-1	Internet-Intranet	Recv	208	55.25	0	0	0	49000	N/A
q1	DC-Client-1	Recv	1317987	96716.01	208	11.12	17.31	24510	NO
q1	DC-Client-2	Recv	821873	52985.37	106	7.4	11.64	24990	NO
q1	DC-Client-1	Send	1314290	97350160	210	10.31	21.26	25010	N/A
q1	DC-Client-2	Send	847903	57291604	109	7.53	11.89	24990	N/A
q2	DC-Client-1	Recv	91058	6260.85	237	15.85	24.94	24510	NO
q2	DC-Client-2	Recv	40378	2232.83	104	5.56	8.75	24990	NO
q2	DC-Client-1	Send	81296	4710764	208	11.12	17.31	25010	N/A
q2	DC-Client-2	Send	40353	2271700	105	5.61	8.83	24990	N/A

Showing 1 to 14 of 14 entries

First

Previous

1

Next

Last

Remote WAN Links

Filter

on

Any column

Apply

Show

100

entries

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

WAN Link	Service	Direction	Congestion
Client-1-WG-1	DC-Client-1	Recv	NO
Client-2-WG-1	DC-Client-2	Recv	NO
q3	DC-Client-1	Recv	NO
q4	DC-Client-1	Recv	NO
q5	DC-Client-2	Recv	NO
q6	DC-Client-2	Recv	NO

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 624

Surveillance des files d’attente MPLS

Accédez à **Moniteur Statistiques**, puis sélectionnez Files d’attente **MPLS** dans la liste déroulante **Afficher**.

Show: **MPLS Queues**
☒ Enable Auto Refresh
5 seconds
Stop
☒ Show latest data.

MPLS Queue Statistics

Filter:
in Any column
Apply

Show 100 entries
Showing 1 to 4 of 4 entries
Processing...

First Previous 1 Next Last

Private MPLS	MPLS Queue	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
EE-Branch1-WL-2	SAMPLE-Queue1	EE-Branch1-WL-2-AI-1	172.184.19.19	N/A	DISABLED	N/A	N/A
EE-Branch1-WL-2	SAMPLE-Queue2	EE-Branch1-WL-2-AI-1	172.184.19.19	N/A	DISABLED	N/A	N/A
VPX-DC-WL-2	DC-Queue1	N/A	172.184.3.19	172.184.3.19	N/A	N/A	N/A
VPX-DC-WL-2	DC-Queue2	N/A	172.184.3.19	172.184.3.19	N/A	N/A	N/A

Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Virtual Path Service Data Rates

Filter:
in Any column
Apply

Show 100 entries
Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	Mismatched DSCP Packets	Mismatched DSCP kB	IP/TCP/UDP Header Compression Bytes Saved
SAMPLE-Queue1	Recv	14279	1177.77	251	20.72	33.15	5932	407.36	0
SAMPLE-Queue1	Send	13400	919.09	217	14.47	23.15	N/A	N/A	0
SAMPLE-Queue2	Recv	12806	705.61	216	11.84	18.95	5803	250.8	0
SAMPLE-Queue2	Send	13953	915.39	241	16.73	26.77	N/A	N/A	0

Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Dépannage des files d’attente MPLS

Pour vérifier l’état des files d’attente MPLS, accédez à **Moniteur > Statistiques** et sélectionnez **Chemins (résumé)** dans la liste déroulante **Afficher**. Dans l’exemple suivant, le chemin de la file d’attente MPLS « q1 » à « q3 » est en état DEAD et affiché en rouge. Le chemin de la file d’attente MPLS « q1 » à « q5 » est en bon état et affiché en vert.

Statistics

Show: Paths (Summary)

☒ Enable Auto Refresh

5 seconds

Stop

☒ Show latest data. Processing...

Path Statistics Summary

Filter:

in Any column

Apply

Show 100 entries

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
5	q2	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
6	Client-1-WL-1	DC-WL-1	GOOD	GOOD	Static	4	2	0.00	19.96	NO
7	q3	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
8	q3	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
9	q4	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
10	q4	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
11	DC-WL-1	Client-2-WL-1	GOOD	GOOD	Static	2	2	0.00	15.12	NO
12	q1	q5	GOOD	GOOD	Static	2	2	0.00	11.53	NO
13	q2	q6	GOOD	GOOD	Static	2	2	0.00	8.51	NO
14	Client-2-WL-1	DC-WL-1	GOOD	GOOD	Static	2	2	0.00	20.09	NO
15	q5	q1	GOOD	GOOD	Static	2	2	0.00	11.69	NO
16	q6	q2	GOOD	GOOD	Static	2	2	0.00	8.82	NO

Pour obtenir des informations détaillées sur les chemins, sélectionnez **Chemins (Détailés)** dans la liste déroulante **Afficher**. Les informations sur les chemins d'accès tels que la raison de l'état, la durée, le port source, le port de destination, le MTU sont disponibles

Dans l'exemple suivant, le chemin de la file d'attente MPLS « q1 » à « q3 » est en état DEAD et la raison est PEER. Le chemin de la file d'attente MPLS « q3 » à « q1 » est mort et la raison est SILENCE. Le tableau suivant fournit la liste des raisons disponibles et ses descriptions.

Raison	Description
PASSERELLE	Le chemin d'accès est DEAD car l'appliance ne peut pas atteindre ou détecter la passerelle
SILENCE	Le chemin d'accès est BAD ou DEAD car l'appliance n'a pas reçu de paquets provenant du site homologue
PERTE	Le chemin est BAD en raison de la perte de paquets
PAIR	Le site homologue signale que le chemin est BAD

Show:

Paths (Detailed)

☒ Enable Auto Refresh

5 seconds

Stop

☒ Show latest data

Processing...

Path Statistics Advanced

Filter: in

Any column

Apply

Show

100

 entries Showing 1 to 16 of 16 entries

FirstPrevious1NextLast

Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	108	0	0.00	12.75	Static
3	q1	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
4	q2	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
5	q2	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
6	Client-1-WL-1	DC-WL-1	NO	GOOD	N/A	21325	GOOD	4980	4980	N/A	4	2	126	0	0.00	17.45	Static
7	q3	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
8	q3	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
9	q4	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
10	q4	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
11	DC-WL-1	Client-2-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	130	0	0.00	14.41	Static
12	q1	q5	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	111	0	0.00	11.69	Static
13	q2	q6	NO	GOOD	N/A	234	GOOD	4980	4980	1488	2	2	107	0	0.00	8.72	Static
14	Client-2-WL-1	DC-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	142	0	0.00	19.40	Static
15	q5	q1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	110	0	0.00	11.27	Static
16	q6	q2	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	107	0	0.00	8.50	Static

Pour vérifier l’interface d’accès et l’adresse IP associées aux files d’attente MPLS, sélectionnez **Interfaces d’accès** dans la liste déroulante **Afficher**.

Show:

Access Interfaces

☒ Enable Auto Refresh

5 seconds

Stop

☒ Show latest data

Processing...

Access Interface Statistics

Filter: in

Any column

Apply

Show

100

 entries Showing 1 to 3 of 3 entries

FirstPrevious1NextLast

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	N/A	N/A	N/A
q1	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A
q2	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A

Showing 1 to 3 of 3 entries

FirstPrevious1NextLast

Virtual Path Service Data Rates

Filter: in

Any column

Apply

Show

100

 entries Showing 1 to 12 of 12 entries

FirstPrevious1NextLast

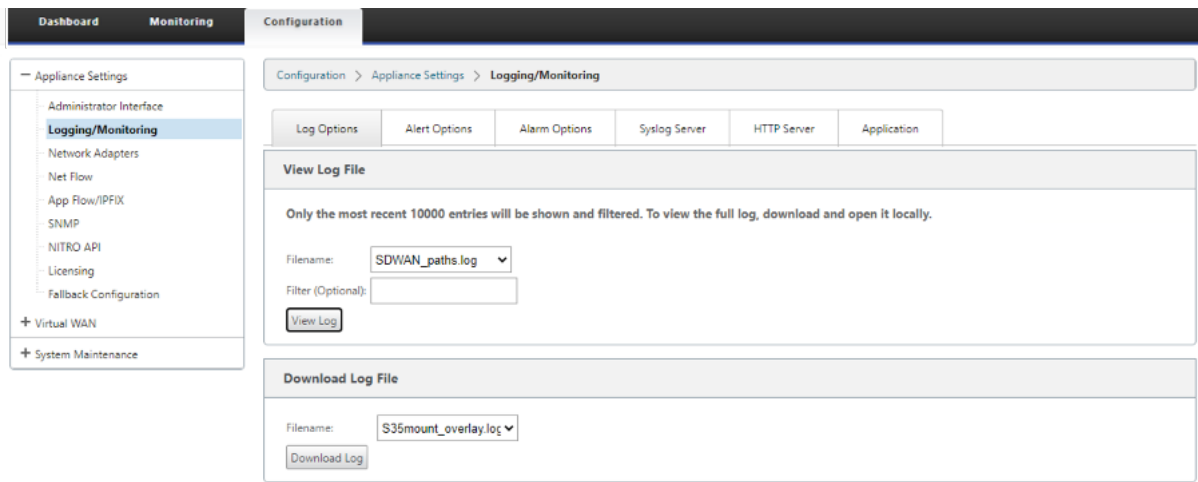
WAN Link	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP/TCP/UDP Header Compression Bytes Saved
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Recv	953815	71018.84	147	13.04	21.11	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Recv	1670099	124524.23	112	10.56	17.1	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Send	925756	62940.27	137	10.22	16.55	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Send	1619424	105451.88	141	11.16	18.07	0
q1	DC-WL-2-AI-1	DC-Client-1	Recv	1530107	96340.46	202	10.82	17.52	0
q1	DC-WL-2-AI-1	DC-Client-2	Recv	828314	52130.2	103	7.21	11.68	0
q1	DC-WL-2-AI-1	DC-Client-1	Send	1507265	94613.25	205	13.25	21.46	0
q1	DC-WL-2-AI-1	DC-Client-2	Send	843865	55794.07	104	7.3	11.61	0

Vous pouvez télécharger les fichiers journaux pour un dépannage ultérieur. Accédez à **Configura-**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

627

tion > **Logging/Monitoring** et sélectionnez **SDWAN_paths.log** ou **SDWAN_common.log** dans l'onglet **Options du journal**.



Rapports

May 6, 2021

[QoE des applications](#)

[Collecteurs de flux net multiples](#)

QoE des applications

May 6, 2021

La **QoE des applications** est une mesure de la qualité de l'expérience des applications dans le réseau SD-WAN. Il mesure la qualité des applications qui circulent à travers les chemins virtuels entre deux appliances SD-WAN. Le score **QoE de l'application** est une valeur comprise entre 0 et 10. La plage de score dans laquelle elle tombe détermine la qualité d'une application.

Qualité	Plage
Bon	8–10
Acceptable	4–8
Médiocre	0–4

Qualité

Plage

Le score **QoE des applications** peut être utilisé pour mesurer la qualité des applications et identifier les tendances problématiques.

Vous pouvez définir les seuils de qualité pour les appliances interactives et en temps réel à l'aide de profils QoE, puis mapper ces profils aux applications ou aux objets applications.

Note :

Pour surveiller la QoE des applications, il est essentiel d'activer l'inspection approfondie des paquets. Pour de plus amples informations, consultez [Classification des applications](#)

QoE des applications en temps réel

Le calcul de la QoE des applications en temps réel utilise une technique innovante Citrix, qui est dérivée du score MOS.

Les valeurs de seuil par défaut sont les suivantes :

- Seuil de latence : 160 ms
- Seuil de gigue : 30 ms
- Seuil de perte de paquets : 2%

Un flux d'une application en temps réel qui respecte les seuils de latence, de perte et de gigue est considéré comme de bonne qualité.

La QoE pour les applications en temps réel est déterminée à partir du pourcentage de flux qui atteignent le seuil divisé par le nombre total d'échantillons de flux.

QoE pour temps réel = (Nombre d'échantillons de débit qui atteignent le seuil / Nombre total d'échantillons de débit) * 100

Il est représenté par un score QoE allant de 0 à 10.

Vous pouvez créer des profils QoE avec des valeurs de seuil personnalisées et les appliquer aux applications ou aux objets d'application.

Note :

La valeur QoE peut être nulle si les conditions réseau sont en dehors des seuils configurés pour le trafic en temps réel.

Application interactive QoE

La QoE des applications interactives utilise une technique innovante Citrix basée sur les seuils de perte de paquets et de taux d'éclatement.

Les applications interactives sont sensibles à la perte et au débit de paquets. Par conséquent, nous mesurons le pourcentage de perte de paquets et le taux d'éclatement du trafic d'entrée et de sortie dans un flux.

Les seuils configurables sont les suivants :

- Pourcentage de perte de paquets.
- Pourcentage du taux d'éclatement prévu de sortie par rapport au taux d'éclatement d'entrée.

Les valeurs de seuil par défaut sont les suivantes :

- Seuil de perte de paquets : 1%
- Taux de rafale : 60%

Un débit est de bonne qualité si les conditions suivantes sont remplies :

- Le pourcentage de perte pour un flux est inférieur au seuil configuré.
- Le taux d'éclatement de sortie est au moins le pourcentage configuré du taux d'éclatement d'entrée.

Configuration de la QoE de l'application

Mappez des objets d'application ou d'application à des profils QoE par défaut ou personnalisés. Vous pouvez créer des profils QoE personnalisés pour le trafic interactif et en temps réel.

Pour créer des profils QoE personnalisés :

1. Dans l'Éditeur de configuration, accédez à **Global > Application QoE > QoE Profils** et cliquez sur **+**.
2. Entrez la valeur des paramètres suivants :
 - **Nom du profil** : nom permettant d'identifier le profil qui définit des seuils pour le trafic interactif et en temps réel.
 - **Temps réel** : Configurez des seuils pour les flux de trafic qui atteignent la stratégie QoS en temps réel. Un flux d'une application en temps réel qui atteint des seuils de latence, de perte et de gigue est considéré comme de bonne qualité.
 - **Latence à sens unique** : seuil de latence en millisecondes. La valeur de profil QoE par défaut est 160 ms.

- **Jitter** : Seuil de gigue en millisecondes. La valeur de profil QoE par défaut est 30 ms.
- **Perte de paquets** : pourcentage de perte de paquets. La valeur de profil QoE par défaut est de 2 %.
- **Interactif** : configurez des seuils pour les flux de trafic qui atteignent la stratégie QoS interactive. Un flux d'une application interactive qui atteint un seuil inférieur pour le rapport d'éclatement et la perte de paquets est considéré comme de bonne qualité.
 - **Taux d'éclatement prévu** : Pourcentage du taux d'éclatement prévu. Le taux d'éclatement de sortie doit être au moins le pourcentage configuré du taux d'éclatement d'entrée. La valeur de profil QoE par défaut est 60 %.
 - **Perte de paquets par flux** : pourcentage de perte de paquets. La valeur de profil QoE par défaut est 1 %.

Section: QoE Profiles

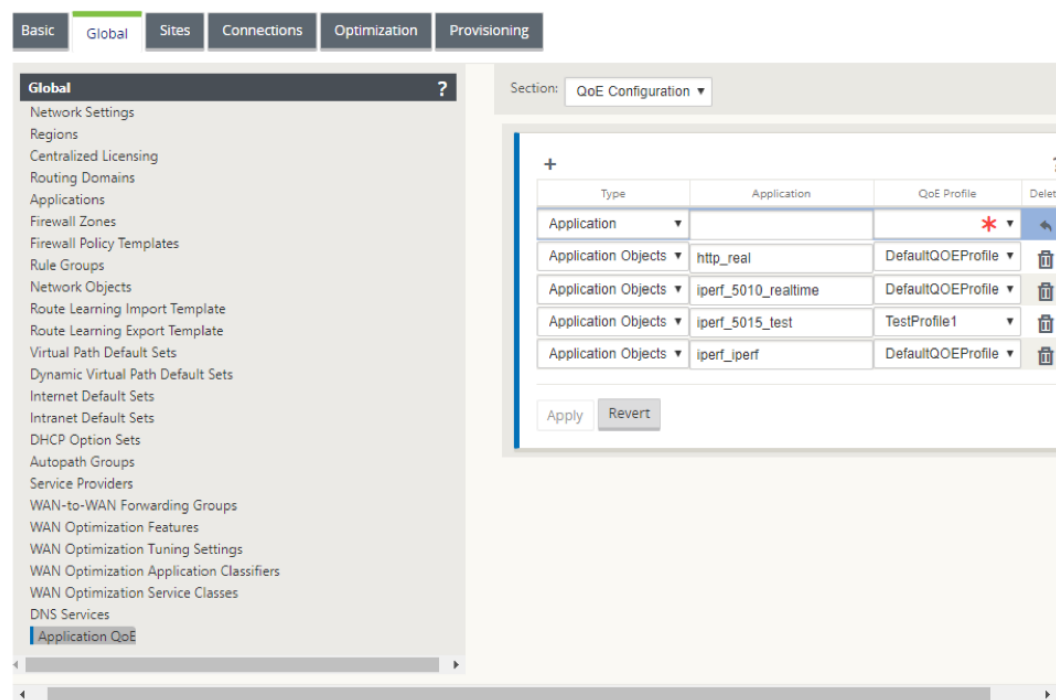
Profile Name	Realtime			Interactive		Delete
	One Way Latency (ms)	Jitter (ms)	Packet Loss (%)	Expected Burst Rate (%)	Packet loss per flow (%)	
TestProfile2	190	30	3.0	60.0	1.0	
DefaultQOEProfile	160	30	2.0	60.0	1.0	
TestProfile1	170	30	2.0	60.0	2.0	

Apply **Revert**

3. Cliquez sur **Appliquer**.

Pour mapper des applications ou des objets d'application avec des profils QoE :

1. Dans l'Éditeur de configuration, accédez à **Global > Application QoE > QoE Configuration** et cliquez sur **+**.
2. Sélectionnez des valeurs pour les paramètres suivants :
 - **Type** : Application PPP ou objet application.
 - **Application** : Recherchez et sélectionnez une application ou un objet d'application en fonction du Type sélectionné.
 - **ProfilQoE** : **sélectionnez un profilQoE** à mapper à l'objet d'application ou d'application.



3. Cliquez sur **Appliquer**.

Vous pouvez mapper jusqu'à 10 applications ou objets d'application avec des profils QoE. Vous pouvez afficher les rapports QoE des applications sur SD-WAN Center. Pour plus d'informations, consultez le [Rapport QOE des applications](#) rapport.

QoE HDX

May 6, 2021

Les paramètres réseau tels que la latence, la gigue et la suppression de paquets affectent l'expérience utilisateur des utilisateurs HDX. Quality of Experience (QoE) est introduit pour aider les utilisateurs à comprendre et à vérifier leur qualité d'expérience ICA. QoE est un indice calculé qui indique les performances du trafic ICA. Les utilisateurs peuvent régler les règles et la politique pour améliorer la QoE.

La QoE est une valeur numérique comprise entre 0 et 100, plus la valeur est élevée, meilleure est l'expérience utilisateur. QoE est activé par défaut pour toutes les applications ICA /HDX.

Les paramètres utilisés pour calculer la QoE sont mesurés entre les deux appliances SD-WAN situées du côté client et serveur et ne sont pas mesurés entre le client ou les appliances serveur elles-mêmes. La latence, la gigue et la chute de paquets sont mesurées au niveau du flux et elles peuvent être différentes des statistiques au niveau du lien. L'application hôte final (client ou serveur) peut ne jamais

savoir qu'il y a une perte de paquets sur le WAN. Si la retransmission réussit, le taux de perte de paquets au niveau du flux est inférieur à la perte de niveau de liaison. Cependant, par conséquent, cela peut augmenter un peu la latence et la gigue.

La configuration par défaut du trafic HDX permet au SD-WAN de retransmettre des paquets, améliorant ainsi la valeur d'index QoE perdue en raison de la perte de paquets dans le réseau.

Dans le tableau de bord HDX sur Citrix SD-WAN Orchestrator, vous pouvez afficher une représentation graphique de la qualité globale des applications HDX. Les applications HDX sont classées dans les trois catégories de qualité suivantes :

Qualité	Gamme QoE
Bon	80–100
Acceptable	50–80
Médiocre	0–50

Une liste des cinq sites les plus bas ayant le moins de QoE est également affichée dans le tableau de bord HDX.

Une représentation graphique de la QoE pour différents intervalles de temps vous permet de surveiller les performances des applications HDX sur chaque site.

Pour de plus amples informations, consultez [Tableau de bord et rapports HDX](#).

Remarque

- Ne vous attendez pas à ce que la latence des liens WAN, la gigue et la suppression des paquets correspondraient toujours à la latence de l'application, à la gigue et à la suppression des paquets. La perte de liaison WAN est corrélée à la perte réelle de paquets WAN, tandis que la perte d'application est après retransmission, ce qui est inférieur à la perte de liaison WAN.
- La latence WAN Link affichée dans l'interface graphique est BOWT (Best One Way Time). Il s'agit de la meilleure mesure du lien comme moyen de mesurer la santé du lien. L'application QoE suit et calcule la latence totale et moyenne de tous les paquets de cette application. Cela ne correspond souvent pas au lien BOWT.
- Lorsqu'une session MSI démarre, pendant l'établissement d'une liaison ICA, la session peut être temporairement comptée comme 4 MSI au lieu de 1 MSI. Une fois la poignée de main terminée, elle convergera en 1 MSI. Si la conversion se produit avant la mise à jour de la table SQL, elle peut apparaître dans ICA_summary pour cette minute.
- Lors de la reconnexion de session, puisque les informations de protocole initiales ne sont pas échangées, SD-WAN n'est pas en mesure d'identifier MSI, de sorte que chaque connexion est comptée comme informations MSI.

- Pour les connexions UDP, une fois la connexion fermée, il peut prendre jusqu'à 5 minutes pour que la connexion s'affiche comme fermée et mise à jour dans ICA_summary. Pour les connexions TCP, une fois la connexion fermée, l'affichage comme étant fermé dans ICA_summary peut prendre jusqu'à 2 minutes.
- La QoE des sessions TCP et UDP peut ne pas être la même sur le même chemin en raison de la différence inhérente entre TCP et UDP.
- Si un utilisateur lance deux postes de travail virtuels, le nombre d'utilisateurs est compté comme deux.

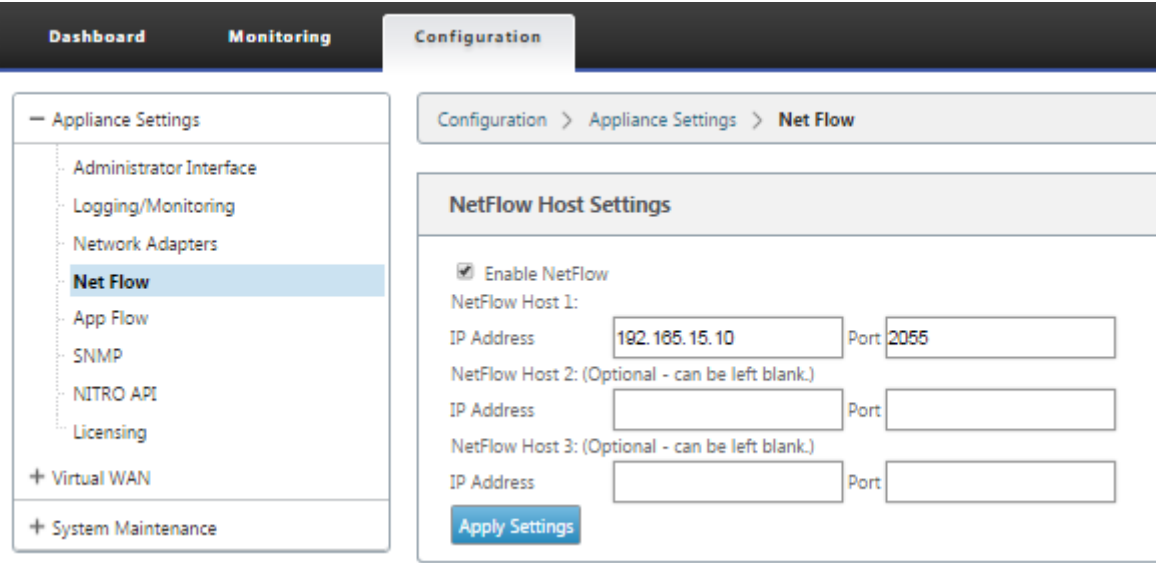
Collecteurs de flux net multiples

February 8, 2022

Net Flow collectors collectent le trafic réseau IP lorsqu'il entre ou quitte une interface SD-WAN. En analysant les données fournies par Net Flow, vous pouvez déterminer la source et la destination du trafic, la classe de service et les causes de la congestion du trafic. Les périphériques Citrix SD-WAN peuvent être configurés pour envoyer des données statistiques de base Net Flow version 5 au collecteur Net Flow configuré. Citrix SD-WAN prend en charge Net Flow pour les flux de trafic qui sont masqués par le protocole fiable de transport. Les périphériques situés à la périphérie WAN de la solution perdent la capacité de collecter des enregistrements Net Flow puisque seuls les paquets UDP encapsulés SD-WAN sont affichés. Net Flow est pris en charge sur les appliances Citrix SD-WAN Standard et Premium (Enterprise) Edition.

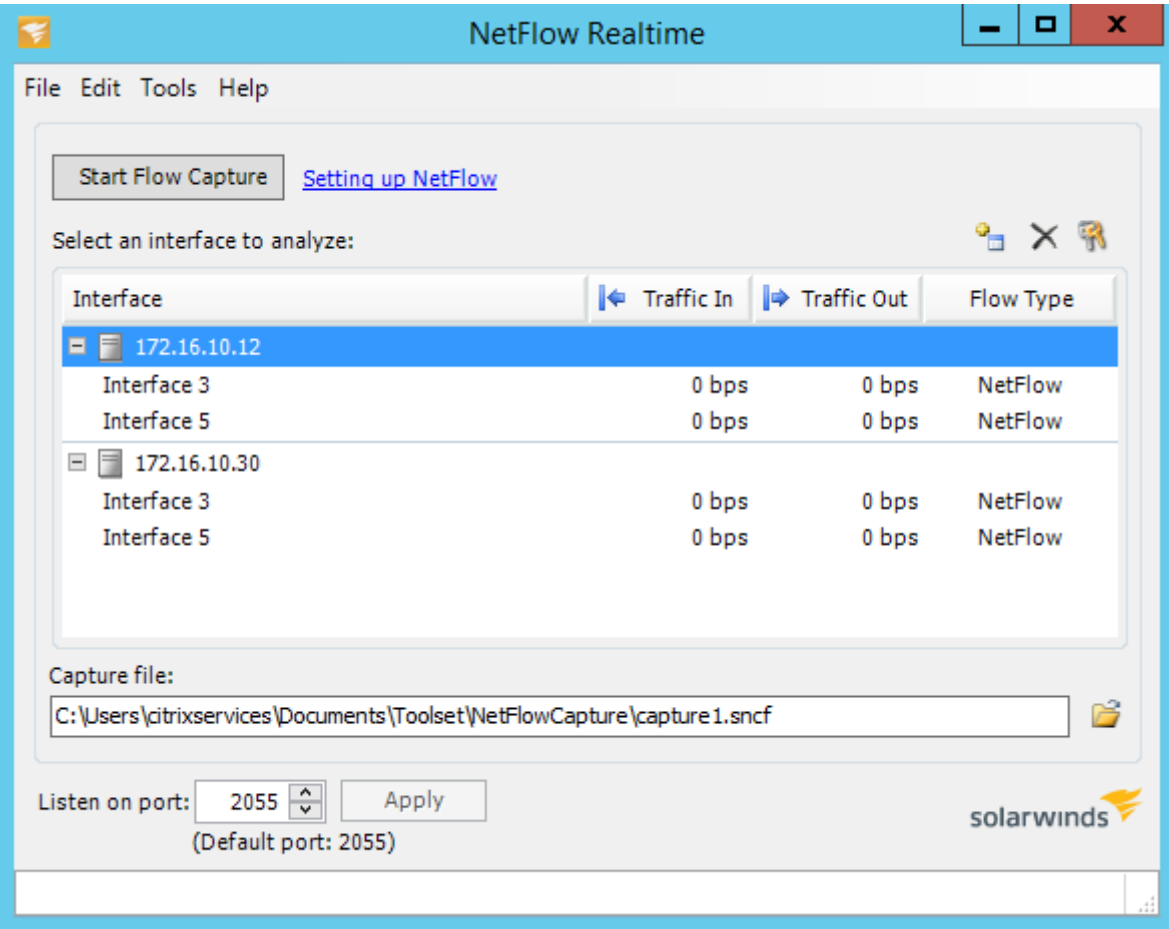
Pour configurer les hôtes Net Flow :

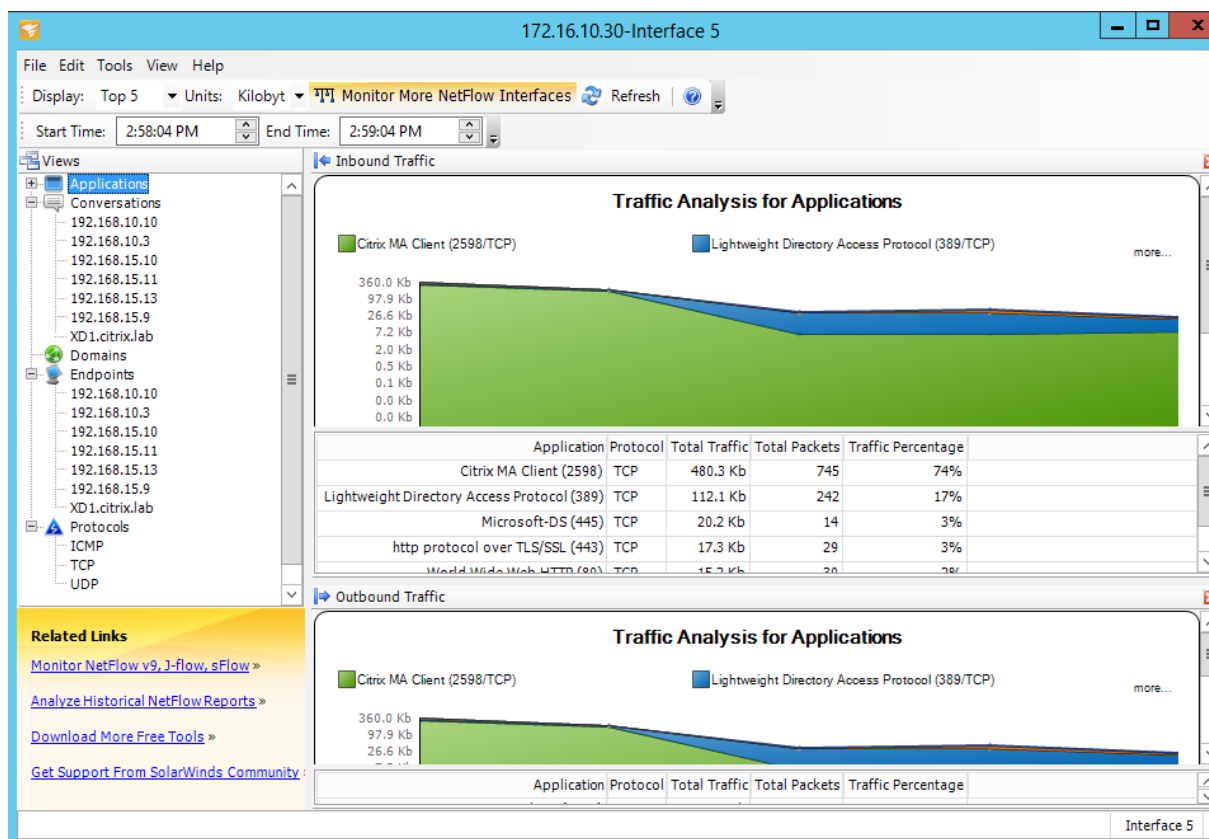
Accédez à **la page Configuration > Paramètres du matériel > Net Flow Paramètres de l'hôte Net-flow** . Cochez la **case Activer NetFlow**, puis saisissez l'**adresse IP** et les numéros de **port** pour un maximum de trois hôtes de flux réseau, puis cliquez sur **Appliquer les paramètres pour** enregistrer les modifications.



Exportation NetFlow

Les données Net Flow sont exportées à partir du port de gestion des périphériques SD-WAN. Sur votre outil de collecteur Net Flow, les périphériques SD-WAN sont répertoriés comme adresse IP de gestion configurée, si SNMP n’est pas configuré. Les interfaces sont répertoriées comme une pour les entrées et une seconde pour les sorties (trafic Virtual Path). Pour plus d’informations, consultez [SNMP](#)





Limitations de NetFlow

- Lorsque Netflow est activé sur les appliances SD-WAN Standard et Premium Edition, les données Virtual Path sont diffusées vers les collecteurs Netflow désignés. Une limitation est que l'on ne peut pas différencier le lien WAN physique utilisé par SD-WAN, car la solution rapporte des informations agrégées de chemin virtuel (un chemin virtuel peut comprendre plusieurs chemins WAN distincts), il n'y a aucun moyen de filtrer les enregistrements Netflow pour les chemins WAN distincts.
- Les bits de contrôle TCP indiquent N/A, ce qui indique que le SD-WAN ne respecte pas la norme Internet pour les exportations Netflow basées sur la [RFC 7011](#) qui a l'ID d'élément 6 pour TCP-ControlBits ([IANA](#)). Sans indicateurs TCP, il n'est pas possible de calculer le temps aller-retour (RTT), la latence, la gigue et d'autres mesures de performance dans les données de flux. Du côté de la sécurité, sans drapeaux TCP, le collecteur Net Flow ne peut pas déterminer s'il y a des analyses FIN, ACK/RST ou SYN.

Statistiques d’itinéraire

May 6, 2021

Pour afficher les statistiques d’itinéraire de vos appliances SD-WAN, dans l’interface utilisateur graphique SD-WAN, accédez à **Surveillance > Statistiques > Itinéraires** .

DashboardMonitoringConfiguration

Statistics

FlowsRouting ProtocolsFirewallIKE/IPsecIGMPPerformance ReportsQos ReportsUsage ReportsAvailability ReportsAppliance ReportsDHCP Server/RelayVRRPPPPoEDNS

Monitoring > Statistics

Statistics

Show Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain: Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 10 of 10 entries

Details#	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
	0	172.186.30.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	55365	YES	N/A	N/A
	1	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
	2	172.186.50.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11	YES	N/A	N/A
	3	172.186.10.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	27912	YES	N/A	N/A
Site Path: Client-1 Optimal Route: NO Summarized / Summary Route: NO/NO																
	4	172.186.20.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
	5	172.186.10.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
	6	172.186.20.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
	7	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	DC	Static	-	-	5	20	YES	N/A	N/A
	8	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	238	YES	N/A	N/A
	9	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

Showing 1 to 10 of 10 entries

Vous pouvez afficher les paramètres suivants :

- **Adresse réseau** : Adresseréseau et masque de sous-réseau de l’itinéraire.
 - **Détails** : Cliquez sur + pour afficher les informations suivantes.
 - **Chemin d’origine** : Chemin du site est une source de mesure de vérité pour le préfixe reçu. Il est utilisé dans les situations où le transfert WAN vers WAN est activé sur plusieurs périphériques et dans le déploiement maillé. Plusieurs préfixes de ce type sont reçus et les administrateurs sont en mesure de juger les attributs du préfixe en affichant le chemin d’accès du site.
- Par exemple, considérez une topologie simple de Branch1, Branch2 et MCN avec un Geo MCN. Branch1 a un préfixe 172.16.1.0/24 et doit arriver à Branch2. Geo MCN et MCN ont le transfert WAN vers WAN activé.
- Le préfixe 172.16.1.0/24 peut accéder à Branch2 via Branch1-MCN-Branch2, Branch1-Geo-Branch2 et Branch1-MCN-Geo-Branch2. Pour chacun de ces préfixes distincts, la table de routage est mise à jour avec sa métrique de chemin de site. La métrique de chemin de site indique l’origine du préfixe d’itinéraire et le coût d’accès à Branch2.

- **Route optimale** : itinéraire optimal indique si l'itinéraire est l'itinéraire optimal pour atteindre ce sous-réseau par rapport à tous les autres itinéraires. Cet itinéraire optimal est exporté vers d'autres sites.
- **Route récapitulée/récapitulative** : Une route récapitulative est une route configurée explicitement par un administrateur pour résumer plusieurs préfixes qui se trouvent dans le superréseau. Les itinéraires synthétisés sont les préfixes qui se trouvent sous l'itinéraire récapitulatif.

Par exemple, supposons que nous avons une route récapitulative 172.16.0.0/16. Il s'agit d'un itinéraire récapitulatif uniquement et non d'un itinéraire récapitulatif. Un itinéraire récapitulatif a le résumé « YES » et le résumé « NO ». S'il y a peu d'autres sous-réseaux comme 172.16.1.0/24, 172.16.2.0/24 et 172.16.3.0/24, ces trois routes tombent sous la route sommaire ou le supernet et sont donc appelées routes synthétisées. Un itinéraire récapitulatif a résumé « YES » et le résumé « NO ».

- **Adresse IP de la Gateway** : adresse IP de la passerelle/route utilisée pour atteindre cet itinéraire.
- **Service** : Type de service Citrix SD-WAN.
- **Zone de pare-feu** : Zone de pare-feu utilisée par l'itinéraire.
- **Accessible** : L'itinéraire est-il accessible ou non.
- **Adresse IP du site** : Adresse IP du site.
- **Site** : nom du site.
- **Type** : Le type d'itinéraire dépend de la source de l'apprentissage de l'itinéraire. Les itinéraires du côté LAN et les itinéraires entrés manuellement lors de la configuration sont des itinéraires statiques. Les itinéraires tirés du SD-WAN ou des homologues de routage dynamique sont des itinéraires dynamiques.
- **Protocole** : Protocole des préfixes.
 - **Local** : adresses IP virtuelles locales de l'appliance.
 - **Réseau étendu virtuel** : préfixes tirés des appliances SD-WAN homologues.
 - **OSPF** : préfixes tirés de l'homologue de routage dynamique OSPF.
 - **BGP** : préfixes tirés de l'homologue de routage dynamique BGP.
- **Voisinage direct** : indique si le sous-réseau est connecté à la branche à partir de laquelle l'itinéraire est arrivé à l'appliance.
- **Coût** : coût utilisé pour déterminer le meilleur chemin d'accès à un réseau de destination.
- **Nombre d'accès** : nombre de fois qu'un itinéraire a été touché pour transférer un paquet vers ce sous-réseau.

- **Éligible** : indique que l'itinéraire est éligible et qu'il est utilisé pour transférer ou acheminer les paquets vers le préfixe touché pendant le traitement du trafic.
- **Type d'admissibilité** : Les deux types d'admissibilité suivants sont disponibles.
 - **Éligibilité** de la Gateway : Détermine si la passerelle est accessible ou non.
 - **Éligibilité du chemin** : Détermine si le chemin est DEAD ou NOT DEAD.
- **Valeur d'éligibilité** : valeur sélectionnée pour la Gateway ou le chemin d'accès dans la configuration pendant la création de l'itinéraire dans le système. Par exemple, un itinéraire peut être appelé éligible en fonction d'un chemin MCN-WL-1->BR1-WL-2. Ainsi, la valeur d'éligibilité pour cette route dans la section routes est la valeur MCN-WL-1->BR1-WL-2.

Routage

May 6, 2021

Routage dynamique

Citrix SD-WAN introduit la prise en charge des protocoles de routage bien connus sous la fonctionnalité **Routage dynamique**. Cette fonctionnalité facilite la découverte des sous-réseaux LAN, annonce des itinéraires de chemins virtuels pour fonctionner de manière plus transparente au sein des réseaux utilisant les protocoles BGP et OSPF, ce qui permet un déploiement sans interruption du SD-WAN dans un environnement existant sans avoir besoin de configurations de routage statique et de basculement de routeur gracieux.

Filtrage d'itinéraire

Pour les réseaux avec l'apprentissage d'itinéraire activé, Citrix SD-WAN fournit plus de contrôle sur les routes SD-WAN annoncées aux voisins de routage plutôt que sur les routes reçues des voisins de routage, plutôt que sur la publicité et l'acceptation de toutes les routes ou pas.

- Les filtres d'exportation sont utilisés pour inclure ou exclure des itinéraires pour la publicité à l'aide des protocoles OSPF et BGP basés sur des critères de correspondance spécifiques.
- Les filtres d'importation sont utilisés pour accepter ou ne pas accepter les itinéraires reçus à l'aide de voisins OSPF et BGP basés sur des critères de correspondance spécifiques.

Le filtrage d'itinéraire est implémenté sur les routes LAN et les routes de chemin virtuel dans un réseau SD-WAN (datacenter ou branche) et est annoncé sur un réseau non-SD-WAN via BGP et OSPF.

Récapitulatif des itinéraires

La synthèse des itinéraires réduit le nombre de routes qu'un routeur doit maintenir. Un itinéraire récapitulatif est un itinéraire unique qui est utilisé pour représenter plusieurs itinéraires. Il permet d'économiser la bande passante en envoyant une seule annonce d'itinéraire, ce qui réduit le nombre de liens entre les routeurs. Il enregistre de la mémoire car une seule adresse de route est conservée. Les ressources CPU sont utilisées plus efficacement en évitant les recherches récursives.

VRRP

Virtual Router Redundancy Protocol (VRRP) est un protocole largement utilisé qui fournit la redondance de périphérique pour éliminer le point de défaillance unique inhérent à l'environnement statique routé par défaut. VRRP vous permet de configurer deux routeurs ou plus pour former un groupe. Ce groupe apparaît comme une passerelle par défaut unique avec une adresse IP virtuelle et une adresse MAC virtuelle.

Citrix SD-WAN (version 10.0 et ultérieure) prend en charge les versions 2 et 3 de VRRP pour interfonctionner avec tous les routeurs tiers. L'appliance SD-WAN agit comme un routeur maître et dirige le trafic vers l'utilisation du service de chemin virtuel entre les sites. Vous pouvez configurer l'appliance SD-WAN en tant que maître VRRP en configurant l'IP de l'interface virtuelle en tant qu'IP VRRP et en définissant manuellement la priorité sur une valeur supérieure à celle des routeurs homologues. Vous pouvez configurer l'intervalle de publication et l'option preempt.

Utilisation de l'interface de ligne de commande pour accéder à la fonctionnalité de routage

Vous pouvez afficher des informations supplémentaires relatives au routage dynamique et à l'état du protocole. Tapez la commande et la syntaxe suivantes pour accéder au démon de routage et afficher la liste des commandes.

```
'  
dynamic_routing?  
'
```

Routage de superposition SD-WAN

May 6, 2021

Citrix SD-WAN offre une connectivité robuste et résiliente entre les sites distants, les centres de données et les réseaux cloud. La solution SD-WAN peut y parvenir en établissant des tunnels entre les appliances SD-WAN dans le réseau, ce qui permet la connectivité entre les sites en appliquant des

tables de routage qui superposent le réseau de sous-couche existant. Les tables de routage SD-WAN peuvent remplacer ou coexister avec l'infrastructure de routage existante.

Les appliances Citrix SD-WAN mesurent les chemins disponibles unidirectionnellement en termes de disponibilité, de perte, de latence, de gigue et de congestion, et sélectionnent le meilleur chemin par paquet. Cela signifie que le chemin choisi entre le site A et le site B, ne doit pas nécessairement être le chemin choisi du site B au site A. Le meilleur chemin à un moment donné est choisi indépendamment dans chaque direction. Citrix SD-WAN offre une sélection de chemin basé sur des paquets pour une adaptation rapide à toute modification du réseau. Les appliances SD-WAN peuvent détecter les pannes de chemin après seulement deux ou trois paquets manquants, ce qui permet un basculement subsecondaire continu du trafic d'applications vers le chemin WAN le plus proche. Les appliances SD-WAN recalculent chaque état de liaison WAN en environ 50 ms. L'article suivant fournit une configuration de routage détaillée au sein du réseau Citrix SD-WAN.

Table de routage Citrix SD-WAN

La configuration SD-WAN permet des entrées d'itinéraire statiques pour des sites spécifiques et des entrées d'itinéraire apprises par le réseau de sous-couche via des protocoles de routage pris en charge, tels que OSPF, eBGP et iBGP. Les itinéraires ne sont pas seulement définis par leur prochain saut, mais par leur type de service. Cela détermine le mode de transfert de l'itinéraire. Les principaux types de services utilisés sont les suivants :

- **Service local** : désigne tout itinéraire ou sous-réseau local vers l'appliance SD-WAN. Cela inclut les sous-réseaux d'interface virtuelle (créé automatiquement des routes locales) et toute route locale définie dans la table de routage (avec un saut suivant local). La route est annoncée à d'autres appliances SD-WAN qui disposent d'un chemin d'accès virtuel vers ce site local sur lequel cette route est configurée lorsqu'elle est approuvée en tant que partenaire.

Remarque

Soyez prudent lors de l'ajout d'itinéraires par défaut et récapitulez les itinéraires en tant que routes locales, car ceux-ci peuvent entraîner des itinéraires de chemins virtuels sur d'autres sites. Vérifiez toujours les tables de routage pour vous assurer que le routage correct est en vigueur.

- **Chemin virtuel** : désigne tout itinéraire local appris à partir d'un site SD-WAN distant accessible sur les chemins virtuels. Ces routes sont normalement automatiques, mais une route de chemin virtuel peut être ajoutée manuellement sur un site. Tout trafic pour cette route est transféré vers le chemin virtuel défini pour cette route de destination (sous-réseau).
- **Intranet** : indique les routes accessibles via une liaison WAN privée (MPLS, P2P, VPN, etc.). Par exemple, une succursale distante qui se trouve sur le réseau MPLS mais ne possède pas d'appliance SD-WAN. Il est supposé que ces routes doivent être transmises à un certain routeur WAN.

Le service Intranet n'est pas activé par défaut. Tout trafic correspondant à cet itinéraire (sous-réseau) est classé comme intranet pour cette appliance en vue d'être livré à un site qui ne possède pas de solution SD-WAN.

Remarque

Notez que lors de l'ajout d'une route Intranet, il n'y a pas de saut suivant, mais plutôt de transfert vers un service Intranet. Le service est associé à une liaison WAN donnée.

- **Internet** —Ceci est similaire à l'intranet, mais est utilisé pour définir le trafic qui circule vers des liaisons WAN Internet publiques plutôt que des liaisons WAN privées. Une différence unique est que le service Internet peut être associé à plusieurs liaisons WAN et réglé sur l'équilibre de charge (par flux) ou être actif/sauvegarde. Un itinéraire Internet par défaut est créé lorsque le service Internet est activé (il est désactivé par défaut). Tout trafic correspondant à cet itinéraire (sous-réseau) est classé comme Internet pour cette appliance en vue de la livraison aux ressources Internet publiques.

Remarque

Les routes du service Internet peuvent être annoncées sur les autres appliances SD-WAN ou ne peuvent pas être exportées, selon que vous liez ou non l'accès Internet via les chemins virtuels.

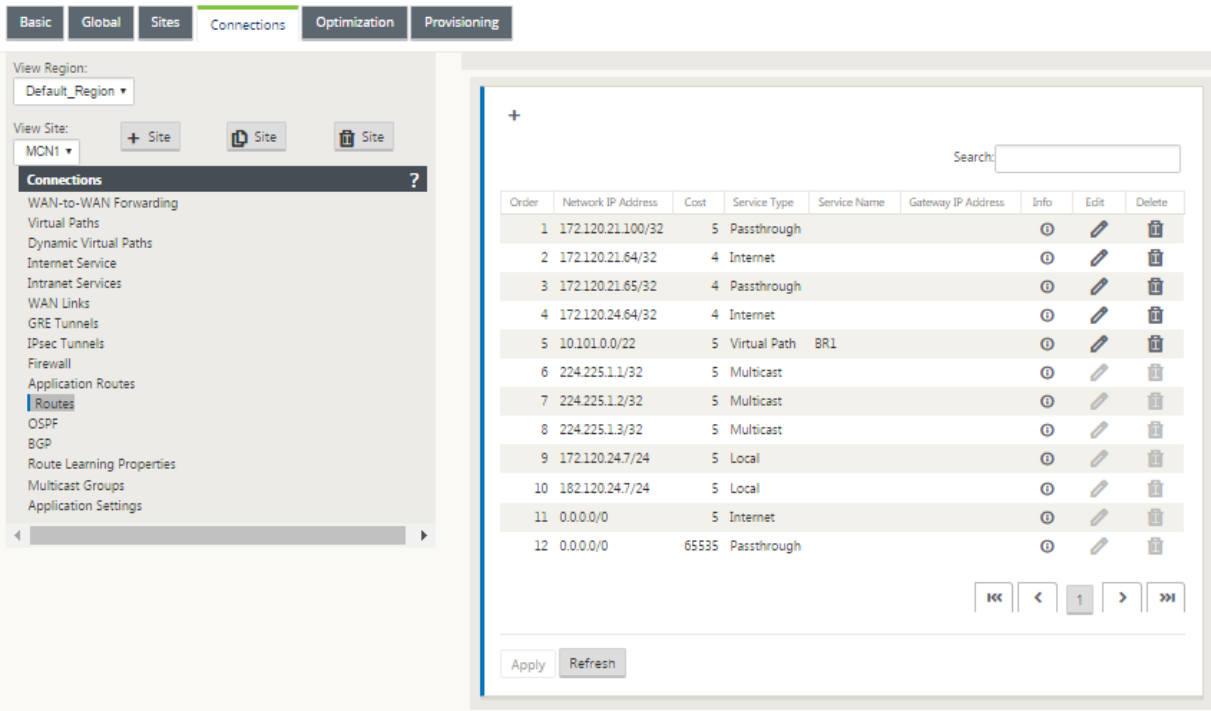
- **Passthrough** : ce service agit comme un service de dernier recours ou de remplacement lorsqu'une appliance est en mode ligne. Si une adresse IP de destination ne correspond pas à un autre itinéraire, l'appliance SD-WAN la transfère simplement sur le saut suivant de liaison WAN. Un itinéraire par défaut : 0.0.0.0/0 coût de 16 itinéraire pass-through est créé automatiquement. Le passage ne fonctionne pas lorsque l'appliance SD-WAN est déployée hors chemin ou en mode Edge/Passerelle. Tout trafic correspondant à cet itinéraire (sous-réseau) est classé comme passthrough pour cette appliance. Il est recommandé que le trafic de transit soit limité autant que possible.

Remarque

La transmission peut être utile lors de l'exécution d'un POC pour éviter d'avoir à configurer de nombreuses gammes, mais soyez prudent en production car le SD-WAN ne tient pas compte de l'utilisation de la liaison WAN pour le trafic envoyé au passage. Il est également utile lorsque vous résolvez des problèmes et que vous souhaitez retirer un certain flux IP de la livraison sur le chemin virtuel.

- **Discard** - Ce n'est pas un service mais un itinéraire de dernier recours qui supprime les paquets s'il correspond. Normalement, cela ne se produit pas s'attendre lorsque l'appliance SD-WAN est déployée hors du chemin d'accès. Vous devez avoir un service Intranet ou une route locale en tant que catch all itinéraire, sinon le trafic est rejeté car il n'y a pas de service passthrough (même si une route passthrough par défaut sera présente).

L'éditeur de configuration SD-WAN permet la personnalisation de la table de routage pour chaque site disponible :



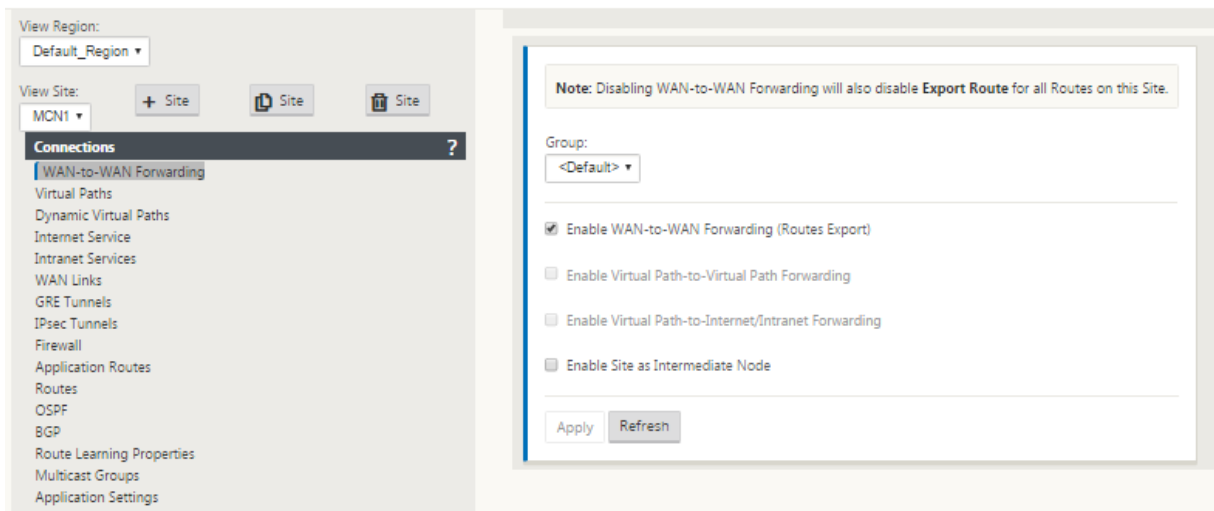
Les entrées de la table de routage sont renseignées à partir de différentes entrées :

- Adresse IP virtuelle configurée (VIP) automatiquement renseignée en tant que route locale de type de service. L'Éditeur de configuration empêche la même affectation VIP à différents nœuds de site.
- Les services Internet activés sur un site local renseignent automatiquement une route par défaut (0.0.0.0/0) localement pour une sortie Internet directe.
- Les itinéraires statiques définis par l'administrateur sur une base par site, qui seront également définis comme un itinéraire local de type de service.
- Une valeur par défaut (0.0.0.0/0) capture tous les itinéraires avec le coût 16 défini comme Passthrough

Les administrateurs peuvent configurer l'une des routes précédentes, mais aussi inclure un type de service, un saut suivant ou une Gateway en fonction du type de service, en plus du coût de l'itinéraire. Un coût d'itinéraire par défaut sera automatiquement ajouté à chaque type d'itinéraire (reportez-vous au tableau suivant pour connaître les coûts d'itinéraire par défaut). En outre, seules les routes de confiance sont annoncées sur d'autres appliances SD-WAN. Les itinéraires non approuvés sont uniquement utilisés par l'appliance locale.

Les routes de noeud client sont uniquement annoncées sur le noeud MCN et aucun autre noeud client par défaut. Pour que les routes de noeud client soient visibles par un autre noeud client Le transfert

WAN vers WAN doit être activé au niveau du nœud MCN.



Lorsque le transfert WAN vers WAN (modèle d'exportation d'itinéraires) est activé sous Paramètres globaux, le site MCN partage les itinéraires annoncés à tous les clients participant à la superposition SD-WAN. L'activation de cette fonctionnalité permet la connectivité IP entre les hôtes de différents sites de nœuds clients, la communication passant par le MCN. La table de routage du nœud client local peut être surveillée sur la page **Surveillance** > **Statistiques** avec Itinéraires sélectionnées dans la liste déroulante **Afficher**.

Statistics

Flows

Routing Protocols

Firewall

IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP Protocol

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 54 of 54 entries

Num#	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
2	172.120.21.65/32	*	Passthrough	Any	YES	*	*	Static	-	-	4	0	YES	N/A	N/A
3	224.225.1.1/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
4	224.225.1.2/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
5	224.225.1.3/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
6	172.120.21.100/32	*	Passthrough	Any	YES	*	*	Static	-	-	5	0	YES	N/A	N/A
7	172.120.24.64/32	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	9	0	YES	N/A	N/A
8	172.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	3458	YES	N/A	N/A
9	182.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
10	172.120.10.0/24	*	MCN1-APAC_RCIN	Default_LAN_Zone	YES	*	APAC_RCIN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
11	172.120.21.0/24	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
12	182.120.10.0/24	*	MCN1-APAC_RCIN	Default_LAN_Zone	YES	*	APAC_RCIN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
13	192.168.255.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
14	192.172.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn01	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
15	192.172.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn02	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
16	192.172.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn03	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
17	192.172.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn04	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
18	192.172.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn05	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
19	192.172.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn06	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
20	192.172.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn07	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
21	192.172.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
22	192.172.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn13	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
23	192.172.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn14	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
24	192.172.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn15	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
25	192.172.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn16	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
26	192.172.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn17	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
27	192.172.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn18	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
28	192.172.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn19	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
29	192.172.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn20	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
30	192.120.10.0/24	*	MCN1-APAC_RCIN	Default_LAN_Zone	YES	*	APAC_RCIN	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
31	172.108.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn01	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
32	172.108.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn02	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
33	172.108.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn03	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
34	172.108.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn04	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
35	172.108.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn05	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
36	172.108.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn06	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
37	172.108.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn07	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
38	172.108.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn08	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
39	172.108.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn13	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
40	172.108.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn14	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
41	172.108.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn15	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
42	172.108.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn16	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
43	172.108.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn17	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
44	172.108.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn18	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
45	172.108.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn19	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
46	172.108.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn20	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
47	10.101.0.0/22	*	MCN1-BR1	Any	YES	*	BR1	Static	-	-	5	0	YES	N/A	N/A
48	10.101.0.0/22	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
49	172.105.96.0/20	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
50	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	5	401109	YES	N/A	N/A
51	0.0.0.0/0	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
52	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	40031844	YES	N/A	N/A
53	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

Showing 1 to 54 of 54 entries

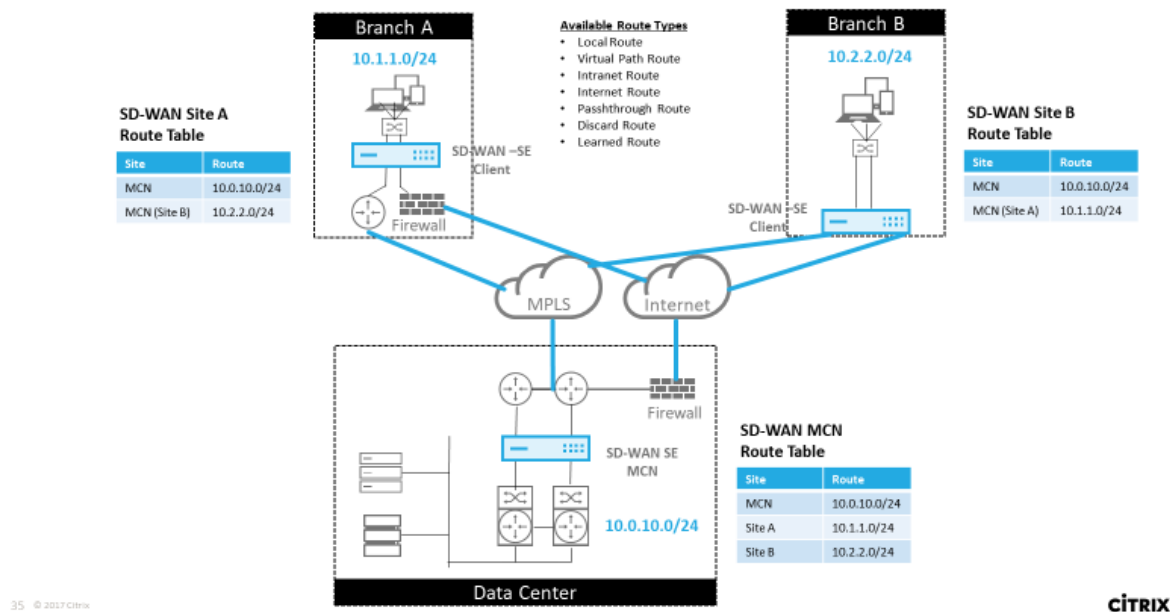
First Previous 1 Next Last

Chaque itinéraire pour les sous-réseaux de succursales distantes est annoncé en tant que service via le chemin virtuel qui se connecte via le MCN, la colonne **Site** étant renseignée avec le nœud client où réside la destination en tant que sous-réseau local.

Dans l'exemple suivant, lorsque le **transfert WAN vers WAN** (Routes Export) est activé, la branche A

dispose d'une entrée de table de routage pour le sous-réseau Branche B (10.2.2.0/24) via le MCN en tant que saut suivant.

SD-WAN Overlay Route Tables



Comment le trafic Citrix SD-WAN correspond sur des itinéraires définis

Le processus de correspondance pour les itinéraires définis sur Citrix SD-WAN est basé sur la correspondance de préfixe la plus longue pour le sous-réseau de destination (similaire à une opération de routeur). Plus l'itinéraire est spécifique, plus le changement est élevé. Le tri est effectué dans l'ordre suivant :

1. Les correspondances de préfixe les plus longues
2. Coût
3. Service

Par conséquent, un itinéraire /32 précède toujours un itinéraire /31. Pour deux /32 itinéraires, un itinéraire de coût 4 précède toujours un itinéraire de coût 5. Pour deux itinéraires /32 coûtent 5, les itinéraires sont choisis en fonction de l'hôte IP commandé. La commande de service est la suivante : Local, Chemin virtuel, Intranet, Internet, Passthrough, Ignorer.

À titre d'exemple, considérez les deux routes suivantes comme suit :

- 192.168.1.0/24 Coût 5
- 192.168.1.64/26 Coût 10

Un paquet destiné à l'hôte 192.168.1.65 utiliserait cette dernière route même si le coût est plus élevé. Sur cette base, il est courant que la configuration soit en place uniquement pour les routes destinées

à être livrées via la superposition de chemin virtuel avec d'autres trafic entrant dans la capture de toutes les routes telles qu'une route par défaut vers le service de passage.

Les itinéraires peuvent être configurés dans une table de routage de noeud de site qui a le même préfixe. Le saut de connexion passe ensuite au coût de l'itinéraire, au type de service (chemin virtuel, intranet, Internet, etc.) et à l'adresse IP de saut suivant.

Flux de paquets de routage Citrix SD-WAN

- Correspondance de l'itinéraire du trafic LAN vers WAN (chemin virtuel) :
 1. Le trafic entrant est reçu par l'interface LAN et est traité.
 2. La trame reçue est comparée à la table de routage pour la correspondance de préfixe la plus longue.
 3. Si une correspondance est trouvée, la trame est traitée par le moteur de règles et un flux est créé dans la base de données de flux.
- Correspondance de l'itinéraire du trafic WAN vers LAN (chemin virtuel) :
 1. Le trafic de chemin virtuel est reçu par SD-WAN du tunnel et est traité.
 2. L'apppliance compare l'adresse IP source pour vérifier si la source est locale.
 - Si oui, alors éligible au réseau WAN et correspond à la destination IP à la table de routage ou au chemin virtuel.
 - Si non, vérifiez le transfert WAN vers WAN activé.
 3. (Retransmission WAN vers WAN désactivée) Transférer vers LAN en fonction des itinéraires locaux.
 4. (Transfert WAN vers WAN activé) Transférer vers le chemin virtuel en fonction de la table de routage.
- Trafic de chemin non virtuel :
 1. Le trafic entrant est reçu sur l'interface LAN et est traité.
 2. La trame reçue est comparée à la table de routage pour la correspondance de préfixe la plus longue.
 3. Si une correspondance est trouvée, la trame est traitée par le moteur de règles et un flux est créé dans la base de données de flux.

Prise en charge du protocole de routage Citrix SD-WAN

Citrix SD-WAN version 9.1 a introduit les protocoles de routage OSPF et BGP dans la configuration. L'introduction de protocoles de routage au SD-WAN a permis d'intégrer plus facilement le SD-WAN dans des réseaux de sous-couche plus complexes où les protocoles de routage sont activement utilisés. Avec les mêmes protocoles de routage activés sur SD-WAN, la configuration des sous-réseaux désignés pour utiliser la superposition SD-WAN a été facilitée. En outre, les protocoles de routage permettent la communication entre les sites SD-WAN et non SD-WAN avec une communication directe avec les routeurs périphériques clients existants utilisant le protocole de routage commun. Citrix SD-WAN participant aux protocoles de routage fonctionnant dans le réseau sous-jacent peut être fait quel que soit le mode de déploiement du SD-WAN (mode Inline, mode Virtual Inline ou mode Edge/Gateway). En outre, le SD-WAN peut être déployé en mode « apprentissage seulement » où le SD-WAN peut recevoir des itinéraires mais ne pas annoncer des itinéraires de retour à la sous-couche. Ceci est utile lors de l'introduction de la solution SD-WAN dans un réseau où l'infrastructure de routage est complexe ou incertaine.

Important

Il est facile de fuir la route indésirable, si vous n'êtes pas prudent.

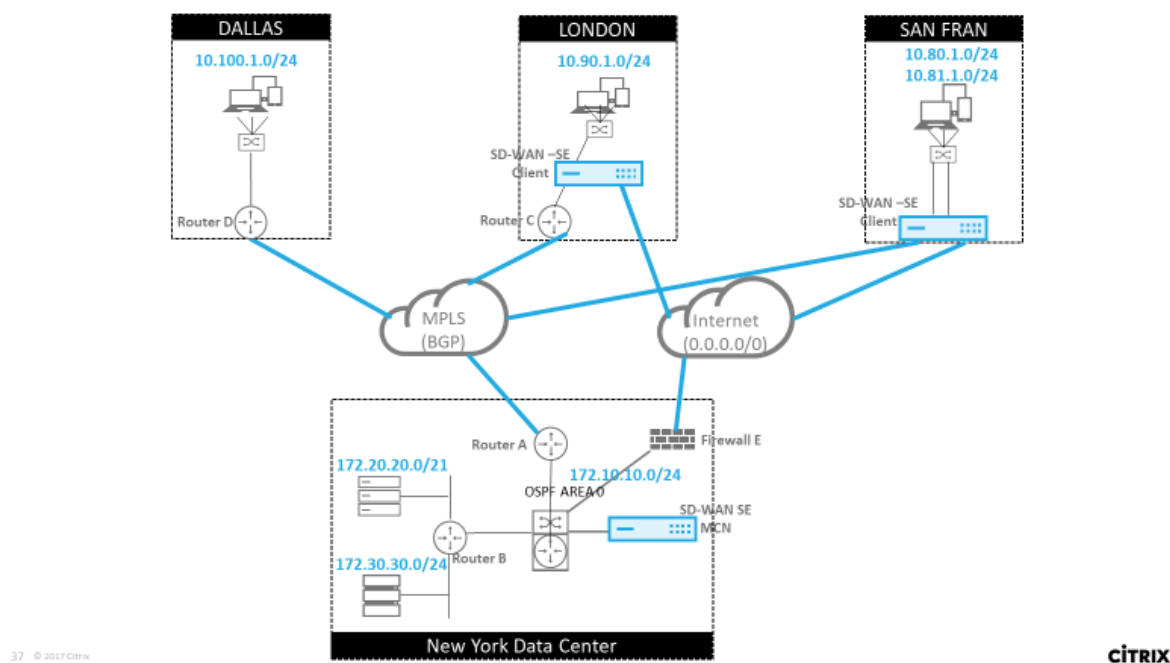
La table de routage SD-WAN Virtual Path fonctionne comme un protocole EGP (External Gateway Protocol), similaire à BGP (pensez site à site). Par exemple, lorsque SD-WAN annonce des itinéraires de l'appliance SD-WAN vers OSPF, ils sont généralement considérés comme externes au site et au protocole.

Remarque

Soyez conscient des environnements qui ont des IGP sur l'ensemble de l'infrastructure (via le WAN) car cela complique l'utilisation des itinéraires annoncés par SD-WAN. L'EIGRP est largement utilisé sur le marché et le SD-WAN n'interagit pas avec ce protocole.

L'une des difficultés rencontrées lors de l'introduction des protocoles de routage à un déploiement SD-WAN est que la table de routage n'est pas disponible tant que le service SD-WAN n'est pas activé et ne fonctionne pas sur le réseau. Par conséquent, il n'est pas recommandé d'activer initialement la publicité des itinéraires à partir de l'appliance SD-WAN. Utilisez les filtres d'importation et d'exportation pour une introduction progressive des protocoles de routage sur SD-WAN.

Jetons un coup d'oeil de plus près en examinant l'exemple suivant :



Dans cet exemple, nous examinons un cas d'utilisation du protocole de routage. Le réseau précédent compte quatre emplacements : New York, Dallas, Londres et San Francisco. Nous déployons des appliances SD-WAN à trois de ces emplacements et utilisons SD-WAN pour créer un réseau WAN hybride où MPLS et Internet WAN Links seront utilisés pour fournir un WAN virtualisé. Étant donné que Dallas n'aura pas de périphérique SD-WAN, nous devons réfléchir à la meilleure façon d'intégrer les protocoles de route existants à ce site afin d'assurer une connectivité complète entre les réseaux de superposition et de sous-couche SD-WAN.

Dans l'exemple de réseau, eBGP est utilisé entre les quatre emplacements du réseau MPLS. Chaque emplacement possède son propre numéro de système autonome (ASN).

Dans le centre de données de New York, OSPF est en cours d'exécution pour annoncer les sous-réseaux de centre de données principaux sur les sites distants et également annoncer une route par défaut à partir du pare-feu de New York (E). Dans cet exemple, tout le trafic Internet est rétroacheminé vers le centre de données, même si les succursales de Londres et de San Francisco ont un chemin vers Internet.

Le site de San Francisco doit également être noté pour ne pas avoir de routeur. Le SD-WAN est déployé en mode Edge/Gateway, cette appliance étant la Gateway par défaut pour le sous-réseau de San Francisco et participant également à l'eBGP vers le MPLS.

- Avec le centre de données de New York, notez que le SD-WAN est déployé en mode virtuel Inline. L'objectif est de participer au protocole de routage OSPF existant pour acheminer le trafic vers l'appliance en tant que Gateway privilégiée.
- Le site londonien est déployé en mode traditionnel en ligne. Le routeur WAN en amont (C) sera toujours la Gateway par défaut pour le sous-réseau London.

- Le site San Francisco est un site nouvellement introduit sur ce réseau et le SD-WAN est prévu pour être déployé en mode Edge/Gateway et agir comme Gateway par défaut pour le nouveau sous-réseau San Francisco.

Examinez certaines tables de routage de sous-couche existantes avant de mettre en œuvre le SD-WAN.

Routeur Core de New York B :

```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:08:56
O>* 10.90.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h00m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

Les sous-réseaux locaux de New York (172.x.x.x) sont disponibles sur le routeur B comme étant directement connecté, et à partir de la table de routage, nous identifions que la route par défaut est 172.10.10.3 (Pare-feu E). En outre, nous pouvons voir que les sous-réseaux Dallas (10.90.1.0/24) et London (10.100.1.0/24) sont disponibles via 172.10.10.1 (MPLS Router A). Les coûts de l'itinéraire indiquent qu'ils ont été tirés de l'eBGP.

Remarque

Dans l'exemple fourni, San Francisco n'est pas répertorié comme itinéraire, car nous n'avons pas encore déployé le site avec SD-WAN en mode Edge/Gateway pour ce réseau.

```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:09:52
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h09m
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 1d23h10m
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h01m
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
C>* 192.168.10.0/24 is directly connected, eth2
O 192.168.65.0/24 [110/20] via 172.10.10.2, 1d19h57m
C>* 192.168.65.0/24 is directly connected, eth0
```

Pour le routeur WAN de New York (A), les itinéraires et les itinéraires appris par OSPF à travers le MPLS via eBGP sont répertoriés. Notez les coûts de l'itinéraire. BGP est un domaine administratif inférieur et le coût par défaut 20/1 par rapport à OSPF 110/10.

Routeur D de Dallas :

Pour le routeur WAN (D) de Dallas, toutes les routes sont apprises à travers le MPLS.

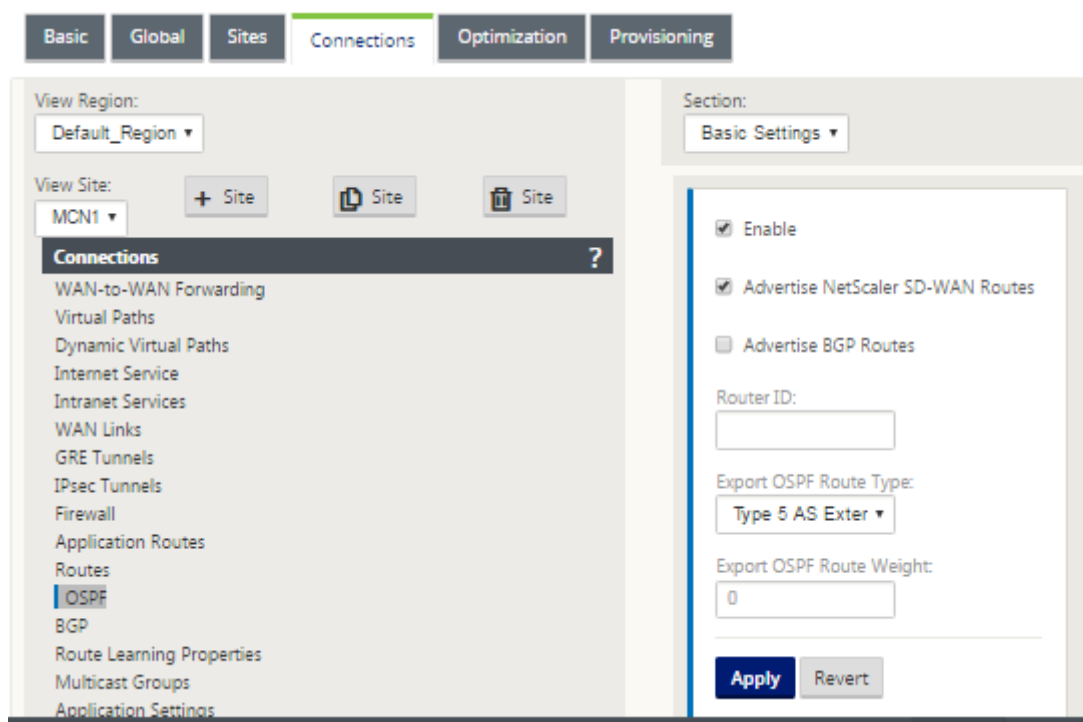
```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:10:17
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h10m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 1d23h10m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

Remarque

Dans cet exemple, vous pouvez ignorer le sous-réseau 192.168.65.0/24. Il s'agit d'un réseau de gestion qui n'est pas pertinent pour l'exemple. Tous les routeurs sont connectés au sous-réseau de gestion, mais ils ne sont annoncés dans aucun protocole de routage.

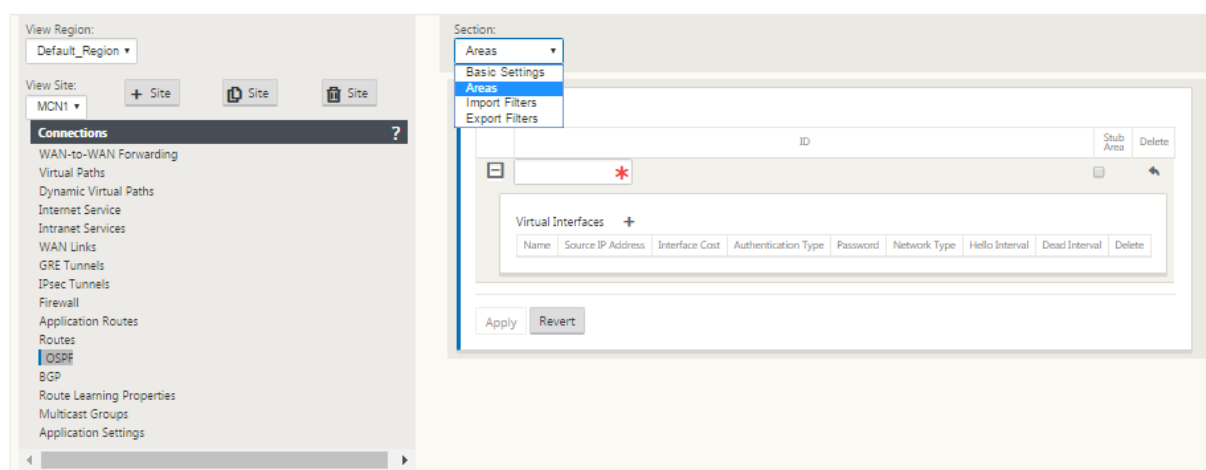
Dans Citrix SD-WAN, nous pouvons ajouter la superposition SD-WAN en activant OSPF sur le SD-WAN situé dans le site de New York sous **Connexions > Afficher le site > OSPF > Paramètres de base** :



Remarque

Par défaut, le type d'**itinéraire d'exportation OSPF est Type 5 Externe**. Cela est dû au fait que la table de routage SD-WAN est considérée comme externe au protocole OSPF et donc OSPF préférera une route apprise interne (intra-zone), donc les routes annoncées par SD-WAN peuvent ne pas avoir priorité.

Lorsque OSPF est utilisé sur le WAN (c'est-à-dire les réseaux MPLS), cela peut être modifié en Type un intra-zone. Les zones OSPF peuvent être configurées comme indiqué ci-dessous.



Zone 0 ajoutée avec le réseau local dérivé de l'interface virtuelle (172.10.10.0), tous les autres paramètres ont été laissés par défaut.

Pour le nouveau site de San Francisco, nous devons activer eBGP car il sera directement connecté au réseau MPLS et fonctionnera comme l'itinéraire périphérique client pour le site. BGP peut être activé sous **Connexions > Afficher le site > BGP > Paramètres de base**.

Notez le numéro 13 du système autonome.

Section: Basic Properties

☒ Enable

☒ Advertise NetScaler SD-WAN Routes

☐ Advertise OSPF Routes

Router ID:
192.168.10.4

Local Autonomous System:
13

Apply Revert

Section: Neighbors

	Virtual Interface	Source IP	Neighbor IP	Neighbor AS	Hold Time(s)	Local Preference	BGP Metric	Multi Hop	Password	Delete														
+	V1	192.168.10.4	192.168.10.1	65011	3600	100		<input checked="" type="checkbox"/>																
Policies + <table border="1"> <thead> <tr> <th>Order</th> <th>Network Address</th> <th>BGP Community(AA:NN)</th> <th>AS Path</th> <th>BGP Policy</th> <th>Direction</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>(auto)</td> <td><Manual></td> <td>*</td> <td><Manual></td> <td>*</td> <td><Accept></td> <td></td> </tr> </tbody> </table>											Order	Network Address	BGP Community(AA:NN)	AS Path	BGP Policy	Direction	Delete	(auto)	<Manual>	*	<Manual>	*	<Accept>	
Order	Network Address	BGP Community(AA:NN)	AS Path	BGP Policy	Direction	Delete																		
(auto)	<Manual>	*	<Manual>	*	<Accept>																			
+	V1	192.168.10.4	192.168.10.2	65012	3600	100		<input checked="" type="checkbox"/>																

Apply Refresh

L'eBGP s'est associé l'un à l'autre emplacement. Chaque ASN est différent.

Il est important de comprendre comment les routes sont passées entre la table de routage Virtual Path et les protocoles de routage dynamiques utilisés. Il est facile de créer des boucles de routage ou d'annoncer des itinéraires d'une manière défavorable. Le mécanisme de filtre nous donne la possibilité de contrôler ce qui entre et sort de la table de routage. Nous considérons chaque emplacement à tour de rôle.

- L'emplacement de San Francisco comporte deux sous-réseaux locaux **10.80.1.0/24** et **10.81.1.0/24**. Nous voulons les faire connaître via eBGP afin que des sites comme Dallas puissent encore atteindre le site de San Francisco via le réseau de sous-couche et que des sites comme Londres et New York puissent encore atteindre San Francisco via le réseau de superposition Virtual Path. Nous voulons également apprendre de l'accessibilité d'eBGP à

tous les sites dans le cas où la superposition du chemin virtuel SD-WAN tombe en panne et que l’environnement doit revenir à l’utilisation du MPLS uniquement. Nous ne voulons pas non plus republier tout ce que le SD-WAN apprend de eBGP aux routeurs SD-WAN. Pour ce faire, les filtres doivent être configurés comme suit :

- Importez toutes les routes depuis eBGP. Ne pas republier/exporter les routes vers des appliances SD-WAN.

Section: Import Filters

Order	Source Router	Destination	Prefix	Next Hop	Protocol	Route Tag	Cost	AS Path Length	Include	Enabled	Delete	Clone
100	*	<Manual>	eq *	*	Any	*	eq *	eq *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<div><input type="checkbox"/> Export Route to Citrix Appliances Citrix SD-WAN Cost: 6 Service Type: Local Service Name: <input type="checkbox"/> Eligibility Based On Gateway Path: <None></div>												
200	*	<Manual>	eq *	*	Any	*	eq *	eq *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
200	*	<Manual>	eq *	*	Any	*	eq *	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

Apply Revert

- Exporter des itinéraires locaux vers eBGP

La règle par défaut pour l’exportation est d’exporter tout. La règle 200 est utilisée pour remplacer la règle d’erreur pour ne pas lire les itinéraires. Toute route correspondant à un préfixe SD-WAN a appris sur les chemins virtuels.

	Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
+	100	<Manual> *	eq 24	eq *	Local	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
+	200	<Manual> 0.0.0.0/0	eq *	eq *	Any	<Any>	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
	(auto)	<Manual> *	eq *	eq *	Any	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Une fois les appliances Citrix SD-WAN déployées, nous pouvons jeter un regard actualisé sur les tables de routage du routeur BGP sur le site de Dallas. Nous voyons que les sous-réseaux 10.80.1.0/24 et 10.81.1.0/24 sont correctement vus via eBGP à partir du SD-WAN de San Francisco.

Routeur Dallas D :

```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

En outre, la table de routage Citrix SD-WAN peut être affichée sur la page **Surveillance > Statistiques > Afficher les itinéraires**.

San Francisco Citrix SD-WAN :

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 16 of 16 entries

FirstPrevious1NextLast

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 16 of 16 entries

FirstPrevious1NextLast

Citrix SD-WAN affiche toutes les routes apprises, y compris les routes disponibles via la superposition Virtual Path.

Considérons 172.10.10.0/24, qui est situé dans le centre de données de New York. Cette voie est ap- prise de deux façons :

- En tant que route de chemin virtuel (numéro 3), service = NYC-SFO avec un coût de 5 et tapez statique. Il s’agit d’un sous-réseau local annoncé par l’appliance SD-WAN à New York. Il est sta- tique en ce sens qu’il est directement connecté à l’appliance ou qu’il s’agit d’une route statique

manuelle entrée dans la configuration. Il est accessible car le chemin virtuel entre les sites est en état de travail/de mise en marche.

- Comme une route annoncée par BGP (numéro 6), avec un coût de 6. Ceci est maintenant considéré comme une route de secours.

Étant donné que le préfixe est égal et que le coût est différent, SD-WAN utilise la route Virtual Path, à moins qu'elle ne devienne indisponible, auquel cas la route de secours est apprise via BGP.

Maintenant, considérons la route 172.20.20.0/24.

- Ceci est appris comme une route de chemin virtuel (numéro 9) mais a un type de dynamique et un coût de 6. Cela signifie que l'apppliance SD-WAN distante a appris cette route via un protocole de routage, dans ce cas OSPF. Par défaut, le coût de l'itinéraire est plus élevé.
- SD-WAN apprend également cette route via BGP avec le même coût, donc dans ce cas cette route peut être préférée à la route Virtual Path.

Pour garantir un routage correct, nous devons augmenter le coût de l'itinéraire BGP pour nous assurer que nous avons un itinéraire Virtual Path et qu'il s'agit de l'itinéraire préféré. Cela peut être fait en ajustant le poids de la route du filtre d'importation pour qu'il soit supérieur à la valeur par défaut de 6.

The screenshot shows the 'Import Route' configuration window in Citrix SD-WAN. The 'NetScaler SD-WAN Cost' field is set to 10. The 'Service Type' is set to 'Local'. The 'Path' is set to '<None>'. The 'Apply' button is highlighted in blue.

Après avoir effectué l'ajustement, nous pouvons actualiser la table de routage SD-WAN sur l'apppliance San Francisco pour voir les coûts d'itinéraire ajustés. Utilisez l'option de filtre pour focaliser la liste affichée.

Routes for routing domain : Default_RoutingDomain

Filter: 172.20.20.0/24 in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries (filtered from 16 total entries)

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
5	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
8	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A

Showing 1 to 2 of 2 entries (filtered from 16 total entries)

Enfin, regardons l'itinéraire par défaut appris sur le SD-WAN de San Francisco. Nous voulons rediriger tout le trafic Internet vers New York. Nous pouvons voir que nous l'envoyons en utilisant le chemin

virtuel, s'il est en place, ou via le réseau MPLS comme un secours.

Routes for routing domain : Default_RoutingDomain

Filter: 0.0.0.0/0 in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 16 total entries)

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
12	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
13	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 16 total entries)

Nous voyons également une route de passage et de rejet avec le coût 16. Il s'agit d'itinéraires automatiques qui ne peuvent pas être supprimés. Si le périphérique est en ligne, la route passthrough est utilisée en dernier recours, donc si un paquet ne peut pas être associé à une route plus spécifique, SD-WAN le transmettra au saut suivant du groupe d'interface. Si le SD-WAN est hors chemin ou en mode bord/passerelle, il n'y a pas de service de transmission, auquel cas SD-WAN supprime le paquet en utilisant la route de rejet par défaut. Le nombre de coups indique le nombre de paquets qui touchent chaque route, ce qui peut être utile lors du dépannage.

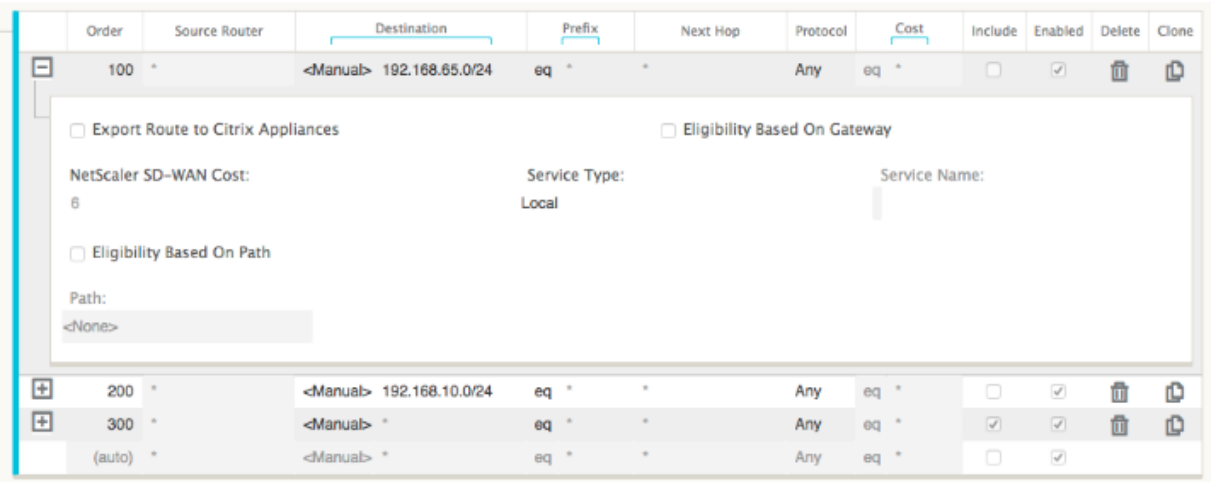
Maintenant, en nous concentrant sur le site de New York, nous voulons que le trafic destiné aux sites distants (Londres et San Francisco) soit dirigé vers l'appliance SD-WAN lorsque le chemin virtuel est actif.

Plusieurs sous-réseaux sont disponibles sur le site de New York :

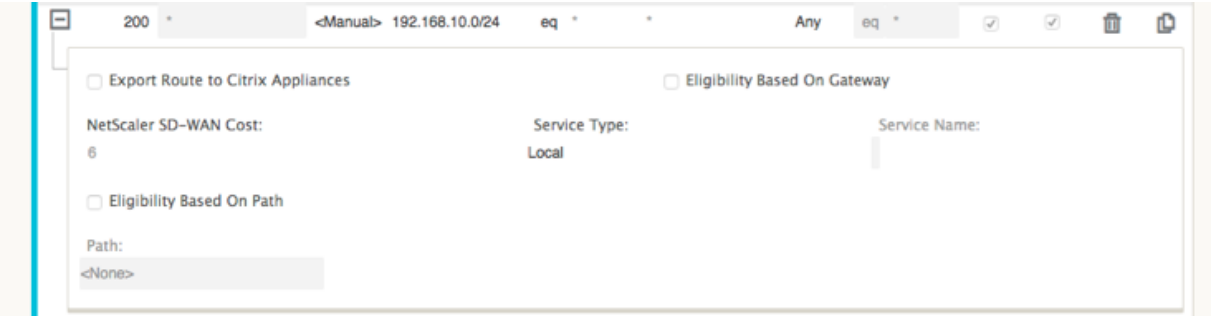
- 172.10.10.0/24 (directement connecté)
- 172.20.20.0/24 (annoncé via OSPF à partir du routeur central B)
- 172.30.30.0/24 (annoncé via OSPF à partir du routeur central B)

Nous sommes également tenus de fournir le flux de trafic vers Dallas (10.100.1.0/24) via MPLS.

Enfin, nous voulons que tout le trafic lié à Internet route vers le pare-feu E à 172.10.10.3 comme un saut suivant. SD-WAN apprend cette route par défaut via OSPF et à faire de la publicité sur le chemin virtuel. Les filtres pour le site de New York sont les suivants :

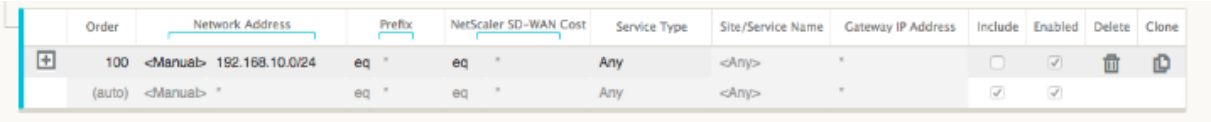


Le site SD-WAN de New York importe toutes les routes du réseau de gestion. Cela peut être ignoré. On peut se concentrer sur le filtre 200.



Le filtre 200 est utilisé pour importer 192.168.10.0/24 (notre noyau MPLS) pour l’accessibilité, mais pas pour l’exporter vers le chemin virtuel. Activez la case à cocher **Inclure** et vérifiez que la case à **cocher Exporter la route vers Citrix Appliances** est désactivée. Toutes les autres routes sont ensuite incluses.

Pour les filtres d’exportation, nous pouvons exclure la route pour 192.168.10.0/24. En effet, en tant que sous-réseau directement connecté sur le site de San Francisco, nous ne pouvons pas filtrer cette route à la source, donc elle est supprimée à cette fin.



Passons maintenant en revue la table des itinéraires actualisés à partir de la route principale sur le site de New York.

Routeur de New York B :

```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 4d22h22m
O>* 10.80.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.81.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.90.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h50m
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 4d22h22m
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 4d22h22m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

Nous pouvons voir les sous-réseaux de San Francisco (10.80.1.0 et 10.81.1.0) et de Londres (10.90.1.0) maintenant annoncés via l’appliance SD-WAN de New York (172.10.10.10). La route 10.100.1.0/24 est toujours annoncée par le biais de la sous-couche MPLS Router A. Voyons la table de route SD-WAN du site de New York.

Site de New York SD-WAN Tableau d’itinéraire :

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 11 of 11 entries

First

Previous

1

Next

Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24	*	Local	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0.0/0	172.10.10.3	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
10	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Nous pouvons voir les routes correctes pour les sous-réseaux locaux appris via OSPF, une route vers le site de Dallas apprise par le routeur MPLS A et les sous-réseaux distants pour les sites de San Francisco et de Londres. Voyons le routeur MPLS A. Ce routeur participe à OSPF et BGP.

```

vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:04:12
O 10.80.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O 10.81.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O 10.90.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 00:05:11
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 00:04:28
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 00:05:24
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 00:05:09
C>* 192.168.10.0/24 is directly connected, eth2
O 192.168.65.0/24 [110/20] via 172.10.10.2, 00:04:12
C>* 192.168.65.0/24 is directly connected, eth0

```

A partir de la table de routage, ce routeur A apprend les sous-réseaux distants via BGP et OSPF avec la distance administrative et le coût de la route BGP (20/5) étant inférieurs à OSPF (110/10) et donc préférés. Dans cet exemple, réseau où il n'y a qu'une seule route principale, cela peut ne pas causer de problème. Toutefois, le trafic arrivant ici serait livré via le réseau MPLS plutôt que d'être envoyé à l'appliance SD-WAN (172.10.10.10). Si nous voulons maintenir une symétrie de routage complète, nous aurions besoin d'une carte de routage pour ajuster le coût AD/métrique afin qu'il y ait une préférence de routage provenant de l'itinéraire 172.10.10.10 plutôt que l'itinéraire appris via eBGP.

Alternativement, une route « backdoor » peut être configurée pour forcer le routeur à préférer la route OSPF sur la route BGP. Notez la route statique de l'adresse IP virtuelle SD-WAN vers l'appliance SD-WAN du site de Londres.

```

S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2

```

Ceci est nécessaire pour vous assurer que le chemin virtuel est réacheminé vers l'appliance SD-WAN du site de New York si le chemin MPLS tombe en panne. Comme il y a une route pour le 10.90.1.0/24 annoncée via 172.10.10.10 (New York SD-WAN). Il est également recommandé de créer une règle de service de remplacement pour supprimer tous les paquets UDP 4 980 sur l'appliance SD-WAN afin d'empêcher le chemin virtuel de revenir sur lui-même.

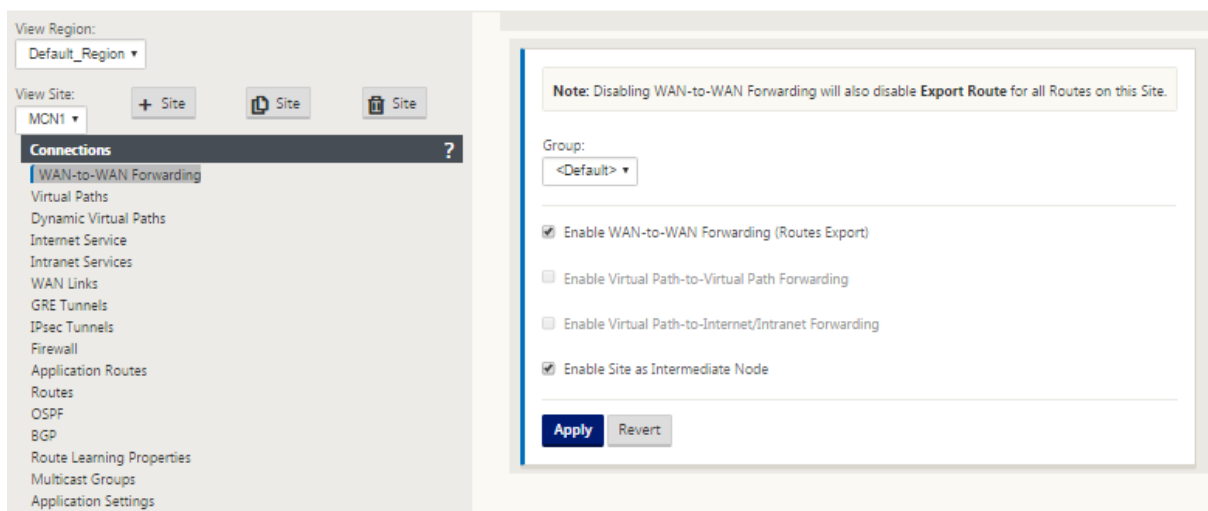
Chemins virtuels dynamiques

Les chemins virtuels dynamiques peuvent être autorisés entre deux nœuds clients pour créer des chemins virtuels à la demande pour une communication directe entre les deux sites. L'avantage d'un chemin virtuel dynamique est que le trafic peut circuler directement d'un nœud client au second sans avoir à traverser le MCN ou deux chemins virtuels, ce qui peut ajouter de la latence au flux de trafic. Les chemins virtuels dynamiques sont créés et supprimés dynamiquement en fonction des seuils de trafic définis par l'utilisateur. Ces seuils sont définis en tant que paquets par seconde (pps) ou bande passante (kbps). Cette fonctionnalité permet une topologie dynamique de superposition SD-WAN à maillage complet.

Une fois que les seuils de chemins virtuels dynamiques sont atteints, les nœuds clients créent dynamiquement leur chemin virtualisé les uns aux autres en utilisant tous les chemins WAN disponibles entre les sites et en font pleinement usage de la manière suivante :

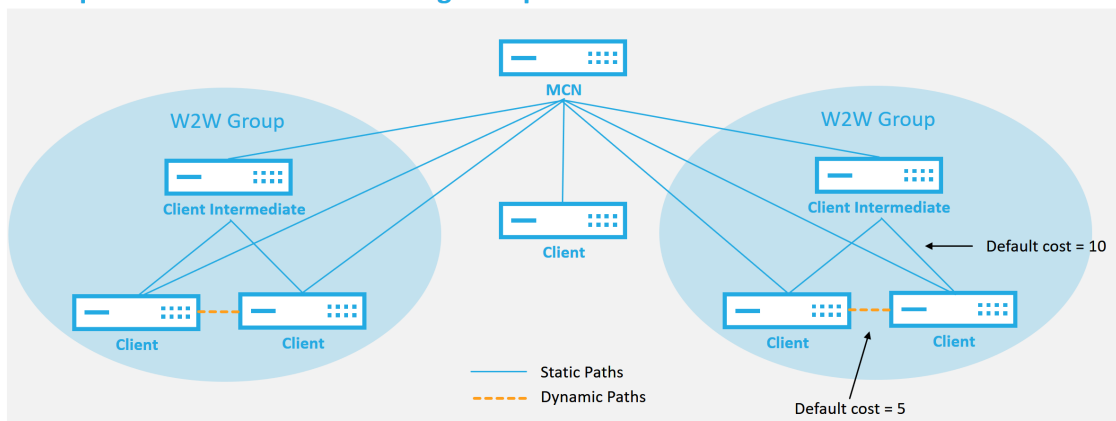
- Envoyer des données groupées le cas échéant et vérifier qu'aucune perte n'est perdue, puis
- Envoyez des données Interactives et vérifiez qu'aucune perte n'est perdue, puis
- Envoyer des données en temps réel après que les données groupées et interactives soient considérées comme stables (aucune perte ou niveaux acceptables)
- S'il n'y a pas de données groupées ou interactives, envoyez des données en temps réel après que le chemin virtuel dynamique soit stable pendant une période
- Si les données utilisateur sont inférieures aux seuils configurés pour une période définie par l'utilisateur, le chemin virtuel dynamique est déchiré

Les chemins virtuels dynamiques ont le concept d'un site intermédiaire. Le site intermédiaire peut être un site MCN ou tout autre site du réseau sur lequel le chemin virtuel statique est configuré et connecté à deux ou plusieurs autres nœuds clients. Une autre exigence de conception est d'activer le transfert WAN vers WAN, ce qui permet de publier toutes les routes de tous les sites vers les nœuds clients où le chemin virtuel dynamique est souhaité. **Activer le site en tant que nœud intermédiaire** doit être activé en plus **du transfert WAN vers WAN** pour ce site intermédiaire afin de surveiller la communication du nœud client et de dicter quand le chemin dynamique doit être établi et arraché.



Plusieurs groupes de redirection WAN à WAN peuvent être autorisés dans la configuration SD-WAN, ce qui permet un contrôle total de l'établissement du chemin entre certains nœuds clients et non pas d'autres.

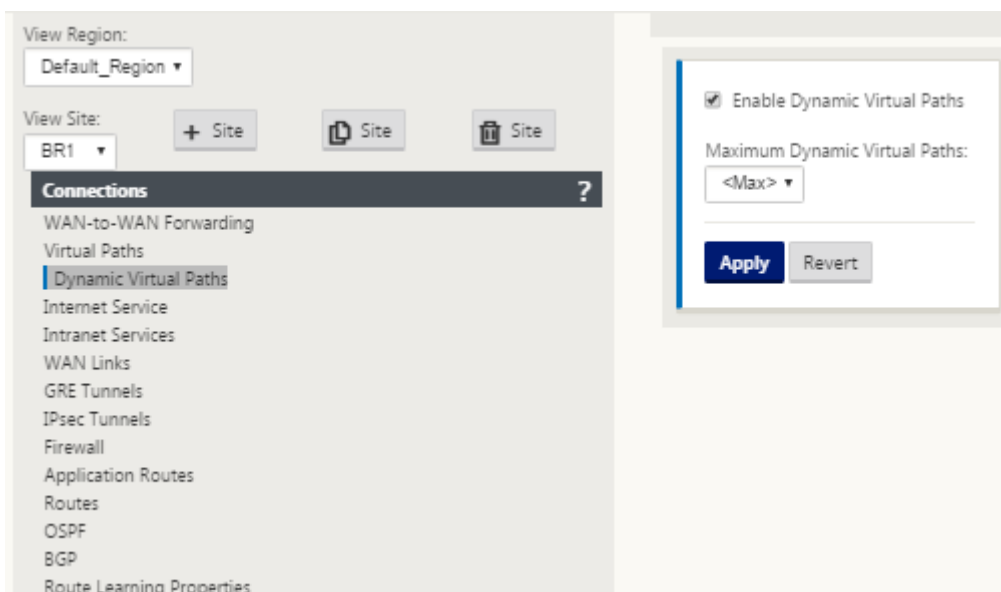
Multiple WAN to WAN Forwarding Groups



WAN to WAN Forwarding Group:

- A network can have multiple WAN to WAN Forwarding Groups
- Direct dynamic path will have a lower cost than through the intermediate node

Pour que les nœuds clients fonctionnent en tant que sites intermédiaires, un chemin virtuel statique doit être configuré entre celui-ci et les clients associés à ce **groupe de transfert WAN** à WAN. En outre, les nœuds clients doivent **activer l'option Activer le chemin virtuel dynamique** activé pour chaque nœud client.



Chaque périphérique SD-WAN possède sa propre table de routage unique avec les détails suivants définis pour chaque itinéraire :

- Num : ordre d'acheminement de cette appliance basé sur le processus de correspondance (le nombre le plus bas est traité en premier)
- Adresse réseau : adresse de sous-réseau ou d'hôte
- Passerelle si nécessaire
- Service —quel service est appliqué pour cet itinéraire
- Zone de pare-feu : classification de zone de pare-feu de l'itinéraire
- Reachable —Identifie si l'état Virtual Path est actif pour ce site
- Site —Nom du site sur lequel l'itinéraire devrait exister
- Type —Identification du type d'itinéraire (statique ou dynamique)
- Voisin Direct
- Coût - coût de l'itinéraire spécifique
- Nombre de coups : combien de fois l'itinéraire a été utilisé par paquet. Cela serait utilisé pour vérifier qu'une route est atteinte correctement.
- Éligible
- Type d'admissibilité
- Valeur d'admissibilité

Voici un exemple de table de routage de site SD-WAN :

Routes for routing domain : Default_RoutingDomain

Filter: in

Show entries Showing 1 to 13 of 13 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 13 of 13 entries

Notez dans la table de routage SD-WAN précédente qu'il y a plus d'éléments qui ne sont pas normalement disponibles dans les routeurs traditionnels. La plus remarquable est la colonne « Reachable », qui rend l'itinéraire actif ou inactif (oui/non) en fonction de l'état du chemin WAN. Les routes répertoriées ici sont supprimées en fonction de différents états du service (le chemin virtuel étant en panne à titre d'exemple). Les autres événements qui peuvent forcer une route à être inéligible sont l'état du chemin vers le bas, le saut suivant inaccessible ou le lien WAN vers le bas.

Dans le tableau précédent, nous pouvons voir 14 itinéraires définis. Une description des itinéraires ou des groupes de routes est décrite comme suit :

- Route 0 —Sur le MCN, il s'agit d'une route de sous-réseau hôte qui réside sur le site DC. 172.16.10.0/24 réside dans le LAN DC et 192.168.15.1 est la Gateway sur le LAN qui est le prochain saut qui arrivera à ce sous-réseau.
- Route 1 —Il s'agit d'un itinéraire local vers ce périphérique SD-WAN qui affiche la table de routage.
- Route 2—4 : il s'agit des sous-réseaux qui font partie des interfaces virtuelles configurées pour le SD-WAN du site DC. Ces sous-réseaux sont dérivés des interfaces virtuelles approuvées définies.
- Route 5 —Il s'agit d'un itinéraire partagé vers un autre nœud client partagé par le MCN avec le statut d'accessibilité Non en raison du chemin virtuel en panne entre ce site et le MCN.
- Route 6—9 —Ces routes existent sur un autre site client. Pour cet itinéraire, un itinéraire Virtual Path est créé pour le trafic d'entrée WAN correspondant destiné au site distant sur le chemin virtuel.
- Route 10 —Avec le service Internet défini, le système ajoute un catch all route pour le breakout internet direct pour ce site local.
- Route 11 —Passthrough est la route par défaut que le système ajoute toujours pour permettre aux paquets de circuler dans le cas où il n'y aurait pas de correspondance sur les routes exis-

tantes. Le Passthrough n'est pas soigné, généralement les émissions locales et le trafic ARP sont mappés à ce service.

- Route 12 —La défausse est la route par défaut que le système ajoute toujours pour supprimer tout ce qui n'est pas défini.

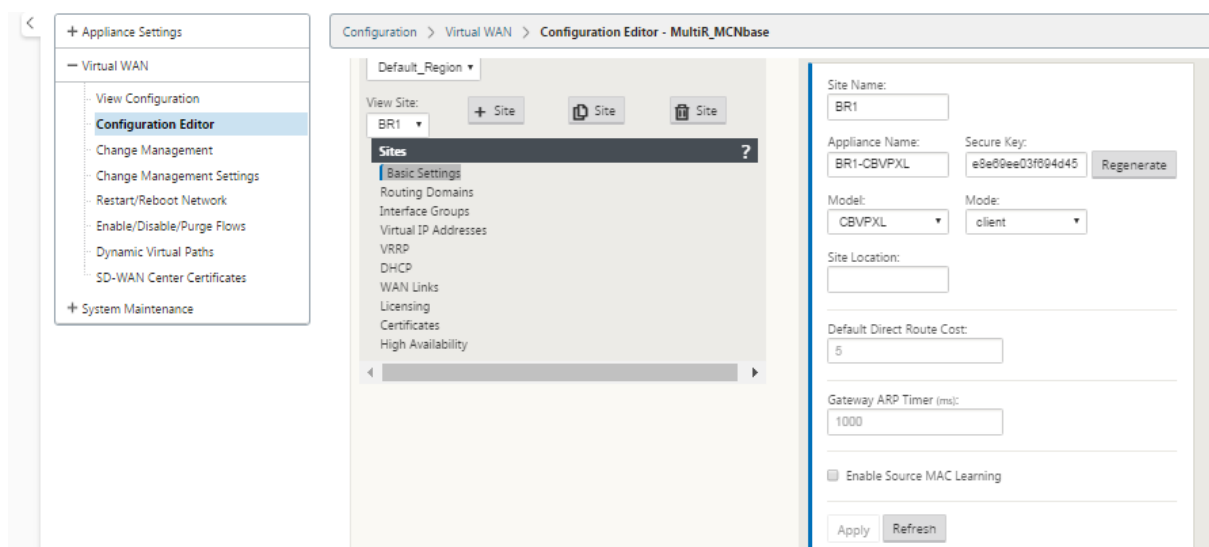
Valeurs de coût d'acheminement par défaut :

- Transfert WAN vers WAN —10
- Coût d'itinéraire direct par défaut —5
- Itinéraires générés automatiquement —5
- Chemin virtuel —5
- Local —5
- Intranet —5
- Internet —5
- Passthrough —5
- Facultatif —l'itinéraire est 0.0.0.0/0 défini comme un niveau de service

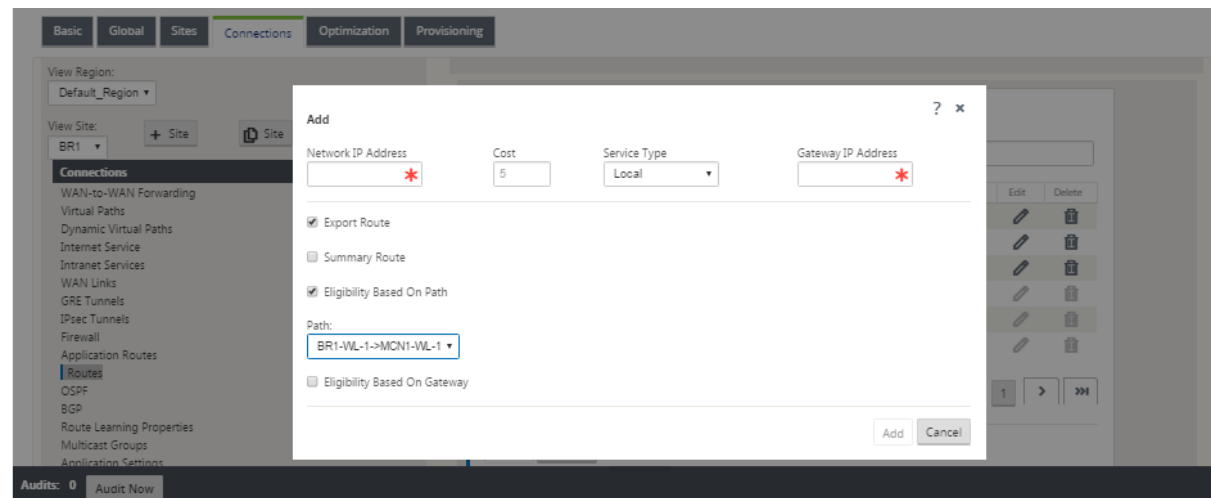
Après avoir défini ces itinéraires, il est important de comprendre comment le trafic circule en utilisant les itinéraires définis. Ces flux de trafic sont répartis entre les flux suivants :

- LAN to WAN (Virtual Path) —Trafic entrant dans le tunnel de superposition SD-WAN
- WAN to LAN (Virtual Path) —Trafic existant dans le tunnel de superposition SD-WAN
- Trafic de chemin non virtuel —Trafic acheminé vers le réseau de sous-couche

Le coût d'itinéraire par défaut peut être modifié par site. La configuration se trouve sous **Afficher le site > Paramètres de base** :



Les itinéraires statiques peuvent être définis par site sous le nœud **Connexions > Site > Routes** :



Vous remarquez que les routes peuvent être liées au chemin virtuel ou à la disponibilité IP de la passerelle. Les routes Internet peuvent être exportées vers la superposition Virtual Path ou non selon le comportement souhaité. Vous pouvez également créer des routes statiques Virtual Path pour forcer le trafic à un Path Virtuel même si nous n’obtenons pas le préfixe annoncé sur SD-WAN (c’est-à-dire une route coûteuse de dernier recours). Le SD-WAN peut également supprimer la publicité des sous-réseaux locaux en rendant l’adresse IP virtuelle (VIP) privée.

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.10.10.10/24	E1Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Trusted	
172.10.10.11/24	E1Vlan0	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply

Revert

Remarque

La configuration nécessite au moins un VIP non privé dans chaque domaine d’itinéraire.

Itinéraires Intranet et Internet

Pour les types de services Intranet et Internet, l'utilisateur doit avoir défini une liaison WAN SD-WAN pour prendre en charge ces types de services. Il s'agit d'une condition préalable à toute liaison définie pour l'un ou l'autre de ces services. Si la liaison WAN n'est pas définie pour prendre en charge le service Intranet, elle est considérée comme une route locale. Les itinéraires Intranet, Internet et Passthrough ne concernent que le site/appliance pour lequel ils sont configurés.

Lors de la définition d'itinéraires Intranet, Internet ou Passthrough, les considérations de conception suivantes sont les suivantes :

- Le service doit être défini sur le lien WAN (Intranet/Internet —requis)
 - Intranet/Internet doit avoir une Gateway définie pour la liaison WAN
 - pertinent pour le périphérique SD-WAN local
 - Les routes intranet peuvent être apprises via le chemin virtuel, mais le sont à un coût plus élevé
 - Avec Internet Service, il y a automatiquement une route par défaut créée (0.0.0.0/0) pour attraper tous les itinéraires avec un coût maximum
 - Ne supposez pas que Passthrough fonctionne, il doit être testé/vérifié, également tester avec Virtual Path down/désactivé pour vérifier le comportement souhaité
 - Les tables de routage sont statiques, sauf si la fonction d'apprentissage de route est activée
- La limite maximale prise en charge pour plusieurs paramètres de routage est la suivante :
- Domaines de routage maximum : 255
 - Interfaces d'accès maximum par liaison WAN : 64
 - Nombre maximum de voisins BGP par site : 255
 - Superficie maximale OSPF par site : 255
 - Interfaces virtuelles maximales par zone OSPF : 255
 - Filtres d'importation maximum par site : 512
 - Filtres d'exportation maximum par site : 512
 - Stratégies de routage BGP maximales : 255
 - Nombre maximal d'objets de chaîne de communauté BGP : 255

Domaine de routage

May 6, 2021

Citrix SD-WAN permet de segmenter les réseaux pour plus de sécurité et de facilité d'administration à l'aide du domaine de routage. Par exemple, vous pouvez séparer le trafic réseau invité du trafic employé, créer des domaines de routage distincts pour segmenter les grands réseaux d'entreprise et segmenter le trafic pour prendre en charge plusieurs réseaux clients. Chaque domaine de routage possède sa propre table de routage et permet la prise en charge des sous-réseaux IP superposés.

Les appliances Citrix SD-WAN implémentent les protocoles de routage OSPF et BGP pour que les domaines de routage contrôlent et segmentent le trafic réseau.

Un chemin virtuel peut communiquer à l'aide de tous les domaines de routage, quelle que soit la définition du point d'accès. Ceci est possible car l'encapsulation SD-WAN inclut les informations de domaine de routage pour le paquet. Par conséquent, les deux réseaux finaux savent à quoi appartient le paquet. Il n'est pas nécessaire de créer un lien WAN ou une interface d'accès pour chaque domaine de routage.

Voici la liste des points à prendre en compte lors de la configuration de la fonctionnalité Domaine de routage :

- Par défaut, les domaines de routage sont activés sur un MCN.
- Les domaines de routage sont activés sur les sites de succursale.
- Chaque domaine de routage activé doit être associé à une interface virtuelle et à une adresse IP virtuelle.
- La sélection de routage fait partie de toutes les configurations suivantes :
 - Groupe d'interface
 - Adresse IP virtuelle
 - GRE
 - Lien WAN -> Interface d'accès
 - Tunnels IPSec
 - Itinéraires
 - Règle
- Les domaines de routage sont exposés dans la configuration de l'interface Web uniquement lorsque plusieurs domaines sont créés.
- Pour un lien Internet public, une seule interface d'accès principale et secondaire peut être créée.
- Pour un lien Intranet/MPLS privé, une interface d'accès principale et secondaire peut être créée par domaine de routage.

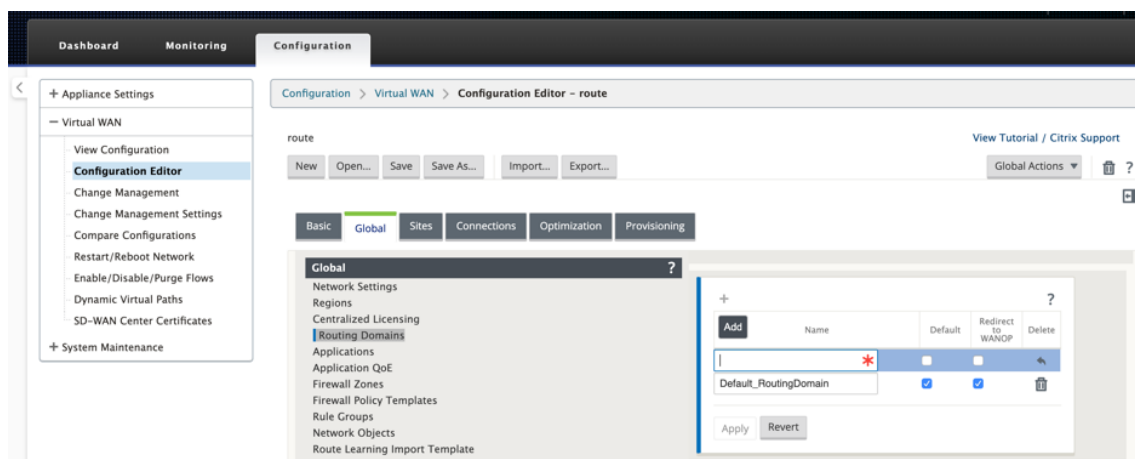
Configurer le domaine de routage

May 6, 2021

Les appliances Citrix SD-WAN permettent de configurer des protocoles de routage fournissant un point d'administration unique pour gérer un réseau d'entreprise, un réseau de succursales ou un réseau de datacenter. Vous pouvez configurer jusqu'à 254 domaines de routage.

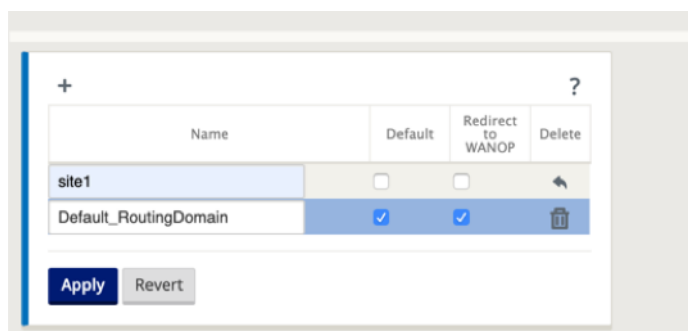
Pour configurer le domaine de routage :

1. Dans l'interface Web SD-WAN, accédez à **Configuration > Réseau étendu virtuel > Éditeur de configuration** . Dans l'**Éditeur de configuration**, accédez à **Global > Domaines de routage**, cliquez sur **Ajouter (+)** et entrez un nom pour votre nouveau domaine de routage.

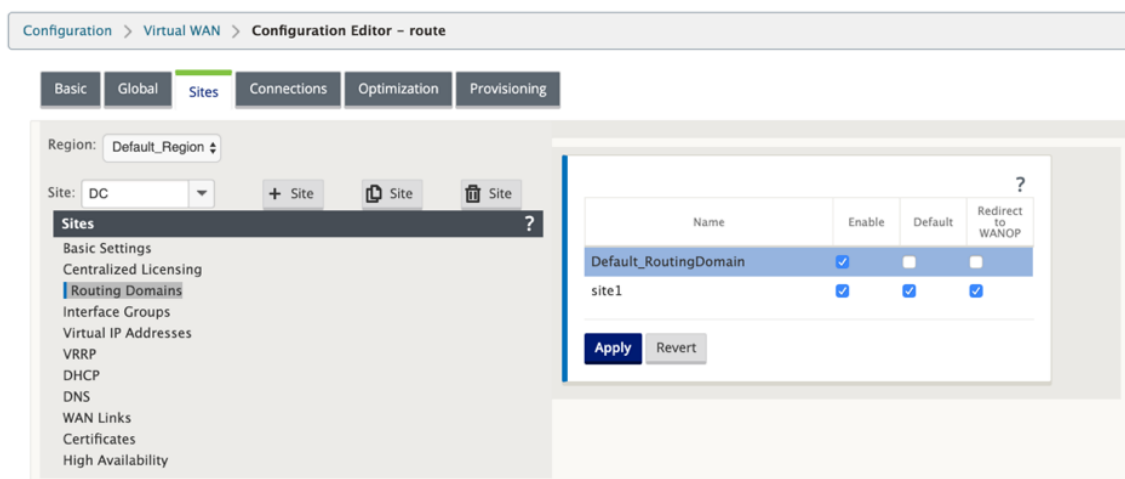


2. Si vous souhaitez utiliser par défaut ce domaine de routage, activez la case à cocher **Par défaut**. Cliquez sur **Appliquer** pour enregistrer les modifications. Si vous prévoyez d'implémenter un seul domaine de routage, aucune configuration explicite n'est requise.

Toutes les nouvelles configurations sont automatiquement renseignées avec un domaine de routage par défaut.



3. Accédez à **Sites** → **[Nom du site client]** > **Domaines de routage**. Cochez la case **Activer** pour activer un domaine de routage configuré pour le site.
4. Activez la case à cocher **Par défaut** pour faire de ce domaine de routage la valeur par défaut du site. Cliquez sur **Appliquer** pour enregistrer les modifications.



Remarque

La désactivation de l'option **Activer** pour un domaine de routage rend celui-ci indisponible pour une utilisation sur le site.

Avec la version 11.0.2, **les domaines de routage sans IP virtuelles (VIP) routables** sont autorisés avec les fonctionnalités suivantes :

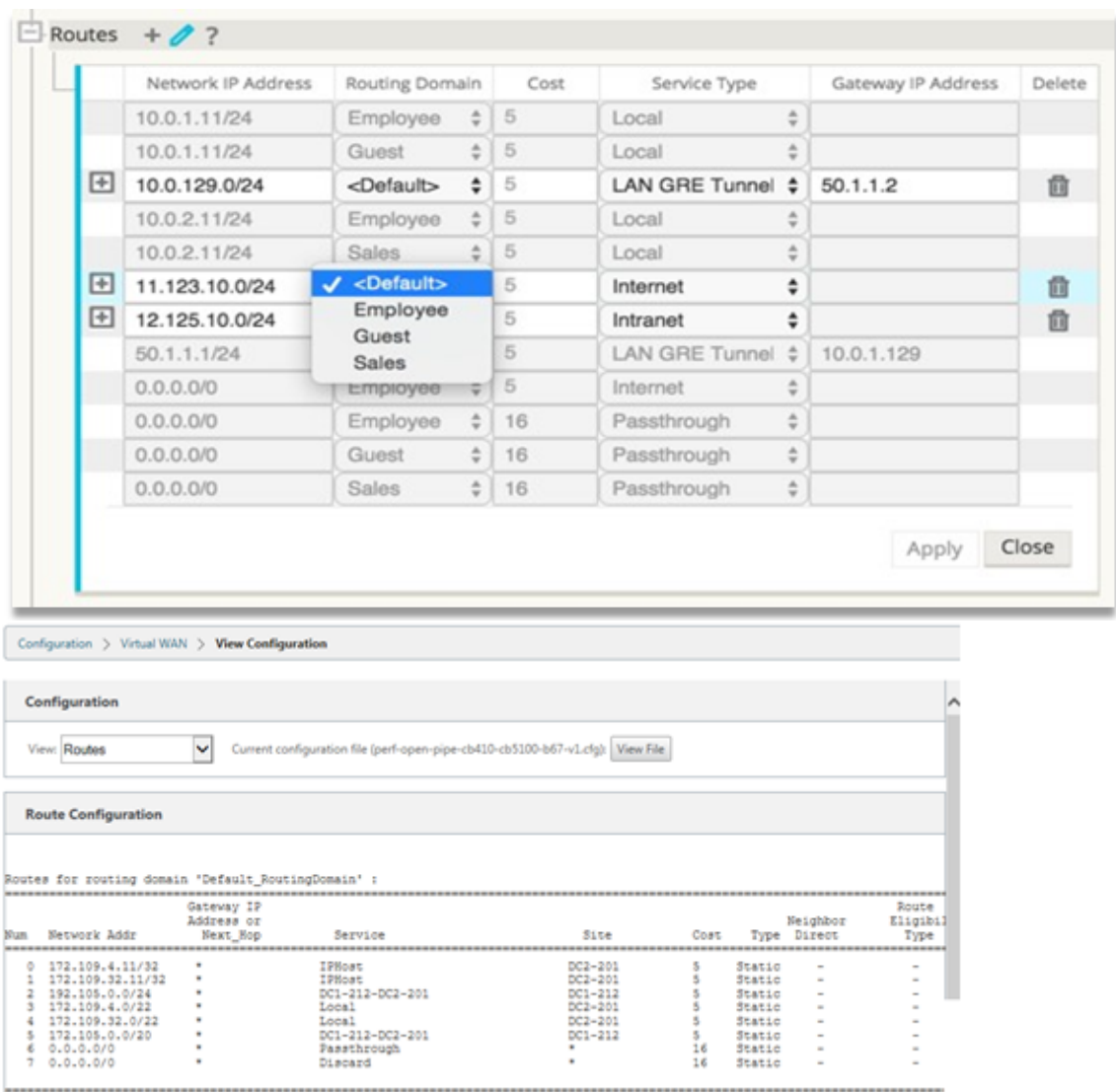
- Autoriser un périphérique à disposer d'un domaine de routage pour des interfaces non approuvées ou sans interface.
- Autoriser les succursales à communiquer entre elles via un domaine de routage qui n'a pas de présence physique sur un site intermédiaire.

Configurer les itinéraires

May 6, 2021

Pour configurer des itinéraires :

1. Dans l'**Éditeur de configuration**, accédez à **Connexions** > **[Nom du site]** > **Itinéraires**.
2. Choisissez un **domaine de routage** dans le menu déroulant. Les nouvelles routes sont automatiquement associées au domaine de routage par défaut. Pour obtenir des instructions détaillées, reportez-vous à la section [configuration des itinéraires](#).



Après avoir configuré des itinéraires, validez les tables de routage pour le domaine de routage configuré en accédant à **Configuration > Réseau étendu virtuel > Affichage > Itinéraires**.

Utiliser l'interface de ligne de commande pour accéder au routage

May 6, 2021

Dans Citrix SD-WAN version 10.0, vous pouvez afficher des informations supplémentaires relatives au routage dynamique et à l'état du protocole. Tapez la commande et la syntaxe suivantes pour accéder au démon de routage et afficher la liste des commandes.

```
1 dynamic_routing?
```

Routage dynamique

November 1, 2021

Les deux protocoles de routage dynamique suivants sont pris en charge par Citrix SD-WAN :

- Ouvrir le chemin le plus court en premier (OSPF)
- Protocole Border Gateway (BGP)

Avant la version 11.3.1 de Citrix SD-WAN, les fonctionnalités de routage dynamique étaient disponibles uniquement pour un seul ID de routeur. Vous pouvez configurer un ID de routeur unique globalement pour l'ensemble du protocole (un pour OSPF et BGP) ou fournir aucun ID de routeur. Si aucun ID de routeur n'est fourni, l'adresse IP la plus basse des instances de réseau virtuel (VNI) participant au routage dynamique est automatiquement sélectionnée comme ID de routeur par défaut.

À partir de la version 11.3.1 de Citrix SD-WAN, vous pouvez non seulement configurer un ID de routeur pour l'ensemble du protocole, mais également configurer un ID de routeur pour chaque domaine de routage. Avec cette amélioration, vous pouvez activer le routage dynamique stable sur plusieurs instances avec différents ID de routeur convergeant de manière stable.

Si vous configurez un ID de routeur pour un domaine de routage spécifique, l'ID de routeur spécifique remplace le domaine de routage au niveau du protocole.

Remarque :

Les ID de routeur dynamique ne sont pas configurables sur les appliances SD-WAN suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

OSPF

OSPF est un protocole de routage développé pour les réseaux IP (Internet Protocol) par le groupe Interior Gateway Protocol (IGP) de l'Internet Engineering Task Force (IETF). Il inclut la première version du protocole de routage IS-IS (Intermediate System to Intermediate System) d'OSI.

Le protocole OSPF est ouvert, ce qui signifie que sa spécification est dans le domaine public (RFC 1247). OSPF est basé sur l'algorithme SPF (Shortest Path First) appelé Dijkstra. Il s'agit d'un protocole de routage d'état de liaison qui appelle à envoyer des annonces d'état de liaison (LSA) à tous les autres routeurs dans la même zone hiérarchique. Les informations sur les interfaces attachées, les mesures utilisées et d'autres variables sont incluses dans les LSA OSPF. Les routeurs OSPF accumulent des

informations sur l'état de liaison, qui sont utilisées par l'algorithme SPF pour calculer le chemin le plus court vers chaque nœud.

Vous pouvez désormais configurer les appliances Citrix SD-WAN (Éditions Standard et Premium (Enterprise)) pour apprendre les itinéraires et annoncer les itinéraires à l'aide d'OSPF.

Remarque

- Les appliances Citrix SD-WAN ne participent pas en tant que routeur désigné (DR) et BDR (routeur désigné de sauvegarde) sur chaque réseau multi-accès, car la priorité de reprise après sinistre par défaut est définie sur « 0 ».
- L'appliance Citrix SD-WAN ne prend pas en charge la synthèse en tant que routeur de bordure de zone (ABR).

Configurer OSPF

Pour configurer OSPF :

1. Dans l'**éditeur de configuration**, accédez à **Connexions > Région > Site > OSPF > Paramètres de base**.
2. Cliquez sur **Activer**, sélectionnez ou saisissez des valeurs pour les paramètres suivants, puis cliquez sur **Appliquer**.
 - **Publicité des routes Citrix SD-WAN** : autorise la publication des routes Citrix SD-WAN via OSPF. Vous pouvez également spécifier une balise pour la redistribution OSPF.
 - **Publicité des routes BGP** : autorise la publication des routes apprises par des homologues BGP via OSPF. Vous pouvez également spécifier une balise pour la redistribution OSPF.
 - **ID du routeur** : Identifiant unique du routeur, le routeur est utilisé pour les publicités OSPF. Si l'ID de routeur n'est pas spécifié, il est automatiquement sélectionné comme adresse IP virtuelle la plus basse hébergée dans le réseau SD-WAN.
 - **Exporter le type de route OSPF** : annoncez les routes Citrix SD-WAN aux homologues OSPF en tant qu'itinéraires intra-zone ou routes externes.
 - **Exporter le poids de routage OSPF** : Lorsque vous exportez des routes Citrix SD-WAN vers OSPF, ajoutez ce poids au coût Citrix SD-WAN de chaque itinéraire.
 - **Préférence de protocole** : si les préfixes sont appris via plusieurs protocoles de routage, la valeur de préférence de protocole détermine la sélection du protocole de routage. Pour plus d'informations, consultez la section [Préférence de protocole](#).

Region: Default_Region

Site: [Dropdown] + Site [Icon] Site [Icon]

Connections

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall
- Application Routes
- Routes
- OSPF**
- BGP
- Route Learning Properties
- Multicast Groups
- Applications

Section: Basic Settings

☒ Enable

☒ Advertise Citrix SD-WAN Routes Tag Value: 10

☒ Advertise BGP Routes Tag Value: 20

Router ID: 5.5.5.5

Export OSPF Route Type: Type 5 AS Extern

Export OSPF Route Weight: 4

Protocol Preference: 150

Apply Revert

3. Développez **OSPF** -> **Zone**, puis cliquez sur **Modifier**.

Section: Areas

+ [Icon] ID Stub Area Delete [Icon]

Name	Source IP Address	Interface Cost	Authentication Type	Password	Network Type	Hello Interval	Dead Interval	Delete
VirtualInterface	172.111.64.5	10	None		Auto	10	40	[Icon]

Apply Revert

- Entrez un **ID de zone** pour apprendre les itinéraires et faire de la publicité vers.
- Si l'identité n'est pas vérifiée pour une adresse IP virtuelle spécifique, l'interface virtuelle associée n'est pas disponible pour les services IP.
- Choisissez l'une des interfaces virtuelles disponibles dans le menu **Nom**. L'interface virtuelle détermine l'**adresse IP source**.
- Entrez le **coût de l'interface** (10 est la valeur par défaut).
- Choisissez un **type d'authentification** dans le menu.
- Si vous avez choisi **Mot de passe** ou **MD5** à l'étape 8, entrez le champ de texte associé au mot de passe.

10. Dans le champ **Hello Intervalle**, entrez le temps d'attente entre l'envoi de paquets de protocole Hello aux voisins directement connectés (10 secondes est la valeur par défaut).
11. Dans le champ **Intervalle mort**, saisissez l'intervalle d'attente avant de marquer un routeur comme mort. L'intervalle mort par défaut est de 40 secondes.
12. Cliquez sur **Appliquer** pour enregistrer vos modifications.

Zone de talon

Les zones stub sont protégées des routes externes et reçoivent des informations sur les réseaux appartenant à d'autres zones du même domaine OSPF.

Activez la case à cocher **Zone de stub**.

Section: Areas

ID	Stub Area	Delete
VirtualInterface-1	<input checked="" type="checkbox"/>	

Virtual Interfaces +

Name	Source IP Address	Interface Cost	Authentication Type	Password	Network Type	Hello Interval	Dead Interval	Delete
VirtualInterface-1	172.111.64.5	10	None		Auto	10	40	

Apply Revert

If enabled, the Area will avoid flooding external routes

Balises de redistribution OSPF

Vous pouvez utiliser des balises OSPF pour empêcher les boucles de routage lors de la redistribution mutuelle entre OSPF et d'autres protocoles. Dans le domaine OSPF, s'il existe des routes SD-WAN et BGP apprises vers le même sous-réseau, le mécanisme de prévention de boucle OSPF l'identifie comme une boucle et ignore les routes. La spécification de différentes balises pour les itinéraires appris SD-WAN et BGP permet d'installer ces routes dans la table de routage OSPF.

Vous pouvez configurer les balises de redistribution OSPF pour les itinéraires appris via SD-WAN et BGP dans la section OSPF, **Paramètres de base**.

Section: Basic Settings ▾

☒ Enable ?

☒ Advertise Citrix SD-WAN Routes Tag Value: 10

☒ Advertise BGP Routes Tag Value: 20

Router ID:
5.5.5.5

Export OSPF Route Type:
Type 5 AS Exterr ▾

Export OSPF Route Weight:
4

Protocol Preference:
150

Apply Revert

BGP

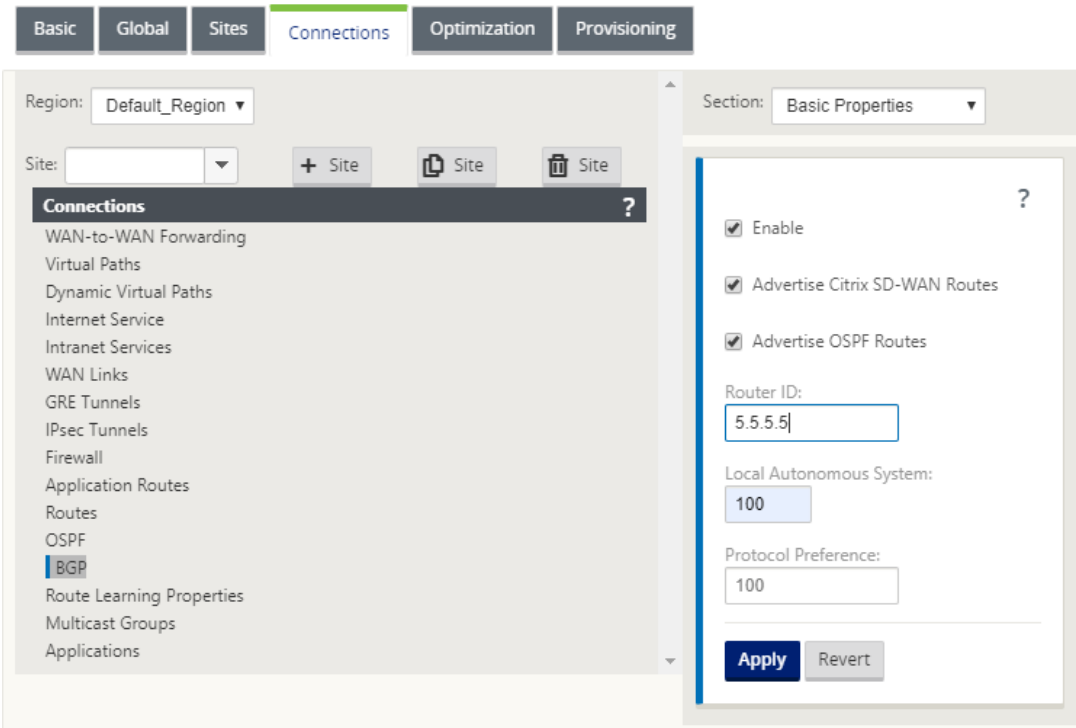
BGP est un protocole de routage système interautonome. Un réseau autonome ou un groupe de réseaux est géré sous une administration commune et avec des règles de routage communes. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les FAI. Les réseaux clients déploient des protocoles de Gateway Interior tels que RIP ou OSPF pour l'échange d'informations de routage au sein de leurs réseaux. Les clients se connectent aux FAI, et les FAI utilisent BGP pour échanger des itinéraires clients et FAI. Lorsque BGP est utilisé entre les systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routes au sein d'un AS, le protocole est appelé Interior BGP (IBGP).

BGP est un protocole de routage robuste et évolutif déployé sur Internet. Pour atteindre l'évolutivité, BGP utilise de nombreux paramètres de routage appelés attributs pour définir des stratégies de routage et maintenir un environnement de routage stable. Les voisins BGP échangent des informations de routage complètes lorsque la connexion TCP entre voisins est établie pour la première fois. Lorsque les modifications apportées à la table de routage sont détectées, les routeurs BGP envoient à leurs voisins uniquement les routes qui ont été modifiées. Les routeurs BGP n'envoient pas de mises à jour périodiques de routage et n'annoncent que le chemin optimal vers un réseau de destination. Vous pouvez configurer les appliances Citrix SD-WAN pour apprendre les itinéraires et annoncer des itinéraires à l'aide de BGP.

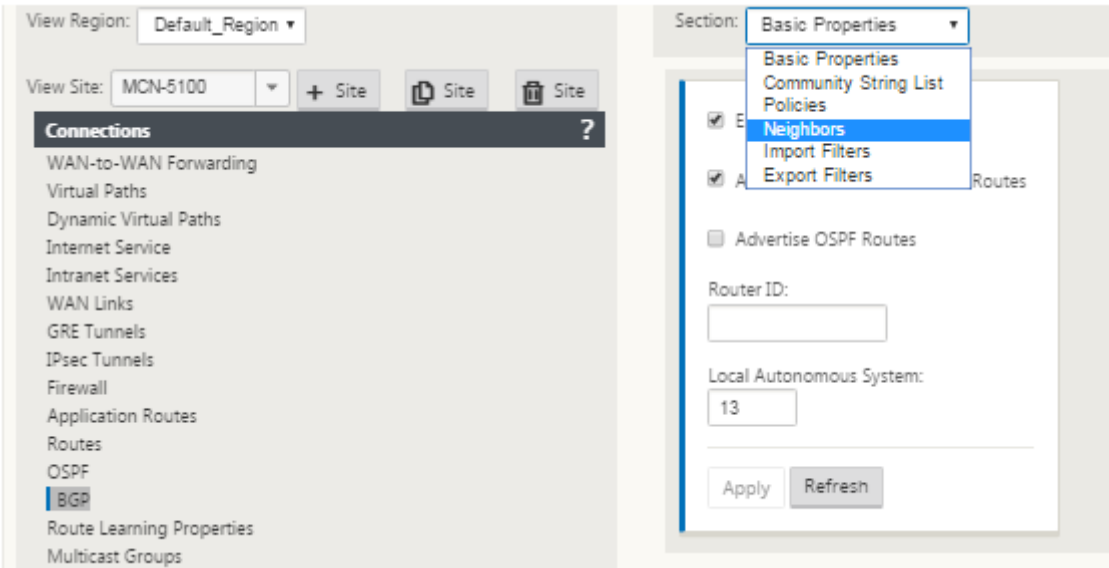
Configurer BGP

Pour configurer BGP :

1. Dans l'**éditeur de configuration**, accédez à **Connexions > Région > Site > BGP > Paramètres de base**.
2. Cliquez sur **Activer**, sélectionnez ou saisissez des valeurs pour les paramètres suivants, puis cliquez sur **Appliquer**.
 - **Publicité des routes Citrix SD-WAN** : autorise la publication des routes Citrix SD-WAN via BGP.
 - **Publicité des routes OSPF** : autorise la publication des routes apprises par des homologues OSPF via BGP.
 - **ID du routeur** : Identifiant unique du routeur, le routeur est utilisé pour les publicités OSPF. Si l'ID de routeur n'est pas spécifié, il est automatiquement sélectionné comme adresse IP virtuelle la plus basse hébergée dans le réseau SD-WAN.
 - **Système autonome local** : Numéro du système autonome local à partir duquel les itinéraires sont appris et annoncés. Le numéro de système autonome doit correspondre à celui des routeurs voisins.
 - **Préférence de protocole** : si les préfixes sont appris via plusieurs protocoles de routage, la valeur de préférence de protocole détermine la sélection du protocole de routage. Pour plus d'informations, consultez la section [Préférence de protocole](#).



3. Développez **Paramètres de base > Voisins** et cliquez sur l'icône **Ajouter (+)** .



Section: Neighbors

	Virtual Interface	Source IP	Neighbor IP	Neighbor AS	Hold Time(s)	Local Preference	BGP Metric	Multi Hop	Password	Delete
	VirtualInterface-	172.111.64.5		13	180	100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Policies +

Order	Network Address	BGP Community(AA:NN)	AS Path	BGP Policy	Direction	Delete
-------	-----------------	----------------------	---------	------------	-----------	--------

Apply Revert

Pour les sites avec plusieurs domaines de routage, choisissez un domaine de routage. Le domaine de routage détermine les interfaces virtuelles disponibles.

4. Choisissez une **interface virtuelle** dans le menu. L'interface virtuelle détermine l'adresse IP source.
5. Entrez l'**adresse IP** du routeur voisin IBGP dans le champ IP du voisin et le numéro **du système autonome local** dans le champ Voisin AS.
6. Dans le champ **Temps d'attente (s)**, saisissez le temps d'attente, en secondes, à attendre avant de déclarer un voisin en panne (la valeur par défaut est 180).
7. Dans le champ **Préférence (s) locale (s)**, entrez la valeur Préférence locale, en secondes, qui est utilisée pour la sélection à partir de plusieurs itinéraires BGP (la valeur par défaut est 100).
8. Cochez la case **Mesure IGP** pour activer la comparaison des distances internes afin de calculer le meilleur itinéraire.
9. Cochez la case **Multi-saut** pour activer plusieurs sauts pour l'itinéraire.
10. Dans le champ **Mot de passe**, entrez un mot de passe pour l'authentification MD5 des sessions BGP (l'authentification n'est pas requise).

Remarque

La configuration des réflecteurs d'itinéraire et des confédérations pour iBGP n'est pas prise en charge dans le réseau SD-WAN.

BGP extérieur (eBGP)

Les appliances Citrix SD-WAN se connectent à un commutateur côté LAN et à un routeur côté WAN. À mesure que la technologie SD-WAN devient de plus en plus intégrée aux déploiements réseau d'entreprise, les appliances SD-WAN remplacent les routeurs. SD-WAN implémente le protocole de routage dynamique eBGP pour fonctionner comme un périphérique de routage dédié.

L'apppliance SD-WAN établit un voisinage avec des routeurs homologues utilisant eBGP vers le côté WAN et est capable d'apprendre, de publier des itinéraires depuis et vers les pairs. Vous pouvez sélectionner l'importation et l'exportation des routes apprises eBGP sur des périphériques homologues. En outre, les itinéraires statiques SD-WAN et virtuels appris par chemin d'accès peuvent être configurés pour faire de la publicité auprès de pairs eBGP.

Pour plus d'informations, consultez les cas d'utilisation suivants :

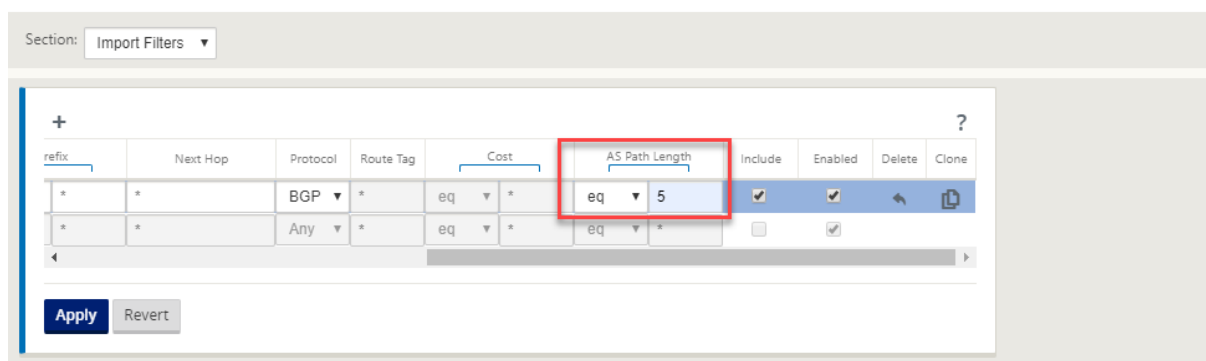
- [Site SD-WAN Communication avec un site non-SD-WAN sur eBGP](#)
- [Communication entre les sites SD-WAN à l'aide du chemin virtuel et de l'eBGP](#)
- [Implémentation d'OSPF dans une topologie à bras unique](#)
- [Déploiement OSPF Type5 vers Type1 dans le réseau MPLS](#)
- [Déploiement OSPF d'une appliance SD-WAN et non SD-WAN \(tierce partie\)](#)
- [Mise en œuvre d'OSPF à l'aide d'un réseau SD-WAN avec configuration haute disponibilité](#)

Longueur du chemin AS

Le protocole BGP utilise l'attribut de **longueur de chemin AS** pour déterminer le meilleur itinéraire. La longueur du chemin AS indique le nombre de systèmes autonomes traversés dans un itinéraire. Citrix SD-WAN utilise l'attribut de **longueur de chemin BGP AS** pour filtrer et importer des itinéraires.

Les appliances non SD-WAN peuvent choisir d'acheminer le trafic vers des appliances SD-WAN DC principal ou DC secondaire en important des itinéraires en fonction de leur longueur de chemin AS. Vous pouvez également diriger dynamiquement le trafic d'un routeur vers le contrôleur de domaine secondaire en augmentant simplement la longueur du chemin AS du dispositif de contrôleur de domaine principal sur le routeur, ce qui le rend non préférable. Suppression de la nécessité de modifier le coût de l'itinéraire et d'effectuer une mise à jour de la configuration.

Pour configurer la longueur du chemin AS dans les filtres d'importation, sélectionnez BGP comme protocole, sélectionnez un prédicat et saisissez la **longueur du chemin AS**. Pour plus d'informations, consultez la section [Filtrage des itinéraires](#)



Surveiller les statistiques d'itinéraire

Accédez à **Moniteur** > **Statistiques**. Sélectionnez **Itinéraires** dans le menu déroulant **Afficher**.

Toutes les fonctions des Routes applicables sont prises en charge dans le réseau Citrix SD-WAN, qu'une route soit dynamique ou statique.

Monitoring > Statistics

Statistics

Show: **Routes** ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 28 of 28 entries

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	115.1.1.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
1	115.168.0.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
2	115.168.0.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
3	115.168.0.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
4	115.168.0.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
5	115.168.0.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	115.14.14.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	115.13.13.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	115.12.12.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	115.10.10.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
10	115.9.9.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
11	115.8.8.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
12	115.7.7.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
13	115.6.6.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
14	115.5.5.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
15	115.4.4.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
16	115.3.3.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
17	115.2.2.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
18	182.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
19	172.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
20	182.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
21	172.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
22	182.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
23	172.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
24	192.120.1.0/24	172.120.1.2	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	75612	YES	N/A	N/A
25	192.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Dynamic	Virtual WAN	YES	6	75612	YES	N/A	N/A
26	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
27	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 28 of 28 entries

OSPF

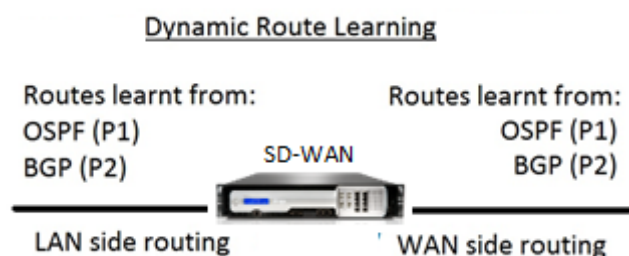
May 6, 2021

Côté LAN : Apprentissage dynamique des itinéraires

OSPF s'exécutant sur le port LAN de l'appliance Citrix SD-WAN déployée en mode passerelle :

Les appliances Citrix SD-WAN effectuent la découverte d'itinéraires des annonces de routage de couche 3 au sein d'un réseau client local (succursale et centre de données) pour chacun des protocoles de routage souhaités (OSPF et BGP). Les routes qui sont apprises sont capturées et affichées dynamiquement.

Cela élimine la nécessité pour les administrateurs SD-WAN de définir statiquement l'environnement de mise en réseau côté LAN pour chaque appliance faisant partie du réseau SD-WAN.



Côté WAN : Partage dynamique d'itinéraires

Appliance Citrix SD-WAN ayant une AREA définie comme une zone STUB en limitant l'apprentissage de type 5 AS-externe LSA.

Les appliances Citrix SD-WAN peuvent annoncer les routes dynamiques apprises localement avec le MCN. Le MCN peut ensuite relayer ces routes vers d'autres appliances SD-WAN du réseau. Cet échange d'informations permet de maintenir dynamiquement la connectivité entre les sites à travers le réseau en évolution.

Modes de déploiement OSPF

Dans les versions précédentes, les routes apprises d'instance OSPF à partir de SD-WAN étaient traitées comme des routes externes avec LSA de type 5 uniquement. Ces routes ont été annoncées à ses routeurs voisins dans la LSA externe de type 5. Il en résulte que les routes SD-WAN sont moins préférées selon l'algorithme de sélection des chemins OSPF.

Avec la dernière version, SD-WAN peut désormais annoncer des routes en tant que routes intra-zone (LSA Type 1) afin d'obtenir une préférence en fonction de son coût d'itinéraire à l'aide de l'algorithme de sélection de chemin OSPF. Le coût de l'itinéraire peut être configuré et annoncé au routeur voisin. Cela permet de déployer l'apppliance SD-WAN dans un mode à bras unique décrit ci-dessous.

Implémentation d'OSPF dans la topologie à bras unique

Dans la configuration à un bras, le routeur a besoin d'une configuration complexe PBR ou WCCP dans les déploiements OSPF. En changeant le type de route d'exportation par défaut de Type 5 à Type 1, nous pouvons simplifier ce déploiement. Si les itinéraires SD-WAN sont annoncés comme des itinéraires intra-zone à moindre coût et que l'apppliance SD-WAN devient active, le routeur voisin sélectionne les itinéraires SD-WAN et commence automatiquement à transférer le trafic via le réseau SD-WAN. Une configuration PBR ou WCCP supplémentaire n'est plus requise.

Conditions préalables :

- Les appliances SD-WAN sur les sites de contrôleur de domaine et de succursale doivent exécuter la dernière version.
- La connectivité IP de bout en bout doit être configurée et fonctionner correctement.
- OSPF est activé sur tous les sites.

Pour configurer OSPF Type 1 :

1. Configurez **les interfaces virtuelles** et les **liens WAN** sur les sites DC et Branche afin que vous puissiez créer le chemin virtuel entre eux.
2. Sous **Connexions** > [MCN] > > **Apprentissage de l'itinéraire** > **OSPF** -> **Paramètres de base**, sélectionnez **Exporter le type d'itinéraire OSPF** pour être **Type 1 Intra Area**.
3. Enregistrez la configuration, le stage et activez la configuration.

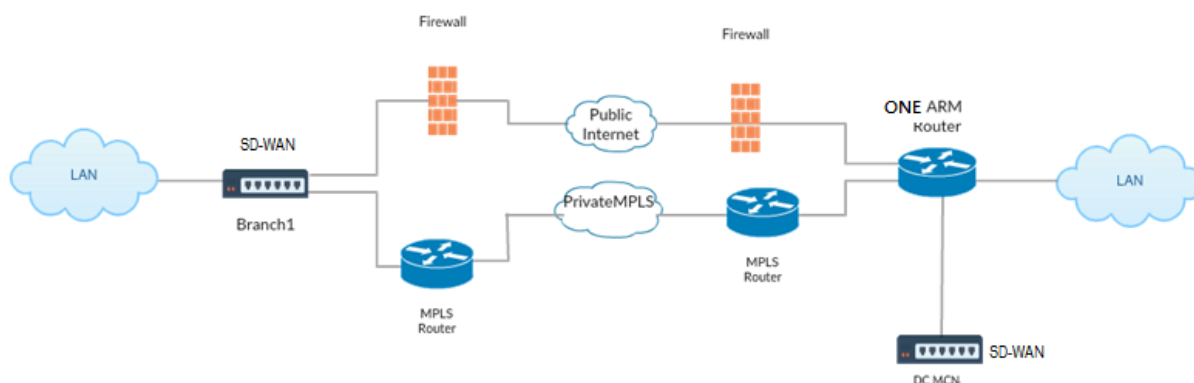
Vous devez être en mesure de voir les types d'itinéraire suivants sous

Exporter le type d'itinéraire OSPF

- Type 5 AS External
- Type 1 Intra Area

Vous devez être en mesure de configurer **Type 5 AS Route externe**.

Après l'activation de la configuration modifiée, vous devez voir les changements de type d'itinéraire sous **Configuration** > **Réseau étendu virtuel** > **View Configuration** > **Routage dynamique**.

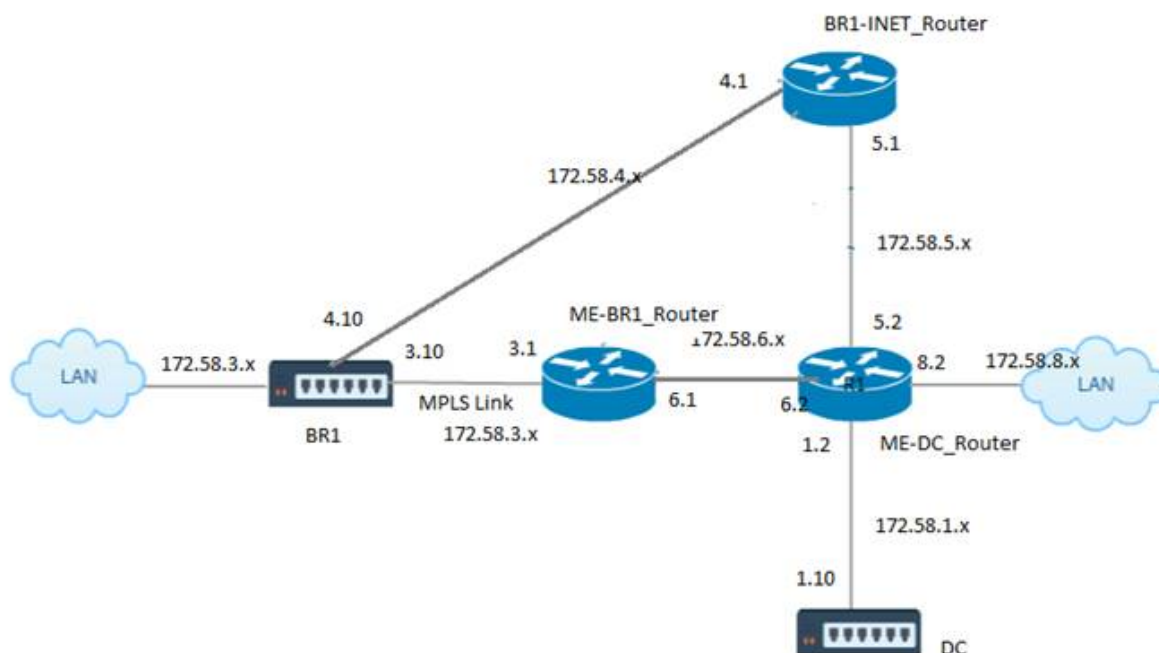


Comme le montre l'illustration ci-dessus, le MCN DC est déployé en topologie à bras unique. Lorsque le site DC est actif, le routeur à bras unique transfère tout le trafic du réseau local vers d'autres sites, tels que le réseau local de la succursale dont l'adresse IP de destination se trouve dans le même sous-réseau vers le SD-WAN, puis l'apppliance SD-WAN encapsule tous les paquets et l'envoie au routeur avec tous les paquets IP de destination dans l'adresse IP virtuelle de la branche. Le routeur transmet ensuite ces paquets au WAN.

Lorsque le site DC est en panne, le routeur transfère tout le trafic du LAN local vers d'autres sites (LAN local du site de succursale, IP de destination se trouve dans le sous-réseau) directement vers le WAN, et non vers l'apppliance SD-WAN.

Déploiement OSPF Type5 à Type1 dans le réseau MPLS

Le mode de déploiement suivant est fourni pour éviter la formation de boucle dans un réseau MPLS configuré à l'aide d'appiances SD-WAN. L'illustration ci-dessous décrit l'implémentation du réseau MPLS standard.



Dans l'illustration ci-dessus :

- OSPF est configuré entre *ME-BR1_Router* et *ME-DC_Router* dans la zone 0.
- OSPF est configuré entre *ME-DC_Router* et *DC* dans la zone 0.

Configuration recommandée :

- DC VW et *ME-DC_Router* sur la zone 0
- *ME-BR1_Router* et *ME-DC_Router* sur la zone 0
- BR1 VW et *ME-BR1_Router* sur la zone 0

Sur le *ME-DC_Router* :

1. Ajouter, route statique pour 172.58.3.10/32 (IP Virtuelle de BR1 pour MPLS Link) à 172.58.6.1
2. Ajouter, route statique pour 172.58.4.10/32 (IP Virtuelle de BR1 pour INET) à 172.58.5.1

L'ajout de routes statiques empêche la formation de boucle entre le routeur *ME-DC_routeur* et le dispositif SD-WAN DC. Si vous n'ajoutez pas de routes statiques, le MCN transfère le trafic vers le routeur *ME-DC*, puis le routeur vers le MCN, ce qui crée une boucle en continu.

Les routes statiques qui ne sont pas des routes PBR mais les routes basées sur IP hôte de destination traversent vers le lien de droite à choisir du côté DC en fonction du chemin choisi et de l'encapsulation effectuée par la suite. Par conséquent, avec ces routes statiques configurées, les paquets encapsulés avec une adresse IP virtuelle de destination de l'appliance SD-WAN BR1 utiliseraient ces liens selon le meilleur chemin sélectionné par le MCN DC.

Ajoutez ACL pour éviter la formation de boucle lorsque les routes IPHOST sont installées (si aucune IP virtuelle statique n'est configurée) :

- Si les routes IPHOST annoncées par l'apppliance SD-WAN BR1 sont installées par le routeur MCN *ME-DC_Router* et non ajoutées en tant que routes statiques comme mentionné ci-dessus, il est possible de formation de boucle si l'interface participante OSPF (172.58.6.x) entre ME-BR1_router et Me-DC_router tombe en panne. En effet, avec cette interface désactivée, les routes IPHOST sont vides de la table de routage de ME-DC_router.
- Si cela se produit, MCN transmet le paquet encapsulé destiné à l'un des VIP BR1 au routeur ME-DC et le retourne du routeur au MCN et boucle en continu.

Sur le routeur ME-BR1_routeur :

Annoncez le réseau 172.58.3.x sur le Me-DC_Router avec un coût plus élevé que le coût annoncé pour le même réseau par DC, si le même AREA-ID est utilisé entre le routeur **ME-BR1_routeur <-> ME-DC_routeur** et le **Me-DC_routeur <-> DC (SD-WAN)**.

- Basé sur le calcul des métriques de coût d'OSPF $10^8/BW$ et le coût des préfixes d'itinéraire sont basés sur le type d'interface. Les appliances SD-WAN annoncent le chemin virtuel et les routes statiques spécifiques au WAN virtuel vers les routeurs externes ou homologues avec le coût SD-WAN par défaut de 5.
- Si le routeur ME-BR1 annonce également 172.58.3.0/24 comme une route OSPF de type 1 interne à côté de DC (SD-WAN) qui annonce également le même préfixe qu'une route OSPF Type 1 interne, alors selon le calcul des coûts, la route du routeur ME-BR1 sera configurée, car le coût est inférieur à celui de SD-WAN coût par défaut de 5. Pour éviter cela et faire en sorte que l'apppliance SD-WAN soit initialement choisie comme route préférée, le coût d'interface de (172.58.3.1) doit être manipulé pour le rendre plus élevé sur le routeur ME-BR1 afin que la route SD-WAN DC soit configurée dans la table de routage du routeur ME-DC_routeur.

Cela garantit également qu'en cas de défaillance du dispositif SD-WAN DC, la route alternative permettant d'utiliser ME-BR1_routeur comme Gateway préférée suivante garantit un flux de trafic ininterrompu.

Utilisez ME-DC_Router comme source pour la publicité du réseau 172.58.8.0/24 à la fois DC SD-WAN et ME-BR1_Router :

Avec cette route, le SD-WAN DC peut envoyer des paquets au routeur en amont étant conscient du sous-réseau LAN après décapsulation. Si DC SD-WAN tombe en panne, l'infrastructure de routage héritée aiderait ME-BR1_Router à utiliser le ME-DC_Router comme saut suivant pour atteindre le réseau 172.58.8.x.

Pour configurer les routes exportées OSPF en tant que Type1 sous **Paramètres OSPF de base** :

1. Configurez **les interfaces virtuelles** et les **liens WAN** sur les sites DC et Branche pour créer le chemin virtuel entre eux.
2. Sous **Connexions** > **[MCN]** > **Route Learning** > **OSPF** > **Basic Settings**, sélectionnez **Exporter le type d'itinéraire OSPF** pour être **Type 1 Intra Area**.
3. Enregistrez la configuration, la mise en scène et activez la même chose. Vous devez être en mesure de voir les deux types de route suivants sous **Exporter le type d'itinéraire OSPF** :
 - Type 5 AS External
 - Type 1 Intra Area

Après l'activation de la configuration modifiée, vous pouvez voir les modifications du type d'itinéraire sous **Configuration** > **Réseau étendu virtuel** > **Afficher la configuration** > **Routage dynamique** .

Les itinéraires doivent être annoncés en tant que AS externe de type5 par l'apppliance SD-WAN. Les routes apprises via SD-WAN doivent être affichées dans les routeurs voisins en tant que routes externes de Type5 AS.

Pour configurer le poids de l'itinéraire exporté par OSPF sous **Paramètres OSPF de base** :

1. Configurez les interfaces virtuelles et les liens WAN sur les sites DC et Branch pour créer le chemin virtuel entre eux.
2. Sous **Connexions** > **[MCN]** > **Formation au routage** > **OSPF** > **Paramètres de base**, configurez **Exporter le poids de routage OSPF** .
3. Enregistrez la configuration, la mise en scène et activez la même chose.
4. Maintenant, configurez Export OSPF Route Weight à n'importe quelle valeur numérique comprise entre **1** et **65529** .
5. Après l'activation de la configuration modifiée, vous pouvez voir le poids de routage sous **Configuration** > **Réseau étendu virtuel** > **Afficher la configuration** > **Routage dynamique** . Le poids d'itinéraire par défaut exporté doit être 0. Le coût réel de l'itinéraire ne doit être que le coût du SD-WAN.

Pour configurer les itinéraires exportés OSPF en tant que Type1 sous Paramètres de filtre d'exportation :

1. Configurez **les interfaces virtuelles** et les **liens WAN** sur DC et Branch afin que nous puissions créer le chemin virtuel entre eux1. Sous **Connexions** > **[MCN]** > **Learning** > **OSPF** > **Filtres d'exportation**, configurez un filtre d'exportation.
2. Développez le filtre. Configurez **Exporter le type d'itinéraire OSPF** vers l'itinéraire **Intra Area Type 1** .
3. Enregistrez la configuration, la mise en scène et activez la même chose. Vous devez être en mesure de voir les deux types de route suivants sous **Exporter le type d'itinéraire OSPF**

- Type 5 AS External
- Type 1 Intra Area

Après l'activation de la configuration modifiée, un utilisateur doit être en mesure de voir les modifications du type d'itinéraire sous **Configuration > Réseau étendu virtuel > Afficher la configuration**. Le type d'itinéraire doit être affiché en tant que Type 5 AS Externe.

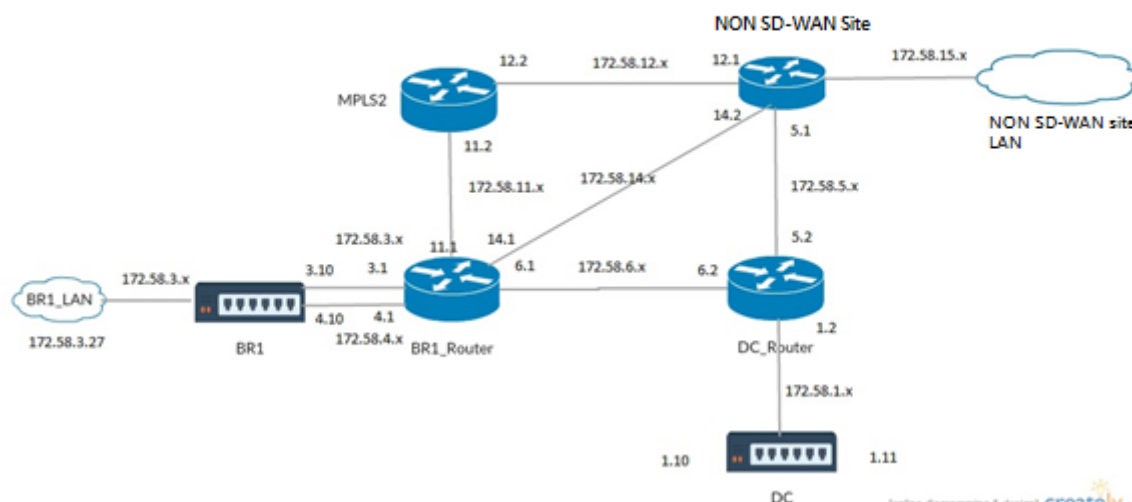
Pour configurer le poids de l'itinéraire exporté OSPF sous Paramètres du filtre d'exportation :

1. Configurez les interfaces virtuelles et les liens WAN sur DC et Branch afin que nous puissions créer le chemin virtuel entre eux.
2. Sous **Connexions > [MCN] -> Formation itinérante > OSPF > Filtres d'exportation**, configurez un filtre d'exportation.
3. Développez le filtre. Configurez Export OSPF Route Weight à n'importe quelle valeur numérique comprise entre **1** et **65529**.
4. Enregistrez la configuration, la mise en scène et activez la même chose.

Après l'activation de la configuration modifiée, un utilisateur doit être en mesure de voir les modifications du type d'itinéraire sous **Configuration > Réseau étendu virtuel > Afficher la configuration**. Le poids de l'itinéraire configuré sous Filtre d'exportation doit remplacer le poids configuré sous **Paramètres OSPF de base**.

Déploiement d'appliances SD-WAN et tierces (non SD-WAN)

Comme le montre l'illustration ci-dessous, le site de l'appliance tierce peut accéder au réseau local du site B en envoyant directement du trafic vers le site B. S'il ne peut pas envoyer de trafic directement, la route de secours va au site A, puis utilise le chemin virtuel entre les sites du contrôleur de domaine et de la branche pour accéder à la branche. Si cela échoue, il utilise MPLS2 pour accéder au site de la branche.



Étapes de configuration :

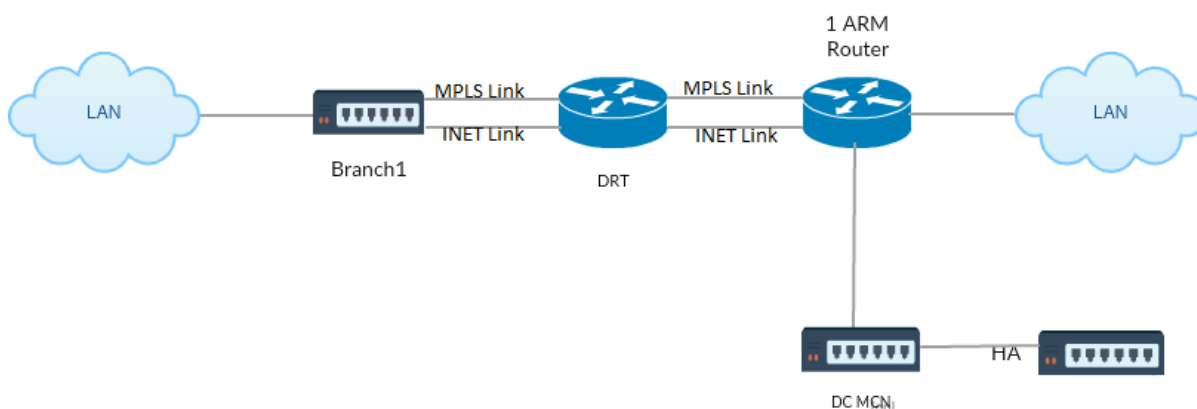
1. Configurez **les interfaces virtuelles** et les **liaisons WAN** sur le contrôleur de domaine et la branche afin qu'un chemin virtuel soit créé entre les sites.
2. Configurez le **type d'itinéraire d'exportation** en tant que **Type1** et affectez le coût comme **195** sur l'apppliance SD-WAN.
3. Enregistrer, mettre en scène et activer la configuration.
4. Envoyer du trafic entre les hôtes de fin sur les sites de contrôleur de domaine et de succursale.
5. Arrêtez la liaison entre R1 et R2.
6. Envoyer du trafic entre les hôtes de fin sur les sites de contrôleur de domaine et de succursale.
7. Annulez l'arrêt de la liaison entre R1 et R2.
8. Envoyer du trafic entre les hôtes de fin sur les sites de contrôleur de domaine et de succursale.
9. Désactivez le service WAN virtuel sur le site DC afin que les chemins d'accès virtuels soient désactivés.
10. Envoyez le trafic entre les hôtes de fin sur les sites de contrôleur de domaine et de succursale.

Vérification de la configuration :

1. Initialement, à l'étape 4, tout le trafic passe par l'apppliance SD-WAN.
2. À l'étape 6, lorsque la liaison entre R1 et R2 est rompue, le trafic est acheminé vers SD-WAN via R3.
3. À l'étape 8, le trafic passe par l'apppliance SD-WAN avec R2 comme prochain saut pour le routeur LAN R1.
4. À l'étape 10, les chemins Virtual WAN passent entre DC et BR1 et le trafic doit circuler normalement comme avant la configuration du réseau SD-WAN.

Le flux de trafic peut être observé dans l'interface graphique SD-WAN sous **Monitoring > Flux**.

Mise en œuvre d'OSPF avec le réseau SD-WAN dans la configuration haute disponibilité



OSPF Type5 à Type1 avec des sites haute disponibilité pendant le basculement vers l'appliance de secours et déployé dans une configuration haute disponibilité :

Pour configurer OSPF dans le déploiement HA :

1. Configurez **les interfaces virtuelles** et les **liaisons WAN** sur DC et Branch pour créer le chemin virtuel entre elles.
2. Configurez la haute disponibilité.
3. Exporter **le type d'itinéraire** configuré comme **Type 1** et **Poids d'itinéraire** comme **50**.
4. Enregistrez la configuration, la mise en scène et activez la même chose.
5. Démarrer le flux de trafic.
6. Notez que sous **Moniteur > Statistiques > Itinéraires**, le nombre d'accès augmente pour les routes OSPF avec les coûts les moins élevés.
7. Amenez le MCN actif vers le bas et observez le comportement.
8. Ramenez le MCN actif d'origine.
9. Le **tableau de bord > État de haute disponibilité** s'affiche correctement pour HA Local Appliance et Peer Appliance pour Active et Veille.
10. Sous **Configuration > Afficher la configuration > Routage dynamique**, OSPF est activé et **export_ospf_route_type** affiche **Type1** et **export_ospf_route_weight** comme **50**.
11. Même après le basculement, l'état de haute disponibilité affiche la configuration OSPF correcte pour l'appliance locale et homologue.
12. Afficher **Moniteur > Statistiques > Itinéraires**. Le nombre de succès augmente pour les routes OSPF à moindre coût.
13. Après le retour arrière, le statut de haute disponibilité affiche la configuration OSPF correcte pour le matériel local et homologue.
14. Vérifiez que le nombre d'accès augmente pour les itinéraires OSPF à faible coût sous la vue **Moniteur > Statistiques > Itinéraires**.

R solution des probl mes

Vous pouvez afficher les param tres OSPF sous **Surveillance > Protocoles de routage**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: OSPF Interface Routing Domain: Default_RoutingDomain Refresh

OSPF Interface

ospf_rdomain_0:
Interface vni-0 (172.58.1.0/24)
Type: broadcast
Area: 0.0.0.0 (0)
State: DROther
Priority: 0
Cost: 10
Hello timer: 10
Wait timer: 40
Dead timer: 40
Retransmit timer: 5
Designated router (ID): 105.105.105.105
Designated router (IP): 172.58.1.28
Backup designated router (ID): 0.0.0.0
Backup designated router (IP): 0.0.0.0

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: OSPF Neighbors Routing Domain: Default_RoutingDomain Refresh

OSPF Neighbors

ospf_rdomain_0:

Router ID	Pri	State	DTime	Interface	Router IP
105.105.105.105	1	Full/DR	00:39	vni-0	172.58.1.28

Vous pouvez  galement observer les journaux de routage dynamique pour voir s’il y a un probl me avec la convergence OSPF.

Diagnose

Debug Logging: ☒ On ☐ Off

Filename: ▼

BGP

May 6, 2021

La fonctionnalité de routage BGP SD-WAN vous permet de :

- Configurez le numéro de système autonome (AS) d'un voisin ou d'un autre routeur homologue (iBGP ou eBGP).
- Créez des stratégies BGP à appliquer de manière sélective à un ensemble de réseaux par voisin, dans les deux sens (importation ou exportation). Une appliance SD-WAN prend en charge huit stratégies par site, avec jusqu'à huit objets réseau (ou huit réseaux) associés à une stratégie.
- Pour chaque stratégie, les utilisateurs peuvent configurer plusieurs chaînes de communauté, AS-PATH-PREPEND, attribut MED. Les utilisateurs peuvent configurer jusqu'à 10 attributs pour chaque stratégie.

Remarque

Seules les préférences locales et la mesure IGP pour la sélection et la manipulation des chemins sont autorisées.

Configuration des stratégies

Dans l'interface de gestion Web SD-WAN, l'éditeur de configuration a une nouvelle section, la stratégie BGP, sous **Route Learning > BGP**. Dans cette section, les utilisateurs peuvent ajouter des attributs BGP qui constituent une stratégie. L'ajout de chaînes de communauté, les chemins d'accès AS prédéfinis et la configuration MED sont pris en charge.

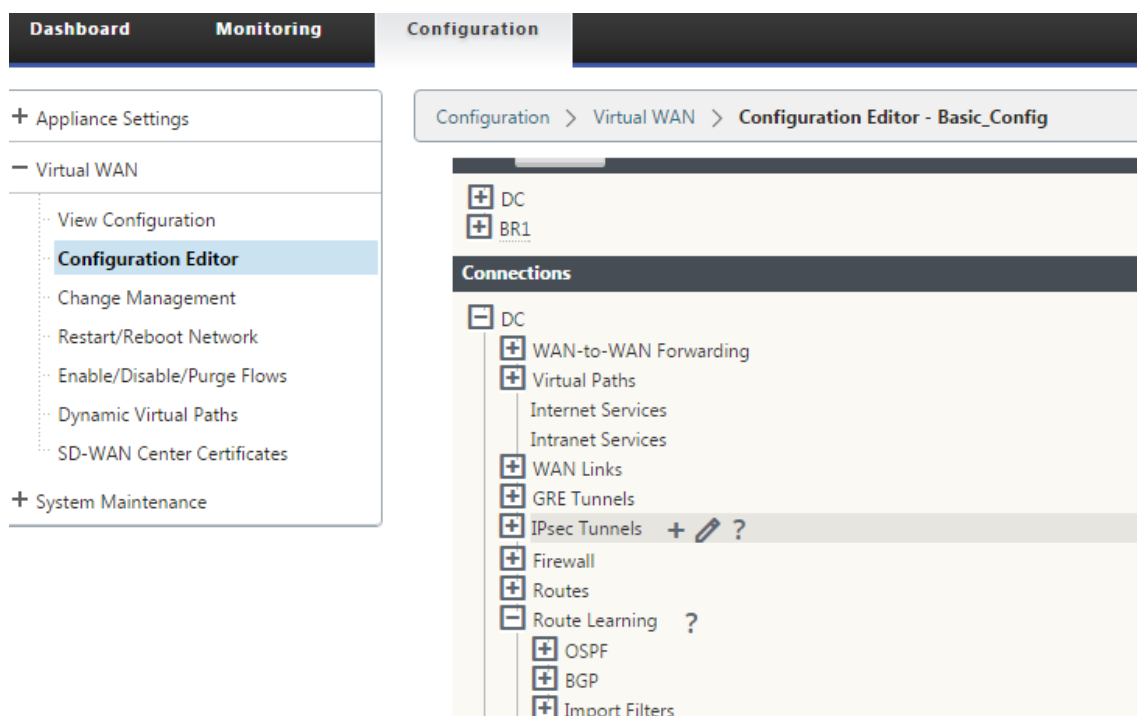
Vous pouvez configurer manuellement chaque chaîne de communauté ou sélectionner aucune annonce ou aucune chaîne de communauté d'exportation dans un menu déroulant. Pour la configu-

ration manuelle, vous pouvez entrer un numéro AS et une communauté. Vous pouvez sélectionner **Insert/Supprimer** pour baliser les itinéraires ou supprimer la communauté des itinéraires.

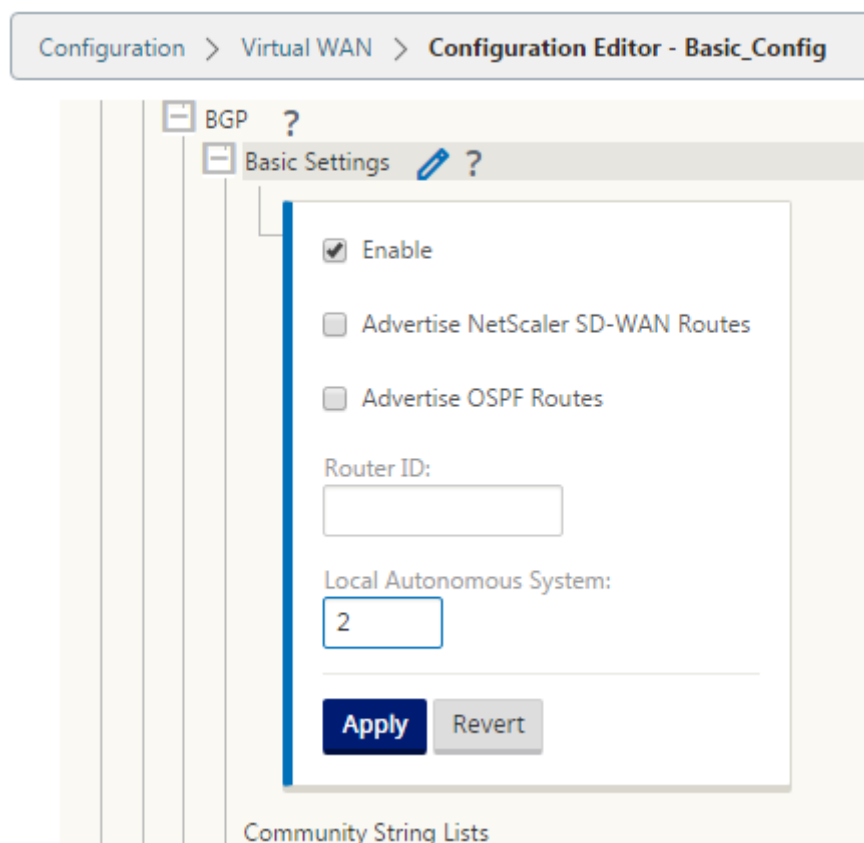
Vous pouvez configurer le nombre de fois que vous souhaitez ajouter le AS local au chemin AS avant de faire de la publicité en dehors du réseau local. Vous pouvez configurer MED pour les itinéraires correspondants.

Pour configurer la stratégie BGP :

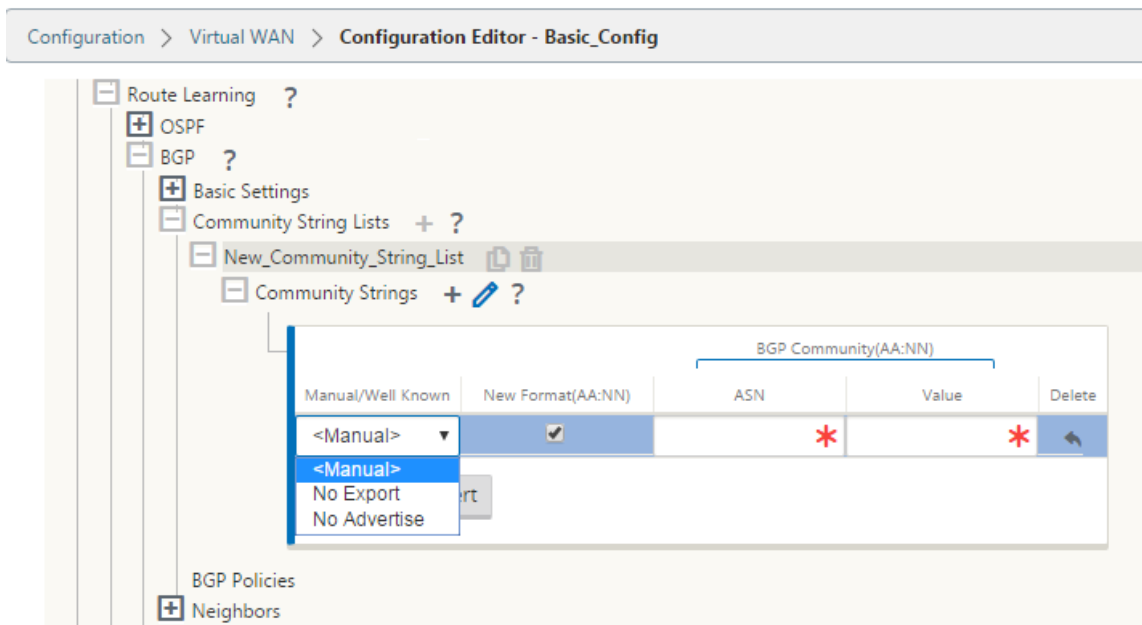
1. Dans l'interface de gestion Web NetScaler SD-WAN, accédez à **Configuration > Virtual WAN > Éditeur de configuration** . Ouvrez un package de configuration existant. Accédez à **Sites > Paramètres de contrôleur de domaine** ou de **succursale**.



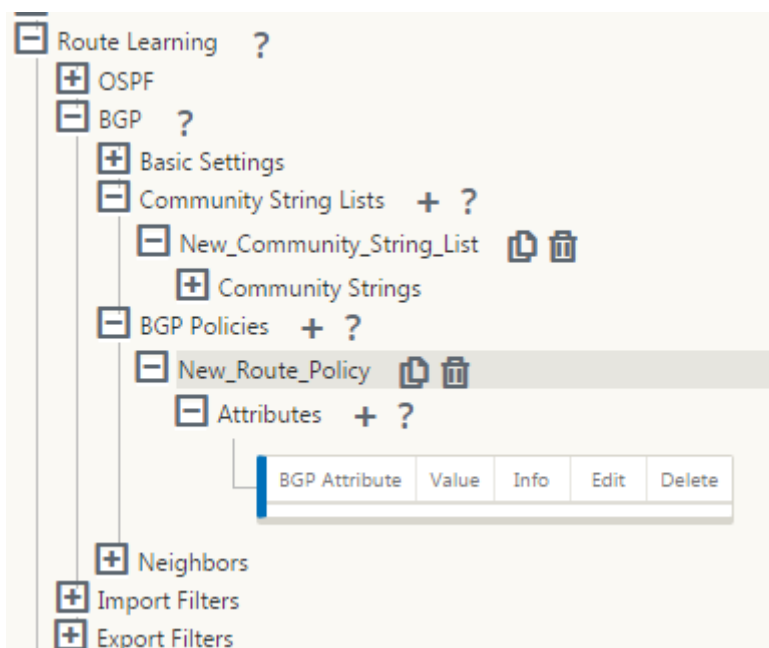
2. Développez **BGP** et cliquez sur **Activer** sous **Paramètres de base** . Entrez l'**ID du routeur** et la valeur **du système autonome local**, puis cliquez sur **Appliquer** .



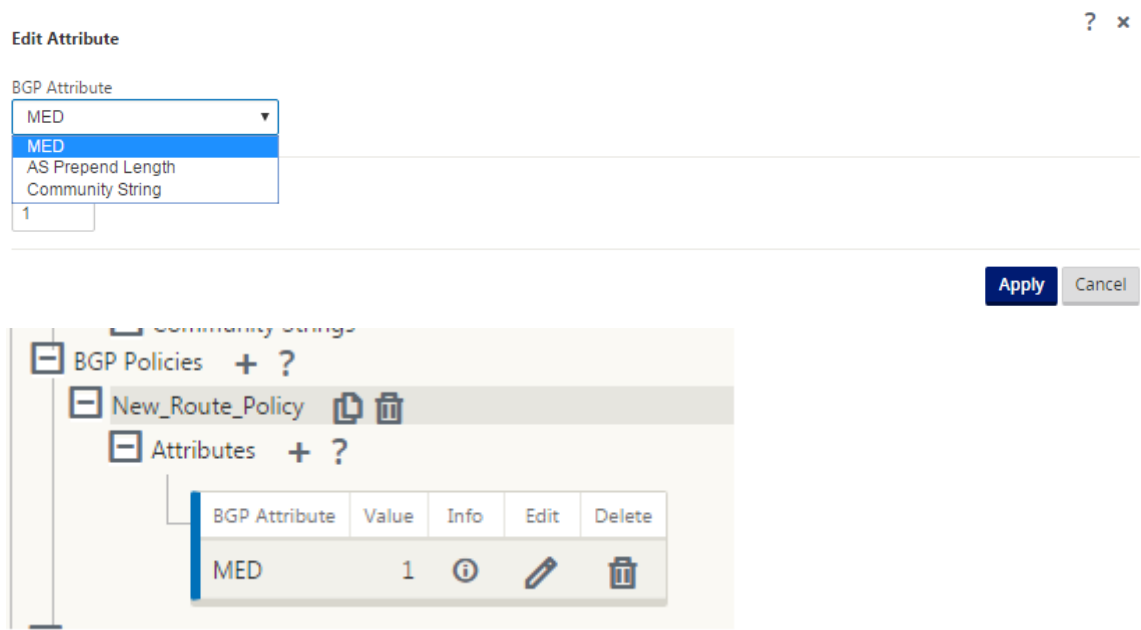
3. Cliquez sur le signe + en regard des **listes de chaînes de communauté** . Configurez chaque chaîne de communauté manuellement ou en sélectionnant aucune chaîne de communauté publicitaire ou aucune chaîne d'exportation dans le menu déroulant. Pour la configuration manuelle, vous pouvez entrer un numéro AS et une communauté. Vous pouvez sélectionner **Insérer ou supprimer** une balise les routes avec la chaîne de communauté ou supprimer la chaîne de communauté des routes reçues des homologues.



4. Configurez la stratégie BGP en développant **les stratégies BGP**. Ajoutez des attributs BGP à la **nouvelle stratégie de routage**.



5. Cliquez sur le **signe+** en regard de **Attributs** pour modifier les attributs BGP. La fenêtre **Modifier les attributs** s'affiche. Sélectionnez l'attribut BGP souhaité dans le menu déroulant. Entrez la valeur souhaitée pour **MED**, **AS Prepend Length** ou **Community Strings** selon votre sélection. Cliquez sur **Apply**.



Remarque

Toute stratégie ne peut avoir qu’une seule occurrence d’un attribut et ne peut pas prendre plusieurs occurrences du même attribut. Vous ne pouvez pas avoir 2 MED ou 2 AS Path Prepend. Il peut avoir soit MED/AS-PATH Prepend/Community String ou une combinaison.

Configuration des voisins

Pour configurer eBGP, une colonne supplémentaire à la section voisins BGP existante est ajoutée pour configurer le numéro AS voisin. Les configurations existantes sont préremplies dans ce champ avec le numéro AS local lorsque vous importez la configuration précédente à l’aide de l’éditeur de configuration SD-WAN 9.2.

La configuration du voisin comporte également une section avancée facultative (ligne extensible) dans laquelle vous pouvez ajouter des stratégies pour chaque voisin.

Configuration des voisins avancés

Avec cette option, vous pouvez ajouter des objets réseau et ajouter une stratégie BGP configurée pour cet objet réseau. Ceci est similaire à la création d’une carte de routage et d’ACL pour correspondre à certains itinéraires et à la configuration des attributs BGP pour ce voisin. Vous pouvez spécifier la direction pour indiquer si cette stratégie est appliquée aux itinéraires entrants ou sortants.

La stratégie par défaut concerne <accept> toutes les routes. Les stratégies d’acceptation et de rejet sont des valeurs par défaut et ne peuvent pas être modifiées.

Vous avez la possibilité de faire correspondre les itinéraires en fonction de l'adresse réseau (adresse de destination), du chemin AS, de la chaîne de communauté et d'affecter une stratégie et de sélectionner la direction de la stratégie à appliquer.

Pour configurer les voisins :

1. Configurez les voisins en cliquant sur **Ajouter** comme indiqué ci-dessous.

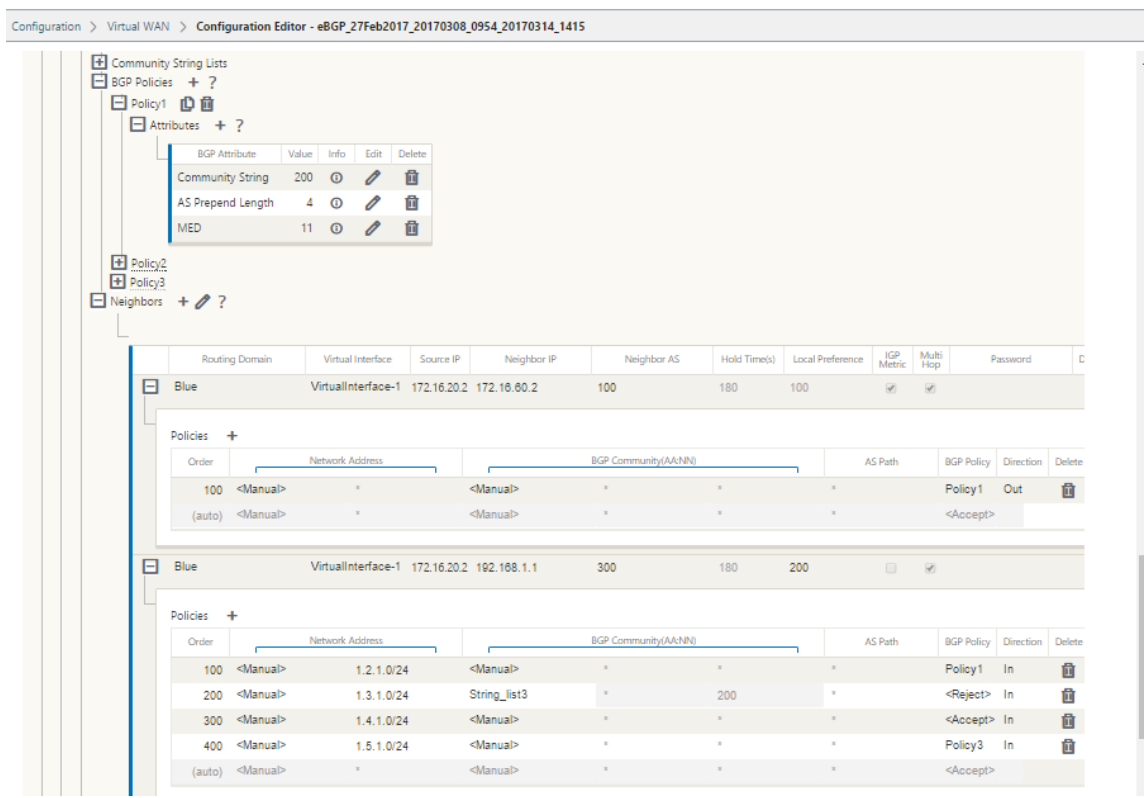
The screenshot shows the 'Neighbors' configuration window. At the top, there is a table with columns: Interface, Source IP, Neighbor IP, Neighbor AS, Hold Time(s), Local Preference, IGP Metric, Multi Hop, Password, and Delete. An 'Add' button is located to the left of the table.

2. Cliquez sur le **signe+** . Sélectionnez une **interface virtuelle**. Entrez l'adresse **IP du voisin** .

The screenshot shows the 'Neighbors' configuration window with one neighbor added. The table has columns: Virtual Interface, Source IP, Neighbor IP, Neighbor AS, Hold Time(s), Local Preference, IGP Metric, Multi Hop, Password, and Delete. The first row shows 'VirtualInterface-1' as the Virtual Interface, '172.58.1.20' as the Source IP, a red asterisk as the Neighbor IP, '2' as the Neighbor AS, '180' as the Hold Time(s), '100' as the Local Preference, and checked boxes for IGP Metric and Multi Hop. Below the table, there is a 'Policies' section with an 'Add' button and a table with columns: Order, Network Address, BGP Community(AA:NN), AS Path, BGP Policy, Direction, and Delete. The 'Apply' and 'Revert' buttons are at the bottom.

3. Ajouter des stratégies. Sélectionnez **l'adresse réseau**, la **communauté BGP** et les détails du **chemin AS** comme vous le souhaitez. Cliquez sur **Apply**.

The screenshot shows the 'Neighbors' configuration window with a policy added. The table has columns: Virtual Interface, Source IP, Neighbor IP, Neighbor AS, Hold Time(s), and Local Preference. The first row shows 'VirtualInterface-1' as the Virtual Interface, '172.58.1.20' as the Source IP, a red asterisk as the Neighbor IP, '2' as the Neighbor AS, '180' as the Hold Time(s), and '100' as the Local Preference. Below the table, there is a 'Policies' section with an 'Add' button and a table with columns: Order, Network Address, BGP Community(AA:NN), and AS Path. The first row shows '100' as the Order, '<Manual>' as the Network Address, '<Manual>' as the BGP Community(AA:NN), and '*' as the AS Path. A dropdown menu is open for the BGP Community(AA:NN) column, showing options: '<Manual>', 'New_Community_String_List', and '*'. The 'Apply' and 'Revert' buttons are at the bottom.



4. Accédez à **Surveillance > Protocoles de routage > Protocoles de routage dynamique** pour surveiller les stratégies BGP configurées et les voisins pour l’appliance de site DC ou Branch.

Vous pouvez activer la journalisation du débogage et afficher les fichiers journaux pour le routage à partir de la page **Moniteur > Protocole de routage** . Les journaux du démon de routage sont divisés en fichiers journaux distincts. Les informations de routage standard sont stockées dans *dynamic_routing.log* tandis que les problèmes de routage dynamique sont capturés dans *dynamic_routing_diagnostics.log* qui peuvent être consultés à partir de la surveillance des protocoles de routage.

Reconfiguration logicielle BGP

Les stratégies de routage pour homologue BGP incluent des configurations telles que la carte de routage, la liste de distribution, la liste de préfix-list et la liste de filtres qui peuvent avoir un impact sur les mises à jour de tables de routage entrantes ou sortantes. En cas de modification de la stratégie de routage, la session BGP doit être effacée ou réinitialisée pour que la nouvelle stratégie prenne effet.

L’effacement d’une session BGP à l’aide d’une réinitialisation matérielle invalide le cache et entraîne un impact négatif sur le fonctionnement des réseaux à mesure que les informations contenues dans le cache deviennent indisponibles.

La fonctionnalité BGP Soft Reset Enhancement fournit une prise en charge automatique de la réinitialisation dynamique des mises à jour de la table de routage BGP entrantes qui ne dépendent pas des informations de mise à jour de la table de routage stockées.

Résolution des problèmes

Pour afficher les paramètres BGP, accédez à **Surveillance > Protocoles de routage** > sélectionnez **État BGP** dans le champ **Affichage**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: BGP State Routing Domain: Default_RoutingDomain BGP Session: <ALL>

Reset Session

Refresh

BGP State

name	proto	table	state	since	info
bgp1_rdomain_0	BGP	T0	up	2020-08-27 10:46:44	Established
Preference: 100					
Input filter: neighbour_0_in					
Output filter: neighbour_0_out					
Routes: 8 imported, 4 exported, 1 preferred					
Route change stats:					
Import updates: received rejected filtered ignored accepted					
Import withdraws: 16 0 0 8 8					
Export updates: 0 0 --- 0 0					
Export withdraws: 43 19 18 --- 6					
Export withdraws: 2 --- --- --- 2					
BGP state: Established					
Neighbor address: 172.58.1.28					
Neighbor AS: 10					
Citrix SD-WAN Interface: vni-0					
Neighbor ID: 105.105.105.105					
Neighbor caps: refresh AS4					
Session: internal multihop AS4					
Source address: 172.58.1.10					
Hold timer: 130/180					
Keepalive timer: 46/60					

Vous pouvez observer les journaux de routage dynamique pour voir s’il y a un problème avec BGP Convergence.

Diagnose

Debug Logging: ☒ On ☐ Off

Filename:

dynamic_routing_diagnostics.log

View Log

iBGP

May 6, 2021

Appliance Citrix SD-WAN avec iBGP côté LAN et eBGP côté WAN :

Les appliances Citrix SD-WAN annoncent toutes les routes eBGP apprises dans le domaine IGP avec NEXT HOP SELF lorsqu'elles sont déployées avec iBGP côté LAN et eBGP côté WAN.

Plusieurs routeurs LAN iBGP dans une topologie de réseau linéaire avec appairage direct et maillé avec Citrix SD-WAN.

Limitations :

- Les attributs « AS-path », « Med » et « Community » ne sont pas pris en charge.
- Le filtrage d'itinéraire entre OSPF et BGP pendant la redistribution n'est pas pris en charge. Soit la totalité (ou) aucune des routes apprises par l'OSPF n'est annoncée aux pairs de BGP et vice-versa.
- L'agrégation d'itinéraires n'est pas prise en charge.
- Seul un maximum de 16 homologues BGP (y compris iBGP et eBGP) peut être configuré.

eBGP

May 6, 2021

Site SD-WAN communiquant avec un site non SD-WAN via eBGP :

Lorsqu'un site sans dispositif SD-WAN communique avec un autre site avec l'appliance SD-WAN (Site-A) sur un seul chemin WAN (seul Internet est disponible), et si le site avec l'appliance SD-WAN (Site-A) perd la connectivité Internet, le site sans SD-WAN peut communiquer avec le site A via un autre SD-WAN site de l'appliance (Site-B). Site-B enfonce le trafic depuis le site sans dispositif SD-WAN vers le Site-A.

Communication entre les sites SD-WAN à l'aide de Virtual Path et eBGP :

Fournit l'apprentissage de l'itinéraire de sous-couche pour communiquer avec les sous-réseaux locaux de site distant lorsque le chemin virtuel est en panne entre deux sites alors que l'appliance Virtual WAN est toujours en service.

Itinéraire des applications

May 6, 2021

Dans un réseau d'entreprise typique, les succursales accèdent aux applications sur le datacenter local, le datacenter cloud ou les applications SaaS. La fonctionnalité de routage des applications vous permet de diriger les applications à travers votre réseau facilement et à moindre coût. Par exemple, lorsqu'un utilisateur sur le site de la succursale tente d'accéder à une application SaaS, le trafic peut être acheminé de telle sorte que les succursales puissent accéder directement aux applications SaaS sur Internet, sans avoir à passer par le centre de données en premier.

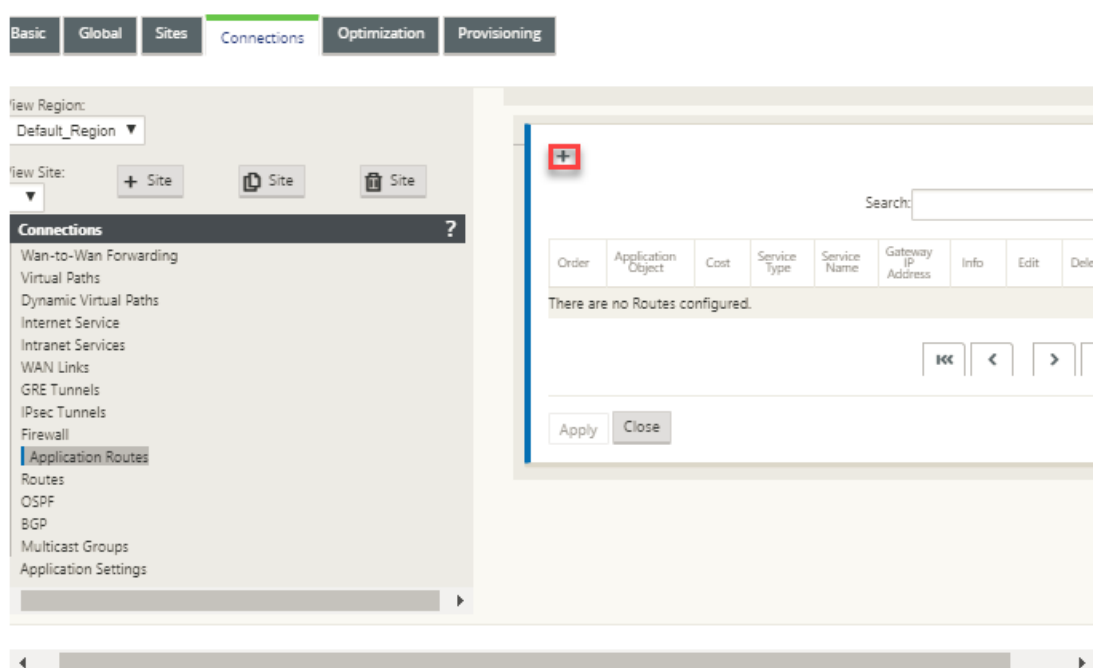
Citrix SD-WAN vous permet de définir les itinéraires d'application pour les services suivants :

- **Chemin d'accès virtuel** : ce service gère le trafic sur les chemins d'accès virtuels. Un chemin virtuel est un lien logique entre deux liaisons WAN. Il comprend une collection de chemins WAN combinés pour fournir une communication de niveau de service élevé entre deux nœuds SD-WAN. L'appliance SD-WAN mesure le réseau sur une base par chemin et s'adapte à l'évolution de la demande et des conditions WAN des applications. Un chemin virtuel peut être statique (existe toujours) ou dynamique (n'existe que lorsque le trafic entre deux appliances SD-WAN atteint un seuil configuré).
- **Internet** : ce service gère le trafic entre un site Enterprise et des sites sur Internet public. Le trafic Internet n'est pas encapsulé. En cas de congestion, le SD-WAN gère activement la bande passante en limitant le trafic Internet par rapport au chemin virtuel et au trafic Intranet.
- **Intranet** : ce service gère le trafic Intranet d'entreprise qui n'a pas été défini pour la transmission sur un chemin virtuel. Le trafic intranet n'est pas encapsulé. Le SD-WAN gère la bande passante en limitant ce trafic par rapport aux autres types de service en période de congestion. Dans certaines conditions, et si l'Intranet Fallback est configuré sur le chemin virtuel, le trafic qui circule habituellement via le chemin virtuel peut être traité comme du trafic intranet.
- **Local** : ce service gère le trafic local vers le site qui ne correspond à aucun autre service. Le SD-WAN ignore le trafic provenant et destiné à une route locale.
- **Tunnel GRE** : Ce service gère le trafic IP destiné à un tunnel GRE et correspond au tunnel LAN GRE configuré sur le site. La fonction Tunnel GRE vous permet de configurer les appliances SD-WAN pour qu'elles terminent les tunnels GRE sur le réseau local. Pour un itinéraire avec le type de service GRE Tunnel, la Gateway doit résider dans l'un des sous-réseaux de tunnel du tunnel GRE local.
- **Tunnel LAN IPsec** : Ce service gère le trafic IP destiné à un tunnel LAN IPsec et correspond au tunnel LAN IPsec configuré sur le site. La fonction LAN IPsec Tunnel vous permet de configurer les appliances SD-WAN pour qu'elles terminent les tunnels IPsec côté LAN ou WAN.

Pour effectuer une direction de service pour les applications, il est important d'identifier une application sur le premier paquet lui-même. Initialement, les paquets traversent la route IP une fois que le trafic est classé et que l'application est connue, la route de l'application correspondante est utilisée. La première classification des paquets est obtenue en apprenant les sous-réseaux IP et les ports associés aux objets d'application. Ils sont obtenus à l'aide des résultats de classification historiques du classificateur DPI et des types de correspondance de port IP configurés par l'utilisateur.

Pour configurer le routage des applications :

1. Dans l'Éditeur de configuration, accédez à **Connexions > Itinéraires des applications**, puis cliquez sur **+**.



2. Dans la page **Ajouter**, définissez les paramètres suivants :
 - **Objet d'application** : Objet d'application que vous souhaitez diriger. Les objets d'application créés par vous sont répertoriés ici. Pour plus d'informations, consultez la section **Objets d'application** dans la [Classification des applications](#) rubrique.

- **Domaine de routage** : Domaine de routage à utiliser par l'itinéraire d'application. Choisissez l'un des domaines de routage configurés.
- **Coût** : Poids pour déterminer la priorité de l'itinéraire pour cet itinéraire. Les itinéraires à moindre coût ont priorité sur les itinéraires à coût élevé. La plage est de 1 à 65534. La valeur par défaut est 5.
- **Type de service** : Sélectionnez l'un des services suivants. Cela mappe l'application à un service.
- **Chemin virtuel** : identifie le trafic d'application comme trafic de chemin virtuel et correspond à un chemin virtuel basé sur les règles de chemin virtuel. Dans le champ **Site de saut suivant**, entrez le site distant de saut suivant vers lequel les paquets de chemin virtuel sont dirigés.

Remarque

Tout flux qui touche les Routes d'application de chemin virtuel ne passe pas sur le chemin virtuel dynamique.

- **Internet** : identifie le trafic d'application comme trafic Internet et correspond au service Internet.
- **Intranet** : identifie le trafic d'application comme trafic Intranet et correspond à un service Intranet basé sur les règles Intranet. Dans le champ **Service intranet**, sélectionnez un service intranet à utiliser pour l'itinéraire.
- **Local** : identifie le trafic d'application comme local vers le site et ne correspond pas à aucun service. Le trafic provenant et destiné à une route locale est ignoré.

Remarque

Pour le type de service local, une fois la classification PPP terminée, les routes IP configurées prennent la décision de routage.

- **Tunnel GRE** : Identifié le trafic de l’application comme étant destiné à un tunnel GRE et correspond au tunnel GRE LAN configuré sur le site. Dans le **champ Adresse IP de la Gateway**, entrez l’adresse IP de la passerelle qui doit se trouver dans le sous-réseau du LAN GRE Tunnel. Sélectionnez **Éligibilité basée sur la passerelle** pour permettre à l’itinéraire de ne pas recevoir de trafic lorsque la passerelle n’est pas accessible.
- **Tunnel IPsec LAN** : Identifié le trafic d’application comme étant destiné à un tunnel IPsec LAN et correspond au tunnel IPsec LAN configuré sur le site. Dans le champ **Tunnel IPsec**, sélectionnez l’un des tunnels IPsec configurés. Sélectionnez **Éligibilité basée sur le tunnel** pour permettre à l’itinéraire de ne pas recevoir de trafic lorsque le tunnel n’est pas accessible.

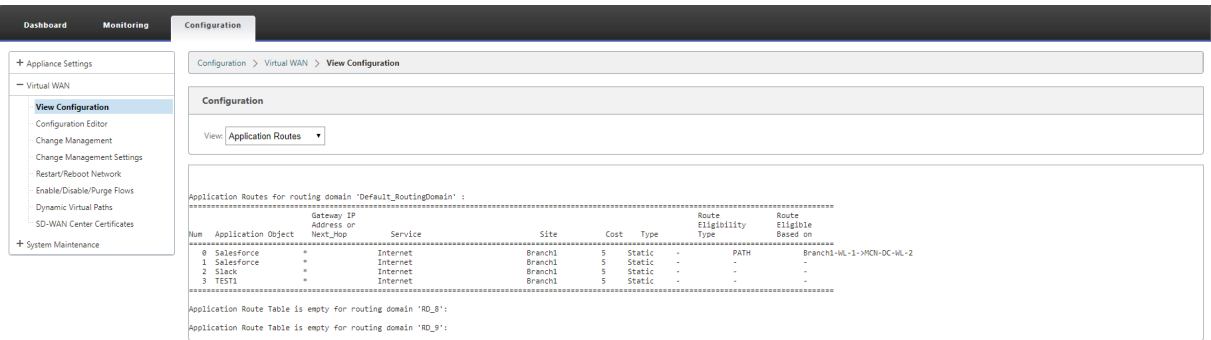
Remarque

Une fois que vous avez sélectionné un service pour une application personnalisée, ne le modifiez pas.

- **Éligibilité basée sur le chemin d’accès** : sélectionnez cette option pour permettre à l’itinéraire de ne pas recevoir de trafic lorsque le chemin d’accès spécifié est en panne. Dans le champ **Chemin d’accès**, spécifiez le chemin à utiliser pour déterminer l’éligibilité de l’itinéraire.

3. Cliquez sur **Apply**.

Pour afficher les itinéraires d’application configurés sur votre appliance SD-WAN. Dans l’interface graphique SD-WAN, accédez à **Configuration > Réseau étendu virtuel > Afficher la configuration** . Sélectionnez **Itinéraires d’application** dans le menu déroulant **Affichage** .



Pour afficher les données de statistiques pour les itinéraires d’application :

1. Dans l’interface graphique SD-WAN, accédez à **Surveillance > Statistiques** .

2. Dans la liste déroulante **Afficher**, sélectionnez **Itinéraires d'application**.

The screenshot shows the 'Monitoring > Statistics' page in the Citrix SD-WAN interface. The left sidebar contains a 'Statistics' menu with options like Flows, Routing Protocols, Firewall, IKE/IPsec, IGMP, Performance Reports, QoS Reports, Usage Reports, Availability Reports, Application Reports, DHCP Server/Relay, and VRRP. The main content area is titled 'Application Route Statistics' and shows a table of application routes for the routing domain 'Default_RoutingDomain'. The table has columns for Num, Application Object, Gateway IP Address, Service, Firewall Zone, Reachable, Site, Type, Cost, Hit Count, Eligible, Eligibility Type, and Eligibility Value. The table displays 4 entries, with the first entry being 'TEST1' and the last entry being 'Salesforce'.

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	TEST1	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A
1	Slack	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A
2	Salesforce	*	Internet	Internet_Zone	YES	Branch1	Static	5	173	YES	Path	Branch1-WL-1->MCN-DC-WL-2
3	Salesforce	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A

Vous pouvez afficher les statistiques suivantes :

- **Application Object** : Nom de l'objet application.
- **Adresse IP de la Gateway** : adresse IP de la passerelle utilisée par les objets d'application avec le type de service de tunnel GRE.
- **Service** : type de service mappé à l'objet d'application.
- **Zone de pare-feu** : zone de pare-feu dans laquelle se trouve cet itinéraire.
- **Accessible** : Statut de l'itinéraire de l'application.
- **Site** : Nom du site.
- **Type** : Indique si l'itinéraire est statique ou dynamique.
- **Coût** : La priorité de l'itinéraire.
- **Nombre de coups** : nombre de fois où l'itinéraire de l'application est utilisé pour diriger le trafic.
- **Admissible** : L'itinéraire de l'application est-il éligible pour envoyer le trafic.
- **Type d'éligibilité** : Type de condition d'éligibilité d'itinéraire appliquée à cet itinéraire. Le type d'éligibilité peut être Chemin d'accès, Passerelle ou Tunnel.
- **Valeur d'éligibilité** : valeur spécifiée pour la condition d'éligibilité de l'itinéraire.

Remarque

Dans la version actuelle, les applications appartenant à la famille d'applications, le type de correspondance défini dans l'objet d'application, ne peuvent pas être orientées.

Résolution des problèmes

Après avoir créé la route d'application, vous pouvez confirmer que l'application est correctement routée vers le service prévu à l'aide de la section **Monitoring**.

Pour voir si l'application est correctement routée vers le service prévu, accédez aux pages suivantes :

- **Surveillance > Statistiques > Routes d'applications**

- **Surveillance > Flux**
- **Surveillance > Pare-feu**

S'il y a un comportement de routage inattendu, collectez le bundle de diagnostics STS pendant que le problème est observé et partagez-le avec l'équipe de support Citrix.

Le pack STS peut être créé et téléchargé à l'aide **de Configuration > Maintenance du système > Diagnostics > Informations de diagnostic**.

Filtrage d'itinéraire

May 6, 2021

Pour les réseaux avec l'apprentissage d'itinéraire activé, Citrix SD-WAN fournit plus de contrôle sur les routes SD-WAN annoncées aux voisins de routage plutôt que sur les routes reçues des voisins de routage, plutôt que sur la publicité et l'acceptation de toutes les routes ou pas.

- Les filtres d'exportation sont utilisés pour inclure ou exclure des itinéraires pour la publicité à l'aide des protocoles OSPF et BGP basés sur des critères de correspondance spécifiques. Les règles de filtrage d'exportation sont les règles qui doivent être respectées lors de la publicité de routes SD-WAN sur des protocoles de routage dynamique. Toutes les routes sont annoncées aux pairs par défaut.
- Les filtres d'importation sont utilisés pour accepter ou ne pas accepter les itinéraires reçus à l'aide de voisins OSPF et BGP basés sur des critères de correspondance spécifiques. Les règles de filtrage d'importation sont les règles qui doivent être respectées avant d'importer des itinéraires dynamiques dans la base de données de routage SD-WAN. Aucune route n'est importée par défaut.

Le filtrage d'itinéraire est implémenté sur les routes LAN et les routes de chemin virtuel dans un réseau SD-WAN (datacenter ou branche) et est annoncé sur un réseau non-SD-WAN via BGP et OSPF.

Vous pouvez configurer jusqu'à 512 filtres d'exportation et 512 filtres d'importation. Il s'agit de la limite globale, et non de la limite de domaine de routage.

Configurer les filtres d'exportation

Dans l'**Éditeur de configuration**, accédez à **Connexions > Régions > Site > OSPF** ou **BGP > Exporter les filtres**.

Section: Export Filters

+

?

Order	Network Address	Prefix	Citrix SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone	
100	<Manual>	10.102.29.220/16	eq 12	eq 10	Virtual Path	Client-1	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Export OSPF Route Type:
Type 5 AS External

Export OSPF Route Weight:
4

100

<Manual>

*

eq

*

eq

*

Any

<Any>

*

☒

☒

Apply

Revert

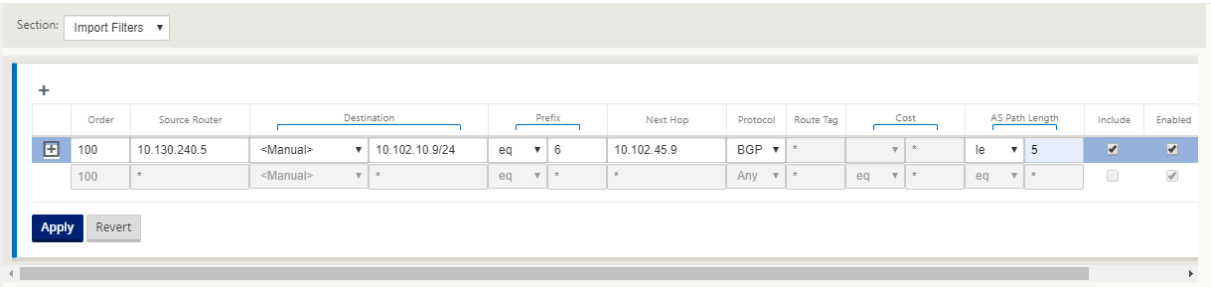
Utilisez les critères suivants pour créer chaque filtre d’exportation que vous souhaitez créer.

Critères de champ	Description	Valeur
Ordre	Ordre dans lequel les filtres sont priorisés. Le premier filtre correspondant à un itinéraire est appliqué à cet itinéraire	100, 200, 300, 400, 500, 600
Adresse réseau	Entrez l’ adresse IP et le masque de sous-réseau de l’objet réseau configuré qui décrit le réseau de l’itinéraire	<ul style="list-style-type: none">Adresse IP
Préfixe	Pour faire correspondre les itinéraires par préfixe, choisissez un prédicat de correspondance dans le menu et entrez un préfixe d’itinéraire dans le champ adjacent	<ul style="list-style-type: none">eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Coût Citrix SD-WAN	Méthode (prédicat) et coût d’itinéraire SD-WAN utilisés pour restreindre la sélection des itinéraires exportés	Valeur numérique
Type de service	Sélectionnez les types de service affectés aux itinéraires correspondants dans une liste de services Citrix SD-WAN	Tout, Local, Chemin d’accès virtuel, Internet, Intranet, LAN Tunnel GRE, LAN Tunnel IPsec
Nom du site/service	Pour Intranet, LAN GRE Tunnel et LAN IPsec Tunnel, spécifiez le nom du type de service configuré à utiliser	Chaîne de texte

Critères de champ	Description	Valeur
Adresse IP de la passerelle	Si vous choisissez LAN GRE Tunnel comme type de service, entrez l'adresse IP de la Gateway pour le tunnel	Adresse IP
Inclure	Activez la case à cocher pour inclure les itinéraires qui correspondent à ce filtre. Sinon, les itinéraires correspondants sont ignorés	Aucune
Activé	Activez la case à cocher Activer ce filtre. Sinon, le filtre est ignoré	Aucune
Supprimer	Sélectionnez l'icône Supprimer pour supprimer ce filtre.	Aucune
Cloner	Cliquez sur l'icône de clone pour créer une copie d'un filtre existant	Aucune

Configurer les filtres d'importation

Dans l'**Éditeur de configuration**, accédez à **Connexions > Régions > Site > OSPF** ou **BGP > Importer les filtres**.



Utilisez les critères suivants pour créer chaque filtre d'exportation que vous souhaitez créer.

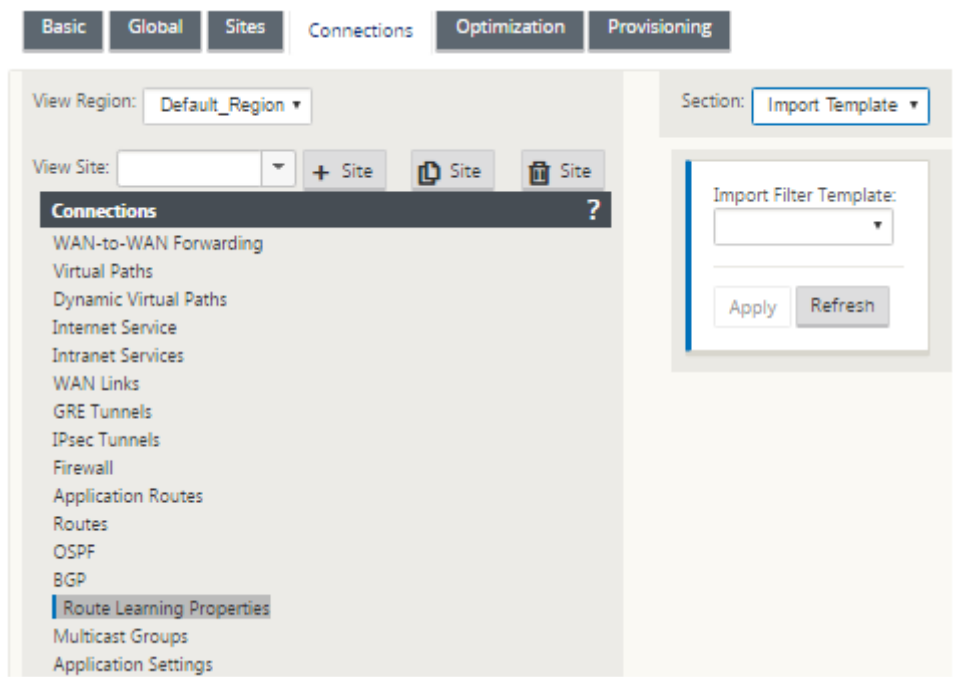
Critères de champ	Description	Valeur
Ordre	Ordre dans lequel les filtres sont priorisés. Le premier filtre correspondant à un itinéraire est appliqué à cet itinéraire	100, 200, 300, 400, 500, 600
Routeur source	L'adresse IP du routeur source, elle est applicable uniquement pour iBGP	• Adresse IP
Destination	L'adresse IP et le masque de sous-réseau de la destination d'un itinéraire	• Adresse IP
Préfixe	Pour faire correspondre les itinéraires par préfixe, choisissez un prédicat de correspondance dans le menu et entrez un préfixe d'itinéraire dans le champ adjacent	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Prochain saut	L'adresse IP du prochain saut	• Adresse IP
Protocole	Protocole de routage à l'aide duquel une route est apprise	OSPF ou BGP
Balise d'itinéraire	La balise Route OSPF correspondant au filtre. Les balises de route OSPF empêchent les boucles de routage lors de la redistribution mutuelle entre OSPF et d'autres protocoles	Valeur numérique
Coût	Coût d'itinéraire utilisé pour correspondre aux itinéraires OSPF pour l'importation	Valeur numérique
Longueur du chemin AS	La longueur du chemin AS utilisée pour correspondre aux routes BGP pour l'importation	Valeur numérique
Inclure	Activez la case à cocher pour inclure les itinéraires qui correspondent à ce filtre. Sinon, les itinéraires correspondants sont ignorés	Aucune

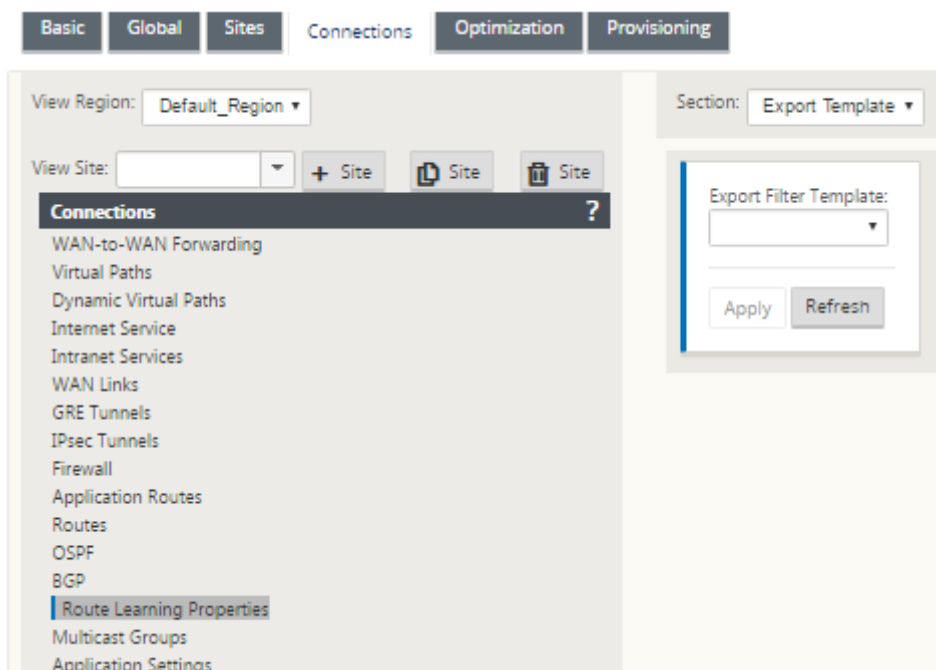
Critères de champ	Description	Valeur
Activé	Activez la case à cocher Activer ce filtre. Sinon, le filtre est ignoré	Aucune
Supprimer	Cliquez sur l'icône Supprimer pour supprimer ce filtre.	Aucune
Cloner	Cliquez sur l'icône de clone pour créer une copie d'un filtre existant	Aucune

Configurer les modèles de filtre de stratégie de routage

Vous pouvez créer plusieurs modèles de filtre d'importation ou d'exportation avec différentes règles de filtre et associer le modèle à chaque site.

Les règles de filtre d'importation/exportation au niveau du site créées par l'utilisateur ont plus de priorité. Les règles de modèle suivent les règles créées par l'utilisateur lorsqu'elles sont associées au site dans la section **Formation itinérante** de Connexions.





Récapitulatif des itinéraires

May 6, 2021

Avec l'augmentation de la taille des réseaux d'entreprise, les routeurs doivent maintenir le grand nombre de routes dans leur table de routage. Les routeurs ont besoin de ressources CPU, mémoire et bande passante accrues pour rechercher les grandes tables de routage et maintenir des itinéraires individuels. Vous pouvez configurer un itinéraire récapitulatif avec les types de service Local et Discard. Cette route récapitulative est annoncée sur les périphériques de saut suivant.

Pour configurer un itinéraire récapitulatif pour un sous-réseau local :

1. Dans l'Éditeur de configuration, accédez à **Connexions** > **Itinéraires** et cliquez sur le **+** pour ajouter un itinéraire.
2. Dans la page **Ajouter un itinéraire**, définissez les paramètres suivants, puis cliquez sur **Ajouter**.
 - **Adresse IP réseau** : Adresse IP de l'itinéraire récapitulatif calculé.
 - **Coût** : Poids pour déterminer la priorité de l'itinéraire pour cet itinéraire. Les routes moins coûteuses ont priorité sur les routes plus coûteuses. La plage est de 1—15. La valeur par défaut est 5.
 - **Domaine** de routage : Protocoles de routage fournissant le point d'administration unique pour gérer un réseau d'entreprise, un réseau de succursales ou un réseau de datacenter.

- **Type de service** : sélectionnez Type de service local.

Remarque

Vous ne pouvez sélectionner que les types de service **Local** et **Discard** pour les itinéraires récapitulatifs.

- **Adresse IP de la passerelle** : adresse IP de la passerelle pour cet itinéraire.
- **Exporter l'itinéraire** : exporte l'itinéraire vers d'autres sites connectés.
- **Route récapitulative** : annonce l'itinéraire sous la forme d'un itinéraire récapitulatif unique vers les autres périphériques connectés, au lieu de tous les autres sous-réseaux correspondants.

Add ? x

Network IP Address	Routing Domain	Cost	Service Type	Gateway IP Address
<input type="text" value="172.16.0.0/22"/>	<input type="text" value="Default_RoutingI"/>	<input type="text" value="5"/>	<input type="text" value="Local"/>	<input type="text"/>

☒ Export Route

☒ Summary Route

☐ Eligibility Based On Path

Path:

☐ Eligibility Based On Gateway

Add **Cancel**

Résolution des problèmes

Les routes résumées configurées sur le MCN sont envoyées à la branche via le chemin virtuel. Si vous ne voyez pas les détails du chemin virtuel dans la table de routage de la branche, vérifiez le tableau de bord Branche. Le tableau de bord affiche l'état du chemin virtuel entre le MCN et la branche.

Dashboard **Monitoring** **Configuration**

System Status

Name:	BR1_VPX
Model:	VPX
Sub-Model:	BASE
Appliance Mode:	Client
Serial Number:	5f4519dd-e39a-d3f6-24a6-6ba0e6578d2c
Management IP Address:	10.105.172.7
Appliance Uptime:	6 days, 56 minutes, 1.4 seconds
Service Uptime:	6 days, 50 minutes, 39.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Local Versions

Configuration Created On:	Wed Sep 2 11:15:54 2020
Software Version:	11.2.1.53.864510
Built On:	Aug 25 2020 at 19:02:21
Hardware Version:	VPX
OS Partition Version:	5.1

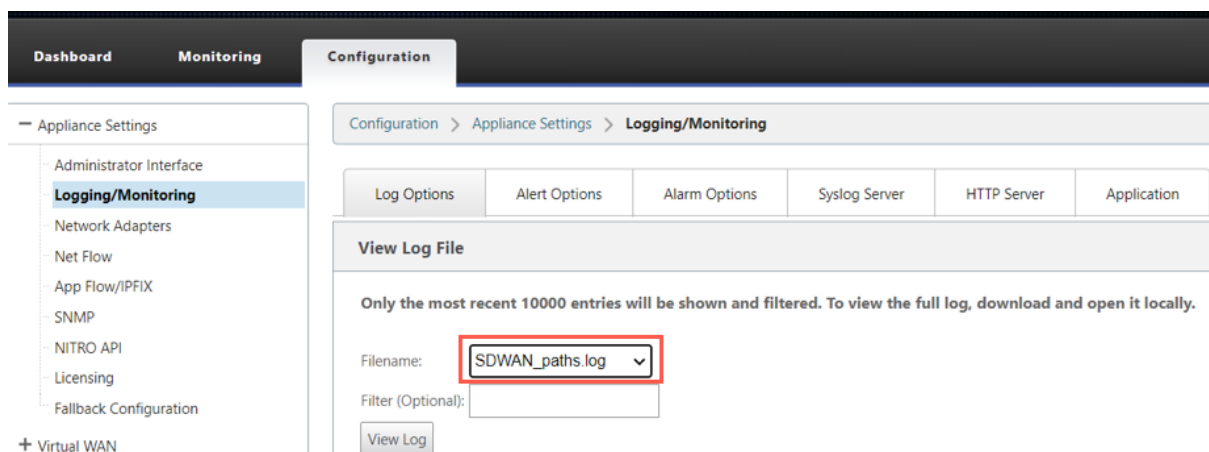
Virtual Path Service Status

Virtual Path MCN_VPX-BR1_VPX	Uptime: 6 days, 50 minutes, 19.0 seconds.
------------------------------	---

Si le chemin virtuel est hors service, vérifiez sa raison sous **Configuration > Logging/Monitoring**.

Sélectionnez l'un des fichiers suivants dans la liste déroulante **nom** de fichier à vérifier :

- SDWAN_paths.log
- SDWAN_common.log



Préférence de protocole

May 6, 2021

La préférence de protocole est une fonctionnalité spécifique à Citrix SD-WAN, qui est similaire à la distance administrative du routeur.

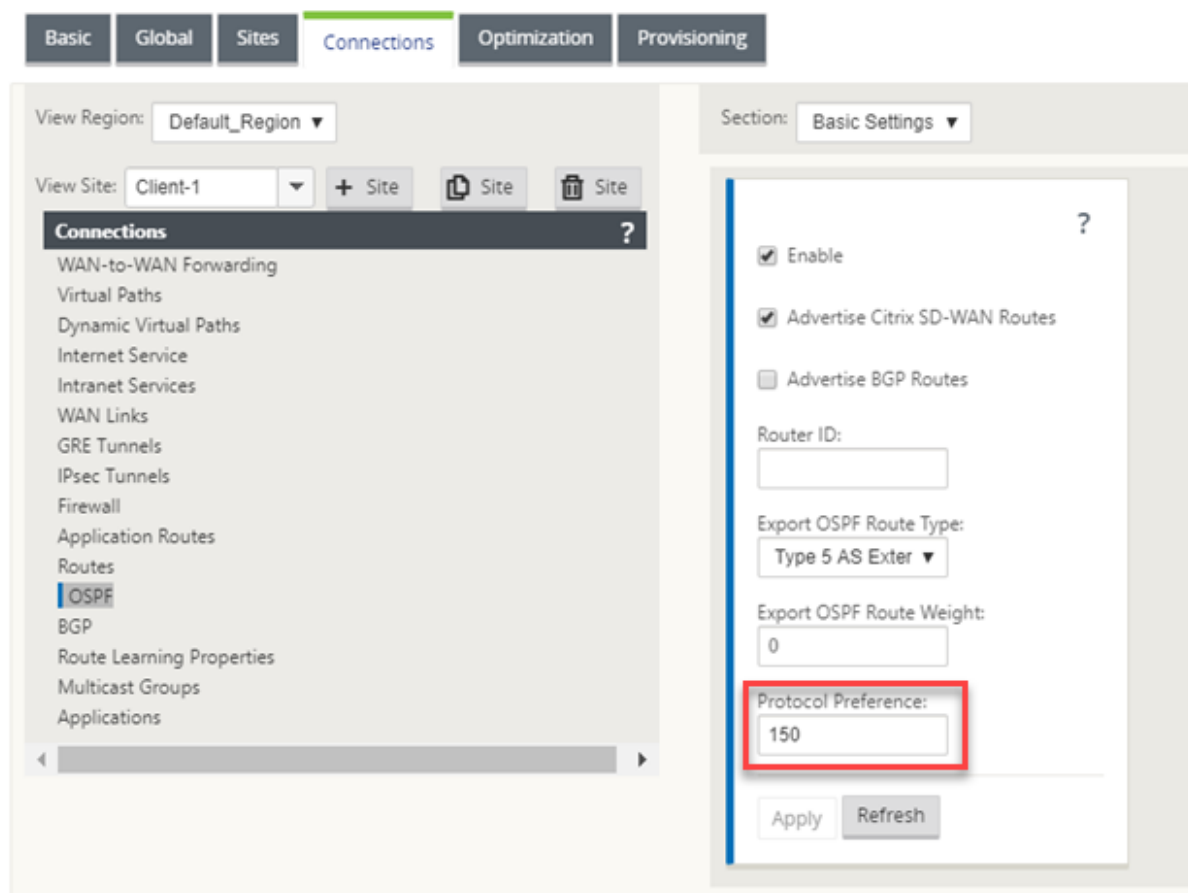
Lorsque Citrix SD-WAN apprend un préfixe d'itinéraire via des chemins virtuels, un protocole OSPF ou un protocole BGP, il suit l'ordre de préférence par défaut suivant.

- OSPF -150
- BGP - 100
- SD-WAN - 250

Le protocole avec l'ordre de préférence le plus élevé est le protocole préféré. Route utilisant le protocole avec la valeur de préférence de protocole la plus élevée

Vous pouvez également choisir d'utiliser le protocole BGP sur le protocole OSPF en définissant la valeur de préférence de protocole, tout en configurant le protocole BGP ou OSPF. Vous pouvez spécifier une préférence comprise entre 100 et 200.

Les informations de priorité de protocole sont locales à l'appliance Citrix SD-WAN et ne sont pas annoncées aux éléments réseau homologues.



Routage multidiffusion

May 6, 2021

Le routage multidiffusion permet une distribution efficace du trafic un-à-plusieurs. Une source de multidiffusion envoie le trafic de multidiffusion dans un seul flux vers un groupe de multidiffusion. Le groupe de multidiffusion contient des récepteurs tels que des hôtes et des routeurs adjacents qui utilisent le protocole IGMP pour la communication multidiffusion. La voix sur IP, la vidéo à la demande, la télévision IP et la vidéoconférence sont quelques-unes des technologies courantes qui utilisent le routage multidiffusion. Lorsque vous activez le routage de multidiffusion sur l'apppliance Citrix SD-WAN, l'apppliance agit comme un routeur de multidiffusion.

Multidiffusion spécifique à la source

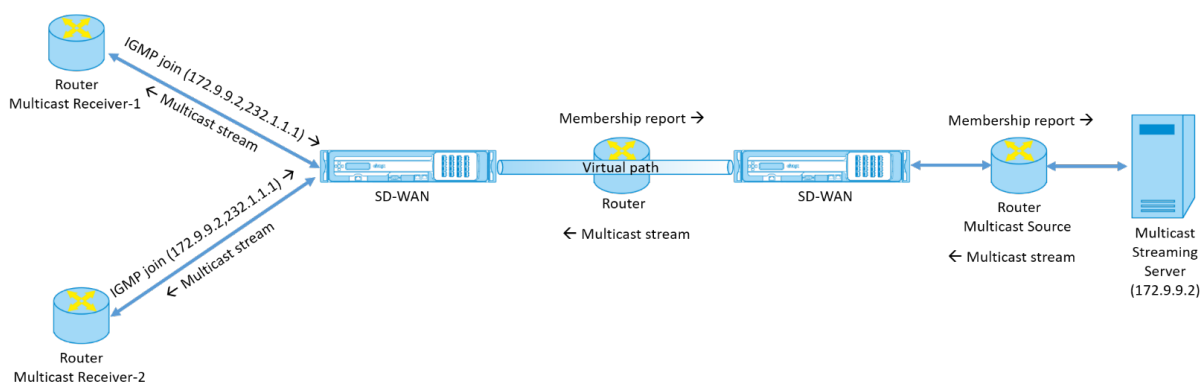
Les protocoles de multidiffusion permettent généralement aux récepteurs de multidiffusion de recevoir du trafic de multidiffusion à partir de n'importe quelle source. Avec la multidiffusion spéci-

fique à la source (SSM), vous pouvez spécifier la source à partir de laquelle les récepteurs reçoivent le trafic de multidiffusion. Il garantit que les récepteurs ne sont pas des écouteurs ouverts pour chaque source qui envoie des flux de multidiffusion, mais plutôt écouter une source de multidiffusion particulière. SSM réduit le coût des ressources utilisées pour consommer le trafic de toutes les sources possibles et fournit également une couche de sécurité en veillant à ce que les récepteurs reçoivent le trafic d'un expéditeur connu.

La topologie suivante montre deux récepteurs de multidiffusion sur un site de succursale et un serveur de multidiffusion (172.9.9.2) dans le centre de données. Le serveur de multidiffusion diffuse le trafic sur un groupe particulier (232.1.1.1), les récepteurs rejoignent le groupe. Tout trafic diffusé sur le groupe de multidiffusion est relayé à tous les récepteurs qui ont rejoint le groupe.

Remarque

Pour que SSM fonctionne, l'IP du groupe de multidiffusion doit se situer dans la plage 232.0.0.0/8.



1. Les récepteurs de multidiffusion envoient une demande de jointure IGMP IP indiquant que les récepteurs souhaitent rejoindre le groupe de multidiffusion et recevoir le flux de multidiffusion à partir de la source. La jointure IGMP comprend 2 attributs la source et le groupe de multidiffusion (S, G). IGMP Version 3 est utilisé pour SSM sur la source de multidiffusion et le récepteur pour relayer certaines adresses source spécifiques INCLUDE. SSM permet aux récepteurs de recevoir explicitement des flux de serveurs Multicast spécifiques, dont l'adresse source est explicitement fournie par les récepteurs dans le cadre de la requête JOIN. Dans cet exemple, une demande de jointure IGMP v3 est déclenchée avec une liste de sources d'inclusion explicite, qui contient la source 172.9.9.2, comme adresse qui envoie le flux de multidiffusion sur le groupe 232.1.1.1.
2. Le Citrix SD-WAN de la succursale écoute toutes les demandes IGMP de ces récepteurs et le convertit en rapport d'appartenance et l'envoie via le chemin virtuel à l'appliance SD-WAN du centre de données.
3. L'appliance Citrix SD-WAN du centre de données reçoit le rapport d'appartenance sur le chemin

virtuel et le transfère à la source de multidiffusion, établissant ainsi un canal de contrôle.

4. La source de multidiffusion transmet le flux de multidiffusion sur le chemin virtuel aux récepteurs de multidiffusion.

Le trafic de canal de contrôle et le flux de multidiffusion traversent le chemin virtuel établi entre la succursale et le centre de données. Le chemin de superposition Citrix SD-WAN assure et isole le trafic multidiffusion contre la dégradation du WAN ou les suppositions de liaison.

Configurer la multidiffusion

Pour configurer la multidiffusion, effectuez les opérations suivantes sur l'apppliance SD-WAN à la source et à la destination.

1. Créer un groupe de multidiffusion : indiquez un nom et une adresse IP pour le groupe de multidiffusion. L'IP du groupe de multidiffusion doit se situer dans la plage 232.0.0.0/8 pour la multidiffusion spécifique à la source.
2. Activer le proxy IGMP : vous pouvez configurer l'apppliance Citrix SD-WAN en tant que proxy IGMP pour transporter les informations de canal de contrôle IGMP pour le routage multidiffusion. IGMP V3 est requis pour la multidiffusion à source unique.
3. Définir les services en amont et en aval - Une interface en amont permet à l'IGMP PROXY de se connecter à l'apppliance SD-WAN plus proche de la source de multidiffusion réelle qui diffuse le trafic. Une interface en aval permet au proxy IGMP de se connecter aux hôtes qui sont plus éloignés de la source de multidiffusion réelle qui diffuse le trafic.
Les services en amont et en aval sont différents pour l'apppliance à la source et l'apppliance à la destination

Pour configurer la multidiffusion sur l'apppliance Citrix SD-WAN, accédez à **Connexions > Groupes de multidiffusion**. Créez un groupe de multidiffusion en fournissant un nom et une adresse IP pour le groupe de multidiffusion. Cliquez sur **Activer le proxy IGMP**.

Multicast Groups: Grp2 Section: Basic Settings

+ Group

Group

?

Group Name:
Grp2

Multicast Group IP:
232.1.1.1

☒ Enable IGMP Proxy

Apply

Revert

Configurez les chemins d'accès en amont et en aval pour les appliances de succursale et de centre de données.

Pour l'appliance plus proche du récepteur de multidiffusion (Branche), elle reçoit le trafic de multidiffusion sur l'interface Virtual Path Interface et envoie le trafic sur l'interface locale vers le récepteur.

Multicast Groups: Grp2 Section: Service

+ Group

Group

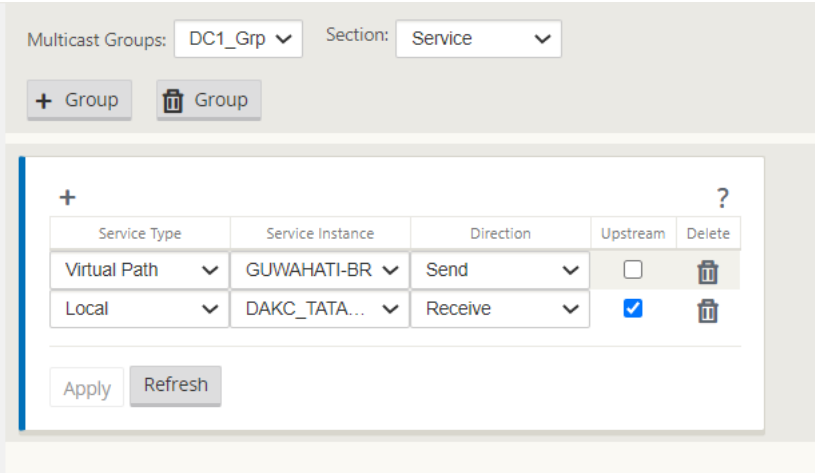
+ ?

Service Type	Service Instance	Direction	Upstream	Delete
Virtual Path	BANGALOR...	Receive	<input checked="" type="checkbox"/>	<div></div>
Local	DAKC_Airtel...	Send	<input type="checkbox"/>	<div></div>

Apply

Refresh

Pour l'appliance plus proche de la source de multidiffusion (centre de données), elle reçoit le trafic de multidiffusion sur l'interface locale et envoie le trafic sur l'interface Virtual Path Interface.



Surveillance

Statistiques IGMP

Lorsque les récepteurs de multidiffusion lancent une demande de groupe de jointure, vous pouvez voir les détails du récepteur sous **Surveillance > IGMP** sur l’appliance. Vous pouvez voir ces informations sur les appliances à la fois à la source et à la destination.

L’image suivante montre qu’une jointure IGMP Version 3 est initiée et que le type de filtre INCLUDE est utilisé pour inclure des adresses source spécifiques. Vous pouvez également voir les statistiques des membres de l’IGMP.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > IGMP

Filter/Purge

Refresh

Purge IGMP Group

Purge IGMP Stats

IGMP PROXY Groups

Max Groups to Display: 50 Service Type to Display: Refresh

Type	Name	Group	Filter	Version	Packets Sent	Bytes Sent
HOST	VIF-1-Bridge-1	232.1.1.1	INCLUDE	IGMPv3	4285	6418930

Total Groups Displayed: 1 out of 1

IGMP Stats

Max IGMP Stats to Display: 50 Stats Type to Display: MEMBER Refresh

Type	Description	Value
MEMBER	Add Member	1
MEMBER	Remove Member	0
MEMBER	Current Member	1

Total IGMP Stats Displayed: 3 out of 70

Configurer le coût de l'itinéraire du chemin virtuel

May 6, 2021

Citrix SD-WAN prend en charge les améliorations de routage suivantes liées à l'administration du datacenter.

Prenons par exemple le réseau SD-WAN avec deux centres de données, l'un en Amérique du Nord et l'autre en Europe. Vous souhaitez que tous les sites en Amérique du Nord acheminent le trafic via le datacenter en Amérique du Nord et tous les sites en Europe utilisent le datacenter Europe. Auparavant, dans SD-WAN 9.3 et versions antérieures, cette fonctionnalité d'administration du centre de données n'était pas prise en charge. Ceci est mis en œuvre avec l'introduction du coût de l'itinéraire de chemin virtuel.

- Coût d'itinéraire de chemin virtuel : Vous pouvez configurer le coût d'itinéraire de chemin

virtuel pour les chemins virtuels individuels ajoutés au coût d'itinéraire lorsqu'un itinéraire est appris à partir d'un site distant.

Cette fonctionnalité invalide ou supprime le coût de transfert WAN vers WAN.

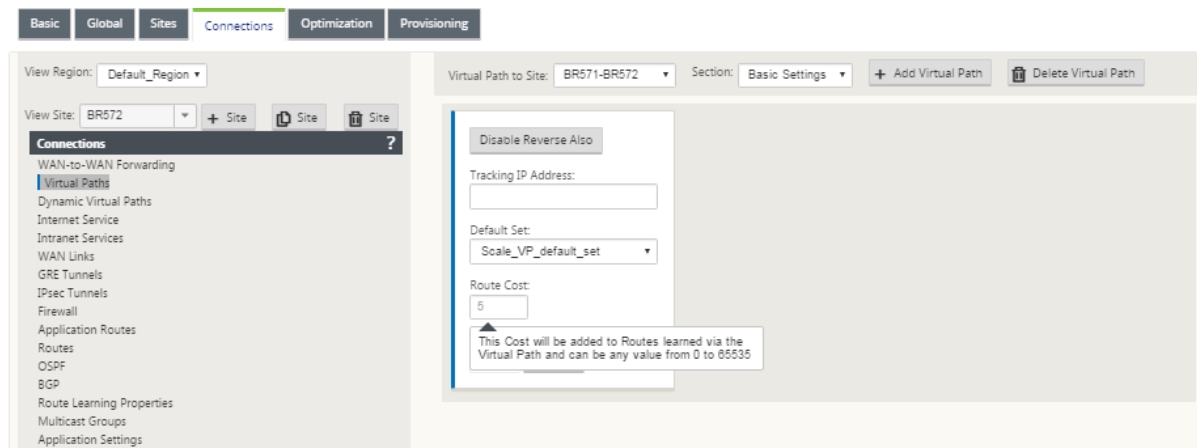
- **Coût d'itinéraire OSPF** : Vous pouvez désormais importer le coût d'itinéraire OSPF (métrique de type 1) en activant **Copier le coût d'itinéraire OSPF** dans les filtres d'importation. Le coût de l'itinéraire OSPF est pris en compte dans la sélection de l'itinéraire au lieu du coût SD-WAN. Le coût jusqu'à 65534 au lieu de 15 est pris en charge, mais il est conseillé de tenir compte d'un coût de route de chemin virtuel approprié qui est ajouté si l'itinéraire est appris à partir d'un site distant.
- **BGP - Coût VP vers MED** : Vous pouvez désormais copier le coût d'itinéraire de chemin virtuel pour les routes SD-WAN dans des valeurs MED BGP lors de l'exportation (redistribution) de routes SD-WAN vers des homologues BGP. Cela peut être défini pour des voisins individuels en créant une stratégie BGP et en l'appliquant dans la direction « OUT » pour chaque voisin.
- N'importe quel site peut avoir plusieurs chemins virtuels vers d'autres sites. Parfois, s'il existe une succursale vers laquelle il existe une connectivité aux services via plusieurs chemins virtuels, il peut y avoir deux chemins virtuels à partir du site Branch. Un chemin virtuel via DC1 et l'autre via DC2. DC1 peut être un MCN et DC2 peut être un Geo-MCN, et peut être configuré comme un autre site avec un chemin virtuel statique.
- Ajoutez un coût par défaut pour chaque VP en tant que 1. Le coût de l'itinéraire de chemin virtuel permet d'associer un coût à chaque chemin virtuel d'un site. Cela permet de manipuler les échanges/mises à jour d'itinéraire sur un chemin virtuel spécifique au lieu du coût du site par défaut. Avec cela, nous pouvons manipuler le centre de données à privilégier pour envoyer le trafic.
- Autoriser la configuration du coût dans une petite plage de valeurs (par exemple, 1 à 10) pour chaque VP.
- Le coût du chemin virtuel doit être ajouté à n'importe quel itinéraire partagé avec les sites voisins pour indiquer la préférence de routage, y compris les itinéraires appris via le routage dynamique.
- Aucun chemin virtuel statique ne doit avoir un coût inférieur à celui d'un chemin virtuel dynamique.

Remarque

Le coût de l'itinéraire VP déprécie le coût de transfert WAN vers WAN qui existait dans les versions antérieures à la version 10.0. Les décisions de routage basées sur les coûts de transfert WAN vers WAN doivent être renforcées en utilisant le coût d'acheminement VP car le coût de transfert WAN vers WAN n'a aucune importance lorsque vous migrez vers la version 10.0.

Comment configurer le coût d'itinéraire de chemin virtuel

Vous pouvez configurer Virtual Path Route dans l'interface graphique SD-WAN sous **Connexions > Afficher la région > Visualiser le site > Chemins virtuels > Paramètres de base**. Toutes les routes sont installées avec un coût Citrix SD-WAN de base + coût d'itinéraire VP pour influencer les coûts d'itinéraire sur plusieurs chemins virtuels.



Cas d'utilisation :

Par exemple, il existe des sous-réseaux 172.16.2.0/24 et 172.16.3.0/24. Supposons qu'il existe deux centres de données DC1 et DC2 qui utilisent ces deux sous-réseaux pour transmettre le trafic vers SD-WAN. Avec le coût d'itinéraire de chemin virtuel par défaut, vous ne pouvez pas influencer le routage car il dépend de la route qui a été installée en premier, il peut être soit le DC2 en premier ou le DC1 suivant.

Avec le chemin virtuel, vous pouvez influencer spécifiquement le chemin virtuel DC2 pour avoir un coût d'itinéraire de chemin virtuel plus élevé (par exemple, 10) tandis que DC1 a le coût d'itinéraire VP par défaut de 5. Cette manipulation permet d'installer des routes avec DC1 d'abord et DC2 ensuite pour les deux.

Vous pouvez avoir quatre routes, deux routes vers 172.16.2.0/24 ; une via DC1 avec un coût inférieur, puis via DC2 avec un coût plus élevé, et 2 autres pour 172.16.3.0/24.

Surveillance et dépannage

La table de routage indique comment les mêmes sous-réseaux annoncés par deux sites connectés à un site de succursale sur le chemin virtuel sont installés avec priorité de coût avec l'ajout de coût d'itinéraire de chemin virtuel.

Pour vérifier le coût de l'itinéraire et les itinéraires utilisés dans la table de routage, accédez à **Surveillance > Statistiques** sous le champ **Afficher**, sélectionnez **Itinéraires**. Les coûts d'itinéraire et le nombre d'accès peuvent être vérifiés sur la même page.

La figure suivante montre la table des itinéraires avec deux coûts différents pour la même route qui est 172.16.6.0/24 avec coût 10 et 11 pour les services **DC-Branch01** et **GeomCN-Branch01** respectivement.

Monitoring > Statistics

Statistics

Show: Routes ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh

Routing Domain: <ALL>

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 18 of 18 entries

First Previous 1

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
<input type="checkbox"/>	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
<input type="checkbox"/>	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
<input type="checkbox"/>	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
<input type="checkbox"/>	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
<input type="checkbox"/>	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
<input type="checkbox"/>	11	172.16.4.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A

Configurer le protocole de redondance du routeur virtuel

May 6, 2021

Virtual Router Redundancy Protocol (VRRP) est un protocole largement utilisé qui fournit la redondance de périphérique pour éliminer le point de défaillance unique inhérent à l'environnement statique routé par défaut. VRRP vous permet de configurer deux routeurs ou plus pour former un groupe. Ce groupe apparaît comme une passerelle par défaut unique avec une adresse IP virtuelle et une adresse MAC virtuelle.

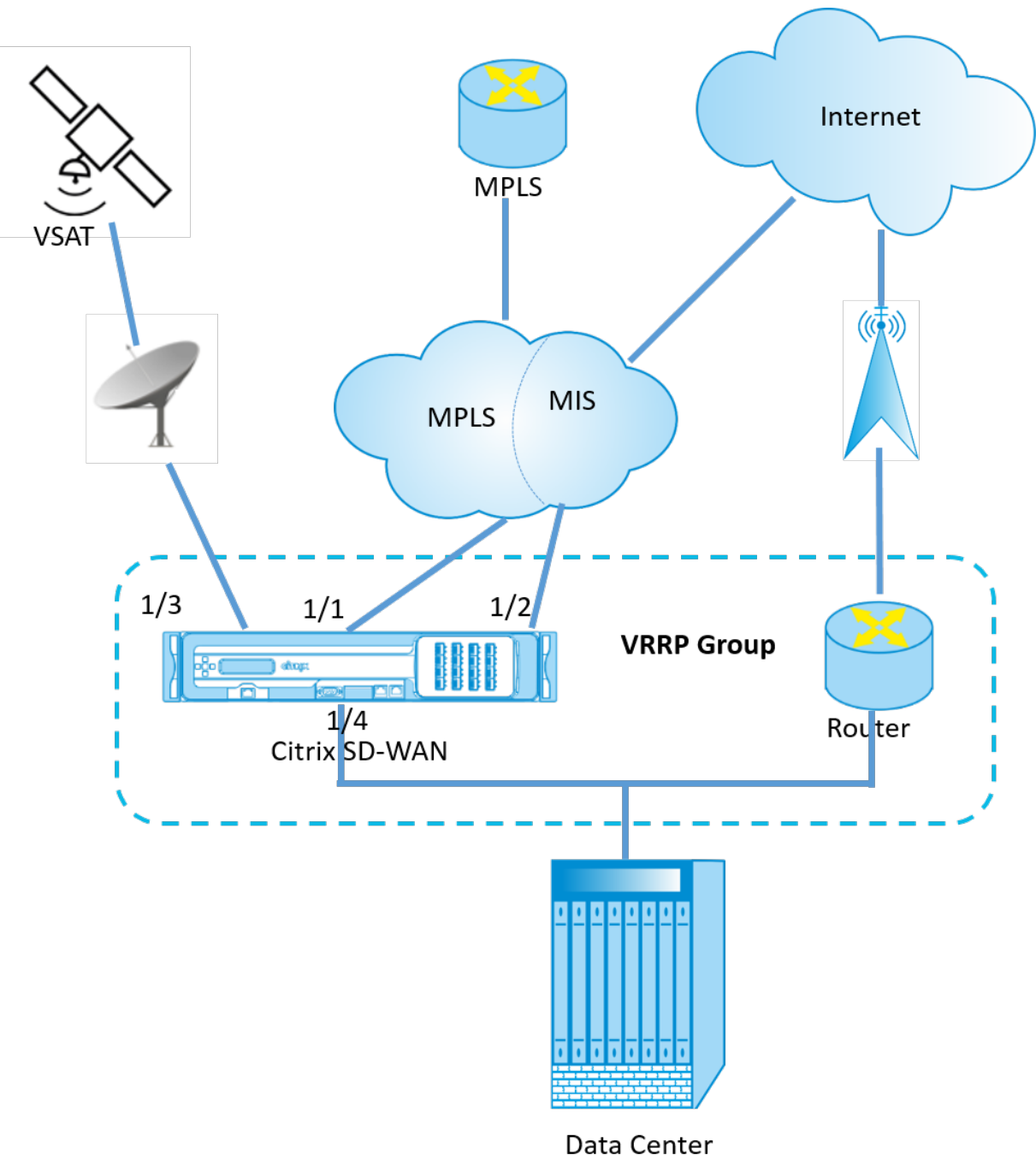
Un routeur de sauvegarde prend automatiquement le relais en cas de défaillance du routeur principal/maître. Dans une configuration VRRP, le routeur maître envoie un paquet VRRP connu sous le nom de publicité aux routeurs de sauvegarde. Si le routeur maître cesse d'envoyer la publicité, le routeur de sauvegarde définit le minuteur d'intervalle. Si aucune annonce n'est reçue pendant cette période de blocage, le routeur de sauvegarde lance la routine de basculement.

VRRP spécifie un processus d'élection dans lequel, le routeur ayant la priorité la plus élevée devient le maître. Si la priorité est la même parmi les routeurs, le routeur avec l'adresse IP la plus élevée devient le maître. Les autres routeurs sont en état de sauvegarde. Le processus d'élection est relancé si le maître échoue, un nouveau routeur rejoint le groupe ou un routeur existant quitte le groupe.

VRRP garantit un chemin par défaut de haute disponibilité sans configurer les protocoles de routage dynamique ou de découverte de routeurs sur chaque hôte final.

Citrix SD-WAN version 10.1 prend en charge les versions 2 et 3 de VRRP pour interagir avec tous les routeurs tiers. L'appliance SD-WAN agit comme un routeur maître et dirige le trafic vers l'utilisation du service de chemin virtuel entre les sites. Vous pouvez configurer l'appliance SD-WAN en tant que maître VRRP en configurant l'IP de l'interface virtuelle en tant qu'IP VRRP et en définissant manuellement la priorité sur une valeur supérieure à celle des routeurs homologues. Vous pouvez configurer l'intervalle de publication et l'option preempt.

Le diagramme de réseau ci-dessous montre une appliance Citrix SD-WAN et un routeur configurés en tant que groupe VRRP. L'appliance SD-WAN est configurée pour être le maître. Si l'appliance SD-WAN tombe en panne, le routeur de sauvegarde prend le relais en quelques millisecondes, ce qui garantit qu'il n'y a pas de temps d'arrêt.



Pour configurer l'instance VRRP :

1. Dans l'Éditeur de configuration, accédez à **Sites > Nom du site > VRRP** et cliquez sur **+**.

+	VRRP Group ID	Version	Priority	Advertisement Interval	Authentication type	Authentication text	Reclaim	Use Check
+	245	V3	255	1000	*	None	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Apply Revert								

1. Configurez une instance VRRP. Entrez les valeurs des champs suivants :

- **ID du groupe VRRP : ID** du groupe VRRP. L'ID de groupe doit être une plage de valeurs comprise entre 1 et 255. Le même ID de groupe doit également être configuré sur les routeurs de sauvegarde.

Remarque

Actuellement, vous pouvez configurer jusqu'à quatre groupes uniquement.

- **Version : Version** du protocole VRRP. Vous pouvez choisir entre le protocole VRRP V2 et V3.
- **Priorité** : priorité de l'appliance Citrix SD-WAN pour le groupe VRRP. La plage de priorités est de 1 à 254. Définissez cette valeur sur 254 maximum pour faire de l'appliance SD-WAN le maître.

Remarque

Si le routeur est le propriétaire de l'adresse IP VRRP, la priorité est définie sur 255 par défaut.

- **Publicité Interval** : Fréquence en millisecondes, avec laquelle les annonces VRRP sont envoyées lorsque l'appliance SD-WAN est le maître. L'intervalle de publication par défaut est d'une seconde.
- **Type d'authentification** : Vous pouvez choisir **Texte brut** pour entrer une chaîne d'authentification. La chaîne d'authentification est envoyée sous forme de texte brut sans cryptage dans les annonces VRRP. Choisissez **Aucun** si vous ne souhaitez pas configurer l'authentification.
- **Texte d'authentification** : chaîne d'authentification à envoyer dans l'annonce VRRP. Cette option est activée si le **Type d'authentification** est **Texte brut**.

Remarque

L'authentification est prise en charge uniquement dans vRRPV2.

- **Réclame** : active la préemption lorsque la priorité de l'appliance SD-WAN est la plus élevée dans le groupe VRRP. Ceci est utilisé dans le processus d'élection du VRRP.
- **Utiliser V2 Checksum** : permet la compatibilité avec les périphériques réseau tiers pour VRRPV3. Par défaut, VRRPV3 utilise la méthode de calcul de somme de contrôle v3. Certains périphériques tiers peuvent uniquement prendre en charge le calcul de la somme de contrôle VRRPV2. Dans de tels cas, activez cette option.

Configurez l'adresse IP VRRP. Entrez des valeurs pour les champs suivants et cliquez sur **Appliquer**.

- **Interface virtuelle** : interface virtuelle à utiliser pour VRRP. Choisissez l'une des interfaces virtuelles configurées.
- **Adresse IP virtuelle** : adresse IP virtuelle attribuée à l'interface virtuelle. Choisissez l'une des adresses IP virtuelles configurées pour l'interface virtuelle.

- **IP du routeur VRRP** : adresse IP du routeur virtuel du groupe VRRP. Par défaut, l'adresse IP virtuelle de l'appliance SD-WAN est affectée en tant qu'adresse IP du routeur virtuel.

VRRP Group ID	Version	Priority	Advertisement Interval	Authentication type	Authentication text	Reclaim	Use V2 Checksum
245	V3	255	1000	None		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Router IPs

Virtual Interface	Virtual IP Address	VRRP Router IP	Delete
VirtualInterface-1	172.16.2.100/24	172.16.2.100	<input type="button" value="Delete"/>

Statistiques VRRP

Vous pouvez afficher les statistiques VRRP sous **Surveillance > Protocole VRRP**.

Dashboard	Monitoring	Configuration
Statistics	Monitoring > VRRP Protocol	
Flows		
Routing Protocols		
Firewall		
IKE/IPsec		
Performance Reports		
Qos Reports		
Usage Reports		
Availability Reports		
Appliance Reports		
DHCP Server/Relay		
VRRP Protocol		

VRRP ID	Version	Interface(s)	State	Priority	Virtual Router IP	Advertisement Interval	Enable	Disable
20	2	LAN-7	Master	250	172.58.7.100	2000	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>
245	3	LAN	Master	200	172.58.5.20	1000	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>

Vous pouvez afficher les données statistiques suivantes :

- **IDVRRP : ID** du groupe VRRP
- **Version : Version** du protocole VRRP.
- **Interface** : Interface virtuelle utilisée pour VRRP.
- **État : état** VRRP de l'appliance SD-WAN. Il indique si l'appliance est un maître ou une sauvegarde.
- **Priorité** : priorité de l'appliance SD-WAN pour un groupe VRRP
- **IP du routeur virtuel** : adresse IP du routeur virtuel pour le groupe VRRP.
- **Intervalle de publicité** : fréquence des annonces VRRP.
- **Activer** : sélectionnez cette option pour activer l'instance VRRP sur l'appliance SD-WAN.
- **Désactiver** : sélectionnez cette option pour désactiver l'instance VRRP sur l'appliance SD-WAN.

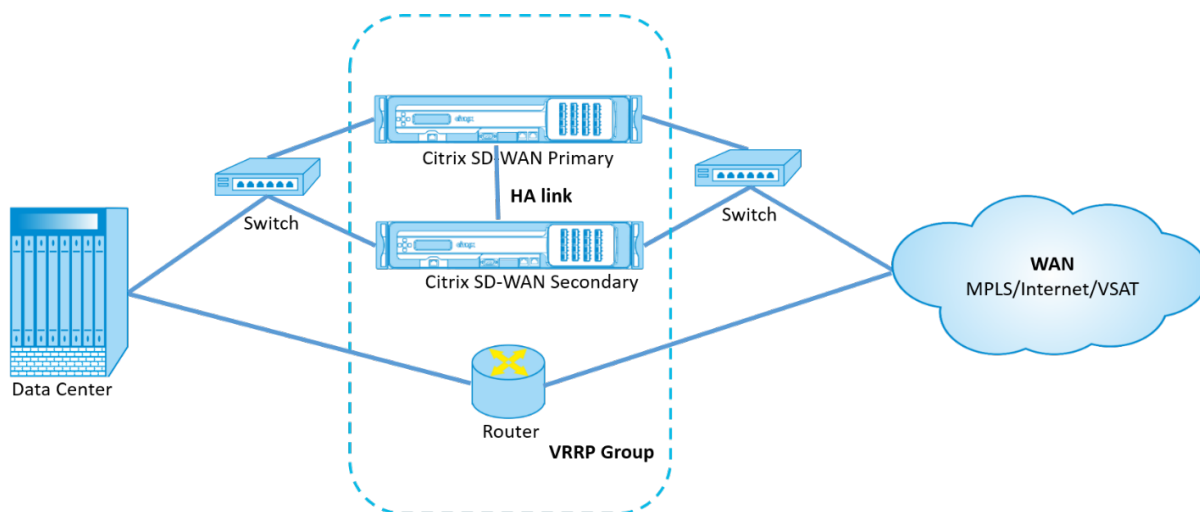
Limitations

- VRRP est pris en charge dans le déploiement en mode passerelle uniquement.

- Vous pouvez configurer jusqu'à quatre ID VRRP (VRID).
- Jusqu'à 16 interfaces réseau virtuelles peuvent participer à VRID.

Haute disponibilité et VRRP

Vous pouvez réduire considérablement les temps d'arrêt du réseau et les perturbations du trafic en tirant parti des fonctionnalités de haute disponibilité et de VRRP de votre réseau SD-WAN. Déployez une paire d'appliances Citrix SD-WAN dans des rôles actif/de secours ainsi qu'un routeur de secours pour former le groupe VRRP. Ce groupe apparaît comme une passerelle par défaut unique avec une adresse IP virtuelle et une adresse MAC virtuelle.



Voici 2 cas avec le déploiement ci-dessus :

1er cas : la minuterie de basculement haute disponibilité sur SD-WAN est égale à la minuterie de basculement VRRP.

Le comportement attendu est le basculement à haute disponibilité avant le basculement VRRP, c'est-à-dire que le trafic continue de circuler à travers la nouvelle appliance Active SD-WAN. Dans ce cas, SD-WAN continue avec le rôle maître VRRP.

2ème cas : minuteur de basculement haute disponibilité sur SD-WAN supérieur au minuteur de basculement VRRP.

Le comportement attendu est que le basculement VRRP vers le routeur se produit, c'est-à-dire que le routeur devient VRRP Master et le trafic peut momentanément circuler à travers le routeur, en contournant l'appliance SD-WAN.

Mais une fois le basculement à haute disponibilité effectué, le SD-WAN redevient VRRP Master, c'est-à-dire que le trafic passe désormais par la nouvelle appliance SD-WAN active.

Pour plus d'informations sur les modes de déploiement haute disponibilité, reportez-vous à la section [Haute disponibilité](#).

Configurer les objets réseau

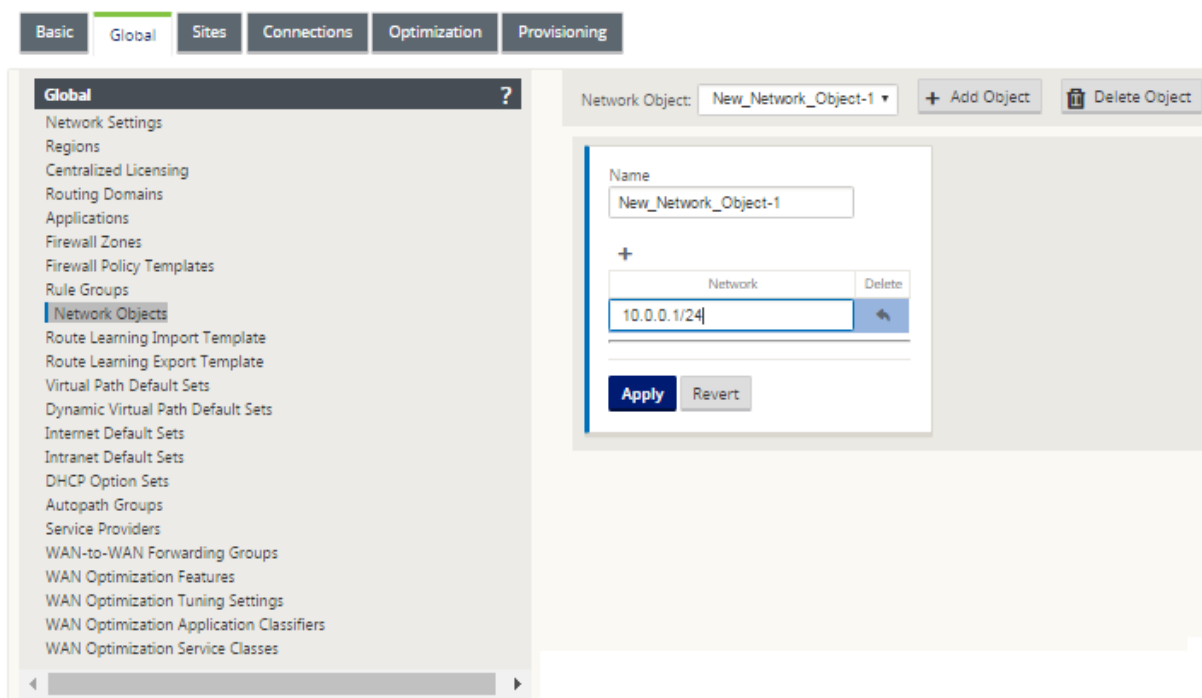
May 6, 2021

Citrix SD-WAN introduit la possibilité d'ajouter des objets réseau sous le panneau **Global** dans l'Éditeur de configuration. Vous pouvez regrouper plusieurs sous-réseaux et référencer un seul objet réseau lors de la définition d'un filtre de routage plutôt que de créer un filtre pour chaque sous-réseau.

Pour configurer les objets réseau :

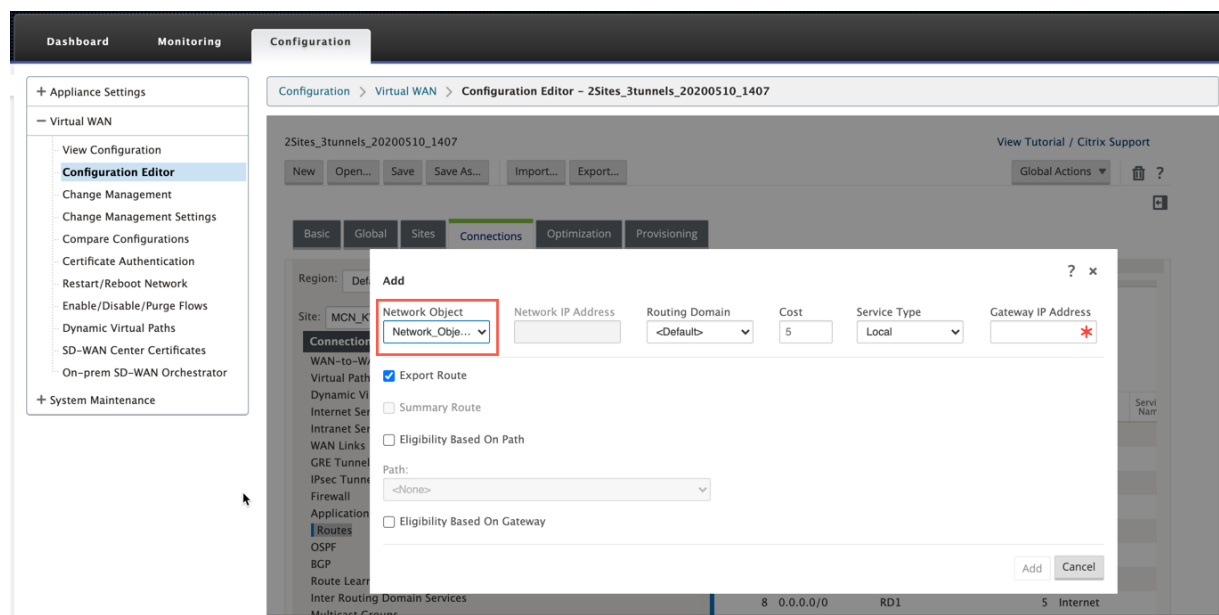
1. Dans l'**Éditeur de configuration**, accédez à **Global** → **Objets réseau**, cliquez sur **Ajouter (+)**.
2. Cliquez sur **Ajouter (+)** sous Réseaux.
3. Entrez l'**adresse IP** et le **sous-réseau** du nouvel objet réseau.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Pour modifier le nom de l'objet réseau, cliquez sur le nom de l'objet réseau et entrez un nouveau nom.

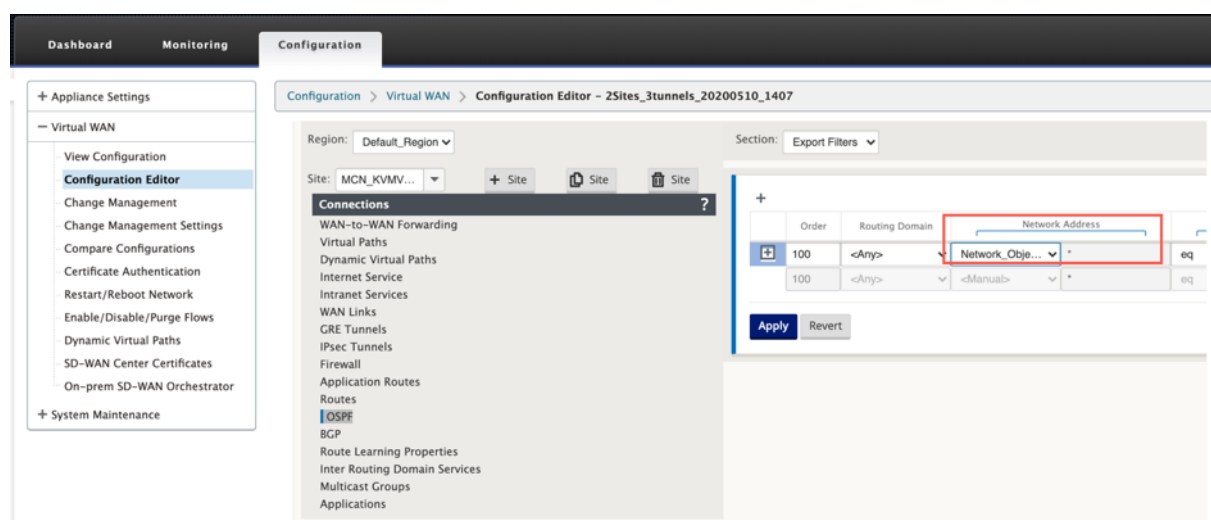


Les fonctionnalités suivantes utilisent les objets réseau :

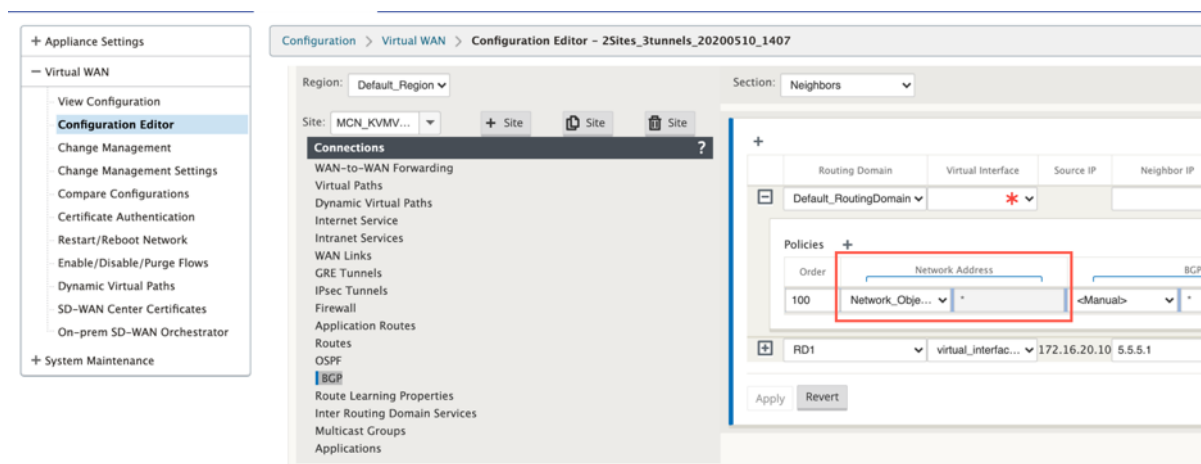
- Itinéraires (**Éditeur de configuration** > **Connexions** > **Itinéraires** > Cliquez + > **Objet réseau**)



- Filtres d'importation et d'exportation BGP et OSPF (**Éditeur de configuration > Connexions > BGP/OSPF > Filtres d'exportation/importation** cliquez + > **Adresse réseau**)



- Stratégies de voisinage BGP (**Éditeur de configuration > Connexions > BGP > Voisins > Stratégies** cliquez + > **Adresse réseau**)



Prise en charge du routage pour la segmentation LAN

May 6, 2021

Les appliances SD-WAN Standard et Premium (Enterprise) Edition implémentent la segmentation LAN sur des sites distincts où l'une ou l'autre des appliances est déployée. Les appliances reconnaissent et tiennent à jour un enregistrement des VLAN côté LAN disponibles, et configurent des règles autour de quels autres segments LAN (VLAN) peuvent se connecter à un emplacement distant avec une autre appliance SD-WAN Standard ou Premium (Enterprise) Edition.

La fonctionnalité ci-dessus est implémentée à l'aide d'une table VRF (Virtual Routing and Forwarding) gérée dans l'appliance SD-WAN Standard ou Premium (Enterprise) Edition, qui assure le suivi des plages d'adresses IP distantes accessibles à un segment LAN local. Ce trafic VLAN-VLAN traverserait toujours le WAN par le même chemin virtuel préétabli entre les deux appliances (aucun nouveau chemin n'a besoin d'être créé).

Un exemple de cas d'utilisation de cette fonctionnalité est qu'un administrateur WAN peut être en mesure de segmenter l'environnement réseau de succursales locales via un VLAN et fournir certains de ces segments (VLAN) accès aux segments LAN côté DC qui ont accès à Internet, tandis que d'autres peuvent ne pas obtenir un tel accès. La configuration des associations VLAN-VLAN est réalisée via l'éditeur de configuration du MCN dans l'interface Web de gestion SD-WAN.

Service de domaine d'interroulage

May 6, 2021

Citrix SD-WAN vous permet de segmenter le réseau à l'aide des domaines de routage, assurant ainsi une sécurité élevée et une gestion facile. Avec l'utilisation du domaine de routage, le trafic est isolé l'un de l'autre dans le réseau de superposition. Chaque domaine de routage conserve sa propre table de routage. Pour plus d'informations sur le domaine de routage, consultez [Domaine de routage](#).

Cependant, nous avons parfois besoin d'acheminer le trafic entre les domaines de routage. Par exemple, si des services partagés tels que l'imprimante, l'analyseur et le serveur de messagerie sont provisionnés en tant que domaine de routage distinct. Le domaine d'inter-routage est requis pour permettre aux utilisateurs de différents domaines de routage d'accéder aux services partagés.

Citrix SD-WAN fournit le service de domaine inter-routage statique, ce qui permet la fuite d'itinéraire entre les domaines de routage au sein d'un site ou entre différents sites. Cela élimine le besoin d'un routeur de bord pour gérer les fuites de route. Le service de domaine d'inter-routage peut également être utilisé pour configurer des itinéraires, des stratégies de pare-feu et des règles NAT.

Une nouvelle zone de pare-feu, **Inter_Routing_Domain_Zone**, est créée par défaut et sert de zone de pare-feu pour les services de domaine inter-routage pour le routage et le filtrage.

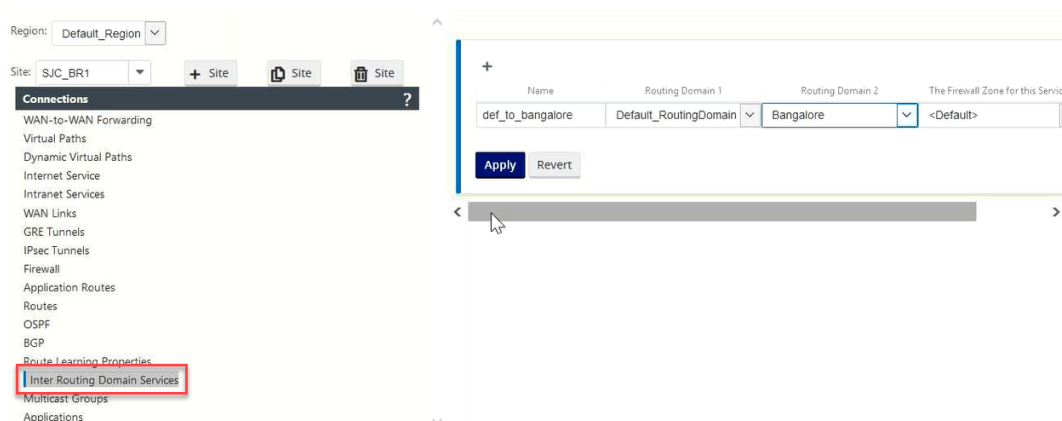
Remarque

Les appliances Citrix SD-WAN PE n'effectuent pas de fonctionnalité d'optimisation WAN sur les paquets de domaine inter-routage.

Pour configurer le service de domaine d'inter-routage entre deux domaines de routage.

Considérez un réseau SD-WAN avec un MCN et 2 branches ou plus avec au moins deux domaines de routage configurés globalement. Par défaut, tous les domaines de routage sont activés sur le MCN. Activez sélectivement les domaines de routage requis sur les autres sites. Pour plus d'informations sur la configuration du domaine de routage, consultez [Configuration du domaine de routage](#).

1. Dans l'Éditeur de configuration SD-WAN, accédez à **Connexions** > Sélectionnez Site > **Service de domaine inter-routage**.
2. Cliquez sur **+** et entrez des valeurs pour les paramètres suivants :
 - **Nom** : Nom du service de domaine inter-routage.
 - **Domaine de routage 1** : premier domaine de routage de la paire.
 - **Domaine de routage 2** : deuxième domaine de routage de la paire.
 - **Zone de pare-feu** : Zone de pare-feu du service.
 - Par défaut : la zone de pare-feu `Inter_Routing_Domain_Zone` est affectée.
 - Aucun : Aucune zone n'est sélectionnée et la zone d'origine du paquet est conservée.
 - Toutes les zones configurées dans le réseau peuvent être sélectionnées.

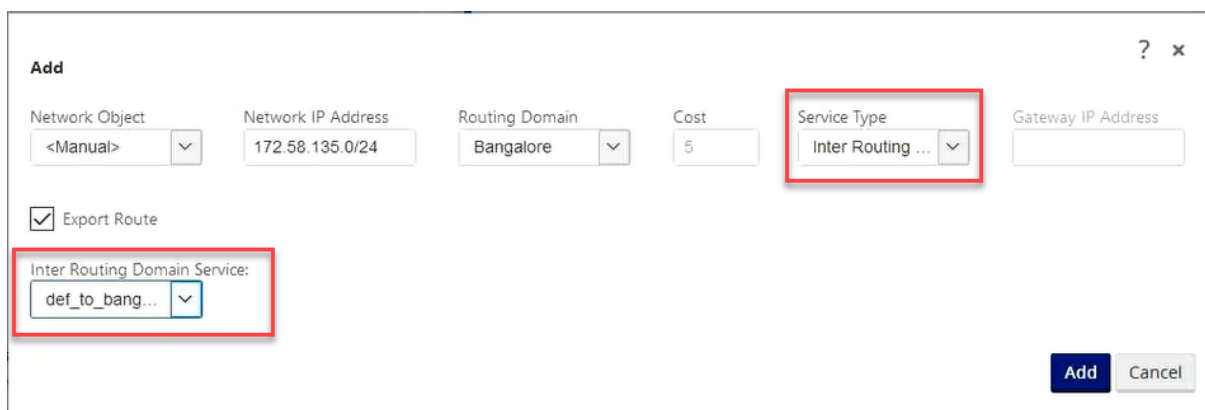


1. Cliquez sur **Appliquer** pour créer le service de domaine inter-routage. Le service créé peut être utilisé pour créer des itinéraires, des stratégies de pare-feu et des stratégies NAT.

Remarque

Vous ne pouvez pas configurer un service de domaine inter-routage à l'aide de domaines de routage qui ne sont pas activés sur un site.

Pour créer des routes à l'aide du service de domaine inter-routage, créez un itinéraire avec le **type de service** en tant que **service de domaine inter-routage** et sélectionnez le service de domaine inter-routage. Pour plus d'informations sur la configuration des itinéraires, reportez-vous à la section [Comment configurer des itinéraires](#).



Ajoutez également une route à partir de l'autre paire de domaines de routage, pour établir une connexion entre les deux domaines de routage.

Vous pouvez également configurer des stratégies de pare-feu pour contrôler le flux de trafic entre les domaines de routage. Dans les stratégies de pare-feu, sélectionnez Service de domaine Inter-routage pour les services source et de destination et sélectionnez l'action de pare-feu requise. Pour plus d'informations sur la configuration des stratégies de pare-feu, consultez [Stratégies](#).

Default_LAN_Zone

Internet_Zone

Untrusted_Internet_Zone

☐

☐

☐

☐

☐

☐

☐

☐

☐

Default_LAN_Zone

Internet_Zone

Untrusted_Internet_Zone

☐

☐

☐

☐

☐

☐

☐

☐

☐

Routing Domain

Any

Traffic Match Type:

IP Protocol

IP Protocol:

Any

DSCP:

Any

☐ Match Established

Application:

Application Family:

Application Objects:

Any

Source Service Type:

Inter Routing Domain

Source Service Name:

def_to_bangalore

Source IP:

*

Source Port:

*

Dest Service Type:

Inter Routing Domain

Dest Service Name:

def_to_bangalore

Dest IP:

*

Dest Port:

*

Actions

Action:

Allow

☒ Allow Fragments

Connection State Tracking:

Use Site Setting

Drop

Reject

Count and Continue

☐ Log Start

☐ Log End

☐ Add Reverse Policy

Vous pouvez également choisir le type de service Intranet pour configurer les stratégies NAT statiques et dynamiques. Pour plus d'informations sur la configuration des stratégies NAT, reportez-vous à la section [Traduction d'adresses réseau](#).

Add

Priority:

100

Routing Domain:

Direction:

Outbound

Type:

Port Restricted

Service Type:

Inter Routing ...

Service Name:

def_to_bang...

Inside Zone:

Any

Inside IP Address:

*

Outside IP Address:

*

☐ Allow Related

☐ IPsec Passthrough

☐ GRE/PPTP Passthrough

☐ Port Parity

☐ Bind Responder Route

Port Forwarding Rules

Routing Domain

Protocol

Outside Port

Inside IP Address

Inside Port

Fragments

Log Interval (s)

Log Start

Log End

Connection State Tracking

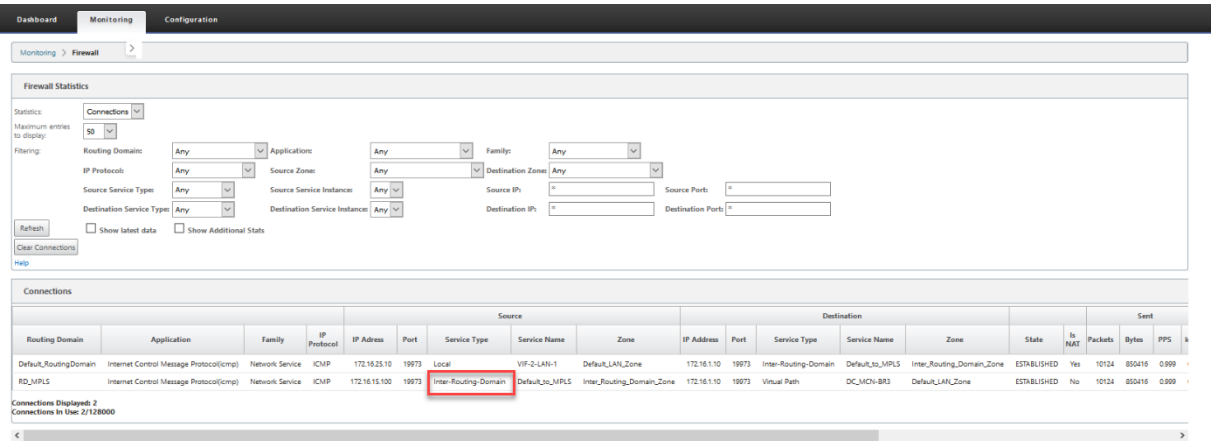
Delete

Add

Cancel

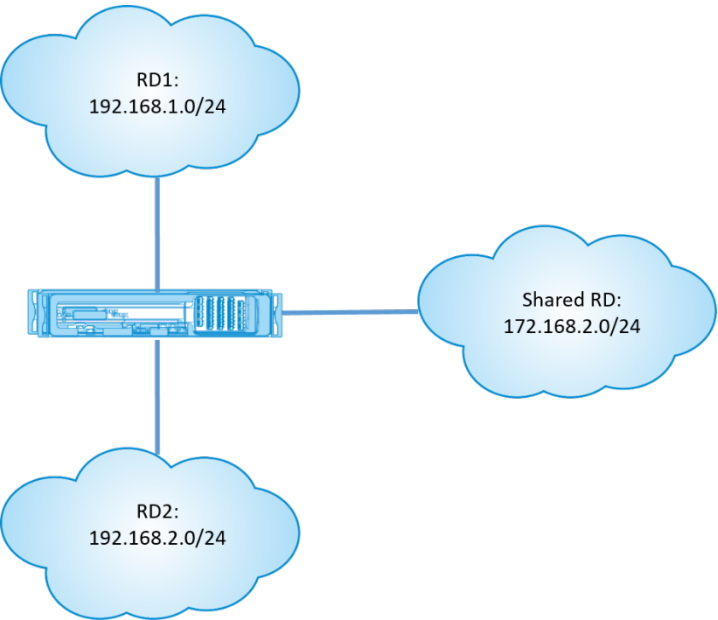
Surveillance

Vous pouvez afficher les statistiques de surveillance des connexions qui utilisent des services inter-routing-domaine sous **Surveillance > Statistiques de pare-feu > Connexions**.



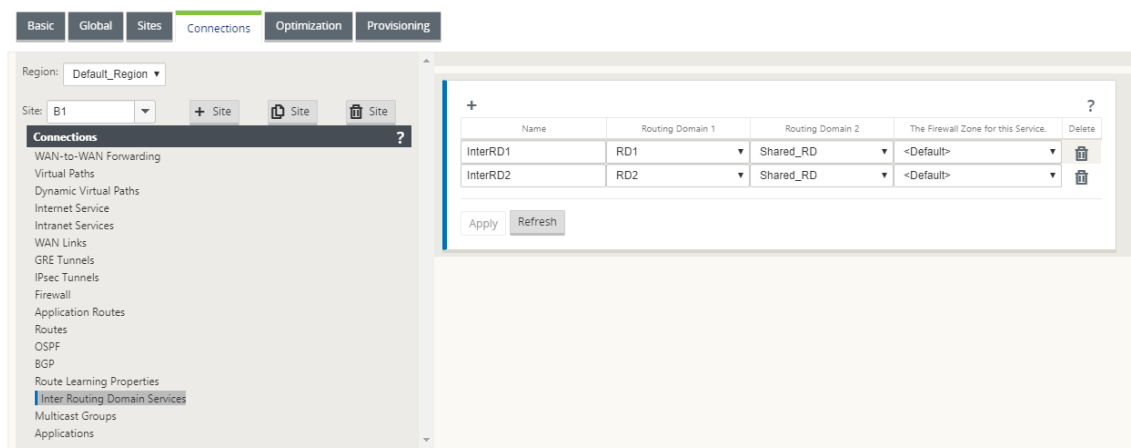
Cas d'utilisation : partage de ressources entre les domaines de routage

Considérons un scénario, dans lequel les utilisateurs dans différents domaines de routage ont besoin d'accéder à des actifs communs, tels qu'une imprimante ou un stockage réseau. Il existe 3 domaines de routage dans une branche RD1, RD2 et Bureau à distance partagé, comme illustré dans la figure.



Pour permettre aux utilisateurs dans RD1 et RD2 d'accéder aux ressources dans le Bureau à distance partagé :

1. Créez un service de domaine inter-routage entre RD1 et Shared Bureau à distance, par exemple **Inter RD1**.
2. Créez un service de domaine inter-routage entre RD2 et Bureau à distance partagée, par exemple **Inter RD2**.



3. Configurez une route statique vers le Bureau à distance partagé à partir de RD1 et RD2. Dans RD1, ajoutez une route 172.168.2.0/24 à InterRD1.

Add ? x

Network Object	Network IP Address	Routing Domain	Cost	Service Type	Gateway IP Address
<Manual>	172.168.2.0/24	RD1	5	Inter Routing Dor	

☒ Export Route

Inter Routing Domain Service:

InterRD1

Add Cancel

4. Dans RD2, ajoutez une route 172.168.2.0/24 à InterRD2.

Add ? x

Network Object	Network IP Address	Routing Domain	Cost	Service Type	Gateway IP Address
<Manual>	172.168.2.0/24	RD2	5	Inter Routing Dor	

☒ Export Route

Inter Routing Domain Service:

InterRD2

Add Cancel

5. Ajoutez une règle NAT dynamique à InterRD1 à l'aide d'un VIP dans les services Bureau à distance partagés. **Activez Bind Responder Route** pour vous assurer que l'itinéraire inverse

utilise le même type de service.

Add

?

x

Priority:

100

Routing Domain:

Shared_RD

Direction:

Outbound

Type:

Port Restricted

Service Type:

Inter Routing Dor

Service Name:

InterRD1

Inside Zone:

Any

Inside IP Address:

0.0.0.0/0

Outside IP Address:

172.168.2.0

☐ Allow Related

☐ IPsec Passthrough

☐ GRE/PPTP Passthrough

☐ Port Parity

☒ Bind Responder Route

Port Forwarding Rules

+

Routing Domain	Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
----------------	----------	--------------	-------------------	-------------	-----------	------------------	-----------	---------	---------------------------	--------

Add

Cancel

6. Ajoutez une règle NAT dynamique à InterRD2 à l'aide d'un VIP dans les services Bureau à distance partagés, par exemple 10.0.0.11. Activez l'itinéraire du répondeur de liaison pour vous assurer que l'itinéraire inverse utilise le même type de service.

Add

?

x

Priority:

100

Routing Domain:

Shared_RD

Direction:

Outbound

Type:

Port Restricted

Service Type:

Inter Routing Dor

Service Name:

InterRD2

Inside Zone:

Any

Inside IP Address:

0.0.0.0/0

Outside IP Address:

172.168.2.0

☐ Allow Related

☐ IPsec Passthrough

☐ GRE/PPTP Passthrough

☐ Port Parity

☒ Bind Responder Route

Port Forwarding Rules

+

Routing Domain	Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
----------------	----------	--------------	-------------------	-------------	-----------	------------------	-----------	---------	---------------------------	--------

Add

Cancel

7. Utilisez des filtres pour limiter les ressources du Bureau à distance partagé qui sont autorisées à accéder par les utilisateurs dans RD1/RD2.

Équilibrage de charge ECMP

February 8, 2022

Les groupes ECMP (Equal Cost Multi-Path) vous permettent de regrouper plusieurs chemins avec le même coût, la destination et le même service. La charge des connexions ou des données de session est équilibrée sur tous les chemins d'accès du groupe ECMP en fonction du type de groupe ECMP. Par

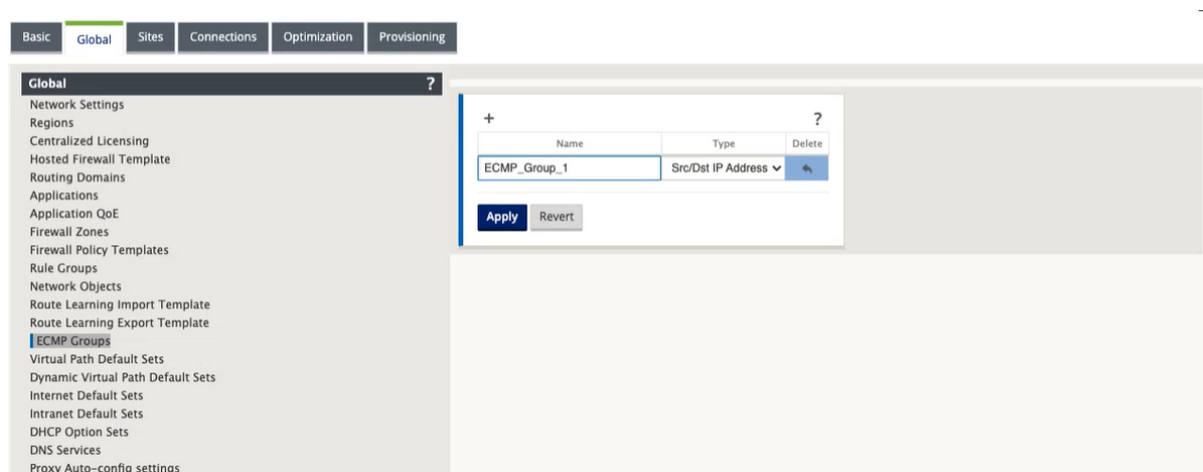
exemple, considérez un réseau avec deux liaisons WAN entre une branche et un centre de données ayant le même coût d'itinéraire. Traditionnellement, l'une des liaisons WAN serait active et l'autre reste dormante agissant comme liaison de secours. Avec les groupes ECMP, vous pouvez regrouper ces liaisons WAN et permettre l'équilibrage de la charge du trafic via les deux liaisons WAN. L'équilibrage de charge ECMP garantit :

- Répartition du trafic sur plusieurs chemins à coût égal.
- Utilisation optimale de la bande passante disponible.
- Transfert dynamique du trafic vers un autre chemin d'accès membre ECMP, en cas d'échec d'une liaison. ECMP prend en charge les routes statiques sur les tunnels IPsec/GRE.

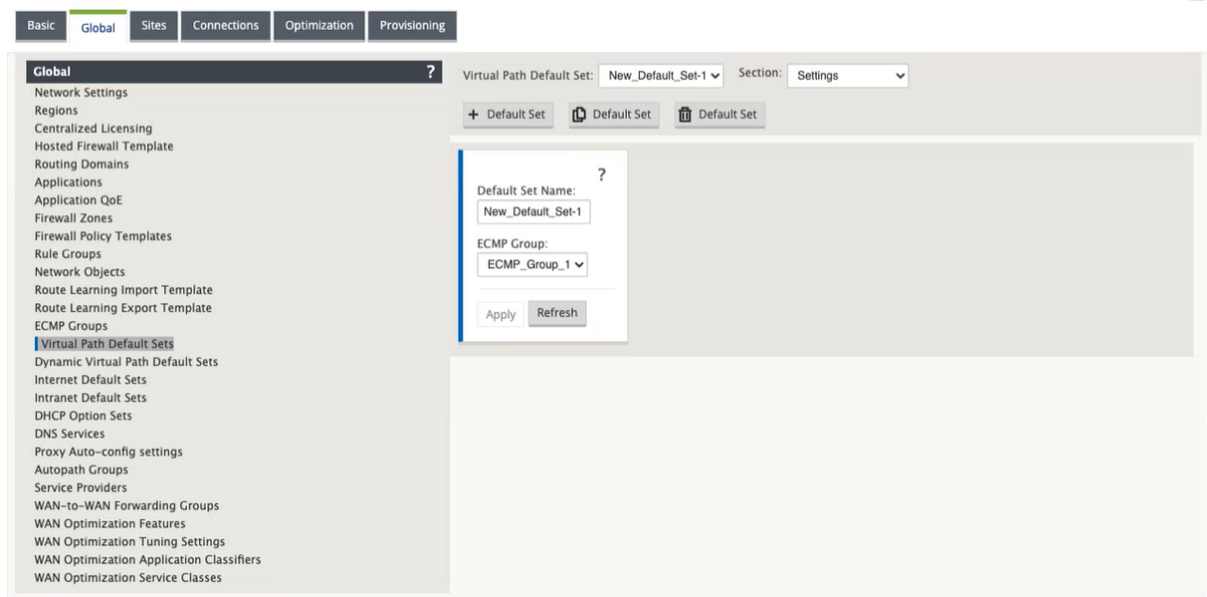
L'équilibrage de charge ECMP est pris en charge sur les chemins virtuels et les services Intranet. Les groupes ECMP sont définis au niveau global. Vous pouvez définir un maximum de 254 groupes ECMP dans votre réseau. Le nombre maximal de routes éligibles ECMP dans un groupe ECMP dépend de votre appliance et du type de licence. Les deux types de groupes ECMP suivants sont pris en charge sur Citrix SD-WAN :

- Adresse IP source/destination : Réseaux où plusieurs clients tentent de se connecter à la même destination, les connexions sont équilibrées en charge sur des liaisons WAN à coût égal.
- Session : Réseaux sur lesquels un seul client est connecté à une destination et où plusieurs sessions sont engendrées. Les données de session sont équilibrées en charge sur des liaisons WAN à coût égal.

Pour configurer un groupe ECMP, dans l'éditeur de configuration, accédez à **Global > Groupes ECMP**. Indiquez un nom pour le groupe ECMP et sélectionnez le type comme **adresse IP Src/Dest** ou **Session** selon les besoins.

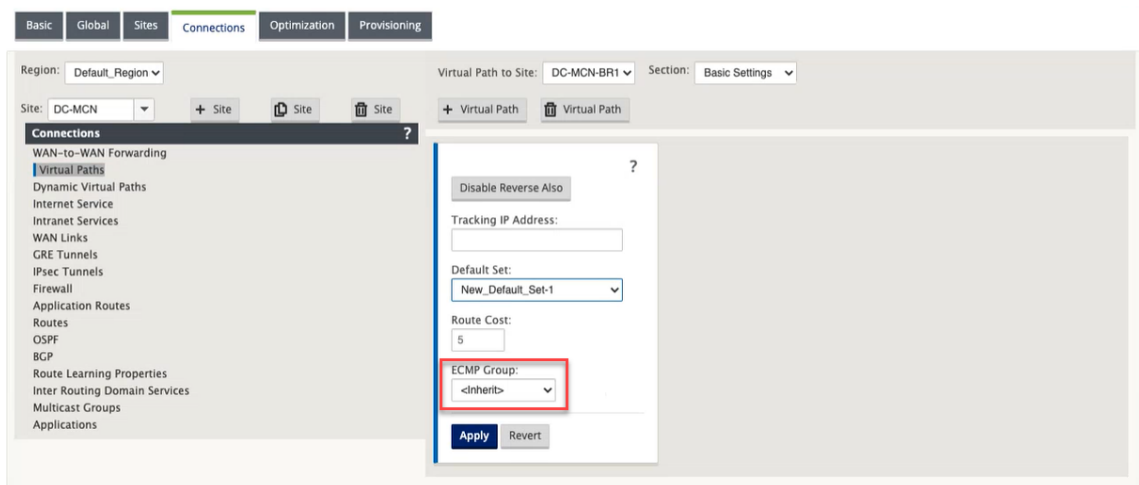


Vous pouvez associer les groupes ECMP à des ensembles de chemins virtuels et intranet par défaut.

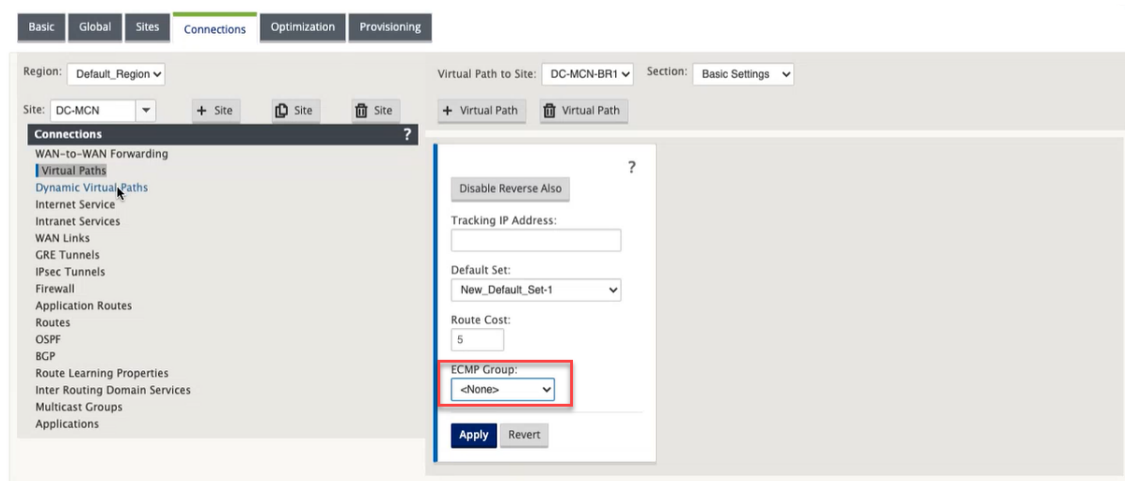


Voici les trois façons d'associer un groupe ECMP aux services Chemin virtuel et Intranet :

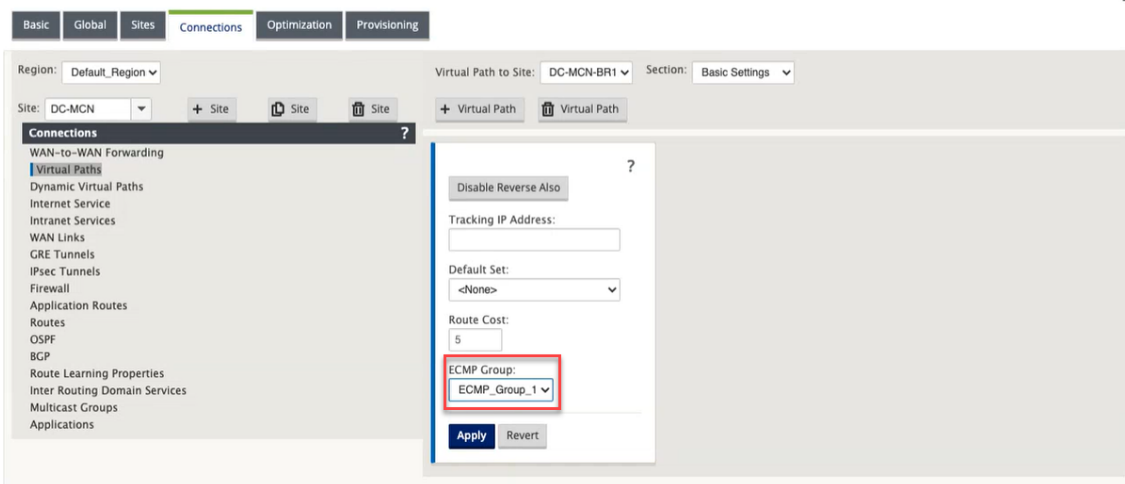
- **Hériter** : le service hérite du groupe ECMP associé au jeu par défaut. Si aucun groupe ECMP n'est associé au jeu par défaut, le service n'est associé à aucun groupe ECMP.



- **Aucun** : le service n'est associé à aucun groupe ECMP même si le jeu par défaut est associé à un groupe ECMP.



- **Groupe ECMP** : sélectionnez l'un des groupes ECMP définis au niveau global pour associer le groupe ECMP au service. Le groupe ECMP sélectionné remplace le groupe ECMP associé au jeu par défaut.



Pour surveiller l'équilibrage de charge ECMP, dans l'interface utilisateur SD-WAN, accédez à **Surveillance > Statistiques > Itinéraires** et filtrez les résultats de la recherche à l'aide du nom du groupe ECMP.

Monitoring > Statistics

Statistics

Show: Routes ☒ Enable Auto Refresh 5 seconds ☒ Clear Counters on Refresh

Routing Domain: <ALL>

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain: Default_RoutingDomain

Filter: Tonowhere in ECMP Group Network Address Type: ALL

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 35 total entries)

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	ECMP Group	Eligible	Eligibility Type	Eligibility Value
<input checked="" type="checkbox"/>	6	6.6.6.0/24	*	New_Intranet_Service-3	Intranet_Zone	YES	BR1	Static	-	-	5	0	Tonowhere	YES	N/A	N/A
<input checked="" type="checkbox"/>	7	5.5.5.0/24	*	New_Intranet_Service-3	Intranet_Zone	YES	BR1	Static	-	-	5	630	Tonowhere	YES	Path	BR1_Inet1->DC_Inet1
<input checked="" type="checkbox"/>	8	5.5.5.0/24	*	New_Intranet_Service-4	Intranet_Zone	YES	BR1	Static	-	-	5	315	Tonowhere	YES	N/A	N/A
<input checked="" type="checkbox"/>	9	4.4.4.0/24	*	New_Intranet_Service-4	Intranet_Zone	YES	BR1	Static	-	-	5	0	Tonowhere	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 35 total entries)

Dans les exemples de données, nous voyons que toutes les routes d'un service ayant un groupe ECMP commun font partie de ce groupe ECMP. Par exemple, 6.6.6.0/24 et 5.5.5.0/24 sont dans le groupe ECMP **Tonowhere**. Toutefois, la charge du trafic est équilibrée entre les services **New_Intranet_Service-3** et **New_Intranet_Service-4** qui partagent une adresse IP de destination 5.5.5.0/24 et sont associés au même groupe ECMP.

Remarque

Pour le service SIA et Zscaler, vous pouvez équilibrer la charge sur deux chemins de tunnel IPsec avec ECMP (actif/actif).

La fonctionnalité d'équilibrage de charge ECMP n'est pas prise en charge sur les appliances SD-WAN suivantes :

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

Peering sécurisé

May 6, 2021

L'appliance Premium (Enterprise) Edition peut être installée dans le centre de données et peut initier l'appairage sécurisé automatique ou manuel, créer un profil SSL et associer une classe de service, et joindre l'appliance à un contrôleur de domaine Windows pour permettre aux utilisateurs/administrateur d'utiliser la fonctionnalité riche étendue de WANOP autonome appliance.

Voici les modes de déploiement pris en charge pour Auto Secure Peering et Manuel Secure Peering :

Déploiements Auto Secure Peering :

Pour effectuer un appairage sécurisé automatique à une appliance PE à partir d'une solution WANOP/SDWAN SE/WANOP autonome sur le site DC.

Étapes à suivre pour lancer ce déploiement :

- L'appliance WANOP DC est en mode LISTEN ON (2312/Tout port non standard) et Branch PE est en mode CONNECT-TO.
- WANOP DC lance le peering sécurisé automatique à une appliance PE qui installe les certificats de CA privés et les paires CERT KEY et configure CONNECT-O sur l'appliance PE avec WANOps LISTEN-ON IP.

Pour effectuer l'appairage auto-sécurisé lancé à partir d'une appliance PE sur le site DC et l'appliance PE du site Branch.

Étapes à suivre pour lancer ce déploiement :

- L'appliance DC PE est en mode LISTEN ON (sur le port 443). Succursale PE est en mode CONNECT-TO.
- L'appliance PE DC lance l'appairage sécurisé automatique vers une appliance PE Branch qui installe les certificats d'autorité de certification privée et les paires CERT KEY et configure CONNECT-O sur l'appliance PE Branch avec l'IP LISTEN-ON de DC PE.
- LISTEN-ON IP for PE se trouve dans l'adresse IP de l'interface associée au domaine de routage pour lequel « Rediriger vers WANOP » est activé.

Peering automatique sécurisé lancé à partir de l'appliance PE sur le site DC et la branche avec l'appliance WANOP/SDWAN SE.

Étapes à suivre pour lancer ce déploiement :

- L'appliance DC PE est en mode LISTEN ON (sur le port 443). Succursale WANOP/SD-WAN SE est en mode CONNECT-TO.
- L'appliance PE DC lance l'appairage sécurisé automatique vers l'appliance Branch WANOP/SD-WAN SE qui installe les certificats de CA privés et les paires CERT KEY et configure CONNECT-O sur l'appliance PE avec l'IP LISTEN-ON de DC PE.

Déploiements Secure Peering manuels :

Peering manuel sécurisé lancé à partir de l'appliance PE sur le site DC vers l'appliance Branch PE.

Étapes à suivre pour lancer ce déploiement :

- L'appliance DC PE est en mode LISTEN ON (sur le port 443). Succursale PE est en mode CONNECT-TO.
- LISTEN-ON IP for PE se trouve dans l'adresse IP de l'interface associée au domaine de routage pour lequel « Rediriger vers WANOP » est activé.

- Chargez manuellement les certificats de paires d'autorité de certification et de clé de certification obtenus à partir d'une source authentique d'autorité de certification.

Peering manuel sécurisé lancé à partir de l'appliance PE sur le site DC vers l'appliance WANOP/SDWAN-SE Branch.

Étapes à suivre pour lancer ce déploiement :

- L'appliance DC PE est en mode LISTEN ON (sur le port 443). Succursale WANOP/SD-WAN SE est en mode CONNECT-TO.
- LISTEN-ON IP for PE se trouve dans l'interface IP associée au domaine de routage pour lequel « Rediriger vers WANOP » est activé
- Chargez manuellement les certificats de paires d'autorité de certification et de clé de certification obtenus à partir d'une source authentique d'autorité de certification.

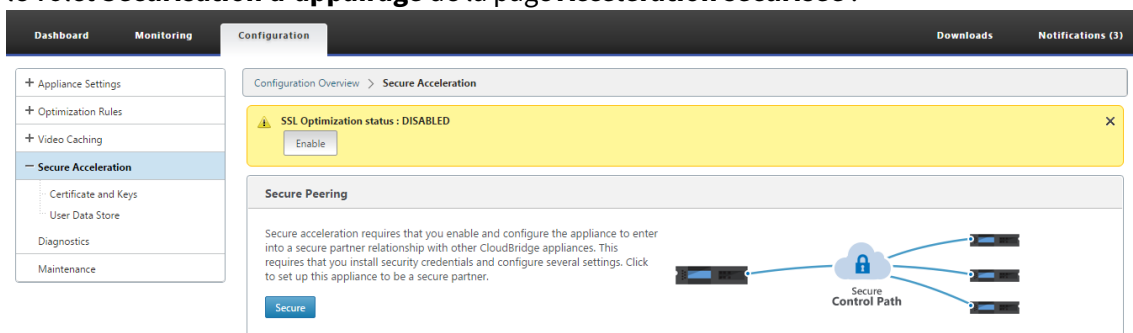
Peering automatique sécurisé vers une appliance PE à partir d'une appliance SD-WAN SE et WANOP autonomes sur le site DC

May 6, 2021

Pour effectuer un appairage sécurisé automatique sur une appliance PE à partir d'une appliance SD-WAN SE et WANOP autonome du côté DC :

- L'appliance WANOP DC est en mode LISTEN ON (2312/Tout port non standard).
- L'appliance Branch PE est en mode CONNECT-TO.
- WANOP DC lance le peering sécurisé automatique à une appliance PE qui installe les certificats de CA privés et les paires CERT KEY et configure CONNECT-O sur l'appliance PE avec WANOps LISTEN-ON IP.

1. Sur une appliance WANOP autonome située au centre de données, cliquez sur **Sécuriser** dans le volet **Sécurisation d'appairage** de la page **Accélération sécurisée**.



2. Configurez les paramètres du keystore en fournissant le **mot de passe du keystore** ou en désactivant le keystore.

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN interface. Under 'Secure Peering', the 'Keystore Settings' section is visible. It includes a text box for 'Keystore Password*', a text box for 'Confirm Keystore Password*', and a checkbox for 'Disable Keystore Password'. At the bottom of this section are 'Save' and 'Cancel' buttons.

3. **Activez l'appairage sécurisé** en sélectionnant Autorité de **certification privée** pour effectuer un PEERING SÉCURISÉ AUTOMATIQUE.

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN interface. Under 'Secure Peering', the 'Secure Peering Certificate and Keys' section is visible. It includes a 'Keystore Status' section showing 'Opened'. Below this, there is a checkbox for 'Enable Secure Peering' which is checked. Under 'Certificate Configuration', there are two radio buttons: 'Private CA' (selected) and 'CA Certificate'. At the bottom of this section are 'Save' and 'Cancel' buttons.

4. Le certificat d'autorité de certification de niveau appliance ainsi que le certificat et la clé privés sont générés sur le WANOP local et une table pour ajouter un appairage sécurisé REMOTE PEER TO Perform AUTO avec est affichée.
5. Cliquez sur l'icône '+' et une fenêtre contextuelle pour ajouter une adresse IP avec nom d'utilisateur et mot de passe s'affiche. Une fois l'authentification réussie avec l'adresse IP distante avec les informations d'identification fournies, une demande est envoyée à la machine distante qui installe le certificat CA et le certificat privé et la clé pour elle-même localement (sur la machine distante).

DashboardMonitoringConfigurationDownloadsNotifications (3)

Back

Secure Peering

Keystore Settings

Keystore StatusOpened

Secure Peering Certificate and Keys

Secure PeeringEnabled	Certificate/Key Pair Nameprivate_10_105_184_74	CA Certificate Store NamePrivateRootCA	Cipher Specification!ADH:!AECDH:!MD5:HIGH:@STRENGTH
-----------------------	--	--	---

Connected Peers

Remarque

- Adresse IP —Adresse IP de L’IP DE GESTION DE L’APPLIANCE PREMIUM (ENTERPRISE) EDI-TION distante
- Nom d’utilisateur —Nom d’utilisateur de L’APPLIANCE PREMIUM EDITION distante (EN-TERPRISE)
- Mot de passe —Mot de passe de l’appliance PREMIUM (ENTERPRISE)

DashboardMonitoringConfigurationDownloadsNotifications (3)

Back

Secure Peering

Keystore Settings

Keystore StatusOpened

Secure Peering Certificate and Keys

Secure PeeringEnabled	Certificate/Key Pair Nameprivate_10_105_184_74	CA Certificate Store NamePrivateRootCA	Cipher Specification!ADH:!AECDH:!MD5:HIGH:@STRENGTH
-----------------------	--	--	---

Connected Peers

Connect Peer

Connect Peer

IP Address10 . 1 . 1 . 1

UsernamePROVIDE_VW_APPLIANCE_UNAME

Password

ConnectClose

Une fois l’authentification réussie, vous verrez Secure Peering comme TRUE et l’adresse IP du partenaire comme l’une des adresses IP virtuelles de l’appliance Premium (Enterprise) Edition distante.

DashboardMonitoringConfigurationDownloadsNotifications (3)

Back

Secure Peering

Keystore Settings

Keystore StatusOpened

Secure Peering Certificate and Keys

Secure PeeringEnabled	Certificate/Key Pair Nameprivate_10_105_184_74	CA Certificate Store NamePrivateRootCA	Cipher Specification!ADH:!AECDH:!MD5:HIGH:@STRENGTH
-----------------------	--	--	---

Connected Peers

Peer Name	IP Address	Secure	Connection Status	Time Connected ↑	Time Since Last Contacted
CloudBridge1	172.184.1.19	True	Connected Available	7m 44s	0m 5s



VIP of Remote EE App

Surveillance

Affichez les informations sur les partenaires sécurisés sur l'apppliance Premium (Enterprise) Edition sous **WANOPTIMISATION > Partenaires** dans la page **Surveillance**.

1. Le chiffrement des magasins de données peut être effectué sur l'apppliance Premium (Enterprise) Edition via l'activation des fonctionnalités à partir du MCN sous le nœud Optimisation pour une appliance Premium (Enterprise) Edition.
2. Pour une appliance Premium (Enterprise) Edition, l'appairage sécurisé est toujours activé.
3. Pour valider si la paire d'**autorité de certification privée** et de **clé de certificat privée** est générée avec succès, consultez les informations ci-dessous :

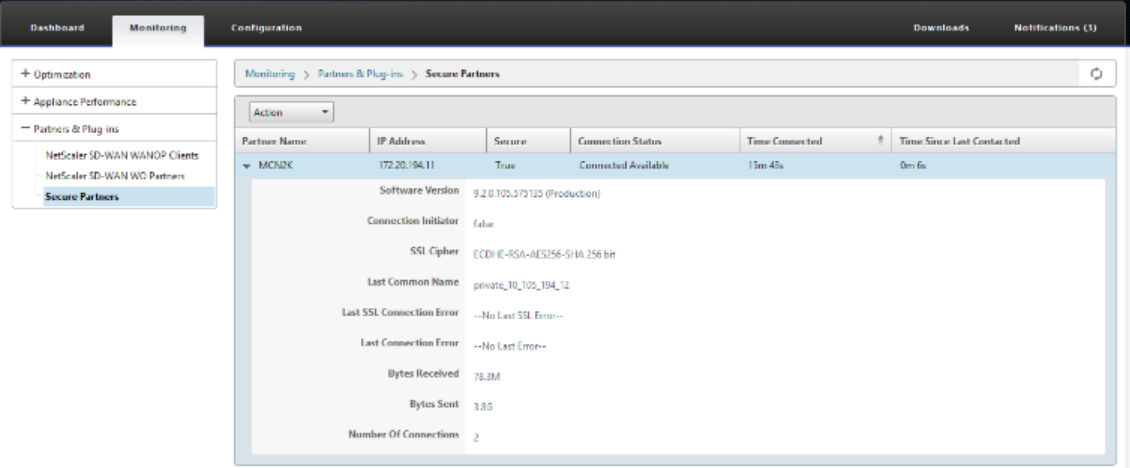
The screenshots show the configuration interface for 'Certificate and Keys'. The first screenshot shows the 'CA Certificates' tab with a table containing one entry: 'PrivateRootCA' with an expiration date of 'Mar 25 19:52:01 2027 GMT' and a count of 1. The second and third screenshots show the 'Certificate Key Pairs' tab with a table containing one entry: 'private_10_105_104_12' with an expiration date of '2027-03-25 13:52:01', a count of 1, and a key type of 'RSA'.

4. Affichez **les informations sur les partenaires sécurisés** sur l'apppliance Premium (Enterprise) Edition sous **Surveillance > Optimisation WAN > Page Partenaires**.

The screenshot shows the 'Partenaires' page under 'Monitoring > WAN Optimization'. It displays system information for agent 10.105.104.12 and a table of secure partners. The table has columns: Partner Name, IP Address, Instance IP, Secure, Connection Status, Time Connected, and Time Since Last Contacted. There is one entry: 'redstone-rp' with IP 172.16.194.3, Instance IP 172.16.194.3, Secure True, Connection Status Connected Available, Time Connected 10m 1s, and Time Since Last Contacted 0m 4s.

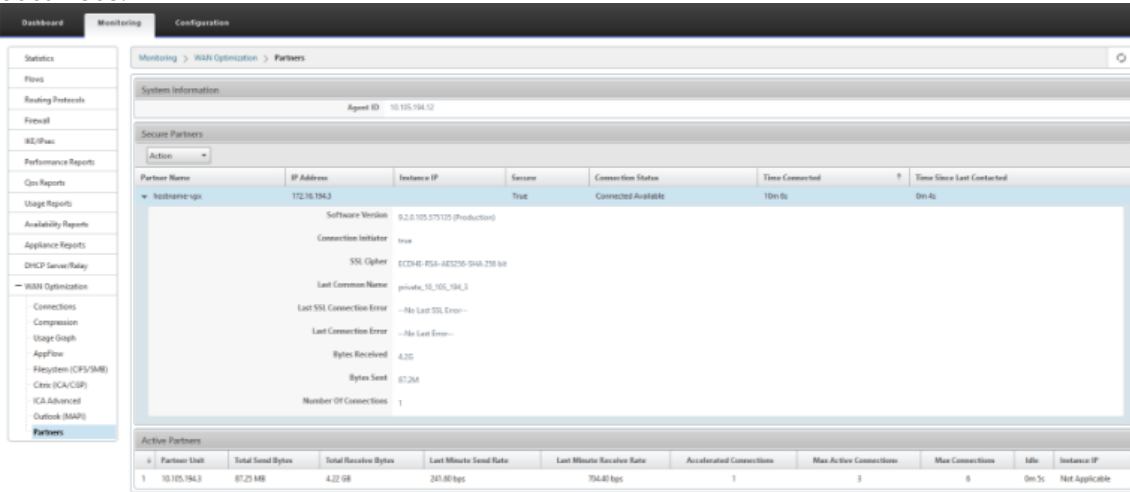
5. Sur l'apppliance partenaire, **affichez les informations de partenaire sécurisé** de l'apppliance

Premium (Enterprise) Edition sous **Surveillance> Partenaires et plug-ins>Partenaires sécurisés.**



Résolution des problèmes

1. Consultez les **informations sur la réussite et l'échec des partenaires sécurisés** sur l'appliance Premium (Enterprise) Edition sous **Surveillance>Optimisation WAN>Partenaires>Partenaires sécurisés.**



2. Sur l'appliance partenaire, consultez Informations sur les partenaires sécurisés sur l'appliance Premium (Enterprise) Edition sous **Surveillance> Partenaires et plug-ins>Partenaires sécurisés.**

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

+ Appliance Performance

- Partners & Plug-ins

NetScaler SD-WAN WANOP Clients

NetScaler SD-WAN WO Partners

Secure Partners

Monitoring > Partners & Plug-ins > Secure Partners

Action

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCH2K	172.20.194.11	True	Connected Available	15m 45s	0m 6s
Software Version 9.2.0.105.379120 (Production)					
Connection Initiator false					
SSL Cipher ECCDHE-RSA-AES256-SHA 256 bit					
Last Common Name private_10_100_194_12					
Last SSL Connection Error --No Last SSL Error--					
Last Connection Error --No Last Error--					
Bytes Received 78.3M					
Bytes Sent 3.85					
Number Of Connections 2					

3. Sur l’appliance partenaire, affichez Secure Partner Information sur l’appliance Premium (Enterprise) Edition sous **Surveillance > Performances de l’appliance > Page Journalisation**.

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

- Appliance Performance

Compression Engine

WCCP

AppFlow

Load Statistics

+ Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Action

Search

Record	Date/Time	Details
5356	Mar 01, 2017 05:50:20	syslog/Mar 1 05:50:20 hostname-vpn NITRO[6762] REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog/Mar 1 05:49:20 hostname-vpn NITRO[6762] RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog/Mar 1 05:49:20 hostname-vpn NITRO[6762] PAYLOAD: [{"params":{"system_info":{"}}
5353	Mar 01, 2017 05:49:20	syslog/Mar 1 05:49:20 hostname-vpn NITRO[6762] REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog/Mar 1 05:48:20 hostname-vpn NITRO[6762] RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog/Mar 1 05:48:20 hostname-vpn NITRO[6762] PAYLOAD: [{"params":{"system_info":{"}}
5350	Mar 01, 2017 05:48:20	syslog/Mar 1 05:48:20 hostname-vpn NITRO[6762] REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog/Mar 1 05:47:20 hostname-vpn NITRO[6762] RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog/Mar 1 05:47:20 hostname-vpn NITRO[6762] PAYLOAD: [{"params":{"system_info":{"}}
5347	Mar 01, 2017 05:47:20	syslog/Mar 1 05:47:20 hostname-vpn NITRO[6762] REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog/Mar 1 05:46:20 hostname-vpn NITRO[6762] RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog/Mar 1 05:46:20 hostname-vpn NITRO[6762] PAYLOAD: [{"params":{"system_info":{"}}
5344	Mar 01, 2017 05:46:20	syslog/Mar 1 05:46:20 hostname-vpn NITRO[6762] REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog/Mar 1 05:45:20 hostname-vpn NITRO[6762] RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog/Mar 1 05:45:20 hostname-vpn NITRO[6762] PAYLOAD: [{"params":{"system_info":{"}}
5341	Mar 01, 2017 05:45:20	syslog/Mar 1 05:45:20 hostname-vpn NITRO[6762] REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog/Mar 1 05:44:20 hostname-vpn NITRO[6762] RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog/Mar 1 05:44:20 hostname-vpn NITRO[6762] PAYLOAD: [{"params":{"system_info":{"}}

Peering automatique sécurisé lancé à partir de l’appliance PE sur le site DC et le site de succursale PE

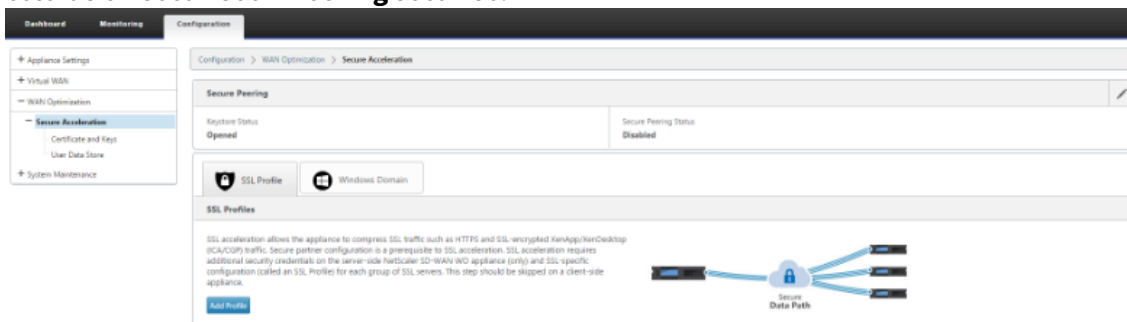
May 6, 2021

Configuration

Pour configurer l'appairage sécurisé automatique sur une nouvelle appliance Premium (Enterprise) Edition au DC :

- L'appliance DC PE est en mode LISTEN ON (sur le port 443). L'appliance Branch PE est en mode CONNECT-TO.
- L'appliance PE DC lance l'appairage sécurisé automatique vers une appliance PE Branch qui installe les certificats d'autorité de certification privée et les paires CERT KEY et configure CONNECT-O sur l'appliance PE Branch avec l'IP LISTEN-ON de DC EE.
- LISTEN-ON IP for PE appliance se trouve dans l'adresse IP d'interface associée au domaine de routage pour lequel « Rediriger vers WANOP » est activé.

1. Dans l'interface graphique Web SD-WAN, accédez à **Configuration > Optimisation WAN > Accélération sécurisée > Peering sécurisé.**



2. Configurez le keystore en fournissant le mot de passe du keystore ou en désactivant le keystore.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*

Open

☐ Change Keystore Password

☐ Disable Keystore Password

☐ Reset Keystore

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

3. Activez **Secure Peering** en sélectionnant **Private CA** pour effectuer le PEERING AUTOMATIQUE SÉCURISÉ.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN VWO partner appliance requires that you generate OpenSSL credentials, including a CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☒ Private CA ☐ CA Certificate

Save

Cancel

Secure Peering Certificate and Keys			
Secure Peering	Certificate/Key Pair Name	CA Certificate Store Name	Cipher Specification
Enabled	private_10_105_194_12	PrivateRootCA	IADH:IAECDH:IMD5:HIGH:@STRENGTH

Secure Peering Certificate and Keys			
Secure Peering	Certificate/Key Pair Name	CA Certificate Store Name	Cipher Specification
Enabled	private_10_105_194_12	PrivateRootCA	IADH:IAECDH:IMD5:HIGH:@STRENGTH

4. Cliquez sur l'icône '+' et ajoutez IP avec nom d'utilisateur et mot de passe. Une fois l'authentification réussie avec l'adresse IP distante et les informations d'identification fournies, une demande est envoyée à la machine distante qui installera le certificat CA ainsi que le certificat privé et la clé pour elle-même localement sur la machine distante.

Remarque

Adresse IP — Adresse IP de EE Appliance MANAGEMENT IP distante

Nom d'utilisateur : nom d'utilisateur de l'appliance EE distante

Mot de passe — Mot de passe de EE Appliance distante

DashboardMonitoringConfiguration

Back

Secure Peering

Keystore Settings

Keystore Status

Opened

Secure Peering Certificate and Keys

Secure Peering

Enabled

Certificate/Key Pair

private_10_105_194_12

Connect Peer

Connect Peer

IP Address

10 . 105 . 194 . 3

Username

admin

Password

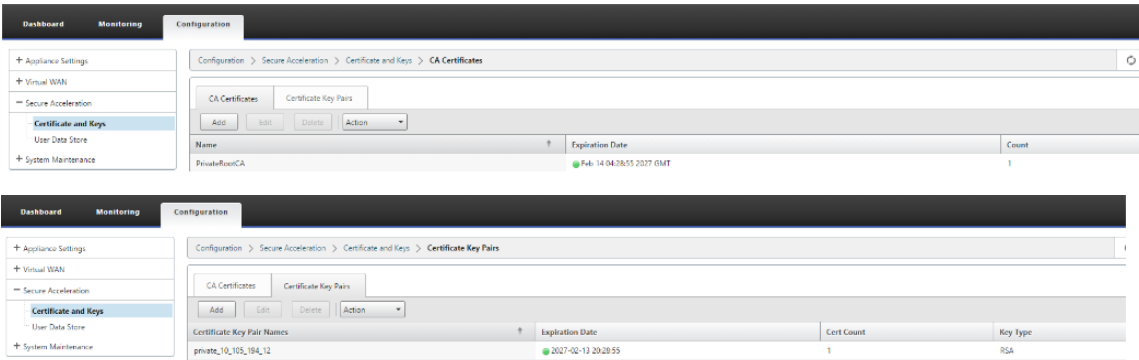
••••••••

Connect

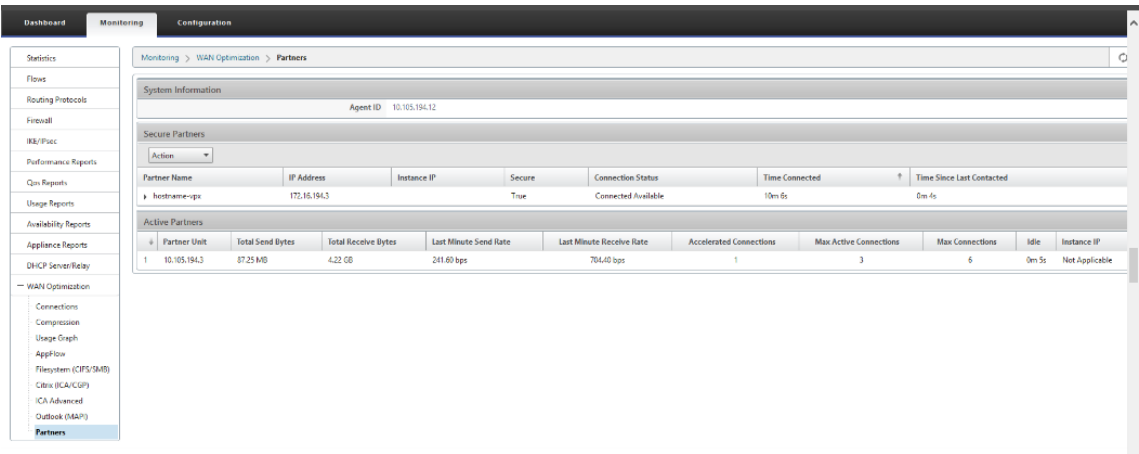
Close

Surveillance

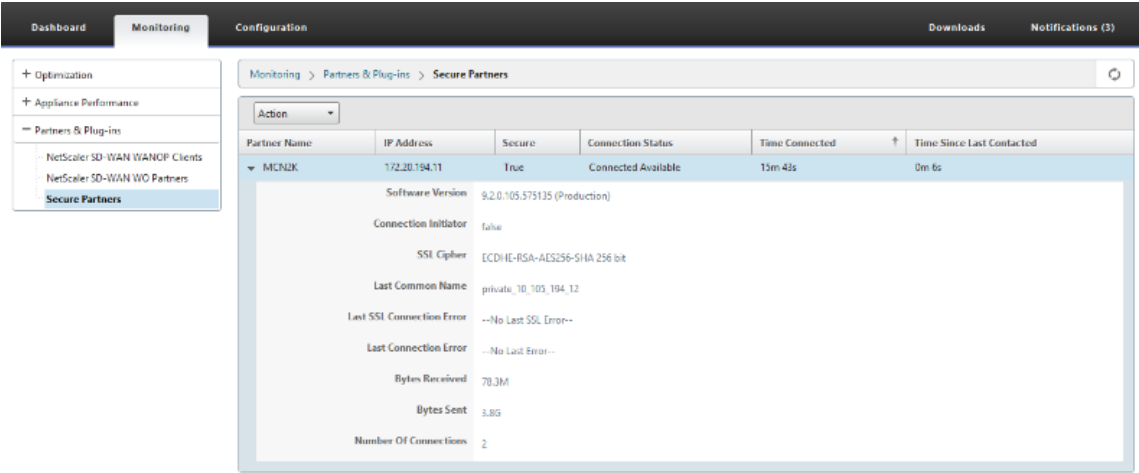
1. Pour valider si la paire d'autorité de certification privée et de clé de certificat privée est générée avec succès, consultez les informations affichées ci-dessous.



2. Affichez **les informations sur les partenaires sécurisés** sur l’appliance Premium (Enterprise) Edition sous **Surveillance > Optimisation WAN > Page Partenaires**.



3. Sur l’appliance partenaire, consultez les informations sur les partenaires sécurisés sur l’appliance Premium (Enterprise) Edition Appliance sous **Surveillance > Partenaires et plug-ins > Partenaires sécurisés**.



Résolution des problèmes

1. Affichez les informations de réussite et d'échec des partenaires sécurisés sur l'appliance Premium (Enterprise) Edition sous **Surveillance > Optimisation WAN > Partenaires > Partenaires sécurisés**.

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hcsname-vps	172.16.194.3		True	Connected Available	10m 4s	0m 4s

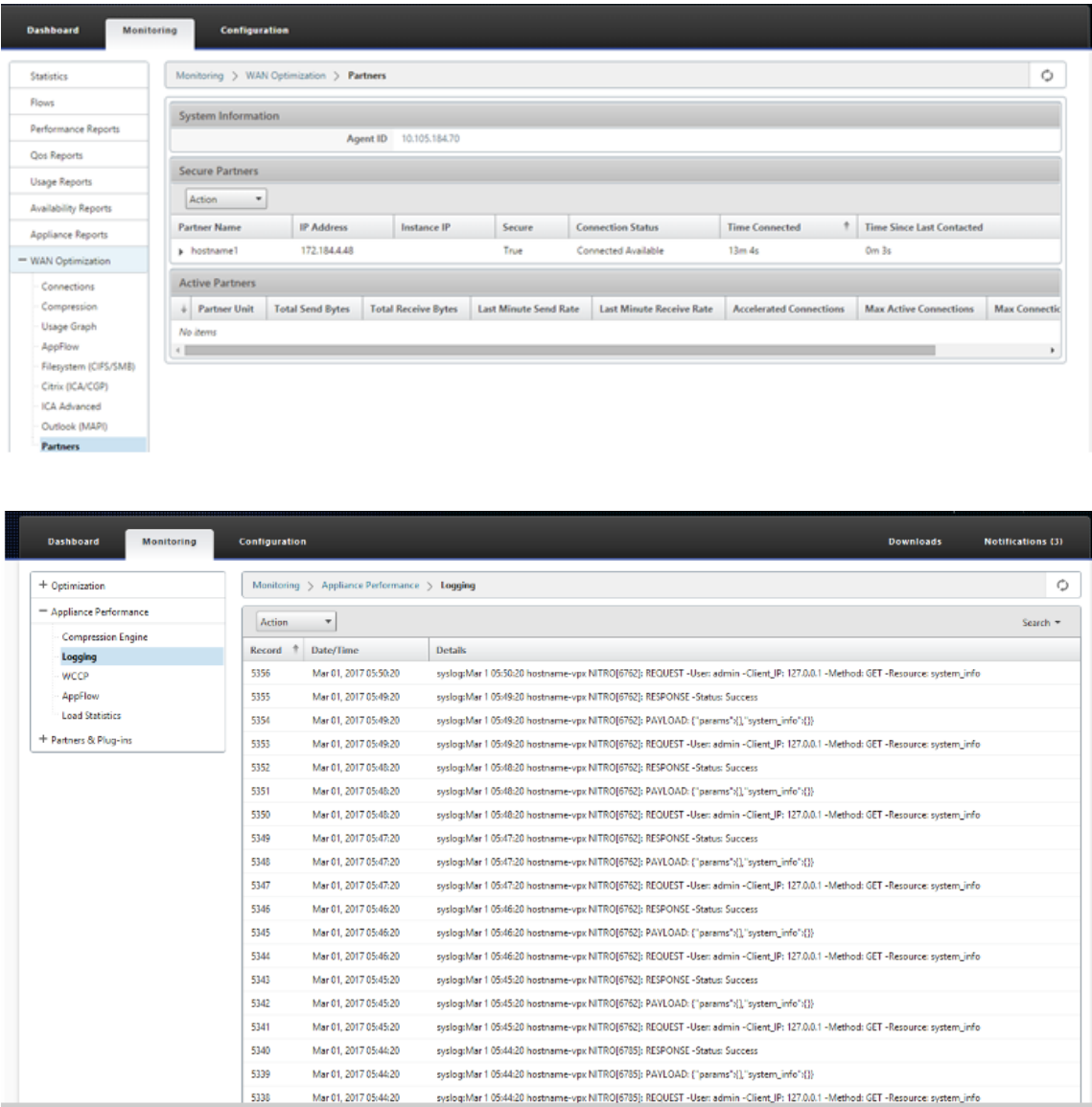
Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hcsname-vps	172.16.194.3		True	Connected Available	10m 4s	0m 4s

2. Sur l'appliance partenaire, consultez les informations sur les partenaires sécurisés sur l'appliance Premium (Enterprise) Edition Appliance sous **Surveillance > Partenaires et plug-ins > Partenaires sécurisés**.

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCN2K	172.20.194.11	True	Connected Available	15m 41s	0m 6s

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCN2K	172.20.194.11	True	Connected Available	15m 41s	0m 6s

3. Sur l'appliance partenaire, consultez Informations sur le partenaire sécurisé sur l'appliance Premium (Enterprise) Edition sous **Surveillance > Performances de l'appliance > Journalisation**.



Peering automatique sécurisé lancé à partir d’une appliance PE sur le site DC et la branche avec une appliance SD-WAN SE et WANOP autonomes

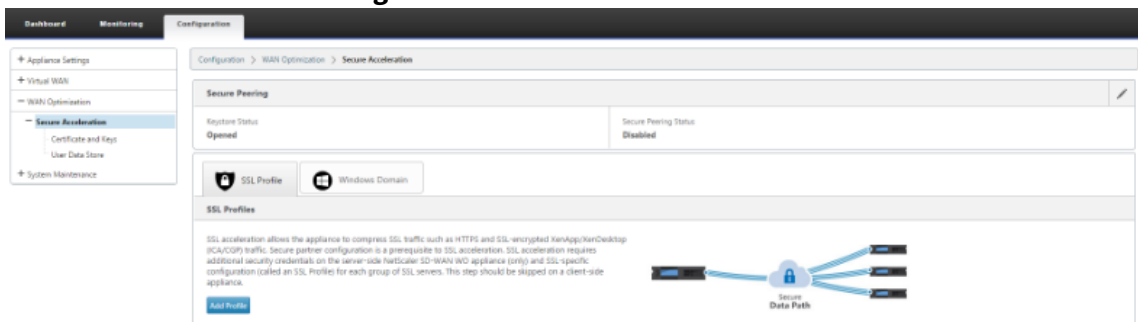
May 6, 2021

Configuration

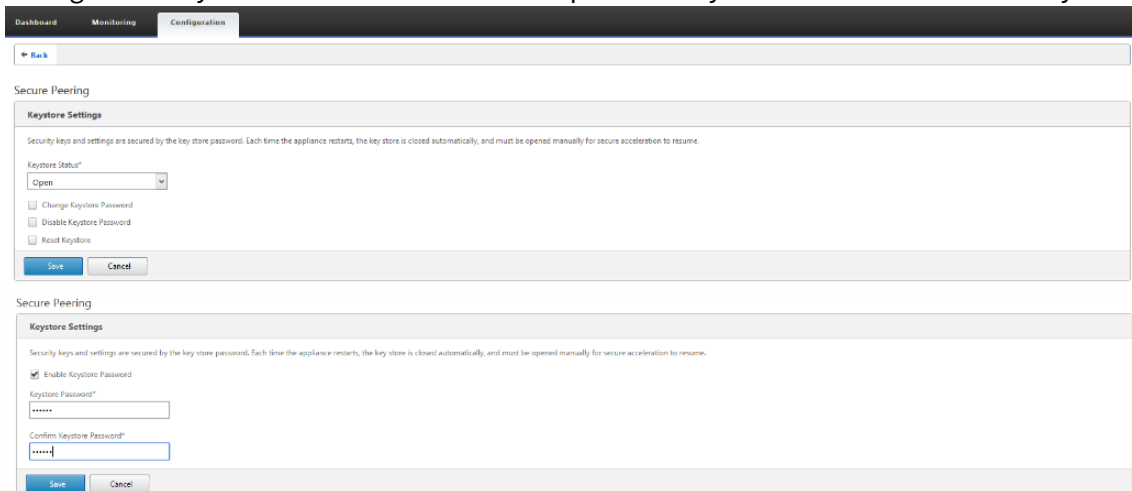
Pour configurer une nouvelle appliance Premium (Enterprise) Edition avec appairage sécurisé automatique sur le site DC et Branch avec dispositif SD-WAN autonome et WANOP :

- L'appliance DC PE est en mode LISTEN ON (sur le port 443).
- Succursale autonome SD-WAN SE et WANOP est en mode CONNECT-To.
- L'appliance PE DC lance l'appairage sécurisé automatique vers l'appliance SD-WAN SE et WANOP autonome Branch qui installe les certificats d'autorité de certification privés et les paires CERT KEY et configure CONNECT-O sur l'appliance PE avec l'IP LISTEN-ON de DC EE.

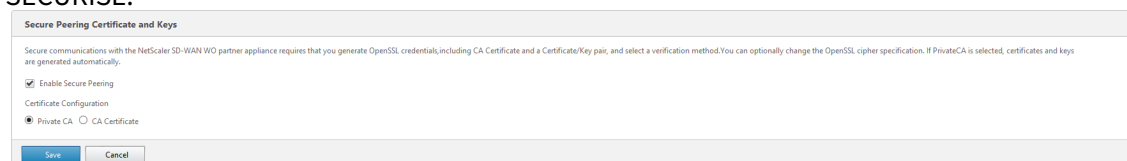
1. Dans l'interface graphique Web SD-WAN, accédez à **Configuration > Optimisation WAN > Accélération sécurisée > Peering sécurisé.**



2. Configurez le keystore en fournissant le mot de passe du keystore ou en désactivant le keystore.



3. Activez **Secure Peering** en sélectionnant **Private CA** pour effectuer le PEERING AUTOMATIQUE SÉCURISÉ.



Secure Peering Certificate and Keys			
Secure Peering Enabled	Certificate/Key Pair Name private_10_105_194_12	CA Certificate Store Name PrivateRootCA	Cipher Specification IA0H:IAECDH:IMD5:HIGH:@STRENGTH

4. Cliquez sur l'icône '+' et ajoutez IP avec nom d'utilisateur et mot de passe. Une fois l'authentification réussie avec l'adresse IP distante et les informations d'identification fournies, une demande est envoyée à la machine distante qui installera le certificat CA ainsi que le certificat privé et la clé pour elle-même localement sur la machine distante.
- Adresse IP : adresse IP de WANOP Standalone ou Standard Edition Appliance MANAGEMENT IP.
 - Nom d'utilisateur : nom d'utilisateur de WANOP Standalone ou Standard Edition Appliance distante.
 - Mot de passe — Mot de passe de WANOP Standalone ou Standard Edition Appliance distante.

The screenshot displays the OpenStack Horizon web interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' tab is active. On the left sidebar, 'Secure Peering' is selected. The main content area shows 'Keystore Settings' with a status of 'Opened', and a table for 'Secure Peering Certificate and Keys' with one entry 'Enabled'. A 'Connect Peer' modal dialog is open in the foreground. It contains three input fields: 'IP Address' with the value '10.105.194.3', 'Username' with the value 'admin', and 'Password' which is masked with dots. At the bottom of the dialog are two buttons: 'Connect' and 'Close'.

Après l'authentification réussie, vous pouvez afficher Secure Peering comme TRUE et l'IP partenaire comme l'une des adresses IP virtuelles de l'appliance WANOP autonome distante.

Dashboard

Monitoring

Configuration

Back

Secure Peering

Keystore Settings

Keystore Status
Opened

Secure Peering Certificate and Keys

Secure Peering
Enabled

Certificate/Key Pair Name
private_18_305_194_12

CA Certificate Store Name
PrivateRootCA

Cipher Specification
128G128GCM128GCM-HIGH-STRENGTH

Connected Peers

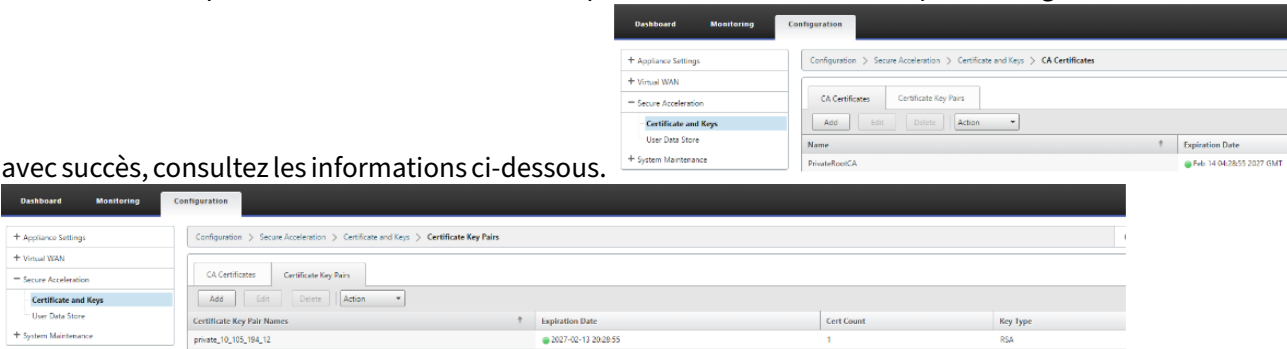
Partner Name	IP Address	Secure	Connection Status	Time Connected *	Time Since Last Contacted
testname-ops	172.16.194.3	True	Connected Available	0m 13s	0m 3s

Done

Surveillance

1. Pour vérifier si la paire d'autorité de certification privée et de clé de certificat privée est générée

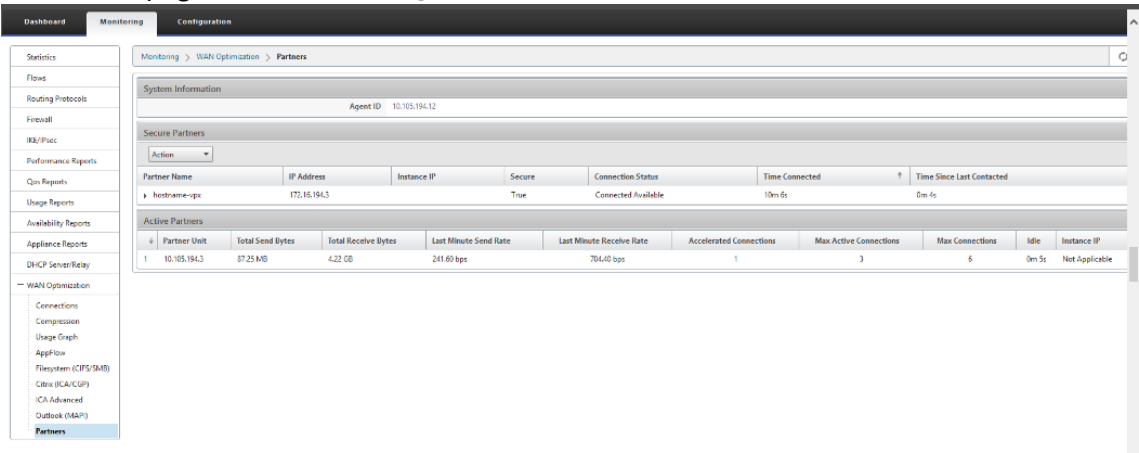
avec succès, consultez les informations ci-dessous.



The screenshot shows the 'Configuration' tab in the Citrix SD-WAN interface. The breadcrumb trail is 'Configuration > Secure Acceleration > Certificate and Keys > CA Certificates'. The 'Certificate Key Pairs' sub-tab is active. A table lists the generated key pairs:

Certificate Key Pair Names	Expiration Date	Cert Count	Key Type
private_10_105_194_12	2027-02-12 20:29:55	1	RSA

2. Affichez les informations sur les partenaires sécurisés sur l'appliance Premium (Enterprise) Edition sous la page **Surveillance > Optimisation du réseau étendu > Partenaires**.

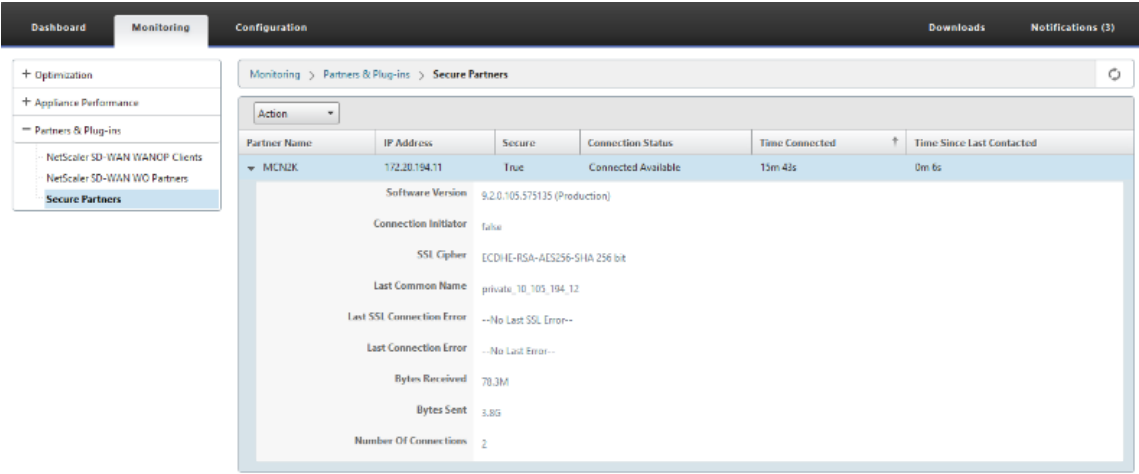


The screenshot shows the 'Monitoring' tab in the Citrix SD-WAN interface. The breadcrumb trail is 'Monitoring > WAN Optimization > Partners'. The 'Secure Partners' section is expanded, showing a table of active partners:

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-gx	172.16.194.3		True	Connected Available	10m 5s	0m 4s

Below this, there is a table for 'Active Partners' with columns: Partner Unit, Total Send Bytes, Total Receive Bytes, Last Minute Send Rate, Last Minute Receive Rate, Accelerated Connections, Max Active Connections, Max Connections, Idle, and Instance IP.

3. Sur l'appliance partenaire, consultez les informations sur les partenaires sécurisés sur l'appliance Premium (Enterprise) Edition sous la page **Surveillance > Partenaires et plug-ins > Partenaires sécurisés**.



The screenshot shows the 'Monitoring' tab in the Citrix SD-WAN interface. The breadcrumb trail is 'Monitoring > Partners & Plug-ins > Secure Partners'. The 'Secure Partners' section is expanded, showing a table of active partners:

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCNJK	172.20.194.11	True	Connected Available	15m 48s	0m 6s

Below this, there is a table for 'Active Partners' with columns: Partner Unit, Total Send Bytes, Total Receive Bytes, Last Minute Send Rate, Last Minute Receive Rate, Accelerated Connections, Max Active Connections, Max Connections, Idle, and Instance IP.

Résolution des problèmes

1. Affichez les informations sur la réussite et l'échec du partenaire sécurisé sur l'appliance Premium (Enterprise) Edition sous la page **Surveillance > Optimisation du réseau étendu > Partenaires > Partenaires sécurisés**.

The screenshot shows the 'Partenaires sécurisés' (Secure Partners) page in the Citrix SD-WAN 11.4 interface. The page is divided into two main sections: 'System Information' and 'Secure Partners'.

System Information:

- Agent ID: 10.105.194.12

Secure Partners:

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
localhost-194	172.16.194.3		True	Connected Available	10m 6s	0m 6s

Below the table, there are detailed statistics for the selected partner:

- Software Version: 9.2.0.105.571135 (Production)
- Connection Initiator: true
- SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_3
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 435
- Bytes Sent: 67.3M
- Number Of Connections: 1

At the bottom, there is a table for 'Active Partners' with columns for Partner Unit, Total Send Bytes, Total Receive Bytes, Last Minute Send Rate, Last Minute Receive Rate, Accelerated Connections, Max Active Connections, Max Connections, Idle, and Instance IP.

2. Sur l'appliance partenaire, consultez les **informations sur les partenaires sécurisés** sur l'appliance Premium (Enterprise) Edition sous **Surveillance > Partenaires et plug-ins > Partenaires sécurisés**.

The screenshot shows the 'Partenaires sécurisés' (Secure Partners) page in the Citrix SD-WAN 11.4 interface on a partner appliance. The page is divided into two main sections: 'System Information' and 'Secure Partners'.

System Information:

- Agent ID: 10.105.194.11

Secure Partners:

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCN2K	172.20.194.11	True	Connected Available	13m 41s	0m 6s

Below the table, there are detailed statistics for the selected partner:

- Software Version: 9.2.0.105.571135 (Production)
- Connection Initiator: false
- SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_12
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 70.3M
- Bytes Sent: 3.8G
- Number Of Connections: 2

3. Sur l'appliance partenaire, consultez **Informations sur le partenaire sécurisé** sur l'appliance Premium (Enterprise) Edition sous la page **Surveillance > Performances de l'appliance > Journalisation**.

Record	Date/Time	Details
5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"}}
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"}}
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"}}
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"}}
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"}}
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"}}
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info

Peering manuel sécurisé lancé à partir de l'appliance PE sur le site DC et l'appliance Branch PE

May 6, 2021

Ce déploiement configure l'appliance DC de site en mode LISTEN ON et l'appliance PE de site de Branch en mode CONNECT TO.

- L'appliance DC PE est en mode LISTEN ON (sur le port 443).
- L'appliance Branch PE est en mode CONNECT-TO.
- LISTEN-ON IP for PE se trouve dans l'adresse IP de l'interface associée au domaine de routage pour lequel « Rediriger vers WANOP » est activé.
- Chargez manuellement les certificats de paires d'autorité de certification et de clé de certification obtenus à partir d'une source authentique d'autorité de certification.

Configuration

Pour configurer l'appairage sécurisé automatique lancé à partir d'une appliance PE sur un site DC et une appliance PE sur un site de succursale :

1. Chargez le **certificat CA** et le **certificat de clé CA** obtenu à partir d'un certificat authentique et fournissez au SD-WAN comme indiqué ci-dessous.

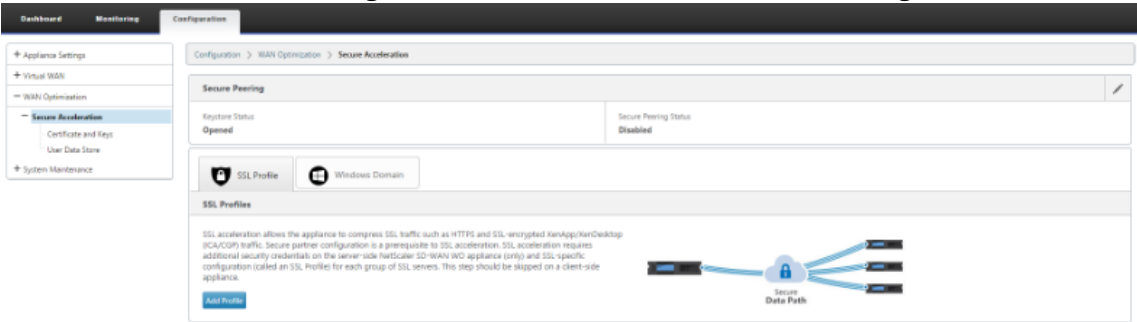
Configuration > Secure Acceleration > Certificate and Keys > CA Certificates

CA Certificates		
Certificate Key Pairs		
Add Edit Delete Action		
Name	Expiration Date	Count
CA	Feb 25 01:39:42 2032 GMT	1

Configuration > Secure Acceleration > Certificate and Keys > Certificate Key Pairs

Certificate Key Pairs			
Add Edit Delete Action			
Certificate Key Pair Names	Expiration Date	Cert Count	Key Type
CAKeyPair	2033-07-18 20:01:18	1	RSA

2. Sur une nouvelle appliance PE sur le site de contrôleur de domaine, dans l’interface graphique Web SD-WAN, accédez à **Configuration > Accélération sécurisée > Peering sécurisé**.



3. Configurez le keystore en fournissant le mot de passe du keystore ou en désactivant le keystore.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password

Save Cancel

Dashboard Monitoring Configuration

Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*
Open

☐ Change Keystore Password
☐ Disable Keystore Password
☐ Reset Keystore

Save Cancel

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

Save Cancel

4. Activez le peering sécurisé en sélectionnant le bouton radio **Certificat de l'autorité** de

certification et en fournissant les certificats de paires de clés de l'autorité de certification et de l'autorité de certification chargés de manière appropriée, comme indiqué ci-dessous.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☐ Private CA

☒ CA Certificate

Certificate/Key Pair Name

CAKeyPair

CA Certificate Store Name

CA

Certificate Verification*

Signature/Expiration

SSL Cipher Specification

!ADH:!AECDH:!MD5:HIGH:@STRENGTH

☐ Edit Cipher Specification

Save

Cancel

5. Fournissez l'adresse IP virtuelle de la machine distante avec le port 443 comme illustré ci-dessous.

Listen On and Connect To

Auto Discovery is typically enabled, when enabled, any authenticated peers can connect via the Listen On addresses. If disabled, secure communications are allowed only with peers on the Connect To list.

☒ Enable Auto-Discovery

Listen On

169.254.1.20

443

×

169.254.1.20

2312

×

+

☒ Publish NAT addresses to peers

NAT Addresses

172.16.120.131

443

×

172.16.120.131

443

×

+

Connect To

172.16.220.140

443

×

172.16.220.140

443

×

+

Save

Cancel

Surveillance

1. Pour valider si l'autorité de **certification privé**et la **paire Clé de certificat privé** est générée correctement, consultez les informations ci-dessous.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IPsec/VPN

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

WAN Optimization

Connections

Compression

Usage Graph

AppFlow

Filesystem (CIFS/SMB)

Citrix (ICA/COP)

ICA Advanced

Outlook (MAPI)

Partners

Monitoring > WAN Optimization > Partners

System Information

Agent ID 10.105.194.12

Secure Partners

Action

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
testname-ops	172.16.194.3		True	Connected Available	10m 5s	0m 4s

Active Partners

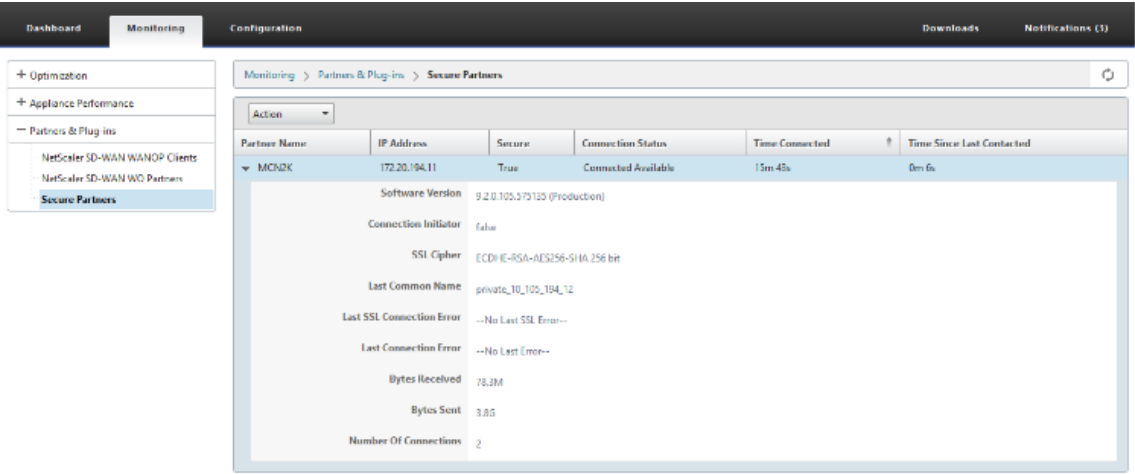
Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.60 bps	1	3	6	0m 5s	Not Applicable

2. Sur l'appliance **partenaire**, affichez les informations **Secure Partner** sur l'appliance Pre-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

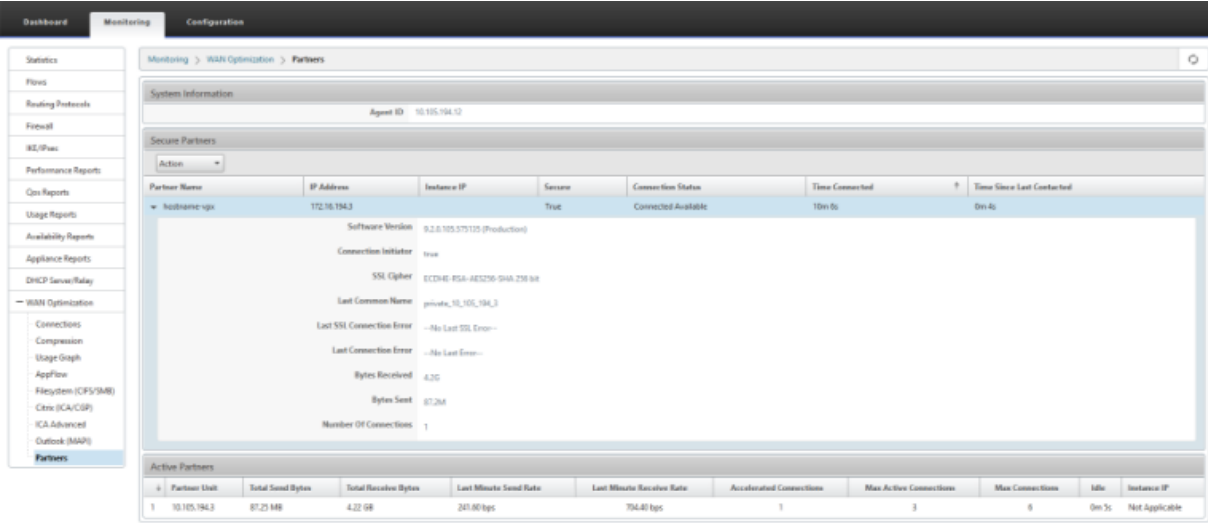
761

mium (Enterprise) Edition sous **Surveillance > Partenaires > Partenaires sécurisés.**



Résolution des problèmes

Affichez les informations de **réussite et d'échec des partenaires sécurisés** sur l'appliance Premium (Enterprise) Edition sous **Surveillance > Optimisation WAN > Partenaires > Partenaires sécurisés.**



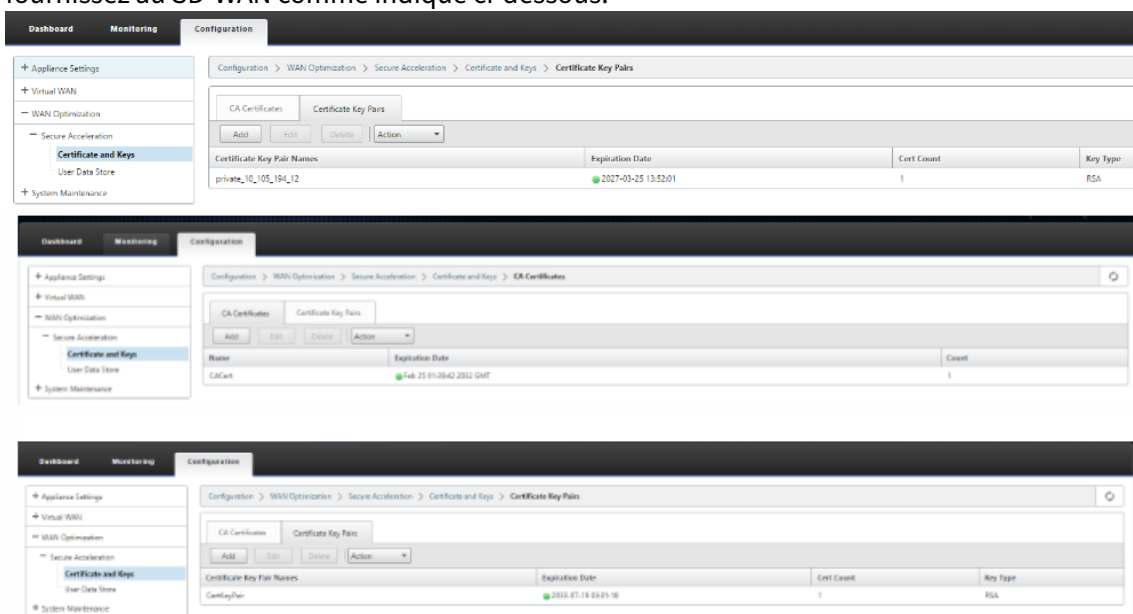
Peering sécurisé manuel lancé à partir de l'appliance PE sur le site DC vers l'appliance SD-WAN autonome Branch et l'appliance WANOP

May 6, 2021

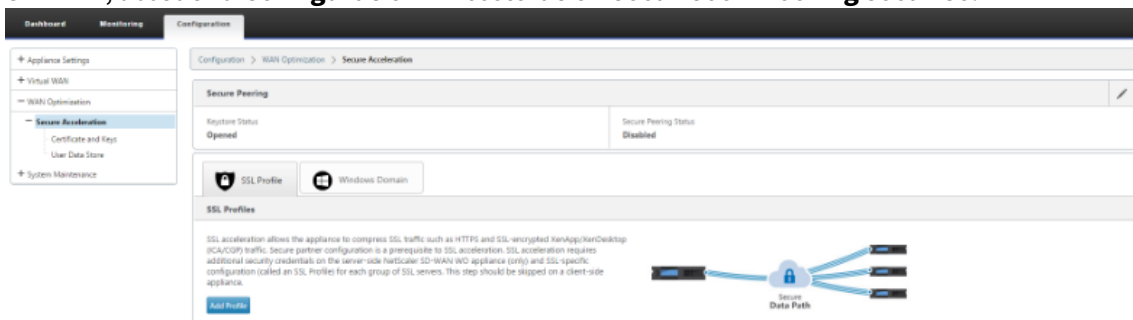
- L'appliance DC PE est en mode LISTEN ON (sur le port 443).
- L'appliance Branch PE est en mode CONNECT-TO.

- LISTEN-ON IP for PE se trouve dans l'adresse IP de l'interface associée au domaine de routage pour lequel « Rediriger vers WANOP » est activé.
- Chargez manuellement les certificats de paires d'autorité de certification et de clé de certification obtenus à partir d'une source authentique d'autorité de certification.

1. Chargez le **certificat CA** et le **certificat de clé CA** obtenu à partir d'un certificat authentique et fournissez au SD-WAN comme indiqué ci-dessous.



2. Sur une nouvelle appliance PE (Premium Edition) sur le site DC, dans l'interface graphique Web SD-WAN, accédez à **Configuration > Accélération sécurisée > Peering sécurisé**.



3. Activez le keystore en fournissant le mot de **passse du keystore** ou désactivez le keystore.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password

DashboardMonitoringConfiguration

Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*
Open

☐ Change Keystore Password
☐ Disable Keystore Password
☐ Reset Keystore

SaveCancel

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

SaveCancel

4. Activez le peering sécurisé en sélectionnant le bouton radio **Certificat de l'autorité** de certification et en fournissant les certificats de paires de clés de l'autorité de certification et de l'autorité de certification chargés de manière appropriée, comme indiqué ci-dessous.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☐ Private CA ☒ CA Certificate

Certificate/Key Pair Name
CAKeyPair

CA Certificate Store Name
CA

Certificate Verification*
Signature/Expiration

SSL Cipher Specification
!ADH:!AECDH:!MD5:HIGH:@STRENGTH

☐ Edit Cipher Specification

SaveCancel

5. Fournissez l'adresse IP virtuelle de la machine distante avec le port 443 comme illustré ci-dessous.

Listen On and Connect To

Connect To
172.16.194.3 443

SaveCancel

Done

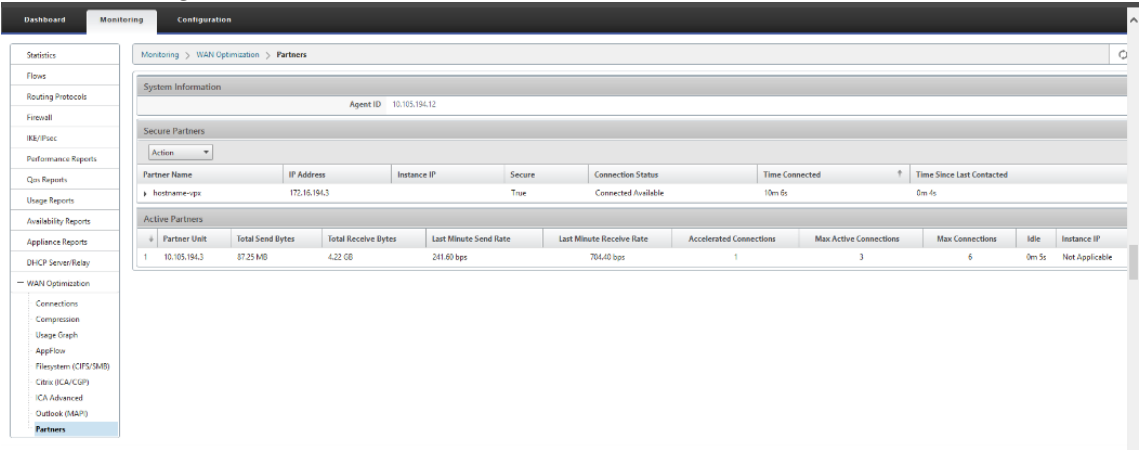
Listen On and Connect To

NAT IP published Yes	Auto Discovery Enabled	Listening On 172.20.194.11:443	Connected to 172.16.194.3:443
-------------------------	---------------------------	-----------------------------------	----------------------------------

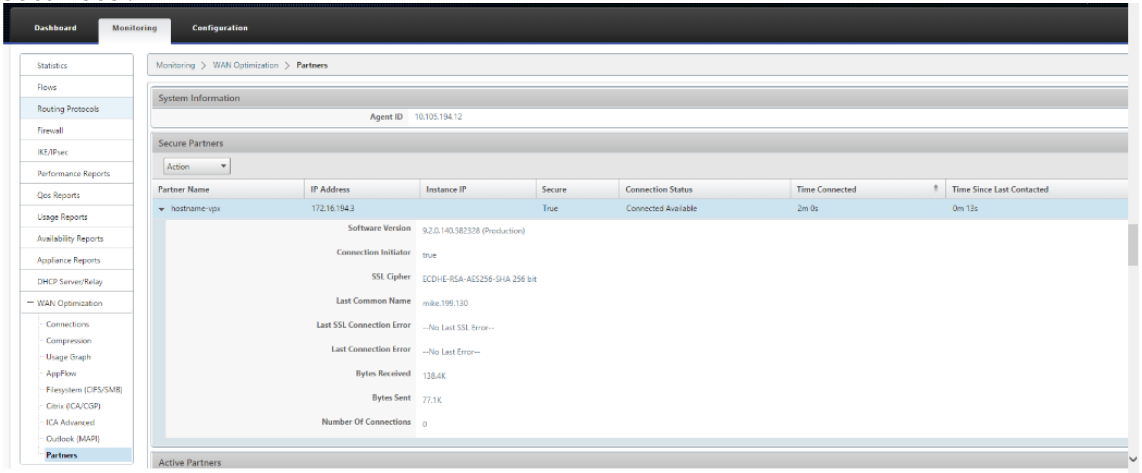
Done

Surveillance

1. Affichez les informations sur les partenaires sécurisés sur l’appliance Premium (Enterprise) Edition sous la page **Surveillance > Optimisation du réseau étendu > Partenaires**.



2. Sur l’appliance partenaire, consultez les informations sur les partenaires sécurisés sur l’appliance Premium (Enterprise) Edition sous la page **Surveillance > Partenaires > Partenaires sécurisés**.



Résolution des problèmes

1. Affichez les **informations sur le succès et les échecs**du partenaire sécurisé sur l’appliance Premium (Enterprise) Edition, sous **Surveillance > Optimisation du réseau étendu > Partenaires > Partenaires sécurisés**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

WSN/Pass

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

WAN Optimization

Partners

Monitoring > WAN Optimization > Partners

System Information

Agent ID: 10.105.194.12

Secure Partners

Action

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 4s	0m 4s

Software Version

6.2.0.101.571315 (Production)

Connection Initiator

true

SSL Cipher

FCDHE-RSA-AES128-GCM-SHA-256 (a)

Last Common Name

private_10_105_194_3

Last SSL Connection Error

--No Last SSL Error--

Last Connection Error

--No Last Error--

Bytes Received

420

Bytes Sent

67284

Number Of Connections

1

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	247.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. Sur l’appliance partenaire, consultez **Informations sur le partenaire sécurisé** sur l’appliance Premium (Enterprise) Edition sous la page **Surveillance > Performances de l’appliance > Journalisation**.

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

Appliance Performance

Compression Engine

Logging

WCCP

AppFlow

Load Statistics

+ Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Action

Search

Record	Date/Time	Details
5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info

Création d'utilisateurs de jointure de domaine et de délégation

May 6, 2021

Pour configurer une nouvelle appliance Premium (Enterprise) Edition (PE) sur le domaine DC to windows :

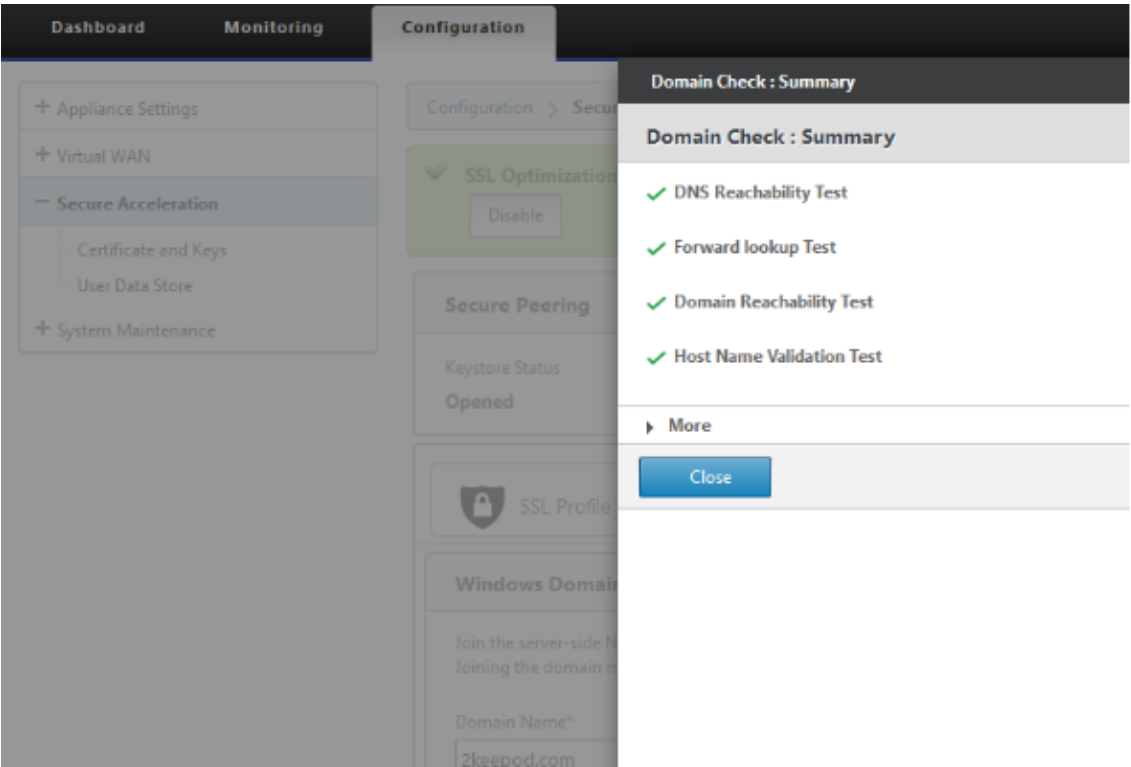
1. Accédez à **Domaine Windows** dans l'interface graphique Web SD-WAN, accédez à **Configuration > Accélération sécurisée >** et cliquez sur **Joindre le domaine Windows**.

The screenshot displays the Citrix SD-WAN Web GUI configuration interface. On the left, a sidebar menu shows 'Secure Acceleration' as the selected section. The main content area is titled 'Configuration > Secure Acceleration'. It features a green banner indicating 'SSL Optimization status : ACTIVE' with a 'Disable' button. Below this, the 'Secure Peering' section shows 'Keystore Status' as 'Opened' and 'Secure Peering Status' as 'Enabled'. The 'Windows Domain' tab is active, showing a 'Join Windows Domain' button. A detailed 'Windows Domain' join form is also visible, containing the following fields and options:

- Domain Name***: A text input field with a 'Check Domain Join' button below it.
- User Name***: A text input field.
- Password***: A text input field.
- Leave Domain**: A checkbox.
- DNS Servers***: A dropdown menu showing '10.105.194.17' and a checkmark icon.

At the bottom of the form are 'OK' and 'Cancel' buttons.

2. Fournissez un **nom de domaine Windows** et effectuez des pré-vérifications de **jointure de domaine**.



3. Après que le récapitulatif de pré-vérification s’affiche comme réussi, entrez les informations d’identification du contrôleur de domaine.

SSL Profile Windows Domain

Windows Domain

Join the server-side NetScaler SD-WAN appliance to a domain that the Windows file server and Exchange server are a part of. Joining the domain makes the appliance a trusted member of the Windows security system.

Domain Name*
2keepod.com [Check Domain Join](#)

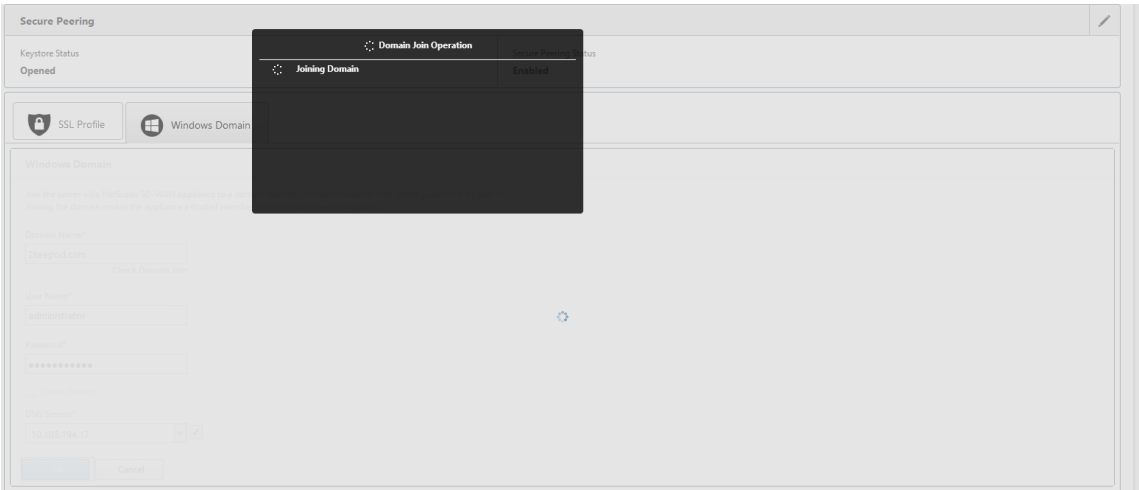
User Name*
administrator

Password*
•••••••• ⓘ

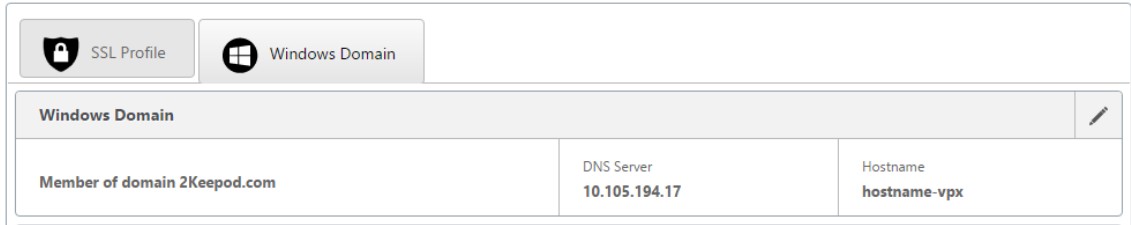
☐ Leave Domain

DNS Servers*
10.105.194.17 ✓

OK Cancel

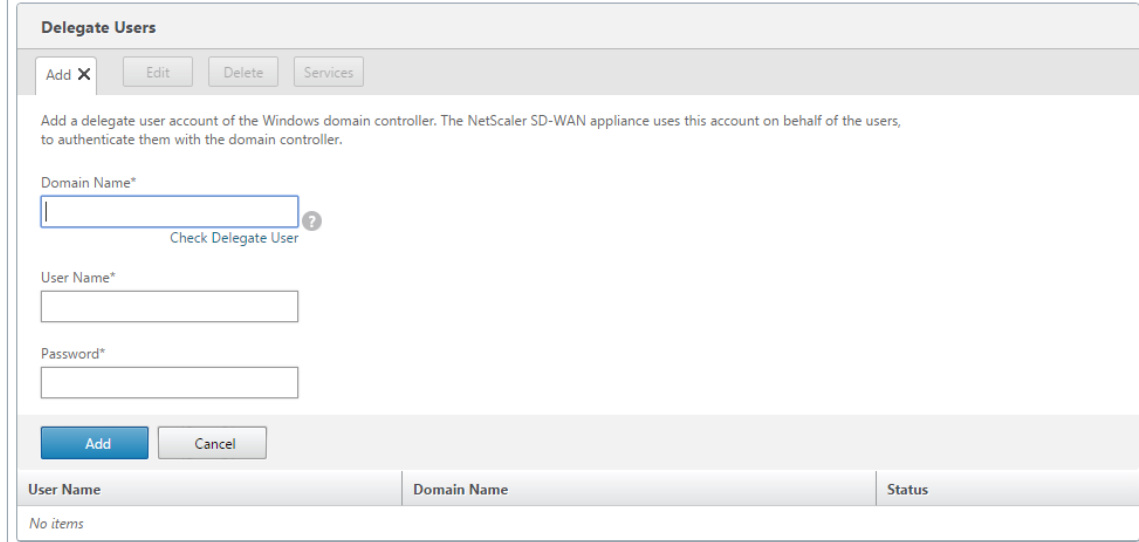


4. En cas de jointure réussie de domaine, vous obtenez la sortie suivante.

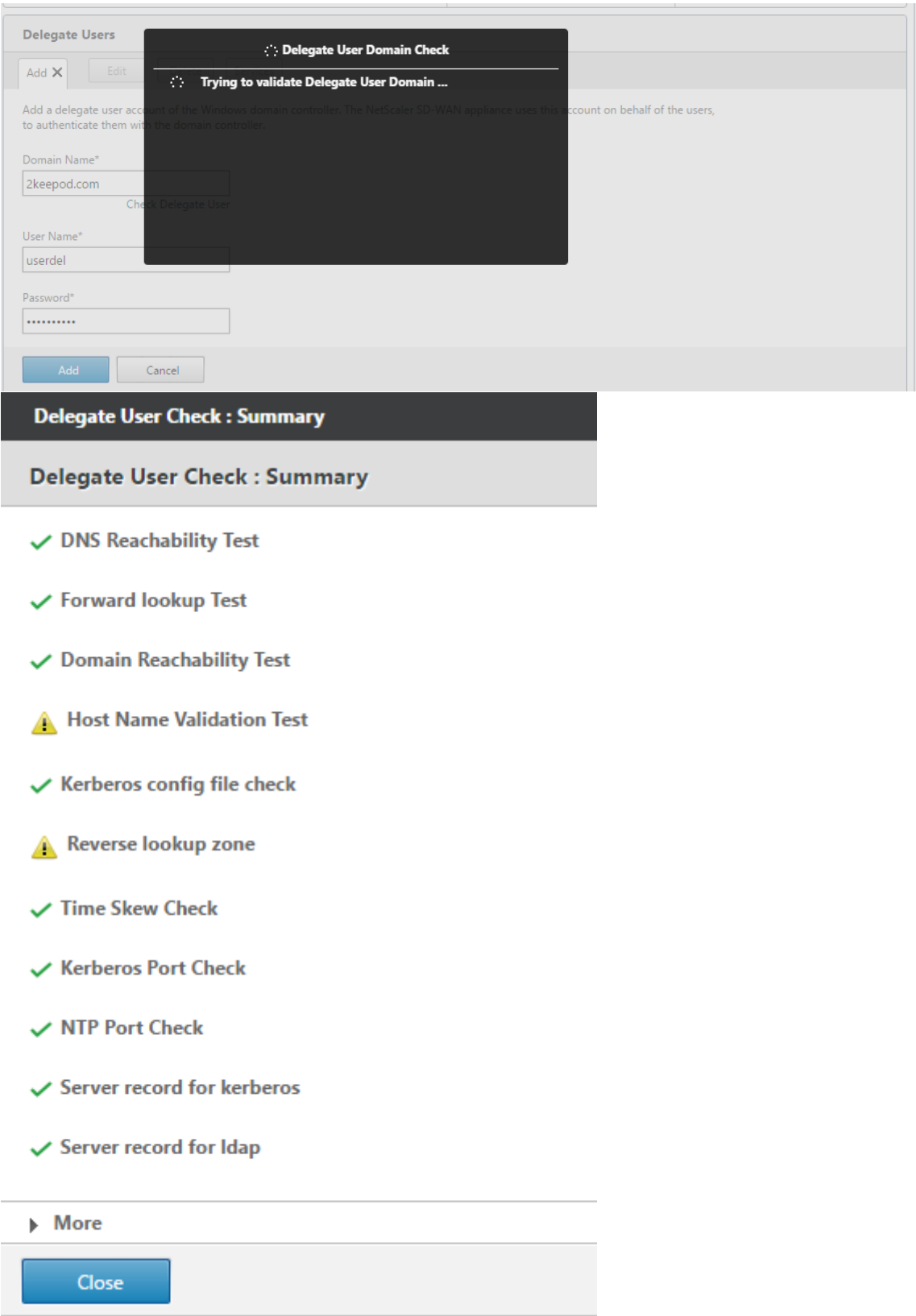


Déléguer l'utilisateur

1. Ajoutez un utilisateur délégué pour déléguer les services comme indiqué ci-dessous.



2. Indiquez le nom de domaine correct et effectuez une pré-vérification de l'utilisateur délégué.



3. Une fois les vérifications préalables de l'utilisateur délégué réussies, fournissez des informa-

tions d'identification valides de l'utilisateur délégué.

Delegate Users

Add X

Edit

Delete

Services

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name*

2keepod.com

Check Delegate User

User Name*

userdel

Password*

.....?

Add

Cancel

4. Une fois l'utilisateur délégué ajouté avec succès au SD-WAN, vous remarquez un message de réussite.

Delegate Users		
<div><div>Add ▼</div><div>Edit</div><div>Delete</div><div>Services</div></div>		
User Name	Domain Name	Status
userdel	ZKEEPOD.COM	Success

5. Pour vérifier quels services sont délégués par l'utilisateur délégué, pointez sur l'utilisateur et sélectionnez les services.

Delegate User Details

Delegate User Details

X

Services

cifs/WIN-KJ8BEBNRUD.2KEEPOD.COM/2KEEPOD.COM

exchangeMDB/WIN-KJ8BEBNRUD.2KEEPOD.COM

Close

Sécurité

May 6, 2021

Les rubriques de cette section fournissent des conseils de sécurité généraux pour les déploiements Citrix SD-WAN.

Instructions de déploiement Citrix SD-WAN

Pour maintenir la sécurité tout au long du cycle de vie du déploiement, Citrix recommande les considérations de sécurité suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

771

- Sécurité physique
- Sécurité de l'apppliance
- Sécurité du réseau
- Administration et gestion

Les rubriques décrites dans les liens suivants fournissent plus d'informations sur la configuration de la sécurité pour les réseaux SD-WAN à l'aide de :

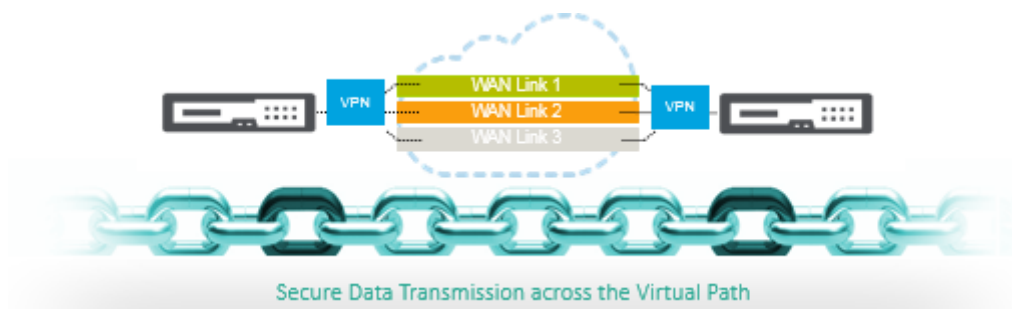
- [Tunnels IPSec](#)
- [Pare-feu](#)

Terminaison du tunnel IPSec

May 6, 2021

Citrix SD-WAN prend en charge les chemins virtuels IPSec, ce qui permet aux périphériques tiers de mettre fin aux tunnels VPN IPSec sur le côté LAN ou WAN d'une appliance Citrix SD-WAN. Vous pouvez sécuriser les tunnels IPSec site à site se terminant sur une appliance SD-WAN à l'aide d'un binaire cryptographique IPSec certifié FIPS 140-2 Niveau 1.

Citrix SD-WAN prend également en charge le tunneling IPSec résilient à l'aide d'un mécanisme de tunneling de chemin virtuel différencié.



Intégration de Citrix SD-WAN avec AWS Transit Gateway

May 6, 2021

Le service Transit Gateway Amazon Web Service (AWS) permet aux clients de connecter leurs Cloud Private Clouds (VPC) Amazon Virtual Private Clouds (VPC) et leurs réseaux locaux à une seule passerelle. À mesure que le nombre de charges de travail exécutées sur AWS augmente, vous pouvez mettre à l'échelle vos réseaux sur plusieurs comptes et VPC Amazon pour suivre la croissance.

Vous pouvez désormais connecter des paires de VPC Amazon à l'aide de l'appairage. Toutefois, la gestion de la connectivité point à point sur de nombreux VPC Amazon, sans la possibilité de gérer de manière centralisée les stratégies de connectivité, peut s'avérer coûteuse et lourde sur le plan opérationnel. Pour la connectivité sur site, vous devez attacher votre VPN AWS à chaque VPC Amazon individuel. Cette solution peut prendre du temps à construire et être difficile à gérer lorsque le nombre de VPC augmente en centaines.

Avec **AWS Transit Gateway**, il vous suffit de créer et de gérer une connexion unique depuis la passerelle centrale vers chaque Amazon VPC, centre de données local ou bureau distant sur votre réseau. Le Transit Gateway agit comme un hub qui contrôle la façon dont le trafic est acheminé entre tous les réseaux connectés qui agissent comme des rayons. Ce modèle de hub et de rayon simplifie considérablement la gestion et réduit les coûts d'exploitation, car chaque réseau ne doit se connecter qu'à la passerelle de transit et non à tous les autres réseaux. Tout nouveau VPC est connecté à Transit Gateway et automatiquement disponible pour tous les autres réseaux connectés à Transit Gateway. Cette facilité de connectivité facilite la mise à l'échelle de votre réseau au fur et à mesure de votre croissance.

Au fur et à mesure que les entreprises migrent un nombre croissant d'applications, de services et d'infrastructures vers le cloud, elles déploient rapidement le SD-WAN pour profiter des avantages de la connectivité haut débit et connecter directement les utilisateurs des sites de succursale aux ressources cloud. La complexité de la création et de la gestion de réseaux privés mondiaux à l'aide de services de transport Internet pour connecter des sites répartis géographiquement et des utilisateurs à des ressources cloud basées sur la proximité pose de nombreux défis. **AWS Transit Gateway Network Manager** modifie ce paradigme. Désormais, les clients de Citrix SD-WAN qui utilisent AWS peuvent utiliser Citrix SD-WAN avec la passerelle de transit AWS en intégrant l'appliance de succursale Citrix SD-WAN AWS Transit Gateway afin d'offrir une expérience de la plus haute qualité aux utilisateurs avec la possibilité d'atteindre tous les VPC connectés à Transit Gateway.

Voici les étapes à suivre pour intégrer Citrix SD-WAN à AWS Transit Gateway :

1. Créez AWS Transit Gateway.
2. Attachez un VPN à Transit Gateway (VPN existant ou nouveau).
3. Attachez un VPN à la passerelle Transit Gateway configurée où le VPN se trouve avec un site SD-WAN situé sur site Web ou dans n'importe quel cloud (AWS, Azure ou GCP).
4. Établissez l'appairage BGP (Border Gateway Protocol) sur le tunnel IPsec avec AWS Transit Gateway à partir de Citrix SD-WAN pour apprendre les réseaux (VPC) connectés à Transit Gateway.

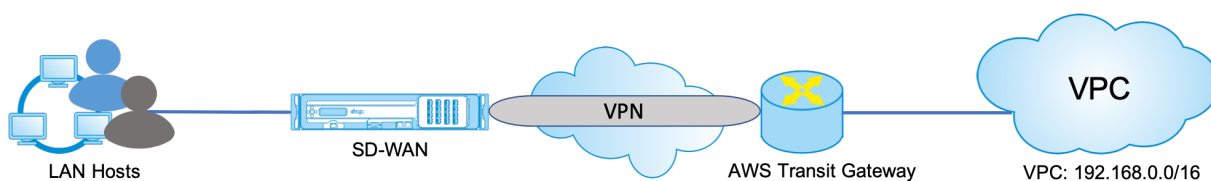
Cas d'utilisation

Le cas d'utilisation consiste à contacter les ressources déployées au sein d'AWS (dans n'importe quel VPC) à partir de l'environnement de branche. L'utilisation d'AWS Transit Gateway permet au trafic

d'atteindre tous les VPC connectés à Transit Gateway sans avoir à gérer les routes BGP. Pour ce faire, effectuez les méthodes suivantes :

- Établissez l'IPsec vers AWS Transit Gateway à partir de l'appliance Citrix SD-WAN de la branche. Dans cette méthode de déploiement, vous n'obtiendrez pas tous les avantages SD-WAN car le trafic passera sur IPsec.
- Déployez une appliance Citrix SD-WAN dans AWS et connectez-la à votre appliance Citrix SD-WAN sur site via un chemin virtuel.

Quelle que soit la méthode choisie, le trafic atteint les VPC connectés à Transit Gateway sans gérer manuellement le routage dans AWS infra.

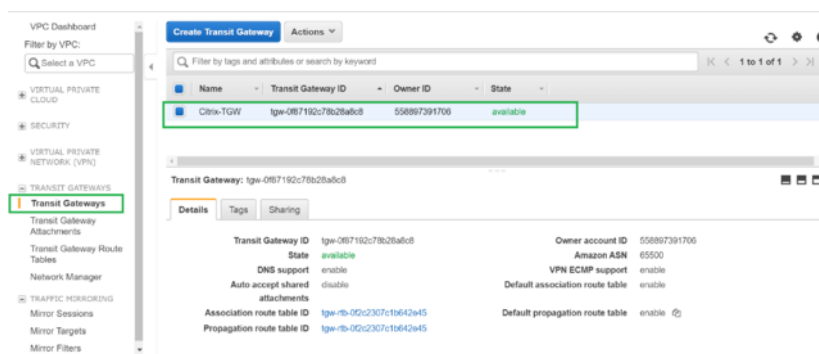


Configuration AWS Transit Gateway

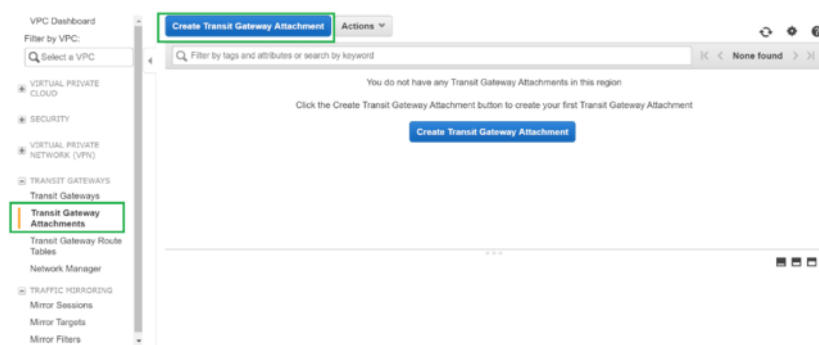
Pour créer **AWS Transit Gateway**, accédez au tableau de bord VPC et accédez à la section **Transit Gateway**.

1. Indiquez le nom, la description et le numéro ASN Amazon Transit Gateway comme indiqué dans la capture d'écran suivante, puis cliquez sur **Créer une passerelle de transit**.

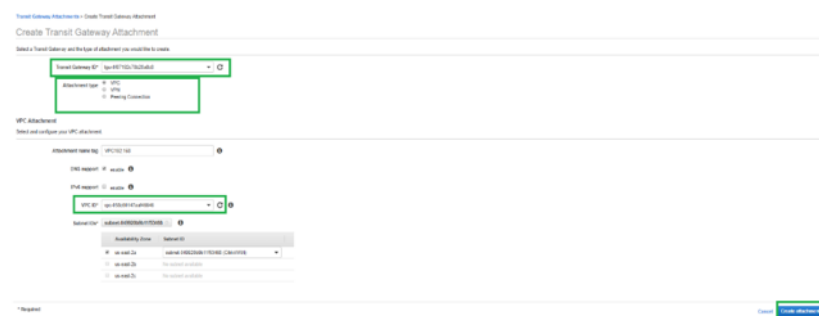
Une fois la création de la passerelle de transit terminée, vous pouvez voir le statut **Disponible**.



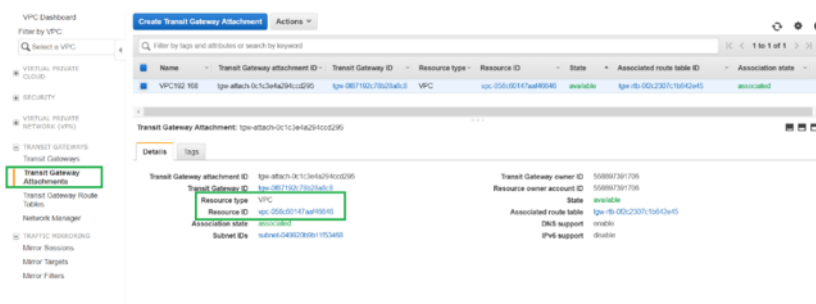
2. Pour créer les **pièces jointes de la passerelle de transit**, accédez à **Passerelles de transit > Pièces jointes de passerelle de transit** et cliquez sur **Créer une pièce jointe de passerelle**



3. Sélectionnez la passerelle Transit créée dans la liste déroulante et sélectionnez le type de pièce jointe en tant que **VPC**. Indiquez la balise de nom de pièce jointe et sélectionnez l'ID de VPC que vous souhaitez attacher à la Transit Gateway créée. L'un des sous-réseaux du VPC sélectionné sera sélectionné automatiquement. Cliquez sur **Créer une pièce jointe** pour attacher VPC à la passerelle Transit.

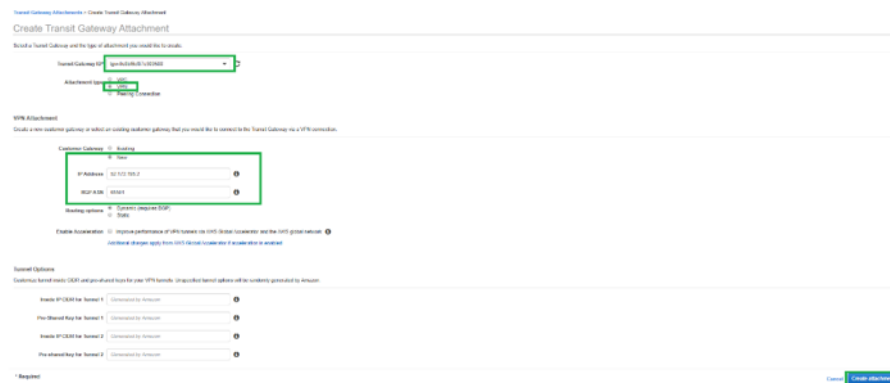


4. Après avoir attaché le VPC à la passerelle de transit, vous pouvez voir que le **type de ressource VPC** a été associé à la passerelle Transit.

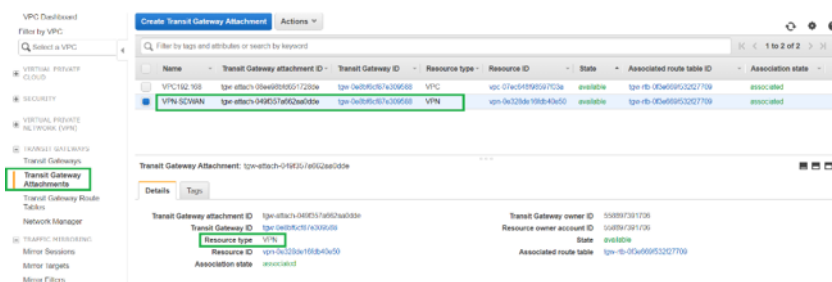


5. Pour attacher le SD-WAN à la passerelle de transit à l'aide du VPN, sélectionnez l'**ID de passerelle Transit** dans la liste déroulante et sélectionnez **Type de pièce jointe** en tant que **VPN**. Assurez-vous de sélectionner le bon ID Transit Gateway.

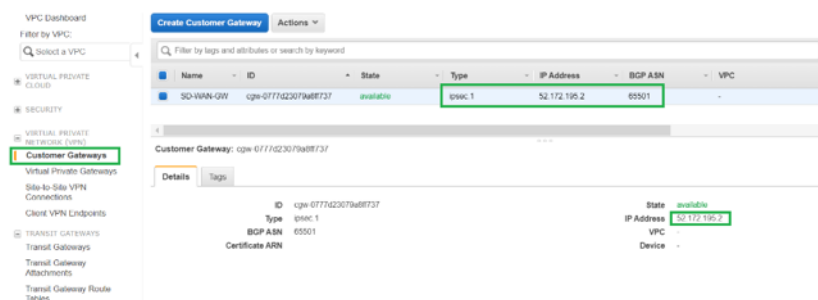
Joignez une nouvelle passerelle client VPN en fournissant l'adresse IP publique du lien WAN SD-WAN et son numéro ASN BGP. Cliquez sur **Créer une pièce jointe** pour attacher VPN à Transit Gateway.



6. Une fois le VPN attaché à la Transit Gateway, vous pouvez afficher les détails comme indiqué dans la capture d'écran suivante :

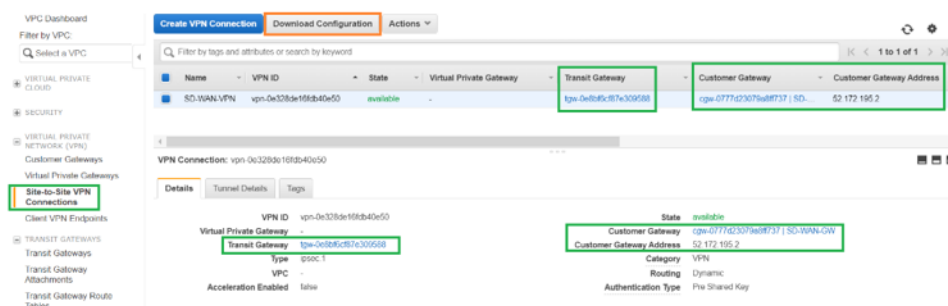


7. Sous **Passerelles client**, la **passerelle** client SD-WAN et la connexion VPN de site à site sont créées dans le cadre de l'Attachement VPN à Transit Gateway. Vous pouvez voir que la passerelle client SD-WAN est créée avec l'adresse IP de cette passerelle client qui représente l'adresse IP publique de liaison WAN du SD-WAN.

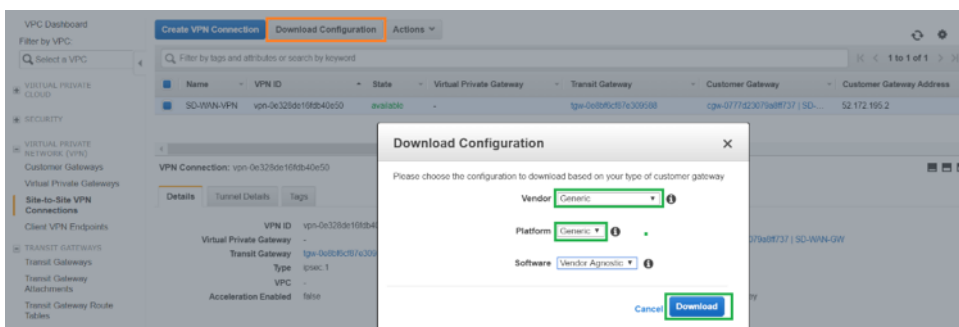


8. Accédez à **Connexions VPN site à site** pour télécharger la **configuration VPN SD-WAN Customer Gateway**. Ce fichier de configuration contient deux détails de tunnel IPsec ainsi que les informations d'homologue BGP. Deux tunnels sont créés à partir du SD-WAN vers Transit Gateway pour la redondance.

Vous pouvez voir que l'adresse IP publique du lien WAN SD-WAN a été configurée en tant qu'adresse de passerelle client.



9. Cliquez sur **Télécharger la configuration** et téléchargez le fichier de configuration VPN. Sélectionnez le **fournisseur**, la **plate-forme** comme **générique** et le **logiciel** comme **fournisseur indépendant**.



Le fichier de configuration téléchargé contient les informations suivantes :

- Configuration IKE
- Configuration IPsec pour AWS Transit Gateway
- Configuration de l'interface tunnel
- Configuration BGP

Ces informations sont disponibles pour deux tunnels IPsec pour la haute disponibilité (HA). Assurez-vous de configurer les deux points d'extrémité du tunnel lors de la configuration dans SD-WAN. Voir la capture d'écran suivante pour référence :

#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is associated with the IPsec tunnel. All traffic transmitted to the tunnel interface is encrypted and transmitted to the Virtual Private Gateway.

The Customer Gateway and Virtual Private Gateway each have two addresses that relate to this IPsec tunnel. Each contains an outside address, upon which encrypted traffic is exchanged. Each also contain an inside address associated with the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway was created. Changing the IP address requires the creation of a new Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel interface.

```
Outside IP Addresses:
- Customer Gateway           : 52.172.195.2
- Virtual Private Gateway    : 3.133.37.22
```

```

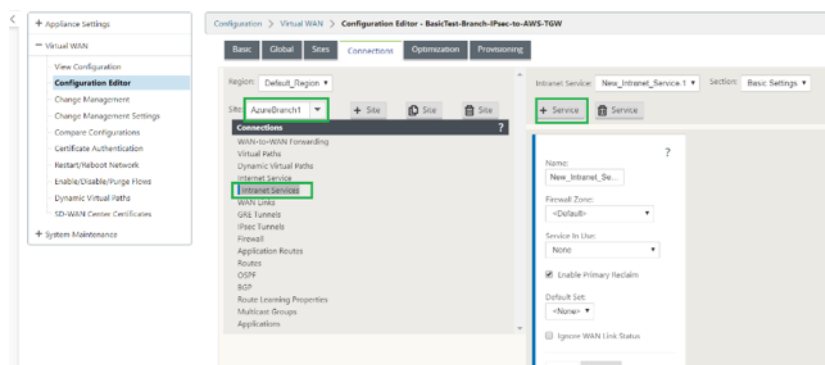
Inside IP Addresses
- Customer Gateway      : 169.254.216.178/30
- Virtual Private Gateway : 169.254.216.177/30

```

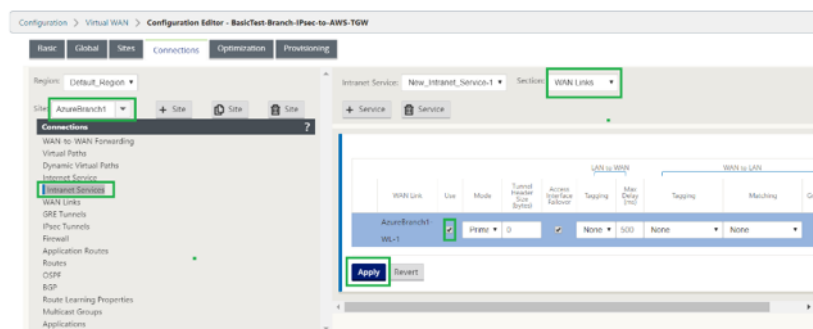
```
Configure your tunnel to fragment at the optimal size:
- Tunnel interface MTU      : 1436 bytes
```

Configurer le service Intranet sur SD-WAN

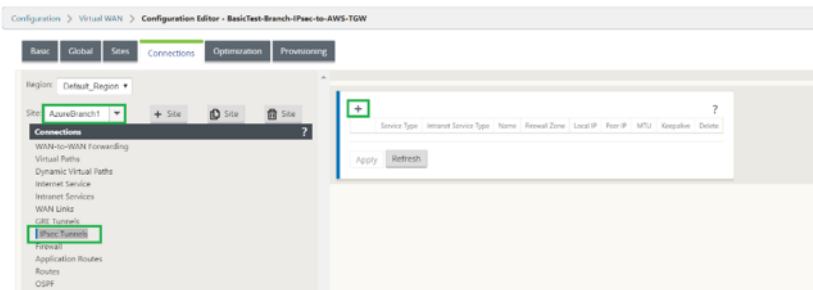
1. Pour configurer le service Intranet utilisé dans la configuration du tunnel IPSec sur SD-WAN, accédez à **Configuration Editor > Connexions**, sélectionnez le site dans la liste déroulante et sélectionnez **Service Intranet**. Cliquez sur **+ Service** pour ajouter un nouveau service Intranet.



- Après l'ajout du service Intranet, sélectionnez le lien WAN (à l'aide duquel vous allez établir le tunnel vers Transit Gateway) qui est utilisé pour ce service.

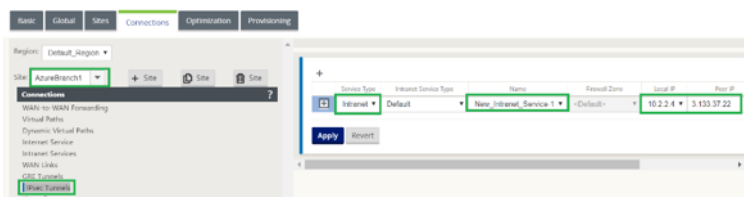


3. Pour configurer le tunnel IPsec vers AWS Transit Gateway, accédez à **Configuration Editor** > **Connexions** sélectionnez le site dans la liste déroulante et cliquez sur **Tunnels IPsec**. Cliquez sur l'option **+** pour ajouter le tunnel IPsec.



4. Sélectionnez le **type de service** en tant qu'**intranet** et sélectionnez le **nom du service Intranet** que vous avez ajouté. Sélectionnez l'adresse **IP locale comme adresse IP** de liaison WAN et l'adresse **d'homologue** comme adresse IP de passerelle privée virtuelle Transit Gateway.

Cochez la case **Keepalive** pour que le tunnel soit lancé par SD-WAN immédiatement après l'activation de la configuration.



5. Configurez les paramètres IKE en fonction du fichier de configuration VPN que vous avez téléchargé à partir d'AWS.

Service Type	Intranet Service Type	Name	Firewall Zone	Local IP	Peer IP
Intranet	Default	New_Intranet_Service-1	<Default>	10.2.2.4	3.133.37.22

IKE Settings

Version: Mode:

Identity: Authentication: Pre-Shared Key:

☒ Validate Peer Identity Peer Identity:

DH Group: Hash Algorithm: Encryption Mode:

Lifetime (s): Lifetime (s) Max: DPD Timeout (s):

6. Configurez les paramètres IPsec en fonction du fichier de configuration VPN que vous avez téléchargé à partir d'AWS. Configurez également **les réseaux protégés IPsec** en fonction du réseau que vous souhaitez envoyer via le tunnel. Vous pouvez voir qu'il est configuré pour autoriser tout trafic via le tunnel IPsec.

IPsec Settings

Tunnel Type: **ESP+Auth**

PFS Group: **Group 2 (MODP1024)**

Encryption Mode: **AES 128-Bit**

Hash Algorithm: **SHA1**

Lifetime (s): **28800**

Lifetime (s) Max: **86400**

Lifetime (KB): **0**

Lifetime (KB) Max: **0**

Network Mismatch Behavior: **Drop**

IPsec Protected Networks + Add

Source IP/Prefix	Destination IP/Prefix
0.0.0.0/0	0.0.0.0/0

Apply **Revert**

7. Configurez la **passerelle client à l'intérieur de l'adresse IP** comme l'une des adresses IP virtuelles du SD-WAN. À partir du fichier de configuration VPN téléchargé, recherchez la Gateway client à l'intérieur de l'adresse IP associée au tunnel-1. Configurez cette passerelle client à l'intérieur de l'adresse IP comme l'une des adresses IP virtuelles sur SD-WAN et activez la case à cocher **Identity**.

Virtual IP Addresses

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Inband Mgmt	Private	Security	Delete
10.2.1.4/24	LAN	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
10.2.2.4/24	WAN	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
10.2.4.1/30	LAN	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Backup Management Network: **<None>**

Apply **Refresh**

8. Ajoutez **des itinéraires** sur SD-WAN pour accéder à la **passerelle privée virtuelle** de Transit Gateway. À partir du fichier de configuration VPN téléchargé, recherchez l'adresse IP à l'intérieur et à l'extérieur de Virtual Private Gateway liée à Tunnel-1. Ajoutez des routes vers l'adresse IP interne et externe de Virtual Private Gateway avec **Type de service** comme **Intranet** et sélectionnez le service Intranet créé dans les étapes ci-dessus.

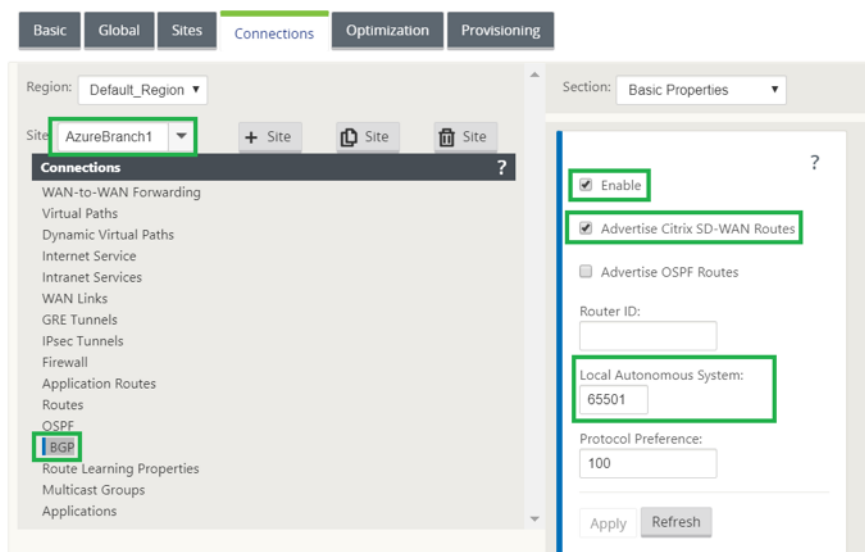
Connections

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	169.254.216.1/32	5	Intranet	New_Intranet_Service-1				
2	3.133.37.22/32	5	Intranet	New_Intranet_Service-1				
3	169.254.216.1/30	5	Local					
4	10.2.1.4/24	5	Local					
5	10.2.2.4/24	5	Local					
6	0.0.0.0/0	5	Intranet	New_Intranet_Service-1				
7	0.0.0.0/0	65535	Passthrough					

9. Configurez **BGP** sur SD-WAN. Activez BGP avec le numéro ASN approprié. Dans le fichier de

configuration VPN téléchargé, recherchez les options de configuration BGP liées au Tunnel-1. Utilisez ces détails pour ajouter un voisin BGP sur SD-WAN.

Pour activer BGP sur SD-WAN, accédez à **Connexions**, sélectionnez le site dans la liste déroulante, puis sélectionnez **BGP**. Cliquez sur **Activer** la case à cocher pour activer BGP. Cliquez sur la case à cocher **Annoncer les routes Citrix SD-WAN** pour annoncer les itinéraires SD-WAN vers Transit Gateway. Utilisez l'**ASN de la passerelle client** à partir des options de configuration BGP et configurez-le en tant que **système autonome local**.



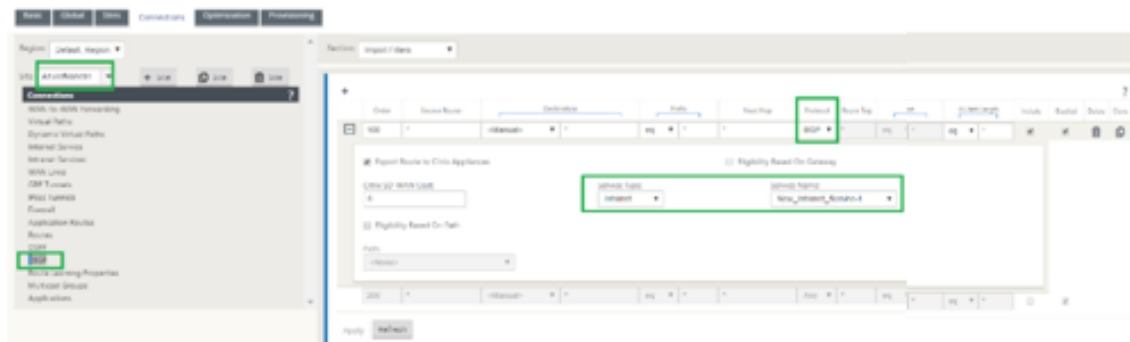
10. Pour ajouter **des voisins** BGP sur SD-WAN, accédez à **Connexions** sélectionnez le site dans la liste déroulante, puis sélectionnez **BGP**. Cliquez sur la section **Voisins** et cliquez sur l'option **+**.

Utilisez l'**adresse IP du voisin** et l'**ASN Virtual Private Gateway** à partir des options de configuration BGP lors de l'ajout d'un voisin. L'adresse **IP source** doit correspondre à la **passerelle client** à l'intérieur de l'adresse IP (configurée en tant qu'adresse IP virtuelle sur SD-WAN) à partir du fichier de configuration téléchargé depuis AWS. Ajoutez BGP Neighbor avec **Multi Hop** activé sur SD-WAN.



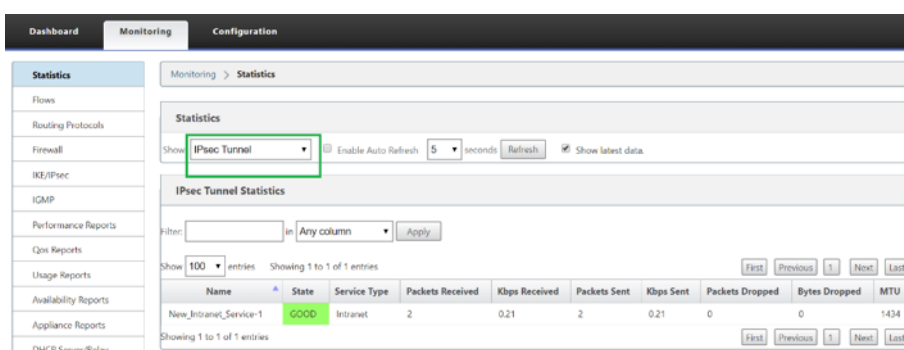
11. Pour ajouter des **filtres d'importation** pour importer des routes BGP sur SD-WAN, accédez à **Connexions**, sélectionnez le site dans la liste déroulante, sélectionnez **BGP** et cliquez sur **Importer la section Filtres**. Cliquez sur l'option **+** pour ajouter un filtre d'importation. Sélectionnez le **protocole** comme **BGP** et corresponde à n'importe quel pour importer tous les itinéraires BGP. Sélectionnez le **type de service** comme **Intranet** et sélectionnez le service Intranet créé.

Il s'agit d'importer des routes BGP avec le type de service en tant qu'Intranet.



Surveillance et dépannage sur SD-WAN

1. Pour vérifier l'état de l'établissement du tunnel IPsec sur SD-WAN, accédez à **Surveillance > Statistiques > Tunnel IPsec**. Dans la capture d'écran suivante, vous pouvez voir que le tunnel IPsec est établi à partir du SD-WAN vers AWS Transit Gateway et que l'état est **GOOD**. En outre, vous pouvez surveiller la quantité de trafic envoyé et reçu via ce tunnel IPsec.



2. Pour vérifier l'état d'appairage BGP sur SD-WAN, accédez à **Surveillance > Protocoles de routage** et sélectionnez **État BGP**. Vous pouvez voir que l'état BGP a été signalé comme **Établi** et que l'adresse IP du voisin et l'ASN Neighbor correspondent aux détails du voisin AWS BGP. Avec cela, vous pouvez vous assurer que l'appairage BGP a été établi à partir du SD-WAN vers AWS Transit Gateway via le tunnel IPsec.

The screenshot shows the 'Configuration' tab with 'Routing Protocols' selected. Under 'Dynamic Routing Protocol', the 'BGP State' is configured for the 'Default_RoutingDomain'. The BGP State is 'Established' for the neighbor address '169.254.216.177' (neighbor AS: citrix-40-wan). The configuration includes details like 'Neighbor ID: 169.254.216.177', 'Neighbor caps: refresh AS4', 'Session: external multi-hop AS4', 'Source address: 169.254.216.178', 'Hold timer: 28/30', and 'Keepalive timer: 2/10'.

Un VPC (192.168.0.0) est attaché à AWS Transit Gateway. Le SD-WAN a appris ce réseau VPC (192.168.0.0) d’AWS Transit Gateway via BGP et cette route a été installée sur SD-WAN avec le type de service comme Intranet selon le filtre d’importation créé dans les étapes ci-dessus.

- Pour vérifier l’installation de l’itinéraire BGP sur SD-WAN, accédez à **Monitoring > Statistiques > Itinéraires** et recherchez le réseau 192.168.0.0/16 installé en tant que route BGP avec le type de service comme Intranet. Cela signifie que vous pouvez apprendre les réseaux connectés à AWS Transit Gateway et vous pouvez communiquer avec ces réseaux via IPsec Tunnel établi.

The screenshot shows the 'Monitoring > Statistics > Routes' page. The 'Routes for routing domain : Default_RoutingDomain' are listed. The route for '192.168.0.0/16' is highlighted, showing it is a 'Dynamic BGP' route with a 'Service' of 'New_Intranet_Service-1' and a 'Type' of 'BGP'.

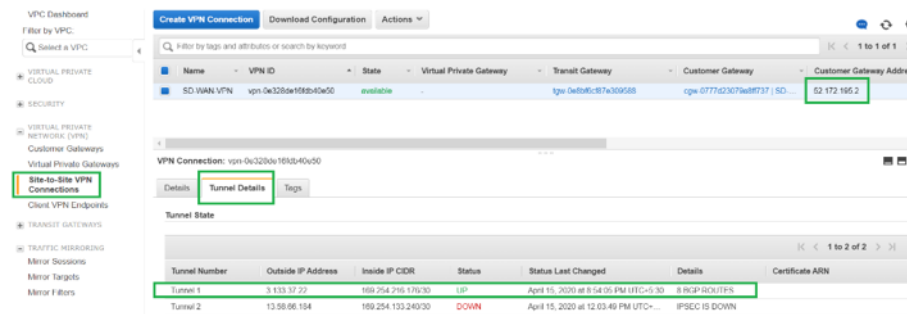
Detail#	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	MR Count	Eligible
0		169.254.216.177/32	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	7	YES
1		3.133.37.22/32	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	11	YES
2		169.254.216.176/30	*	Local	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES
3		192.1.0/24	*	Local	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES
4		10.2.2.0/24	*	Local	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES
5		10.1.2.0/24	*	DCMON-AzureBranch1	Default_LAN_Zone	YES	*	DCMON	Dynamic	Virtual WAN	YES	10	0	YES
6		10.1.1.0/24	*	DCMON-AzureBranch1	Default_LAN_Zone	YES	*	DCMON	Dynamic	Virtual WAN	YES	10	0	YES
7		192.168.0.0/16	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Dynamic	BGP	-	6	0	YES
8		0.0.0.0/0	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES

Surveillance et dépannage sur AWS

- Pour vérifier l’état de l’établissement du tunnel IPsec sur AWS, accédez à **RÉSEAU PRIVÉ VIRTUEL (VPN) > Connexions VPN de site à site**. Dans la capture d’écran suivante, vous pouvez observer que l’adresse de passerelle client représente l’adresse IP publique SD-WAN Link à l’aide de laquelle vous avez établi le tunnel.

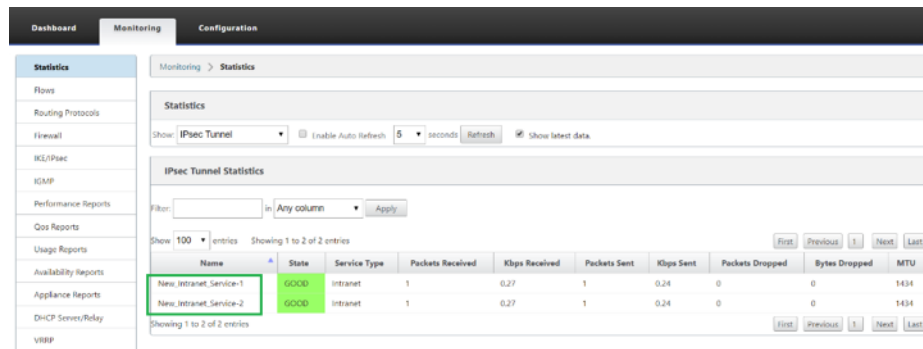
L’état du tunnel s’affiche comme **UP**. On peut également observer qu’AWS a appris **8 ROUTES**

BGP de SD-WAN. Cela signifie que SD-WAN est capable d'établir Tunnel avec AWS Transit Gateway et peut également échanger des itinéraires via BGP.

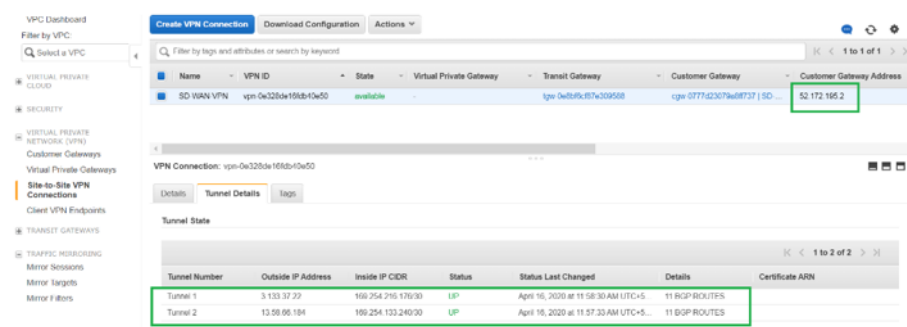


2. Configurez les détails IPsec et BGP relatifs au deuxième tunnel en fonction du fichier de configuration téléchargé sur SD-WAN.

L'état des deux tunnels peut être surveillé sur SD-WAN comme suit :



3. L'état des deux tunnels peut être surveillé sur AWS comme suit :

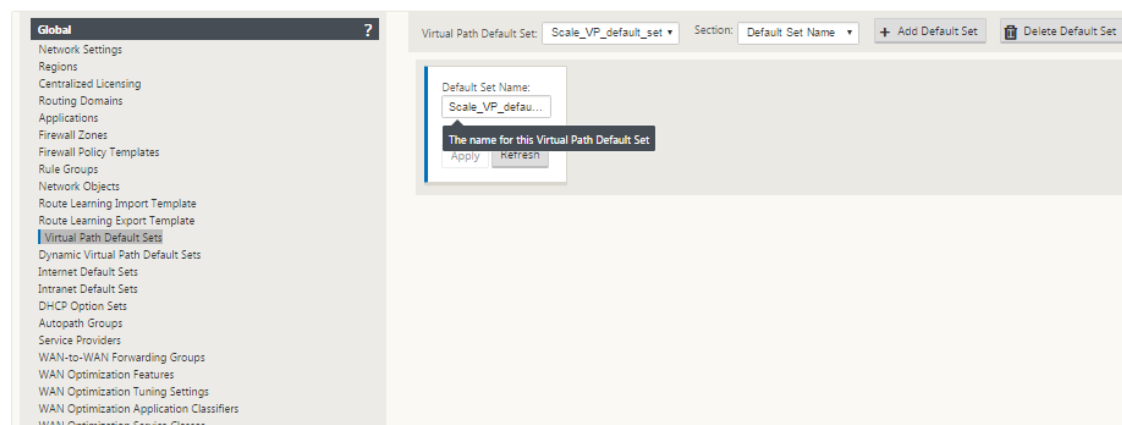


Comment configurer les tunnels IPsec pour les chemins virtuels et dynamiques

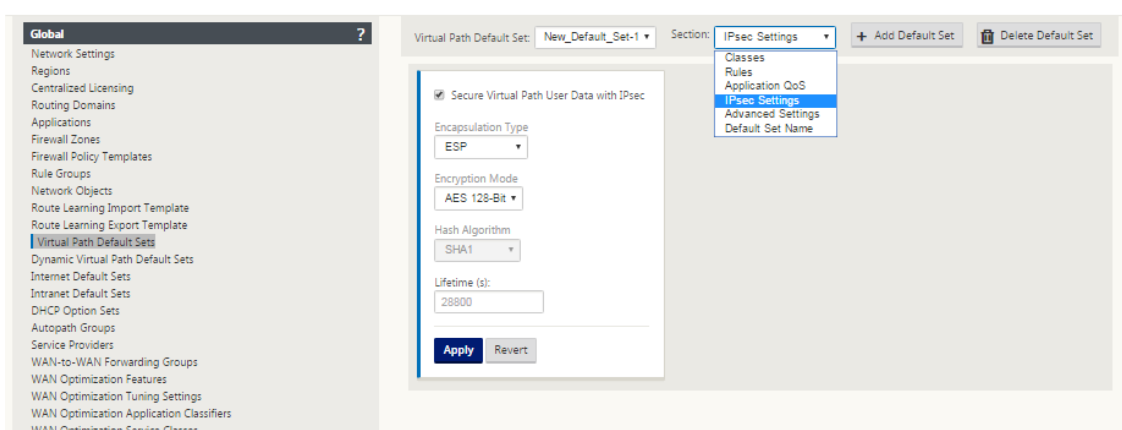
May 6, 2021

Pour configurer les tunnels IPSec pour les chemins virtuels virtuels et dynamiques entre des sites de succursales Citrix SD-WAN :

1. Accédez à **Global > Jeux par défaut de chemins virtuels ou Jeuxpar défaut de chemins virtuels dynamiques**.



2. Créez un nouveau jeu par défaut (chemin virtuel virtuel ou dynamique) et activez **Secure Virtual Path User Data avec IPsec**.
3. Choisissez l'une des options disponibles pour le chiffrement IPsec :
 - Types d'encapsulation : ESP, AH ou ESP+AH
 - Modes de chiffrement : AES-CBC, AES 128 ou 256 bits
 - Algorithme de hachage : SHA1 ou SHA-256
4. Appliquez le jeu par défaut de chemin virtuel créé au nœud MCN. Cela applique automatiquement le même jeu par défaut à tous les nœuds client qui ont le chemin virtuel vers le MCN.

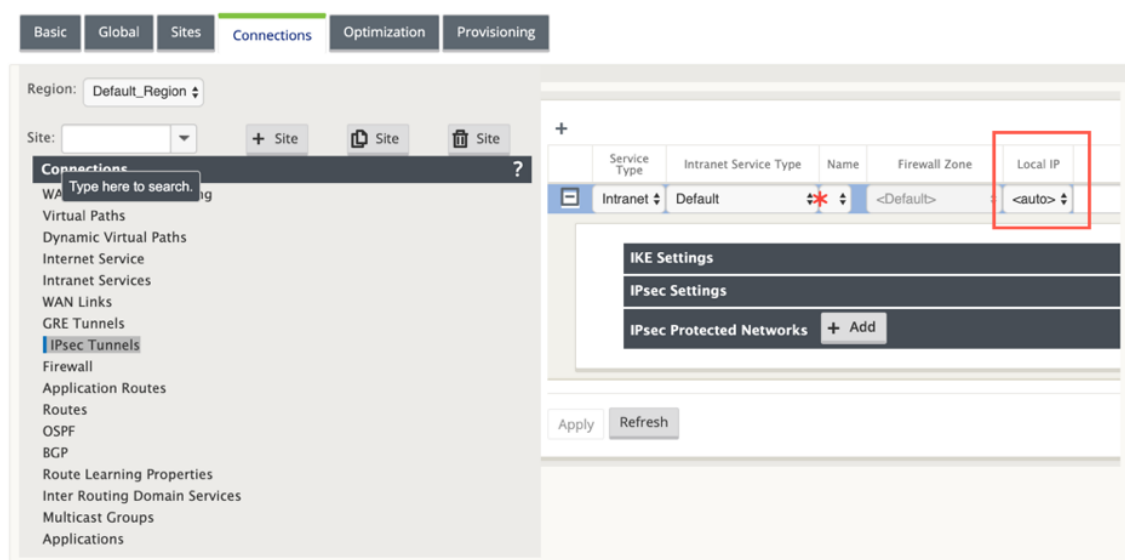


Comment configurer le tunnel IPSec entre SD-WAN et des périphériques tiers

November 1, 2021

Pour configurer le tunnel IPSec pour un service intranet ou LAN :

1. Dans l'**Éditeur de configuration**, accédez à **Connexions** > **Afficher le site** > **[Nom du site]** > **Tunnels IPSec**. Choisissez un **type de service** (réseau local ou intranet).
2. Entrez un **nom** pour le type de service. Pour le type de service Intranet, le serveur Intranet configuré détermine les adresses IP locales disponibles.



Citrix SD-WAN peut désormais établir des tunnels IPSec lorsqu'une liaison WAN est interrompue directement sur l'apppliance et qu'une adresse IP dynamique est affectée à la liaison WAN.

Avec la version 11.1.0, les tunnels IPSec Intranet doivent être configurables lorsque l'adresse IP du tunnel local n'est pas ou ne peut pas être connue. Cela aide à créer des tunnels IPSec sur les interfaces dont l'adresse est attribuée via DHCP.

Lors de la configuration de l'interface pour le tunnel IPSec, une adresse IP de tunnel locale doit être mentionnée. Cette interface est modifiée pour permettre la sélection d'une adresse IP vide lorsque le type de tunnel est **Intranet**.

En outre, l'étiquette d'une adresse non définie est remplacée par **Auto** lorsque le type de tunnel est **Intranet**.

Si l'adresse IP locale est définie comme **Auto**, elle a la possibilité de prendre l'adresse IP qui est incorporée pour l'interface d'accès sur cette liaison WAN. Cette interface d'accès à la liaison

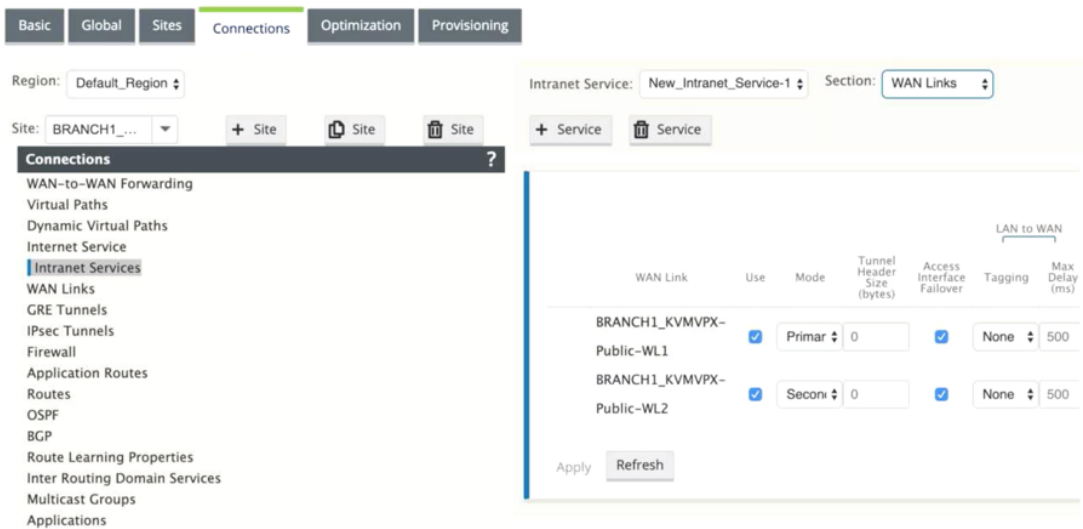
WAN peut obtenir l'adresse IP soit configurée statiquement, soit à partir de DHCP. Le tunnel IPsec est établi à l'aide de l'interface d'accès de liaison WAN principale par défaut.

Auparavant, vous pouvez établir des tunnels IPsec sur une seule liaison WAN. Cela expose l'environnement de la branche à une perte de service pendant les périodes de pannes de liaison pure et simple et lorsque la perte de paquets sur une liaison est élevée par inadvertance pour permettre une connectivité fiable.

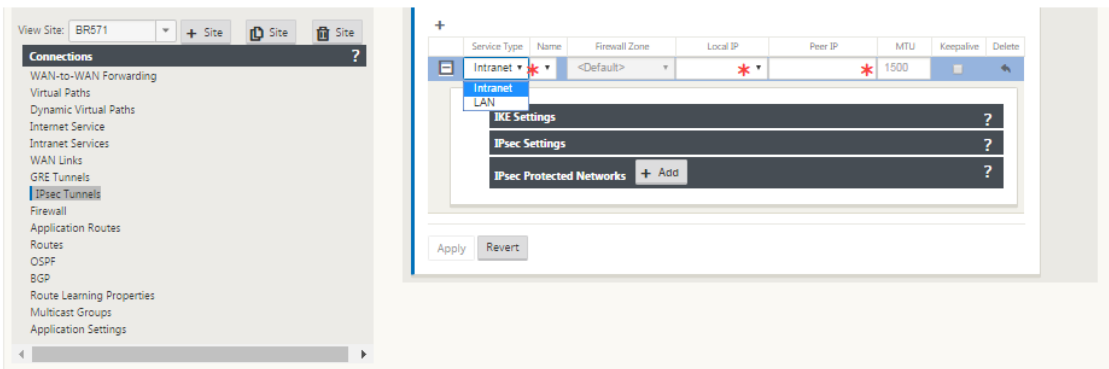
À partir de la version 11.1.0, vous pouvez utiliser deux liaisons WAN pour établir des tunnels IPsec afin de protéger les environnements de branche contre les périodes d'interruption de service. Si le lien principal tombe en panne, le lien secondaire devient actif/haut en quelques millisecondes.

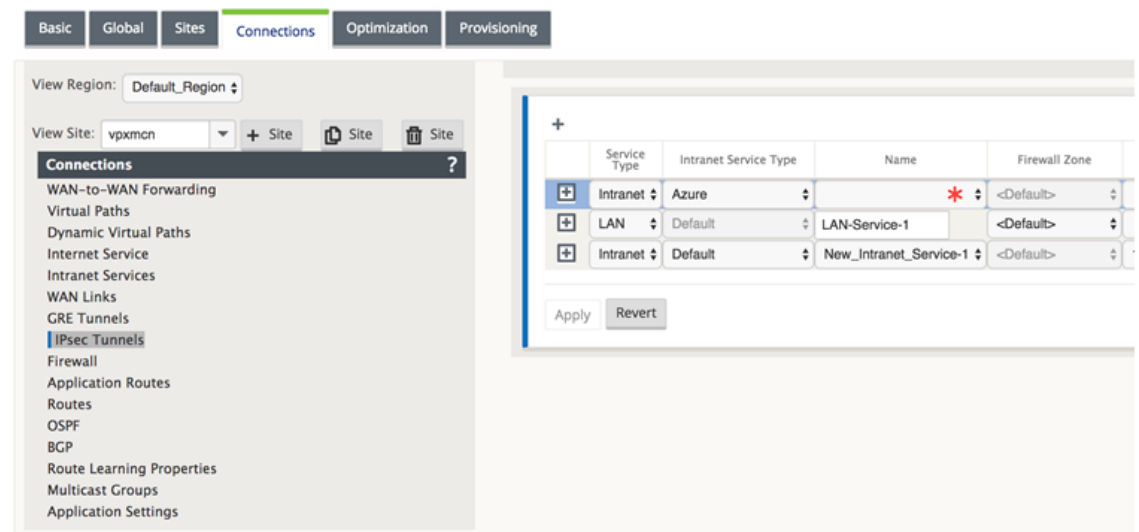
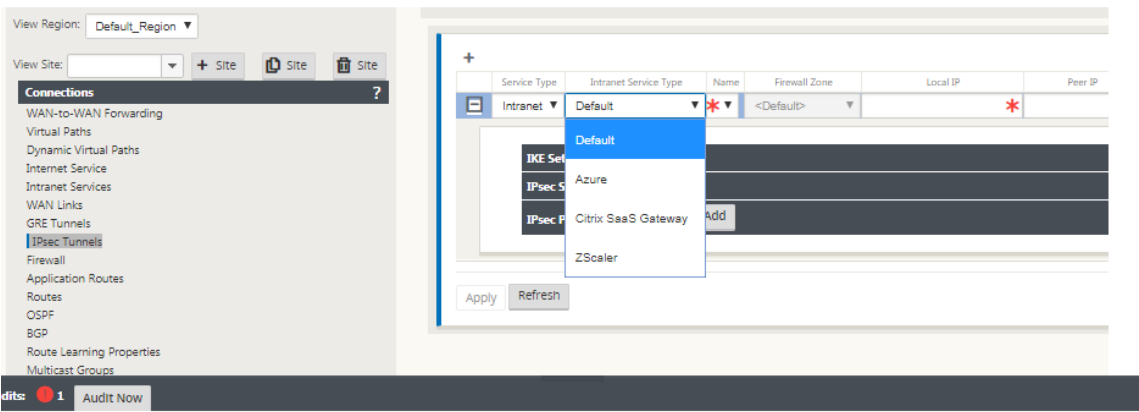
Remarque

Lorsque l'option < Auto >est **sélectionnée**, le tunnel IPsec est établi à l'aide de l'interface d'accès à la liaison WAN principale. Si la liaison WAN principale tombe en panne, le tunnel IPsec est établi à l'aide de l'interface d'accès à la liaison WAN secondaire.



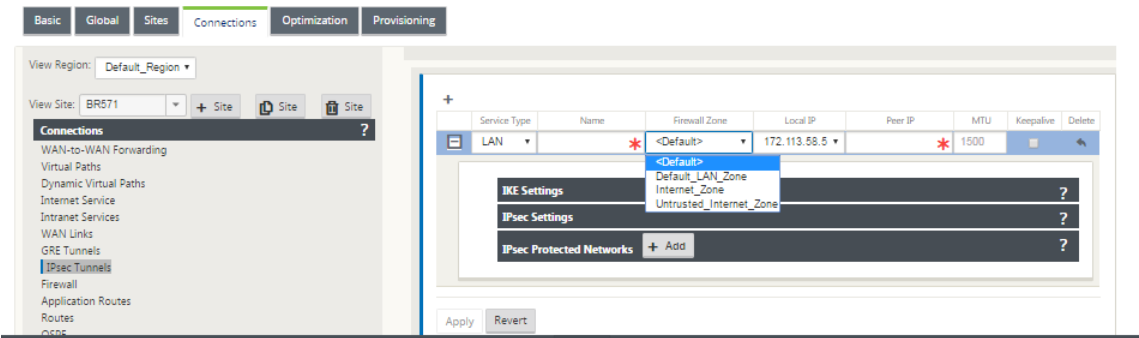
3. Sélectionnez l'adresse **IP locale** disponible et entrez l'adresse **IP homologue** du tunnel IPsec.





Remarque

Si le type de service est Intranet, l'adresse IP est prédéterminée par le service intranet choisi.



4. Configurez les paramètres IPsec en appliquant les critères décrits dans les tableaux suivants. Lorsque vous avez terminé, cliquez sur **Appliquer** pour enregistrer vos paramètres.

Champ	Description	Valeur
Type de service	Choisissez un type de service dans le menu déroulant	Intranet, LAN
Nom	Si le type de service est Intranet, choisissez dans la liste des services intranet configurés dans le menu déroulant. Si le type de service est LAN, entrez un nom unique	Chaîne de texte
IP locale	Choisissez l'adresse IP locale du tunnel IPsec dans le menu déroulant des adresses IP virtuelles disponibles configurées sur ce site	Adresse IP
IP homologue	Entrez l'adresse IP homologue du tunnel IPSec	Adresse IP
MTU	Entrez le MTU pour fragmenter les fragments IKE et IPSec	Valeur par défaut : 1500
Paramètres IKE	Version : Choisissez une version IKE dans le menu déroulant	IKEv1 IKEv2
Mode	Choisissez un mode dans le menu déroulant	Conforme FIPS : Principal, non conforme FIPS : Agressif
Identité	Choisissez une identité dans le menu déroulant	Adresse IP automatique Manuel Adresse IP Adresse IP Utilisateur FQDN
Authentification	Choisissez le type d'authentification dans le menu déroulant	Clé pré-partagée : si vous utilisez une clé pré-partagée, copiez-la dans ce champ. Cliquez sur l'icône Eyeball () pour afficher la clé pré-partagée. Certificat : Si vous utilisez un certificat d'identité, sélectionnez-le dans le menu déroulant.
Valider l'identité homologue	Activez cette case à cocher pour valider le pair de l'IKE. Si le type d'ID du pair n'est pas pris en charge, n'activez pas cette fonctionnalité	Aucun

Champ	Description	Valeur
Groupe DH	Choisissez le groupe Diffie-Hellman à utiliser pour la génération de clés IKE dans le menu déroulant	Non-conforme aux normes FIPS : Groupe 1, conforme aux normes FIPS : Groupe 2 Groupe 5 Groupe 14 Groupe 15 Groupe 16 Groupe 19 Groupe 20 Groupe 21
Algorithme de hachage	Choisissez un algorithme dans le menu déroulant pour authentifier les messages IKE	Non-conforme FIPS : MD5 conforme FIPS : SHA1 SHA-256
Mode de chiffrement	Choisissez le mode de chiffrement des messages IKE dans le menu déroulant.	AES 128 bits AES 192 bits AES 256 bits
Durée de vie (s)	Entrez la durée préférée, en secondes, pour qu'une association de sécurité IKE existe	3600 secondes (par défaut)
Durée de vie (s) max	Entrez la durée maximale préférée, en secondes, pour permettre l'existence d'une association de sécurité IKE	86400 secondes (par défaut)
Délai (s) DPD	Entrez le délai d' expiration de détection des pairs morts , en secondes, pour les connexions VPN	300 secondes (par défaut)
IKEv2	Authentification homologue : choisissez Authentification homologue dans le menu déroulant	Certificat de clé pré-partagée en miroir
IKE2 - Clé pré-partagée	Clé pré-partagée homologue : collez la clé pré-partagée IKEv2 homologue dans ce champ pour l'authentification. Cliquez sur l'icône du globe oculaire () pour afficher la clé pré-partagée	Chaîne de texte

Champ	Description	Valeur
Algorithme d'intégrité	Choisissez un algorithme comme algorithme de hachage à utiliser pour la vérification HMAC dans le menu déroulant	Non-conforme FIPS : MD5 conforme FIPS : SHA1 SHA-256

Remarque :

Si le routeur IPsec terminant inclut le code HMAC (Message Authentication Code) basé sur le hachage dans la configuration, changez le mode IPsec en **Exp+Auth** avec un algorithme de hachage **SHA1**.

IKE Settings?

Version: IKEv1 ▼

Mode: Aggressive ▼

Identity: Auto ▼

Authentication: Pre-Shared Key ▼

Pre-Shared Key:

👁

 *

☒ Validate Peer Identity

Peer Identity: Auto ▼

DH Group: Group 1 (MODP768) ▼

Hash Algorithm: MD5 ▼

Encryption Mode: AES 128-Bit ▼

Lifetime (s): 3600

Lifetime (s) Max: 86400

DPD Timeout (s): 300

IPsec Settings?

IPsec Protected Networks

+ Add

?

IKE Settings?

Version:
IKEv2

Identity:
Auto

Authentication:
Pre-Shared Key

Pre-Shared Key:

Peer Authentication:
Mirrored

☒ Validate Peer Identity

Peer Identity:
Auto

DH Group:
Group 1 (MODP768)

Hash Algorithm:
MD5

Integrity Algorithm:
MD5

Encryption Mode:
AES 128-Bit

Lifetime (s):
3600

Lifetime (s) Max:
86400

DPD Timeout (s):
300

IPsec Settings?

IPsec Protected Networks

+ Add

?

Paramètres réseau protégés IPsec et IPsec :

Champ	Description	Valeur (s)
Type de tunnel	Choisissez le type de tunnel dans le menu déroulant	ESP ESP+Auth ESP+NULL AH
Groupe PFS	Choisissez le groupe Diffie-Hellman à utiliser pour une génération parfaite de clés de secret dans le menu déroulant	Aucun Groupe 1 Groupe 2 Groupe 5 Groupe 14 Groupe 15 Groupe 16 Groupe 19 Groupe 20 Groupe 21
Mode de chiffrement	Choisissez le mode de chiffrement pour les messages IPsec dans le menu déroulant	Si vous avez choisi ESP ou ESP+Auth, sélectionnez l’une des options suivantes : AES 128 bits, AES 192 bits, AES 256 bits, AES 128 bits GCM 64 bits, AES 192 bits GCM 64 bits, AES 256 bits GCM 64 bits, AES 128 bits GCM 96 bits, AES 192 bits GCM 96 bits, AES 256 bits GCM 96 bits, AES 128 bits GCM 128 bits, AES 198 bits GCM 128 bits, AES 256 bits GCM 128 bits. Les AES 128/192/256 bits sont pris en charge par CBC.

Champ	Description	Valeur (s)
Durée de vie (s)	Entrez le temps, en secondes, pour permettre à une association de sécurité IPSec d'exister	28800 secondes (par défaut)
Maximum (s) à vie	Entrez la durée maximale, en secondes, pour permettre l'existence d'une association de sécurité IPSec	86400 secondes (par défaut)
Durée de vie (Ko)	Entrez la quantité de données, en kilo-octets, pour qu'une association de sécurité IPSec existe	Kilo-octets
Durée de vie (Ko) Max	Entrez la quantité maximale de données, en kilo-octets, pour permettre l'existence d'une association de sécurité IPSec	Kilo-octets
Comportement de non-correspondance réseau	Choisissez l'action à entreprendre si un paquet ne correspond pas aux réseaux protégés du tunnel IPsec dans le menu déroulant	Déposer, envoyer non chiffré, utiliser une route non IPSec
Réseaux protégés IPSec	Source IP/préfixe : Après avoir cliqué sur le bouton Ajouter (+ Ajouter), entrez l' adresse IP source et le préfixe du trafic réseau que le tunnel IPsec protégera	Adresse IP
Réseaux protégés IPSec	IP/préfixe de destination : Entrez l' adresse IP de destination et le préfixe du trafic réseau que le tunnel IPsec protégera	Adresse IP

IPsec Settings ?

Tunnel Type: ESP PFS Group: <None>

Encryption Mode: AES 128-Bit

Lifetime (s): 28800 Lifetime (s) Max: 86400

Lifetime (KB): 0 Lifetime (KB) Max: 0

Network Mismatch Behavior: Drop

IPsec Protected Networks + Add ?

Apply

Revert

Remarque

Citrix SD-WAN prend en charge la connectivité à Oracle Cloud Infrastructure (OCI) via IPsec.

Surveiller les tunnels IPsec

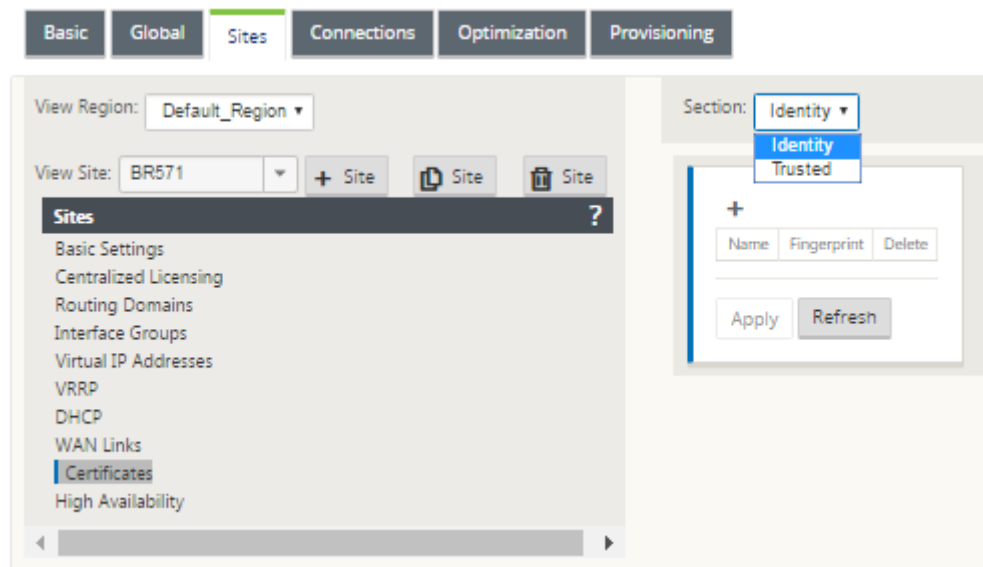
Accédez à **Monitoring > IKE/IPsec** dans l'interface graphique de l'apppliance SD-WAN pour afficher et surveiller la configuration du tunnel IPsec.

Comment ajouter des certificats IKE

May 6, 2021

Pour implémenter des certificats pour la négociation IKE :

1. Accédez à **Sites > Certificats** et ajoutez les certificats nécessaires.



Comment afficher la configuration du tunnel ipsec

May 6, 2021

Pour afficher la configuration du tunnel ipsec :

1. Accédez à **Configuration > Réseau étendu virtuel > Afficher la configuration** .
2. Sélectionnez **Service de chemin virtuel** dans le menu déroulant. Les paramètres IPsec ne s'affichent que si IPsec est activé dans l'éditeur de configuration.

DashboardMonitoringConfiguration

Configuration > Virtual WAN > View Configuration

Configuration

View: Virtual Path Service

Virtual Path Service Configuration

Virtual Path 515 = HCN-5100-88572

Local site(HCN-5100)

Remote site(88572)

Local send rate=20000 kbps

Remote send rate=20000 kbps

On-demand standby link trigger threshold %

IPsec settings=

Routing Domain Enabled:

Default_RoutingDomain

PATHS:

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Alternate Src Port	Alternate Dst Port	Alternate Src Port	Alternate Dst Port	IP DSCP	Encrypt	Loss	Sensitive To
0	HCN-5100-HL-1	88572-HL-1	172.111.64.5	172.111.59.5	-	-	4800	4800	-	-	-	+	ses128	YES
3	HCN-5100-HL-2	88572-HL-2	172.111.65.5	192.113.59.6	-	-	4800	4800	-	-	-	+	ses128	YES
1	HCN-5100-HL-1	88572-HL-2	172.111.64.5	192.113.59.6	-	-	4800	4800	-	-	-	+	ses128	YES
2	HCN-5100-HL-2	88572-HL-1	172.111.65.5	172.111.59.5	-	-	4800	4800	-	-	-	+	ses128	YES
0	88572-HL-1	HCN-5100-HL-1	172.111.59.5	172.111.64.5	-	-	4800	4800	-	-	-	+	ses128	YES
3	88572-HL-2	HCN-5100-HL-2	192.113.59.6	172.111.65.5	-	-	4800	4800	-	-	-	+	ses128	YES
1	88572-HL-1	HCN-5100-HL-2	172.111.59.5	172.111.65.5	-	-	4800	4800	-	-	-	+	ses128	YES
2	88572-HL-2	HCN-5100-HL-1	192.113.59.6	172.111.64.5	-	-	4800	4800	-	-	-	+	ses128	YES

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
HCN-5100-HL-1	88572-HL-1	YES	YES	YES	0	n/a	n/a
HCN-5100-HL-2	88572-HL-2	YES	YES	YES	0	n/a	n/a
HCN-5100-HL-1	88572-HL-2	YES	YES	YES	0	n/a	n/a
HCN-5100-HL-2	88572-HL-1	YES	YES	YES	0	n/a	n/a
88572-HL-1	HCN-5100-HL-1	YES	YES	YES	0	n/a	n/a
88572-HL-2	HCN-5100-HL-2	YES	YES	YES	0	n/a	n/a
88572-HL-1	HCN-5100-HL-2	YES	YES	YES	0	n/a	n/a
88572-HL-2	HCN-5100-HL-1	YES	YES	YES	0	n/a	n/a

CLASSES:

Classes on virtual path "HCN-5100-88572":

#	Traffic Type	Rate (kbps)	Initial Period (ms)	Initial Rate (kbps)	Sustain Rate (kbps)
0	REALTIME	0	0	6000	
1	INTERACTIVE	0	0	2000	
2	INTERACTIVE	0	0	800	
3	INTERACTIVE	0	0	200	
4	BULK	0	0	800	1
5	BULK	0	0	1	1
6	BULK	0	0	1	1
7	BULK	0	0	1	1
8	BULK	0	0	1	1
9	BULK	0	0	1	1
10	REALTIME	0	0	6000	
11	INTERACTIVE	0	0	4000	
12	INTERACTIVE	0	0	3000	
13	INTERACTIVE	0	0	1400	
14	INTERACTIVE	0	0	600	
15	BULK	0	0	6000	
16	BULK	0	0	1	1

3. Sélectionnez **Tunnels IPsec** dans le menu déroulant pour afficher la configuration du tunnel IPsec.

Configuration

View: IPsec Tunnels

IPsec Tunnel Configuration

Name: VPN-ASA-1

ipsec_service_type=intranet

ike_local_ip_addr=10.0.0.6

ike_remote_ip_addr=10.101.0.100

network_mtu=1500

ike_version=2

ike_auth=psk

ike_identity=auto

ike_peer_auth=cert

ike_validate_peer_identity=1

ike_hash_algorithm=sha256

ike_integ_algorithm=sha256

ike_encryption_mode=aes256

ike_dhgroup=group2

ike_lifetime_s=300

ike_lifetime_s_max=86400

ike_dpd_s=300

ipsec_tunnel_mode=tunnel

ipsec_tunnel_type=esp_auth

ipsec_encryption_mode=aes128

ipsec_hash_algorithm=sha

ipsec_pfsgroup=none

ipsec_lifetime_s=28800

ipsec_lifetime_s_max=86400

ipsec_lifetime_kb=0

ipsec_lifetime_kb_max=0

ipsec_mismatch_behavior=drop

Protected Networks:

[1] 10.0.0.0/16 -> 10.101.0.0/16

[2] 10.4.0.0/16 -> 10.101.0.0/16

[3] 10.3.0.0/16 -> 10.101.0.0/16

[4] 10.2.0.0/16 -> 10.101.0.0/16

[5] 10.1.0.0/16 -> 10.101.0.0/16

4. Chaque chemin virtuel affichera son propre état de tunnel IPsec comme indiqué ci-dessous.

DashboardMonitoringConfiguration

System Status

Name:MCN-5100

Model:5100

Appliance Mode:MCN

Serial Number:4H30GCNPD0

Management IP Address:10.199.107.201

Appliance Uptime:1 weeks, 3 days, 2 hours, 7 minutes, 28.6 seconds

Service Uptime:6 hours, 21 minutes, 54.0 seconds

Routing Domain Enabled:Default_RoutingDomain

Local Versions

Software Version:10.0.0.193.659091

Built On:Feb 17 2018 at 17:32:45

Hardware Version:5100

OS Partition Version:4.6

Virtual Path Service Status

Virtual Path MCN-5100-BR572:

Uptime: 5 hours, 59 minutes, 34.0 secondsIPsec state: GOOD.

Virtual Path MCN-5100-BR573:

Uptime: 5 hours, 45 minutes, 0.0 seconds.IPsec state: GOOD.

Virtual Path MCN-5100-BR574:

Uptime: 4 hours, 56 minutes, 48.0 seconds.

Virtual Path 'MCN-5100-BR575' is currently dead.

Virtual Path MCN-5100-RCN1-5100:

Uptime: 2 hours, 7 minutes, 3.0 seconds.

Virtual Path 'MCN-5100-RCN3-2100' is currently dead (Configuration version mismatch)

Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.

Virtual Path 'MCN-5100-RCN4-ESxil' is currently dead.

Surveillance et journalisation IPsec

May 6, 2021

Pour surveiller les statistiques de tunnel ipsec :

1. Accédez à **Moniteur > Statistiques**. Choisissez **Tunnel IPsec** dans le menu déroulant **Afficher** comme indiqué ci-dessous :

Statistics

Show: IPsec Tunnel Enable Auto Refresh 5 seconds Show latest data.

IPsec Tunnel Statistics

Filter: In Any column Apply

Show 100 entries Showing 1 to 8 of 8 entries

Name	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropped	MTU
AS-TB-NCN-AS-TB-CL-1	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-2	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-3	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-4	GOOD	Conduit	0	0	0	0	0	0	1359
VPN-ASA-1	GOOD	Intranet	0	0	0	0	0	0	1427
VPN-ASA-2	GOOD	LAN	0	0	0	0	0	0	1377
VPN-PaloAlto	GOOD	Intranet	0	0	0	0	0	0	1439
VPN-SonicWall	GOOD	Intranet	0	0	0	0	0	0	1456

Showing 1 to 8 of 8 entries

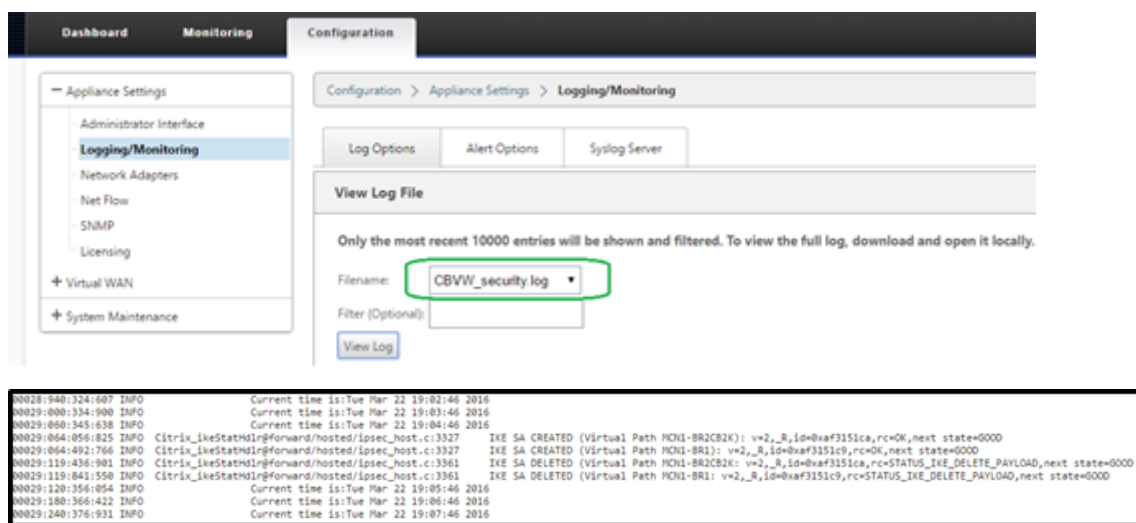
2. Accédez à **Moniteur > IKE/IPsec** . Observez les tunnels IPsec configurés, les associations de services IKE et IPsec entre deux points de terminaison VPN en mode ou configurés dans le réseau

SD-WAN.

Comment surveiller les journaux ipec

1. Accédez à **Configuration > Paramètres de l'appliance > Logging/Monitoring** . Sélectionnez **Nom de fichier** dans le menu déroulant et cliquez sur **Afficher le journal** . Vous pouvez afficher les détails du journal suivants pour le tunnel IPsec :

- Création et suppression du tunnel IPsec
- Modification de l'état du tunnel IPsec



Comment afficher les alertes de tunnel ipsec

1. Accédez à **Configuration > Paramètres de l'appliance > Logging/Monitoring > Options d'alerte** .
2. Créez des alertes Email et Syslog pour les rapports d'état de tunnel IPsec.
 - Prend en charge IPSEC_TUNNEL comme l'un des types d'événements qui vous permet de configurer les filtres de gravité Email et Syslog.

← Appliance Settings

Administrator Interface

Logging/Monitoring

Network Adapters

Net Flow

App Flow

SNMP

NETRO API

Licensing

+ Virtual WAN

+ System Maintenance

Configuration > Appliance Settings > Logging/Monitoring

Log OptionsAlert OptionsAlarm OptionsSyslog Server

Email Alerts

☐ Enable Email Alerts

Send Test Email

Destination Email Address(es):

SMTP Server Hostname or IP Address:

SMTP Server Port:

Source Email Address:

You may enter multiple destination email addresses separated with semicolons (;)

☐ Enable SMTP Authentication

SMTP User Name:

SMTP Password:

Verify SMTP Password:

General Event Configuration

Event Type	Alert if State Persists	Email	Email Severity Filter	Syslog	Syslog Severity Filter	SNMP	SNMP Severity Filter
SERVICE	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
VIRTUAL PATH	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
WAN LINK	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
PATH	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
DYNAMIC VIRTUAL PATH	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
WAN_LINK_CONGESTION	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
USAGE_CONGESTION	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
HARD_DISK		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
APPLIANCE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
USER EVENT		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
CONFIG_UPDATE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
SOFTWARE_UPDATE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
PROXY_ARP		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
ETHERNET		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
WATCHDOG		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
APPLIANCE_SETTINGS_UPDATE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
DISCOVERED_MTU		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
GRE_TUNNEL		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
IPSEC_TUNNEL		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
VIRTUAL_INTERFACE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
LICENSE_EVENT		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼

Apply Settings

Comment surveiller les événements de tunnel ipsec

1. Accédez à **Configuration > Maintenance du système > Diagnostics > Événements** .
2. Ajoutez des événements en fonction du type d'objet **IPSEC_TUNNEL** . Créez des filtres pour tous les événements liés à IPSec.

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

System Maintenance

System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Insert Event

Object Type:USER EVENT

Event type:UNDEFINED

Severity:DEBUG

Add Event

Download Events

There are currently 487678 in the Events database, spanning from event 183612 at 2018-01-18 18:24:55 to event 671289 at 2018-03-17 18:14:15. You can download some or all of them in CSV format. You may wish to limit the amount to download because some common spreadsheet programs limit you to 65,536 rows.

Download events starting from2018January18182456Download487678 events

Alert Count

Alert Type	Alerts Sent
Emails:	0
syslog Messages:	0
SNMP Traps:	0

View Events

Quantity:25

Filter: Object Type = AnyEvent type = AnySeverity = Any

Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
671289	0	MCN-5100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671288	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671287	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671286	2	MCN-5100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:14	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671285	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671284	0	MCN-5100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671283	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671282	2	MCN-5100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671281	3	MCN-5100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671280	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671279	1	MCN-5100-WL-1->BR574-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-2 state has changed from BAD to GOOD because notified by peer.
671278	2	MCN-5100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671277	2	MCN-5100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671276	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671275	3	MCN-5100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.
671274	1	MCN-5100-WL-1->BR574-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671273	3	MCN-5100-WL-2->BR574-WL-2	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from BAD to GOOD because notified by peer.
671272	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671271	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:06:08	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671270	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671269	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671268	3	MCN-5100-WL-2->BR574-WL-2	PATH	2018-02-17 18:05:57	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671267	1	MCN-5100-WL-1->BR573-WL-2	PATH	2018-02-17 18:05:09	GOOD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671266	3	MCN-5100-WL-2->BR572-WL-2	PATH	2018-02-17 18:05:09	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671265	1	MCN-5100-WL-1->BR573-WL-2	PATH	2018-02-17 18:04:58	BAD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.

Éligibilité pour les routes de chemin non virtuel ipsec

May 6, 2021

Dans les versions précédentes, les routes de tunnel ipsec restaient dans la table de routage, même si le tunnel devenait indisponible.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

800

Monitoring > Statistics

Statistics

Show: Routes ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11389	YES	N/A	N/A
3	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES	*	BRANCH2	Static	-	-	5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.186.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

L’utilisation de l’option Keepalive sous **Connexions** > [Nom de site] > **Tunnels IPsec** améliore ce comportement de sorte que les routes de chemin non virtuel IPsec sont désormais considérées comme inéligibles lorsque le tunnel IPsec n’est plus disponible. Lorsque l’option keepalive est activée, les SA sont créées automatiquement sans qu’aucun trafic ne soit envoyé par le tunnel.

Basic Global Sites **Connections** Optimization Provisioning

View Region: Default_Region

View Site: BR573 + Site Site Site

Connections ?

WAN-to-WAN Forwarding

Virtual Paths

Dynamic Virtual Paths

Internet Service

Intranet Services

WAN Links

GRE Tunnels

IPsec Tunnels

Firewall

Application Routes

Routes

OSPF

BGP

Route Learning Properties

Multicast Groups

Application Settings

Audits: 0 Audit Now

+ Service Type Name Firewall Zone Local IP Peer IP MTU Keepalive Delete

Intranet * <Default> * * 1500 ☒

IKE Settings ?

IPsec Settings ?

IPsec Protected Networks + Add ?

Apply Revert

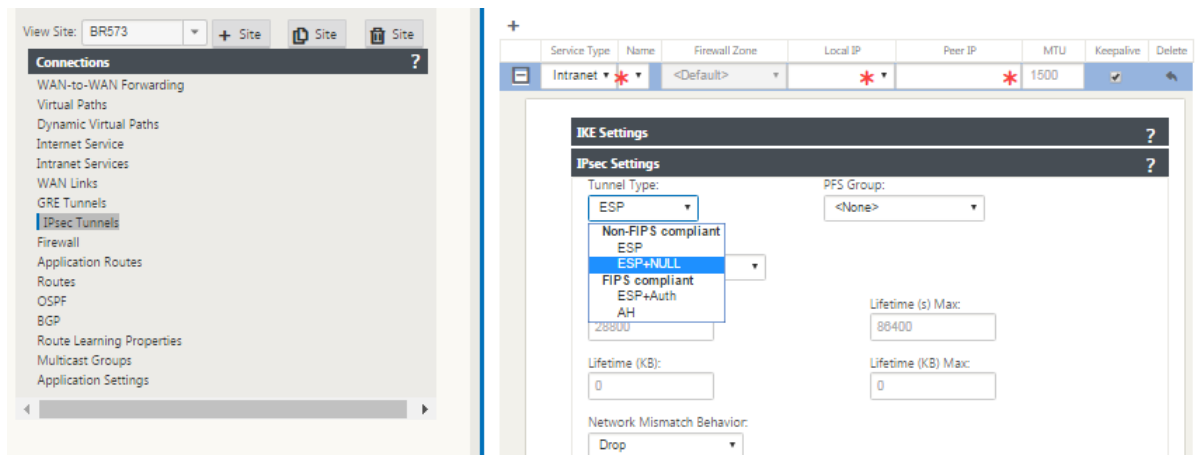
Chiffrement nul IPsec

May 6, 2021

Dans les versions précédentes, le type de tunnel ESP+NULL a été introduit. Lors de l’utilisation du protocole IPsec ESP, le trafic est généralement chiffré et authentifié. Toutefois, vous pouvez choisir

de ne pas utiliser le chiffrement en utilisant le chiffrement Null. Dans le type de tunnel ESP + NULL, les paquets sont authentifiés mais non chiffrés.

Vous pouvez configurer le tunnel IPsec avec le type de tunnel ESP+NULL dans l'éditeur de configuration, sous la section **Paramètres IPsec**.



Conformité aux normes FIPS

May 6, 2021

Dans Citrix SD-WAN, le mode FIPS oblige les utilisateurs à configurer les paramètres conformes FIPS pour leurs tunnels IPsec et les paramètres IPsec pour les chemins virtuels.

- Affiche le mode IKE compatible FIPS.
- Affiche un groupe IKE DH conforme FIPS dans lequel les utilisateurs peuvent sélectionner les paramètres requis pour configurer l'apppliance en mode conforme FIPS (2,5,14 —21).
- Affiche le type de tunnel IPsec compatible FIPS dans les paramètres IPsec pour les chemins virtuels
- Mode d'intégrité IKE et (IKEv2), mode d'authentification IPsec.
- Effectue des erreurs d'audit pour les paramètres de vie basés sur FIPS

Pour activer la conformité FIPS à l'aide de l'interface graphique Citrix SD-WAN :

1. Accédez à **Configuration > Réseau étendu virtuel > Éditeur de configuration > Global**, puis sélectionnez **Activer le mode FIPS**.

L'activation du mode FIPS impose des vérifications pendant la configuration afin de s'assurer que tous les paramètres de configuration liés à IPsec respectent les normes FIPS. Les erreurs d'audit et les avertissements vous invitent à configurer IPsec.

Pour configurer les paramètres IPsec du chemin virtuel :

- Activez Virtual Path Tunnels IPsec pour tous les chemins virtuels où la conformité FIPS est requise. Les paramètres IPsec pour les chemins virtuels sont contrôlés via les ensembles par défaut.
- Configurez l'authentification des messages en changeant le mode IPsec en AH ou ESP+Auth et utilisez une fonction de hachage approuvée par FIPS. SHA1 est accepté par FIPS, mais SHA256 est fortement recommandé.
- La durée de vie IPsec ne doit pas être configurée plus de 8 heures (28 800 secondes).

Le réseau WAN virtuel utilise IKE version 2 avec des clés pré-partagées pour négocier des tunnels IPsec via le chemin virtuel en utilisant les paramètres suivants :

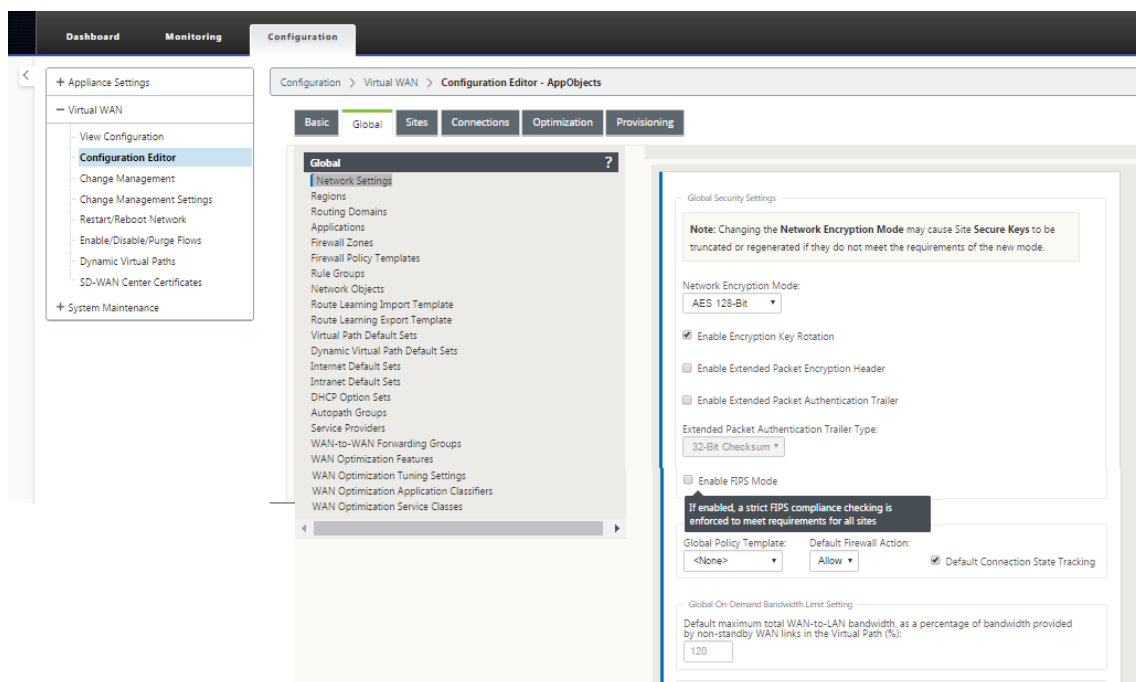
- DH Groupe 19 : ECP256 (courbe elliptique 256 bits) pour la négociation des clés
- Cryptage AES-CBC 256 bits
- Hachage SHA256 pour l'authentification des messages
- Hachage SHA256 pour l'intégrité des messages
- DH Groupe 2 : MODP-1024 pour un secret parfait avant

Pour configurer IPsec Tunnel pour un tiers, utilisez les paramètres suivants :

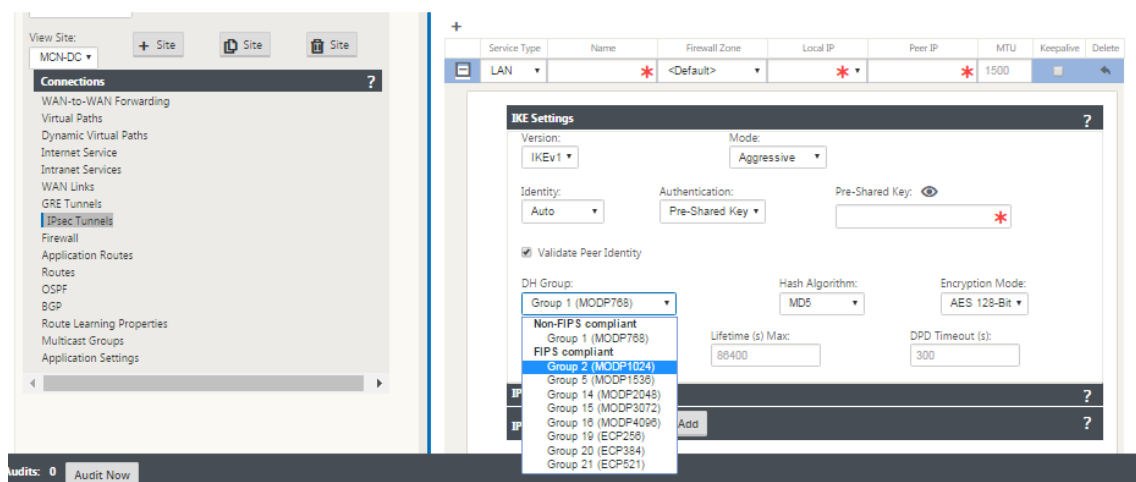
1. Configurer le groupe DH approuvé par FIPS. Les groupes 2 et 5 sont autorisés dans le cadre de la FIPS, mais les groupes 14 et plus sont fortement recommandés.
2. Configurer la fonction de hachage approuvée par FIPS. SHA1 est accepté par FIPS, mais SHA256 est fortement recommandé.
3. Si vous utilisez IKEv2, configurez une fonction d'intégrité approuvée par FIPS. SHA1 est accepté par FIPS, mais SHA256 est fortement recommandé.
4. Configurez une durée de vie IKE et une durée de vie maximale ne dépassant pas 24 heures (86 400 secondes).
5. Configurez l'authentification des messages IPsec en changeant le mode IPsec en AH ou ESP+Auth et utilisez une fonction de hachage approuvée par FIPS. SHA1 est accepté par FIPS, mais SHA256 est fortement recommandé.
6. Configurez une durée de vie IPsec et une durée de vie maximale ne dépassant pas huit heures (28 800 secondes).

Pour configurer les tunnels IPsec :

1. Sur l'appliance MCN, accédez à **Configuration > Virtual WAN > Éditeur de configuration**. Ouvrez un package de configuration existant. Accédez à **Connexions > Tunnels IPsec**.



2. Accédez à **Connexions > Tunnels IPSec**. Avec **LAN** ou **Intranet Tunnel** sélectionné, l'écran distingue les groupes conformes FIPS dans les paramètres IKE de ceux qui ne sont pas conformes, de sorte que vous pouvez facilement configurer la conformité FIPS.



L'écran indique également si l'algorithme de hachage est conforme à la norme FIPS, comme illustré dans la figure suivante.

	Service Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
	LAN	*	<Default>	*	*	1500		

IKE Settings?

Version:

IKEv1

Mode:

Aggressive

Identity:

Auto

Authentication:

Pre-Shared Key

Pre-Shared Key:

☒ Validate Peer Identity

DH Group:

Group 1 (MODP768)

Hash Algorithm:

MD5

Encryption Mode:

AES 128-Bit

Lifetime (s):

3600

Lifetime (s) Max:

86400

DPD Timeout (s):

300

Non-FIPS compliant

MD5

FIPS compliant

SHA1

SHA-256

IPsec Settings?

IPsec Protected Networks

+ Add

?

Options de conformité FIPS pour les paramètres IPsec :

	Service Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
	LAN	*	<Default>	*	*	1500		

IKE Settings?

IPsec Settings?

Tunnel Type:

ESP

PFS Group:

<None>

Non-FIPS compliant

ESP

ESP+NULL

FIPS compliant

ESP+Auth

AH

Lifetime (s) Max:

86400

Lifetime (KB):

0

Lifetime (KB) Max:

0

Network Mismatch Behavior:

Drop

IPsec Protected Networks

+ Add

?

Si la configuration IPsec n'est pas conforme aux normes FIPS lorsqu'elle est activée, une erreur d'audit peut être déclenchée. Voici le type d'erreurs d'audit qui s'affichent dans l'interface graphique.

- Lorsque, le mode FIPS est activé et l'option non conforme FIPS est sélectionnée.
- Lorsque, le mode FIPS est activé et une valeur de vie incorrecte est entrée.

- Lorsque, le mode FIPS est activé et les paramètres IPsec pour le chemin virtuel par défaut sont également activés, et le mode Tunnel incorrect est sélectionné (ESP vs ESP_Auth/AH).
- Lorsque le mode FIPS est activé, les paramètres IPsec pour le chemin virtuel par défaut sont également activés et une valeur de durée de vie incorrecte est entrée.

Passerelle Web sécurisée Citrix SD-WAN

May 6, 2021

Pour sécuriser le trafic et appliquer des stratégies, les entreprises utilisent souvent des liens MPLS pour rediriger le trafic des succursales vers le datacenter de l'entreprise. Le centre de données applique des stratégies de sécurité, filtre le trafic via les appliances de sécurité pour détecter les logiciels malveillants et achemine le trafic via un fournisseur de services Internet. Un tel réacheminement sur des liaisons MPLS privées est coûteux. Cela entraîne également une latence importante, ce qui crée une mauvaise expérience utilisateur sur le site de la succursale. Il existe également un risque que les utilisateurs contournent vos contrôles de sécurité.

Une alternative au réacheminement consiste à ajouter des dispositifs de sécurité à la succursale. Toutefois, le coût et la complexité augmentent à mesure que vous installez plusieurs appliances pour maintenir des stratégies cohérentes sur l'ensemble des sites. Et si vous avez de nombreuses succursales, la gestion des coûts devient peu pratique.

Zscaler :

La solution idéale pour appliquer la sécurité sans augmenter les coûts, la complexité ou la latence consiste à acheminer tout le trafic Internet des succursales de l'appliance Citrix SD-WAN vers la plateforme de sécurité Zscaler Cloud. Vous pouvez ensuite utiliser une console Zscaler centrale pour créer des stratégies de sécurité granulaires pour vos utilisateurs. Les stratégies sont appliquées de manière cohérente, que l'utilisateur se trouve dans le centre de données ou dans un site de succursale. Étant donné que la solution de sécurité Zscaler est basée sur le cloud, vous n'avez pas à ajouter d'autres appliances de sécurité au réseau.

Conformité FIPS :

Le National Institute for Standards and Technology (NIST) élabore des normes fédérales de traitement de l'information (FIPS) dans des domaines pour lesquels il n'existe aucune norme volontaire. FIPS aborde les problèmes suivants :

- Compatibilité entre différents systèmes.
- Portabilité des données et des logiciels.
- Sécurité informatique rentable et confidentialité des informations sensibles.

FIPS spécifie les exigences de sécurité pour un module cryptographique utilisé dans les systèmes de sécurité. Pour appliquer ces normes de sécurité au traitement effectué par une appliance Citrix SD-WAN, configurez le mode FIPS.

Point de force :

À l'aide de Citrix SD-WAN, vous pouvez utiliser la fonctionnalité de redirection du pare-feu (proxy transparent par NAT de destination) pour rediriger le trafic Internet (HTTP et HTTPS) d'une appliance SD-WAN à la périphérie de l'entreprise vers le module de sécurité hébergé dans le cloud Forcepoint. Vous pouvez rediriger le trafic HTTP du port 80 au port 8081 et le trafic HTTPS du port 443 au port 8443 du serveur proxy de cloud Forcepoint le plus proche.

Intégration de Zscaler à l'aide des tunnels GRE et IPsec

November 1, 2021

Zscaler Cloud Security Platform agit comme une série de postes de contrôle de sécurité dans plus de 100 centres de données à travers le monde. En redirigeant simplement votre trafic Internet vers Zscaler, vous pouvez immédiatement sécuriser vos magasins, succursales et sites distants. Zscaler connecte les utilisateurs et Internet, inspectant chaque octet de trafic, même s'il est crypté ou compressé.

Les appliances Citrix SD-WAN peuvent se connecter à un réseau cloud Zscaler via des tunnels GRE sur le site du client. Un déploiement Zscaler utilisant des appliances SD-WAN prend en charge les fonctionnalités suivantes :

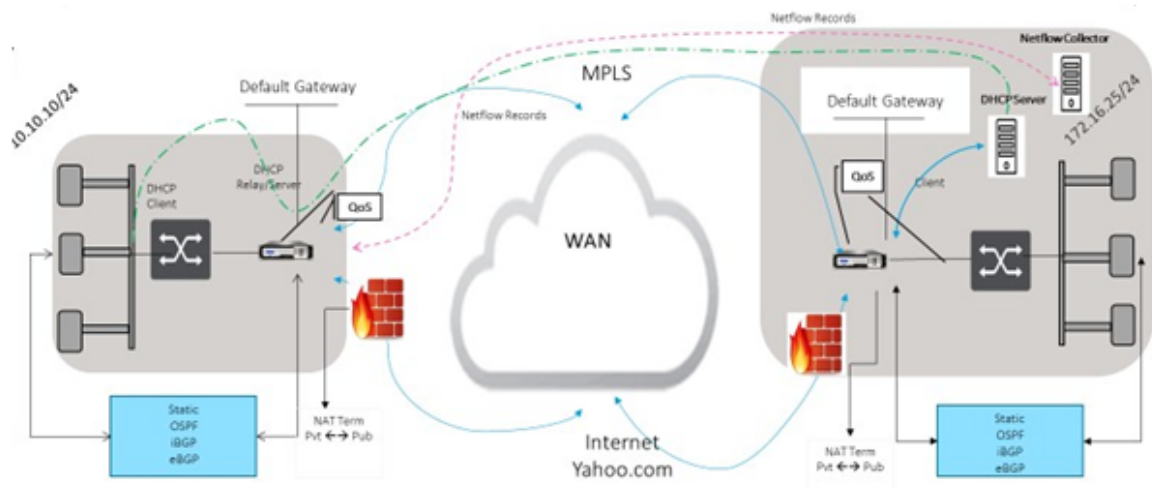
- Transférer tout le trafic GRE à Zscaler, ce qui permet une ventilation directe de l'Internet.
- Accès direct à Internet (DIA) utilisant Zscaler sur une base par site client.
 - Sur certains sites, vous pouvez fournir à DIA un équipement de sécurité local et ne pas utiliser Zscaler.
 - Sur certains sites, vous pouvez choisir de rediriger le trafic vers un autre site client pour accéder à Internet.
- Déploiements de routage et de transfert virtuels.
- Une liaison WAN dans le cadre des services Internet.

Zscaler est un service cloud. Vous devez le configurer en tant que service et définir les liens WAN sous-jacents :

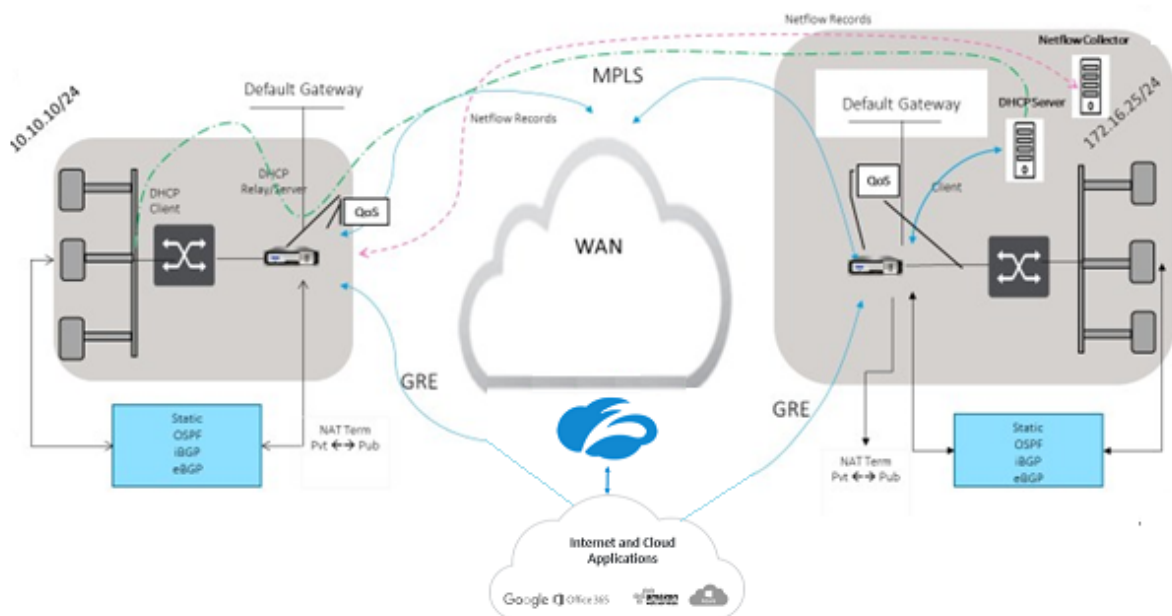
- Configurez un service Internet dans le centre de données et la succursale via GRE.
- Configurez un lien Internet public approuvé au niveau du centre de données et des sites de succursale.

Topologie

CURRENT DEPLOYMENT MODEL WITH ON-PREMISE FIREWALL



ZSCALER SECURITY AS SERVICE DEPLOYMENT MODEL



Pour utiliser le transfert de trafic de tunnel GRE ou de tunnel IPsec :

1. Connectez-vous au portail d'aide Zscaler à l'adresse suivante : <https://help.zscaler.com/submit-ticket>.
2. Levez un ticket et fournissez l'adresse IP publique statique, qui est utilisée comme l'adresse IP source du tunnel GRE ou du tunnel IPsec.

Zscaler utilise l'adresse IP source pour identifier l'adresse IP du client. L'adresse IP source doit être une adresse IP publique statique. Zscaler répond avec deux adresses IP ZEN (primaire et secondaire) pour transmettre le trafic. Les messages de maintien en vie GRE peuvent être utilisés pour déterminer la santé des tunnels.

Zscaler utilise la valeur de l'adresse IP source pour identifier l'adresse IP du client. Cette valeur doit être une adresse IP publique statique. Zscaler répond avec deux adresses IP ZEN [DR1] vers lesquelles rediriger le trafic. Les messages de type « keep-alive » du GRE peuvent être utilisés pour déterminer la santé des tunnels.

Exemples d'adresses IP

Primary

Adresse IP du routeur interne : 172.17.6.241/30 Adresse IP
interne ZEN : 172.17.6.242/30

Secondary

Adresse IP du routeur interne : 172.17.6.245/30 Adresse IP
interne ZEN : 172.17.6.246/30

Configuration d'un service Internet

Pour configurer un service Internet :

1. Accédez à **Connexions- Services Internet**. Configurer le service Internet.
2. Sélectionnez **+ Service** et activez les paramètres (paramètres de base, liens WAN et règles) si nécessaire.
3. Sélectionnez **Appliquer**.

Pour plus d'informations sur l'activation du service Internet pour un site, consultez la section [Direct Internet Breakout at Branch with Integrated Firewall](#).

Vous pouvez configurer les paramètres suivants sur un service Internet :

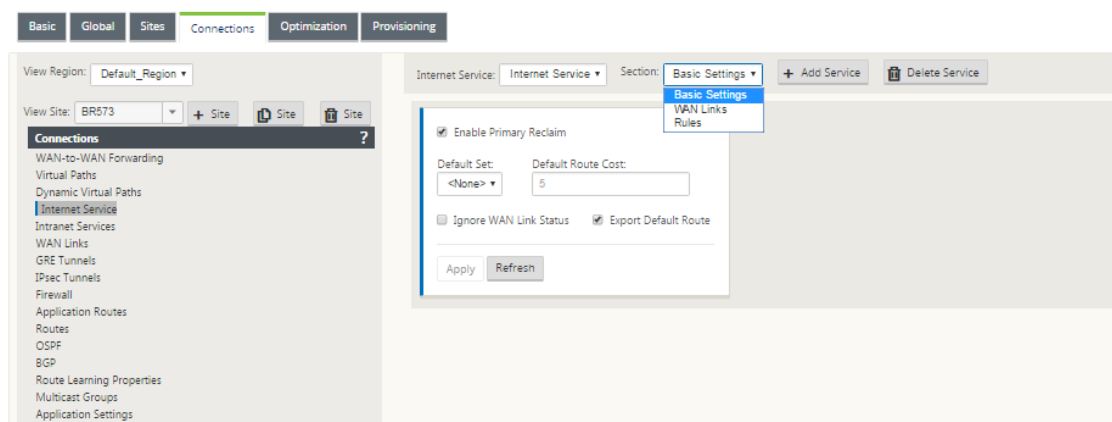
- [Paramètres de base](#)
- [Liens WAN](#)
- [Règle](#)

Paramètres de base

Un paramètre de zone de pare-feu n'est pas configurable pour un service Internet. Si le service Internet est approuvé, il est affecté à **Internet_Zone**. Si le service Internet n'est pas approuvé, il est affecté à **Untrusted_Internet_Zone**.

Les paramètres de base configurables sont décrits ci-dessous :

- **Activer la récupération principale** : si cette option est activée, l'utilisation (utilisation = principale) associée à ce service sur une liaison WAN réclame avec force le statut de service actif sur cette liaison WAN.
- **Jeu par défaut** : nom du jeu par défaut Internet qui remplit les règles du service Internet sur le site.
- **Coût de l'itinéraire par défaut** : coût de route associé à la route Internet par défaut (0.0.0.0/0).
- **Ignorer l'état de la liaison WAN** : si cette option est activée, les paquets destinés à ce service choisissent toujours ce service même si toutes les liaisons WAN de ce service ne sont pas disponibles.
- **Exporter l'itinéraire par défaut** : si cette option est activée, la route par défaut du service Internet, 0.0.0.0/0, est exportée vers d'autres sites si le transfert WAN vers WAN est activé.



Liens WAN

Les paramètres de liaison WAN configurables sont décrits ci-dessous :

- **Utilisation** : autorise le service à utiliser cette liaison WAN. Lorsque l'option Utiliser est désactivée, toutes les autres options ne sont pas disponibles.
- **Mode** : mode de service (principal, secondaire ou équilibrage) pour la redondance du trafic ou l'équilibrage de charge.
- **Taille de l'en-tête du tunnel (octets)** : taille de l'en-tête du tunnel, en octets, le cas échéant.

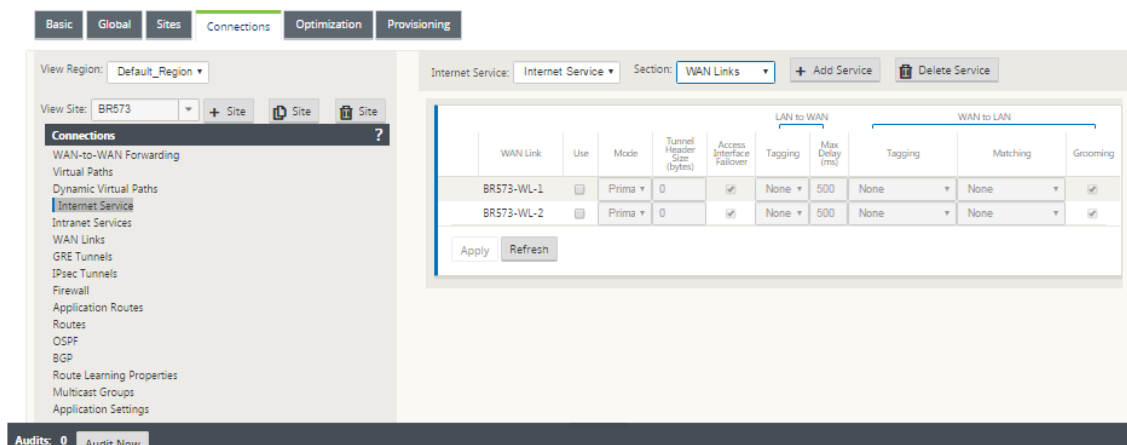
- **Basculement de l'interface d'accès** : si cette option est activée, les paquets Internet ou Intranet dont les VLAN ne correspondent pas peuvent toujours utiliser le service.

LAN vers WAN

- **Balisage** : balise DSCP à appliquer aux paquets LAN vers WAN sur le service.
- **Délai maximal (ms)** : durée maximale, en millisecondes, de mise en mémoire tampon des paquets lorsque la bande passante des liaisons WAN est dépassée.

WAN vers LAN

- **Balisage** : balise DSCP à appliquer aux paquets WAN vers LAN sur le service.
- **Correspondance** : les paquets Internet WAN vers LAN correspondant à cette balise sont attribués au service.
- **Grooming** : si cette option est activée, les paquets sont supprimés de manière aléatoire pour empêcher le trafic WAN vers LAN de dépasser la bande passante allouée du service.



Règle

Le trafic Internet est identifié en fonction des règles définies. Une définition de règle est utilisée pour faire correspondre un flux de trafic spécifique. Une fois la correspondance effectuée, vous devez définir l'action à appliquer pour le flux de trafic.

La liste des règles disponibles est décrite ci-dessous :

- **Ordre** : séquence dans laquelle les règles sont appliquées et redistribuées automatiquement.
- **Nom du groupe de règles** : nom donné à une règle qui permet d'ajouter les statistiques de règle en groupes lorsqu'elles sont affichées. Toutes les statistiques relatives aux règles portant le même nom de groupe de règles peuvent être consultées ensemble.

- **Source** : adresse IP source et masque de sous-réseau correspondant à la règle.
- **Dest-Src** : si cette option est activée, l'adresse IP source est également utilisée comme adresse IP de destination.
- **Dest** : adresse IP de destination et masque de sous-réseau qui correspondent à la règle.
- **Protocole** : nom du protocole qui correspond au filtre.
- **Numéro de protocole** : numéro de protocole correspondant au filtre.
- **DSCP** : balise DSCP dans l'en-tête IP qui correspond à la règle.

La liste des actions disponibles est décrite ci-dessous :

- **Lien WAN** : lien WAN à utiliser par les flux correspondant à la règle lorsque l'équilibrage de charge Internet est activé.
- **Override Service** : service de destination des flux correspondant à la règle.
 - **Discard** : abandonnez le trafic.
 - **Passthrough** : Mappez le flux vers le relais et autorisez le trafic à passer par l'apppliance sans modification.

The screenshot shows the 'Internet Service' configuration page in the Citrix SD-WAN interface. The 'Section' is set to 'Rules'. A table lists the configured rules. The first rule, with Order 100 and Rule Group Name '<None>', is selected. Below the table, the configuration details for this rule are shown:

IP Address				Port				DSCP	VLAN	Rebind Flow on Change	Delete	Clone
Order	Rule Group Name	Source	Dest-Src	Dest	Protocol	Protocol #	Source					
100	<None>	*		*	Any	0	*		*	Any		

Below the table, the configuration details for the selected rule are shown:

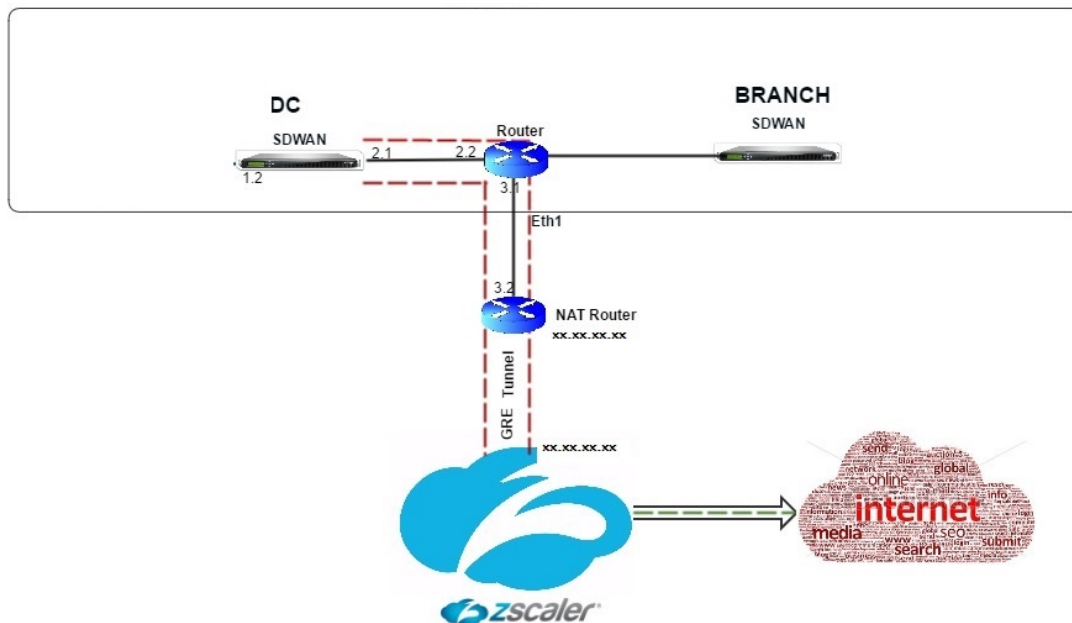
Mode: WAN Link
 WAN Link: <N/A>
 Override Service: <N/A>
☐ Enable Passive FTP Detection

Buttons: Apply, Revert

Configurer le tunnel GRE

1. L'adresse IP source est l'adresse IP de la source du tunnel. Si l'adresse IP de la source du tunnel est NATted, l'adresse IP de la source publique est l'adresse IP de la source de tunnel publique, même si elle est NATted sur un autre périphérique intermédiaire.
2. L'adresse IP de destination est l'adresse IP ZEN fournie par Zscaler.
3. L'adresse IP source et l'adresse IP de destination sont les en-têtes GRE du routeur lorsque la charge utile d'origine est encapsulée.

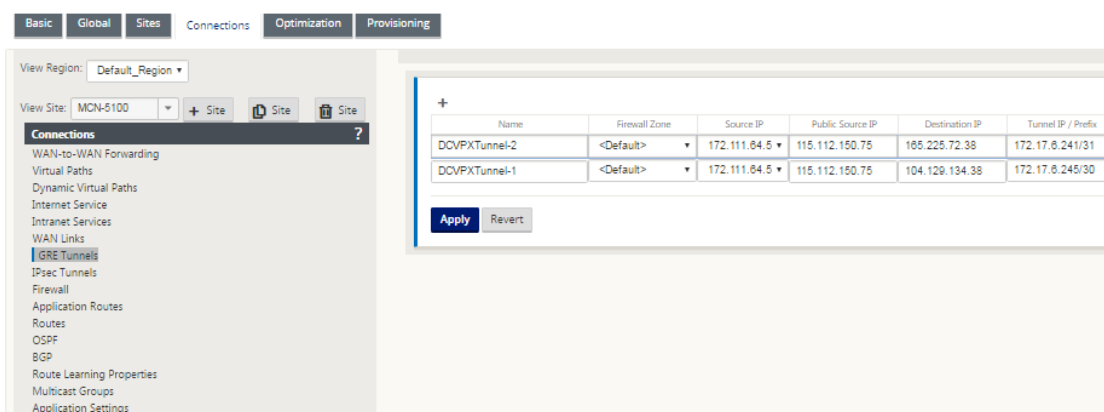
4. L'adresse IP du tunnel et le préfixe sont l'adresse IP du tunnel GRE lui-même. Ceci est utile pour acheminer le trafic sur le tunnel GRE. Le trafic a besoin de cette adresse IP comme adresse de passerelle.



Pour configurer GRE Tunnel :

1. Dans l'éditeur de configuration, accédez à **Connexions > Site > Tunnels GRE** et configurez des routes pour transférer les services de préfixe Internet vers les tunnels GRE Zscaler.

L'adresse IP source ne peut être choisie que dans l'interface réseau virtuel sur les liens approuvés. Reportez-vous à la section [Comment configurer le tunnel GRE](#).



Configurer les itinéraires pour les tunnels GRE

Configurez des itinéraires pour transférer les services de préfixe Internet vers les tunnels GRE Zscaler.

- L'adresse IP ZEN (IP de destination Tunnel, illustrée par 104.129.194.38 dans la figure ci-dessus) doit être définie sur Internet de type service. Ceci est nécessaire pour que le trafic destiné à Zscaler soit comptabilisé à partir du service Internet.
- Tout le trafic destiné à Zscaler doit correspondre à la route par défaut 0/0 et être transmis via le tunnel GRE. Assurez-vous que l'itinéraire 0/0 utilisé pour [DR1] le tunnel GRE a un coût inférieur à celui du relais ou de tout autre type de service.
- De même, le tunnel GRE de sauvegarde vers Zscaler doit avoir un coût plus élevé que celui du tunnel GRE primaire.
- Assurez-vous qu'il existe des itinéraires non récursifs pour l'adresse IP ZEN.

Pour configurer des itinéraires pour GRE Tunnel :

1. Accédez à **Connexions > Site > Itinéraires**, puis suivez les procédures décrites dans [Configuration des itinéraires](#) pour obtenir des instructions sur la création d'itinéraires.

BasicGlobalSitesConnectionsOptimizationProvisioning

View Region: Default_Region

View Site: MCN-5100 + Site Site

Connections ?

WAN-to-WAN ForwardingVirtual PathsDynamic Virtual PathsInternet ServiceIntranet ServicesWAN LinksGRE TunnelsIPsec TunnelsFirewallApplication RoutesRoutesOSPFBGPRoute Learning PropertiesMulticast GroupsApplication Settings

+Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	104.129.194.38/32	5	Internet			ⓘ	✎	✖
2	165.225.72.38/32	5	Internet			ⓘ	✎	✖
3	172.17.6.241/30	5	GRE Tunnel		165.225.72.38	ⓘ		
4	172.17.6.245/30	5	GRE Tunnel		104.129.194.38	ⓘ		
5	172.16.1.2/24	5	Local			ⓘ		
6	172.16.4.0/24	5	Local		172.16.1.1	ⓘ	✎	✖
7	0.0.0.0/0	3	GRE Tunnel		172.17.6.242	ⓘ	✎	✖
8	0.0.0.0/0	4	GRE Tunnel		172.17.6.246	ⓘ	✎	✖
9	0.0.0.0/0	5	Internet			ⓘ		
10	0.0.0.0/0	16	Passthrough			ⓘ		

⏪ < 1 > ⏩

ApplyRefresh

Audits: 0Audit Now

Remarque

Si vous n'avez pas de routes spécifiques pour l'adresse IP Zscaler, configurez le préfixe de route 0.0.0.0/0 pour qu'il corresponde à l'adresse IP ZEN et routez-le via une boucle d'encapsulation de tunnel GRE. Cette configuration utilise les tunnels en mode de sauvegarde active. Avec les valeurs indiquées dans la figure ci-dessus, le trafic passe automatique-

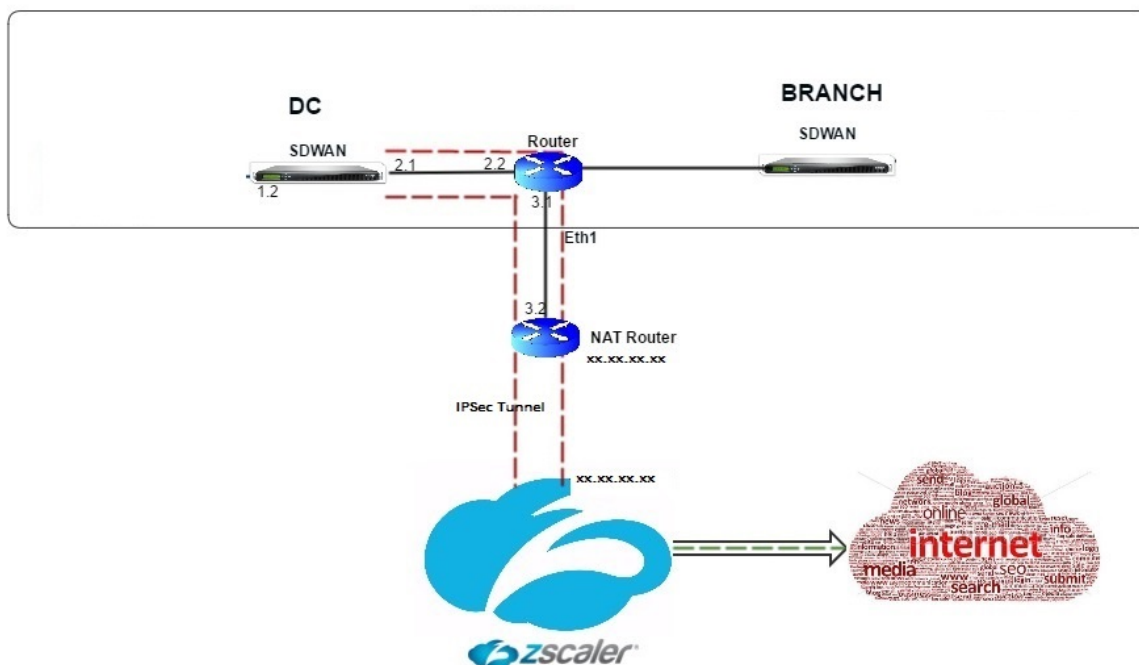
ment au tunnel avec l'adresse IP de la Gateway 172.17.6.242. Si vous le souhaitez, configurez une route de chemin virtuel de backhaul. Sinon, définissez l'intervalle keep-alive du tunnel de sauvegarde sur zéro. Cela permet un accès Internet sécurisé à un site même si les deux tunnels vers Zscaler échouent.

Les messages GRE keep-alive sont pris en charge. Un nouveau champ appelé **IP source publique** qui fournit l'adresse NAT de l'adresse source GRE est ajouté à l'interface graphique Citrix SD-WAN (dans le cas où la source du tunnel de l'appliance SD-WAN est NATted par un périphérique intermédiaire). L'interface graphique Citrix SD-WAN inclut un champ appelé IP source publique, qui fournit l'adresse NAT de l'adresse source GRE lorsque la source du tunnel de l'appliance Citrix SD-WAN est traduite par un périphérique intermédiaire.

Limitations

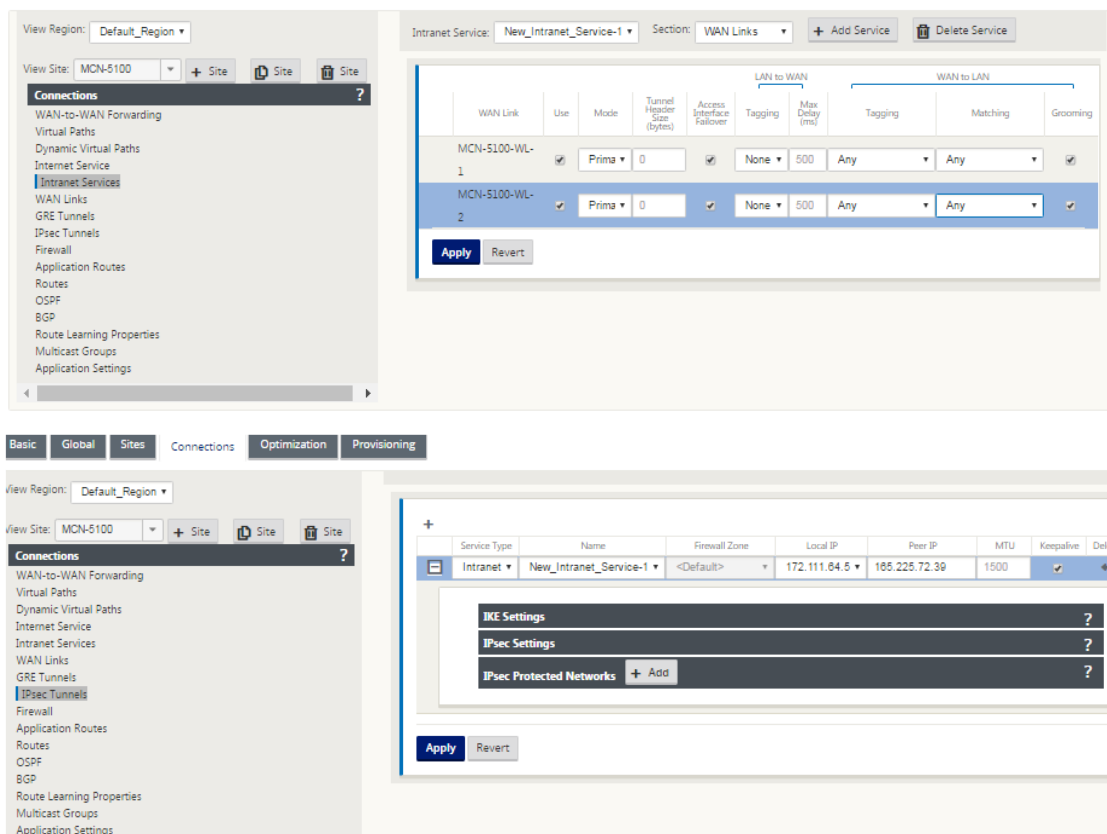
- Plusieurs déploiements VRF ne sont pas pris en charge.
- Les tunnels GRE de sauvegarde primaire sont pris en charge uniquement pour un mode de conception haute disponibilité.

Configurer les tunnels IPSec

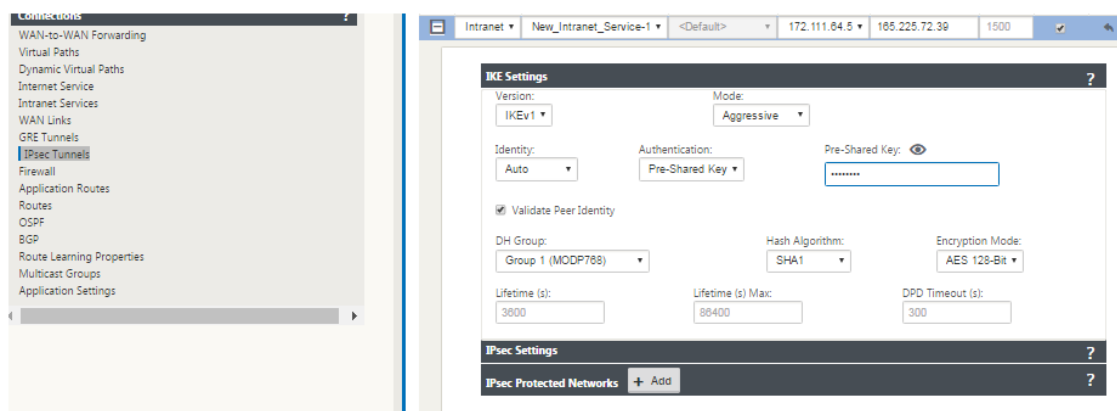


Pour configurer les tunnels IPSec pour les services intranet ou LAN dans l'interface graphique de l'appliance Citrix SD-WAN :

1. Dans l'éditeur de configuration, accédez à **Connexions** > **<SiteName>** > **Tunnels IPsec** et choisissez un type de service (LAN ou Intranet).
2. Entrez un nom pour le type de service. Pour le type de service Intranet, le serveur intranet configuré détermine les adresses IP locales disponibles.
3. Sélectionnez l'adresse IP locale disponible et entrez l'adresse IP homologue pour le chemin virtuel vers l'homologue distant.



4. Sélectionnez **IKEv1** pour les **paramètres IKE**. Zscaler ne prend en charge que IKEv1.



5. Sous Paramètres IPsec, sélectionnez **ESP-NUL** pour le **type de tunnel**, pour rediriger le trafic

vers Zscaler via le tunnel IPsec. Le tunnel IPsec ne chiffre pas le trafic.

IKE Settings?

IPsec Settings?

Tunnel Type:ESP+NULL

PFS Group:<None>

Hash Algorithm:SHA1

Lifetime (s):28800

Lifetime (s) Max:86400

Lifetime (KB):0

Lifetime (KB) Max:0

Network Mismatch Behavior:Drop

IPsec Protected Networks

+ Add

?

6. Étant donné que le trafic Internet est redirigé, l'IP/préfixe de destination peut être n'importe quelle adresse IP.

IKE Settings?

Version:IKEv1

Mode:Aggressive

Identity:Auto

Authentication:Pre-Shared Key

Pre-Shared Key:*****

☒ Validate Peer Identity

DH Group:Group 1 (MODP768)

Hash Algorithm:SHA1

Encryption Mode:AES 128-Bit

Lifetime (s):3600

Lifetime (s) Max:86400

DPD Timeout (s):300

IPsec Settings?

IPsec Protected Networks

+ Add

?

Source IP/Prefix	Destination IP/Prefix	Delete
172.16.4.0/24	0.0.0.0/0	

Apply

Revert

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

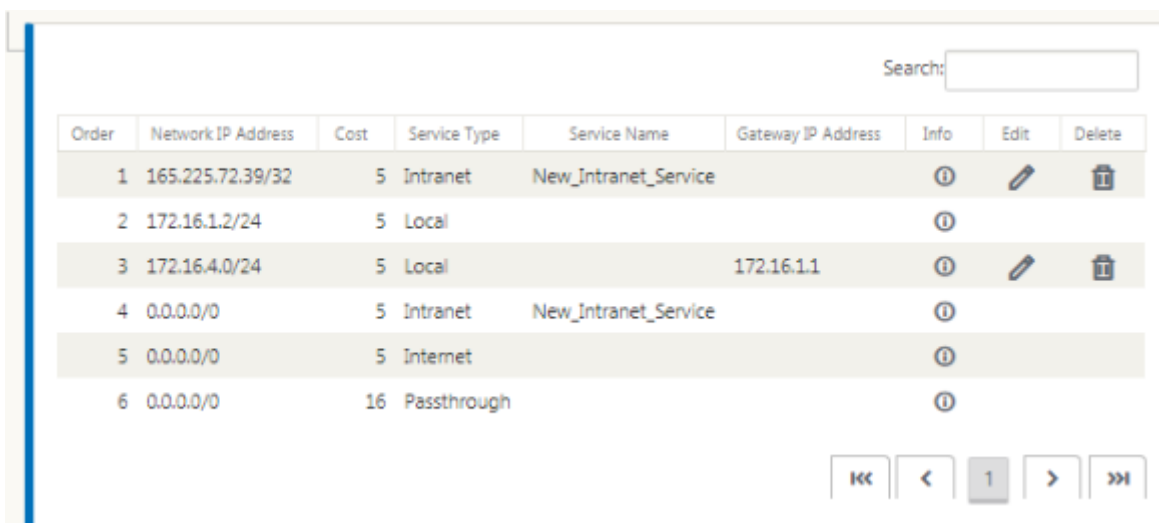
817

Pour plus d'informations sur la configuration des tunnels IPsec à l'aide de l'interface Web Citrix SD-WAN, reportez-vous à la rubrique [Tunnels IPsec](#).

Configurer les itinéraires pour les tunnels IPsec

Pour configurer des itinéraires IPsec :

1. Accédez à **Connexions > DC > Routes** et suivez les procédures décrites dans [Configuration des itinéraires](#) pour obtenir des instructions sur la création d'itinéraires.



Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	165.225.72.39/32	5	Intranet	New_Intranet_Service		ⓘ	✎	🗑️
2	172.16.1.2/24	5	Local			ⓘ		
3	172.16.4.0/24	5	Local		172.16.1.1	ⓘ	✎	🗑️
4	0.0.0.0/0	5	Intranet	New_Intranet_Service		ⓘ		
5	0.0.0.0/0	5	Internet			ⓘ		
6	0.0.0.0/0	16	Passthrough			ⓘ		

Pour surveiller les statistiques des tunnels GRE et IPsec :

Dans l'interface Web SD-WAN, accédez à **Tunnel IPsec**.
Surveillance > Statistiques > [Tunnel GRE]

Pour plus d'informations, consultez la rubrique [Surveillance des tunnels IPsec](#) et des [tunnels GRE](#).

Prise en charge de la redirection du trafic de pare-feu à l'aide de Forcepoint dans Citrix SD-WAN

May 6, 2021

Forcepoint prend en charge les fonctionnalités suivantes, bien que SD-WAN ne prenne en charge que la fonction de redirection du pare-feu :

- IPsec avec PKI

- IPsec avec PSK
- Chaîne proxy à l'aide de la configuration du fichier PAC
- Enchaînement proxy avec des en-têtes standard
- Enchaînement proxy avec des en-têtes propriétaires éliminant la nécessité de configurer la plage IP du client - partenariat/développement
- Redirection du pare-feu (proxy transparent par NAT de destination)

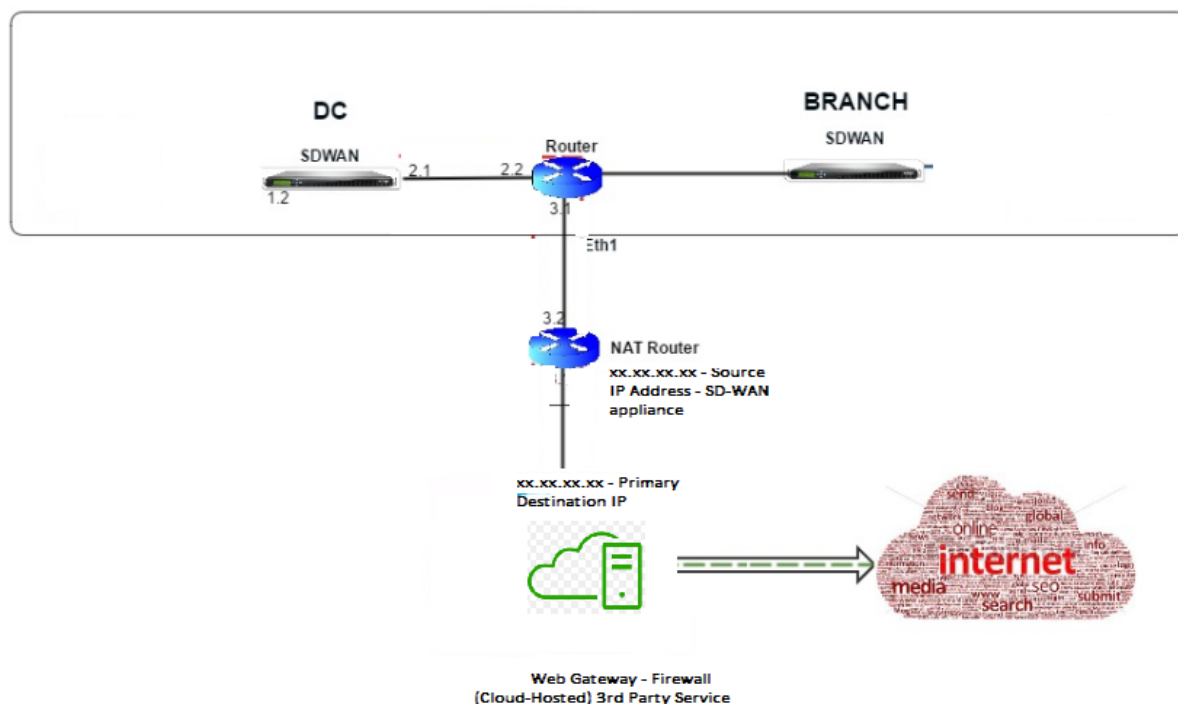
La stratégie NAT de destination permet aux entreprises d'acheminer le trafic Internet via un service de sécurité hébergé dans le cloud à l'aide de ForcePoint.

Consultez le cas d'utilisation suivant pour comprendre comment configurer le NAT de destination dans les appliances SD-WAN et rediriger le trafic Internet via un service de pare-feu sécurisé basé sur le cloud.

Conditions préalables :

1. Connectez-vous à [laSite portail Forcepoint](#). Créez une stratégie en fournissant l'adresse IP publique d'entreprise via laquelle le trafic Internet doit être redirigé vers Forcepoint. Obtenez les adresses IP principales et secondaires vers lesquelles le trafic Internet doit être redirigé.
2. Dans l'interface graphique SD-WAN, sur une appliance SD-WAN sur le site DC, configurez le service Internet associé aux liaisons WAN.
3. Le NAT de destination est effectué à l'aide de l'adresse IP de destination du trafic Internet. Cette adresse de destination est remplacée par l'adresse IP publique Forcepoint.
4. Configurez la stratégie NAT de destination en fournissant l'adresse IP source et l'adresse IP principale. L'adresse IP source est l'adresse IP Internet de l'appliance SD-WAN à l'intérieur des ports 80 (http) et 443 (https) qui est redirigée/traduite en l'adresse IP de destination principale de la Gateway de pare-feu basée sur un cloud avec les ports extérieurs 8081 (http) et 8443 (https) respectivement.
5. Après avoir configuré la stratégie DNAT, assurez-vous que le type de service Internet est sélectionné pour l'adresse IP du réseau SD-WAN sur les routes configurées sur le contrôleur de domaine.

Pour plus d'informations sur la prise en charge NAT dans Citrix SD-WAN, consultez la rubrique suivante : [Configurer NAT](#)



Configuration du NAT de destination (DNAT)

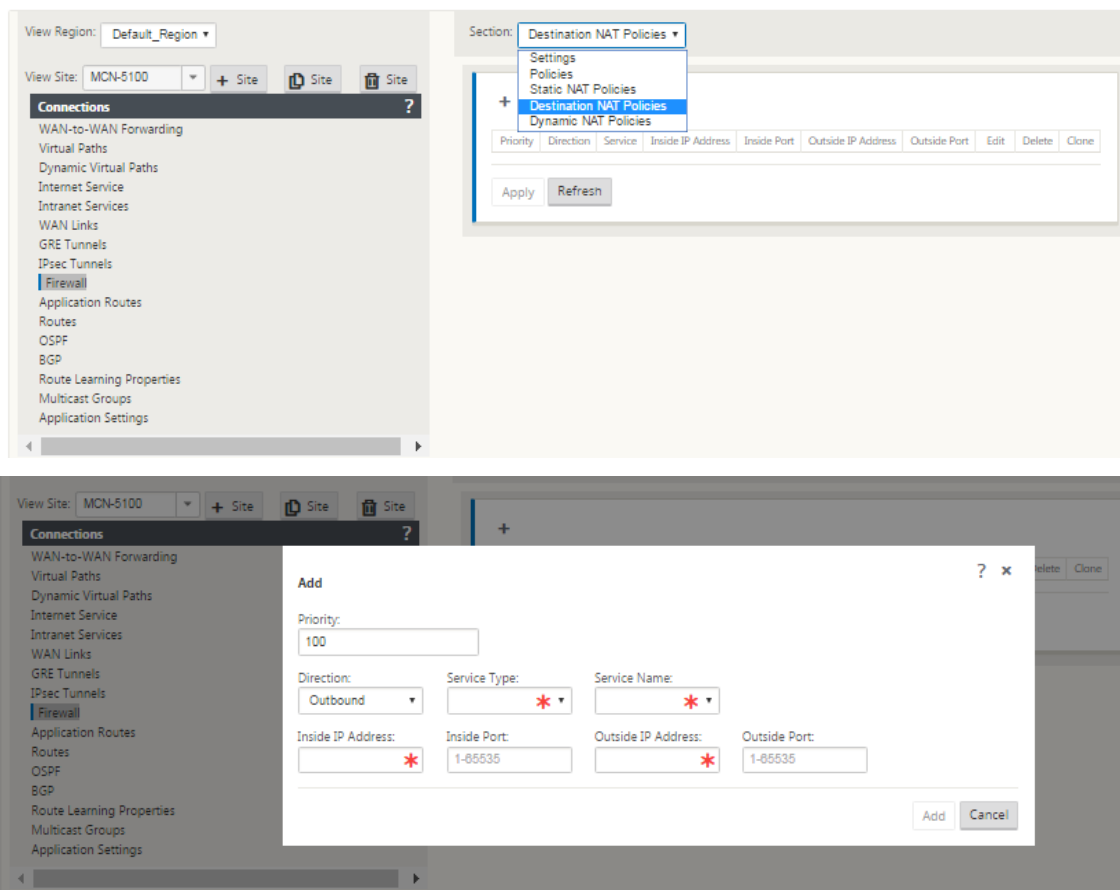
Utilisez l'interface graphique Citrix SD-WAN pour configurer Destination NAT (DNAT). Dans la configuration, ajoutez une ou plusieurs stratégies DNAT qui redirigent le trafic correspondant à une adresse IP et un port de destination spécifiques.

Pour configurer le NAT de destination :

Dans l'interface graphique SD-WAN SE/VPX, accédez à **Configuration** -> **Virtual WAN** -> Configuration Editor. Cliquez sur **Ouvrir** pour ouvrir un package existant. Sélectionnez un package de configuration enregistré. Vous pouvez également créer des règles DNAT lors de la création de la configuration réseau.

1. Sur le contrôleur de domaine (MCN), configurez le service Internet. Allez dans **Connexions** -> **Pare-feu**.
2. Cliquez sur **+ Ajouter** pour ajouter une stratégie DNAT.
3. Dans la boîte de dialogue **Ajouter une stratégie NAT de destination**, fournissez les informations suivantes :
 - Priority
 - Sens
 - Type de service
 - Nom du service

- Adresse IP intérieure
- Port intérieur
- Adresse IP extérieure
- Port extérieur



4. Provisionner les règles NAT de destination pour la redirection du trafic du pare-feu, similaire à NAT statique.
5. Entrez les critères de correspondance et l'IP/port de destination à traduire.
6. Effectuer la correspondance de connexion de la règle DNAT avec les statistiques.
7. Supprimer ou mettre à jour les règles DNAT lors de la mise à jour de la configuration.

Surveillance d'une stratégie NAT de destination (pare-feu)

Vous pouvez également utiliser l'interface graphique Citrix SD-WAN pour surveiller la configuration de stratégie DNAT actuelle.

Pour surveiller la configuration actuelle de la stratégie NAT de destination :

1. Dans l'interface graphique Citrix SD-WAN, accédez à **Surveillance** > **Pare-feu** > **Stratégies NAT**.
2. Sélectionnez l'onglet qui inclut les statistiques que vous souhaitez surveiller.

The first screenshot shows the 'Firewall Statistics' tab in the Citrix SD-WAN GUI. The 'Statistics' dropdown is set to 'NAT Policies'. The 'Maximum entries to display' is set to 50. The 'NAT' section shows filters for IP Protocol (Any), NAT Type (Any), and Dynamic NAT Type (Any). The 'Service Type' is set to Any, and the 'Service Name' is set to Any. The 'Inside IP' is set to *, and the 'Inside Port' is set to *. The 'Outside IP' is set to *, and the 'Outside Port' is set to *. The 'Refresh' button is visible. Below the statistics, the 'NAT Policies' table is shown.

ID	Rule Type	Rule	Direction	IP Protocol	Service Type	Service Name	IP Address	Port	IP Address	Port	Allow Related	Allow IPsec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
1	Dynamic PR	-	Outbound	*	Internet	-	*	*	172.16.2.101/32	0-65535	No	No	No	253825	26477410	452674	614179776	3	[Connections]

The second screenshot shows the 'Connections' tab in the Citrix SD-WAN GUI. The 'Statistics' dropdown is set to 'Connections'. The 'Maximum entries to display' is set to 50. The 'Filtering' section shows filters for IP Protocol (Any), Source Zone (Any), Destination Zone (Any), Source Service Type (Any), Destination Service Type (Any), Source Service Instance (Any), Destination Service Instance (Any), Source IP (Any), Destination IP (Any), Source Port (Any), and Destination Port (Any). The 'Refresh' button is visible. Below the statistics, the 'Connections' table is shown.

Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State
Domain Name Service(dns)	Network Service	UDP	172.16.6.10	36080	Virtual Path	DC-MCN-BR3-CS2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED
Domain Name Service(dns)	Network Service	UDP	172.16.16.1	56451	Virtual Path	DC-MCN-BR1-CS2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED

Intégration de Palo Alto à l'aide de tunnels IPsec

May 6, 2021

Les réseaux Palo Alto fournissent une infrastructure de sécurité basée sur le cloud pour protéger les réseaux distants. Il assure la sécurité en permettant aux organisations de configurer des pare-feu régionaux basés sur le cloud qui protègent la structure SD-WAN.

Le service Prisma Access pour les réseaux distants vous permet d'intégrer des emplacements réseau distants et d'assurer la sécurité des utilisateurs. Il élimine la complexité de la configuration et de la gestion des périphériques à chaque emplacement distant. Le service offre un moyen efficace d'ajouter facilement de nouveaux emplacements réseau distants et de minimiser les défis opérationnels en veillant à ce que les utilisateurs de ces sites soient toujours connectés et sécurisés. Il vous permet

de gérer les stratégies de manière centralisée à partir de Panorama pour une sécurité cohérente et rationalisée pour vos emplacements réseau.

Pour connecter vos emplacements réseau distants au service Prisma Access, vous pouvez utiliser le pare-feu de nouvelle génération de Palo Alto Networks ou un périphérique tiers compatible IPsec incluant

SD-WAN, qui peut établir un tunnel IPsec vers le service.

- Planifier le service d'accès Prisma pour les réseaux distants
- Configurer le service d'accès Prisma pour les réseaux distants
- Réseaux distants intégrés avec importation de configuration

La solution Citrix SD-WAN offrait déjà la possibilité de sortir le trafic Internet de la succursale. Ceci est essentiel pour offrir une expérience utilisateur plus fiable et à faible latence, tout en évitant l'introduction d'une pile de sécurité coûteuse à chaque succursale. Citrix SD-WAN et Palo Alto Networks offrent désormais aux entreprises distribuées un moyen plus fiable et plus sûr de connecter les utilisateurs des succursales aux applications dans le cloud.

Les appliances Citrix SD-WAN peuvent se connecter au réseau Palo Alto (Prisma Access Service) via des tunnels IPsec à partir d'emplacements d'appliances SD-WAN avec une configuration minimale. Vous pouvez configurer le réseau Palo Alto dans Citrix SD-WAN Center.

Avant de commencer à configurer le service d'accès Prisma pour les réseaux distants, assurez-vous que la configuration suivante est prête pour vous assurer que vous êtes en mesure d'activer le service et d'appliquer la stratégie pour les utilisateurs de vos emplacements réseau distants :

1. **Connexion de service** : si vos emplacements réseau distants nécessitent un accès à l'infrastructure de votre siège social pour authentifier les utilisateurs ou pour activer l'accès aux ressources réseau critiques, vous devez configurer Accès à votre réseau d'entreprise de sorte que le siège social et les emplacements réseau distants soient connectés.

Si l'emplacement réseau distant est autonome et n'a pas besoin d'accéder à l'infrastructure à d'autres emplacements, vous n'avez pas besoin de configurer la connexion de service (sauf si vos utilisateurs mobiles ont besoin d'un accès).

1. **Modèle** : le service Prisma Access crée automatiquement une pile de modèles (Remote_Network_Template_Stack) et un modèle de niveau supérieur (Remote_Network_Template) pour le service Prisma Access pour les réseaux distants. Pour configurer le service d'accès Prisma pour les réseaux distants, vous configurez le modèle de niveau supérieur à partir de zéro ou utilisez votre configuration existante, si vous exécutez déjà un pare-feu réseau Palo Alto sur site.

Le modèle nécessite les paramètres pour établir le tunnel IPsec et la configuration IKE (Internet Key Exchange) pour la négociation de protocole entre votre emplacement réseau distant et le

service Prisma Access pour les réseaux distants, les zones que vous pouvez référencer dans la stratégie de sécurité et un profil de transfert de journal afin que vous peut transférer les journaux du service Prisma Access pour les réseaux distants vers le service de journalisation.

2. **Groupe de périphériques parent** : le service Prisma Access pour les réseaux distants requiert que vous spécifiez un groupe de périphériques parent qui inclut votre stratégie de sécurité, vos profils de sécurité et d'autres objets de stratégie (tels que les groupes d'applications et les objets et les groupes d'adresses), ainsi que la stratégie d'authentification afin que le Le service Prisma Access pour les réseaux distants peut appliquer systématiquement une stratégie pour le trafic acheminé via le tunnel IPSec vers le service Prisma Access pour les réseaux distants. Vous devez définir des règles et des objets de stratégie sur Panorama ou utiliser un groupe de périphériques existant pour sécuriser les utilisateurs dans l'emplacement réseau distant.

Remarque :

Si vous utilisez un groupe de périphériques existant qui référence des zones, assurez-vous d'ajouter le modèle correspondant qui définit les zones à `Remote_Network_Template_Stack`.

Cela vous permet de terminer le mappage de zone lorsque vous configurez le service d'accès Prisma pour les réseaux distants.

3. **Sous-réseaux IP** : pour que le service Prisma Access achemine le trafic vers vos réseaux distants, vous devez fournir des informations de routage pour les sous-réseaux que vous souhaitez sécuriser à l'aide du service Prisma Access. Vous pouvez définir un itinéraire statique vers chaque sous-réseau à l'emplacement réseau distant, ou configurer BGP entre vos emplacements de connexion de service et le service Prisma Access, ou utiliser une combinaison des deux méthodes.

Si vous configurez à la fois des routes statiques et activez BGP, les routes statiques ont priorité. Bien qu'il puisse être pratique d'utiliser des routes statiques si vous n'avez que quelques sous-réseaux à vos emplacements distants, dans un déploiement volumineux avec de nombreux réseaux distants avec des sous-réseaux superposés, BGP vous permettra d'évoluer plus facilement.

Réseau Palo Alto à SD-WAN Center

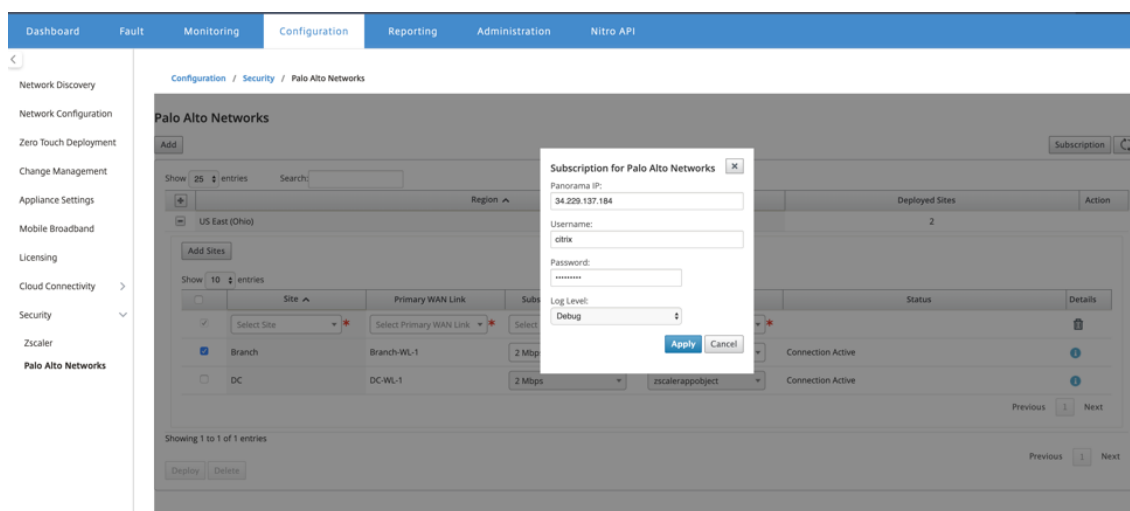
Assurez-vous que les conditions préalables suivantes sont remplies :

- Obtenir l'adresse IP panoramique du service PRISMA ACCESS.
- Obtenez le nom d'utilisateur et le mot de passe utilisateur dans le service PRISMA ACCESS.
- Configurez les tunnels IPSec dans l'interface graphique de l'appliance SD-WAN.

- Assurez-vous que le site n'est pas intégré à une région, qui a déjà un site différent configuré avec des profils ike/ipsec autres que Citrix-IKE-Crypto-Default/Citrix-IPsec-Crypto-Default/Crypto-Default.
- Assurez-vous que la configuration de Prisma Access n'est pas modifiée manuellement lorsque la configuration est mise à jour par SD-WAN Center.

Dans l'interface graphique du Centre Citrix SD-WAN, fournissez les informations d'abonnement à Palo Alto.

- Configurez l'adresse IP panoramique. Vous pouvez obtenir cette adresse IP auprès de Palo Alto (service PRISMA ACCESS).
- Configurez le nom d'utilisateur et le mot de passe utilisés dans le service PRISMA ACCESS.



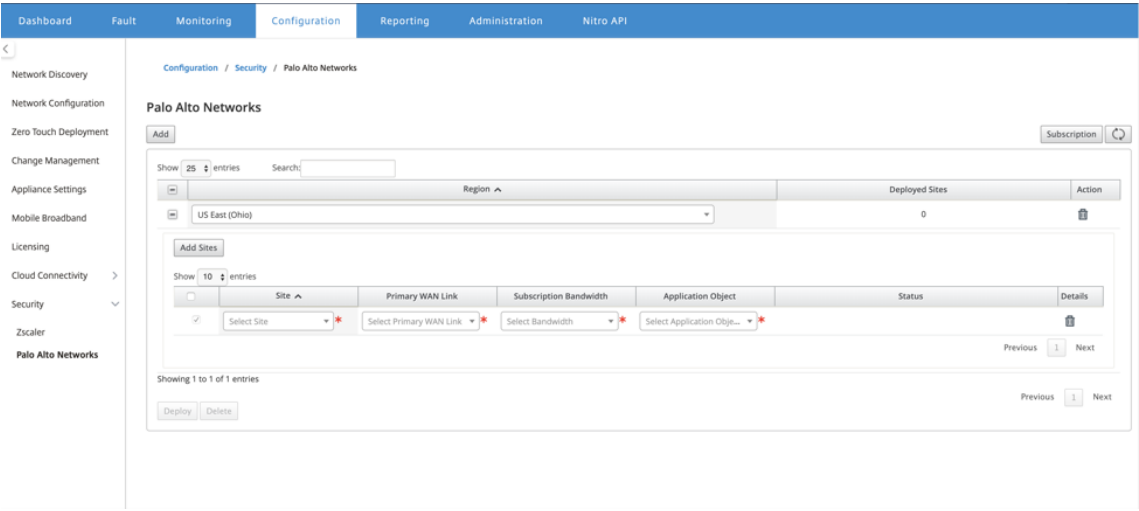
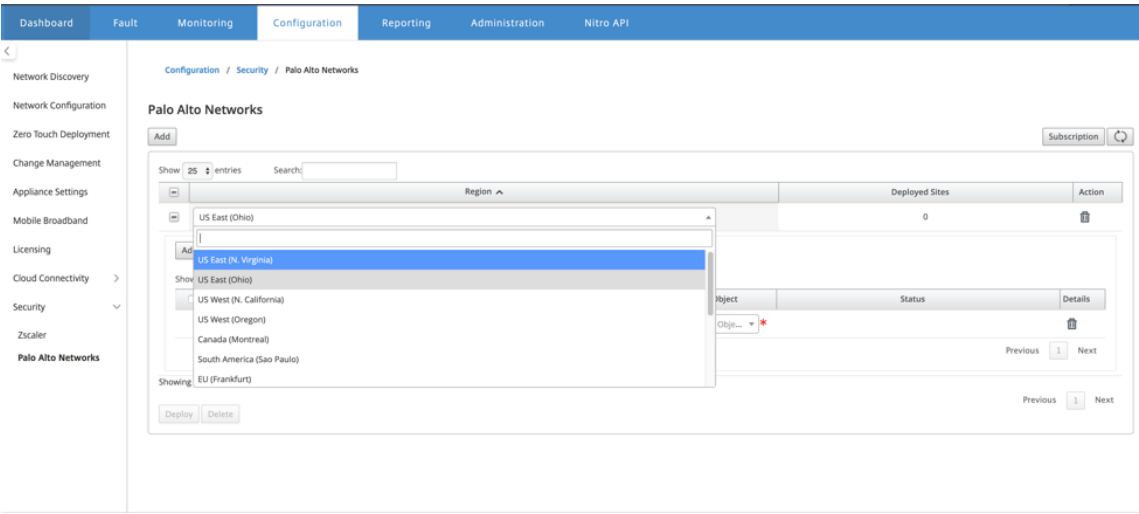
Ajouter et déployer des sites

1. Pour déployer les sites, choisissez la région réseau PRISMA ACCESS et le site SD-WAN à configurer pour la région Prisma Access, puis sélectionnez la liaison WAN du site, la bande passante et l'objet d'application pour la sélection du trafic.

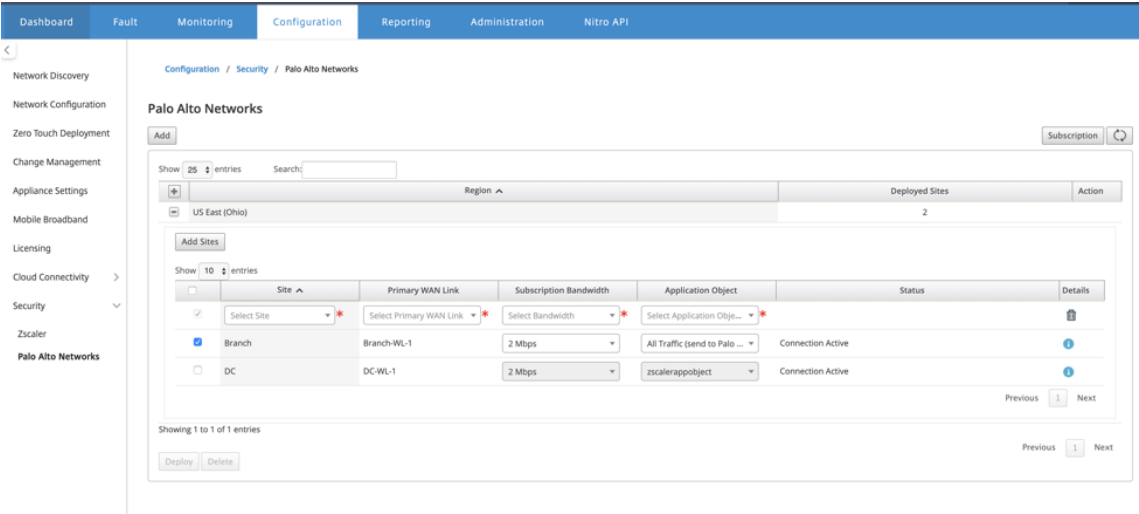
Remarque :

Le flux de trafic est affecté si la bande passante sélectionnée dépasse la plage de bande passante disponible.

Vous pouvez choisir de rediriger tout le trafic lié à Internet vers le service PRISMA ACCESS en sélectionnant l'option **Tout le trafic** sous la sélection d'objet Application.

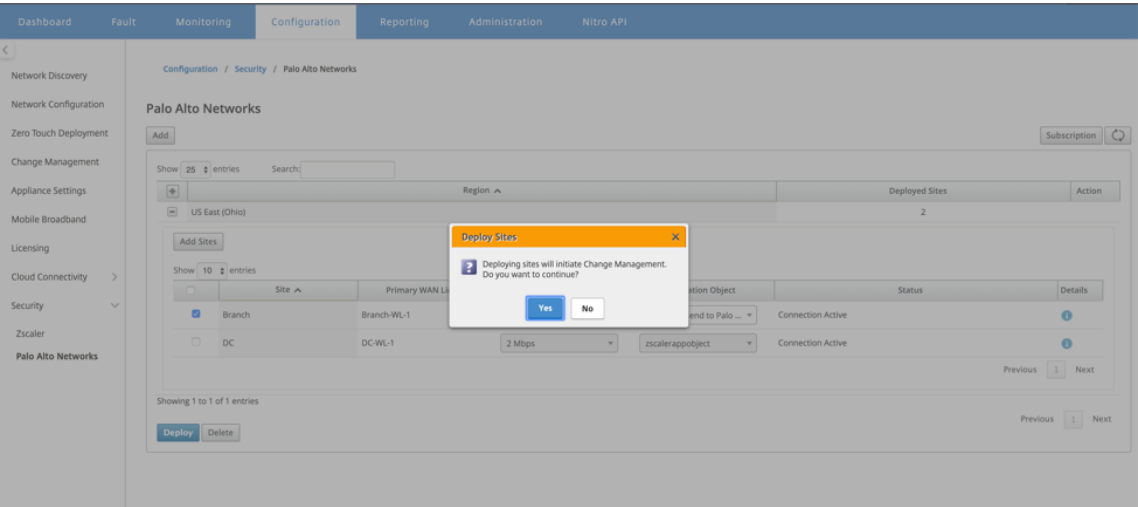


2. Vous pouvez continuer à ajouter d'autres sites de succursale SD-WAN selon vos besoins.



3. Cliquez sur **Déployer**. Le processus de gestion du changement est lancé. Cliquez sur **Oui** pour

continuer.



Après le déploiement, la configuration du tunnel IPsec utilisée pour établir les tunnels est la suivante.

Palo Alto Site Details

Application Object

Application Object Name: appobject

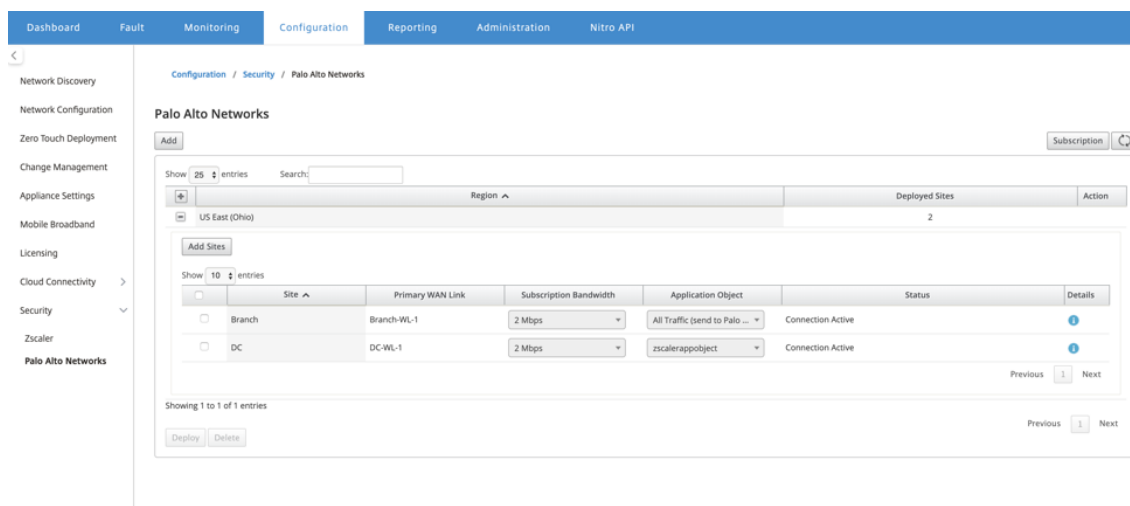
Match Criteria

Match Type	Application	Application Family	Protocol
application	Office 365 Default[office365_default]	-	-

IPsec Tunnels

panw_service_066318_1	
Local IP: 192.168.100.3	Peer IP: 13.52.159.66
MTU: -	Firewall Zone: -
IKE Version: ikev2	DH Group: group2
IKE Hash Algorithm: sha256	IKE Integrity: sha256
IKE Encryption: aes256	IKE Identity: auto
Identity Data: -	IPsec Tunnel Type: esp
PF5 Group: none	IPsec Mismatch Behaviour: drop

La page de destination affiche la liste de tous les sites configurés et regroupés sous différentes régions SD-WAN.



Vérifiez la connexion du trafic de bout en bout :

- À partir du sous-réseau LAN de la branche, accéder aux ressources Internet.
- Vérifiez que le trafic passe par le tunnel IPsec Citrix SD-WAN vers l'accès Palo Alto Prisma.
- Vérifiez que la stratégie de sécurité Palo Alto est appliquée sur le trafic sous l'onglet Surveillance.
- Vérifiez que la réponse d'Internet à l'hôte d'une succursale arrive.

Prise en charge du pare-feu avec état et NAT

May 6, 2021

Cette fonctionnalité fournit un pare-feu intégré à l'application SD-WAN. Le pare-feu autorise les stratégies entre les services et les zones et prend en charge le NAT statique, le NAT dynamique (PAT) et le NAT dynamique avec transfert de port. Plus de fonctionnalités de pare-feu sont les suivantes :

- Assurer la sécurité du trafic utilisateur au sein du réseau SD-WAN (fournisseurs d'entreprise et de services)
- (Potentiel) Réduction du matériel externe (entreprises et prestataires de services)
- Utilisation du même espace d'adressage IP pour plusieurs clients : Capacité NAT (fournisseurs de services)
- Appliquer plusieurs pare-feu dans une perspective globale (Fournisseurs de services)
- Filtrage des flux de trafic entre les zones
- Filtrage du trafic entre les services dans une zone
- Filtrage du trafic entre les services résidant dans différentes zones
- Filtrage du trafic entre les services d'un site

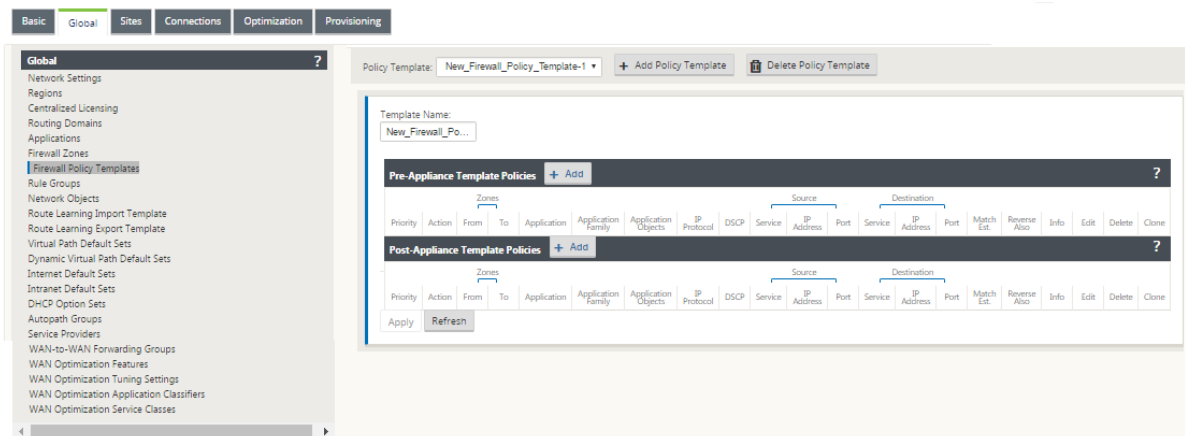
- Définition de stratégies de filtrage pour autoriser, refuser ou rejeter des flux
- Suivi de l'état du flux pour les flux sélectionnés
- Application de modèles de stratégie globale
- Prise en charge de la traduction d'adresses de port pour le trafic vers Internet sur un port non approuvé, ainsi que du transfert de port entrant et sortant
- Fournir la traduction statique d'adresses réseau (NAT statique)
- Fournir la traduction dynamique des adresses réseau (NAT dynamique)
- Traduction d'adresses de port (PAT)
- Transfert de port

Pour simplifier le processus de configuration, les stratégies de pare-feu sont créées au niveau de la configuration globale. Cette configuration globale comprend des modèles de stratégie de site pré-appliance et post-appliance qui peuvent être appliqués à tous les sites du réseau SD-WAN.

Remarque

Pour des raisons de sécurité, il n'est pas recommandé d'utiliser le pare-feu en mode Inline Fail-to-Wire.

Modèles de stratégie globale



Modèle pré-stratégie

Priority:

100

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action:

Allow

Log Interval (s):

0

☐ Log Start

☐ Log End

Connection State Tracking:

Use Site Setting

Match Type:

IP Protocol

Application Objects:

Any

Application:

Application Family:

IP Protocol:

Any

DSCP:

Any

☒ Allow Fragments

☐ Reverse Also

☐ Match Established

Source Service Type:

Any

Source Service Name:

Any

Source IP:

*

Source Port:

*

Dest Service Type:

Any

Dest Service Name:

Any

Dest IP:

*

Dest Port:

*

Add

Cancel

Modèle post-stratégie

Add

?

x

Priority:

100

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action:

Allow

Log Interval (s):

0

☐ Log Start

☐ Log End

Connection State Tracking:

Use Site Setting

Match Type:

IP Protocol

Application Objects:

Any

Application:

Application Family:

IP Protocol:

Any

DSCP:

Any

☒ Allow Fragments

☐ Reverse Also

☐ Match Established

Source Service Type:

Any

Source Service Name:

Any

Source IP:

*

Source Port:

*

Dest Service Type:

Any

Dest Service Name:

Any

Dest IP:

*

Dest Port:

*

Add

Cancel

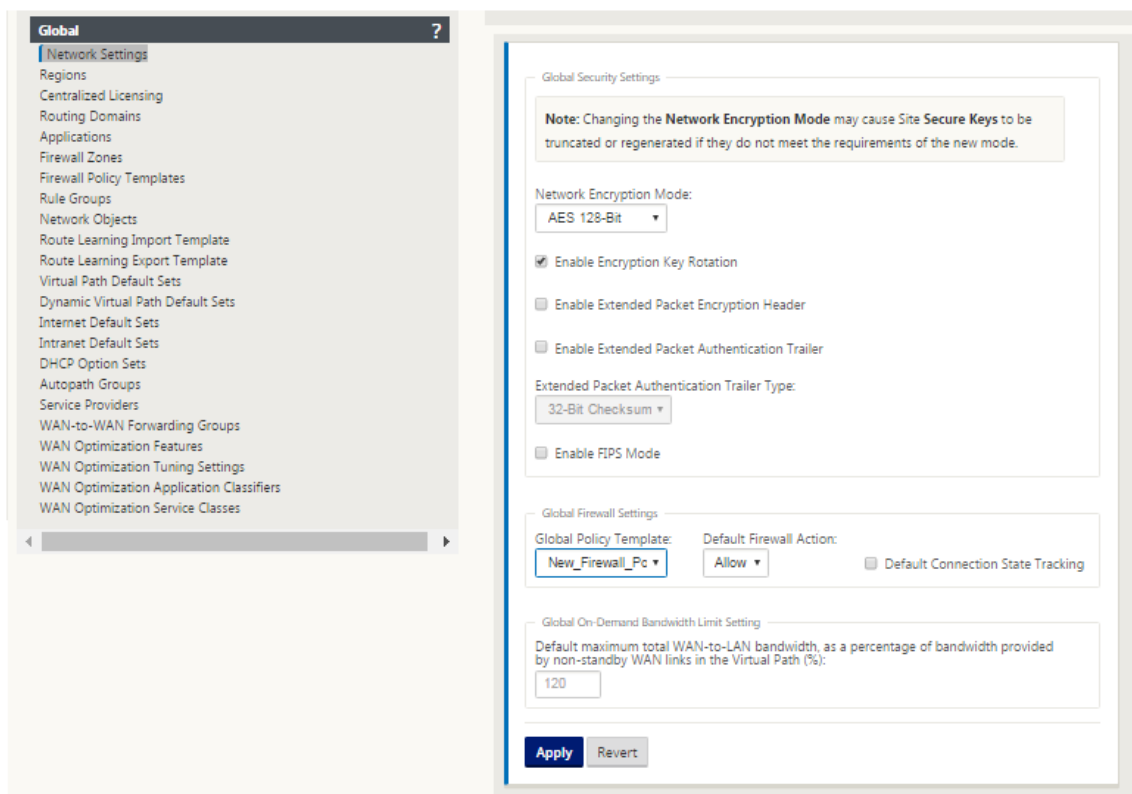
Paramètres globaux du pare-feu

May 6, 2021

Une fois que vous avez créé les modèles de stratégie de pare-feu, vous pouvez utiliser cette stratégie pour configurer les paramètres de pare-feu pour NetScaler SD-WAN Network. En utilisant les paramètres du pare-feu global, vous pouvez configurer les paramètres du pare-feu global, ces paramètres sont appliqués à tous les sites sur le réseau WAN virtuel.

Pour configurer les paramètres de pare-feu globaux :

- 1. Dans l'Éditeur de configuration, accédez à Global> Paramètres réseau et cliquez sur l'icône Modifier.



2. Dans la section **Paramètres globaux du pare-feu**, sélectionnez les valeurs pour les options suivantes :
 - **Modèle de stratégie globale** - Sélectionnez un modèle de stratégie de pare-feu à appliquer à toutes les appliances du réseau SD-WAN, **Actions de pare-feu par défaut** - Sélectionnez Autoriser pour autoriser les paquets ne correspondant pas à la stratégie de filtre. Sélectionnez Déposer, pour supprimer les paquets ne correspondant pas à la stratégie de filtre, **Suivi de l'état de connexion par défaut** - Cette option active le suivi de l'état de la connexion directionnelle pour les flux TCP, UDP et ICMP qui ne correspondent pas à une stratégie de filtre ou à une règle NAT. Cela bloque le flux asymétrique, même lorsqu'aucune stratégie de pare-feu n'est définie.
3. Cliquez sur **Appliquer**.

Remarque

Vous pouvez également configurer ces paramètres au niveau du site, ce qui remplacera le paramètre global.

Paramètres avancés du pare-feu

May 6, 2021

Vous pouvez configurer individuellement les paramètres avancés du pare-feu pour chaque site. Cela remplacera les paramètres globaux.

Pour configurer les paramètres avancés du pare-feu :

1. Dans l'**Éditeur de configuration**, accédez à **Connexions > Afficher le site > Pare-feu > Paramètres**.

The screenshot shows the 'Advanced' configuration page for a firewall policy. At the top, there's a 'Section:' dropdown set to 'Settings'. Below it is a 'Policy Templates' section with a table:

Priority	Name	Delete
100	Policy_New	[Delete icon]

Below the table is the 'Advanced' section with various settings:

- Default Firewall Action:** Allow (dropdown)
- Default Connection State Tracking:** Use Global Setting (dropdown)
- ☒ **Source Route Validation**
- Max New Connections per Source:** 100 (input)
- Max Connections per Source:** 0 (input)
- Untracked and Denied Timeout (s):** 30 (input)
- TCP Initial Timeout (s):** 120 (input)
- TCP Idle Timeout (s):** 7440 (input)
- TCP Closing Timeout (s):** 60 (input)
- TCP Time Wait Timeout (s):** 120 (input)
- TCP Closed Timeout (s):** 10 (input)
- UDP Initial Timeout (s):** 30 (input)
- UDP Idle Timeout (s):** 300 (input)
- ICMP Initial Timeout (s):** 30 (input)
- ICMP Idle Timeout (s):** 60 (input)
- Generic Initial Timeout (s):** 30 (input)
- Generic Idle Timeout (s):** 300 (input)

At the bottom are 'Apply' and 'Revert' buttons.

2. Dans la section **Modèle de stratégie**, cliquez sur **Ajouter** . Entrez des valeurs pour les paramètres suivants.
 - **Priorité** - Ordre dans lequel la stratégie est appliquée sur le site.
 - **Nom** : nom du modèle de stratégie à utiliser sur le site.
3. Cliquez sur **Avancé**. Entrez des valeurs pour les paramètres suivants :
 - **Action par défaut du pare-feu** - Sélectionnez l'une des options suivantes.
 - **Utiliser le paramètre global**- Utiliser le paramètre global configuré dans les paramètres NetScaler SD-WAN
 - **Autoriser**- Les paquets ne correspondant à aucune stratégie de filtre sont autorisés.

- **Drop** - Les paquets ne correspondant à aucune stratégie de filtre sont supprimés.
 - **Suivi de l'état de connexion par défaut** —Sélectionnez l'une des options suivantes.
 - **Utiliser le paramètre global** - Utiliser le paramètre global configuré dans les paramètres NetScaler SD-WAN
 - **Aucun suivi - Le suivi** de l'état de la connexion bidirectionnelle ne sera pas effectué sur les paquets ne correspondant à aucune stratégie de filtre
 - **Track** - Le suivi de l'état de la connexion bidirectionnelle sera effectué sur les paquets TCP, UDP et ICMP qui ne correspondent à aucune stratégie de filtre ou règle NAT. Cela bloque le flux asymétrique, même lorsqu'aucune stratégie de pare-feu n'est définie.
 - **Validation de l'itinéraire source** : si cette option est activée, les paquets sont supprimés lorsqu'ils sont reçus sur une interface différente de la route du paquet, telle que déterminée par l'adresse IP source. Seul l'itinéraire que le paquet correspondrait actuellement est pris en compte.
 - **Nombre maximal de nouvelles connexions par source** : Nombre maximal de connexions non établies à autoriser par adresse IP source. 0 signifie illimité. Utilisez ce paramètre pour empêcher les attaques par déni de service sur le pare-feu.
 - **Nombre maximal de connexions par source** : Nombre maximal de connexions à autoriser par adresse IP source. 0 signifie illimité. Utilisez ce paramètre pour empêcher les attaques par déni de service sur le pare-feu.
4. Configurez les différents paramètres de délai d'expiration et cliquez sur **Appliquer**.

Zones

May 6, 2021

Vous pouvez configurer des zones dans le réseau et définir des stratégies pour contrôler la manière dont le trafic entre et quitte les zones. Par défaut, les zones suivantes sont créées :

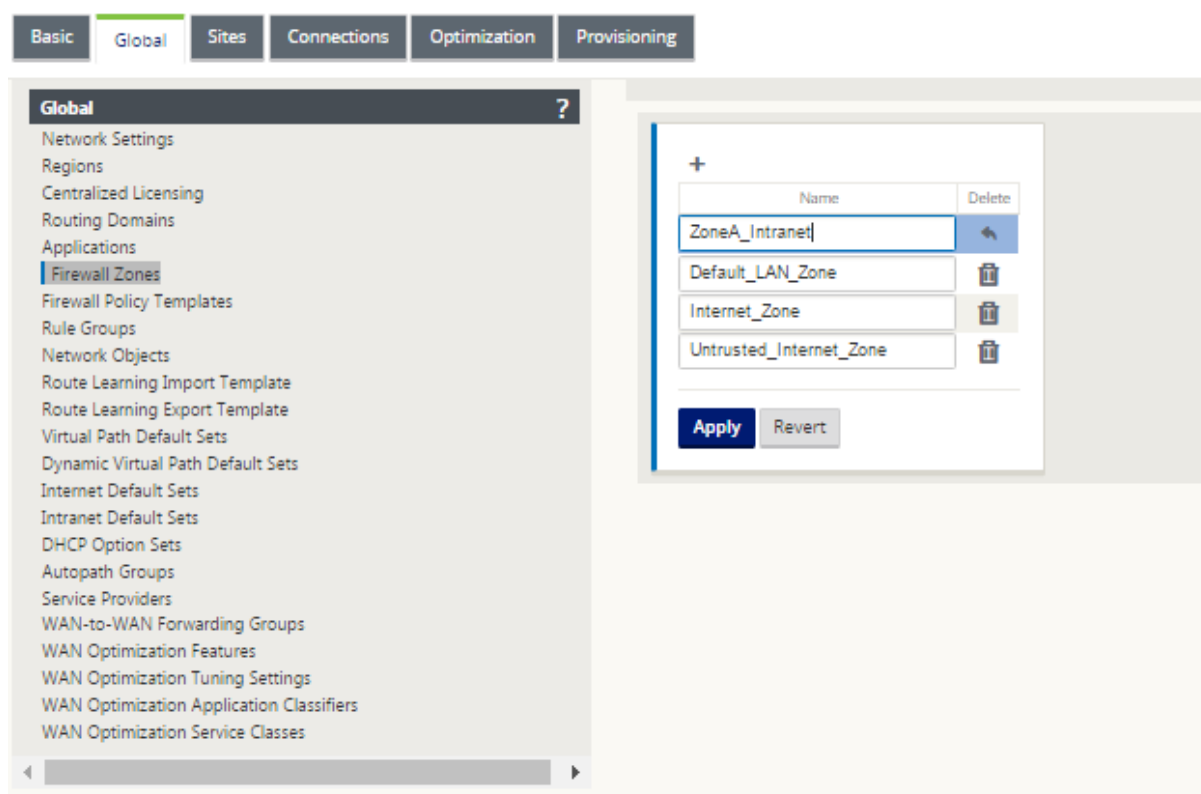
- Internet_Zone
 - S'applique au trafic à destination ou en provenance d'un service Internet utilisant une interface de confiance.
- Sans confiance Internet_Zone
 - S'applique au trafic à destination ou en provenance d'un service Internet utilisant une interface non approuvée.

- Default_LAN_Zone
 - S'applique au trafic à destination ou en provenance d'un objet avec une zone configurable, où la zone n'a pas été définie.

Vous pouvez créer vos propres zones et les affecter aux types d'objets suivants :

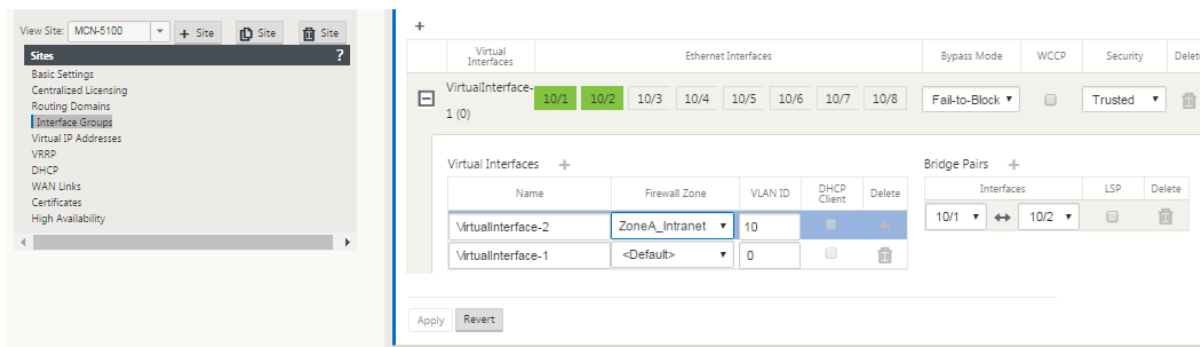
- Interfaces réseau virtuelles (VNI)
- Services Intranet
- Tunnels GRE
- Tunnels IPsec LAN

L'illustration suivante affiche les trois zones préconfigurées. En outre, vous pouvez créer vos propres zones selon vos besoins. Dans cet exemple, la zone « ZoneA_Intranet » est une zone créée par l'utilisateur. Il est affecté à l'interface virtuelle du segment de contournement (ports 1 et 2) de l'appliance SD-WAN.



La zone source d'un paquet est déterminée par le service ou l'interface réseau virtuelle sur laquelle un paquet est reçu. L'exception est le trafic de chemin d'accès virtuel. Lorsque le trafic entre dans un chemin virtuel, les paquets sont marqués par la zone à l'origine du trafic et cette zone source est transportée par le chemin virtuel. Cela permet à l'extrémité de réception du chemin d'accès virtuel de prendre une décision de stratégie basée sur la zone source d'origine avant d'entrer dans le chemin d'accès virtuel.

Par exemple, un administrateur réseau peut vouloir définir des stratégies de sorte que seul le trafic provenant du VLAN 30 sur le site A soit autorisé à entrer VLAN 10 sur le site B. L'administrateur peut affecter une zone à chaque VLAN et créer des stratégies qui autorisent le trafic entre ces zones et bloquent le trafic provenant d'autres zones. La capture d'écran ci-dessous montre comment un utilisateur attribuerait la zone « ZoneA_Intranet » au VLAN 10. Dans cet exemple, la zone « ZoneA_Intranet » a été précédemment définie par l'utilisateur afin de l'affecter à l'Interface Virtuelle « Interface Virtuelle 2 ».

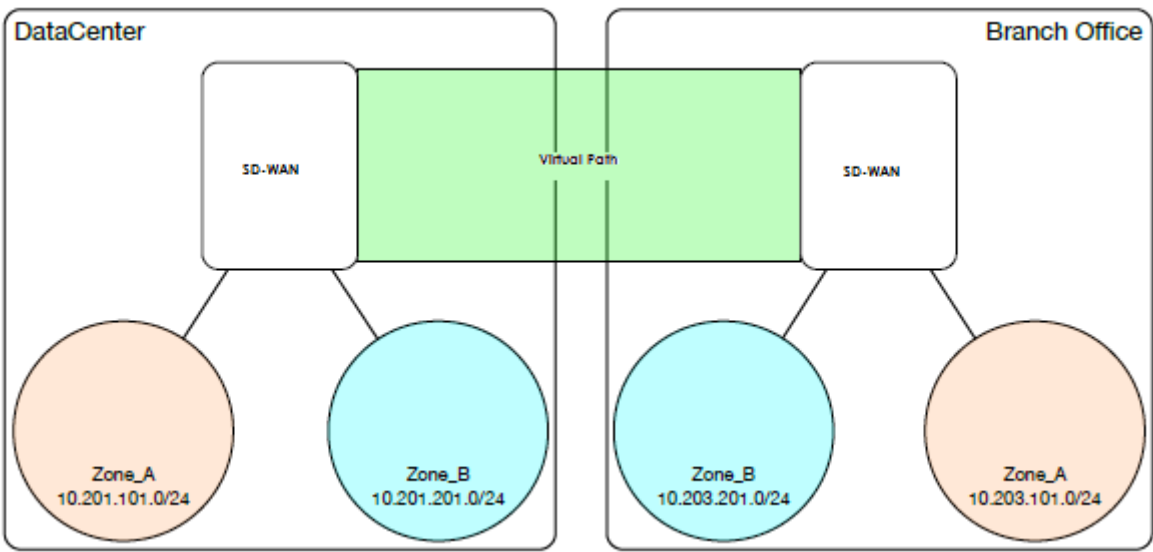


La zone de destination d'un paquet est déterminée en fonction de la correspondance d'itinéraire de destination. Lorsqu'une appliance SD-WAN recherche le sous-réseau de destination dans la table de routage, le paquet correspond à un itinéraire auquel une zone lui est affectée.

- Zone source
 - Chemin non virtuel : Déterminé par le paquet d'interface réseau virtuelle a été reçu le.
 - Chemin virtuel : Déterminé par le champ de zone source dans l'en-tête de flux de paquets.
 - Interface réseau virtuelle - le paquet a été reçu sur le site source.
- Zone de destination
 - Déterminé par la recherche d'itinéraire de destination du paquet.

Les itinéraires partagés avec des sites distants dans le SD-WAN conservent les informations sur la zone de destination, y compris les itinéraires appris par le protocole de routage dynamique (BGP, OSPF). Grâce à ce mécanisme, les zones acquièrent une importance globale dans le réseau SD-WAN et permettent un filtrage de bout en bout au sein du réseau. L'utilisation de zones fournit à un administrateur réseau un moyen efficace de segmenter le trafic réseau en fonction du client, de l'unité commerciale ou du service.

La capacité du pare-feu SD-WAN permet à l'utilisateur de filtrer le trafic entre les services au sein d'une seule zone ou de créer des stratégies qui peuvent être appliquées entre les services situés dans différentes zones, comme le montre la figure ci-dessous. Dans l'exemple ci-dessous, nous avons Zone_A et Zone_B, dont chacun a une interface réseau virtuel LAN.



La capture d'écran ci-dessous affiche l'héritage de zone pour une IP virtuelle (VIP) à partir de son interface réseau virtuelle (VNI) assignée.

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Stratégies

May 6, 2021

Les stratégies permettent d'autoriser, de refuser, de rejeter ou de compter et de poursuivre des flux de trafic spécifiques. Il serait difficile d'appliquer ces politiques individuellement à chaque site à mesure que les réseaux SD-WAN se développent. Pour résoudre ce problème, des groupes de filtres de pare-feu peuvent être créés avec un modèle de stratégie de pare-feu. Un modèle de stratégie de pare-feu peut être appliqué à tous les sites du réseau ou uniquement à des sites spécifiques. Ces stratégies sont classées sous la forme de stratégies de modèle d'appliance ou de stratégies de modèle post-appliance. Les stratégies de modèle pré-appliance et post-appliance à l'échelle du réseau sont configurées au niveau global. Les stratégies locales sont configurées au niveau du site sous Connexions et s'appliquent uniquement à ce site spécifique.

Pre-Appliance Template Policies

Template	Routing Domain	Action	Zones		Application	Application Family	Application Objects	Source			Destination			IP Address	Port
			From	To				IP Protocol	DSCP	Service	IP Address	Port	Service		
Local Policies		+ Add													

Priority	Routing Domain	Action	Zones		Application	Application Family	Application Objects	Source			Destination			IP Address	Port
			From	To				IP Protocol	DSCP	Service	IP Address	Port	Service		

Post-Appliance Template Policies

Template	Routing Domain	Action	Zones		Application	Application Family	Application Objects	Source			Destination			IP Address	Port
			From	To				IP Protocol	DSCP	Service	IP Address	Port	Service		

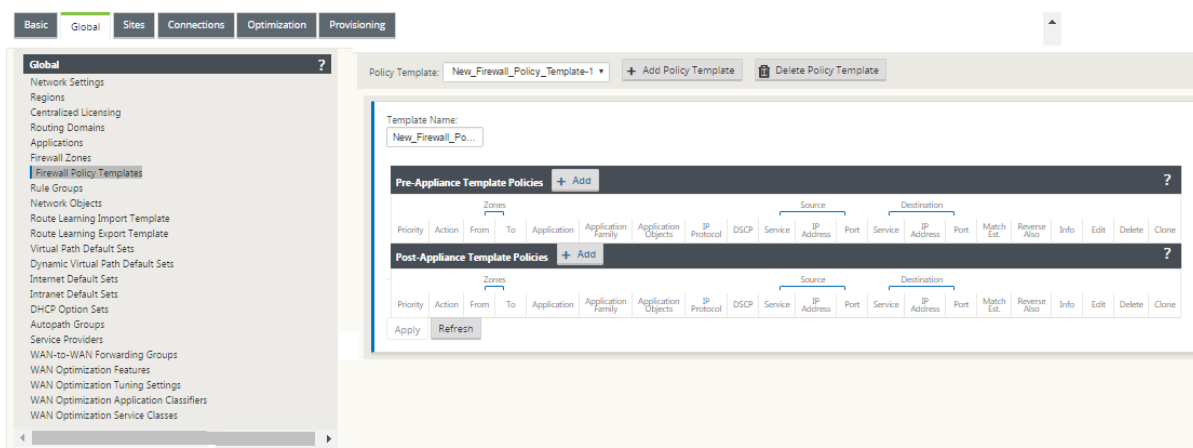
Les stratégies de modèle pré-appliance sont appliquées avant toute stratégie de site locale. Les stratégies de site locales sont ensuite appliquées, suivies des stratégies de modèle post-appliance. L'objectif est de simplifier le processus de configuration en vous permettant d'appliquer des stratégies globales tout en conservant la flexibilité nécessaire pour appliquer des stratégies spécifiques au site.

Ordre d'évaluation des stratégies de filtrage

1. Pré-modèles : règles compilées à partir de toutes les sections « PRE » des modèles.
2. Pré-global —Politiques compilées à partir de la section Global « PRE ».
3. Stratégies locales au niveau de l'appareil.
4. Génération automatique locale : stratégies générées automatiquement locales.
5. Post-templates : règles compilées à partir de toutes les sections « POST » des modèles.
6. Post-global —politiques compilées à partir de la section « POST » globale.

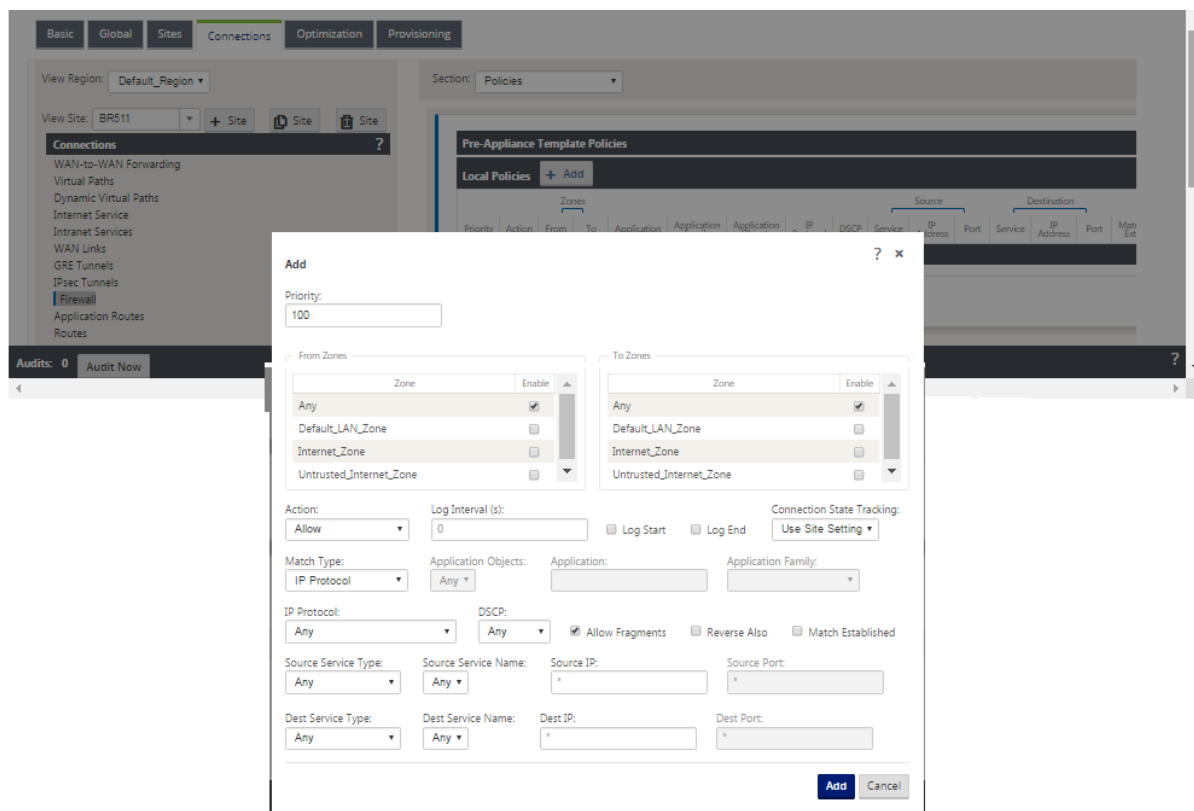
Définitions des stratégies - Globale et Locale (site)

Vous pouvez configurer les stratégies de modèle pré-appliance et post-appliance à un niveau global. Les stratégies locales sont appliquées au niveau du site d'une appliance.



La capture d'écran ci-dessus montre le modèle de stratégie qui s'appliquerait au réseau SD-WAN à l'échelle mondiale. Pour appliquer un modèle à tous les sites du réseau, accédez à **Global > Paramètres réseau > Modèle de stratégie globale**, puis sélectionnez une stratégie spécifique. Au niveau du site, vous pouvez ajouter d'autres modèles de stratégie, ainsi que créer des stratégies spécifiques au site.

Les attributs configurables spécifiques d'une stratégie sont affichés dans la capture d'écran ci-dessous, ceux-ci sont les mêmes pour toutes les stratégies.



Attributs de stratégie

- **Priorité** : ordre dans lequel la stratégie sera appliquée dans toutes les stratégies définies. Les stratégies de priorité inférieure sont appliquées avant les stratégies de priorité supérieure.
- **Zone** : les flux ont une zone source et une zone de destination.
 - **De la zone** : zone source de la stratégie.
 - **Zone de destination** : zone de destination de la stratégie.
- **Action** : action à effectuer sur un flux apparié.
 - **Autoriser** —**Autoriser** le flux à travers le pare-feu.
 - **Déposer** —refuser le flux à travers le pare-feu en déposant les paquets.
 - **Rejeter** : refusez le flux à travers le pare-feu et envoyez une réponse spécifique au protocole. TCP enverra une réinitialisation, ICMP enverra un message d'erreur.
 - **Count and Continue** : comptez le nombre de paquets et d'octets pour ce flux, puis continuez vers le bas dans la liste des stratégies.
- **Intervalle de journal** : délai en secondes entre la consignation du nombre de paquets correspondant à la stratégie au fichier journal du pare-feu ou au serveur syslog, s'il est configuré.
 - **Début du journal** : si cette option est sélectionnée, une entrée de journal est créée pour le nouveau flux.
 - **Fin du journal** : enregistre les données d'un flux lors de la suppression du flux.

Remarque

La valeur par défaut de l'intervalle de journalisation est 0 ce qui signifie qu'il n'y a pas de journalisation.

- **Track** : permet au pare-feu de suivre l'état d'un flux et d'afficher ces informations dans le tableau **Surveillance > Pare-feu > Connexions** . Si le flux n'est pas suivi, l'état affichera NOT_TRACKED. Consultez le tableau ci-dessous pour le suivi de l'état basé sur le protocole. Utilisez le paramètre défini au niveau du site sous **Pare-feu > Paramètres > Avancé > Suivi par défaut**.
 - **Aucune piste** : l'état du flux n'est pas activé.
 - **Track** : affiche l'état actuel du flux (correspondant à cette stratégie).
- **Type de correspondance** : sélectionnez l'un des types de correspondance suivants
 - **Protocole IP** : si ce type de correspondance est sélectionné, sélectionnez un protocole IP auquel le filtre correspondra. Les options incluent ANY, TCP, UDP ICMP et ainsi de suite

- **Application** : si ce type de correspondance est sélectionné, spécifiez l'application utilisée comme critère de correspondance pour ce filtre.
- **Famille d'applications** : si ce type de correspondance est sélectionné, sélectionnez une famille d'applications utilisée comme critère de correspondance pour ce filtre.
- **Objet application** : si ce type de correspondance est sélectionné, sélectionnez une famille d'applications utilisée comme critère de correspondance pour ce filtre.

Pour plus d'informations sur l'application, la famille d'applications et l'objet d'application, reportez-vous à la section [Classification des applications](#).

- **DSCP** : permet à l'utilisateur de faire correspondre un paramètre de balise DSCP.
- **Autoriser les fragments** : autoriser les fragments IP correspondant à cette stratégie de filtre.

Remarque

Le pare-feu ne réassemble pas les cadres fragmentés.

- **Inverser également** : ajoutez automatiquement une copie de cette stratégie de filtre avec les paramètres source et destination inversés.
- **Correspondance établie** : correspond aux paquets entrants pour une connexion à laquelle les paquets sortants ont été autorisés.
- **Type de service source** —en référence à un service SD-WAN —Local (à l'appliance), Virtual Path, Intranet, IPhost ou Internet sont des exemples de types de service.
- **Option IPhost** - Il s'agit d'un nouveau type de service pour le pare-feu et est utilisé pour les paquets générés par l'application SD-WAN. Par exemple, l'exécution d'un ping à partir de l'interface utilisateur Web du SD-WAN entraîne un paquet provenant d'une adresse IP virtuelle SD-WAN. La création d'une stratégie pour cette adresse IP nécessiterait que l'utilisateur sélectionne l'option IPhost.
- **Nom du service source** : nom d'un service lié au type de service. Par exemple, si le chemin d'accès virtuel est sélectionné pour le type de service source, il s'agit du nom du chemin d'accès virtuel spécifique. Ce n'est pas toujours nécessaire et dépend du type de service sélectionné.
- **Adresse IP source** : **adresse** IP typique et masque de sous-réseau que le filtre utilisera pour faire correspondre.
- **Port source** : port source que l'application spécifique utilisera.
- **Type de service de destination** : en référence à un service SD-WAN : Local (à l'appliance), Virtual Path, Intranet, IPhost ou Internet sont des exemples de types de service.
- **Nom du service de destination** : nom d'un service lié au type de service. Ce n'est pas toujours nécessaire et dépend du type de service sélectionné.

- **Adresse IP de destination : adresse** IP typique et masque de sous-réseau que le filtre utilisera pour faire correspondre.
- **Port** de destination : port de destination que l'application spécifique utilisera (port de destination HTTP 80 pour le protocole TCP).

L'option piste fournit beaucoup plus de détails sur un flux. Les informations d'état suivies dans les tables d'état sont incluses ci-dessous.

Table d'état de l'option piste

Il n'y a que quelques États qui sont cohérents :

- Connexion **INIT**- créée, mais le paquet initial n'était pas valide.
- Les paquets **O_DENIED**- qui ont créé la connexion sont refusés par une stratégie de filtre.
- Les paquets **R_DENIED**- du répondeur sont refusés par une stratégie de filtre.
- **NOT_TRACKED**- la connexion n'est pas suivie de manière dynamique mais est autorisée dans le cas contraire.
- **CLOSED**- la connexion a expiré ou a été fermée par le protocole.
- **DELETED** - la connexion est en cours de suppression. L'état DELETED ne sera presque jamais vu.

Tous les autres états sont spécifiques au protocole et nécessitent l'activation du suivi avec état.

TCP peut signaler les états suivants :

- **SYN_SENT** - premier message TCP SYN vu.
- **SYN_SENT2** - Message SYN vu dans les deux sens, pas SYN+ACK (AKA ouvert simultanément).
- **SYN_ACK_RCVD** - SYN+ACK reçu.
- **ESTABLISHED**- deuxième ACK reçu, la connexion est entièrement établie.
- **FIN_WAIT** - premier message FIN vu.
- **CLOSE_WAIT** - Message FIN vu dans les deux sens.
- **TIME_WAIT** - dernier ACK vu dans les deux sens. La connexion est maintenant fermée en attendant la réouverture.

Tous les autres protocoles IP (notamment ICMP et UDP) ont les états suivants :

- **NEW** - paquets vus dans une direction.
- **ESTABLISHED** - paquets vus dans les deux sens.

Traduction d'adresses réseau (NAT)

May 6, 2021

Network Address Translation (NAT) effectue la conservation des adresses IP afin de préserver le nombre limité d'adresses IPv4 enregistrées. Il permet aux réseaux IP privés qui utilisent des adresses IP non enregistrées de se connecter à Internet. La fonctionnalité NAT sur Citrix SD-WAN connecte votre réseau SD-WAN privé à l'Internet public. Il traduit les adresses privées dans le réseau interne en une adresse publique légale. NAT assure également une sécurité supplémentaire en annonçant une seule adresse pour l'ensemble du réseau sur Internet, cachant l'ensemble du réseau interne. Citrix SD-WAN prend en charge les types NAT suivants :

- NAT statique un-à-un
- NAT dynamique (traduction d'adresse de port PAT-)
- NAT dynamique avec règles de transfert de port

Remarque

La fonctionnalité NAT ne peut être configurée qu'au niveau du site. Il n'y a pas de configuration globale (modèles) pour NAT. Toutes les stratégies NAT sont définies à partir d'une traduction Source-NAT (« SNAT »). Les règles Destination-NAT correspondantes (« DNAT ») sont créées automatiquement pour l'utilisateur.

NAT statique

June 8, 2022

Le NAT statique est un mappage un-à-un d'une adresse IP privée ou d'un sous-réseau à l'intérieur du réseau SD-WAN vers une adresse IP publique ou un sous-réseau en dehors du réseau SD-WAN. Configurez le NAT statique en saisissant manuellement l'adresse IP interne et l'adresse IP externe vers laquelle il doit traduire. Vous pouvez configurer NAT statique pour les services de domaine Local, Virtual Paths, Internet, Intranet et Inter-routage.

NAT entrant et sortant

La direction d'une connexion peut être de l'intérieur vers l'extérieur ou de l'extérieur vers l'intérieur. Lorsqu'une règle NAT est créée, elle est appliquée aux deux directions en fonction du type de correspondance de direction.

- Entrant : l'adresse source est traduite pour les paquets reçus sur le service. L'adresse de destination est traduite pour les paquets transmis sur le service. Par exemple, service Internet au service LAN — Pour les paquets reçus (Internet vers LAN), l'adresse IP source est traduite. Pour les paquets transmis (LAN vers Internet), l'adresse IP de destination est traduite.
- Sortant : l'adresse de destination est traduite pour les paquets reçus sur le service. L'adresse source est traduite pour les paquets transmis sur le service. Par exemple, le service LAN au service Internet — pour les paquets transmis (LAN à Internet), l'adresse IP source est traduite. Pour les paquets reçus (Internet vers LAN), l'adresse IP de destination est traduite.

Dérivation de zone

Les zones de pare-feu source et de destination pour le trafic entrant ou sortant ne doivent pas être identiques. Si les zones de pare-feu source et de destination sont toutes les deux identiques, NAT n'est pas effectué sur le trafic.

Pour le NAT sortant, la zone extérieure est automatiquement dérivée du service. Chaque service sur SD-WAN est associé à une zone par défaut. Par exemple, le service Internet sur un lien Internet approuvé est associé à la zone Internet de confiance. De même, pour un NAT entrant, la zone interne est dérivée du service.

Pour un service de chemin virtuel, la dérivation de la zone NAT ne se produit pas automatiquement, vous devez entrer manuellement la zone intérieure et extérieure. Le NAT est effectué sur le trafic appartenant à ces zones uniquement. Les zones ne peuvent pas être dérivées pour les chemins virtuels car il peut y avoir plusieurs zones dans les sous-réseaux de chemins virtuels.

Configurer les stratégies NAT statiques

Pour configurer des stratégies NAT statique, dans l'Éditeur de configuration, accédez à **Connexions > Pare-feu > Stratégies NAT statiques**.

Static NAT Strategy configuration window:

- Priority: 100
- Direction: Outbound
- Service Type: Internet
- Service Name: Internet
- Inside Zone: Default_LAN_Zo
- Inside IP Address: 172.57.79.179/32
- Outside IP Address: 172.57.52.174/32
- ☐ Bind Responder Route
- ☐ Proxy ARP
- Buttons: Apply, Cancel

- **Priorité** : Ordre dans lequel la stratégie sera appliquée dans toutes les stratégies définies. Les stratégies de priorité inférieure sont appliquées avant les stratégies de priorité supérieure.
- **Direction** : la direction dans laquelle le trafic circule, du point de vue de l'interface virtuelle ou du service. Il peut s'agir d'un trafic entrant ou sortant.
- **Type de service** : Types de service SD-WAN auxquels la stratégie NAT est appliquée. Pour NAT statique, les types de service pris en charge sont les services de domaine Local, Virtual Paths, Internet, Intranet et Inter-routage
- **Nom du service** : sélectionnez un nom de service configuré qui correspond au type de service.
- **Zone intérieure** : Type de correspondance de zone de pare-feu intérieur à partir de laquelle le paquet doit être pour permettre la traduction.
- **Zone extérieure** : type de correspondance de zone de pare-feu extérieur à partir de laquelle le paquet doit être pour permettre la traduction.
- **Adresse IP interne** : l'adresse IP interne et le préfixe qui doivent être traduits si les critères de correspondance sont remplis.
- **Adresse IP externe** : adresse IP externe et préfixe vers lesquels l'adresse IP interne est traduite si les critères de correspondance sont remplis.
- **Route du répondeur de liaison** : garantit que le trafic de réponse est envoyé sur le même service que celui sur lequel il est reçu, afin d'éviter un routage asymétrique.
- **ARP proxy** : garantit que l'appliance répond aux demandes ARP locales pour l'adresse IP externe.

Stratégies NAT statiques pour le service Internet IPv6

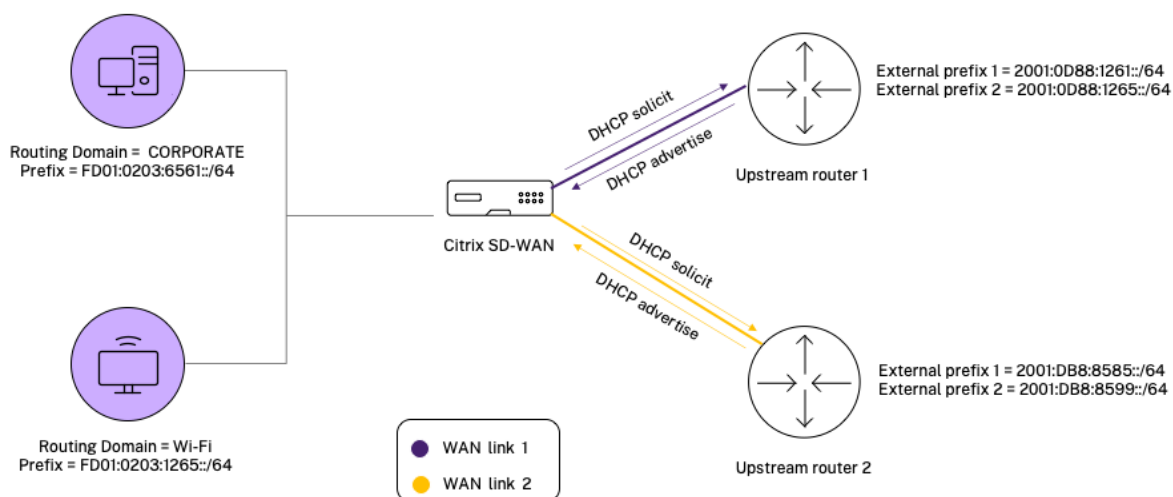
Citrix SD-WAN prend en charge les stratégies NAT statiques pour le service Internet IPv6 à partir de la version 11.4.0. Une stratégie NAT statique pour le service Internet IPv6 spécifie le mappage d'un préfixe réseau interne à un préfixe réseau externe. Le nombre de stratégies NAT statiques requises dépend du nombre de réseaux internes et du nombre de réseaux externes (liaisons WAN). S'il existe un nombre **M** de réseaux internes et un nombre **N** de liaisons WAN, le nombre de stratégies NAT statiques requises est **M x N**.

À partir de Citrix SD-WAN version 11.4.0, lors de la création d'une stratégie NAT statique, vous pouvez entrer manuellement l'adresse IP externe ou activer l'**Autolearn via DP**. Lorsque l'**Autolearn via DP** est activé, l'appliance Citrix SD-WAN reçoit des préfixes délégués du routeur délégué en amont via la délégation de préfixe DHCPv6. Avant Citrix SD-WAN version 11.4.0, l'adresse IP externe était dérivée automatiquement du service et il n'était pas possible de saisir manuellement l'adresse IP externe. Si vous mettez à niveau un dispositif vers la version 11.4.0 ou une version ultérieure et que des stratégies NAT statiques sont configurées pour le service Internet IPv6, vous devez mettre à jour manuellement les stratégies.

Exemple de configuration

Dans la topologie suivante, l'apppliance Citrix SD-WAN est configurée avec 2 réseaux internes et 2 liaisons WAN :

- Le réseau interne 1 réside dans le domaine de routage CORPORATE avec le préfixe réseau FD01:0203:6561::/64
- Le réseau interne 2 réside dans le domaine de routage Wi-Fi avec le préfixe réseau FD01:0203:1265::/64
- Via la liaison WAN 1, l'apppliance SD-WAN reçoit du routeur délégué amont via la délégation de préfixe DHCPv6, 2 préfixes délégués 2001:0D88:1261::/64 et 2001:0D88:1265::/64. Ces 2 préfixes délégués sont utilisés comme préfixes de réseau externe lorsque le trafic provenant des réseaux internes transite par la liaison WAN 1.
- Via la liaison WAN 2, l'apppliance SD-WAN reçoit du routeur délégué amont via la délégation de préfixe DHCPv6, 2 préfixes délégués 2001:DB8:8585::/64 et 2001:DB8:8599::/64. Ces 2 préfixes délégués sont utilisés comme préfixes de réseau externe lorsque le trafic provenant des réseaux internes transite par la liaison WAN 2.



Dans ce scénario, il y a $M=2$ à l'intérieur des réseaux et des liaisons WAN $N=2$. Par conséquent, le nombre de stratégies NAT statiques requises pour un déploiement correct du service Internet IPv6 est de $2 \times 2 = 4$. Ces 4 stratégies NAT statiques spécifient la traduction d'adresse pour :

- Réseau interne 1 via la liaison WAN 1
- Réseau interne 1 via la liaison WAN 2
- Réseau interne 2 via la liaison WAN 1
- Réseau interne 2 via la liaison WAN 2

Pour configurer ces stratégies NAT statiques, dans l'éditeur de configuration, accédez à **Connexions > Pare-feu > Stratégies NAT statiques**.

Section: Static NAT Policies

Priority	Routing Domain	Direction	Service	Inside Zone	Inside IP Address	Outside Zone	Outside IP Address	Edit	Delete	Clone
100	CORPORATE	Outbound	Internet	*	FD01:0203:6561::/64	Untrusted_Internet_Zone				
200	CORPORATE	Outbound	Internet	*	FD01:0203:6561::/64	Untrusted_Internet_Zone				
300	WIFI	Outbound	Internet	*	FD01:0203:1265::/64	Untrusted_Internet_Zone				
400	WIFI	Outbound	Internet	*	FD01:0203:1265::/64	Untrusted_Internet_Zone				

Apply Refresh

Lors de la création de stratégies NAT, veuillez à sélectionner le **type de service** comme **Internet** et le type d'**adresse IP** comme **IPv6**. Sélectionnez le lien WAN et, dans le champ **Adresse IP interne**, entrez le préfixe réseau interne (seuls les préfixes /64 sont autorisés). Dans le champ **Adresse IP extérieure**, vous pouvez soit entrer manuellement le préfixe réseau externe, soit activer la case à cocher **AutoLearn via DP**.

Voici un exemple dans lequel l'adresse IP externe est entrée manuellement dans la stratégie NAT statique.

Priority: 100 Routing Domain: CORPORATE

Direction: Outbound Service Type: Internet Service Name: Internet WAN Link: O365t1-WL-1

Inside Zone: <Any> IP Address Type: IPv6 Inside IP Address: FD01:0203:6561:...

Outside IP Address: 2001:0D88:1265::/64 ☐ AutoLearn via PD

☒ Bind Responder Route ☐ Proxy ARP/NDP ☒ Allow Related

Apply Cancel

Si vous activez la case à cocher **AutoLearn via DP**, assurez-vous que le routeur amont prend en charge la délégation de préfixe DHCPv6. Citrix SD-WAN demande un préfixe au routeur délégué en amont et le routeur délégué répond par un préfixe à Citrix SD-WAN. Citrix SD-WAN utilise ce préfixe délégué pour traduire l'adresse IP interne en adresse IP externe.

Voici un exemple dans lequel l'**apprentissage automatique via DP** est activé, de sorte que le préfixe réseau externe est obtenu via la délégation de préfixe DHCPv6.

Priority:	Routing Domain		
<input type="text" value="200"/>	<input type="text" value="CORPORATE"/>		
Direction:	Service Type:	Service Name:	WAN Link:
<input type="text" value="Outbound"/>	<input type="text" value="Internet"/>	<input type="text" value="Internet"/>	<input type="text" value="O365t1-WL-2"/>
Inside Zone:	IP Address Type:	Inside IP Address:	
<input type="text" value="<Any>"/>	<input type="text" value="IPv6"/>	<input type="text" value="FD01:0203:6561:..."/>	
Outside IP Address:	<input checked="" type="checkbox"/> AutoLearn via PD		
<input checked="" type="checkbox"/> Bind Responder Route <input type="checkbox"/> Proxy ARP/NDP <input checked="" type="checkbox"/> Allow Related			
<div>Apply Cancel</div>			

Surveillance

Pour surveiller NAT, accédez à **Surveillance > Statistiques du pare-feu > Connexions**. Pour une connexion, vous pouvez voir si NAT est fait ou non.

Dashboard Monitoring Configuration

Monitoring > Firewall

Firewall Statistics

Statistics: **Connections**

Maximum entries to display: **50**

Filtering:

Application: **Any** Family: **Any**

IP Protocol: **Any** Source Zone: **Any** Destination Zone: **Any**

Source Service Type: **Any** Source Service Instance: **Any** Source IP: ***** Source Port: *****

Destination Service Type: **Any** Destination Service Instance: **Any** Destination IP: ***** Destination Port: *****

Refresh ☐ Show latest data ☐ Show Additional Stats

Clear Connections

Help

Connections

			Source					Destination							Sent				Received				
Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	Kbps	Packets	Bytes	PPS	Kbps	Age (s)
Internet Control Message Protocol(Icmp)	Network Service	ICMP	172.57.79.179	3261	Local	Guest_The_rjd	Default_LAN_Zone	172.57.70.176	3261	Internet	MCN-PA-Internet	Internet_Zone	ESTABLISHED	Yes	6	504	1.004	0.675	6	504	1.004	0.675	6

Connections Displayed: 1
Connections In Use: 1/128000

Pour vérifier si l'apprentissage automatique via PD est configuré pour une règle NAT, accédez à **Configuration > Virtual WAN > View Configuration** et choisissez **Pare-feu** dans la liste déroulante **View**. Les colonnes **Auto-learn via PD** et **PD prefix ID** affichent les détails.

[illegible]

Pour afficher plus en détail le mappage de l'adresse IP interne à l'adresse IP externe, cliquez sur **NAT post-route** sous **Objets associés** ou accédez à **Surveillance > Statistiques de pare-feu > Stratégies NAT**.

La capture d'écran suivante montre le mappage de l'adresse interne à l'adresse externe dans une stratégie NAT statique IPv4.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any

Service Type: Any Service Name: Any

Inside IP: * Inside Port: * Outside IP: * Outside Port: *

Refresh

Show latest data.

Help

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside		Outside		Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
							IP Address	Port	IP Address	Port									
1	Static	-	Outbound	*	Internet	-	172.57.79.179/32	*	172.57.52.174/32	*	No	No	No	1971	165564	1635	137340	1	[Connections]

NAT Policies Displayed: 1
NAT Policies In Use: 1/1000
Port Restricted Dynamic NAT Policies In Use: 0/100
Destination NAT Policies In Use: 0/100

La capture d'écran suivante montre le mappage de l'adresse interne à l'adresse externe dans une stratégie NAT statique IPv6.

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any

Service Type: Any Service Name: Any

Inside IP: * Inside Port: * Outside IP: * Outside Port: *

Refresh

Show latest data.

Help

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside		Outside		Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
							IP Address	Port	IP Address	Port									
1	Static	-	Outbound	*	Internet	-	2006::/64	*	2004::/64	*	Yes	No	No	26	2144				
2	Dynamic PR	-	Outbound	*	Internet	-	*	*	172.170.11.85/32	*	No	No	No	390832	71419346	409			
3	Dynamic Sym	-	Outbound	*	Internet	-	*	*	2004::85/128	*	No	No	No	51	4112				

NAT Policies Displayed: 3
NAT Policies In Use: 3/1000
Port Restricted Dynamic NAT Policies In Use: 2/100
Destination NAT Policies In Use: 0/100

Journaux

Vous pouvez afficher les journaux liés à NAT dans les journaux de pare-feu. Pour afficher les journaux pour NAT, créez une stratégie de pare-feu qui correspond à votre stratégie NAT et assurez-vous que

la journalisation est activée sur le filtre de pare-feu. Les journaux NAT affichent les informations suivantes :

- Date et heure
- Domaine de routage
- Protocole IP
- Port source
- Adresse IP source
- Adresse IP traduite
- Port traduit
- Adresse IP de destination
- Port de destination

Edit ? x

Priority: 100 Policy Type: Built-in Firewall

Match Criteria

From Zones	To Zones
Zone	Zone
Any <input checked="" type="checkbox"/>	Any <input checked="" type="checkbox"/>
Default_LAN_Zone <input type="checkbox"/>	Default_LAN_Zone <input type="checkbox"/>
gre_zone <input type="checkbox"/>	gre_zone <input type="checkbox"/>
Inter Routing Domain Zone <input type="checkbox"/>	Inter Routing Domain Zone <input type="checkbox"/>

Routing Domain: Any

Traffic Match Type: IP Protocol IP Protocol: Any DSCP: Any ☐ Match Established

Application: Application Family: Application Objects: Any

Source Service Type: Any Source Service Name: Any Source IP: * Source Port: *

Dest Service Type: Any Dest Service Name: Any Dest IP: * Dest Port: *

Actions

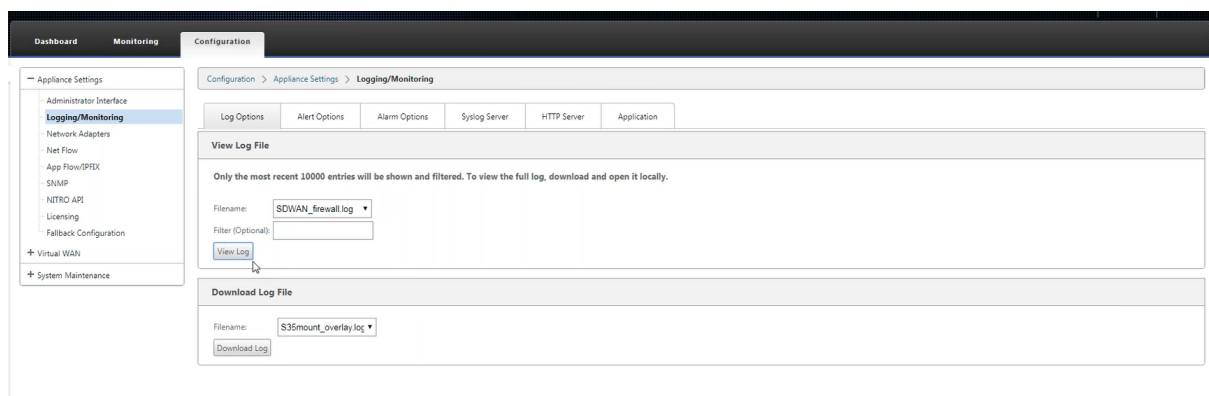
Action: Allow ☒ Allow Fragments Connection State Tracking: Use Site Setting

Logging & Other Options

Log Interval (s): 60 ☒ Log Start ☒ Log End ☐ Add Reverse Policy

Apply **Cancel**

Pour générer des journaux NAT, accédez à **Logging/Monitoring > Log Options**, sélectionnez **SDWAN_firewall.log**, puis cliquez sur **View Log**.



Les détails de connexion NAT sont affichés dans le fichier journal.

```

2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/ NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:44.750109+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981584+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108299+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299585+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 58 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)

2022-02-14T11:43:53.184990+0000 WARN find_and_update_connection@forward/firewall/connection.c:4828 Conn 0x7ffffdbf5f168 Aborted, NAT
2022-02-14T11:43:53.185044+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:43:53.565134+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:43:59.572977+0000 INFO t2_firewall_monitor.pl Connection DELETED for (Routing Domain Default_RoutingDomain) IPv6_ICMP
2022-02-14T11:45:12.399564+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) UDP 1
2022-02-14T11:45:48.516174+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:45:48.717951+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 488 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:18.786955+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:21.760939+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:21.761368+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 3 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:27.766610+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:32.774464+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:32.775063+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)

```

NAT dynamique

June 8, 2022

Le NAT dynamique est un mappage plusieurs-à-un d'une adresse IP privée ou de sous-réseaux à l'intérieur du réseau SD-WAN vers une adresse IP publique ou un sous-réseau en dehors du réseau SD-WAN. Le trafic provenant de différentes zones et sous-réseaux sur des adresses IP de confiance (internes) dans le segment LAN est envoyé sur une seule adresse IP publique (externe).

Types NAT dynamiques

Dynamic NAT effectue la traduction d'adresses de port (PAT) ainsi que la traduction d'adresses IP. Les numéros de port sont utilisés pour distinguer quel trafic appartient à quelle adresse IP. Une seule

adresse IP publique est utilisée pour toutes les adresses IP privées internes, mais un numéro de port différent est attribué à chaque adresse IP privée. PAT est un moyen économique d'autoriser plusieurs hôtes à se connecter à Internet à l'aide d'une seule adresse IP publique.

- **Port Restreint** : Port Restreint NAT utilise le même port externe pour toutes les traductions liées à une paire d'adresses IP internes et de ports. Ce mode est généralement utilisé pour autoriser les applications P2P Internet.
- **Symétrique** : le NAT symétrique utilise le même port externe pour toutes les traductions liées à une adresse IP intérieure, un port intérieur, une adresse IP extérieure et un tuple de port externe. Ce mode est généralement utilisé pour améliorer la sécurité ou augmenter le nombre maximal de sessions NAT.

NAT entrant et sortant

La direction d'une connexion peut être de l'intérieur vers l'extérieur ou de l'extérieur vers l'intérieur. Lorsqu'une règle NAT est créée, elle est appliquée aux deux directions en fonction du type de correspondance de direction.

- **Sortant** : l'adresse de destination est traduite pour les paquets reçus sur le service. L'adresse source est traduite pour les paquets transmis sur le service. Le NAT dynamique sortant est pris en charge sur les services de domaine Local, Internet, Intranet et Inter-routage. Pour les services WAN tels que les services Internet et Intranet, l'adresse IP de liaison WAN configurée est choisie dynamiquement comme adresse IP externe. Pour les services de domaine Local et Inter-routage, fournissez une adresse IP externe. La zone extérieure est dérivée du service sélectionné. Un cas d'utilisation typique de NAT dynamique sortant consiste à permettre simultanément à plusieurs utilisateurs de votre réseau local d'accéder en toute sécurité à Internet à l'aide d'une seule adresse IP publique.
- **Entrant** : l'adresse source est traduite pour les paquets reçus sur le service. L'adresse de destination est traduite pour les paquets transmis sur le service. Le NAT dynamique entrant n'est pas pris en charge sur les services WAN tels qu'Internet et Intranet. Il y a une erreur d'audit explicite pour indiquer la même chose. Le NAT dynamique entrant est pris en charge uniquement sur les services de domaine Local et Inter-routage. Indiquez une zone extérieure et une adresse IP externe à traduire. Un cas d'utilisation typique du NAT dynamique entrant consiste à autoriser les utilisateurs externes à accéder à des serveurs de messagerie ou Web hébergés dans votre réseau privé.

Configurer les stratégies NAT dynamiques

Pour configurer des stratégies NAT dynamique, dans l'Éditeur de configuration, accédez à **Connexions > Pare-feu > Stratégies NAT dynamiques**.

? x

Add

Priority:
100

Direction: Outbound ▼ Type: Port Restricted ▼ Service Type: Internet ▼ Service Name: Internet ▼

Inside Zone: Any ▼ Inside IP Address: *

☒ Allow Related
 ☐ IPsec Passthrough
 ☐ GRE/PPTP Passthrough
☒ Port Parity
☐ Bind Responder Route

Port Forwarding Rules +

Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete

Add Cancel

- **Priorité** : Ordre dans lequel la stratégie est appliquée dans toutes les stratégies définies. Les stratégies de priorité inférieure sont appliquées avant les stratégies de priorité supérieure.
- **Direction** : la direction dans laquelle le trafic circule, du point de vue de l'interface virtuelle ou du service. Il peut s'agir d'un trafic entrant ou sortant.
- **Type** : type de NAT dynamique à exécuter, restreint par port ou Symétrique.
- **Type de service** : Types de service SD-WAN sur lesquels la stratégie NAT dynamique est appliquée. Le NAT dynamique entrant est pris en charge sur les services de domaine local et inter-routage. NAT dynamique sortant est pris en charge sur les services de domaine local, Internet, Intranet et Inter-routage
- **Nom du service** : sélectionnez un nom de service configuré qui correspond au type de service.
- **Zone intérieure** : Type de correspondance de zone de pare-feu intérieur à partir de laquelle le paquet doit être pour permettre la traduction.
- **Zone extérieure** : pour le trafic entrant, spécifiez le type de correspondance de zone de pare-feu externe à partir de laquelle le paquet doit être pour autoriser la traduction.
- **Adresse IP interne** : l'adresse IP interne et le préfixe qui doivent être traduits si les critères de correspondance sont remplis. Entrez « * » pour indiquer une adresse IP interne.
- **Adresse IP externe** : adresse IP externe et préfixe vers lesquels l'adresse IP interne est traduite si les critères de correspondance sont remplis. Pour le trafic sortant utilisant les services Internet et Intranet, l'adresse IP de liaison WAN configurée est choisie dynamiquement comme adresse IP externe.
- **Autoriser apparenté** : Autoriser le trafic lié au flux correspondant à la règle. Par exemple, la redirection ICMP liée au flux spécifique correspondant à la stratégie, s'il y avait un type d'erreur lié au flux.
- **Passer IPsec** : Autoriser une session IPsec (AH/ESP) à être traduite.
- **Transformation GRE/PPTP** : Autoriser la traduction d'une session GRE/PPTP.
- **Parité de port** : Si cette option est activée, les ports externes pour les connexions NAT conser-

vent la parité (même si le port intérieur est pair, impair si le port extérieur est impair).

- **Bind Responder Route** : garantit que le trafic de réponse est envoyé sur le même service que celui sur lequel il est reçu, afin d'éviter le routage asymétrique.

Transfert de port

NAT dynamique avec transfert de port vous permet de transférer le trafic spécifique vers une adresse IP définie. Ceci est généralement utilisé pour les hôtes internes tels que les serveurs Web. Une fois le NAT dynamique configuré, vous pouvez définir les stratégies de transfert de port. Configurez NAT dynamique pour la traduction d'adresses IP et définissez la stratégie de transfert de port pour mapper un port externe à un port intérieur. Le transfert de port NAT dynamique est généralement utilisé pour permettre aux hôtes distants de se connecter à un hôte ou à un serveur sur votre réseau privé. Pour un cas d'utilisation plus détaillé, reportez-vous à la section [Citrix SD-WAN Dynamic NAT expliquée](#).

Add ? x

Priority:
200

Direction: Inbound Type: Symmetric Service Type: Local Service Name: VirtualInterfac...

Inside IP Address: * Outside Zone: Internet_Zone Outside IP Address: 172.147.12.83

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☐ Bind Responder Route

Port Forwarding Rules +

Routing Domain	Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
Default_RoutingDomain	Both	443	15.15.15.1	443	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	Use Site Setting	

Add **Cancel**

- **Protocole** : TCP, UDP ou les deux.
- **Port extérieur** : Port externe qui est port avant vers le port intérieur.
- **Adresse IP intérieure** : Adresse interne pour transférer les paquets correspondants.
- **Port intérieur** : Port intérieur dans lequel le port extérieur sera transféré.
- **Fragments** : Autoriser le transfert de paquets fragmentés.
- **Intervalle des journaux** : Temps en seconde entre la consignation du nombre de paquets correspondant à la stratégie à un serveur syslog. La valeur par défaut de 0 signifie qu'il n'y a pas de journalisation.
- **Début du journal** : Si cette option est sélectionnée, une nouvelle entrée de journal est créée pour le nouveau flux.
- **Findu journal** : Consigner les données d'un flux lorsque le flux est supprimé.
- **Suivi** : Le suivi bidirectionnel de l'état de connexion est effectué sur les paquets TCP, UDP et ICMP correspondant à la règle. Cette fonctionnalité bloque les flux qui semblent illégitimes, en

raison d’un routage asymétrique ou d’un échec de la somme de contrôle, validation spécifique au protocole. Les détails de l’état sont affichés sous

Surveillance > Pare-feu > Connexions.

- **Aucun suivi :** Le suivi bidirectionnel de l’état de connexion n’est pas effectué sur les paquets correspondant à la règle.

Chaque règle de transfert de port a une règle NAT parent. L’adresse IP externe est tirée de la règle NAT parent.

Stratégies NAT dynamiques créées automatiquement

Les stratégies NAT dynamiques pour le service Internet sont créées automatiquement dans les cas suivants :

- Configuration du service Internet sur une interface non approuvée (lien WAN).
- Activation de l’accès Internet pour tous les domaines de routage sur un seul lien WAN. Pour plus de détails, consultez la section [Configurer la segmentation du pare-feu](#).
- Configuration des redirecteurs DNS ou du proxy DNS sur SD-WAN. Pour plus de détails, consultez la section [Système de noms de domaine](#).

Surveillance

Pour surveiller le NAT dynamique, accédez à **Surveillance > Statistiques du pare-feu > Connexions**. Pour une connexion, vous pouvez voir si NAT est fait ou non.

DashboardMonitoringConfiguration

StatisticsFlowsRouting ProtocolsFirewallIKE/SecIGMPPerformance ReportsQos ReportsUsage ReportsAvailability ReportsAppliance ReportsDHCP Server/RelayVRRPPPPoEDNS

Monitoring > Firewall

Firewall Statistics

Statistics:ConnectionsMaximum entries to display:50Filtering:Application:AnyFamily:AnyIP Protocol:AnySource Zone:AnyDestination Zone:AnySource Service Type:AnySource Service Instance:AnySource IP:AnySource Port:AnyDestination Service Type:AnyDestination Service Instance:AnyDestination IP:AnyDestination Port:AnyRefreshClear ConnectionsHelp

Connections

Application	Family	IP Protocol	Source				Destination				State	Is NAT	Sent							
			IP Address	Port	Service Type	Zone	IP Address	Port	Service Type	Zone			Packets	Bytes	PPS	kpps				
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	34202	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	140	0.008	0.004	2	4
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	42261	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	140	0.008	0.004	2	4
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	34058	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	114	0.008	0.004	2	1
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	50486	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	114	0.008	0.004	2	1
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	33928	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	124	0.008	0.004	2	1
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	50354	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	124	0.008	0.004	2	1

Pour afficher plus en détail le mappage de l’adresse IP interne vers l’adresse IP externe, cliquez sur **NAT pré-itinéraire** ou **NAT post-route** sous **Objets associés** ou accédez à **Surveillance > Statistiques du pare-feu > Stratégies NAT**.

La capture d’écran suivante montre les statistiques de la règle NAT dynamique de type symétrique et de sa règle de transfert de port correspondante.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any

Service Type: Any Service Name: Any

Inside IP: * Inside Port: * Outside IP: * Outside Port: *

Refresh

Show latest data.

Help

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside IP Address	Port	Outside IP Address	Port	Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
1	Dynamic Sym	-	Outbound	*	Internet	-	*	*	172.147.12.83/32	*	No	No	No	0	0	0	0	0	0
2	Port Forward	1	Outbound	*	Internet	-	172.147.90.12/32	5001-5010	172.147.12.83/32	5001-5010	No	No	No	82	47232	8928	13374144	0	

NAT Policies Displayed: 2
NAT Policies In Use: 2/1000
Port Restricted Dynamic NAT Policies In Use: 0/100
Destination NAT Policies In Use: 0/100

Lorsqu’une règle de transfert de port est créée, une règle de pare-feu correspondante est également créée.

Site: Branch1 + Site ID Site Site

Connections

WAN-to-WAN Forwarding

Virtual Paths

Dynamic Virtual Paths

Internet Service

Intranet Services

WAN Links

GRE Tunnels

IPsec Tunnels

Firewall

Application Routes

Routes

OSPF

BCP

Route Learning Properties

Inter Routing Domain Services

Multicast Groups

Applications

Pre-Appliance Template Policies

Local Policies + Add

Priority	Routing Domain	Action	From	To	Application	Application Family	Application Objects	IP Protocol	DSCP	Service	IP Address	Port	Match Edit	Add Reverse Policy	Info	Edit	Delete	Clone
(auto)	*	Allow	*	*	*	*	*	Any	*	IP Host	*	*	*	*				
(auto)	*	Allow	Internet_Zone	*	*	*	*	Any	*	Internet	*	*	*	Yes				
(auto)	*	Allow	Internet_Zone	*	*	*	*	TCP (6)	*	Internet	*	0-65535	*	15.15.15.1	443			
(auto)	*	Allow	Internet_Zone	*	*	*	*	UDP (17)	*	Internet	*	0-65535	*	15.15.15.1	443			
(auto)	*	Drop	*	*	*	*	*	Any	*	Internet	*	*	*	*				

Post-Appliance Template Policies

Apply Refresh

Vous pouvez afficher les statistiques de stratégie de filtrage en accédant à **Surveillance > Statistiques du pare-feu > Stratégies de filtrage**.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics: Filter Policies

Maximum entries to display: 50

Filtering: Routing Domain: Any Application: Any Family: Any IP Protocol: Any

Filter Policy Action: Any Source Service Type: Any Source Service Name: Any Source IP: *

Source Port: * Destination Service Type: Any Destination Service Name: Any Destination IP: *

Destination Port: * Source Zone: Any Destination Zone: Any DSCP: Any

Refresh

Show latest data.

Help

Filter Policies

Default Policy=Allow(Not Tracked) Packets=3414 Bytes=213489

Match In Progress Packets=0 Bytes=0

ID	Routing Domain	Application	Family	IP Protocol	DSCP	Service Type	Service Name	IP Address	Port or ICMP Type	Zone	Service Type	Service Name	IP Address	Port or ICMP Code	Zone	Action	Conn Match Type	Track Connection	Allow Fragments	Log Connection Start	Log Connection End	Packets	Bytes	Related Objects
1	*	*	*	*	*	IPHost	-	*	NA	*	*	*	*	NA	*	Allow	Default	No	Yes	No	No	0	0	
2	*	*	*	*	*	Internet	-	*	NA	Internet_Zone	*	*	*	NA	*	Allow	Established	No	Yes	No	No	0	0	
3	*	*	*	TCP	*	Internet	-	*	*	Internet_Zone	*	*	15.15.15.1/32	443	*	Allow	Default	No	Yes	No	No	0	0	
4	*	*	*	UDP	*	Internet	-	*	*	Internet_Zone	*	*	15.15.15.1/32	443	*	Allow	Default	No	Yes	No	No	0	0	
5	*	*	*	*	*	Internet	-	*	NA	*	*	*	*	NA	*	Drop	Default	No	Yes	No	No	0	0	

Journaux

Vous pouvez afficher les journaux liés à NAT dans les journaux de pare-feu. Pour afficher les journaux pour NAT, créez une stratégie de pare-feu qui correspond à votre stratégie NAT et assurez-vous que la journalisation est activée sur le filtre de pare-feu. Les journaux NAT contiennent les informations suivantes :

- Date et heure
- Domaine de routage
- Protocole IP
- Port source
- Adresse IP source
- Adresse IP traduite
- Port traduit
- Adresse IP de destination
- Port de destination

Edit ? x

Priority: Policy Type: Built-in Firewall ▼

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
gre_zone	<input type="checkbox"/>
Inter Routing Domain Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
gre_zone	<input type="checkbox"/>
Inter Routing Domain Zone	<input type="checkbox"/>

Routing Domain: Any ▼

Traffic Match Type: IP Protocol ▼ IP Protocol: Any ▼ DSCP: Any ▼ ☐ Match Established

Application: Application Family: ▼ Application Objects: Any ▼

Source Service Type: Any ▼ Source Service Name: Any ▼ Source IP: Source Port:

Dest Service Type: Any ▼ Dest Service Name: Any ▼ Dest IP: Dest Port:

Actions

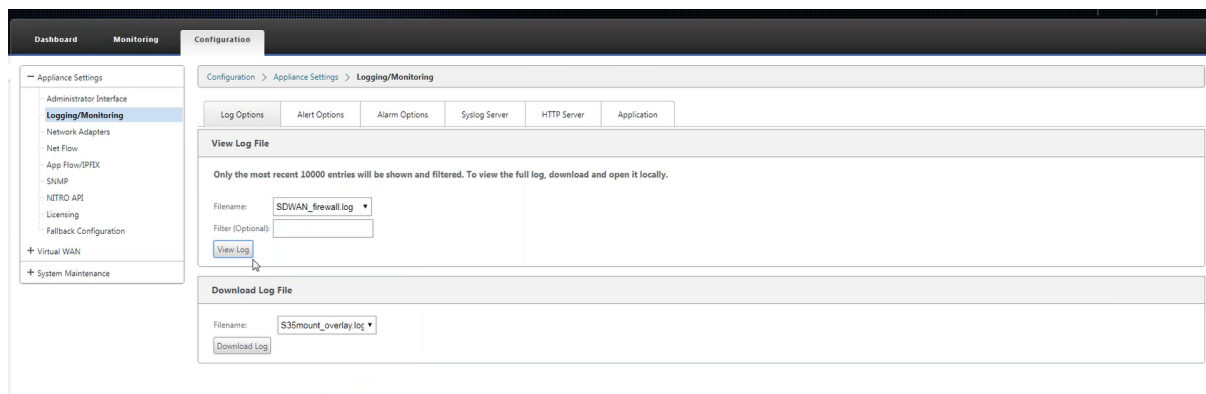
Action: Allow ▼ ☒ Allow Fragments Connection State Tracking: Use Site Setting ▼

Logging & Other Options

Log Interval (s): ☒ Log Start ☒ Log End ☐ Add Reverse Policy

Apply Cancel

Pour générer des journaux NAT, accédez à **Logging/Monitoring > Log Options**, sélectionnez **SDWAN_firewall.log**, puis cliquez sur **View Log**.



Les détails de connexion NAT sont affichés dans le fichier journal.

```
2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/ Firewall Connection Deleted - Removed 3 Connections
2020-05-11T10:15:44.750109+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:20.108292+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112659+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374698+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

Configurer le service WAN virtuel

May 6, 2021

La configuration Citrix SD-WAN décrit et définit la topologie de votre réseau Citrix SD-WAN. Avant de pouvoir déployer un réseau SD-WAN, vous devez définir la configuration du réseau WAN virtuel. Pour ce faire, utilisez l'Éditeur de configuration dans l'Interface Web de gestion Citrix SD-WAN sur l'appli-
ance MCN.

Sécurité et cryptage

L'activation du chiffrement pour SD-WAN (pour les chemins virtuels) est facultative. Les instructions de configuration de cette fonctionnalité sont fournies dans la [Activation et configuration de la sécurité et du chiffrement du réseau étendu virtuel \(facultatif\)](#) section

Lorsque le chiffrement est activé, SD-WAN utilise la norme AES (Advanced Encryption Standard) pour sécuriser le trafic sur le chemin virtuel. Les chiffrements AES 128 bits et 256 bits (tailles de clés) sont

pris en charge par les appliances SD-WAN et sont des options configurables. Vous pouvez sélectionner, activer et configurer ces options ainsi que les autres options de chiffrement à l'aide de l'Éditeur de configuration de l'Interface Web de gestion sur le Node de contrôle de gestion (MCN). Vous devez disposer d'un accès administratif sur le MCN pour modifier la configuration et distribuer vos modifications sur le réseau SD-WAN. Une fois le MCN sécurisé, les paramètres de chiffrement et leur distribution sont également sécurisés.

Authentification entre les fonctions des sites avec la configuration de réseau étendu virtuel.

La configuration réseau dispose d'une clé secrète pour chaque site. Pour chaque chemin virtuel, la configuration réseau génère une clé en combinant les clés secrètes des sites à chaque extrémité du chemin virtuel. L'échange de clés initial qui se produit après la configuration d'un chemin virtuel dépend de la capacité de chiffrer et de déchiffrer les paquets avec cette clé combinée.

Activation du service WAN virtuel

S'il s'agit d'une installation et d'une configuration initiales, vous devez activer manuellement le service Virtual WAN sur chaque appliance SD-WAN de votre réseau. L'activation du service active et démarre le démon virtuel WAN.

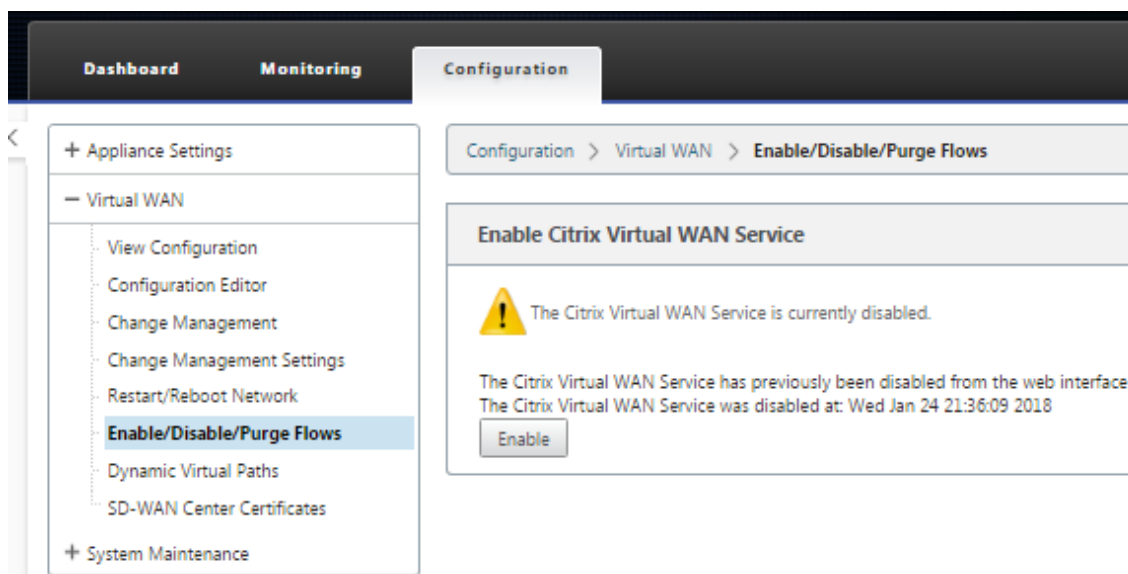
Remarque

Si vous reconfigurez un déploiement existant, le MCN active automatiquement le service lorsqu'il distribue les packages d'appliance mis à jour aux sites clients. Dans ce cas, vous pouvez ignorer cette étape finale.

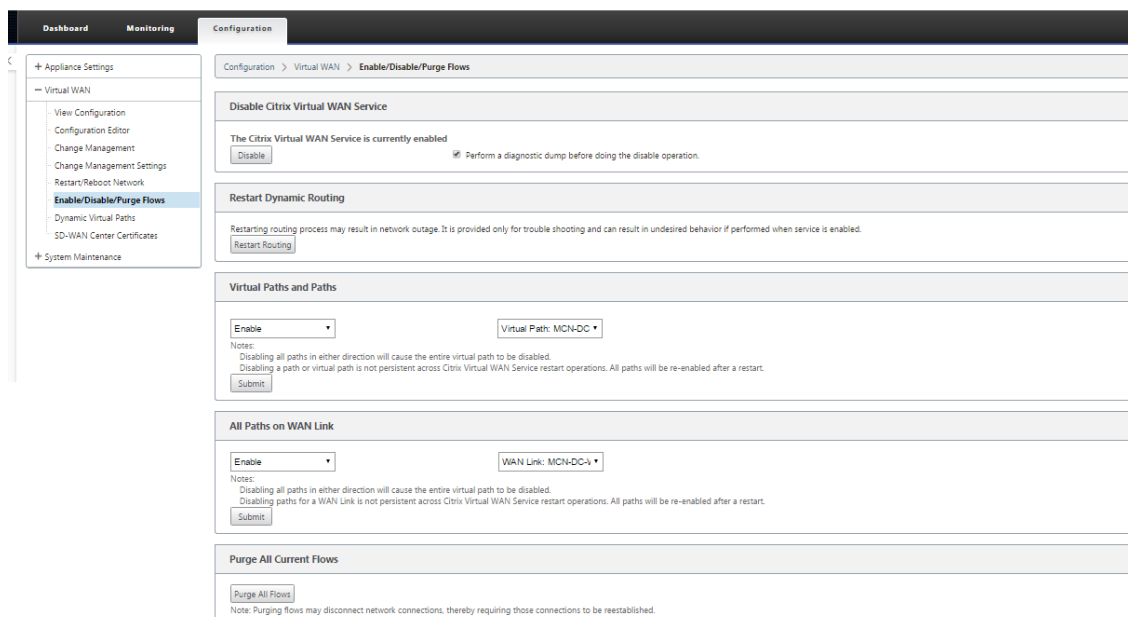
Pour activer manuellement le service Virtual WAN sur une appliance, procédez comme suit :

1. Connectez-vous à l'interface Web de gestion de l'appliance que vous souhaitez activer.
2. Sélectionnez l'onglet **Configuration**.
3. Dans le volet de navigation, ouvrez la branche Virtual WAN et sélectionnez **Activer, désactiver/purger les flux**.

Si le service WAN virtuel est désactivé, la page Activer le service WAN virtuel s'affiche, comme illustré ci-dessous. Si le service est déjà activé, la page Activer, désactiver/purger les flux s'affiche.



4. Cliquez sur **Activer**. Ceci active le service et affiche la page Activer, **désactiver/purger les flux**



Lorsque le service WAN virtuel est activé, un message d'état à cet effet s'affiche dans la section supérieure de la page.

Remarque

Cette page présente également des options pour activer/désactiver des chemins d'accès spécifiques et des chemins d'accès virtuels dans votre réseau, ainsi qu'une option pour purger tous les flux.

L'installation et l'activation du SD-WAN sur le MCN et les appliances clientes du site de succursale

sont terminées. Vous pouvez désormais utiliser les pages Surveillance pour vérifier l'activation et diagnostiquer tout problème de configuration existant ou potentiel.

Configurer la segmentation du pare-feu

May 6, 2021

La segmentation du pare-feu Virtual Route Forwarding (VRF) permet d'accéder à plusieurs domaines de routage à Internet via une interface commune, le trafic de chaque domaine étant isolé de celui des autres. Par exemple, les employés et les invités peuvent accéder à Internet via la même interface, sans aucun accès au trafic de l'autre.

- Accès Internet invité local
- Accès Internet employé et utilisateur pour des applications définies
- Les employés-utilisateurs peuvent continuer à épingler tout autre trafic vers le MCN
- Autoriser l'utilisateur à ajouter des itinéraires spécifiques pour des domaines de routage spécifiques.
- Lorsqu'elle est activée, cette fonctionnalité s'applique à tous les domaines de routage.

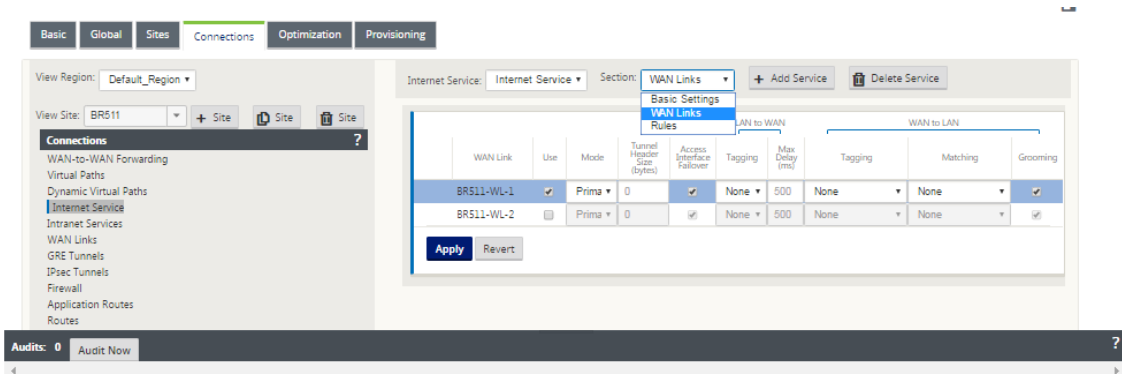
Vous pouvez également créer plusieurs interfaces d'accès pour accueillir des adresses IP publiques distinctes. L'une ou l'autre des options fournit la sécurité nécessaire pour chaque groupe d'utilisateurs.

Remarque

Pour plus d'informations, voir comment [configurer les VRF](#).

Pour configurer les services Internet pour tous les domaines de routage :

1. Créer un service Internet pour un site. Accédez à **Connexions** > **Voir la région** > **Voir le site** > **Nom de site** > **Service Internet** > **Section** > **Liens WAN**, sous Liens WAN, activez la case à cocher **Utiliser**.



Remarque

Vous devriez voir que 0.0.0.0/0 itinéraires ajoutés, un par domaine de routage, sous **Con-nexions > Voir la région > Voir le site >[] > Itinéraires** .

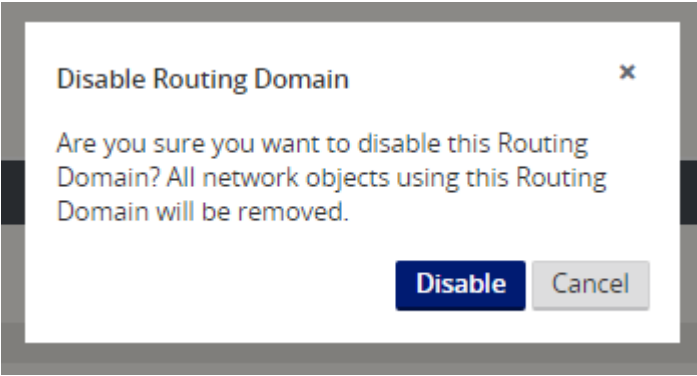
Search:

Order	Network IP Address	Routing Domain	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.200.247.41/24	Default	5	Local			i		
2	10.200.247.42/24	Default	5	Local			i		
3	10.200.247.6/24	Default	5	Local			i		
4	11.123.10.0/24		5	Intranet	Intranet-0		i		
5	11.20.20.11/24	Guest	5	Local			i		
6	12.125.10.0/24		5	Internet			i		
7	0.0.0.0/0	Default	5	Internet			i		
8	0.0.0.0/0	Guest	5	Internet			i		
9	0.0.0.0/0	Default	16	Passthrough			i		
10	0.0.0.0/0	Guest	16	Passthrough			i		

« < 1 > »

Il n'est plus nécessaire que tous les domaines de routage soient activés sur le MCN.

2. Si vous désactivez les domaines de routage sur le MCN, le message suivant s'affiche si les domaines sont utilisés sur un site de succursale :



3. Vous pouvez confirmer que chaque domaine de routage utilise le service Internet en cochant la colonne Domaine de routage dans la table Flux de l'interface de gestion Web sous **Moniteur > Flux** .

Flows List

Toggle Columns

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (ms)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
Guest	11.20.20.20	12.125.10.20	WAN Ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Guest	12.125.10.20	11.20.20.20	WAN Egress	0	19456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

4. Vous pouvez également vérifier la table de routage pour chaque domaine de routage sous **Moniteur > Statistiques > Itinéraires**.

Routes for routing domain: Guest

Filter: in Any column

Show 100 entries Showing 1 to 5 of 5 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static			5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static			5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static			5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static			16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static			16	0	YES	N/A	N/A

Showing 1 to 5 of 5 entries

1

Cas d'utilisation

Dans les versions précédentes de Citrix SD-WAN, le routage et le transfert virtuels présentaient les problèmes suivants, qui ont été résolus.

- Les clients ont plusieurs domaines de routage sur un site de succursale sans avoir à inclure tous les domaines du centre de données (MCN). Ils ont besoin de la capacité d'isoler le trafic des différents clients de manière sécurisée
- Les clients doivent pouvoir disposer d'une seule adresse IP publique accessible avec pare-feu pour plusieurs domaines de routage afin d'accéder à Internet sur un site (au-delà de VRF lite).
- Les clients ont besoin d'un itinéraire Internet pour chaque domaine de routage prenant en charge différents services.
- Plusieurs domaines de routage sur un site de succursale.
- Accès Internet pour différents domaines de routage.

Plusieurs domaines de routage sur un site de succursale

Grâce aux améliorations apportées à la segmentation Virtual Forwarding and Routing Firewall, vous pouvez :

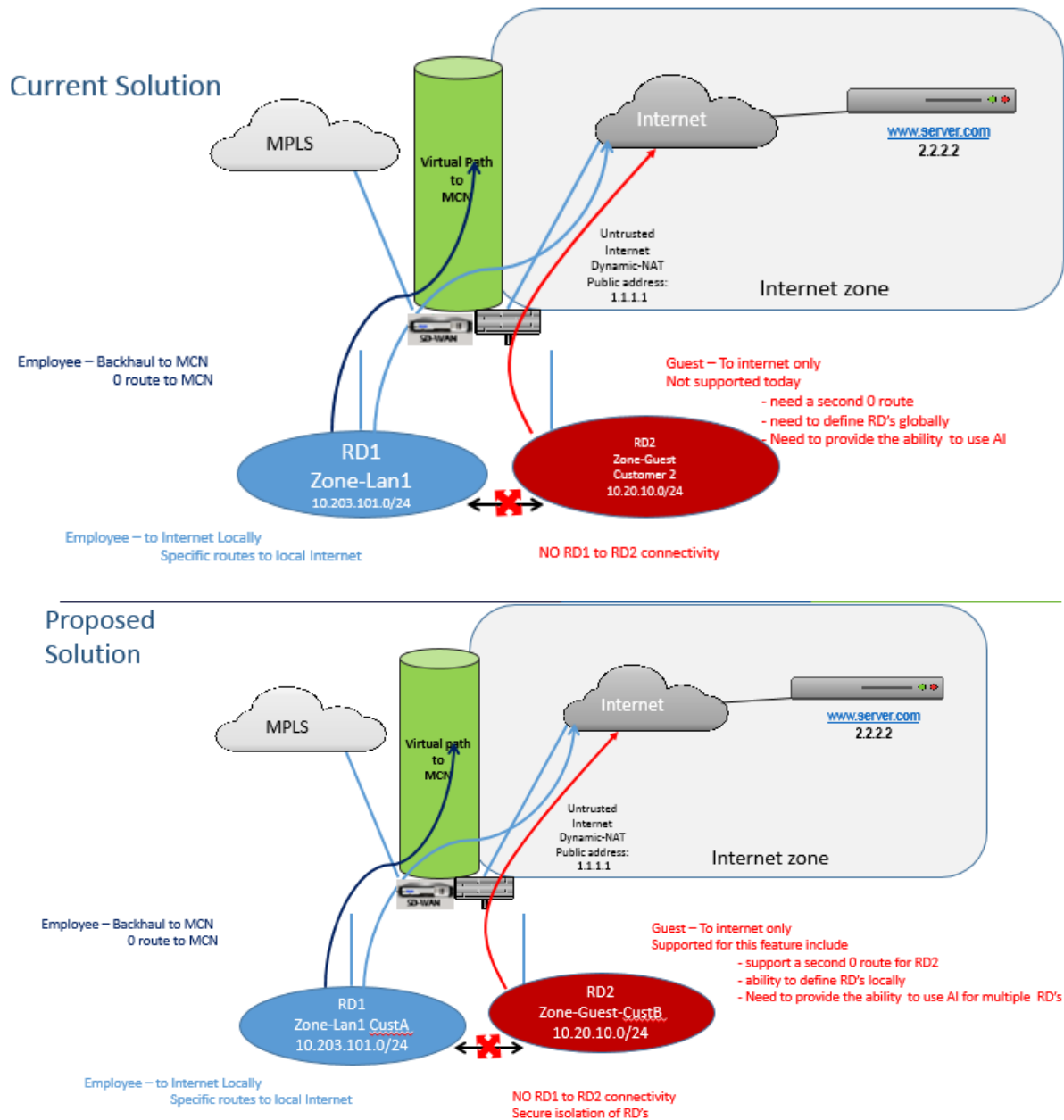
- Fournir une infrastructure, sur le site de la succursale, qui prend en charge une connectivité sécurisée pour au moins deux groupes d'utilisateurs, tels que les employés et les invités. L'infrastructure peut prendre en charge jusqu'à 16 domaines de routage.
- Isolez le trafic de chaque domaine de routage du trafic de tout autre domaine de routage.
- Fournir un accès Internet pour chaque domaine de routage ;
 - Une interface d'accès commune est requise et acceptable
 - Une interface d'accès pour chaque groupe avec des adresses IP publiques distinctes
- Le trafic de l'employé peut être acheminé directement vers l'internet local (applications spécifiques)

- Le trafic de l'employé peut être acheminé ou redirigé vers le MCN pour un filtrage étendu (itinéraire 0)
- Le trafic du domaine de routage peut être acheminé directement vers l'Internet local (itinéraire 0)
- Prend en charge des itinéraires spécifiques par domaine de routage, si nécessaire
- Les domaines de routage sont basés sur un VLAN
- Supprime l'obligation pour le Bureau à distance de résider au MCN
- Le domaine de routage peut désormais être configuré sur un site de succursale uniquement
- Permet d'affecter plusieurs services Bureau à distance à une interface d'accès (une fois activée)
- Chaque Bureau à distance se voit attribuer un itinéraire 0.0.0.0
- Permet d'ajouter des itinéraires spécifiques pour une Bureau à distance
- Permet au trafic provenant de différents services Bureau à distance de quitter Internet à l'aide de la même interface d'accès
- Permet de configurer une interface d'accès différente pour chaque Bureau à distance
- Doit être des sous-réseaux uniques (les services Bureau à distance sont affectés à un VLAN)
- Chaque Bureau à distance peut utiliser la même zone FW par défaut
- Le trafic est isolé via le domaine de routage
- Les flux sortants ont le Bureau à distance comme composant de l'en-tête de flux. Permet au SD-WAN de mapper les flux de retour pour corriger le domaine de routage.

Conditions préalables pour configurer plusieurs domaines de routage :

- L'accès Internet est configuré et attribué à une liaison WAN.
- Pare-feu configuré pour NAT et stratégies correctes appliquées.
- Deuxième domaine de routage ajouté globalement.
- Chaque domaine de routage ajouté à un site.
- Dans **Sites** > Nom du site > **Liens WAN** > WL2[nom] > **Interface d'accès**, vérifiez que la case à cocher est disponible et que le service Internet a été correctement défini. Si vous ne pouvez pas cocher la case, le service Internet n'est pas défini ou affecté à une liaison WAN pour le site.

Scénarios de déploiement



Limitations

- Le service Internet doit être ajouté à la liaison WAN avant de pouvoir activer l'accès Internet pour tous les domaines de routage. (Jusqu'à ce que vous le fassiez, la case à cocher pour activer cette option est grisée).

Après avoir activé l'accès Internet pour tous les domaines de routage, ajoutez automatiquement une règle NAT dynamique.

- Jusqu'à 16 domaines de routage par site.
- Interface d'accès (IA) : IA unique par sous-réseau.
- Plusieurs IA nécessitent un VLAN distinct pour chaque IA.
- Si vous disposez de deux domaines de routage sur un site et que vous disposez d'une liaison WAN unique, les deux domaines utilisent la même adresse IP publique.
- Si l'accès Internet à tous les domaines de routage est activé, tous les sites peuvent router vers Internet. (Si un domaine de routage ne nécessite pas d'accès à Internet, vous pouvez utiliser le pare-feu pour bloquer son trafic.)
- Aucune prise en charge du même sous-réseau dans plusieurs domaines de routage.
- Il n'y a pas de fonctionnalité d'audit
- Les liaisons WAN sont partagées pour l'accès à Internet.
- Pas de QOS par domaine de routage ; premier arrivé, premier servi.

Authentification par certificats

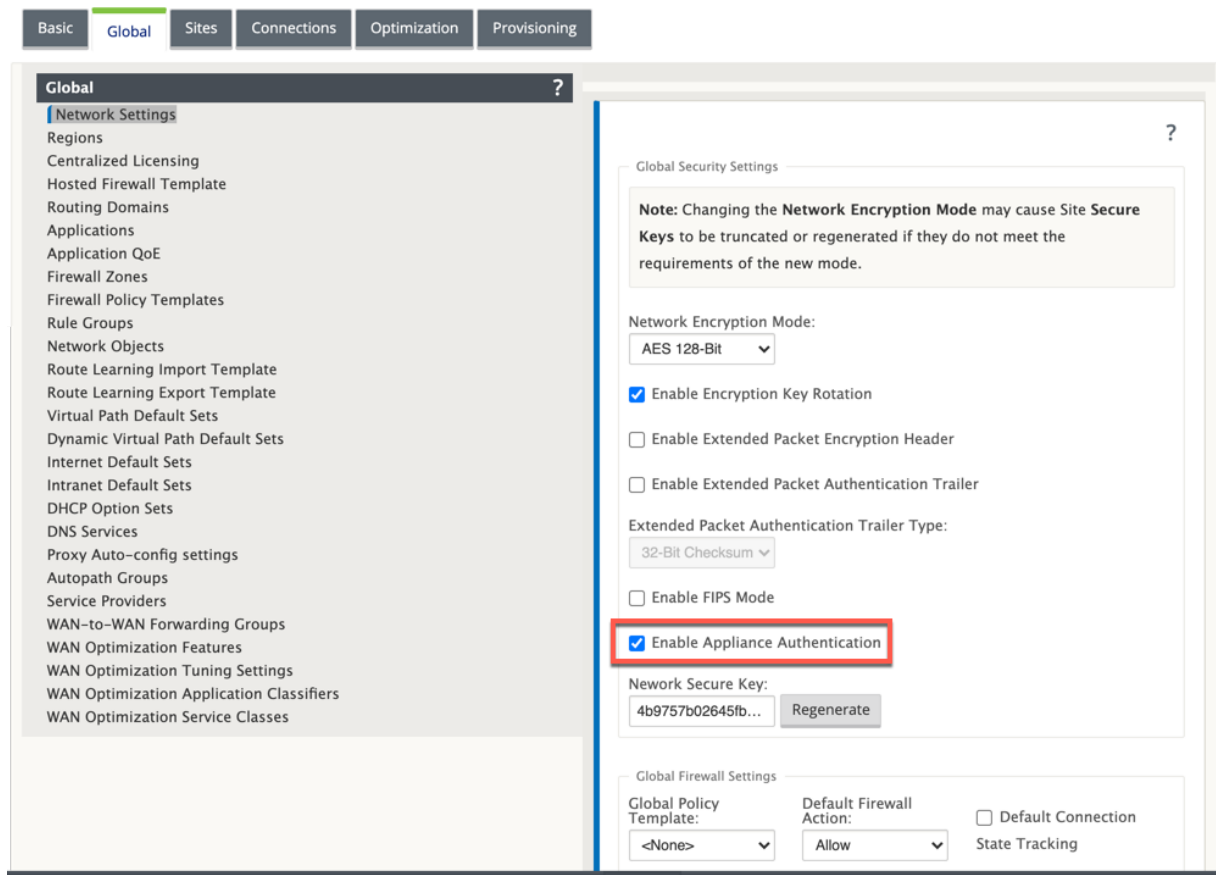
May 6, 2021

Citrix SD-WAN garantit que des chemins sécurisés sont établis entre les appliances du réseau SD-WAN à l'aide de techniques de sécurité telles que le chiffrement du réseau et les tunnels IPsec de chemin virtuel. Outre les mesures de sécurité existantes, l'authentification basée sur les certificats est introduite dans Citrix SD-WAN 11.0.2.

Authentification de certificat, permet aux organisations d'utiliser des certificats émis par leur autorité de certification privée pour authentifier les appliances. Les appliances sont authentifiées avant d'établir les chemins virtuels. Par exemple, si une appliance de succursale tente de se connecter au centre de données et que le certificat de la succursale ne correspond pas au certificat attendu par le centre de données, le chemin d'accès virtuel n'est pas établi.

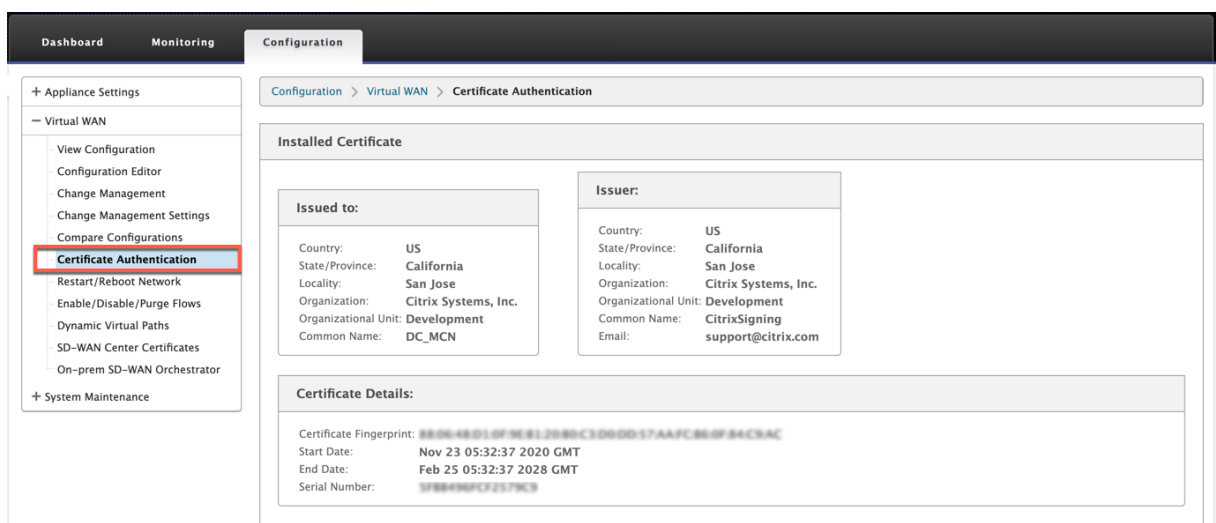
Le certificat émis par l'autorité de certification lie une clé publique au nom de l'appliance. La clé publique fonctionne avec la clé privée correspondante possédée par l'appliance identifiée par le certificat.

Pour activer l'authentification de l'appliance, dans l'éditeur de configuration, accédez à **Global > Paramètres réseau** et sélectionnez **Activer l'authentification de l'appliance**.



Une fois la configuration effectuée et appliquée, une nouvelle option d'**authentification de certificat** est répertoriée sous **Configuration > Réseau étendu virtuel**.

Vous pouvez gérer tous les certificats utilisés pour l'authentification de chemin d'accès virtuel à partir de la page **Authentification de certificat**.



Remarque

Si vous mettez à niveau le logiciel de l'appliance du SD-WAN version 11.0 vers la version 11.1 ou ultérieure, décochez l'option **Activer l'authentification du matériel** et effectuez la mise à niveau logicielle. Une fois le processus de mise à niveau terminé, sélectionnez l'option **Activer l'authentification du matériel**.

Certificat installé

La section **Certificat installé** fournit un résumé du certificat installé sur l'appliance. L'appliance utilise ce certificat pour s'identifier dans le réseau.

La section **Délivré à** fournit des détails sur les personnes auxquelles le certificat a été délivré. Le **nom commun** du certificat correspond au nom de l'appliance, car le certificat est lié au nom de l'appliance. La section **Émetteur** fournit les détails de l'autorité de signature du certificat, qui a signé le certificat. Les détails du certificat incluent l'empreinte digitale du certificat, le numéro de série et la période de validité du certificat.

Installed Certificate	
Issued to:	Issuer:
Country: US	Country: US
State/Province: California	State/Province: California
Locality: San Jose	Locality: San Jose
Organization: Citrix Systems, Inc.	Organization: Citrix Systems, Inc.
Organizational Unit: Development	Organizational Unit: Development
Common Name: DC	Common Name: CitrixSigning
	Email: support@citrix.com
Certificate Details:	
Certificate Fingerprint: [REDACTED]	
Start Date:	Aug 13 13:45:47 2019 GMT
End Date:	Aug 10 13:45:47 2029 GMT
Serial Number:	[REDACTED]

Charger le bundle d'identité

Le bundle Identity inclut une clé privée et le certificat associé à la clé privée. Vous pouvez télécharger le certificat de l'appliance émis par l'autorité de certification dans l'appliance. Le bundle de certificats est un fichier PKCS 12, avec l'extension .p12. Vous pouvez choisir de le protéger avec un mot de passe. Si vous laissez le champ de mot de passe vide, il est traité comme aucune protection par mot de passe.

Upload Identity Bundle (PKCS12)	
File:	C:\ID\SD-WAN\11.0.2\S Browse...
Password:
<input type="button" value="Upload Identity Bundle"/>	

Télécharger le lot d'autorité de certification

Chargez l'ensemble PKCS 12 correspondant à l'autorité de signature de certificat. Le bundle d'autorité de certification comprend la chaîne complète de signatures, la racine et toute l'autorité signataire intermédiaire.

Upload Certificate Authority Bundle (PKCS12)	
File:	C:\ID\SD-WAN\11.0.2\S Browse...
<input type="button" value="Upload CA Bundle"/>	

Upload Network Certificates (PEM)	
File:	C:\ID\SD-WAN\11.0.2\S Browse...
<input type="button" value="Upload Network Bundle"/>	

Créer une demande de signature de certification

L'appliance peut générer une certification non signée et créer une demande de signature de certificat (CSR). L'autorité de certification peut ensuite télécharger le CSR à partir de l'appliance, le signer et le télécharger à nouveau au format PEM ou DER. Il est utilisé comme certificat d'identité pour l'appliance. Pour créer un CSR pour une appliance, indiquez le nom commun, les détails de l'organisation et l'adresse de l'appliance.

Create Certificate Signing Request (CSR)			
Common Name:	<input type="text" value="DC"/>	Business name / Organization:	<input type="text" value="Citrix"/>
Department Name / Organizational Unit:	<input type="text" value="Networks"/>	Town / City:	<input type="text" value="New York"/>
Province, Region, County or State:	<input type="text" value="USA"/>	Country:	<input type="text" value="US"/>
Email address:	<input type="text" value="johndoe@citrix"/>		
<input type="button" value="Create CSR"/>			

Gestionnaire de liste de révocation de certificats

Une liste de révocation de certificats (CRL) est une liste publiée de numéros de série de certificats qui ne sont plus valides sur le réseau. Le fichier CRL est régulièrement téléchargé et stocké localement

sur toute l'appliance. Lorsqu'un certificat est authentifié, le répondeur examine la liste de révocation pour voir si le certificat d'initiateurs a déjà été révoqué. Citrix SD-WAN prend actuellement en charge les LCR version 1 au format PEM et DER.

Pour activer la liste de révocation de révocation de révocation de révocation, sélectionnez l'option Indiquez l'emplacement où le fichier CRL est conservé. Les emplacements HTTP, HTTPS et FTP sont pris en charge. Spécifiez l'intervalle de temps pour vérifier et télécharger le fichier CRL, la plage est de 1 à 1440 minutes.

Certificate Revocation List Management (CRL)	
CRL Enabled:	<input checked="" type="checkbox"/>
CRL URI:	<input type="text" value="https://[redacted]/signingc"/>
CRL Update Interval (Minutes):	<input type="text" value="10"/>
<input type="button" value="Update Settings"/>	

Remarque

La période de réauthentification pour un chemin virtuel peut être comprise entre 10 et 15 minutes. Si l'intervalle de mise à jour de la liste de révocation de certificats est défini sur une durée plus courte, la liste de révocation de certificats mise à jour peut inclure un numéro de série actuellement actif. Rendre un certificat révoqué activement disponible sur votre réseau pour une courte durée.

AppFlow et IPFIX

September 26, 2023

AppFlow et IPFIX sont des normes d'exportation de flux utilisées pour identifier et collecter des données d'application et de transaction dans l'infrastructure réseau. Ces données offrent une meilleure visibilité sur l'utilisation et les performances du trafic des applications.

Les données collectées, appelées enregistrements de flux, sont transmises à un ou plusieurs collecteurs IPv4 ou IPv6. Les collecteurs regroupent les enregistrements de flux et génèrent des rapports en temps réel ou historiques.

AppFlow

AppFlow exporte les données de niveau de flux pour les connexions HDX/ICA uniquement. Vous pouvez activer le TCP uniquement pour le modèle de jeu de données HDX ou le modèle de jeu de données HDX. Le TCP uniquement pour le jeu de données HDX fournit [données multi-sauts](#). Le jeu de données HDX fournit [Données d'aperçu HDX](#).

Remarque

Le modèle HDX est disponible pour Citrix SD-WAN PE Edition et les appliances à deux boîtes uniquement. Il doit être activé sur l'appliance Data Center.

Les collecteurs AppFlow comme Splunk et Citrix ADM ont des tableaux de bord pour interpréter et présenter ces modèles.

IPFIX

IPFIX est un protocole d'exportation de collecteur utilisé pour exporter des données de niveau de flux pour toutes les connexions. Pour toute connexion, vous pouvez afficher des informations telles que le nombre de paquets, le nombre d'octets, le type de service, la direction de flux, le domaine de routage, le nom d'application, etc. Les flux IPFIX sont transmis via l'interface de gestion. La plupart des collecteurs peuvent recevoir des enregistrements de flux IPFIX, mais peuvent avoir besoin de créer un tableau de bord personnalisé pour interpréter le modèle IPFIX.

Le modèle IPFIX définit l'ordre dans lequel le flux de données doit être interprété. Le collecteur reçoit un enregistrement de modèle, suivi des enregistrements de données. Citrix SD-WAN utilise les modèles 611 et 613 pour exporter les données de flux IPv4 IPFIX, 615 et 616 pour exporter les données de flux IPv6 IPFIX avec le modèle Options 612.

Application Flow Info (IPFIX) exporte des ensembles de données selon les modèles 611 pour les flux IPv4, 615 pour les flux IPv6 et 612 options Modèle avec informations sur l'application.

Les propriétés de base (IPFIX) exportent des ensembles de données selon les modèles 613 pour les flux IPv4 et 616 pour les flux IPv6.

Les tableaux suivants fournissent la liste détaillée des données de flux associées à chaque modèle IPFIX.

Infos sur le flux d'applications (IPFIX) - Modèles V10**ID de modèle - 611**

Info Element (IE)	Nom et ID IE	Type and len	Description
ID du point d'observation	observationPointId, 138	Unsigned32, 4	
ID de processus d'exportation	exportingProcessId, 144	Unsigned32, 4	
ID de flux	flowId, 148	Unsigned64, 8	

Info Element (IE)	Nom et ID IE	Type and len	Description
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Address, 12	Ipv4address, 4	
Ipv4 version	IPVersion, 60	Unsigned8, 1	Set à 4.
IP protocol number	protocolIdentifier, 4	Unsigned8, 1	
Rembourrage	S.O.	Unsigned16, 2	
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Nombre d'octets	octetDeltaCount, 1	Unsigned64, 8	
Temps de la première pkt en microsecondes	flowStartMicroseconds, 154	DateTimeMicroseconds, 8	
Temps de la dernière pkt en microsecondes	FlowendMicroSeconds, 155	DateTimeMicroseconds, 8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Indicateurs de flux	TCPControlBits, 6	Unsigned8, 2	Présentement réglé sur 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow 0x01: les flux Flowwan-WAN et LAN-LAN sont une possibilité dans SDWAN
Interface d'entrée	ingressInterface, 10	Unsigned32, 4	La charge Citrix SD-WAN équilibre les flux de données via plusieurs chemins d'accès de membres. Par conséquent, un flux de données unique peut avoir plusieurs combinaisons d'interface entrée/sortie.

Info Element (IE)	Nom et ID IE	Type and len	Description
Interface de sortie	egressInterface, 14	Unsigned32, 4	La charge Citrix SD-WAN équilibre les flux de données via plusieurs chemins d'accès de membres. Par conséquent, un flux de données unique peut avoir plusieurs combinaisons d'interface entrée/sortie.
ID Vlan d'entrée	vlanId, 58	Unsigned16, 2	
ID Vlan de sortie	postVlanId, 59	Unsigned16, 2	
VRF ID	IngressVRFID, 234	Unsigned32, 4	
Indicateur clé de débit	flowKeyIndicator, 173	Unsigned64, 8	
ID de l'application	applicationId, 95	octetArray, variable	L'ID d'application est identique à celui des applications classées par le moteur DPI. Les ID d'application restent constants. Les ID d'application pour les applications basées sur un nom de domaine personnalisé changent à chaque mise à jour de configuration.

ID de modèle —615 (flux IPv6)	Info Element (IE) IE name & ID Type and len Commentaires
	- - - -
	ID du point d'observation observationPointId, 138 Unsigned32, 4
	ID de processus d'exportation exportingProcessId, 144 Unsigned32, 4
	ID de flux flowId, 148 Unsigned64, 8
	Ipv6 SRC IP sourceIPv6Address, 27 IPv6address, 16
	IP d'heure d'été Ipv6 destinationIPv6Addres, 28 IPv6address, 16

IPversion	IPVersion, 60	Non signée8, 1	Définir à 6	
Numéro de protocole IP	protocoldentificateur, 4	Non signée8, 1		
Padding	N/A	Non signée16, 2		
Port SRC	SourceTransport	Désigné16, 2		
DST	Destination	Transport	Transport	Transport
Pkt compte	PacketDeltaCount, 2	Unsigned64, 8		
Compte d'octetetetetDeltaCount, 1	Unsigned64, 8			Heure pour la première pkt en microsecondes
154	DateTimeMicroseconds, 8			Temps pour lastpkt en microsecondes
155	Temps pour lastpkt en			
microsecondes	FlowendMicrotimseconds, 155	Temps pour lastpkt en microsecondes	FlowendMicrotimseconds,	
155	Temps pour lastpkt en microsecondes	FMicroSecondes, 8		
IP Tos	IPclassofService, 5	Non signée8, 1		
Indicateurs de flot	TCPControlBits, 6	Non signées8, 2	Actuellement réglé sur 0.	
Direction du flux, 61	Non signée8, 1	0x00 :		
entrée flow0x01 : flux flux flux de sortie FlowWan-WAN et LAN-LAN sont une possibilité dans SDWAN				
Interface d'entrée	Interface ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN équilibre la charge	
des flux de données via plusieurs chemins d'accès membres, de sorte qu'un seul flux de données				
peut avoir plusieurs combinaisons d'interfaces d'entrée/sortie.				
Interface de sortie	EgressInterface, 14	Unsigned32, 4	Citrix SD-WAN équilibre la charge des flux de	
données via plusieurs chemins de membres, donc un flux de données unique peut avoir plusieurs				
combinaisons d'interfaces d'entrée/sortie.				
ID VLAN d'entrée	VLANID, 58	Non signée16, 2		
ID VLAN de sortie	PostvlanID, 59	Non signée16, 2		
IDVRF	IngressVrfid, 234	Non signée32, 4		
Indicateur de clé de flot	FlowKeyIndicator, 173	Non signée64, 8	Réglée à 0x1E0 37F.	
ID d'application	ID d'application, 95	OctetArray , variable	L'ID de l'application est identique à l'	
ID des applications classées par le moteur DPI. Les ID d'application restent constants. Les ID d'
application pour les applications basées sur des noms de domaine personnalisés changent à chaque
mise à jour de configuration. |

Modèle 612 (Modèle d'options)

Info Element (IE)	Nom et ID IE	Type	Commentaires
ID de l'application	applicationId, 95	octetArray	L'ID d'application est identique à celui des applications classées par le moteur DPI. Les ID d'application restent constants. Les ID d'application pour les applications basées sur un nom de domaine personnalisé changent à chaque mise à jour de configuration.
Nom de l'application	applicationName, 96	string	Spécifie le nom de l'application propriétaire spécifique de Citrix SDWAN.
Description de l'application	ApplicationDescription, 94	string	Spécifie la description de l'application.

Propriétés de base (IPFIX) —Modèle compatible V9 - Modèle 613 (flux IPv4)

Info Element (IE)	Nom et ID IE	Type and len	Commentaires
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIPv4Address, 12	Ipv4address, 4	
Ipv4 version	IPVersion, 60	Unsigned8, 1	
IP protocol number	protocolIdentifier, 4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow 0x01: les flux Flowwan-WAN et LAN-LAN sont une possibilité dans SDWAN

Info Element (IE)	Nom et ID IE	Type and len	Commentaires
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	DestinationTransport, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Nombre d'octets	octetDeltaCount, 1	Unsigned64, 8	
Interface d'entrée	ingressInterface, 10	Unsigned32, 4	La charge Citrix SD-WAN équilibre les flux de données via plusieurs chemins d'accès de membres. Par conséquent, un flux de données unique peut avoir plusieurs combinaisons d'interface entrée/sortie.
Interface de sortie	egressInterface, 14	Unsigned32, 4	
ID Vlan d'entrée	vlanId, 58	Unsigned16, 2	
ID Vlan de sortie	postVlanId, 59	Unsigned16, 2	

ID de modèle — 616 (flux IPv6) |Info Element (IE)|IE name & ID|Type and len|Commentaires|

| - | - | - | - |

|IPv6 SRC IP|sourceIPv6Address, 27|Ipv6address, 16|

|IP d'heure d'été Ipv6|destinationIpv6Addres, 28|Ipv6address, 16|

|IPversion|IPversion, 60|Non signée8, 1|Définir à 6| |

|Numéro de protocole IP|ProtocolDentificateur, 4|Désigné8, 1| |

|IP Tos|IPclassofService, 5|Non signé8, 1| |

|Direction du flux, 61|Désigné8, 1|0x00 : entrée flow0x01 : les flux Flowwan-wan et LAN-LAN de sortie sont une possibilité dans SDWAN|

|Port

SRC|SourceTransportPort, 7|Non signée16, 2| |Port DestinationTransport, 11|Non signée16, 2| |

|Pkt Count|PacketDeltaCount, 2|Non signée64, 8| |

|Compte d'octet|tetDeltaCount, 1|Non signée64, 8| |Interface d'

entrée|IngressInterface, 10|Non signée32, 4|Citrix SD-WAN charge équilibre les flux de données via plusieurs chemins d'accès membres, de sorte qu'un seul flux de données peut avoir plusieurs combinaisons d'interfaces d'entrée/sortie. |

|Interface de sortie|EgressInterface, 14|Unsigned32, 4|Citrix SD-WAN équilibre la charge des flux de données via plusieurs chemins de membres, donc un flux de données unique peut avoir plusieurs combinaisons d'interfaces d'entrée/sortie. |

|ID VLAN d'entrée|VLANID, 58|Non signée16, 2| |

|ID Vlan de sortie|PostvlanID, 59|Non signée16, 2| |

Limitations

- AppFlow ne prend pas en charge les enregistrements de collecteur et de flux IPv6.
- L'intervalle d'exportation pour le flux net passe de 15 secondes à 60 secondes.
- Les flux AppFlow/IPfix sont transmis via UDP, en cas de perte de connexion, toutes les données ne sont pas retransmises. Si l'intervalle d'exportation est défini sur X minutes, l'appliance stocke uniquement X minutes de données. Qui est retransmis après X minutes de perte de connexion.
- Dans Citrix SD-WAN, version 10 version 2, les paramètres **AppFlow** sont définis en local pour chaque appliance, alors que dans les versions précédentes, il s'agissait d'un paramètre global. Si la version du logiciel SD-WAN est rétrogradée vers l'une des versions précédentes et si AppFlow est configuré sur l'une des appliances, elle sera appliquée globalement à toutes les alliances.

Configuration de AppFlow/IPFix

Vous pouvez configurer AppFlow/IPFIX sur des appliances SD-WAN individuelles ou le configurer sur SD-WAN Center et pousser la configuration à un groupe d'appliances.

Pour configurer AppFlow/IPFIX sur des appliances SD-WAN :

1. Dans l'interface Web Citrix SD-WAN SE/PE, accédez à **Configuration > AppFlow/IPfix**.
2. Cliquez sur **Activer**.

The screenshot displays the 'Configuration' tab in the Citrix SD-WAN management console. The left sidebar shows the 'App Flow/IPFIX' configuration page. The main content area is titled 'AppFlow Host Settings' and includes the following sections:

- AppFlow Host Settings:**
 - ☒ Enable
 - Data Update Interval (minutes):
 - Appflow Data Set:
 - ☒ TCP only for HDX
 - ☐ HDX
- AppFlow / IPFIX Collector 1:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☐ Application Flow Info (IPFIX)
 - ☐ Citrix ADM Citrix ADM user: Password:
- AppFlow / IPFIX Collector 2:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☐ Application Flow Info (IPFIX)
 - ☒ Citrix ADM Citrix ADM user: Password:
- AppFlow / IPFIX Collector 3:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☒ Application Flow Info (IPFIX)
 - ☐ Citrix ADM Citrix ADM user: Password:
- AppFlow / IPFIX Collector 4:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☒ Application Flow Info (IPFIX)
 - ☐ Citrix ADM Citrix ADM user: Password:

3. Dans le champ **Intervalle de mise à jour des données**, spécifiez l'intervalle de temps, en minutes, auquel les rapports de flux sont exportés vers le collecteur AppFlow/IPFIX. L'intervalle maximal est de 10 minutes.
4. Sélectionnez le modèle **jeu de données AppFlow**, vous pouvez choisir l'un des modèles de jeu de données suivants :
 - **TCP uniquement pour HDX (AppFlow)** : modèle de jeu de données AppFlow pour collecter et envoyer des données multi-hop de connexions ICA au collecteur AppFlow.
 - **HDX (AppFlow)** : modèle de jeu de données AppFlow pour collecter et envoyer des données d'aperçu HDX des connexions ICA au collecteur AppFlow.

Remarque

Le modèle **HDX** est disponible uniquement pour les appliances Citrix SD-WAN PE et Two Box.

5. Vous pouvez configurer jusqu'à quatre collecteurs AppFlow/IPFIX. Pour chaque collecteur, spécifiez les paramètres suivants :

- **Adresse IP : Adresse** IP du système de collecteur AppFlow/IPFIX externe.
- **Port** : numéro de port sur lequel le système de collecteur AppFlow/IPFIX externe écoute. La valeur par défaut est 4739. Vous pouvez modifier le numéro de port en fonction du collecteur utilisé.
- **Application Flow Info (IPFIX)** : envoie des enregistrements de flux, conformément aux modèles IPFIX 611, 615 et 612 aux collecteurs IPFIX.
- **Propriétés de base (IPFIX)** : envoie des enregistrements de flux, conformément aux modèles IPFIX 613 et 616 aux collecteurs IPFIX.
- **Citrix ADM** : sélectionnez cette option pour utiliser Citrix ADM comme collecteur AppFlow.

Remarque

- Citrix ADM ne prend actuellement pas en charge la collection IPFIX.
- Citrix ADM ne prend pas en charge les adresses IPv6 pour AppFlow et IPFIX.
- **Utilisateur Citrix ADM** : nom d'utilisateur du collecteur Citrix ADM
- **Mot de passe** : mot de passe du collecteur Citrix ADM.

Le nom d'utilisateur et le mot de passe sont utilisés pour se connecter en toute transparence à Citrix ADM et stocker les données de flux.

6. Cliquez sur **Appliquer les paramètres**.

Pour configurer le collecteur **AppFlow/IPFIX** à l'aide de Citrix SD-WAN Center :

1. Dans l'interface utilisateur de gestion Citrix SD-WAN Center, accédez à **Configuration > Paramètres de l'appliance**.
2. Accédez à la section **AppFlow/IPFIX** et choisissez **Inclure dans le fichier**.
3. Sélectionnez **Activer IPFIX/AppFlow Collection**.

4. Dans le champ **Intervalle de mise à jour des données**, spécifiez l'intervalle de temps, en minutes, auquel les rapports AppFlow sont exportés vers le collecteur AppFlow/IPFIX.
5. Sélectionnez le modèle **jeu de données AppFlow**, vous pouvez choisir l'un des modèles de jeu de données suivants :
 - **TCP uniquement pour HDX** : modèle de jeu de données AppFlow pour collecter et envoyer des données multi-saut de connexions ICA au collecteur AppFlow.
 - **HDX** : modèle de jeu de données AppFlow pour collecter et envoyer des données d'aperçu HDX des connexions ICA au collecteur AppFlow.

Remarque

Le modèle **HDX** est disponible uniquement pour les appliances Citrix SD-WAN PE et Two Box.

6. Vous pouvez configurer jusqu'à quatre collecteurs AppFlow/IPFIX. Pour chaque collecteur, spécifiez les paramètres suivants :
 - **IPFIX/AppFlow Collector** : Adresse IP du système de collecteur AppFlow/IPFIX externe.
 - **Port** : numéro de port sur lequel le système de collecteur AppFlow/IPFIX externe écoute. La valeur par défaut est 4739. Vous pouvez modifier le numéro de port en fonction du collecteur utilisé.
 - **Informations sur le flux d'application** : envoie des enregistrements de flux, conformément aux modèles IPFIX 611, 615 et 612 aux collecteurs IPFIX.
 - **Propriétés de base (IPFIX)** : envoie des enregistrements de flux, conformément aux modèles IPFIX 613 et 616 aux collecteurs IPFIX.
 - **Citrix ADM** : sélectionnez cette option pour utiliser Citrix ADM comme collecteur AppFlow.

Remarque

Citrix ADM ne prend actuellement pas en charge la collection IPFIX.

- **Utilisateur Citrix ADM** : nom d'utilisateur du collecteur Citrix ADM.
- **Mot de passe** : mot de passe du collecteur Citrix ADM.

Le nom d'utilisateur et le mot de passe sont utilisés pour se connecter en toute transparence à Citrix ADM et stocker les données de flux.

7. **Enregistrez** et **exportez** la configuration vers les appliances gérées.

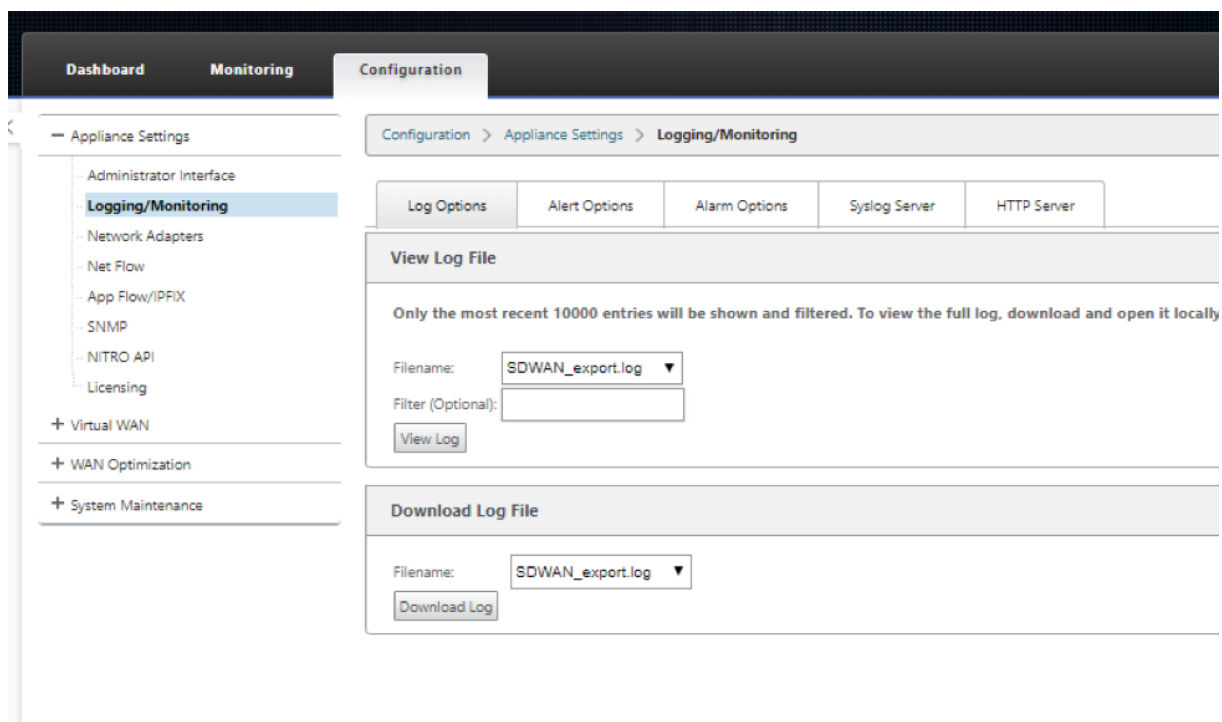
Remarque

Si la version SD-WAN Center est inférieure à 10.2 et si la version des appliances SD-WAN est 10.2 et supérieure, vous pouvez observer les conditions suivantes.

- Si les collecteurs locaux sont activés sur les appliances, la configuration AppFlow/IPFIX poussée à partir de SD-WAN Center n'affecte pas la configuration existante.
- Si les collecteurs locaux ne sont pas activés sur les appliances, la configuration AppFlow/IPfix poussée à partir de SD-WAN Center sera appliquée à l'appliance.
- Si la configuration globale AppFlow/IPfix est activée dans la configuration SD-WAN Center, tous les collecteurs locaux sont activés sur les appliances.

Fichiers journaux

Pour résoudre les problèmes liés aux protocoles d'exportation AppFlow/IPFIX, vous pouvez afficher et télécharger les fichiers SDWAN_export.log. Accédez à **Configuration > Journalisation/Surveillance** et sélectionnez les fichiers **SDWAN_export.log**.



SNMP

November 16, 2022

Citrix SD-WAN prend en charge la fonctionnalité SNMPV1/V2 et un seul compte d'utilisateur pour chaque fonctionnalité SNMPv3. Cette restriction offre les avantages suivants :

- Garantir la conformité SNMPv3 pour les périphériques réseau
- Vérification de la capacité SNMPv3
- Configuration facile de SNMPv3

Pour configurer l'interrogation et les interruptions SNMPv3, accédez à la section SNMPv3 de la page **Configuration -> Paramètres de l'appliance -> SNMP**, puis remplissez les champs requis.

REMARQUE

Pour configurer une adresse IPv6, assurez-vous que le serveur SNMP est également configuré avec une adresse IPv6.

Dashboard

Monitoring

Configuration

<

Appliance Settings

- Administrator Interface
- Logging/Monitoring
- Network Adapters
- Net Flow
- App Flow
- SNMP**
- NITRO API
- Licensing

+ Virtual WAN

+ System Maintenance

Configuration > Appliance Settings > SNMP

Managers

Download MIB File

SNMP

UDP Port: 161

System Description: Citrix Virtual WAN Appliance

System Contact: support@citrix.com

System Location: Citrix

SNMP v1/v2

☐ Enable v1/v2 Agent

Community String: public

☐ Enable v1/v2 Traps

Send v1/v2 Test Trap

Destination IP Address(es):

Port: 162

SNMP v3

☐ Enable v3 Agent

User Name:

Password:

Verify Password:

Authentication: MD5

Encryption: None

☐ Enable v3 Traps

Send v3 Test Trap

Destination IP Address(es):

Port: 162

User Name:

Password:

Verify Password:

Authentication: MD5

Encryption: None

Apply Settings

Prise en charge MIB standard

Les MIB standard suivants sont pris en charge par les appliances SD-WAN.

MIB	RFC (Lien de définition)
DISMAN-EVENT-MIB	https://www.ietf.org/rfc/rfc2981.txt
IF-MIB	https://www.ietf.org/rfc/rfc2863.txt
IP-FORWARD-MIB	https://www.ietf.org/rfc/rfc4292.txt
IP-MIB (partiel)	https://www.ietf.org/rfc/rfc4293.txt
Q-BRIDGE-MIB (Partiel)	http://www.ieee802.org/1/files/public/MIBs/IEEE8021-Q-BRIDGE-MIB-201112120000Z.mib
RFC1213-MIB	https://www.ietf.org/rfc/rfc1213.txt
SNMPv2-MIB	https://www.ietf.org/rfc/rfc3418.txt
TCP-MIB	https://www.ietf.org/rfc/rfc4022.txt
P-BRIDGE-MIB.txt	http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt
RMON2-MIB.txt	https://www.ietf.org/rfc/rfc3273.txt
TOKEN-RING-RMON-MIB.txt	http://www.icir.org/fenner/mibs/extracted/TOKEN-RING-RMON-MIB-rmonmib-01.txt

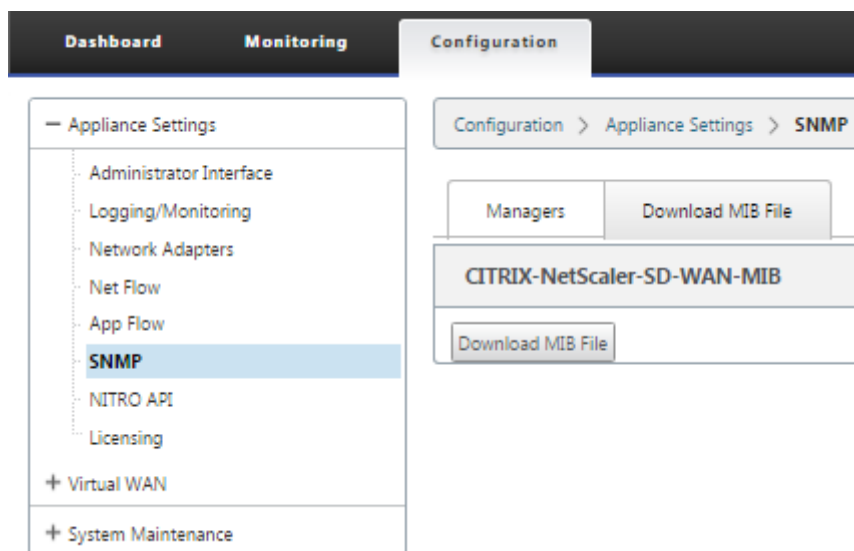
Vous devez télécharger les fichiers SNMP suivants avant de pouvoir commencer à surveiller une appliance Citrix SD-WAN :

- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

Les fichiers MIB sont utilisés par les gestionnaires SNMPv3 et les écouteurs d'interruptions SNMPv3. Les fichiers incluent les MIB d'entreprise de l'appliance SD-WAN, qui fournissent des événements spécifiques au SD-WAN. Pour télécharger les fichiers MIB, dans l'interface de gestion Web SD-WAN :

1. Accédez à **la page Configuration > Paramètres du matériel > SNMP > Télécharger le fichier MIB**.
2. Sélectionnez le fichier **MIB** requis.
3. Cliquez sur **Afficher**.

Le fichier MIB s'ouvre dans le navigateur MIB.



Remarque

- La prise en charge de ces MIB est fournie par défaut par le processus de démon **snmpd net-snmp** sur les systèmes Linux. Les MIB servent de base à la prise en charge des applications de gestion de réseau.
- Les compteurs de paquets et d'octets du port Ethernet se trouvent dans le MIB **IF-MIB** à l'intérieur de la **table IF**. Les informations système se trouvent dans l'objet système.
- Les ports Ethernet sont inclus dans l'**IFTable**, desorte que la marche doit être suffisante pour s'assurer que le sous-système SNMP est en cours d'exécution.
- La prise en charge des **Q-BRIDGE-MIB** et **IP-MIB** permet de prendre en charge l'application de cartographie réseau.

Interface administrative

May 6, 2021

Vous pouvez gérer et maintenir vos appliances Citrix SD-WAN à l'aide des options d'administration suivantes :

- Comptes utilisateur
- Serveur RADIUS
- Serveur TACACS+
- Cert HTTPS
- Paramètres HTTPS
- Divers

Comptes utilisateur

Vous pouvez ajouter de nouveaux comptes d'utilisateurs et gérer les comptes d'utilisateurs existants sous **Configuration > Paramètres du matériel > Page Interface administrateur > onglet Comptes d'utilisateurs**.

Vous pouvez choisir d'authentifier les comptes d'utilisateur nouvellement ajoutés soit localement par l'apppliance SD-WAN, soit à distance. Les comptes d'utilisateur authentifiés à distance sont authentifiés via les serveurs d'authentification RADIUS ou TACACS+.

Rôles des utilisateurs

Les rôles utilisateur suivants sont pris en charge :

- **Visualiseur** : Le compte Viewer est un compte en lecture seule avec accès aux pages **Tableau de bord, Reporting et Monitoring**.
- **Admin** : Le compte d'administrateur dispose des privilèges d'administration et d'un accès en lecture-écriture à toutes les sections.

Un super administrateur (admin) dispose des privilèges suivants :

- Peut exporter la configuration vers la boîte de réception de gestion des modifications pour effectuer une configuration et une mise à jour logicielle sur le réseau.
 - Peut également basculer l'accès en lecture-écriture des administrateurs réseau et de sécurité.
 - Maintient à la fois les paramètres réseau et liés à la sécurité.
- **Administrateur de sécurité** : un administrateur de sécurité dispose d'un accès en lecture-écriture uniquement pour le pare-feu et les paramètres liés à la sécurité dans l'**Éditeur de configuration**, tout en disposant d'un accès en lecture seule aux sections restantes. L'administrateur de sécurité a également la possibilité d'activer ou de désactiver l'accès en écriture au pare-feu pour d'autres utilisateurs à l'exception du super administrateur (admin).
- **Administrateur réseau** : un administrateur réseau dispose d'autorisations en lecture-écriture sur toutes les sections et peut fournir une branche entièrement à l'exception du pare-feu et des

paramètres liés à la sécurité dans l'**Éditeur de configuration**. Le nœud de pare-feu hébergé n'est pas disponible pour l'administrateur réseau. Dans ce cas, l'administrateur réseau doit importer une nouvelle configuration.

L'administrateur réseau et l'administrateur de sécurité peuvent apporter des modifications à la configuration et les déployer sur le réseau.

REMARQUE

L'administrateur réseau et l'administrateur de la sécurité ne peuvent pas ajouter ou supprimer des comptes utilisateur. Ils ne peuvent modifier que leurs propres mots de passe de compte.

The screenshot displays the Citrix SD-WAN VPX-50-SE web interface. The top navigation bar includes the title 'Citrix SD-WAN VPX-50-SE', site name 'MCN_DC-MCN_DC-VPX', IP address '11.3.0.123.888881', and a 'Logout' button. The main menu on the left lists various configuration options under 'Appliance Settings', with 'Administrator Interface' selected. The main content area shows the 'Administrator Interface' configuration page, which includes tabs for 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', 'HTTPS Settings', and 'Miscellaneous'. The 'Change Local User Password' section contains fields for 'User Name' (set to 'admin'), 'Current Password', 'New Password', and 'Confirm New Password', along with a 'Change Password' button. Below this is the 'Delete Workspace For User' section, which includes a 'Delete Selected User's Workspace' button. The 'Manage Users' section features an 'Add User...' button and a 'Delete Selected User' button. The 'Firewall Access' section includes a 'Disable Firewall Access' button.

Ajouter un utilisateur

Pour ajouter un utilisateur, cliquez sur **Ajouter un utilisateur** dans la section **Gérer les utilisateurs**. Indiquez le **nom d'utilisateur et le mot de passe**. Sélectionnez le rôle utilisateur dans la liste déroulante **Niveau utilisateur**, puis cliquez sur **Appliquer**.

Vous pouvez également supprimer un compte utilisateur, si nécessaire. La suppression d'un utilisateur supprime également les fichiers locaux appartenant à cet utilisateur. Pour supprimer, sous la

section **Gérer les utilisateurs**, sélectionnez l'utilisateur dans la liste déroulante **Nom d'utilisateur** et cliquez sur **Supprimer l'utilisateur sélectionné**.



Modifier le mot de passe d'un utilisateur

Le rôle d'administrateur peut modifier le mot de passe d'un compte utilisateur authentifié localement par l'appliance SD-WAN.

Pour modifier le mot de passe, sous la section **Modifier le mot de passe utilisateur local**, sélectionnez l'utilisateur dans la liste déroulante **Nom d'utilisateur**. Entrez le mot de passe actuel et le nouveau mot de passe. Cliquez sur **Modifier le mot de passe**.

Supprimer l'espace de travail pour un utilisateur

Vous pouvez supprimer l'espace de travail **Éditeur de configuration** pour un utilisateur. La suppression de l'espace de travail ne supprime pas le compte d'utilisateur. Il supprime toutes les configurations enregistrées et les cartes réseau pour l'utilisateur sélectionné.

Pour supprimer l'espace de travail d'un utilisateur, sous la section **Supprimer l'espace de travail pour l'utilisateur**, sélectionnez l'utilisateur dans la liste déroulante **Nom d'utilisateur**. Cliquez sur **Supprimer l'espace de travail de l'utilisateur sélectionné**.

Désactiver l'accès au pare-feu

Vous pouvez désactiver l'accès par pare-feu à un compte d'utilisateur. Pour le désactiver, sélectionnez l'utilisateur dans la liste déroulante **Nom d'utilisateur** et cliquez sur **Désactiver l'accès au pare-feu**.

Serveur RADIUS

Vous pouvez configurer une appliance SD-WAN pour authentifier l'accès utilisateur avec un ou trois serveurs RADIUS au maximum. Le port par défaut est 1812.

Pour configurer le serveur RADIUS :

1. Accédez à **Configuration > Paramètres du matériel > Interface Administrateur > RADIUS**.
2. Activez la case à cocher **Activer RADIUS**.
3. Entrez l'**adresse IP du serveur** et le **port d'authentification**. Un maximum de trois adresses IP de serveur peut être configuré.

REMARQUE

Pour configurer une adresse IPv6, assurez-vous que le serveur RADIUS est également configuré avec une adresse IPv6.

4. Entrez la **clé du serveur** et confirmez.
5. Entrez la valeur **Délai** d'attente en secondes.
6. Cliquez sur **Enregistrer**.

Vous pouvez également tester la connexion au serveur RADIUS. Entrez le **nom d'utilisateur et le mot de passe**. Cliquez sur **Vérifier**.

Configuration > Appliance Settings > Administrator Interface

User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous
---------------	---------------	---------	------------	----------------	---------------

RADIUS

Enable RADIUS☒

Server 1 IP Address:

Authentication Port:

Server 2 IP Address (Optional):

Authentication Port:

Server 3 IP Address (Optional):

Authentication Port:

Server Key:

Confirm Server Key:

Timeout (seconds):

(Optional)

Apply

Test RADIUS Server Connection

User Name:

Password:

Verify

Serveur TACACS+

Vous pouvez configurer un serveur TACACS+ pour l'authentification. Comme pour l'authentification RADIUS, TACACS+ utilise une clé secrète, une adresse IP et le numéro de port. Le numéro de port par défaut est 49.

Pour configurer le serveur TACACS+ :

1. Accédez à **Configuration > Paramètres de l'appliance > Interface Administrateur > TACACS+**.
2. Activez la case à cocher **Activer TACACS+**.
3. Entrez l'**adresse IP du serveur** et le **port d'authentification**. Un maximum de trois adresses IP de serveur peut être configuré.

REMARQUE

Pour configurer une adresse IPv6, assurez-vous que le serveur TACACS+ est également configuré avec une adresse IPv6.

4. Sélectionnez **PAP** ou **ASCII** comme Type d'authentification.
 - PAP : utilise le protocole PAP (Password Authentication Protocol) pour renforcer l'authentification des utilisateurs en attribuant un secret partagé fort au serveur TACACS+.
 - ASCII : utilise le jeu de caractères ASCII pour renforcer l'authentification de l'utilisateur en attribuant un secret partagé fort au serveur TACACS+.
5. Entrez la **clé du serveur** et confirmez.
6. Entrez la valeur **Délai** d'attente en secondes.
7. Cliquez sur **Enregistrer**.

Vous pouvez également tester la connexion au serveur TACACS+. Entrez le **nom d'utilisateur et le mot de passe**. Cliquez sur **Vérifier**.

Configuration > Appliance Settings > Administrator Interface

User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous
---------------	--------	---------	------------	----------------	---------------

TACACS+

Enable TACACS+ ☒

Server 1 IP Address: Authentication Port:

Server 2 IP Address (Optional): Authentication Port:

Server 3 IP Address (Optional): Authentication Port:

Authentication Type: ☒ PAP ☐ ASCII

Server Key:

Confirm Server Key:

Timeout (seconds): (Optional)

Test TACACS+ Server Connection

User Name:

Password:

Publicité de routeur NDP et groupe de délégation de préfixe

May 6, 2021

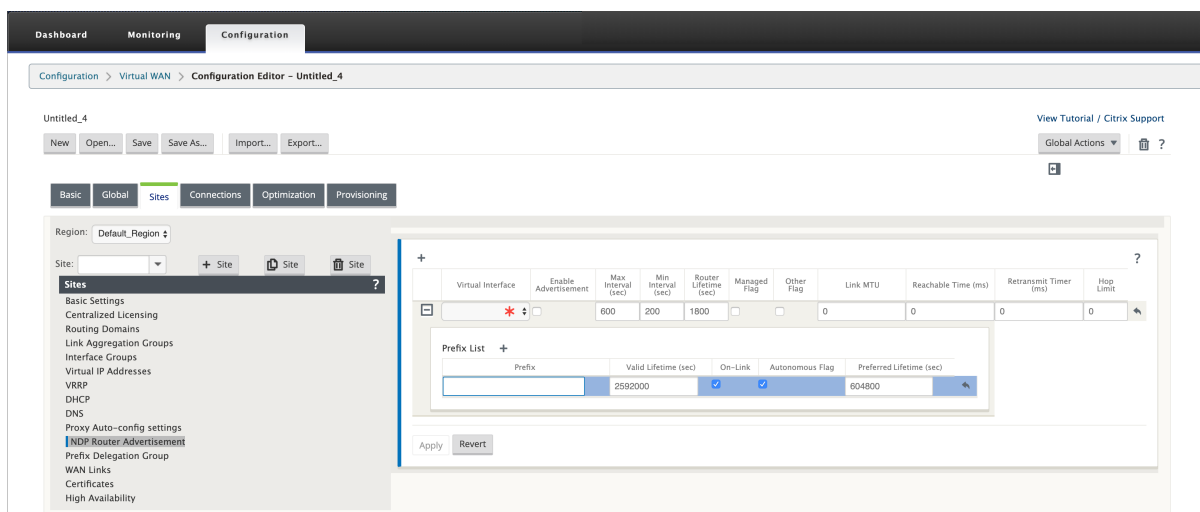
Publicité du routeur NDP

Dans un réseau IPv6, l'appliance SD-WAN multidiffuse périodiquement des messages RA (Router Advertisement) pour annoncer sa disponibilité et transmettre des informations aux appliances voisines du réseau SD-WAN. Les publicités du routeur incluent les informations de préfixe IPv6. Le protocole NDP (NDP) de Neighbor Discovery s'exécutant sur des appliances SD-WAN utilise ces publicités de routeur pour déterminer les périphériques voisins sur la même liaison. Il détermine également les adresses de couche de liaison de l'autre, recherche des voisins et conserve les informations d'accessibilité sur les chemins vers les voisins actifs.

Pour configurer la publicité du routeur NDP,

1. Dans l'Éditeur de configuration, accédez à **Sites > Publicité de routeur NDP**.
2. Cliquez sur **+** et sélectionnez l'une des interfaces virtuelles configurées dans la liste déroulante **Interface virtuelle**.
3. Activez la case à cocher **Activer la publicité** pour activer l'envoi d'annonces périodiques de routeur et la réponse aux sollicitations de routeurs pour l'interface virtuelle sélectionnée.

4. Spécifiez les intervalles de vie maximum, minimum et de durée de vie du routeur.
 - **Intervalle maximal** : Durée maximale (en secondes) autorisée entre l'envoi périodique de publicités de routeur multidiffusion non sollicitées.
 - **Intervalle min** : Temps minimum (en secondes) autorisé entre l'envoi d'annonces périodiques non sollicitées de routeurs multidiffusion.
 - **Durée de vie du routeur : durée**(en secondes) pendant laquelle le routeur est considéré comme valide par les hôtes. 0 indique que le routeur ne peut pas être utilisé comme routeur par défaut.
5. Activez la case à cocher **Indicateur géré** si les adresses IP sont disponibles via le protocole DHCPv6.
6. Activez la case à cocher **Autre indicateur** si les informations de configuration (autres que les adresses IP) sont disponibles via le protocole DHCPv6.
7. Spécifiez les valeurs suivantes pour l'interface sélectionnée.
 - **Link MTU** : Unité de transmission maximale (MTU) recommandée pour l'interface.
 - **Temps d'accès** : le temps (en millisecondes) pendant lequel le protocole NDP reste à l'état **Reachable**.
 - **Minuterie de retransmission** : Temps (en millisecondes) entre la retransmission des messages de sollicitation de voisin lors de la résolution d'une adresse IP ou de l'exploration d'un voisin.
 - **Limite de saut** : nombre maximal de sauts à inclure dans la publicité du routeur.
8. Entrez les détails associés au préfixe.
 - **Préfixe** : longueur du préfixe et du préfixe dans la notation CIDR (Classless Inter-Domain Routing).
 - **Durée de vie valide : Durée** en secondes jusqu'à laquelle le préfixe est valide. -1 représente l'infini, ce qui signifie que le préfixe reste pour toujours.
 - **On-link** : lorsqu'il est sélectionné, le préfixe est considéré comme local pour le réseau.
 - **Indicateur autonome** : lorsqu'il est activé, le préfixe est utilisé par la configuration automatique d'adresse sans état (SLAAC) de l'hôte pour générer l'adresse IP.
 - **Durée de vie du préfixe : Durée**(en secondes) jusqu'à laquelle le préfixe est considéré comme préféré.
9. Cliquez sur **Appliquer**.
10. Pour configurer plus d'interfaces virtuelles pour la publicité de routeur NDP, cliquez sur **+**.



Groupe de délégation de préfixe

REMARQUE

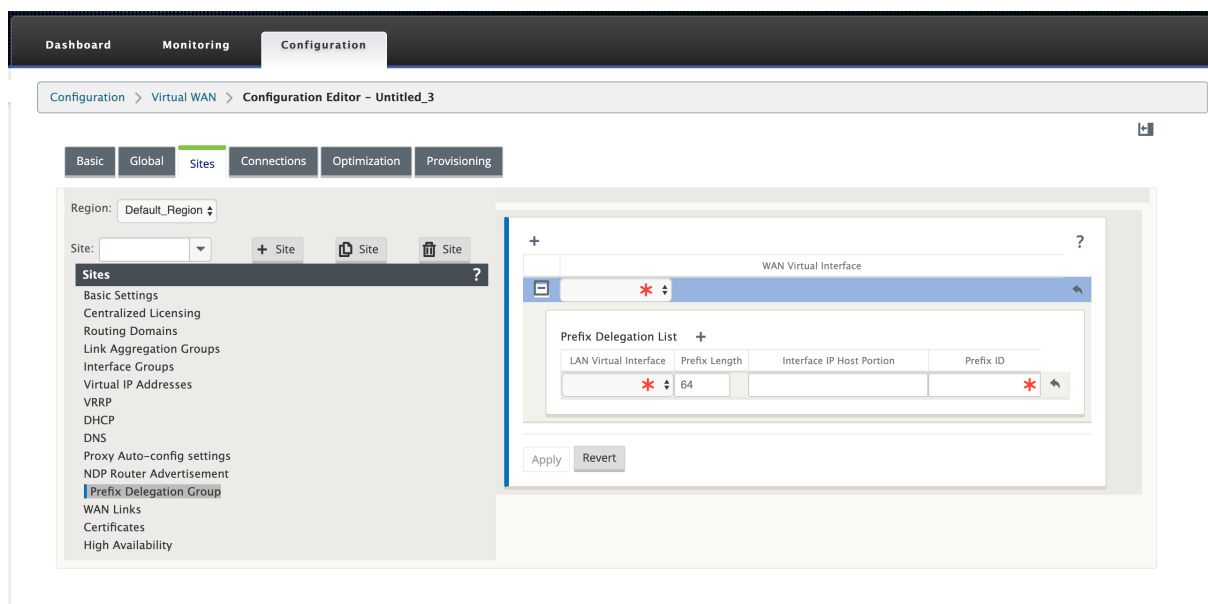
La délégation de préfixe n'est pas prise en charge dans Citrix SD-WAN 11.3 version.

Les appliances Citrix SD-WAN peuvent être configurées en tant que client DHCPv6 pour demander un préfixe au fournisseur de services Internet à l'aide du port WAN configuré. Une fois que l'appliance Citrix SD-WAN reçoit le préfixe, elle utilise le préfixe pour créer un pool d'adresses IP pour répondre aux clients LAN. L'appliance Citrix SD-WAN se comporte ensuite comme un serveur DHCP et annonce le préfixe sur les ports LAN aux clients côté LAN.

Pour configurer la délégation de préfixe,

1. Dans l'Éditeur de configuration, accédez à **Sites > Groupe de délégation de préfixe**.
2. Cliquez sur **+** et choisissez une interface virtuelle WAN configurée sur laquelle le préfixe est demandé au fournisseur de services Internet.
3. Fournissez les détails suivants :
 - **Interface virtuelle LAN** : sélectionnez l'une des interfaces virtuelles LAN configurées pour lesquelles le préfixe est demandé.
 - **Longueur du préfixe** : nombre de bits d'une adresse IPv6 monodiffusion globale qui font partie du préfixe.
 - **Interface IP Host Portion** : Partie hôte à utiliser pour l'adresse IP de l'interface.
 - **ID de préfixe** : identifiant unique permettant d'identifier les demandes de délégation de préfixe pour l'interface LAN.
4. Cliquez sur **Appliquer**.

5. Pour configurer plus d'interfaces virtuelles WAN dans le cadre du groupe de délégation de préfixe, cliquez sur +.



Optimisation WAN

May 6, 2021

L'appliance Citrix SD-WAN WANOP optimise les liaisons WAN, garantissant une réactivité et un débit maximaux. Les appliances Citrix SD-WAN WANOP fonctionnent par paires, une à chaque extrémité d'une liaison, pour accélérer le trafic sur la liaison. Voici quelques-unes des fonctionnalités de Citrix SD-WAN WANOP-

- Compression SSL
- Accélération du protocole TCP
- Gestion du trafic
- Accélération des applications
- Accélération Citrix XenApp/XenDesktop (HDX)
- Intégration
- Suivi et gestion

Pour plus d'informations sur l'installation, le déploiement et la configuration des fonctionnalités de Citrix SD-WAN WANOP 10.2, reportez-vous à la [Citrix SD-WAN WANOP documentation](#). Les fonctionnal-

ités et procédures de Citrix SD-WAN WANOP 10.2 sont similaires aux procédures documentées dans la version WANOP SD-WAN Citrix.

Vous pouvez activer et configurer la fonctionnalité d'optimisation WAN sur votre Citrix SD-WAN Premium Edition. Pour plus d'informations, consultez Citrix SD-WAN [Édition Premium](#).

Vous pouvez accélérer le réseau sur n'importe quel ordinateur portable Windows distant ou station de travail à l'aide du logiciel WANOP Client Plug-in. Pour plus d'informations, reportez-vous à la section [Plug-in client WANOP](#).

Citrix SD-WAN édition premium

May 6, 2021

La section fournit des instructions étape par étape pour activer et configurer les fonctionnalités d'optimisation WAN SD-WAN Premium (Enterprise) Edition pour votre réseau WAN virtuel. Pour ce faire, vous utilisez les formulaires de section **Optimisation** dans l'**Éditeur de configuration** dans l'Interface de gestion Web sur le MCN.

Remarque

Vous devez disposer d'une licence SD-WAN Premium (Enterprise) Edition installée pour accéder, activer, configurer et activer les fonctionnalités d'optimisation WAN dans votre réseau WAN virtuel. SD-WAN Standard Edition ne prend pas en charge ces fonctionnalités.

Il existe deux étapes de niveau supérieur pour configurer les jeux et paramètres **de la section Optimisation**. Ceux-ci sont les suivants, énumérés par ordre de dépendance :

1. Activez l'optimisation WAN et personnalisez la configuration **par défaut**, ou acceptez les valeurs par défaut.

La configuration **par défaut** est utilisée comme configuration d'**optimisation** de base pour tous les sites éligibles à l'optimisation WAN. La configuration **par défaut** est préconfigurée et peut être personnalisée.

Remarque

Pour obtenir des instructions, reportez-vous à la section [Activation de l'optimisation et configuration des paramètres par défaut](#).

2. (Facultatif) Personnalisez la configuration d'optimisation WAN pour chacun des sites de branche individuels ou acceptez **les jeux et paramètres par défaut pour chacun**.

Par défaut, la configuration **par défaut** est initialement appliquée à chaque site de succursale éligible à l'optimisation WAN. L'optimisation WAN est prise en charge uniquement pour les appliances matérielles 1000-EE (édition premium) et 2000-EE (édition premium). Pour chaque site de succursale pris en charge, vous pouvez choisir d'accepter ou de modifier n'importe quelle combinaison **des ensembles et paramètres par défaut**, ou tout sous-ensemble de ceux-ci. Pour obtenir des instructions, veuillez consulter la section [Configuration de l'optimisation pour un site de succursale](#).

Pour effectuer ces étapes, vous utilisez les formulaires de configuration de la section **Optimisation** de l'Éditeur de **configuration**. La section **Optimisation** est organisée comme suit :

- **Valeurs par défaut**** : la branche par défaut contient les succursales enfants suivantes, qui à leur tour contiennent un ou plusieurs formulaires pour configurer leurs ensembles et paramètres respectifs :
 - **Fonctionnalités par défaut**
 - **Paramètres de réglage par défaut**
 - **Valeurs par défaut Classificateurs d'applications (jeu)**
 - **Classes de service par défaut (jeu)**
- ****<Client Site Name>—L'arborescence de configuration **de la section Optimisation** contient une succursale pour chaque nœud client (site de succursale) qui prend en charge l'optimisation WAN. Si un nœud client est un modèle d'appliance non pris en charge, le site ne sera pas inclus dans l'arborescence de configuration **de la section Optimisation**. Chaque branche de l'arborescence contient les succursales enfants suivantes, qui à leur tour contiennent un ou plusieurs formulaires pour configurer leurs ensembles et paramètres respectifs :
 - **Fonctionnalités par défaut**
 - **Paramètres de réglage par défaut**
 - **Classificateurs d'applications par défaut (jeu)**
 - **Classes de service par défaut (jeu)**

La section suivante fournit des instructions pour activer l'optimisation WAN pour votre réseau WAN virtuel et configurer **les ensembles et paramètres par défaut**.

Activer l'optimisation et configurer les paramètres de fonctionnalité par défaut

May 6, 2021

L'activation de l'optimisation WAN dans votre réseau WAN virtuel implique les procédures suivantes :

1. Activez l'optimisation WAN dans les paramètres **Fonctionnalités** de la **section Optimisation**.
Les instructions relatives à cette partie du processus sont fournies dans cette section.
2. Configurez le paramètre de stratégie **Accélération** pour chaque classe de service applicable dans le tableau **Classes de service**.

Cette procédure se produit plus loin, une fois que vous avez terminé le reste de la configuration **d'optimisation**. Les instructions sont fournies dans la section [Configuration des classes de service par défaut d'optimisation](#). À ce stade, l'optimisation WAN a été activée dans votre configuration, mais pas encore activée et activée dans votre réseau WAN virtuel. Pour activer et activer l'optimisation WAN dans votre réseau WAN virtuel, vous devez terminer la configuration du réseau WAN virtuel, puis générer, préparer le déploiement et activer les packages d'appli-ance WAN virtuel sur les sites éligibles de votre déploiement, comme indiqué dans les chapitres suivants de ce guide.

Pour activer l'optimisation WAN et configurer les paramètres des **fonctionnalités** de la section Paramètres **par défaut**, procédez comme suit :

- a) Si nécessaire, reconnectez-vous à l'interface Web de gestion et ouvrez l'**éditeur de configuration**.

Pour ouvrir l'**Éditeur de configuration**, procédez comme suit :

- i. Sélectionnez l'onglet **Configuration** en haut de la page pour ouvrir l'arborescence **de navigation Configuration** (volet gauche).
- ii. Dans l'arborescence de navigation, cliquez sur **+** à gauche de la succursale **Virtual WAN** pour ouvrir cette branche.
- iii. Dans la branche **Virtual WAN**, sélectionnez **Éditeur de configuration**.

- b) Ouvrez le package de configuration que vous souhaitez modifier.

Cliquez sur **Ouvrir** pour afficher la boîte de dialogue **Ouvrir le package de configuration**, puis sélectionnez le package dans le menu déroulant **Packages enregistrés**.

Cela charge le package sélectionné dans l'**éditeur de configuration** et l'ouvre pour modification.

Si vous disposez d'une licence valide et actuelle qui inclut des fonctionnalités d'optimisation WAN, la section **Optimisation** est disponible dans l'**Éditeur de configuration**.

Remarque

Si la section **Optimisation** n'est pas disponible, vérifiez que vous avez installé une licence SD-WAN Premium (Enterprise) Edition dans votre réseau WAN virtuel. SD-WAN Standard Edition ne prend pas en charge les fonctionnalités d'optimisation WAN.

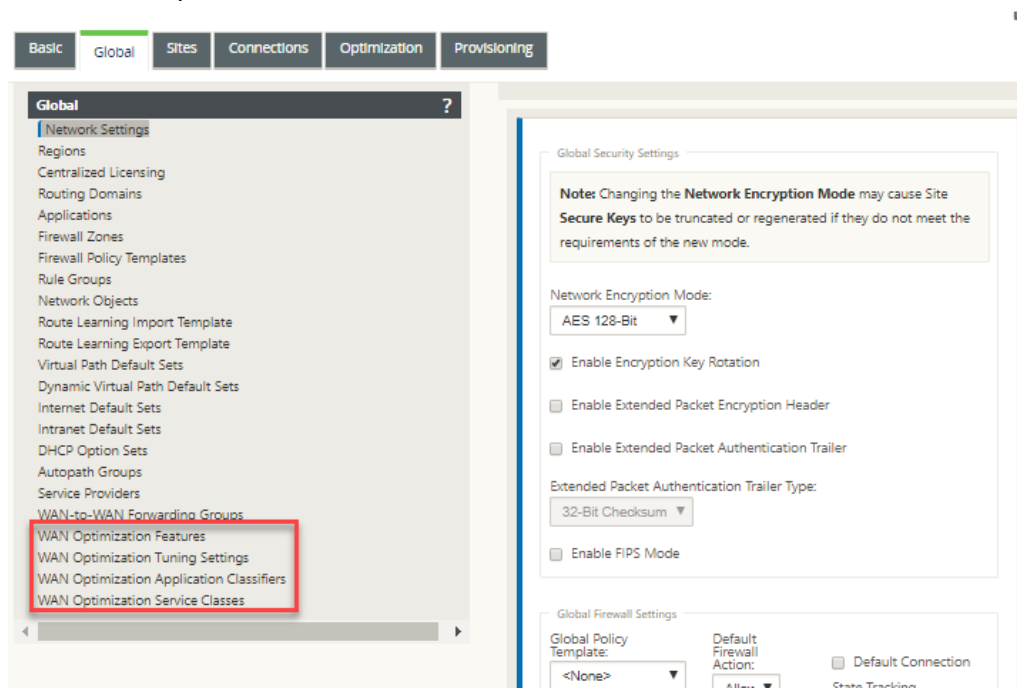
Pour plus de détails et d'instructions, consultez les sections suivantes :

- [Les éditions SD-WAN](#)
- [Système de licences](#)

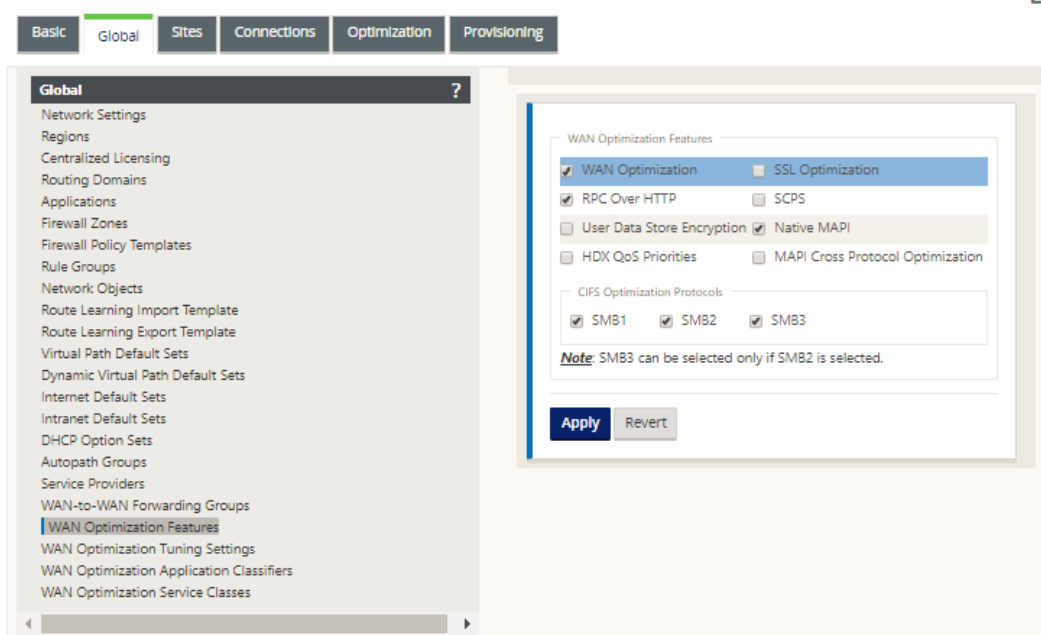
c) Cliquez sur l'onglet **Global**.

Vous pouvez configurer les paramètres par défaut suivants pour l'optimisation WAN à partir de l'onglet **Global**.

- Fonctionnalités d'optimisation WAN
- Paramètres de réglage de l'optimisation WAN
- Classificateurs d'applications d'optimisation WAN
- Classe de service d'optimisation WAN



d) Cliquez sur **Fonctionnalités d'optimisation WAN**.



- e) Activez la case à cocher **Optimisation WAN**.

La case à cocher **Optimisation WAN** se trouve dans le coin supérieur gauche de la section **Fonctionnalités d'optimisation WAN**. Cela permet de modifier le formulaire et révèle les boutons **Appliquer** et **Rétablir**.

Remarque

Cette fonction sélectionne cette fonction pour l'activation, uniquement. L'optimisation du réseau étendu ne sera pas activée dans la section **Optimisation** ou dans le package de configuration tant que vous n'aurez pas cliqué sur **Appliquer**, après avoir terminé la configuration **des fonctionnalités**. En outre, vous devez également configurer le paramètre **Accélération** pour chaque classe de service applicable dans le tableau Classes de service, comme indiqué plus loin dans le processus **de configuration d'optimisation**. (Les instructions sont fournies dans la section [Configuration des classes de service par défaut d'optimisation](#)) Enfin, l'optimisation du réseau étendu ne sera pas activée et activée dans votre réseau étendu virtuel tant que vous n'aurez pas terminé la configuration complète du réseau étendu virtuel, puis généré, préparé pour être déployé, distribué et activé les packages d'appliance virtuelle WAN sur les sites éligibles de votre réseau étendu virtuel.

- f) Configurez les paramètres **Fonctionnalités**.

Activez une case à cocher pour sélectionner ou désélectionner une option. Vous pouvez accepter les paramètres par défaut présélectionnés dans le formulaire ou les personnaliser.

Remarque

Par défaut, les paramètres que vous configurez dans l'onglet **Global** sont automatiquement appliqués à chaque site de succursale inclus dans l'arborescence. Toutefois, vous pouvez personnaliser la configuration d'**optimisation** pour une succursale spécifique, comme indiqué dans la section, [Configuration de l'optimisation pour un site de succursale](#).

L'écran de configuration des **fonctionnalités** contient deux sections :

- **Fonctionnalités d'optimisation WAN**
- **Protocoles d'optimisation CIFS**

Les paramètres **des fonctionnalités d'optimisation WAN** sont les suivants :

- **Optimisation WAN** —Activez la case à cocher pour activer l'optimisation WAN pour cette configuration. Cela permet également la compression, la déduplication et l'optimisation du protocole TCP.

Remarque

L'option Optimisation WAN doit être sélectionnée pour que les autres options de la section Optimisation soient disponibles.

- **SCPS** —Activez la case à cocher pour activer l'optimisation du protocole TCP pour les liaisons satellites.
- **Priorités QoS HDX** : activez la case à cocher pour activer l'optimisation du trafic ICA en fonction de la hiérarchisation des sous-canaux HDX.
- **Optimisation Cross Protocol MAPI** —Activez la case à cocher pour activer l'optimisation interprotocole du trafic MAPI (Microsoft Outlook).
- **Optimisation SSL** : activez la case à cocher pour activer l'optimisation des flux de trafic avec chiffrement SSL.
- **RPC sur HTTP** : activez la case à cocher pour activer l'optimisation du trafic Microsoft Exchange qui utilise RPC sur HTTP.
- **Chiffrement du magasin de données utilisateur** — Activez la case à cocher pour activer la sécurité des données via le chiffrement de l'historique de compression WAN Optimization.
- **MAPI natif** : activez la case à cocher pour activer l'optimisation du trafic Microsoft Exchange.

Les options **des protocoles d'optimisation CIFS** sont les suivantes :

- **SMB1** —Activez la case à cocher pour activer l'optimisation du partage de fichiers Windows (SMB1)
- **SMB2** —Activez la case à cocher pour activer l'optimisation du partage de fichiers Windows (SMB2)
- **SMB3** —Activez la case à cocher pour activer l'optimisation du partage de fichiers Windows (SMB3). Vous devez d'abord sélectionner l'option **SMB2** avant de pouvoir sélectionner **SMB3**.

g) Cliquez sur **Appliquer** pour activer et ajouter les **fonctionnalités par défaut** sélectionnées au package de configuration.

L'étape suivante consiste à configurer les **paramètres de réglage** par défaut de l'**optimisation**.

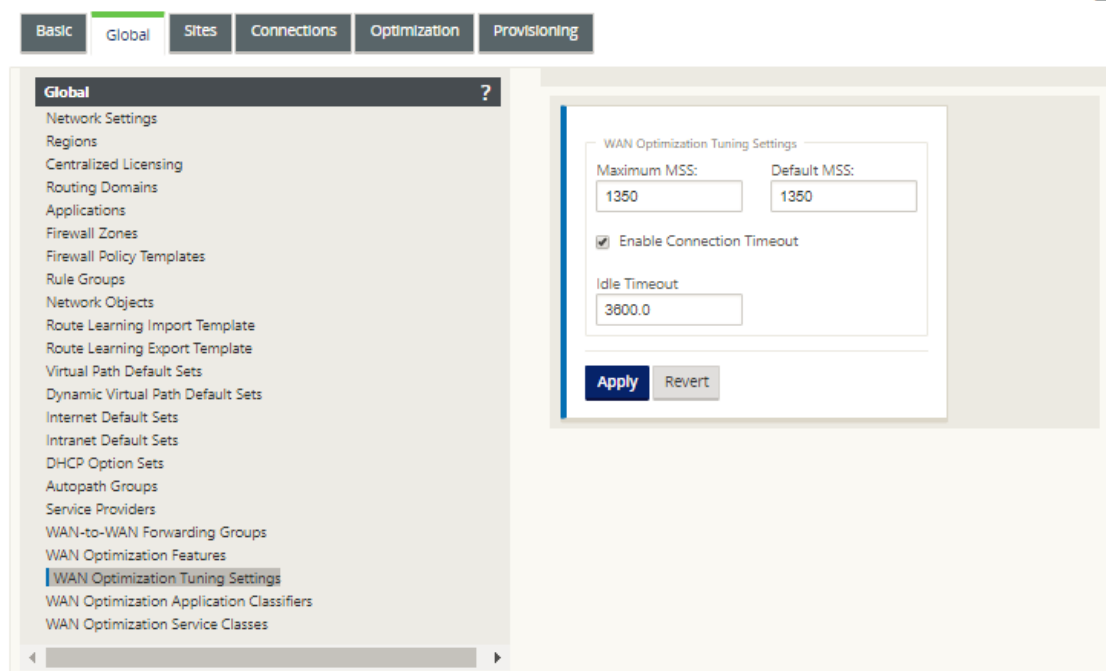
Configurer les paramètres de réglage par défaut de l'optimisation

May 6, 2021

Vous pouvez configurer les paramètres de réglage par défaut de l'optimisation WAN dans l'onglet **Global**.

Pour configurer les **paramètres de réglage** par défaut de l'optimisation WAN, procédez comme suit :

1. Dans l'onglet **Global**, cliquez sur **Paramètres de réglage de l'optimisation WAN**.



2. Sélectionnez et configurez les **paramètres de réglage**.

Les options **Réglage des paramètres** sont les suivantes :

- **Maximum MSS** : saisissez la taille maximale (en octets) de la taille maximale de segment (MSS) d'un segment TCP.
- **MSS par défaut** : saisissez la taille par défaut (en octets) du MSS pour les segments TCP.
- **Activer le délai d'expiration de la connexion** : sélectionnez cette option pour activer la résiliation automatique d'une connexion lorsque le seuil d'inactivité est dépassé.
- **Délai d'inactivité** : saisissez une valeur de seuil (en secondes) pour spécifier le temps d'inactivité autorisé avant la fin d'une connexion inactive. Vous devez d'abord sélectionner **Activer le délai d'expiration de la connexion** avant de pouvoir configurer ce champ.

3. Cliquez sur **Appliquer**.

Cela applique les **paramètres de réglage** modifiés à la configuration globale.

L'étape suivante consiste à configurer l'ensemble par défaut des Classificateurs d'applications d'optimisation WAN.

Configurer les classificateurs d'applications par défaut d'optimisation

May 6, 2021

Vous pouvez configurer les paramètres par défaut du classificateur d'application d'optimisation WAN dans l'onglet **Global**.

Pour configurer l'ensemble par défaut des Classificateurs d'applications d'optimisation WAN, procédez comme suit :

1. Dans l'onglet **Global**, cliquez sur **Classificateurs d'applications d'optimisation WAN**.

Cela ouvre le tableau **Classificateurs d'applications**, affichant l'ensemble par défaut des Classificateurs d'applications.

Global ?				
Basic Global Sites Connections Optimization Provisioning				
Network Settings Regions Centralized Licensing Routing Domains Applications Firewall Zones Firewall Policy Templates Rule Groups Network Objects Route Learning Import Template Route Learning Export Template Virtual Path Default Sets Dynamic Virtual Path Default Sets Internet Default Sets Intranet Default Sets DHCP Option Sets Autopath Groups Service Providers WAN-to-WAN Forwarding Groups WAN Optimization Features WAN Optimization Tuning Settings WAN Optimization Application Classifiers WAN Optimization Service Classes				
	Name	Application Group	Classification Parameters	Edit Delete
	ACTNET	legacy or non-ip	TCP Port: 5411	
	AFS	file server	TCP Port: 1483, 7004	
	ALC	host access	TCP Port: 47806	
	ALHTTP	web	TCP Port: 8008	
	AOL IM File	messaging	TCP Port: 2516-2518	
	ASP.NET Session State	session	TCP Port: 42424	
	AURP	routing protocols	TCP Port: 387	
	America OnLine (TCP)	messaging	TCP Port: 5191-5193	
	AppleTalk	legacy or non-ip	TCP Port: 548	
	AppleTalk Filing Protocol	legacy or non-ip	TCP Port: 2794	
	Ariel	content delivery	TCP Port: 419, 422	
	Avamar	backup and replication	TCP Port: 27000	

Ce tableau est également un formulaire de configuration. Vous pouvez utiliser ce formulaire pour configurer (modifier), supprimer et ajouter des Classificateurs d'applications afin de créer un jeu par défaut personnalisé. Le jeu de **Classificateurs d'applications** par défaut modifié et les paramètres individuels du Classificateur d'applications que vous configurez sont automatiquement appliqués comme valeurs par défaut à n'importe quel site de succursale inclus dans l'arborescence **de la section Optimisation**.

Remarque

Vous pouvez également personnaliser le jeu et les paramètres **des Classificateurs d'applications** pour chaque site de succursale spécifique. Pour obtenir des instructions, reportez-vous à la section [Configuration de l'optimisation pour un site de succursale](#).

2. Pour configurer un Classificateur d'applications existant, cliquez sur Modifier (icône en forme de crayon), dans la colonne **Modifier** de cette entrée de classificateur.

Cela ouvre un écran contextuel **Modifier** les paramètres pour configurer le Classificateur d'applications sélectionné.

3. Dans le champ **Port**, entrez le numéro de port du Classificateur d'applications ou acceptez la valeur par défaut.
4. Ajoutez ou supprimez des groupes d'applications dans la liste **Configuré**, ou acceptez les valeurs par défaut.

- **Pour ajouter un groupe d'applications à la liste** : sélectionnez-le dans la liste **Groupes d'applications** à gauche, puis cliquez sur la flèche Ajouter à droite (>) pour ajouter le groupe à la liste **Configuré** à droite. Pour ajouter tous les **groupes d'applications** à la liste à la fois, cliquez sur la double flèche de droite Ajouter tout (>>).
- **Pour supprimer un groupe d'applications de la liste** : sélectionnez-le dans la liste **Configuré** à droite, puis cliquez sur la flèche gauche Supprimer (<). Pour supprimer tous les **groupes d'applications** de la liste à la fois, cliquez sur la double flèche gauche Supprimer tous (<<).

5. Cliquez sur **Appliquer**.

Cela applique vos modifications au Classificateur d'applications et rejette l'écran **Modifier** la configuration.

6. (Facultatif) Personnalisez le jeu de **Classificateurs d'applications** par défaut.

Vous pouvez ajouter ou supprimer des Classificateurs d'applications pour personnaliser le jeu par défaut, comme suit :

- **Pour supprimer un Classificateur d'applications de l'ensemble :**

Cliquez sur l'icône de la corbeille dans la colonne **Supprimer** d'une entrée du **Classificateur d'applications** pour supprimer cette entrée du tableau.

- **Pour ajouter un classificateur d'applications à l'ensemble :**

- a) Cliquez sur **+** à droite de l'étiquette de succursale **Classificateur d'applications**.

Cette option affiche l'écran **Ajouter** une configuration.

- b) Entrez le nom et le numéro de port du Classificateur d'applications dans les champs **Nom** et **Port**, respectivement.

- c) Ajoutez ou supprimez des groupes d'applications dans la liste **Configuré**.

Pour ajouter un groupe d'applications à la liste : sélectionnez-le dans la liste **Groupes d'applications** à gauche, puis cliquez sur la flèche Ajouter à droite (>) pour ajouter le groupe à la liste **Configuré** à droite. Pour ajouter tous les **groupes d'applications** à la liste à la fois, cliquez sur la double flèche de droite Ajouter tout (»).

Pour supprimer un groupe d'applications de la liste : sélectionnez-le dans la liste **Configuré** à droite, puis cliquez sur la flèche gauche Supprimer (<). Pour supprimer tous les **groupes d'applications** de la liste à la fois, cliquez sur la double flèche gauche Supprimer tous («).

- d) Cliquez sur **Appliquer**.

Cela ajoute le nouveau Classificateur d'applications à l'ensemble et rejette le formulaire **Ajouter** de configuration.

L'étape suivante consiste à configurer l'ensemble par défaut de classes de service d'optimisation WAN.

Configurer les classes de service par défaut d'optimisation

May 6, 2021

Vous pouvez configurer les paramètres de classe de service par défaut d'optimisation WAN dans l'onglet **Global**.

Pour configurer l'ensemble par défaut de classes de service d'optimisation WAN, procédez comme suit :

1. Dans l'onglet **Global**, cliquez sur **Classes de service d'optimisation WAN**.

Cela ouvre le tableau **Classes de service**, affichant le jeu par défaut de Classes de service.

The screenshot shows the Citrix SD-WAN 11.4 configuration interface. The 'Global' tab is selected, and the 'WAN Optimization Service Classes' section is highlighted in the left-hand navigation pane. The main area displays a table of service classes.

Order	Name	Status	Acceleration	Edit	Delete
100	ICA	ENABLED	none		
200	Web (Private)	ENABLED	none		
300	Web (Private-Secure)	ENABLED	none		
400	Web (Internet)	ENABLED	none		
500	Web (Internet-Secure)	ENABLED	none		
600	CIFS	ENABLED	none		
700	NFS	ENABLED	none		
800	Microsoft Exchange (MAPI)	ENABLED	none		
900	Mail (Other)	ENABLED	none		
1000	VOIP and Multimedia	ENABLED	none		
1100	FTP Data	ENABLED	none		
1200	FTP Control	ENABLED	none		
1300	Instant Messaging	ENABLED	none		
1400	Session Applications	ENABLED	none		
1500	Directory and Security	ENABLED	none		
1600	Database Applications	ENABLED	none		

Ce tableau est également un formulaire de configuration. Vous pouvez utiliser ce formulaire pour configurer (modifier), supprimer et ajouter des classes de service afin de créer un jeu par défaut personnalisé. Le jeu **de classes de service** par défaut modifié et les paramètres de classe de service individuels que vous configurez sont automatiquement appliqués comme valeurs par défaut à n'importe quel site de succursale inclus dans l'arborescence **de la section Optimisation**.

Remarque

Vous pouvez également personnaliser le jeu et les paramètres de **classes de service** pour chaque site de succursale spécifique. Pour obtenir des instructions sur la personnalisation **de la configuration d'optimisation** pour un site de succursale, reportez-vous à la section [Configuration de l'optimisation pour un site de succursale](#).

2. Pour configurer une classe de service existante, cliquez sur Modifier (icône en forme de crayon), dans la colonne **Modifier** de cette entrée de classe dans le tableau Classes de service.

Cela ouvre un écran contextuel **Modifier** les paramètres pour configurer la classe de service sélectionnée.

Edit

Name: Order: ☒ Enabled

Acceleration Policy:

☒ Enable AppFlow Reporting ☐ Exclude from SSL Tunnel

Filter Rules +

Application	Source IP Address	Destination IP Address	Direction	Edit	Delete
ICA, ICA CGP			BIDIRECTIONAL		

3. Configurez les paramètres de base de la classe de service.

Les paramètres de base sont les suivants :

- **Activé** : sélectionnez cette option pour activer la nouvelle classe de service. La classe est activée par défaut.
- **Stratégie d'accélération** : sélectionnez une stratégie dans le menu déroulant **Stratégie d'accélération**. Les options sont les suivantes :
 - **disk** : sélectionnez cette stratégie pour spécifier le disque de l'appliance comme emplacement de stockage de l'historique du trafic utilisé pour la compression. Cela active la stratégie de compression basée sur le disque (DBC) pour cette classe de service. En règle générale, une stratégie de **disque** est généralement le meilleur choix, car l'appliance sélectionne automatiquement le **disque** ou la **mémoire** comme emplacement de stockage, en fonction de celui qui convient le mieux au trafic.
 - **none** : sélectionnez cette option si vous ne souhaitez pas activer une stratégie d'accélération pour cette classe de service. Une politique **nulle n'** est généralement utilisée que pour le trafic chiffré non compressible et la vidéo en temps réel.
 - **contrôle de flux uniquement** : sélectionnez cette stratégie pour désactiver la compression mais activer l'accélération du contrôle de flux. Sélectionnez cette option pour les services toujours chiffrés et pour le canal de contrôle FTP.
 - **memory** : sélectionnez cette stratégie pour spécifier la mémoire comme emplacement de stockage de l'historique du trafic utilisé pour la compression.
- **Activer les rapports AppFlow** —Sélectionnez cette option pour activer les rapports AppFlow pour cette classe de service. AppFlow est une norme de l'industrie pour le déverrouillage des données transactionnelles d'application traitées par l'infrastructure réseau.

L'interface AppFlow d'optimisation WAN fonctionne avec n'importe quel collecteur AppFlow pour générer des rapports. Le collecteur reçoit des informations détaillées de l'appliance, à l'aide de la norme ouverte AppFlow (<http://www.appflow.org>).

Pour plus d'informations sur AppFlow, consultez la documentation produit Citrix CloudBridge 7.4 disponible sur le portail de documentation citrix<http://docs.citrix.com/>.

Remarque

Pour afficher les rapports AppFlow Optimization WAN, sélectionnez l'onglet **Surveillance**^{**,*}, puis dans l'arborescence de navigation (volet gauche), ouvrez la branche **Optimisation WAN**, puis sélectionnez **AppFlow**. Consultez également la section [Surveillance du réseau étendu virtuel](#).

- **Exclure du tunnel SSL** : sélectionnez cette option pour exclure le trafic associé à la classe de service du tunnel SSL.

4. Configurez les **règles de filtrage** pour la classe de service.

Pour modifier une règle existante, procédez comme suit :

- a) Dans le tableau Règles de filtrage (en bas du formulaire), cliquez sur Modifier (icône en forme de crayon) dans la colonne Modifier de la règle à modifier.

Cela révèle les paramètres Règles de filtre pour la règle de filtre sélectionnée.

Edit

Name: ☒ Enabled

Acceleration Policy:

☒ Enable AppFlow Reporting ☐ Exclude from SSL Tunnel

Filter Rules +

Direction:

Applications:

Available:

- ACTNET
- AFS
- ALC
- ALTHTP
- AOL IM File

Configured:

- ICA
- ICA CGP

Source IP Address: +

Destination IP Address: +

Apply Cancel

b) Sélectionnez la direction du filtre dans le menu déroulant Direction.

Sélectionnez l'une des options suivantes :

- **BIDIRECTIONNEL**
- **UNIDIRECTIONNEL**

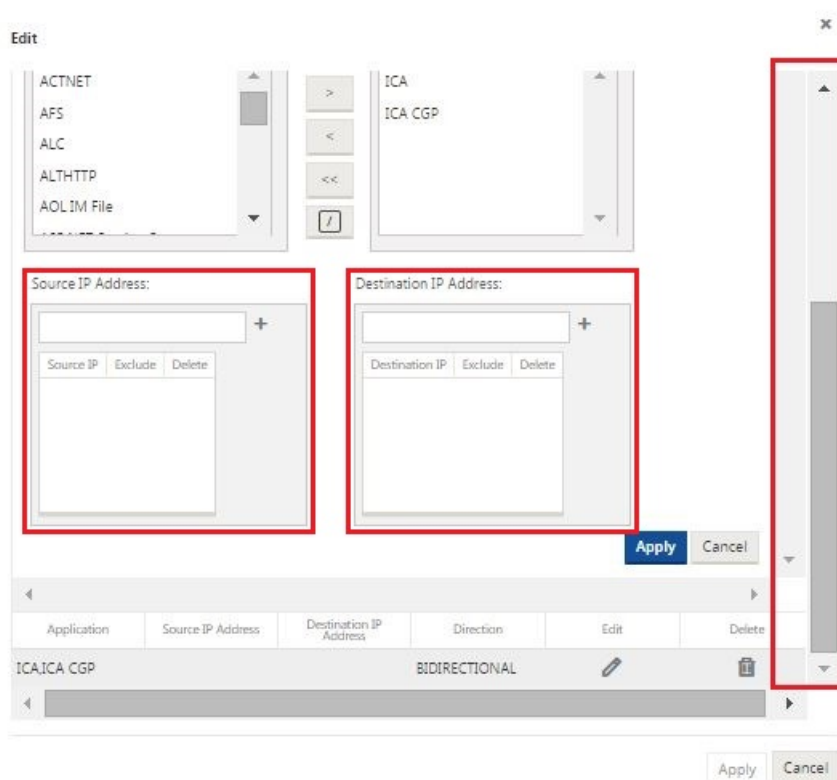
c) Ajouter ou supprimer des applications dans la liste **Configuré**.

Pour ajouter une application à la liste : sélectionnez-la dans la liste **Applications** à gauche, puis cliquez sur la flèche Ajouter à droite (>) pour ajouter le groupe à la liste **Configuré** à droite. Pour ajouter toutes les **applications** à la liste à la fois, cliquez sur la double flèche de droite Ajouter tout (»).

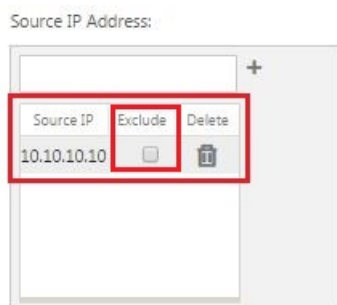
Pour supprimer une application de la liste : sélectionnez-la dans la liste Configuré à droite, puis cliquez sur la flèche gauche Supprimer (<). Pour supprimer toutes les **applications** de la liste à la fois, cliquez sur la double flèche gauche Supprimer toutes («).

d) Faites défiler vers le bas pour révéler la partie tronquée du formulaire.

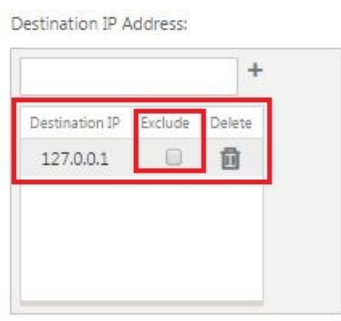
La section Paramètres des **règles de filtrage** est un peu longue. Vous devrez donc utiliser les barres de défilement pour afficher la partie tronquée du formulaire.



- e) Entrez l'adresse IP source dans le champ **Adresse IP source** .
- f) Cliquez sur **+** à droite de l'adresse IP source que vous venez de saisir.
- Cela ajoute l'adresse IP spécifiée à la table **Adresse IP source**.



- g) Indiquez s'il faut inclure ou exclure l'adresse IP source pour cette règle de filtre.
- Cochez la case **Exclude** pour exclure l'adresse IP source spécifiée de cette règle de filtre. Décochez la case pour inclure l'adresse.
- h) Entrez l'adresse IP de destination dans le champ **Adresse IP de destination** .
- i) Cliquez sur **+** à droite de l'adresse IP de destination que vous venez de saisir.
- Cela ajoute l'adresse IP spécifiée à la table **Adresse IP source**.



- j) Indiquez s'il faut inclure ou exclure l'adresse IP de destination pour cette règle de filtre.

Cochez la case **Exclude** pour exclure l'adresse IP de destination spécifiée de cette règle de filtre. Décochez la case pour inclure l'adresse.

- k) Cliquez sur **Appliquer**.

Cela applique vos modifications à la règle et masque la section Paramètres des **règles de filtrage**.

5. (Facultatif) Personnalisez le jeu **de classes de service** par défaut.

Vous pouvez ajouter ou supprimer des classes de service pour personnaliser le jeu par défaut, comme suit :

- **Pour supprimer une classe de service de l'ensemble :**

Cliquez sur l'icône Corbeille dans la colonne **Supprimer** d'une entrée de classe de service du tableau pour supprimer cette entrée.

- **Pour ajouter une classe de service à l'ensemble :**

- a) Cliquez sur **+** à droite de l'étiquette de succursale **Classe de service**.

Cette option affiche l'écran **Ajouter** une configuration.

- b) Entrez le nom de la nouvelle classe de service dans le **champ Nom**.

- c) Configurez la nouvelle classe de service.

Les étapes de configuration d'une nouvelle classe de service sont les mêmes que pour la modification d'une classe de service existante. Pour obtenir des instructions, reportez-vous aux étapes suivantes, plus haut dans cette section :

“3. Configurez les paramètres de base de la classe de service.”

“4. Configurez les règles de filtrage pour la classe de service.”

- d) Cliquez sur **Ajouter** pour ajouter la nouvelle classe de service au jeu par défaut et fermer l'écran **Ajouter une configuration**.

6. (Facultatif, recommandé) **Enregistrez** le package de configuration.

Vous avez maintenant terminé la configuration globale de l'optimisation WAN et pouvez commencer à configurer les jeux et paramètres d'**optimisation** pour les sites de branche.

Configurer l'optimisation d'un site de succursale

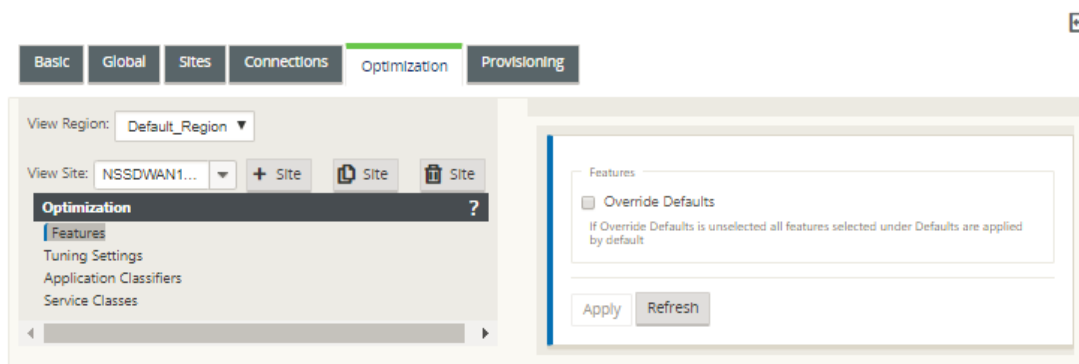
May 6, 2021

Une fois la configuration globale par défaut terminée, vous avez la possibilité de personnaliser les ensembles et les paramètres de chacun des sites de succursale.

Les paramètres globaux que vous venez de configurer sont automatiquement appliqués à chaque site de succursale inclus dans la section **Optimisation**. Vous pouvez choisir d'accepter les valeurs par défaut ou de personnaliser la configuration pour une succursale donnée. Les procédures de configuration des jeux et paramètres d'**optimisation** pour un site de succursale sont les mêmes que pour la configuration des valeurs par défaut globales, avec quelques différences mineures.

Pour personnaliser la configuration d'**optimisation** d'un site de succursale, procédez comme suit :

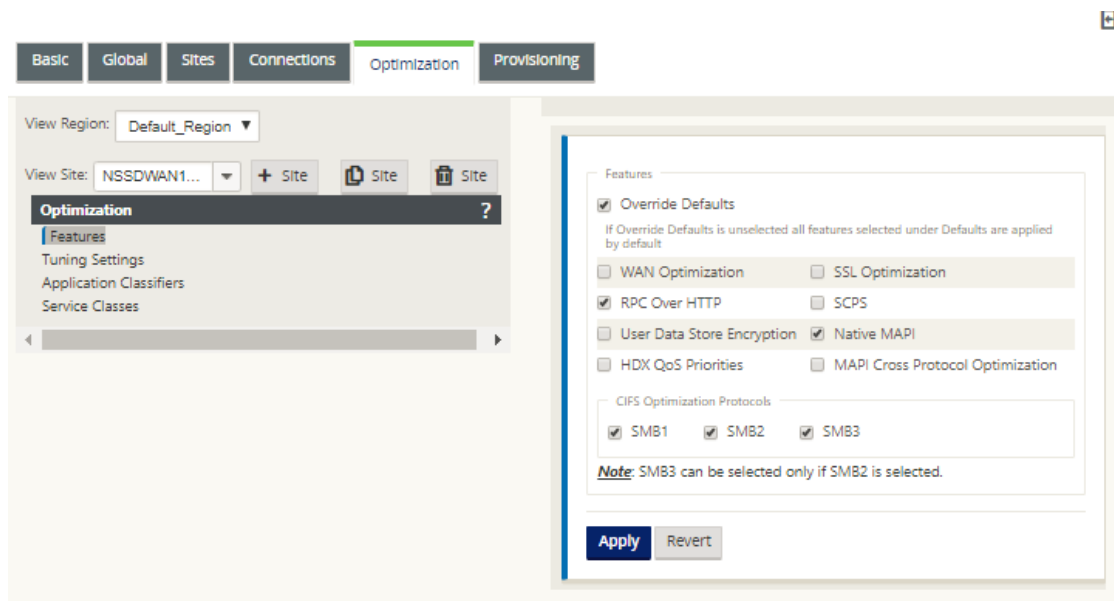
1. Cliquez sur **l'onglet Optimisation**, dans le champ Afficher le site, sélectionnez un site.



2. Cochez la case **Remplacer les valeurs par défaut**.

Cela révèle le formulaire de configuration de niveau supérieur pour cette catégorie de configuration et l'ouvre pour modification.

L'image ci-dessous montre un exemple de formulaire de configuration des paramètres de niveau supérieur, dans ce cas pour le jeu de **fonctionnalités**.



3. Entrez vos modifications de configuration.

À partir de ce moment, le processus de configuration pour chaque catégorie d'**optimisation de** site de branche est le même que pour la catégorie de section globale correspondante. Pour obtenir des instructions sur la configuration d'une catégorie particulière de jeux ou de paramètres, consultez la section appropriée ci-dessous :

- [Activation de l'optimisation et de la configuration des paramètres des fonctionnalités par défaut.](#)
- [Configuration des paramètres de réglage par défaut de l'optimisation.](#)
- [Configuration des classificateurs d'applications par défaut d'optimisation.](#)
- [Configuration des classes de service par défaut d'optimisation.](#)

4. (Facultatif, recommandé) **Enregistrez** le package de configuration.

Vous avez maintenant terminé la configuration des jeux et paramètres **de la section Optimisation** pour votre réseau étendu virtuel.

Configurer les profils SSL

May 6, 2021

Toute la configuration liée au SSL est disponible via le nouvel éditeur de configuration de l'appliance pour plus de sécurité et de facilité d'utilisation. Sur l'édition SD-WAN Premium (Enterprise) et les déploiements à deux boîtes, les classes de service sont configurées à partir de l'éditeur de configuration

et vous ne pouvez donc pas attacher de profils SSL. Pour tenir compte de l'expression du mappage de profil SSL à une classe de service, le flux de travail pour les profils SSL est modifié pour permettre d'attacher des classes de service dans le nœud de profil.

L'une des limitations est que le profil SSL sera attaché à toutes les règles d'une classe de service. Si vous devez attacher le profil SSL de manière sélective à une règle particulière, la configuration de la classe de service est divisée en règles détaillées pour une sélection ultérieure.

Remarque

Seules les classes de service dont la direction des règles de filtre est définie sur unidirectionnelle peuvent être associées aux profils SSL.

The screenshot shows the 'SSL Profile' configuration page in the Citrix SD-WAN interface. The 'Configuration' tab is selected. The 'SSL Profile' section is expanded, showing the following fields:

- Profile Name***: Test
- Profile Enabled**: ☒
- Parse Subject Alternative Names**: ☐
- Virtual Host Name**: (empty field)

A red box highlights the **Service Classes** section, which contains two lists:

- Available (19)**: RPCoverHTTP, ICA, Web (Private), Web (Private-Secure). Each item has a '+' icon and a vertical scrollbar.
- Configured (3)**: Iperf, Secure Applications, Web (Internet-Secure). Each item has a '-' icon.

Below the Service Classes section, the **Proxy Type** is set to **Split** (radio button selected).

Pour créer un profil SSL sur une nouvelle appliance Premium (Enterprise) Edition au niveau du centre de données, procédez comme suit :

1. Dans l'interface graphique Web SD-WAN, accédez à la page **Configuration > Accélération sécurisée** . Cliquez sur **Ajouter un profil**. Créez le **profil SSL**.

Dashboard

Monitoring

Configuration

+ Appliance Settings

+ Virtual WAN

+ WAN Optimization

Secure Acceleration

Certificate and Keys

User Data Store

+ System Maintenance

Configuration > WAN Optimization > Secure Acceleration

Secure Peering

Keystore Status
Opened

Secure Peering Status
Disabled


SSL Profile

Windows Domain

SSL Profiles

SSL acceleration allows the appliance to compress SSL traffic such as HTTPS and SSL-encrypted XenApp/XenDesktop (ICA/COP) traffic. Secure partner configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server-side NetScaler SD-WAN WO appliance (only) and SSL-specific configuration (called an SSL Profile) for each group of SSL servers. This step should be skipped on a client-side appliance.

Add Profile



Back

Create SSL Profile

☒ Manually add Profile

☐ Import Profile

Profile Name*

☒ Profile Enabled

☐ Parse Subject Alternative Names

Virtual Host Name

Service Classes

Available (21)Select All

ICA

+

Web (Private)

+

Web (Private-Secure)

+

Web (Internet)

+

Configured (0)Remove All

No items

Proxy Type

☐ Split

☒ Transparent

SSL Server's Private Key*

private_10_105_199_6

+

2. Dans la page **Créer un profil SSL**, indiquez un nom de profil et sélectionnez **Classes de service** qui seront associées à ce profil. Choisissez **Type de proxy** et fournissez les données pertinentes,

puis cliquez sur **Créer** .

Create SSL Profile

Manually add Profile

Import Profile

Profile Name*

SampleProfile

Profile Enabled

Parse Subject Alternative Names

Virtual Host Name

Service Classes

Available (20)Select All

Web (Private)+

ICA+

Web (Private-Secure)+

Web (Internet-Secure)+

Configured (1)Remove All

Web (Internet)-

Proxy Type

Split

Transparent

SSL Server's Private Key*

private_10_105_199_6

Create

Close

3. Une fois le profil SSL créé avec succès et la classe de service associée, affichez les informations de profil SSL comme indiqué ci-dessous.

<div><div>SSL Profile</div><div>Windows Domain</div></div>			
<div><div>Add</div><div>Edit</div><div>Delete</div><div>Action</div></div>			
Profile Name	Proxy Type	Profile In Use	Profile Enabled
SampleProfile	transparent	✓	✓

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

916

Plug-in client d'optimisation de Citrix WAN

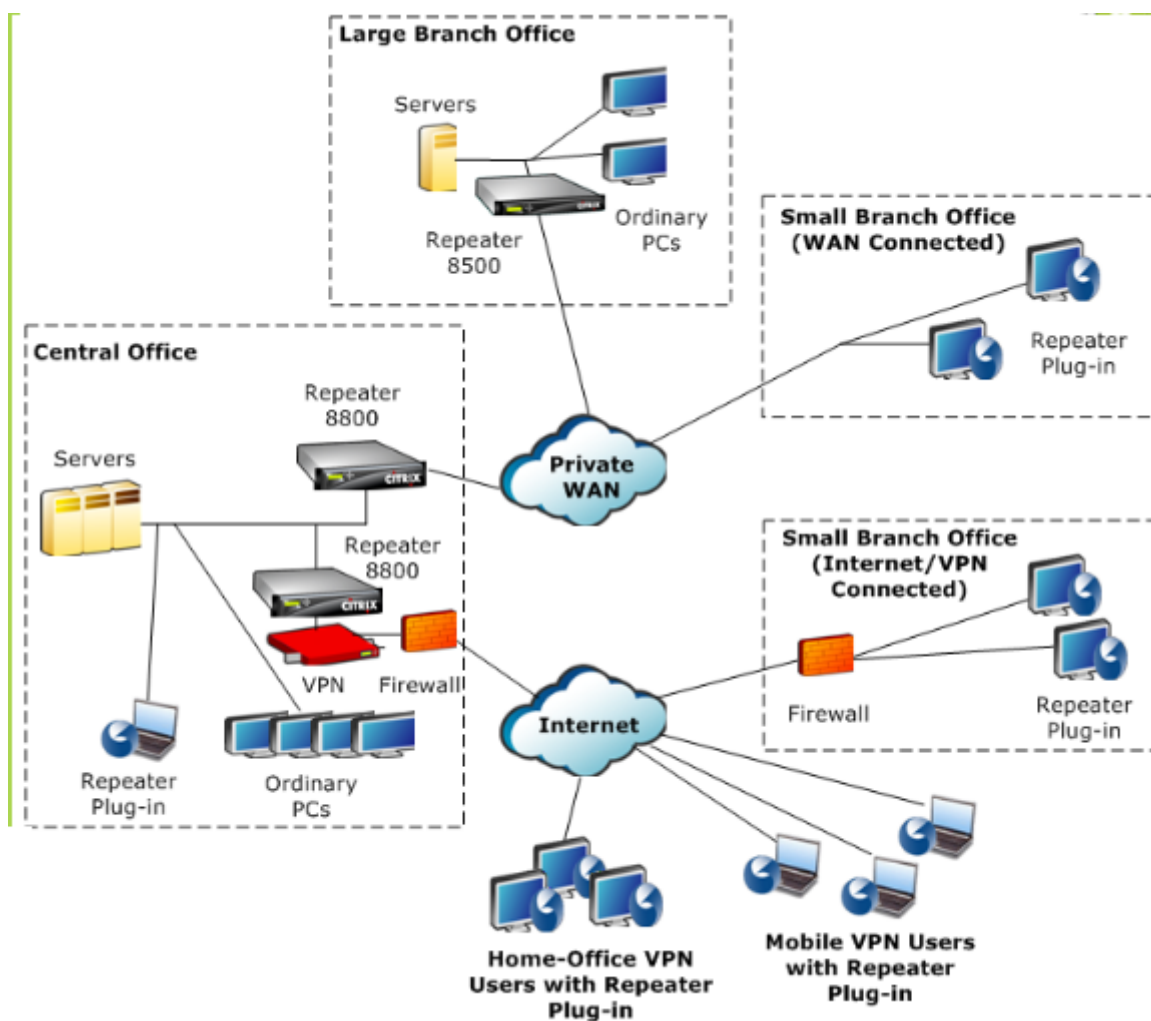
May 6, 2021

Le plug-in client Citrix WANOP est un accélérateur de réseau basé sur un logiciel qui s'exécute sur des ordinateurs portables et des stations de travail Windows, offrant une accélération partout, pas seulement dans les bureaux avec les appliances WANOP Client Plug-in. Il se connecte à une appliance Citrix WANOP Client Plug-in à l'autre extrémité de la liaison.

Les principes de fonctionnement du plug-in client WANOP sont généralement les mêmes que ceux d'un plug-in client WANOP. Pour les rubriques qui ne sont pas incluses dans la documentation du plug-in, reportez-vous à l'ensemble de documentation plus volumineux.

Le plug-in est distribué sous la forme d'un fichier d'installation Microsoft standard (MSI). Le déploiement du plug-in nécessite une configuration spécifique du plug-in des appliances WANOP Client Plug-in aux autres extrémités des liens. Si vous personnalisez le fichier MSI avec les adresses DNS ou IP des appliances WANOP Client Plug-in et quelques autres paramètres, vos utilisateurs n'ont pas à saisir d'informations de configuration lors de l'installation du plug-in sur leurs ordinateurs Windows.

Figure 1. Réseau de plug-in client WANOP typique Affichage du plug-in client WANOP



Remarque

Le plug-in est pris en charge par Citrix Receiver 1.2 ou version ultérieure et peut être distribué et géré par Citrix Receiver.

Configuration matérielle et logicielle requise

May 6, 2021

Du côté client de la liaison accélérée, le plug-in client WANOP est pris en charge sur les ordinateurs de bureau et portables Windows, mais pas sur les netbooks ou les clients légers. Citrix recommande les spécifications matérielles minimales suivantes pour l'ordinateur exécutant le plug-in client WANOP :

- Processeur Pentium 4 classes

- 2 Go de RAM
- 2 Go d'espace disque libre

Le plug-in client WANOP est pris en charge sur la plate-forme Windows 10 et nécessite la configuration système suivante :

- 4 Go de RAM
- 10 Go d'espace disque libre

Le plug-in client WANOP est pris en charge sur les systèmes d'exploitation suivants :

- Windows XP Édition Familiale
- Windows XP Professionnel
- Windows Vista (toutes les versions 32 bits de Familiale Basique, Familiale Premium, Professionnel, Entreprise et Intégrale)
- Windows 7 (toutes les versions 32 bits et 64 bits de Familiale Basique, Familiale Premium, Professionnel, Entreprise et Intégrale)
- Windows 8 (versions 32 bits et 64 bits de Premium (Enterprise) Edition)
- Windows 10 (versions 32 bits et 64 bits de Premium (Enterprise) Edition)

Côté serveur, les appliances suivantes prennent actuellement en charge les déploiements de plug-in client WANOP :

- Répéteur série 8500
- Répéteur série 8800
- Plug-in client WANOP VPX
- Plug-in client WANOP 2000
- Plug-in client WANOP 3000
- Plug-in client WANOP 4000
- Plug-in client WANOP 5000

Fonctionnement du plug-in WANOP

May 6, 2021

Les produits WANOP Client Plug-in utilisent votre infrastructure WAN/VPN existante. Un ordinateur sur lequel le plug-in est installé continue d'accéder au LAN, au WAN et à Internet comme il l'a fait avant

l'installation du plug-in. Aucune modification n'est requise pour vos tables de routage, paramètres réseau, applications clientes ou applications serveur.

Les VPN Citrix Access Gateway nécessitent une petite quantité de configuration spécifique au plug-in client WANOP.

Il existe deux variations dans la façon dont les connexions sont gérées par le plug-in et l'appliance : le *mode transparent* et le *mode redirecteur*. Le redirecteur est un mode hérité qui n'est pas recommandé pour les nouveaux déploiements.

- Le **mode transparent** pour l'accélération plug-in-appliance est très similaire à l'accélération appliance-appliance. L'appliance WANOP Client Plug-in doit se trouver dans le chemin emprunté par les paquets lorsqu'ils se déplacent entre le plug-in et le serveur. Comme pour l'accélération appliance-appliance, le mode transparent fonctionne comme un proxy transparent, préservant l'adresse IP source et de destination et les numéros de port d'une extrémité de la connexion à l'autre.
- Le **mode redirecteur** (non recommandé) utilise un proxy explicite. Le plug-in adresse à nouveau les paquets sortants à l'adresse IP du redirecteur de l'appliance. L'appliance réachemine les paquets au serveur, tout en changeant l'adresse de retour pour qu'elle pointe vers elle-même au lieu du plug-in. Dans ce mode, l'appliance n'a pas besoin d'être physiquement intégrée au chemin entre l'interface WAN et le serveur (bien qu'il s'agisse du déploiement idéal).

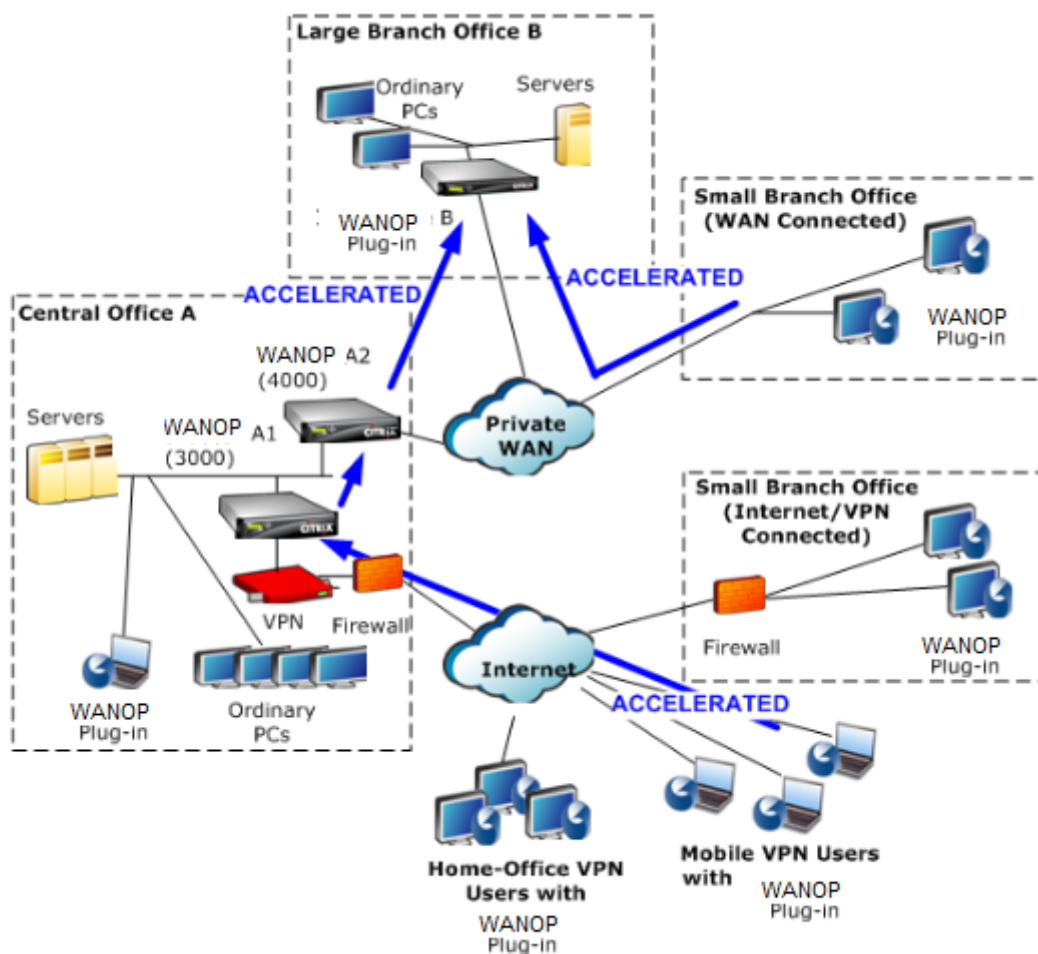
Meilleure pratique : utilisez le mode transparent lorsque vous le pouvez, et le mode redirecteur lorsque vous le devez.

Mode transparent

En mode transparent, les paquets pour les connexions accélérées doivent passer par l'appliance cible, tout comme ils le font pour l'accélération appliance-appliance.

Le plug-in est configuré avec une liste des appliances disponibles pour l'accélération. Il tente de contacter chaque appliance, ouvrant une connexion de signalisation. Si la connexion de signalisation réussit, le plug-in télécharge les règles d'accélération à partir de l'appliance, qui envoie les adresses de destination pour les connexions que l'appliance peut accélérer.

Figure 1. Mode transparent, mise en évidence de trois trajectoires d'accélération



Remarque

- Flux de trafic : le mode transparent accélère les connexions entre un plug-in client WANOP et une appliance compatible plug-in.
- Licence : les appliances ont besoin d'une licence pour prendre en charge le nombre de plug-ins souhaité. Dans le diagramme, le répéteur A2 n'a pas besoin d'être autorisé pour l'accélération du plug-in, car le répéteur A1 fournit l'accélération du plug-in pour le site A.
- daisy-chaining : si la connexion passe par plusieurs appliances en cours de route vers l'appliance cible, l'option « daisy-chaining » doit être activée pour les appliances du milieu, sinon l'accélération est bloquée. Dans le diagramme, le trafic des utilisateurs VPN de bureau à domicile et mobiles qui est destiné aux grandes succursales B est accéléré par le répéteur B. Pour que cela fonctionne, les répéteurs A1 et A2 doivent avoir activé le chaînage en marguerite.

Chaque fois que le plug-in ouvre une nouvelle connexion, il consulte les règles d'accélération. Si l'adresse de destination correspond à l'une des règles, le plug-in tente d'accélérer la connexion en at-

tachant des options d'accélération au paquet initial de la connexion (le paquet SYN). Si une appliance connue du plug-in attache des options d'accélération au paquet de réponse SYN-ACK, une connexion accélérée est établie avec cette appliance.

L'application et le serveur ne savent pas que la connexion accélérée a été établie. Seuls le logiciel plug-in et l'appliance savent que l'accélération est en cours.

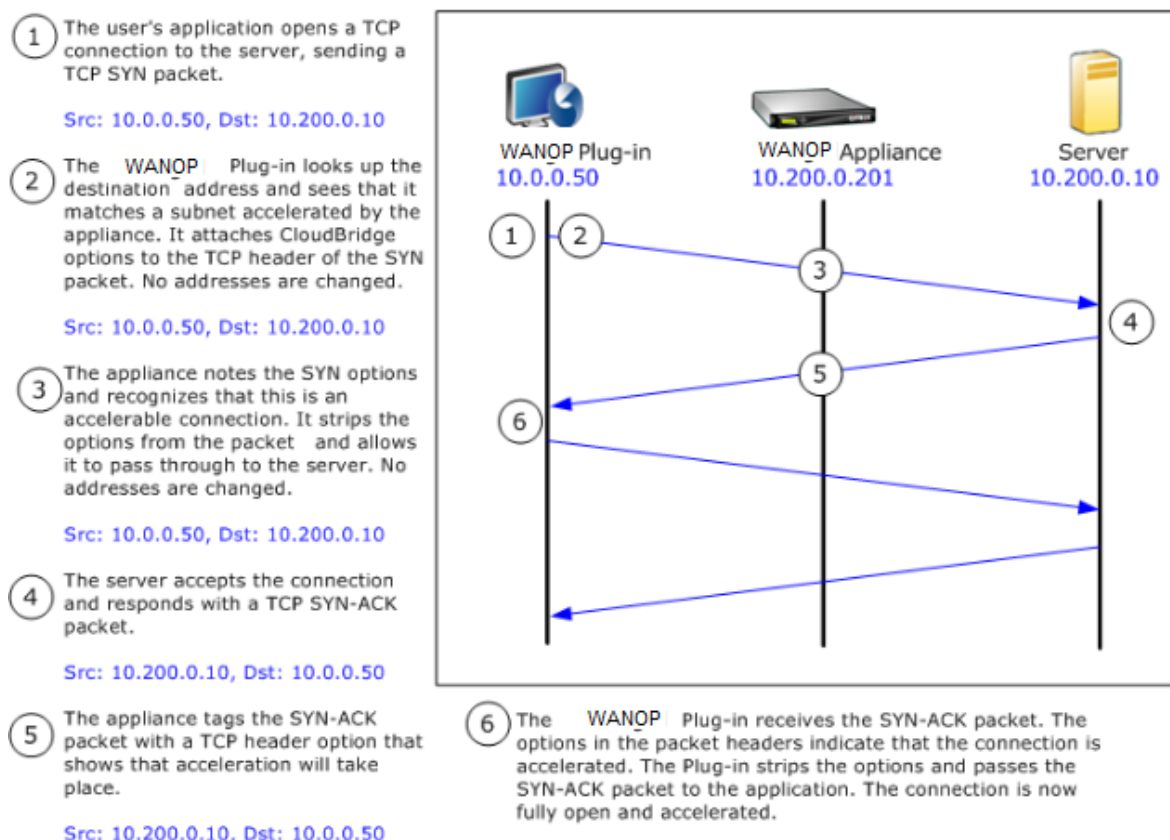
Le mode transparent ressemble à l'accélération appliance-appliance, mais n'est pas identique à celui-ci. Les différences sont les suivantes :

- Connexions initiées par le client uniquement : le mode transparent accepte uniquement les connexions initiées par le système équipé d'un plug-in. Si vous utilisez un système équipé d'un plug-in en tant que serveur, les connexions au serveur ne sont pas accélérées. D'autre part, l'accélération appliance-appliance fonctionne indépendamment du côté du client et du serveur. (Le FTP en mode actif est traité comme un cas particulier, car la connexion initiant le transfert de données demandé par le plug-in est ouverte par le serveur.)
- Connexion de signalisation : le mode transparent utilise une connexion de signalisation entre le plug-in et l'appliance pour la transmission des informations d'état. l'accélération appliance-appliance ne nécessite pas de connexion de signalisation, à l'exception des relations homologues sécurisées, qui sont désactivées par défaut. Si le plug-in ne peut pas ouvrir une connexion de signalisation, il ne tente pas d'accélérer les connexions via l'appliance.
- Chaîne en marguerite : pour une appliance située dans le chemin d'accès entre un plug-in et son matériel cible sélectionné, vous devez activer le chaînage en marguerite dans le menu **Configuration : Réglage**.

Le mode transparent est souvent utilisé avec les VPN. Le plug-in client WANOP est compatible avec la plupart des VPN IPsec et PPTP, ainsi qu'avec les VPN Citrix Access Gateway.

La figure suivante montre le flux de paquets en mode transparent. Ce flux de paquets est presque identique à l'accélération appliance-appliance, sauf que la décision de tenter ou non d'accélérer la connexion repose sur des règles d'accélération téléchargées sur la connexion de signalisation.

Figure 2. Flux de paquets en mode transparent



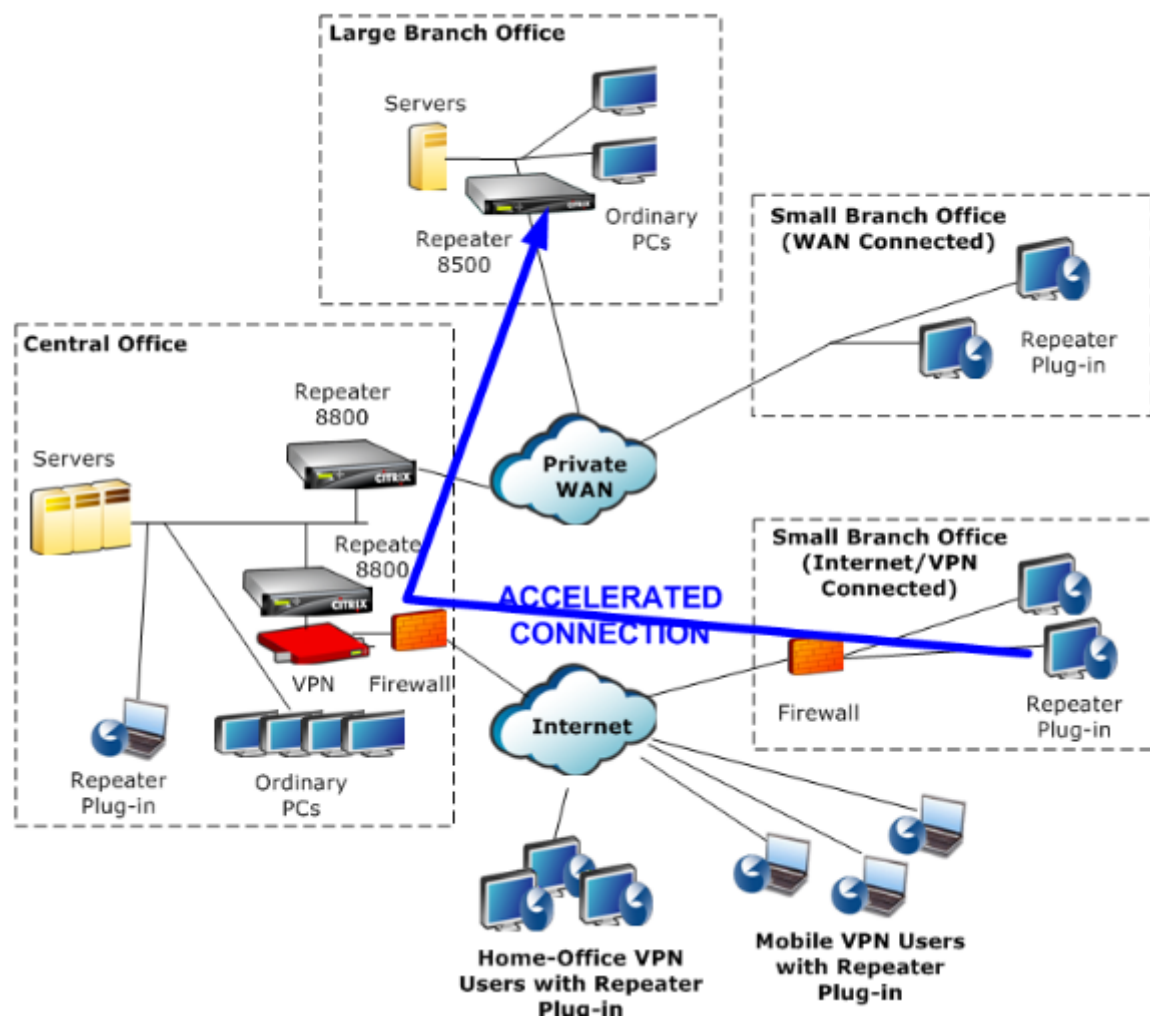
Mode redirecteur

Le mode redirecteur fonctionne différemment du mode transparent de la manière suivante :

- Le plug-in client WANOP redirige les paquets en les adressant explicitement à l'appliance.
- Par conséquent, l'appliance en mode redirecteur n'a pas à intercepter tout le trafic WAN Link. Comme les connexions accélérées lui sont adressées directement, il peut être placé n'importe où, tant qu'il peut être atteint à la fois par le plug-in et le serveur.
- L'appliance effectue ses optimisations, puis redirige les paquets de sortie vers le serveur, en remplaçant l'adresse IP source des paquets par sa propre adresse. Du point de vue du serveur, la connexion provient de l'appliance.
- Le trafic de retour du serveur est adressé à l'appliance, qui effectue des optimisations dans le sens de retour et transfère les paquets de sortie au plug-in.
- Les numéros de port de destination ne sont pas modifiés, de sorte que les applications de surveillance réseau peuvent toujours classer le trafic.

La figure ci-dessous montre comment fonctionne le mode Redirecteur.

Figure 1. Mode redirecteur



La figure ci-dessous montre le flux de paquets et le mappage d'adresses en *mode redirecteur*.

Figure 2. Flux de paquets en mode redirecteur

- 1 The user's application opens a TCP connection to the server, sending a TCP SYN packet.

Src: 10.0.0.50, Dst: 10.200.0.10

- 2 The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.

Src: 10.0.0.50, Dst: 10.200.0.201

(10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

- 3 The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and giving itself as the src.

Src: 10.200.0.201, Dst: 10.200.0.10

- 4 The server accepts the connection and responds with a TCP SYN-ACK packet.

Src: 10.200.0.10, Dst: 10.200.0.201

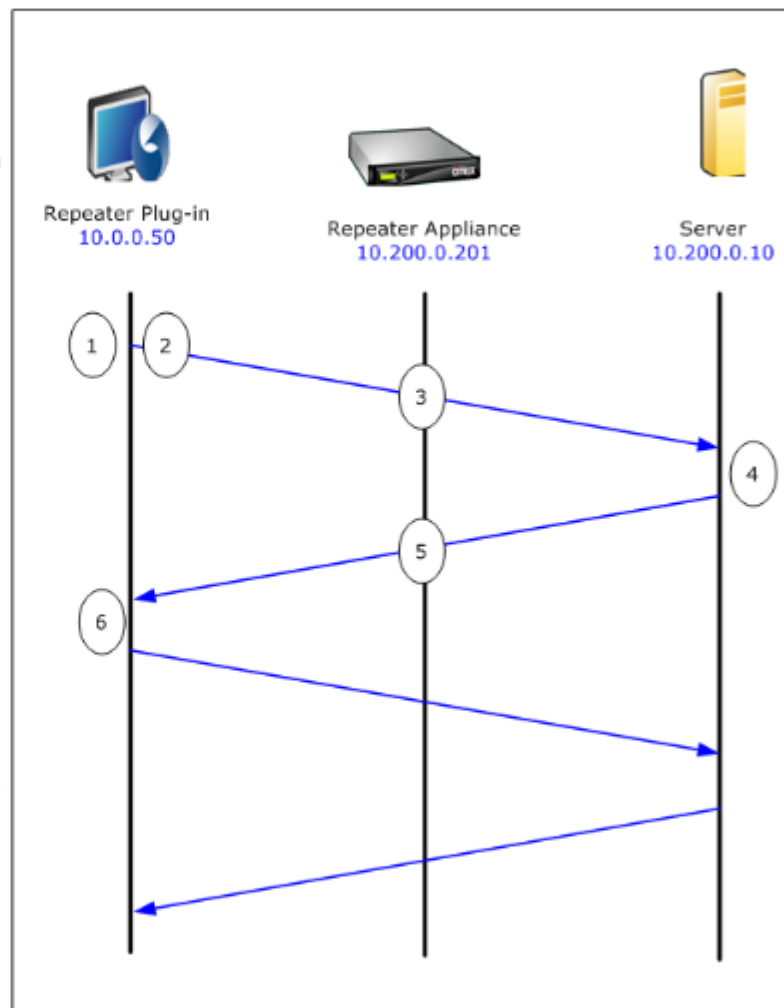
- 5 The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

Src: 10.200.0.201, Dst: 10.0.0.50

- 6 The connection is now fully open. The client and server send packets back and forth via the appliance.

While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.



Mode de sélection d'une appliance par le plug-in

Chaque plug-in est configuré avec une liste des appliances qu'il peut contacter pour demander une connexion accélérée.

Les appliances disposent chacune d'une liste de règles d'accélération, qui est une liste d'adresses ou de ports cibles auxquels l'appliance peut établir des connexions accélérées.** Le plug-in télécharge ces règles à partir des appliances et correspond à l'adresse et au port de destination de chaque connexion avec l'ensemble de règles de chaque appliance. Si un seul appareil propose d'accélérer une connexion donnée, la sélection est facile. Si plusieurs appliances proposent d'accélérer la connexion, le plug-in doit choisir l'une des appliances.

Les règles de sélection de l'appliance sont les suivantes :

- Si toutes les appliances proposant d'accélérer la connexion sont des appliances en mode redirecteur, l'appliance la plus à gauche dans la liste des appliances du plug-in est sélectionnée. (Si les appliances ont été spécifiées en tant qu'adresses DNS et que l'enregistrement DNS comporte plusieurs adresses IP, celles-ci sont également analysées de gauche à droite.)
- Si certaines des appliances proposant d'accélérer la connexion utilisent le mode redirecteur et d'autres le mode transparent, les appliances en mode transparent sont ignorées et la sélection est effectuée à partir des appliances en mode redirecteur.
- Si toutes les appliances proposant d'accélérer la connexion utilisent le mode transparent, le plug-in ne sélectionne pas un appareil spécifique. Il initie la connexion avec les options SYN du plug-in client WANOP, et quelle que soit l'appliance candidate attache les options appropriées au paquet SYN-ACK de retour utilisé. Cela permet à l'appliance qui est en ligne avec le trafic de s'identifier au plug-in. Toutefois, le plug-in doit avoir une connexion de signalisation ouverte avec l'appliance répondant, sinon l'accélération n'a pas lieu.
- Certaines informations de configuration sont considérées comme globales. Ces informations de configuration proviennent de l'appliance la plus à gauche de la liste pour laquelle une connexion de signalisation peut être ouverte.

Déployer des appliances à utiliser avec des plug-ins

May 6, 2021

L'accélération du client nécessite une configuration spéciale sur l'appliance WANOP Client Plug-in. Parmi les autres considérations, mentionnons le placement de l'appliance. Les plug-ins sont généralement déployés pour les connexions VPN.

Utiliser une appliance dédiée si possible

Il est souvent difficile d'utiliser la même appliance pour l'accélération de plug-in et l'accélération de liaison, car les deux utilisations exigent parfois que l'appliance se trouve à des points différents du centre de données, et les deux utilisations peuvent appeler à des règles de classe de service différentes.

En outre, une appliance peut servir de point de terminaison pour l'accélération de plug-in ou de point de terminaison pour l'accélération de site à site, mais elle ne peut pas servir les deux objectifs pour la même connexion en même temps. Par conséquent, lorsque vous utilisez une appliance pour l'accélération de plug-in pour votre VPN et pour l'accélération de site à site vers un datacenter distant, les utilisateurs de plug-in ne reçoivent pas d'accélération de site à site. La gravité de ce problème dépend de la quantité de données utilisées par les utilisateurs de plug-in provient de sites distants.

Enfin, étant donné que les ressources d'une appliance dédiée ne sont pas réparties entre les demandes de plug-in et de site à site, elles fournissent davantage de ressources et donc des performances supérieures à chaque utilisateur de plug-in.

Utiliser le mode en ligne lorsque cela est possible

Une appliance doit être déployée sur le même site que l'unité VPN qu'elle prend en charge. Typiquement, les deux unités sont alignées les unes avec les autres. Un déploiement en ligne offre la configuration la plus simple, le plus grand nombre de fonctionnalités et les performances les plus élevées. Pour de meilleurs résultats, l'appliance doit être directement en ligne avec l'unité VPN.

Toutefois, les appliances peuvent utiliser n'importe quel mode de déploiement, à l'exception du mode groupe ou du mode haute disponibilité. Ces modes conviennent à l'accélération appliance-appliance et client-à-matériel. Ils peuvent être utilisés seuls (*mode transparent*) ou en combinaison avec le mode redirecteur.

Placez les appliances dans une partie sécurisée de votre réseau

Une appliance dépend de votre infrastructure de sécurité existante de la même manière que vos serveurs. Il doit être placé du même côté du pare-feu (et de l'unité VPN, le cas échéant) que les serveurs.

Éviter les problèmes NAT

La traduction d'adresses réseau (NAT) côté plug-in est gérée de manière transparente et n'est pas un problème. Du côté de l'appliance, la NAT peut être gênante. Appliquez les instructions suivantes pour assurer un déploiement sans heurts :

- Placez l'apppliance dans le même espace d'adressage que les serveurs, de sorte que les modifications d'adresse utilisées pour atteindre les serveurs soient également appliquées à l'apppliance.
- N'accédez jamais à l'apppliance à l'aide d'une adresse qu'elle n'associe pas elle-même.
- L'apppliance doit pouvoir accéder aux serveurs à l'aide des mêmes adresses IP auxquelles les utilisateurs du plug-in accèdent aux mêmes serveurs.
- En résumé, n'appliquez pas NAT aux adresses des serveurs ou des appliances.

Sélectionner le mode softboost

Sur la page Configurer les paramètres : Gestion de la bande passante, sélectionnez Mode Softboost. Softboost est le seul type d'accélération pris en charge avec le plug-in client WANOP.

Définir les règles d'accélération du plug-in

L'apppliance gère une liste de règles d'accélération indiquant aux clients le trafic à accélérer. Chaque règle spécifie une adresse ou un sous-réseau et une plage de ports que l'apppliance peut accélérer.

Ce qu'il faut accélérer - Le choix du trafic à accélérer dépend de l'utilisation de l'apppliance :

- Accélérateur VPN : si l'apppliance est utilisée comme accélérateur VPN, avec tout le trafic VPN passant par l'apppliance, tout le trafic TCP doit être accéléré, quelle que soit la destination.
- Mode redirecteur : contrairement au mode transparent, une appliance en mode redirecteur est un proxy explicite, ce qui fait que le plug-in transfère son trafic à l'apppliance en mode redirecteur même si cela n'est pas souhaitable. L'accélération peut être contre-productive si le client transfère le trafic vers une appliance éloignée du serveur, en particulier si cette « route triangulaire » introduit une liaison lente ou peu fiable. Par conséquent, Citrix recommande que les règles d'accélération soient configurées pour permettre à une appliance donnée d'accélérer son propre site uniquement.
- Autres utilisations - Lorsque le plug-in n'est utilisé ni comme accélérateur VPN ni en mode redirecteur, les règles d'accélération doivent inclure des adresses distantes aux utilisateurs et locales aux centres de données.

Définissez les règles - Définissez les règles d'accélération sur l'apppliance, sous l'onglet **Configuration : WANOP Client Plug-in : Acceleration Rules**.

Les règles sont évaluées dans l'ordre et l'action (Accélérer ou Exclure) est effectuée à partir de la première règle de correspondance. Pour qu'une connexion soit accélérée, elle doit correspondre à une règle Accélération.

L'action par défaut consiste à ne pas accélérer.

Figure 1. Définition des règles d'accélération

[Signaling Channel Configuration](#)
[Acceleration Rules](#)
[General Configuration](#)

Repeater Plug-In: Acceleration Rules

[Apply](#)
[Cancel](#)
[Add](#)
[Delete](#)
[Up](#)
[Down](#)

Rule	Rule Type	Destination IP/Mask	Port
1	Exclude	10.200.33.102	All
2	Exclude	10.200.33.100	All
3	Exclude	10.200.33.104	All
4	Exclude	10.200.33.105	All
5	Accelerate	10.0.0.0/8	All
Default	Exclude	All	All

1. Dans l'onglet Configuration : WANOP Plug-in : Règles d'accélération :

- Ajoutez une règle Accelerated pour chaque sous-réseau LAN local auquel l'appliance peut accéder. Autrement dit, cliquez sur **Ajouter**, sélectionnez **Accélérer** et tapez l'adresse IP du sous-réseau et le masque.
 - Répétez la procédure pour chaque sous-réseau local de l'appliance.
2. Si vous devez exclure une partie de la plage incluse, ajoutez une règle Exclure et déplacez-la au-dessus de la règle plus générale. Par exemple, 10.217.1.99 ressemble à une adresse locale. S'il s'agit vraiment du point de terminaison local d'une unité VPN, créez une règle Exclure pour elle sur une ligne au-dessus de la règle Accélération pour 10.217.1.0/24.
 3. Si vous souhaitez utiliser l'accélération pour un seul port (non recommandé), tel que le port 80 pour HTTP, remplacez le caractère générique dans le champ Ports par le numéro de port spécifique. Vous pouvez prendre en charge des ports supplémentaires en ajoutant des règles supplémentaires, une par port.
 4. En général, lister les règles étroites (généralement des exceptions) avant les règles générales.
 5. Cliquez sur **Appliquer**. Les modifications ne sont pas enregistrées si vous quittez cette page avant de les appliquer.

Utilisation du port IP

Utilisez les instructions suivantes pour l'utilisation du port IP :

- **Ports utilisés pour la communication avec le plug-in client WANOP** : le plug-in maintient une boîte de dialogue avec l'appliance via une connexion de signalisation, qui est par défaut sur le port 443 (HTTPS), qui est autorisé par la plupart des pare-feu.
- **Ports utilisés pour la communication avec les serveurs** : la communication entre le plug-in client WANOP et l'appliance utilise les mêmes ports que le client utiliserait pour la communication avec le serveur si le plug-in et l'appliance n'étaient pas présents. Autrement dit, lorsqu'un client ouvre une connexion HTTP sur le port 80, il se connecte à l'appliance sur le port 80. L'appliance contacte le serveur sur le port 80.

En mode redirecteur, seul le port connu (c'est-à-dire le port de destination sur le paquet TCP SYN) est conservé. Le port éphémère n'est pas conservé. En mode transparent, les deux ports sont conservés.

L'appliance suppose qu'elle peut communiquer avec le serveur sur n'importe quel port demandé par le client et qu'elle peut communiquer avec l'appliance sur n'importe quel port souhaité. Cela fonctionne bien si l'appliance est soumise aux mêmes règles de pare-feu que les serveurs. Dans ce cas, toute connexion qui réussirait dans une connexion directe réussirait dans une connexion accélérée.

Utilisation de l'option TCP et pare-feu

Les paramètres du plug-in client WANOP sont envoyés dans les options TCP. Les options TCP peuvent se produire dans n'importe quel paquet et sont garanties d'être présentes dans les paquets SYN et SYN-ACK qui établissent la connexion.

Votre pare-feu ne doit pas bloquer les options TCP dans la plage de 24-31 (décimale), sinon l'accélération ne peut pas avoir lieu. La plupart des pare-feu ne bloquent pas ces options. Cependant, un pare-feu Cisco PIX ou ASA avec le firmware de la version 7.x peut le faire par défaut, et par conséquent vous devrez peut-être ajuster sa configuration.

Personnaliser le fichier MSI du plug-in

May 6, 2021

Vous pouvez modifier les paramètres dans le fichier de distribution du plug-in client WANOP, qui est au format Microsoft Installer (MSI) standard. La personnalisation nécessite l'utilisation d'un éditeur MSI.

Remarque

Les paramètres modifiés dans votre édition. Le fichier MSI s'applique uniquement aux nouvelles installations. Lorsque des utilisateurs de plug-in existants sont mis à jour vers une nouvelle version, leurs paramètres existants sont conservés. Par conséquent, après avoir modifié les paramètres, vous devriez conseiller à vos utilisateurs de désinstaller l'ancienne version avant d'installer la nouvelle.

Pratiques exemplaires :

Créez une entrée DNS qui se résout à l'appliance plug-in la plus proche. Par exemple, définissez « Repeater.myCompany.com » et faites en sorte qu'il soit résolu en fonction de votre appliance, si vous n'avez qu'un seul appareil. Ou, si vous avez, disons, cinq appareils, ont Repeater.mycompany.com résoudre à l'un de vos cinq appareils, avec l'appareil sélectionné sur la base de la proximité avec le client ou l'unité VPN. Par exemple, un client utilisant une adresse associée à un VPN particulier doit voir Repeater.mycompany.com résoudre l'adresse IP du plug-in client WANOP connecté à ce VPN. Construisez cette adresse dans votre binaire de plug-in avec un éditeur MSI, tel que Orca. Lorsque vous ajoutez, déplacez ou supprimez des appliances, la modification de cette définition DNS unique sur votre serveur DNS met automatiquement à jour la liste des appliances de vos plug-ins.

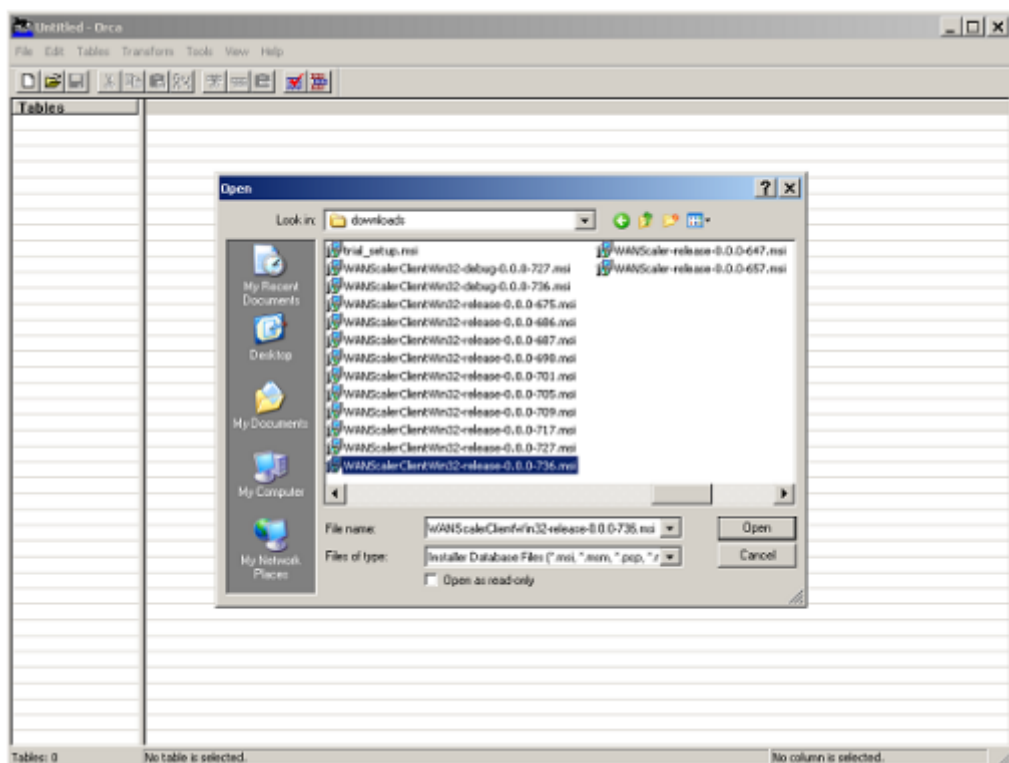
L'entrée DNS peut également être résolue sur plusieurs appliances, mais cela n'est pas souhaitable, sauf si toutes les appliances sont configurées de manière identique, car le plug-in prend certaines caractéristiques de l'appliance la plus à gauche de la liste et les applique globalement (y compris les caractéristiques de compression SSL). Cela peut conduire à des résultats indésirables et déroutants, en particulier si le serveur DNS fait pivoter l'ordre des adresses IP pour chaque requête.

Installez l'éditeur Orca MSI :

Il existe de nombreux éditeurs MSI tels que Orca, qui fait partie du SDK gratuit de plate-forme de Microsoft et peut être téléchargé à partir de Microsoft.

- Pour installer Orca MSI Editor
 1. Téléchargez la version PSDK-x86.exe du SDK et exécutez-la. Suivez les instructions d'installation.
 2. Une fois le SDK installé, l'éditeur Orca doit être installé. Il sera sous Microsoft Platform SDK\Bin\Orca.Msi. Lancez Orca.msi pour installer l'éditeur Orca (orca.exe).
 3. **Running Orca**—Microsoft fournit sa documentation Orca en ligne. Les informations suivantes décrivent comment modifier les paramètres de plug-in client WANOP les plus importants.
 4. Lancez Orca avec **Démarrer > Tous les programmes > Orca**. Lorsqu'une fenêtre Orca vide apparaît, ouvrez le fichier MSI Plug-in Client WANOP Plug-in avec **Fichier > Ouvrir**.

Figure 1. Utilisation d'Orca



5. Dans le menu **Tables**, cliquez sur **Propriété**. Une liste de toutes les propriétés modifiables du fichier .MSI s'affiche. Modifiez les paramètres affichés dans le tableau suivant. Pour modifier un paramètre, double-cliquez sur sa valeur, tapez la nouvelle valeur et appuyez sur **Entrée**.

Paramètre	Description	Mode par défaut	Commentaires
WSAPPLIANCES	Liste des appliances	Aucune	Entrez ici les adresses IP ou DNS de vos appliances WANOP, dans une liste séparée par des virgules sous la forme de {appliance1, appliance2, appliance3}. Si le port utilisé pour la signalisation des connexions est différent du port par défaut (443), spécifiez le port sous la forme Appliance1:Port_Number .
DBCMINSIZE	Espace disque minimum à utiliser pour la compression, en mégaoctets	250	La modification de cette valeur à une valeur plus élevée (par exemple, 2000) améliore les performances de compression mais empêche l'installation si l'espace disque est insuffisant. Le plug-in ne sera pas installé sauf s'il y a au moins 100 Mo d'espace disque libre en plus de la valeur que vous spécifiez pour DBCMINSIZE.

Paramètre	Description	Mode par défaut	Commentaires
EKEYPEM	Clé privée pour le plug-in. Partie de la paire certificat/clé utilisée avec la compression SSL	Aucune	Utilisez la commande Coller la cellule d'Orca. La fonction Coller normale ne préserve pas le format de la clé. Doit être une clé privée au format PEM (commençant par—BEGIN RSA PRIVATE KEY—)
X509CERTPEM	Certificat pour le plug-in. Partie de la paire certificat/clé utilisée avec la compression SSL	Aucune	Utilisez la commande Coller la cellule d'Orca. La fonction Coller normale ne préserve pas le format de la clé. Doit être un certificat au format PEM (commençant par —BEGIN CERTIFICATE —)
CACERTPEM	Certificat d'autorité de certification pour le plug-in. Utilisé avec la compression SSL	Aucune	Utilisez la commande Coller la cellule d'Orca. La fonction Coller normale ne préserve pas le format de la clé. Doit être un certificat au format PEM (commençant par —BEGIN CERTIFICATE —)

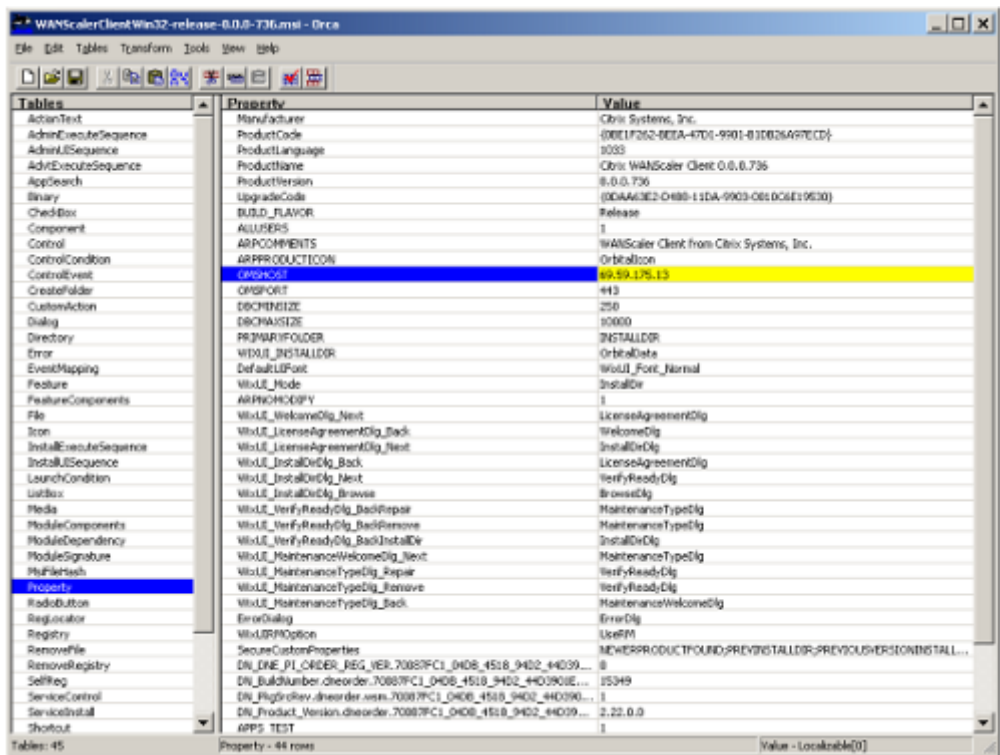
6. Dans le menu Tables, cliquez sur Propriété. Une liste de toutes les propriétés modifiables du fichier .MSI s'affiche. Modifiez les paramètres affichés dans le tableau suivant. Pour modifier un paramètre, double-cliquez sur sa valeur, tapez la nouvelle valeur et appuyez sur **Entrée**.

Paramètre	Description	Mode par défaut	Commentaires
WSAPPLIANCES	Liste des appliances	Aucune	Entrez ici les adresses IP ou DNS de vos appliances WANOP Client Plug-in, dans une liste séparée par des virgules, sous la forme de { <i>appliance1</i> , <i>appliance2</i> , <i>appliance3</i> }. Si le port utilisé pour la signalisation des connexions est différent du port par défaut (443), spécifiez le port sous la forme <i>Appliance1:Port_Number</i> . La modification de cette valeur à une valeur plus élevée (par exemple, 2000) améliore les performances de compression mais empêche l'installation si l'espace disque est insuffisant. Le plug-in ne sera pas installé sauf s'il y a au moins 100 Mo d'espace disque libre en plus de la valeur que vous spécifiez pour DBCMINSIZE.
DBCMINSIZE	Espace disque minimum à utiliser pour la compression, en mégaoctets	250	

Paramètre	Description	Mode par défaut	Commentaires
PRIVATEKEYPEM	Clé privée pour le plug-in. Partie de la paire certificat/clé utilisée avec la compression SSL	Aucune	Utilisez la commande Coller la cellule d'Orca. La fonction Coller normale ne préserve pas le format de la clé. Doit être une clé privée au format PEM (commençant par—BEGIN RSA PRIVATE KEY—)
X509CERTPEM	Certificat pour le plug-in. Partie de la paire certificat/clé utilisée avec la compression SSL	Aucune	Utilisez la commande Coller la cellule d'Orca. La fonction Coller normale ne préserve pas le format de la clé. Doit être un certificat au format PEM (commençant par —BEGIN CERTIFICATE —)
CACERTPEM	Certificat d'autorité de certification pour le plug-in. Utilisé avec la compression SSL	Aucune	Utilisez la commande Coller la cellule d'Orca. La fonction Coller normale ne préserve pas le format de la clé. Doit être un certificat au format PEM (commençant par —BEGIN CERTIFICATE —)

7. Lorsque vous avez terminé, utilisez la commande **Fichier : Enregistrer sous** pour enregistrer votre fichier modifié avec un nouveau nom de fichier ; par exemple, test.msi.

Figure 2 : Modification des paramètres dans Orca :



8. Lorsque vous avez terminé, utilisez la commande **Fichier : Enregistrer sous** pour enregistrer votre fichier modifié avec un nouveau nom de fichier ; par exemple, test.msi.

Votre logiciel de plug-in a maintenant été personnalisé.

Remarque

Certains utilisateurs ont vu un bug dans orca qui l'entraîne à tronquer les fichiers à 1 Mo. Vérifiez la taille du fichier enregistré. S'il a été tronqué, faites une copie du fichier d'origine et utilisez la commande Enregistrer pour remplacer l'original.

Une fois que vous avez personnalisé la liste des appliances avec Orca et distribué le fichier MSI personnalisé à vos utilisateurs, l'utilisateur n'a pas besoin de saisir les informations de configuration lors de l'installation du logiciel.

Déployer des plug-ins sur les systèmes Windows

May 6, 2021

Le plug-in client WANOP est un fichier exécutable Microsoft Installer (MSI) que vous téléchargez et installez comme avec tout autre programme distribué sur le Web. Obtenez ce fichier à partir de la section MyCitrix du site Web Citrix.com.

Remarque :

l'interface utilisateur WANOP Client Plug-in se réfère à elle-même comme **Citrix Acceleration Plug-in Manager**.

La seule configuration utilisateur requise par le plug-in est la liste des adresses de matériel. Cette liste peut consister en une liste d'adresses IP ou DNS séparées par des virgules. Les deux formes peuvent être mélangées. Vous pouvez personnaliser le fichier de distribution de sorte que la liste pointe vers votre appliance par défaut. Une fois installé, le fonctionnement est transparent. Le trafic vers les sous-réseaux accélérés est envoyé via une appliance appropriée, et tout autre trafic est envoyé directement au serveur. L'application utilisateur ne sait pas que tout cela se produit.

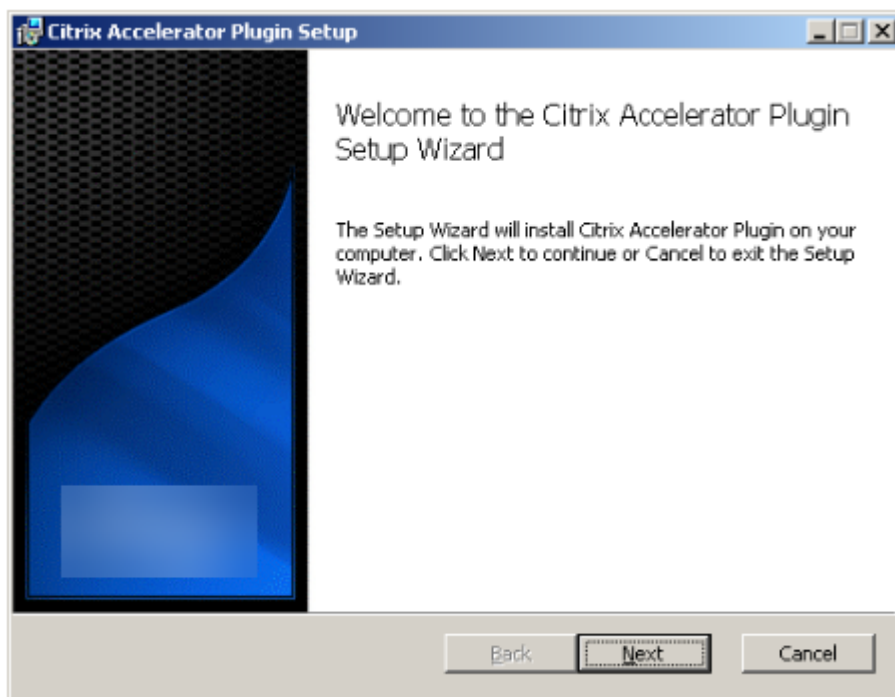
Installation**Pré-requis :**

Windows 10 exige que tous les pilotes disposent d'une signature numérique valide pour effectuer l'installation sans aucune erreur.

Pour installer WANOP Client Plug-in Accelerator sur le système Windows :

1. Le fichier Repeater*.msi est un fichier d'installation. Fermez toutes les applications et toutes les fenêtres qui pourraient être ouvertes, puis lancez le programme d'installation de la manière habituelle (double-cliquez sur dans une fenêtre de fichier, ou utilisez la commande run).

Figure 1. Écran d'installation initiale :

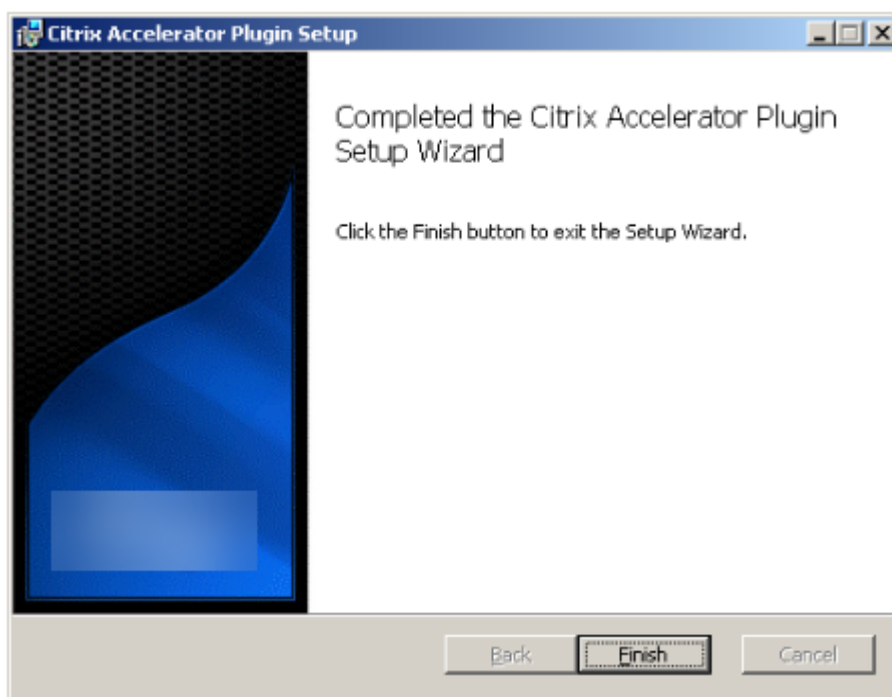


Les étapes ci-dessous sont pour une installation interactive. Une installation silencieuse peut être effectuée avec la commande :

« **msiexec /i client_msi_file /qn** »

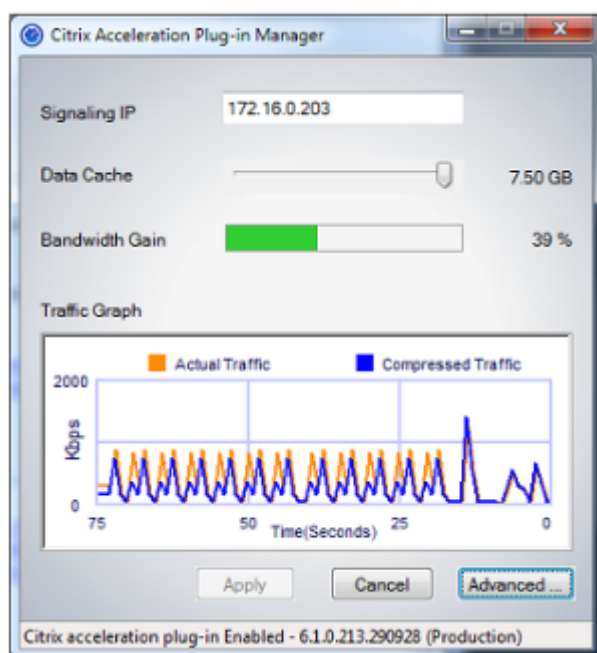
2. Le programme d'installation vous invite à indiquer l'emplacement où installer le logiciel. Le répertoire que vous spécifiez est utilisé à la fois pour le logiciel client et pour l'historique de compression sur disque. Ensemble, ils nécessitent un minimum de 500 Mo d'espace disque.
3. Une fois le programme d'installation terminé, il peut vous demander de redémarrer le système. Après un redémarrage, le plug-in client WANOP démarre automatiquement.

Figure 2. Écran d'installation finale



4. Cliquez avec le bouton droit sur l'icône Accelerator dans la barre des tâches et sélectionnez **Gérer l'accélération** pour lancer Citrix Plug-in Accelerator Manager.

Figure 3. Gestionnaire de prise Citrix Accelerator, affichage initial (de base)



5. Si le fichier .MSI n'a pas été personnalisé pour vos utilisateurs, spécifiez l'adresse de signalisation et la quantité d'espace disque à utiliser pour la compression :

- Dans le champ Appliances : Adresses de signalisation, tapez l'adresse IP de signalisation de votre appliance. Si vous disposez de plusieurs appliances Plug-in, listez-les tous, séparés par des virgules. Les adresses IP ou DNS sont acceptables.
- À l'aide du curseur Data Cache, sélectionnez la quantité d'espace disque à utiliser pour la compression. Plus il y en a, mieux c'est. 7,5 Go n'est pas trop, si vous avez autant d'espace disque disponible.
- Appuyez sur Appliquer.

L'accélérateur WANOP Client Plug-in est en cours d'exécution. Toutes les futures connexions aux sous-réseaux accélérés seront accélérées

Dans l'onglet Règles avancées du plug-in, la liste Règles d'accélération doit afficher chaque appliance comme Connecté et les sous-réseaux accélérés de chaque appliance comme Accéléré. Si ce n'est pas le cas, vérifiez le champ IP Adresses de signalisation et votre connectivité réseau en général.

Dépannage des plug-ins

L'installation du plug-in se déroule généralement sans problème. Si ce n'est pas le cas, vérifiez les problèmes suivants :

Problèmes courants :

- Si vous ne redémarrez pas le système, le plug-in client WANOP ne s'exécute pas correctement.
- Un disque très fragmenté peut entraîner de mauvaises performances de compression.
- Une défaillance de l'accélération (aucune connexion accélérée répertoriée dans l'onglet **Diagnostics**) indique généralement que quelque chose empêche la communication avec l'appliance. Vérifiez la liste **Configuration : Règles d'accélération** du plug-in pour vous assurer que l'appliance est correctement contactée et que l'adresse cible est incluse dans l'une des règles d'accélération. Les causes typiques des échecs de connexion sont :
 - L'appliance n'est pas en cours d'exécution ou l'accélération a été désactivée.
 - Un pare-feu dépouille les options TCP du plug-in client WANOP à un moment donné entre le plug-in et l'appliance.
 - Le plug-in utilise un VPN non pris en charge.

Erreur de verrouillage de l'activateur de réseau déterministe

Dans de rares cas, après avoir installé le plug-in et redémarré votre ordinateur, le message d'erreur suivant s'affiche deux fois :

L'installation de l'Enhancer de réseau déterministe nécessite d'abord un redémarrage, pour libérer les ressources verrouillées. Veuillez réexécuter cette installation après avoir redémarré l'ordinateur.

Si cela se produit, procédez comme suit :

1. Accédez à **Ajout/Suppression de programmes** et supprimez le plug-in client WANOP, le cas échéant.
2. Accédez au **Panneau de configuration > Cartes réseau > Connexion au réseau local > Propriétés**, recherchez l'entrée pour l'Enhancer de réseau déterministe, désactivez la case à cocher et cliquez sur **OK** . (Votre carte réseau peut être appelée par un nom autre que « Connexion au réseau local ».)
3. Ouvrez une fenêtre de commande et allez dans c:windowsinf (ou dans le répertoire équivalent si vous avez installé Windows dans un emplacement non standard).
4. Exécutez la commande suivante :
trouver « dne2000.cat » oem*.inf
5. Recherchez le fichier oem*.inf le plus grand numéro qui a renvoyé une ligne correspondante (la ligne correspondante est CatalogFile= dne2000.cat) et modifiez-la. Par exemple :
bloc-notes oem13.inf

6. Supprimez tout sauf les trois lignes en haut qui commencent par des points-virgules, puis enregistrez le fichier. Cela effacera les paramètres inappropriés ou obsolètes et la prochaine installation utilisera les valeurs par défaut.
7. Réessayez l'installation.

Autres problèmes d'installation

Tout problème lié à l'installation du plug-in client WANOP est généralement dû à l'interférence du réseau, du pare-feu ou du logiciel antivirus existant dans l'installation. Habituellement, une fois l'installation terminée, il n'y a pas d'autres problèmes.

Si l'installation échoue, procédez comme suit :

1. Assurez-vous que le fichier d'installation du plug-in a été copié sur votre système local.
2. Déconnectez tous les clients VPN/réseau distant actifs.
3. Désactivez temporairement tout pare-feu et logiciel antivirus.
4. Si cela est difficile, faites ce que vous pouvez.
5. Réinstallez le plug-in client WANOP.
6. Si cela ne fonctionne pas, redémarrez le système et réessayez.

Commandes GUI du plug-in WANOP

May 6, 2021

L'interface graphique du plug-in client WANOP apparaît lorsque vous cliquez avec le bouton droit de la souris sur l'icône **Plug-in Citrix Accelerator** et sélectionnez **Gérer l'accélération**. L'affichage de base de l'interface graphique apparaît en premier. Il y a aussi un affichage avancé qui peut être utilisé si vous le souhaitez.

Affichage de base

Sur la page de base, vous pouvez définir deux paramètres :

- Le champ Adresses de signalisation spécifie l'adresse IP de chaque appliance à laquelle le plug-in peut se connecter. Citrix recommande de n'afficher qu'une seule appliance, mais vous pouvez créer une liste séparée par des virgules. Il s'agit d'une liste ordonnée, les appliances les plus à gauche ayant priorité sur les autres. L'accélération est tentée avec l'appareil le plus à gauche

pour lequel une connexion de signalisation peut être établie. Vous pouvez utiliser à la fois des adresses DNS et des adresses IP.

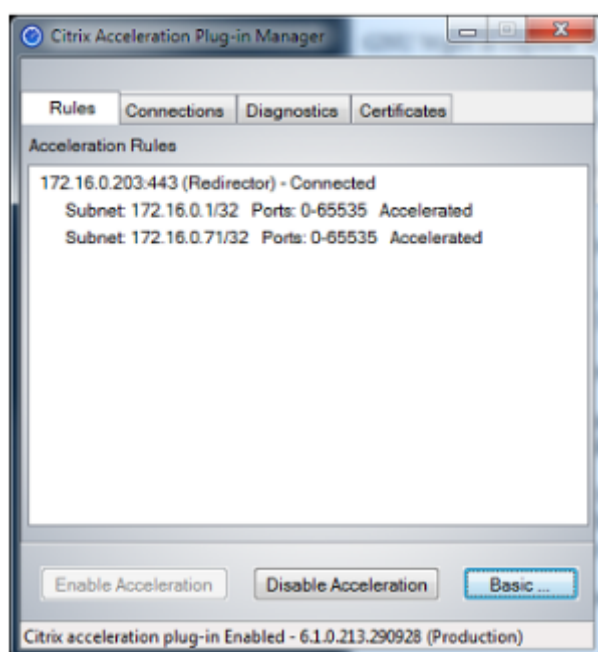
Exemples : 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

- Le curseur Data Cache ajuste la quantité d'espace disque allouée à l'historique de compression sur disque du plug-in. Plus il y en a, mieux c'est.

En outre, il y a un bouton pour passer à l'affichage Avancé.

Affichage avancé

La page Avancé contient quatre onglets : Règles, Connexions, Diagnostics et Certificats.



Au bas de l'écran se trouvent des boutons pour activer l'accélération, désactiver l'accélération et revenir à la page de base.

Onglet Règles

L'onglet Règles affiche une liste abrégée des règles d'accélération téléchargées depuis les appliances. Chaque élément de liste affiche l'adresse et le port de signalisation de l'appliance, le mode d'accélération (redirecteur ou transparent) et l'état de connexion, suivi d'un résumé des règles de l'appliance.

Onglet Connexions

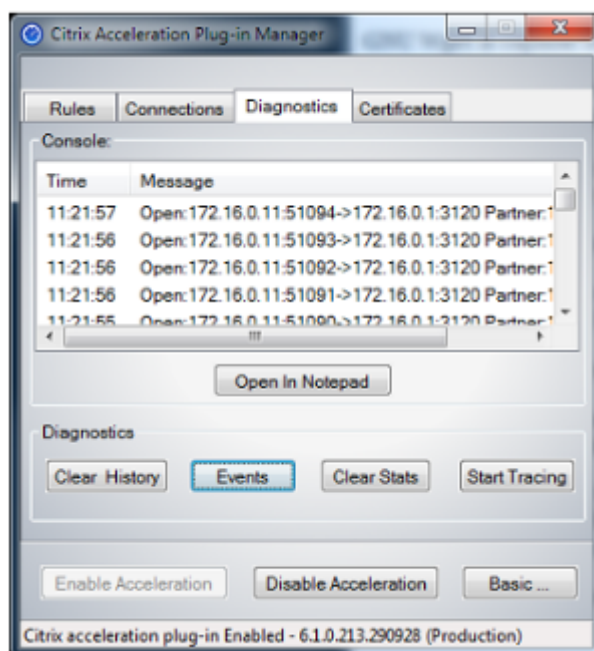
L'onglet **Connexions** répertorie le nombre de connexions ouvertes de différents types :

- **Connexions accélérées** : nombre de connexions ouvertes entre le plug-in client WANOP et les appliances. Ce numéro inclut une connexion de signalisation par appliance, mais n'inclut pas les connexions CIFS accélérées. Cliquez sur Plus pour ouvrir une fenêtre avec un bref résumé de chaque connexion. (Tous les boutons Plus vous permettent de copier les informations de la fenêtre dans le Presse-papiers, si vous souhaitez les partager avec le Support.)
- **Connexions CIFS accélérées** : nombre de connexions ouvertes et accélérées avec des serveurs CIFS (système de fichiers Windows). Ceci est généralement le même que le nombre de systèmes de fichiers réseau montés. Cliquez sur Plus pour afficher les mêmes informations que pour les connexions accélérées, ainsi qu'un champ d'état indiquant Actif si la connexion CIFS est en cours d'exécution avec les optimisations CIFS spéciales du plug-in client WANOP.
- **Connexions MAPI accélérées** : nombre de connexions Outlook/Exchange ouvertes et accélérées.
- **Connexions ICA accélérées** : nombre de connexions XenApp et XenDesktop ouvertes et accélérées utilisant les protocoles ICA ou CGP.
- **Connexions non accélérées** : ouvre les connexions qui ne sont pas accélérées. Vous pouvez cliquer sur Plus pour afficher une brève description des raisons pour lesquelles la connexion n'a pas été accélérée. En général, la raison en est qu'aucune appliance n'accélère l'adresse de destination, qui est signalée comme règle de stratégie de service.
- **Ouvrir/fermer les connexions** : connexions qui ne sont pas entièrement ouvertes, mais qui sont en cours d'ouverture ou de fermeture (connexions TCP « semi-ouvertes » ou « demi-fermées »). Le bouton Plus affiche des informations supplémentaires sur ces connexions.

Onglet Diagnostics

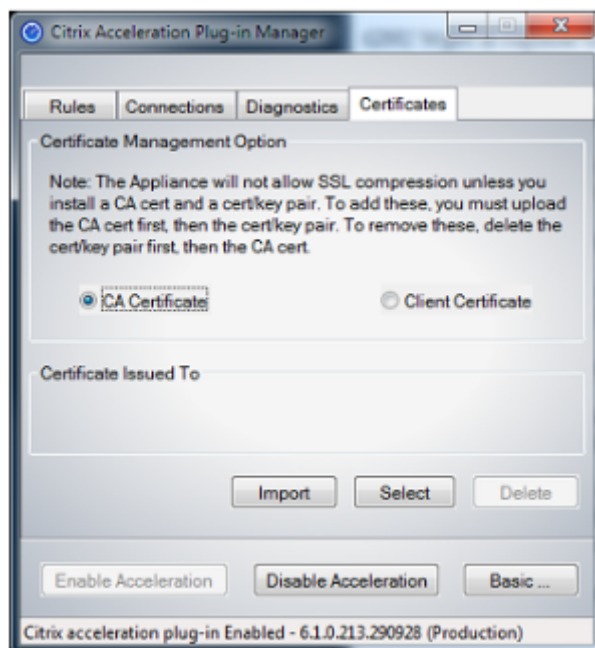
La page Diagnostics indique le nombre de connexions dans différentes catégories et d'autres informations utiles.

- **Démarrer le traçage/Arrêter le traçage** : si vous signalez un problème, votre représentant Citrix peut vous demander d'effectuer un suivi de connexion pour identifier les problèmes. Ce bouton démarre et arrête la trace. Lorsque vous arrêtez le suivi, une fenêtre contextuelle affiche les fichiers de suivi. Envoyez-les à votre représentant Citrix par les moyens qu'il recommande.
- **Effacer l'historique**—Cette fonctionnalité ne doit pas être utilisée.
- **Effacer les statistiques** : en appuyant sur ce bouton, les statistiques sont effacées dans l'onglet Performances.
- **Console** : fenêtre déroulante avec des messages d'état récents, principalement des messages d'ouverture de connexion et de fermeture de connexion, mais aussi des messages d'erreur et d'état divers.



Onglet Certificats

Sous l'onglet Certificats, vous pouvez installer des informations d'identification de sécurité pour la fonctionnalité d'appairage sécurisé facultative. Ces informations d'identification de sécurité ont pour but de permettre à l'appliance de vérifier si le plug-in est un client approuvé ou non.



Pour télécharger le certificat de l'autorité de certification et la paire de clés de certificat :

1. Sélectionnez **Gestion des certificats** de l'autorité de certification.
2. Cliquez sur **Importer**.
3. Chargez un certificat d'autorité de certification. Le fichier de certificat doit utiliser l'un des types de fichiers pris en charge (.pem, .crt., .cer ou .spc). Une boîte de dialogue peut s'afficher, vous demandant de sélectionner le magasin de certificats que vous souhaitez utiliser et de vous présenter une liste de mots-clés. Sélectionnez le premier mot clé dans la liste.
4. Sélectionnez **Gestion des certificats client**.
5. Cliquez sur **Importer**.
6. Sélectionnez le format de la paire de clés de certificat (PKCS12 ou PEM/DER).
7. Cliquez sur **Soumettre**.

Remarque

Dans le cas de PEM/DER, il existe des cases de téléchargement distinctes pour le certificat et la clé. Si votre paire de clés de certificat est combinée dans un seul fichier, spécifiez le fichier deux fois, une fois pour chaque case.

Mettre à jour le plug-in WANOP

May 6, 2021

Pour installer une version plus récente du plug-in client WANOP, suivez la procédure que vous avez utilisée lors de l'installation du plug-in pour la première fois.

Désinstaller le plug-in client WANOP

Pour désinstaller le plug-in client WANOP, utilisez l'utilitaire Ajout/Suppression de programmes Windows. Le plug-in client WANOP est répertorié comme **plug-in Citrix Accélération** dans la liste des programmes actuellement installés. Sélectionnez-le et cliquez sur **Supprimer**.

Vous devez redémarrer le système pour terminer la désinstallation du client.

Résoudre les problèmes liés au plug-in WANOP

May 6, 2021

- **Problème** : Je suis confronté à des problèmes de connectivité des canaux de signalisation. Comment puis-je résoudre ces problèmes ?

Résolution : pour résoudre les problèmes de connectivité des canaux de signalisation, effectuez les étapes de dépannage suivantes :

- Vérifiez que vous avez correctement configuré l'adresse IP de signalisation. Vous pouvez le faire en envoyant un ping à l'adresse IP de signalisation et en vérifiant la réponse.
- Vérifiez que l'état de la signalisation est activé sur l'appliance WANOP.
- Vérifiez que le pare-feu installé sur le réseau ne supprime pas les options TCP WANOP.
- Vérifiez qu'une licence de plug-in WANOP valide est installée sur l'appliance WANOP.
- Vérifiez que la configuration de filtrage des sources du canal de signalisation ne bloque pas l'adresse IP de la source du client.
- Si vous avez activé la détection de réseau local, vérifiez que le temps d'aller-retour entre le plug-in WANOP et l'appliance WANOP est une valeur acceptable.

- **Problème** : sur une appliance WANOP 4000, je ne suis pas en mesure de désactiver le plug-in WANOP.

Cause : Il s'agit d'un problème connu.

Résolution : Néant. Vous ne pouvez pas désactiver le plug-in WANOP sur une appliance WANOP 4000.

- **Problème** : lors de la connexion à l'appliance WANOP à l'aide du plug-in WANOP, l'entrée de message d'erreur suivante est enregistrée sous l'onglet Alertes :

Plus de plug-ins WANOP que la limite actuelle de <Number> ont tenté de se connecter à cette appliance.

Cause : le nombre de connexions à l'appliance WANOP a dépassé la limite d'utilisateurs sous licence.

Résolution : attendez qu'un utilisateur se déconnecte ou terminez une connexion.

- **Problème** : Une adresse IP de signalisation incorrecte est configurée sur une appliance WANOP 4000 ou 5000.

Résolution : Pour mettre à jour l'adresse IP de signalisation sur une appliance WANOP 4000 ou 5000, procédez comme suit :

1. Ouvrez une session sur l'instance NetScaler de l'appliance WANOP.
2. Accédez à la page Gestion du trafic > Équilibrage de charge > Serveurs virtuels > BR_LB_VIP_SIG.

3. Mettez à jour l'adresse IP de signalisation.

4. Enregistrez la configuration.

- **Problème** : le trafic CIFS et ICA ne s'accélère pas.

Résolution : Pour résoudre ce problème, effectuez les étapes de dépannage suivantes :

- Vérifiez que les règles d'accélération pour les adresses IP et les numéros de port sont correctement définies pour le plug-in WANOP.
- Vérifiez que les connexions CIFS ou ICA sont établies une fois la connexion de signalisation réussie.
- Vérifiez la stratégie d'accélération de la classe de service utilisée.

Connexion SMB 3.1.1

May 6, 2021

Le protocole SMB (Server Message Block) est un protocole de partage de fichiers réseau. Les paquets de messages qui définissent une version particulière du protocole s'appellent un dialecte. Le protocole CIFS (Common Internet File System) est un dialecte de SMB.

Dans Citrix SD-WAN version 10 version 1, le protocole SMB 3.1.1 est introduit sur les plates-formes WANOP et Premium Edition Citrix SD-WAN.

Le Citrix SD-WAN WANOP prend en charge les connexions SMB 3.1.1. Les connexions SMB 3.1.1 sont applicables lorsque le client est Windows 10 et que le serveur est Windows Server 2016.

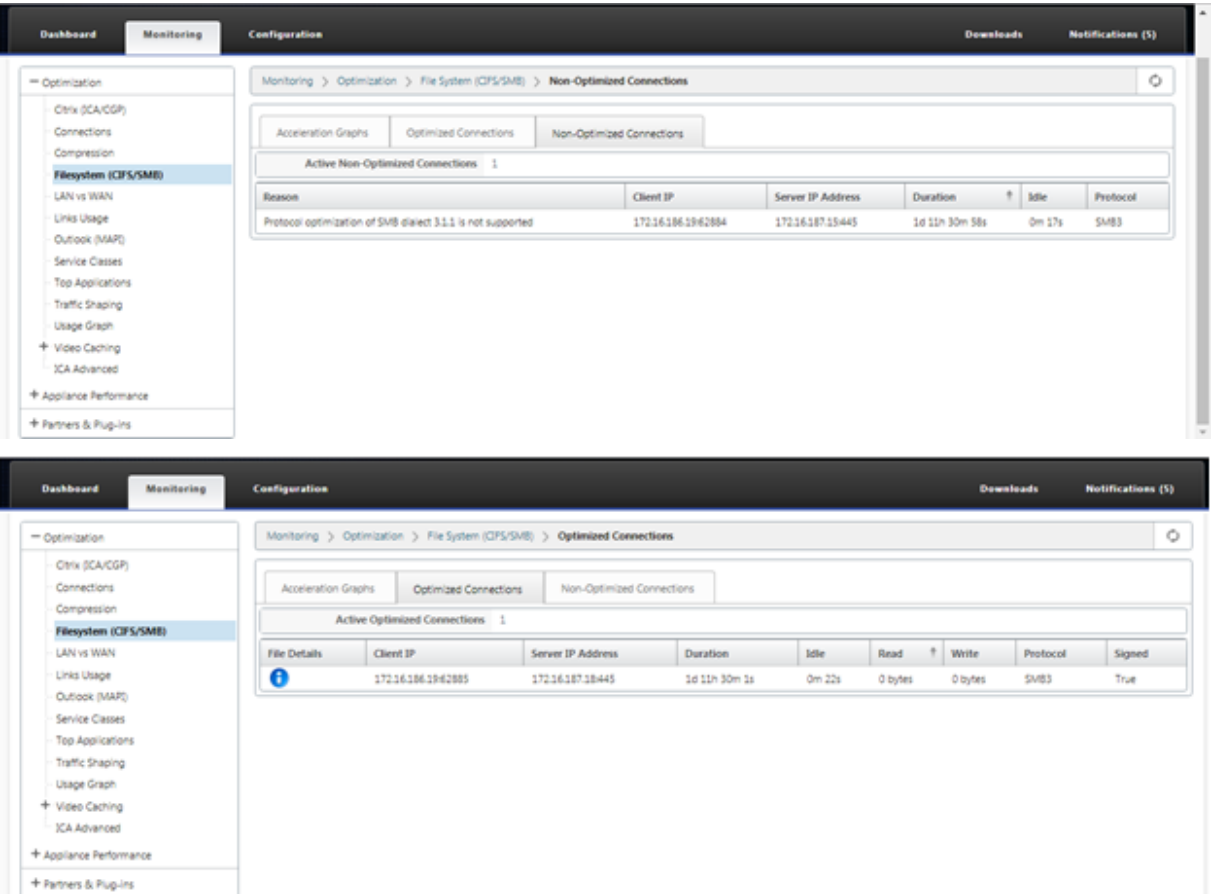
Lorsque le trafic SMB 3.1.1 passe par le module WANOP :

- Il est compté/visible dans le cadre de connexions non optimisées SMB 3.1 CIFS
- Le message de suivi suivant s'affiche, « Passer à travers cette connexion en tant que SMB 3.1.1 n'est pas pris en charge ».

Client	Serveur	Version SMB
Windows 10	Gagner 2016, 2012R2	SMB 3.1.1, 3.0.2
Windows 8.1	SMB 3.0	SMB 3.0
Windows 7	SMB 3.0	SMB 3.0

Pour les connexions non optimisées, l'interface utilisateur graphique de l'appliance Citrix SD-WAN WANOP affiche un message pour SMB 3.1.1.

Dans l'interface graphique de l'appliance Citrix SD-WAN WANOP, accédez à **Surveillance** > Système de **fichiers (CIFS/SMB)** . Cliquez sur l'onglet **Connexions non optimisées**, le message suivant s'affiche, *l'optimisation du protocole du dialecte SMB 3.1.1 n'est pas prise en charge* . Aucune entrée de journal n'est disponible et aucune nouvelle configuration n'est requise dans SD-WAN WANOP pour prendre en charge cette opération.



Comment les articles

August 31, 2022

Le « How-to-Articles » décrit la procédure de configuration des fonctionnalités prises en charge par Citrix SD-WAN. Ces articles contiennent des informations sur certaines des caractéristiques importantes suivantes :

Cliquez sur le nom d'une fonctionnalité ci-dessous pour afficher la liste des articles pratiques pour cette fonctionnalité.

- [Routage et transfert virtuels](#)
- [Activation de RED pour l'équité QoS](#)
- [Configuration](#)
- [Routage dynamique](#)
- [Serveur DHCP et relais DHCP](#)
- [Filtres de routage](#)
- [Terminaison et surveillance IPsec](#)
- [Secure Web Gateway](#)
- [QoS](#)
- [Opération conforme FIPS - Tunnel IPsec](#)
- [Configuration NAT dynamique](#)
- [Détection adaptative de la bande passante](#)
- [Test de la bande passante active](#)
- [Améliorations BGP](#)
- [Association de classe de service avec les profils SSL](#)
- [Peering sécurisé et Peering sécurisé manuel](#)
- [Déploiement sans contact](#)
- [Déploiement en mode deux boîtes](#)

Groupes d'interface

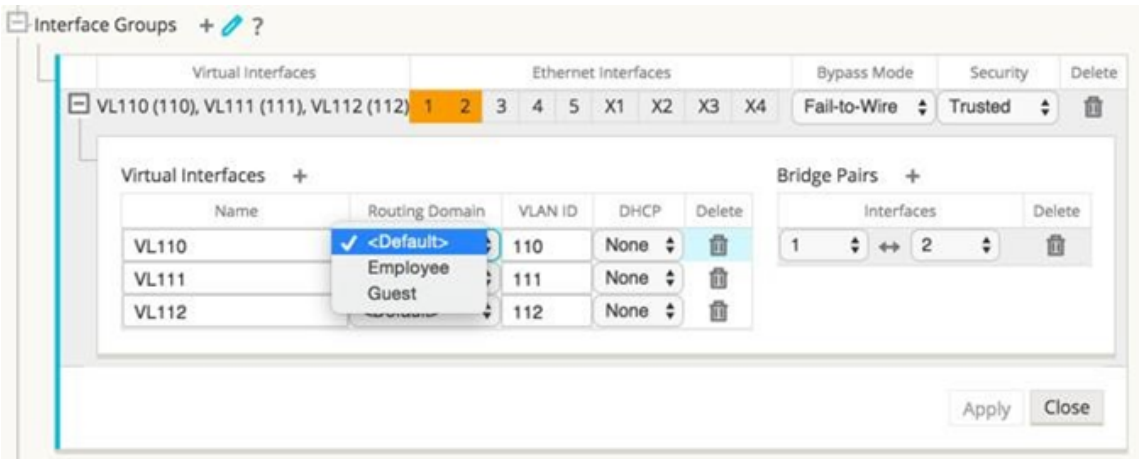
May 6, 2021

Pour configurer des groupes d'interface :

1. Dans l'**Éditeur de configuration**, accédez à **Sites** > **[Nom du site client]** > **Groupes d'interface**, choisissez un **domaine de routage** dans le menu déroulant lors de la configuration des interfaces virtuelles. Pour obtenir des instructions détaillées, consultez la section [configuration de groupes d'interface](#).

Remarque

Une fois les interfaces virtuelles associées à un domaine de routage spécifique, seules ces interfaces seront disponibles lors de l'utilisation de ce domaine de routage.



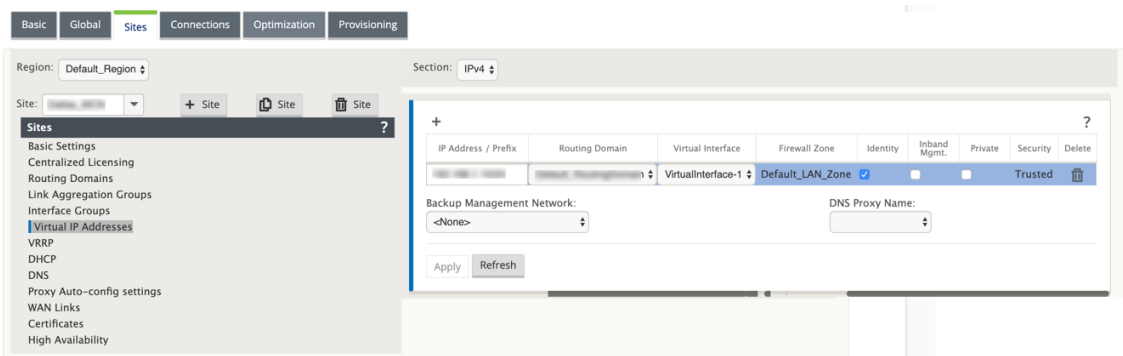
Configurer l'identité d'adresse IP virtuelle

May 6, 2021

L'interface réseau virtuel peut héberger plusieurs adresses IP dans des sous-réseaux identiques ou différents. Mais, vous ne pouvez sélectionner qu'une seule adresse IP virtuelle avec l'identité définie sur true qui peut être utilisée pour les protocoles de routage dynamique tels que BGP/OSPF, serveur/relais DHCP et gestion In-band.

Pour configurer l'identité de l'adresse IP virtuelle :

1. Dans l'**Éditeur de configuration**, accédez à **Sites**> **[Nom du site]**> **Adresses IP virtuelles**.
2. Activez la case à cocher **Identité** pour une adresse IP virtuelle pour l'utiliser pour les services IP.



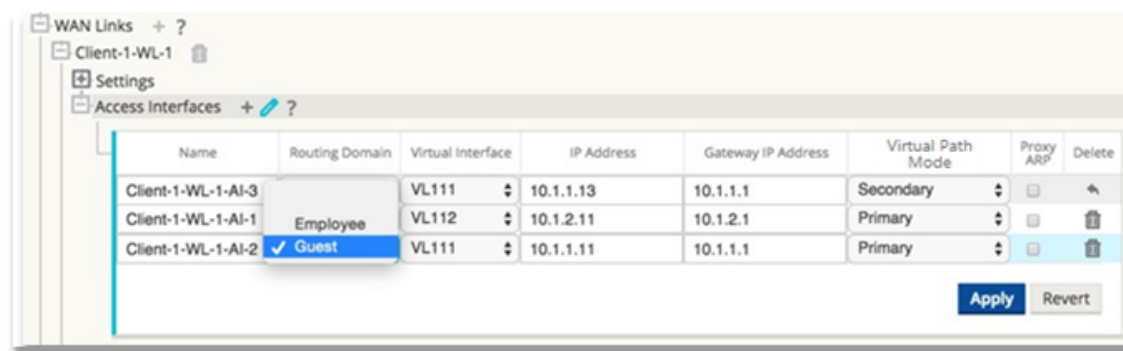
Configurer l'interface d'accès

September 26, 2023

Pour configurer l'interface d'accès :

1. Dans l'**Éditeur de configuration**, accédez à **Sites** > **[Nom du site client]** > **Liens WAN** > **[Nom du lien WAN]** > **Interfaces d'accès**.
2. Choisissez un **domaine de routage** dans le menu déroulant lors de la configuration d'une interface d'accès.

Pour obtenir des instructions détaillées, consultez la section **Comment configurer l'interface d'accès** dans la rubrique [Configurer MCN](#).



Configurer les adresses IP virtuelles

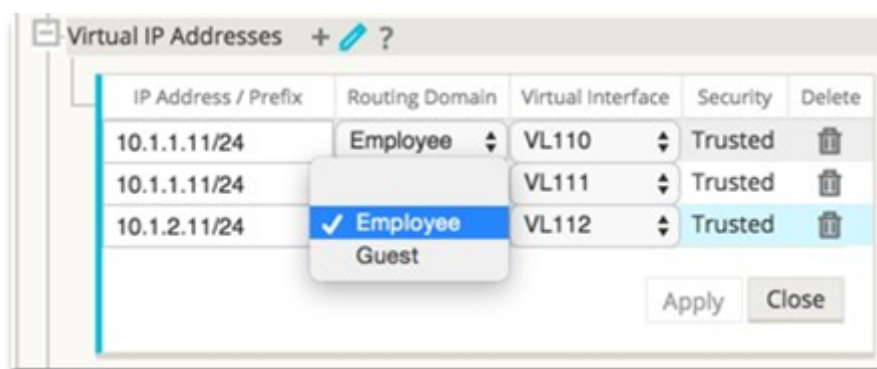
May 6, 2021

Pour configurer les adresses IP virtuelles :

1. Dans l'**Éditeur de configuration**, accédez à **Sites** > **[Nom du site client]** > **Adresses IP virtuelles**.
2. Choisissez un **domaine de routage** dans le menu déroulant lors de la configuration des adresses IP virtuelles.

Pour obtenir des instructions détaillées, consultez la section [configuration des adresses IP virtuelles](#).

Le domaine de routage choisi détermine les interfaces virtuelles disponibles dans le menu déroulant.



Configurer les tunnels GRE

May 6, 2021

Pour configurer les tunnels GRE :

1. Dans l'éditeur de configuration, accédez à **Connexions> Site> Tunnels GRE**. L'adresse IP source ne peut être choisie que dans l'interface réseau virtuelle sur les liens approuvés.
2. Entrez un nom pour le tunnel GRE.
3. Sélectionnez l'adresse **IP source** disponible dans le menu déroulant. Le domaine de routage détermine les adresses IP source disponibles dans le menu déroulant.
4. (Facultatif) Sélectionnez l'**adresse IP source publique**. Ce champ peut être vide si cette adresse est identique à l'adresse IP source.
5. Entrez l'adresse **IP de destination** du tunnel GRE.
6. Entrez l'adresse **IP/préfixe** du tunnel GRE Tunnel.
7. Cliquez sur **Somme de contrôle**, si vous souhaitez utiliser la somme de contrôle dans l'en-tête de tunnel GRE.
8. Entrez une valeur pour la **période Keepalive** en secondes. Si vous configurez 0, aucun paquet keepalive n'est transmis, mais le tunnel GRE sera actif.
9. Entrez une valeur pour les **tentatives Keepalive**. Cette valeur détermine le nombre de tentatives de nouvelles tentatives de keepalive avant que l'appliance SD-WAN désactive le tunnel GRE.

Reportez-vous [configuration des tunnels GRE](#) au site MCN pour plus d'informations.

Name	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	*		*	*		10	3	

Apply Revert

Pour plus d'informations sur la sécurisation de la Gateway Web à l'aide de tunnels GRE, voir ;[Secure Web Gateway](#)

Configuration des chemins dynamiques pour la communication de succursale à succursale

May 6, 2021

Avec la demande de VoIP et de visioconférence, le trafic se déplace de plus en plus entre les bureaux. Il est inefficace de configurer des connexions de maillage complet via des centres de données, ce qui peut prendre du temps.

Avec Citrix SD-WAN, vous n'avez pas besoin de configurer des chemins entre chaque bureau. Vous pouvez activer la fonctionnalité Chemin dynamique et la solution SD-WAN crée automatiquement des chemins entre les bureaux à la demande. La session utilise initialement un chemin fixe existant. Et lorsque la bande passante et le seuil temporel sont atteints, un chemin est créé dynamiquement si ce nouveau chemin présente de meilleures caractéristiques de performances que le chemin fixe. Le trafic de session est transmis par le nouveau chemin d'accès. Il en résulte une utilisation efficace des ressources. Les chemins n'existent que lorsqu'ils sont nécessaires et réduisent la quantité de trafic transmis vers et depuis le centre de données.

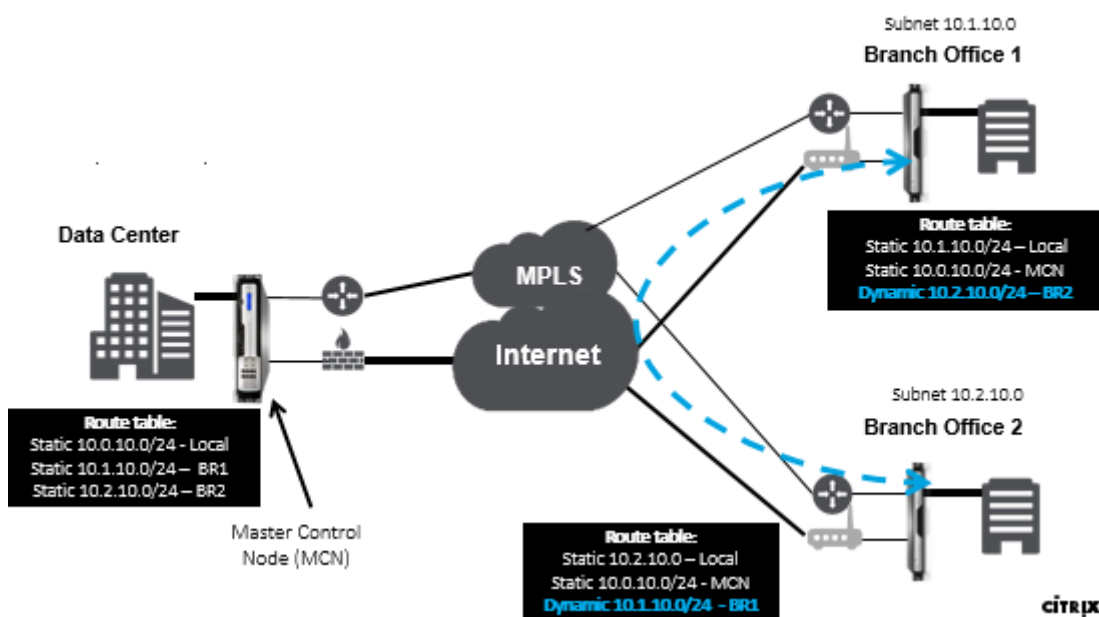
Les avantages supplémentaires du réseau SD-WAN comprennent :

- Seuils de bande passante et de PPS pour permettre les connexions de succursale à succursale
- Réduction des besoins en bande passante à l'intérieur et à l'extérieur du datacenter tout en minimisant la latence
- Les chemins créés à la demande dépendent de seuils définis
- Libérer dynamiquement les ressources réseau lorsque cela n'est pas nécessaire
- Réduction de la charge sur le nœud de contrôle maître et de la latence

Communication de succursale à succursale à l'aide de chemins virtuels dynamiques :



Réseau SD-WAN avec chemin dynamique :



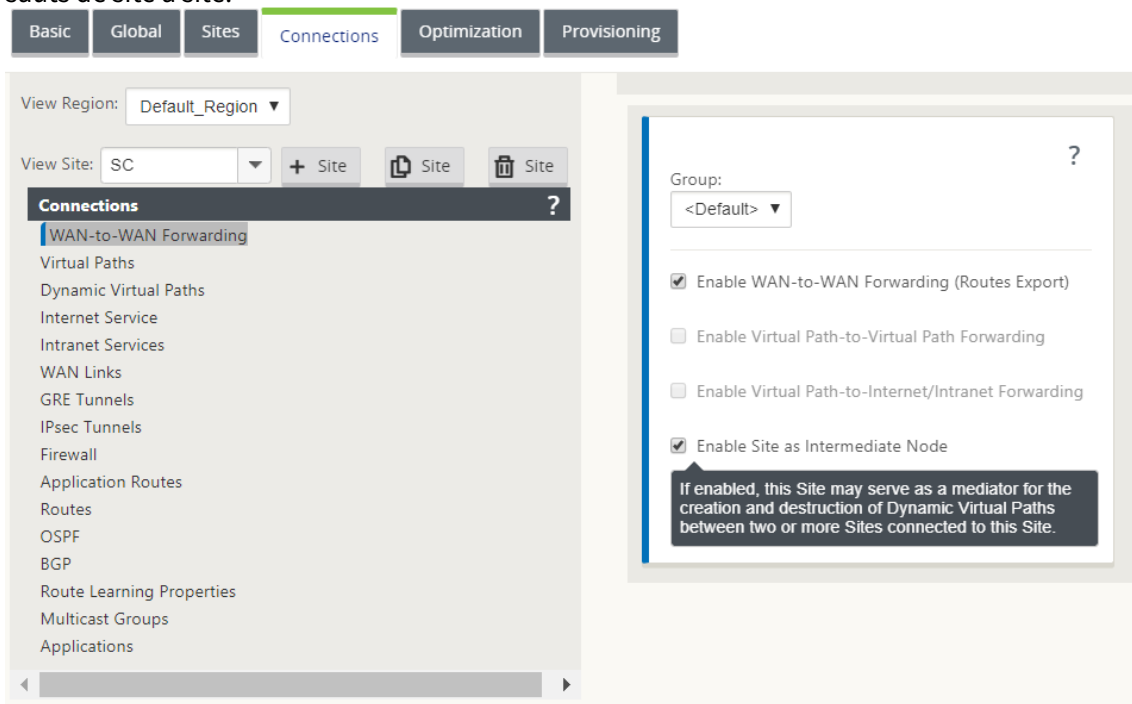
- Les chemins virtuels dynamiques sont utilisés pour les déploiements à grande échelle, tels que les entreprises
- Les déploiements plus petits utilisent des chemins virtuels statiques et tous les chemins virtuels
- Toujours utiliser des chemins virtuels statiques entre deux centres de données (DC à DC)
- Tous les chemins WAN ne doivent pas être configurés pour utiliser le chemin virtuel dynamique
- Chaque appliance SD-WAN dispose d'un nombre limité de chemins virtuels dynamiques (8 limites minimales dynamiques, 8 limites inférieures statiques = total 16) qui peuvent être configurés.

Comment activer le chemin virtuel dynamique dans l'interface graphique SD-WAN

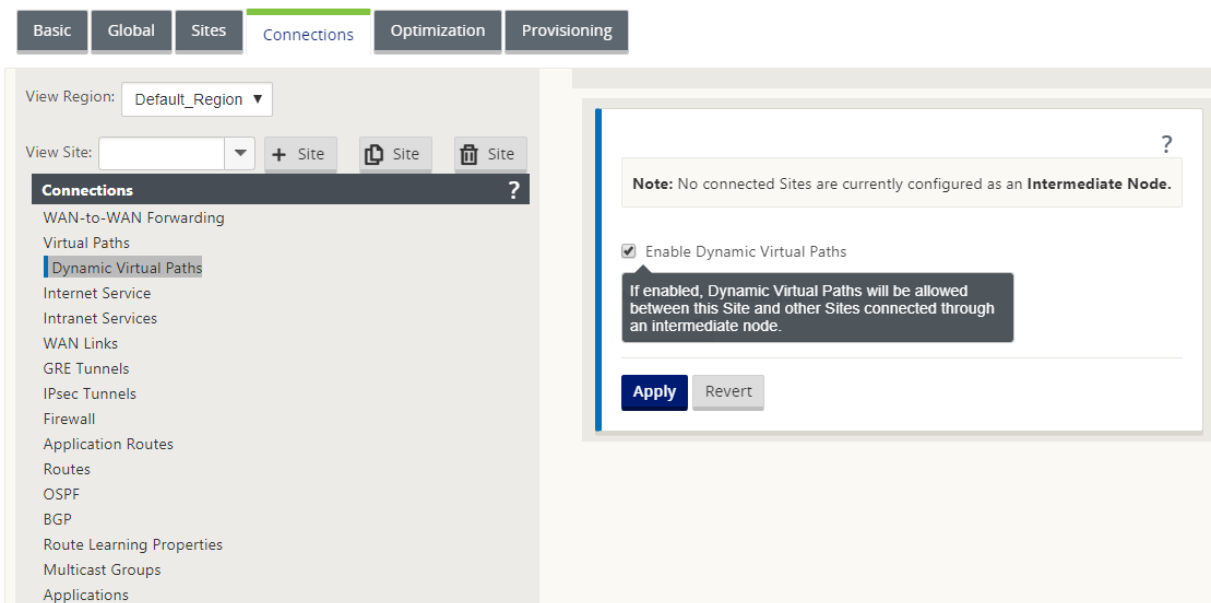
Pour activer les chemins virtuels dynamiques :

1. Dans l'interface graphique Citrix SD-WAN, sous le volet **Connexions**, créez un groupe de transfert WAN vers WAN.
2. Accédez à **Connexions > [Nom du site client] > Transfert WAN vers WAN**.

3. Activez le **transfert WAN vers WAN** pour permettre au site de servir de proxy pour un site multi-hop à site.
4. Activer le **site en tant que nœud intermédiaire**
5. Accédez à **Connexions > Site distant > Transfert WAN vers WAN**.
6. Activez le transfert WAN vers WAN pour permettre au site de servir de proxy pour plusieurs sauts de site à site.

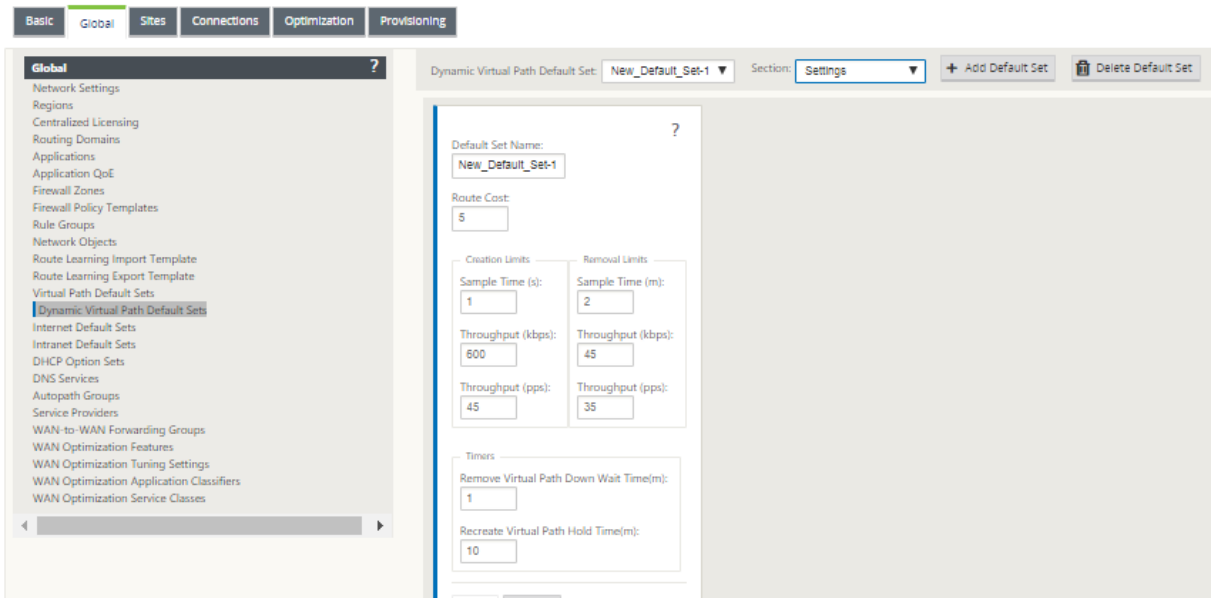


7. Accédez à **Connexions > Site distant > Chemin virtuel > Chemin virtuel dynamique**.
8. Activez les **chemins virtuels dynamiques**.
9. Définissez le nombre maximal de chemins dynamiques.



Comment créer un chemin virtuel dynamique

- La configuration détermine quand un chemin virtuel dynamique est actif ou inactif.
- Configurez l'exemple de nombre de paquets (pps) ou de bande passante (kbps) dans un délai.
- Peut être défini globalement ou avec WAN Link configuré au niveau du nœud intermédiaire.



Surveillance et dépannage

May 6, 2021

Vous pouvez utiliser l'interface de gestion Web de l'appliance Citrix SD-WAN pour surveiller et dépanner les fonctionnalités prises en charge. Vous trouverez ci-dessous les liens vers les rubriques Surveillance et dépannage applicables aux appliances Citrix SD-WAN.

[Surveillance du réseau étendu virtuel](#)

[Affichage des informations statistiques](#)

[Affichage des informations de flux](#)

[Affichage de rapports](#)

[Affichage des statistiques du pare-feu](#)

[Outil de diagnostic](#)

[Amélioration du mappage des chemins et de la](#)

[Résolution des problèmes IP de gestion](#)

[Test de la bande passante active](#)

[Détection adaptative de la bande passante](#)

Surveillance du réseau étendu virtuel

May 6, 2021

Affichage des informations de base d'une appliance

Utilisez un navigateur pour vous connecter à l'interface Web de gestion de l'appliance que vous souhaitez surveiller, puis cliquez sur l'onglet Tableau de **bord** pour afficher les informations de base relatives à cette appliance.

La page Tableau de **bord** affiche les informations de base suivantes pour l'appliance locale :

État du système :

- **Nom** : il s'agit du nom que vous avez attribué à l'appliance lorsque vous l'avez ajoutée au système.
- **Modèle** : il s'agit du numéro de modèle de l'appliance Virtual WAN.

- **Mode Appliance** : indique si cette appliance a été configurée en tant que MCN principal ou secondaire ou en tant qu'appliance client.
- **Adresse IP de gestion** : il s'agit de l'adresse IP de gestion de l'appliance.
- **Temps de disponibilité de l'appliance** : indique la durée pendant laquelle l'appliance s'exécute depuis le dernier redémarrage.
- **Service Uptime** : indique la durée pendant laquelle le service Virtual WAN s'exécute depuis le dernier redémarrage.

Statut du service de chemin d'accès virtuel :

[Nom du site]Chemin d'accès virtuel : affiche l'état de tous les chemins d'accès virtuels associés à cette appliance. Si le service WAN virtuel est activé, cette section est incluse dans la page. Si le service WAN virtuel est désactivé, une icône d'alerte (delta de la verge d'or) et un message d'alerte à cet effet s'affichent à la place de cette section.

Informations sur la version locale :

- **Version du logiciel** : il s'agit de la version du package logiciel CloudBridge Virtual Path actuellement activée sur l'appliance.
- **Build on** : il s'agit de la date de génération de la version du produit actuellement en cours d'exécution sur l'appliance locale.
- **Version matérielle** : il s'agit du numéro de modèle matériel et de la version de l'appliance.
- **Version de partition du système d'exploitation** : il s'agit de la version de la partition du système d'exploitation actuellement active sur l'appliance.

La figure ci-dessous montre un exemple de page Tableau de bord.

Dashboard	Monitoring	Configuration
<div>System Status</div> <div> Name: MCN_23 Model: VPX Sub-Model: BASE Appliance Mode: MCN Serial Number: 67e0772c-5190-a2ee-d183-9244189b30a0 Management IP Address: 10.102.78.154 Appliance Uptime: 6 days, 13 hours, 22 minutes, 23.0 seconds Service Uptime: 6 days, 13 hours, 14 minutes, 46.0 seconds Routing Domain Enabled: Default_RoutingDomain </div>		
<div>Local Versions</div> <div> Software Version: 10.1.0.111.690027 Built On: Jun 21 2018 at 23:42:30 Hardware Version: VPX OS Partition Version: 4.6 </div>		
<div>Virtual Path Service Status</div> <div> Virtual Path MCN_23-Site1: Uptime: 6 days, 13 hours, 11 minutes, 45.0 seconds. </div>		

Affichage des informations statistiques

May 6, 2021

Cette section fournit des instructions de base pour l’affichage des informations sur les statistiques de réseau étendu virtuel.

1. Connectez-vous à l’interface Web de gestion du MCN.
2. Sélectionnez l’onglet **Surveillance**.

L’arborescence de navigation **Monitoring** s’ouvre dans le volet gauche. Par défaut, la page **Statistiques** affiche également les **chemins d’accès présélectionnés** dans le champ **Afficher**. Il contient un tableau détaillé des statistiques de chemin d’accès.

Remarque

Si vous accédez à une autre page **Surveillance** (par exemple, **Flux**), vous pouvez revenir à cette page en sélectionnant **Statistiques** dans l’arborescence de navigation **Surveillance** (volet gauche).

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	MCN-DC-WL-1	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	59.95	NO
2	MCN-DC-WL-1	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	8.72	NO
3	MCN-DC-WL-2	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	8.72	NO
4	MCN-DC-WL-2	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	11.82	NO
5	Branch1-WL-1	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	8.89	NO
6	Branch1-WL-1	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	25.19	NO
7	Branch1-WL-2	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	11.84	NO
8	Branch1-WL-2	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	8.73	NO

Avec la version 11.1.0, l’option NDP (Neighbor Discovery Protocol) est ajoutée pour le débogage des problèmes de découverte de voisins.

1. Sélectionnez l’option NDP dans le menu déroulant Afficher et vous pouvez afficher l’état de NDP ainsi que les adresses IPv6.

Statistics

Show: NDP

Enable Auto Refresh

 5 seconds

Refresh

NDP Statistics

Filter:

Any column

Apply

Show 100 entries Showing 1 to 2 of 2 entries

First

Previous

 1

Next

Last

Num	Interface	VLAN	IP Addr	MAC Addr	Type	State	Is Router	Clear NDP Entry
0	2	0	2607:f0d0:2001:a::20	02:63:d7:64:85:4e	PERSISTENT	NDP_STATE_REACHABLE	Y	
1	2	0	fe80::63:d7ff:fe64:854e	02:63:d7:64:85:4e	END_USER	NDP_STATE_STALE	N	<div>Clear</div>

Showing 1 to 2 of 2 entries

First

Previous

 1

Next

Last

2. Sélectionnez Lien WAN dans le menu déroulant. Vous pouvez également afficher l'adresse IPv6 si vous avez configuré sous l'onglet Adresse IP.

Statistics

Show: WAN Link

Enable Auto Refresh

 5 seconds

Refresh

Show latest data.

WAN Link Statistics

Filter:

Any column

Apply

Show 100 entries Showing 1 to 6 of 6 entries

First

Previous

 1

Next

Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
demo_cl1_inet	N/A	2607:f0d0:2001:b::10	N/A	N/A	N/A	N/A
demo_cl1_inet2	N/A	172.16.100.1	N/A	N/A	N/A	N/A
demo_cl2_inet	N/A	2607:f0d0:2001:c::10	N/A	N/A	N/A	N/A
demo_cl2_inet2	N/A	172.16.150.1	N/A	N/A	N/A	N/A
demo_mcn_inet	demo_mcn_inet-AI-1	2607:f0d0:2001:a::10	N/A	N/A	N/A	N/A
demo_mcn_inet2	demo_mcn_inet2-AI-1	172.16.200.1	N/A	DISABLED	N/A	N/A

Showing 1 to 6 of 6 entries

First

Previous

 1

Next

Last

Virtual Path Service Data Rates

Filter:

Any column

Apply

3. Vous pouvez également afficher les statistiques de l'interface d'accès.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Statistics

Statistics

Show: Access Interfaces

Enable Auto Refresh

 5 seconds

Refresh

Show latest data.

Access Interface Statistics

Filter:

Any column

Apply

Show 100 entries Showing 1 to 2 of 2 entries

First

Previous

 1

Next

Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
demo_mcn_inet	demo_mcn_inet-AI-1	2607:f0d0:2001:a::10	N/A	N/A	N/A	N/A
demo_mcn_inet2	demo_mcn_inet2-AI-1	172.16.200.1	N/A	N/A	N/A	N/A

Showing 1 to 2 of 2 entries

First

Previous

 1

Next

Last

Virtual Path Service Data Rates:

Filter:

Any column

Apply

Show 100 entries Showing 1 to 8 of 8 entries

First

Previous

 1

Next

Last

WAN Link	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved
demo_mcn_inet	demo_mcn_inet-AI-1	demo_mcn-demo_cl2	Recv	20220845	3240115.88	413	74.23	46.47	0
demo_mcn_inet	demo_mcn_inet-AI-1	demo_mcn-demo_cl1	Recv	20196856	3252489.44	289	30.05	18.82	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

961

4. Ouvrez le menu déroulant **Afficher**.

En plus des **statistiques** Chemins, NDP, Access Interface et **WAN Links**, le menu **Afficher** offre plusieurs options supplémentaires de filtrage et d’affichage des informations statistiques.

Statistics

Flows

Routing Protocols

Firewall

IKE/Ipsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRPP Protocol

Monitoring > Statistics

Statistics

Show Paths (Summary) Enable Auto Refresh 5 seconds Refresh Show latest data.

Filter

Access Interfaces

Applications

ARP

Classes

Virtual Path Services

Ethernet

Ethernet MAC Learning

Intranet

Observed Protocols

1 Paths (Summary)

2 Paths (Detailed)

3 Routes

4 Application QoS

5 Rules

6 Rule Groups

7 Site

8 WAN Link

9 MPLS Clouds

10 WAN Link Usage

To Link

Path State

Virtual Path Service State

Virtual Path Service Type

BOWT

Jitter (mS)

Loss %

kbps

Congestion

Branch1-WL-1

GOOD

GOOD

Static

2

3

0.00

59.95

NO

Branch1-WL-2

GOOD

GOOD

Static

2

3

0.00

8.72

NO

Branch1-WL-1

GOOD

GOOD

Static

2

3

0.00

8.72

NO

Branch1-WL-2

GOOD

GOOD

Static

2

3

0.00

11.82

NO

MCN-DC-WL-1

GOOD

GOOD

Static

2

3

0.00

8.89

NO

MCN-DC-WL-2

GOOD

GOOD

Static

2

3

0.00

25.19

NO

Branch1-WL-1

GOOD

GOOD

Static

2

3

0.00

11.84

NO

MCN-DC-WL-1

GOOD

GOOD

Static

2

3

0.00

8.73

NO

Showing 1 to 8 of 8 entries

Bandwidth calculated over the last 41278.42 seconds

First Previous 1 Next Last

Sélectionnez un filtre dans le menu **Afficher** pour afficher un tableau d’informations statistiques pour cette rubrique.

Affichage des informations de flux

February 8, 2022

Cette section fournit des instructions de base pour afficher les informations de flux WAN virtuel.

Pour afficher les informations de flux, procédez comme suit :

1. Connectez-vous à l’interface Web de gestion du MCN, puis sélectionnez l’onglet **Surveillance** . Il ouvre l’arborescence de navigation **Surveillance** dans le volet gauche.
2. Sélectionnez la branche **Flux** dans l’arborescence de navigation. Elle affiche la page **Flux** avec **LAN to WAN** présélectionné dans le champ **Type de flux**.

Statistics

Flows

Routing Protocols

Firewall

IKE/Ipsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRPP Protocol

Monitoring > Flows

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): Help

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

Toggle Columns

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Typ
172.147.21.53	172.147.12.83	LAN to WAN	2312	50829	TCP	default	3	Virtual Path	MCN-DC-Branch1	LOCAL	5292	2	104	0.237	0.099	0.100	0.000	65	N/A	13	INTERACT
172.147.12.83	172.147.21.53	WAN to LAN	50829	2312	TCP	default	3	Virtual Path	MCN-DC-Branch1	LOCAL	5328	3	180	0.355	0.170	0.151	0.000	132	N/A	N/A	

Total LAN to WAN flows displayed: 1 out of 1
Total WAN to LAN flows displayed: 1 out of 1

3. Sélectionnez le **type de flux**. Le champ **Type de flux** se trouve dans la section **Sélectionner les flux** en haut de la page **Flux** . En regard du champ **Type de flux** se trouve une ligne d’options de case à cocher permettant de sélectionner les informations de flux que vous souhaitez afficher. Vous pouvez cocher une ou plusieurs cases pour filtrer les informations à afficher.
4. Sélectionnez le **Flux maximum à afficher** dans le menu déroulant situé à côté de ce champ.
5. Il détermine le nombre d’entrées à afficher dans la table **Flux**. Les options sont : **50, 100, 1000**.
6. (Facultatif) Entrez le texte de recherche dans le champ **Filtre** . Il filtre les résultats du tableau de sorte que seules les entrées contenant le texte de recherche s’affichent dans le tableau.

Conseil

Pour obtenir des instructions détaillées sur l’utilisation de filtres pour affiner les résultats de la table de **flux**, cliquez sur **Aide** à droite du champ **Filtre** . Pour fermer l’écran d’aide, cliquez sur **Actualiser** dans le coin inférieur gauche de la section **Sélectionner les flux** .

7. Cliquez sur **Actualiser** pour afficher les résultats du filtre. La figure présente un exemple d’affichage filtré de page **Flux** avec tous les types de flux sélectionnés.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☒ Internet Load Balancing Table☒ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

172.79.2.83

Help

Refresh

Flows Data

Toggle Columns

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	TCP	default	9577	Virtual Path	DC-BR	LOCAL	5332	12038	1020734	0.079	0.033	0.031
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	TCP	default	9631	Virtual Path	DC-BR	LOCAL	5346	12199	1075706	0.079	0.033	0.031
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	TCP	default	18025	Virtual Path	DC-BR	LOCAL	5346	18025	1294598	0.157	0.052	0.062
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	TCP	default	18244	Virtual Path	DC-BR	LOCAL	5360	18244	1389118	0.157	0.052	0.062

Total LAN to WAN flows displayed: 2 out of 305

Total WAN to LAN flows displayed: 2 out of 305

Internet Load Balancing Flows

LAN IP	WAN IP	Age (mS)	WAN Link	Flow Count
--------	--------	----------	----------	------------

Note: Only the active flows will be displayed and the total number of flows include active and inactive flows.

TCP Terminated Flows

Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Age (mS)	From Wan kbps	To Wan kbps	Bytes Pending To LAN	Bytes Pending To WAN	State
-------------------	-----------------	-------------	-----------	-----	----------	---------------	-------------	----------------------	----------------------	-------

Total TCP Terminated flows displayed: 0 out of 305

8. (Facultatif) Sélectionnez les colonnes à inclure dans le tableau. Procédez comme suit :
9. Cliquez sur **Basculer les colonnes** dans le coin supérieur droit du tableau **Données de flux** . Il affiche toutes les colonnes désélectionnées et ouvre une case à cocher au-dessus de chaque

colonne pour sélectionner ou désélectionner cette colonne. Les colonnes désélectionnées s’affichent en grisé, comme le montre la figure.

Remarque

Par défaut, toutes les colonnes sont sélectionnées, ce qui peut entraîner la tronque de la table dans l’affichage, masquant le bouton **Basculer les colonnes**. Si tel est le cas, une barre de défilement horizontale s’affiche sous le tableau. Faites glisser la barre de défilement vers la droite pour afficher la section tronquée du tableau et faire apparaître le bouton **Basculer les colonnes** . Si la barre de défilement n’est pas disponible, essayez de redimensionner la largeur de la fenêtre de votre navigateur jusqu’à ce que la barre de défilement soit affichée.

Monitoring > Flows

Balancing Table

TCP Termination Table

Apply

Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
9598	Virtual Path	DC-BR	LOCAL	2435	12065	1023038	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
9652	Virtual Path	DC-BR	LOCAL	2434	12226	1078010	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
18064	Virtual Path	DC-BR	LOCAL	2448	18064	1297454	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable
18283	Virtual Path	DC-BR	LOCAL	2447	18283	1391974	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable

10. Activez une case à cocher pour sélectionner ou désélectionner une colonne.

- **Adresse IP source** : adresse IP source pour les paquets de ce flux.
- **Adresse IP Dest** : adresse IP de destination pour les paquets de ce flux.
- **Direction** - La direction des paquets sur ce flux - LAN vers WAN ou WAN vers LAN.
- **Port source**: port source pour les paquets de ce flux.
- **Port de destination** : port de destination des paquets de ce flux.
- **IPP** : numéro de protocole IP pour les paquets de ce flux.
- **IP DSCP** : paramètre de balise IP DSCP pour les paquets de ce flux.
- **Nombre d’accès** : nombre de fois où ce flux a été recherché et trouvé.
- **Type de service** : indique si ce type de flux est un chemin d’accès virtuel, Internet ou un trafic intranet.

- **Nom du service** : nom du chemin virtuel utilisé par le trafic du chemin d'accès virtuel.
- **IP LAN GW** : adresse IP de la passerelle LAN, si elle est spécifiée.
- **Age (mS)** : temps (en millisecondes) écoulé depuis qu'un paquet a été classé dans ce flux.
- **Paquets** : nombre de paquets envoyés pendant la durée de vie du flux.
- **Bytes** : nombre d'octets envoyés pendant la durée de vie du flux.
- **PPS** : paquets par seconde sur la période écoulée depuis le dernier rafraîchissement.
- **Kbits/s client/ Kbits/s de surcharge de chemin virtuel / Kbits/s de surcharge IPsec** - Kilobits par seconde sur la période écoulée depuis la dernière actualisation.
- **ID de règle** : ID de la règle à laquelle le trafic de ce flux correspondait.
- **ID de règle d'application** : ID de l'application de la règle à laquelle le trafic de ce flux correspondait.
- **Classe** : ID de la classe de chemin virtuel utilisée par le trafic.
- **Type de classe** : type de classe de chemin virtuel (temps réel, interactif, groupé) utilisé par le trafic.
- **Path** - Le chemin emprunté par le trafic.
- **Octets enregistrés par compression Hdr** - Le nombre d'octets enregistrés en raison de la compression d'en-tête.
- **Type de transmission** : type de transmission utilisé par le trafic.
- **Application** : nom de l'application en cours d'utilisation.

11. Cliquez sur **Appliquer** (au-dessus du coin supérieur droit du tableau). Il rejette les options de sélection et actualise la table pour inclure uniquement les colonnes sélectionnées.

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table
Max Flows to Display (Per Flow Type):
Filter (Optional): [Help](#)

Flows Data

Toggle Columns

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	9613	Virtual Path	DC-BR	LOCAL	12022	12084	1024626
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	9667	Virtual Path	DC-BR	LOCAL	12040	12246	1080066
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	18092	Virtual Path	DC-BR	LOCAL	12040	18092	1299440
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	18312	Virtual Path	DC-BR	LOCAL	12056	18312	1394758

Total LAN to WAN flows displayed: 2 out of 306
Total WAN to LAN flows displayed: 2 out of 306

Applications DPI dans SD-WAN Center

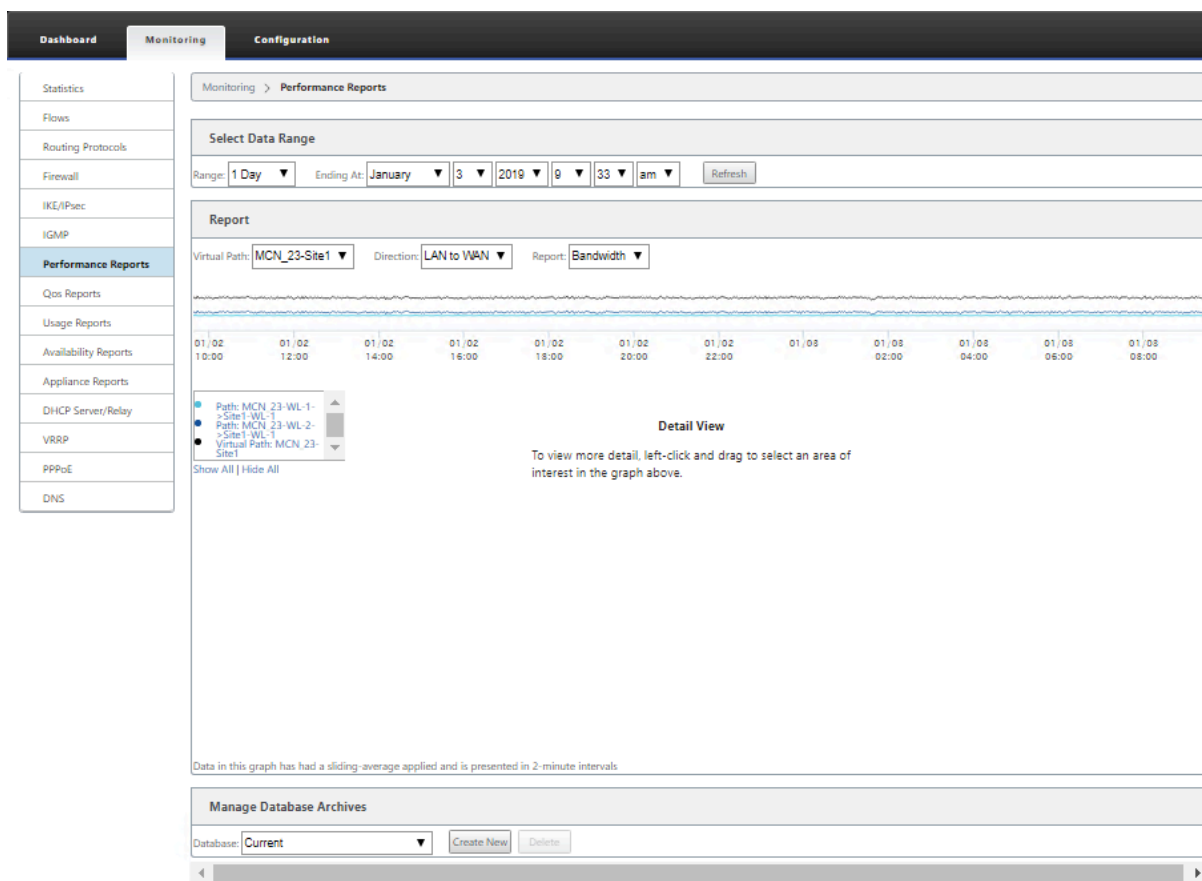
Dans les versions antérieures, environ 4 000 applications et configurées avec 800 services (550 chemins virtuels, 256 services intranet) peuvent être identifiées. Le stockage de ces données aurait un impact sur les performances globales du système (cycles CPU et espace disque requis pour stocker les données). Il a également un impact, si le reporting sur les données par utilisation ou chemin est pris en charge.

Alors que le chemin de données fournit des informations sur chaque application recueillie en une minute, le rapport de statistiques par minute détermine les 100 applications les plus importantes et le rapport sur l'ensemble de toutes les autres applications en tant que « autre ». S'il y a une grande diversité d'applications traçables dans leur réseau, cela peut affecter la clarté des données, en particulier si nous voulons suivre l'utilisation d'une application au fil du temps et que l'application tombe hors de la limite supérieure des 100.

Affichage de rapports

May 6, 2021

Cette section fournit des instructions de base pour la génération et l'affichage des rapports Virtual WAN sur l'appliance locale à l'aide de l'interface Web de gestion. Une appliance peut conserver jusqu'à 30 archives et purger les archives les plus anciennes qui comptent plus de 30 entrées.



Remarque

Les rapports générés sur l'interface Web de gestion s'appliquent uniquement à l'appliance locale. Pour générer et afficher des rapports pour le réseau WAN virtuel, utilisez l'interface Web du centre WAN virtuel.

Pour générer et afficher des rapports Virtual WAN, procédez comme suit :

1. Connectez-vous à l'interface Web de gestion du MCN, puis sélectionnez l'onglet **Surveillance**.
L'arborescence de navigation **Monitoring** s'ouvre dans le volet gauche.

2. Sélectionnez un type de rapport dans l'arborescence de navigation.

Les types de rapports sont répertoriés en tant que branches dans l'arborescence de navigation, juste en dessous de la succursale **Flux**.



Les types de rapport disponibles sont les suivants :

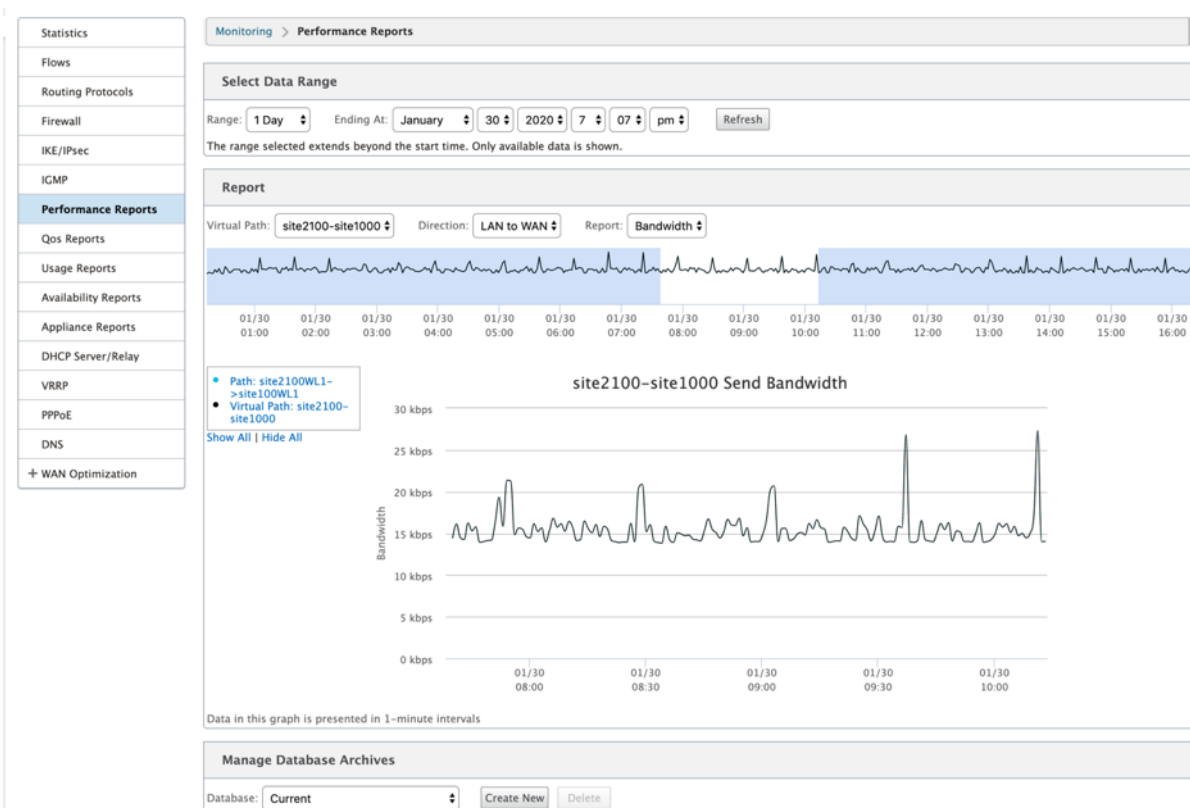
- **Rapports sur le rendement**
- **Rapports QoS**
- **Rapports d'utilisation**
- **Rapports de disponibilité**
- **Rapports sur les appliances**

3. Sélectionnez les options du rapport.

Outre les différents types de rapports, pour chaque type de rapport, il existe de nombreuses options et filtres pour affiner les résultats des rapports.

Rapports sur le rendement

Citrix SD-WAN peut afficher des statistiques de performances au niveau du site, du chemin virtuel ou de la direction (LAN vers WAN et WAN vers LAN). Avec Citrix SD-WAN, vous pouvez collecter des mesures qui montrent l'efficacité de chaque lien en millisecondes. Pour afficher plus de détails, cliquez avec le bouton gauche de la souris et sélectionnez une zone spécifique de chemin ou de période dans la ligne du graphique.

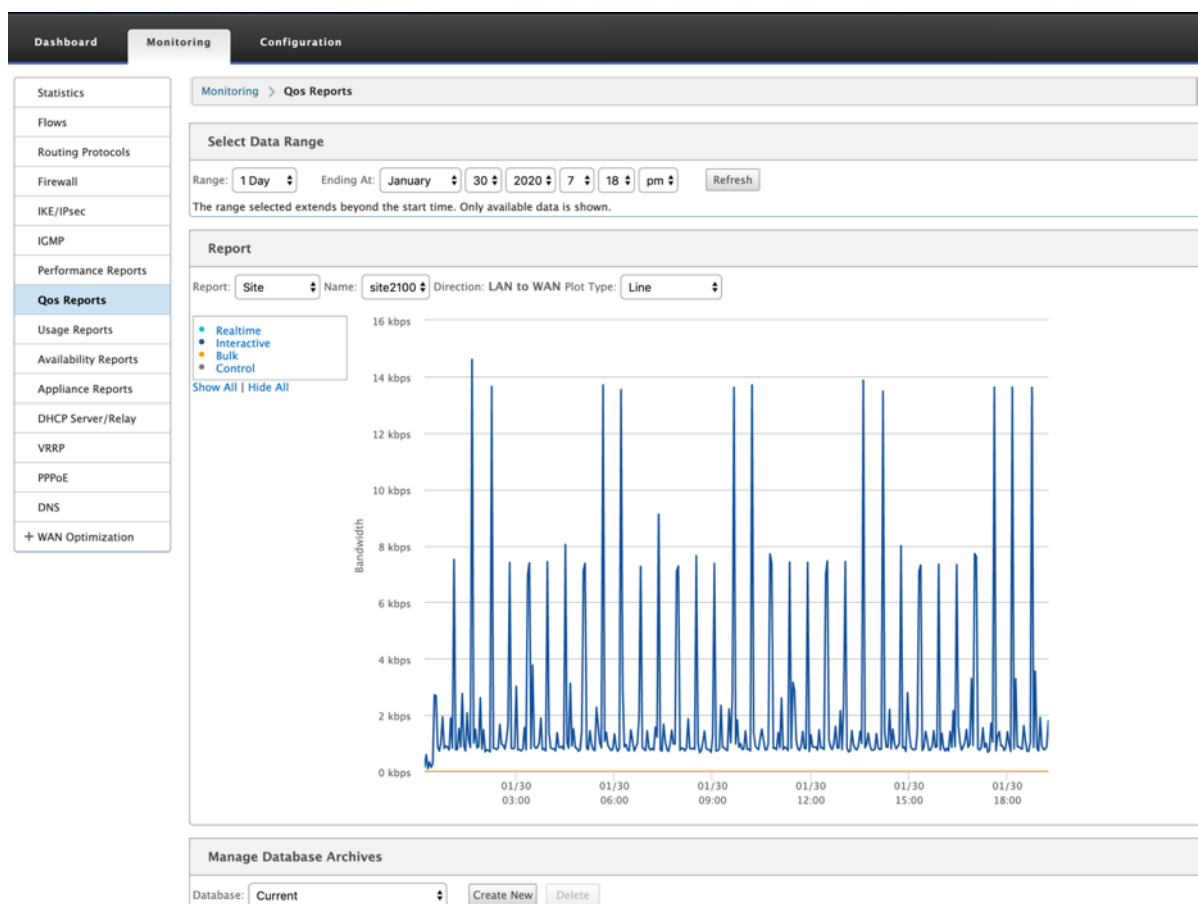


Vous pouvez sélectionner la plage de données selon vos besoins avec les champs suivants pour afficher le rapport de performances :

- **Chemin virtuel** : sélectionnez le chemin virtuel dans la liste déroulante.
- **Direction** : Sélectionnez la direction selon vos besoins (LAN vers WAN ou WAN vers LAN).
- **Rapport** : sélectionnez les paramètres réseau suivants pour afficher le rapport :
 - Bande passante
 - Latence
 - Variation
 - Perte
 - Qualité

Rapports QoS

Vous pouvez surveiller le rapport QoS de l'application, tel que le nombre de paquets ou d'octets téléchargés, téléchargés ou supprimés à chaque niveau de site, de lien WAN, de chemin virtuel et de chemin d'accès.

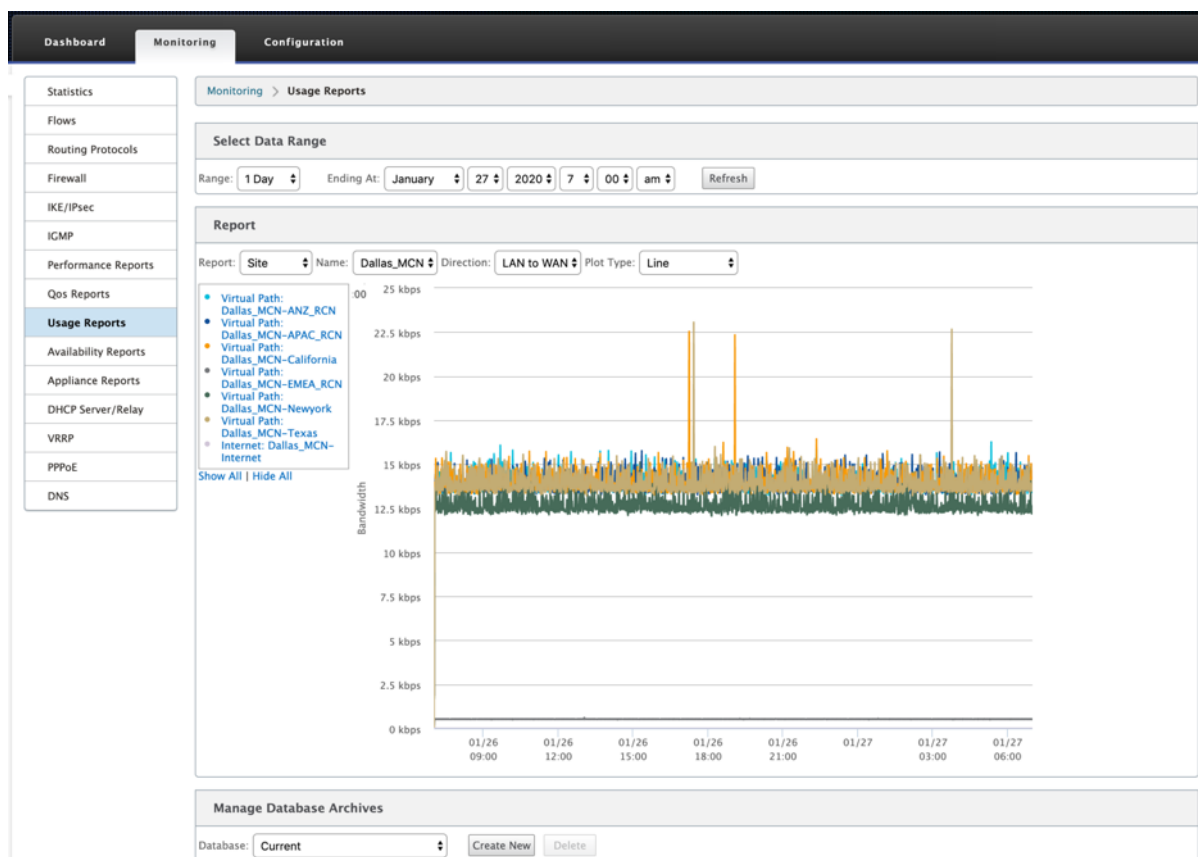


Vous pouvez afficher les mesures suivantes :

- **Temps réel** : Bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration Citrix SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau. Un paquet retardé est pire qu'un paquet perdu (par exemple, VoIP, Skype for Business).
- **Interactif** : Bande passante consommée par les applications appartenant au type de classe interactif dans la configuration Citrix SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau et de la perte de paquets (par exemple, XenDesktop, XenApp).
- **En vrac** : Bande passante consommée par les applications appartenant au type de classe en bloc dans la configuration Citrix SD-WAN. Ces applications impliquent peu d'intervention humaine et sont principalement gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).
- **Contrôle** : Bande passante utilisée pour transférer des paquets de contrôle contenant des informations de routage, de planification et de liaison statistiques.

Rapports d'utilisation

Les rapports d'utilisation fournissent les informations d'utilisation des chemins virtuels.



- **Rapport** : sélectionnez **Site** ou **WAN Link** dans la liste déroulante pour afficher le rapport.

- **Nom :** Sélectionnez le nom du site ou du lien WAN dans la liste déroulante.
- **Direction :** Sélectionnez la direction requise (LAN vers WAN ou WAN vers LAN).
- **Type de tracé :** sélectionnez le type de tracé dans la liste déroulante (Ligne ou Zone).

Rapports de disponibilité

Dans ce rapport, vous pouvez afficher les données de disponibilité des liens WAN, chemins d'accès et chemins d'accès virtuels. Vous pouvez également passer ou choisir une période spécifique, telle que 1 heure, 24 heures et 7 jours pour afficher les données disponibles. Les données Paths et Chemins virtuels sont représentées au format **DD:HH:MM:SS**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Availability Reports

Select Timeframe

For the period from 7:01 on 1/26/2020 to 7:01 on 1/27/2020 | Switch to: 1 hour | 24 hours | 7 days | All Available Data

All times are represented in days (if available), hours (if available), minutes and seconds. DD:HH:MM:SS

Paths and Virtual Paths

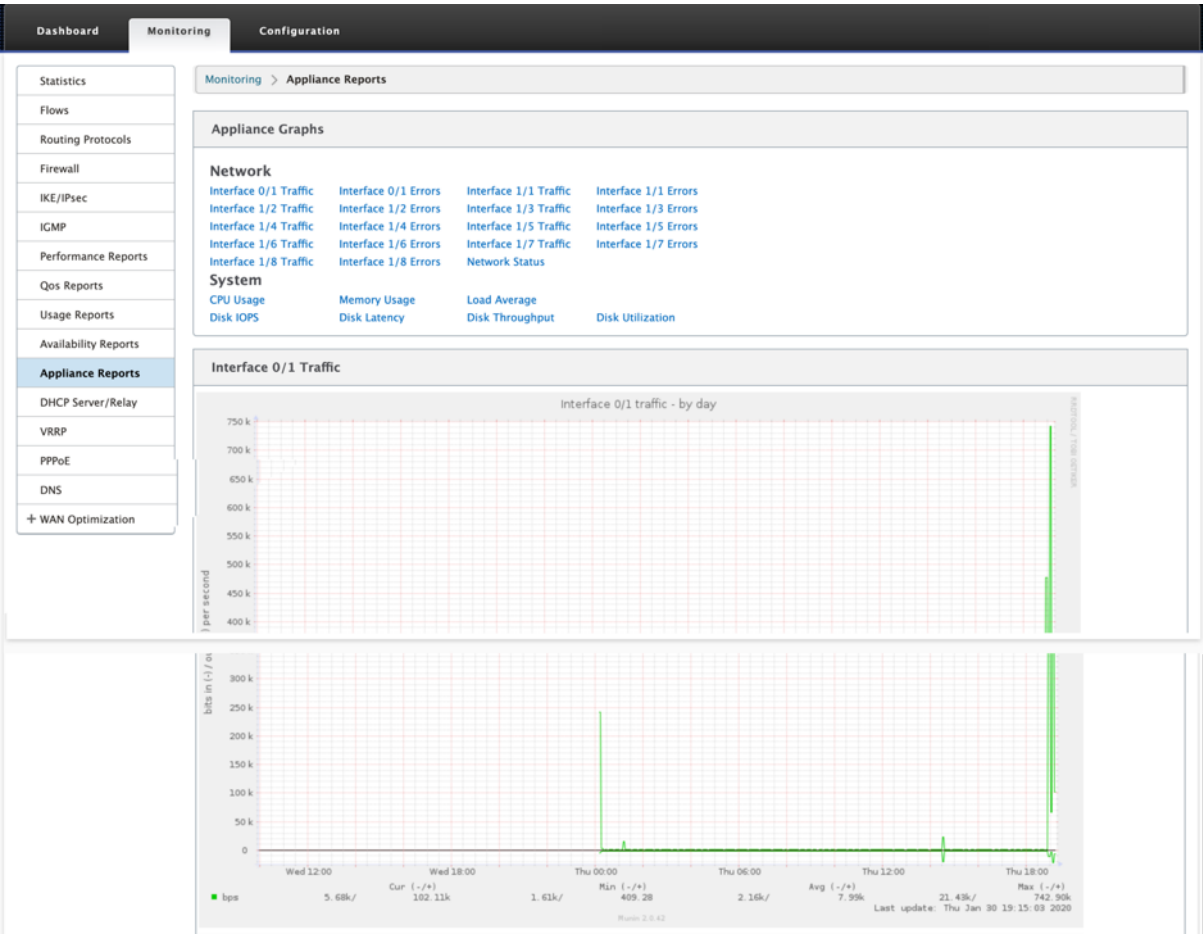
	Uptime	Goodtime	Badtime				Downtime			Incidents			
			Total	Loss	Silence	Peer	Total	Silence	Peer	Total	Loss	Silence	Peer
Virtual Path Dallas_MCN-ANZ_RCN	1:00:00:00	1:00:00:00	0:00	0:00	5								
Dallas_MCN-queue1->ANZ_RCN-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
ANZ_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:10	0:50	0:00	0:50	---	0:00	0:00	---	5	0	5	---
Virtual Path Dallas_MCN-APAC_RCN	1:00:00:00	1:00:00:00	0:00	0:00	14								
Dallas_MCN-queue1->APAC_RCN-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
APAC_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:57:40	2:20	0:00	2:20	---	0:00	0:00	---	14	0	14	---
Virtual Path Dallas_MCN-California	1:00:00:00	23:59:42	0:18	0:00	2								
Dallas_MCN-queue1->California-queue1	23:58:36	23:58:36	0:00	---	0:00	0:00	0:00	0:00	0:00	2	---	0	2
California-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:40	0:20	0:00	0:20	---	0:00	0:00	---	2	0	2	---
Virtual Path Dallas_MCN-EMEA_RCN	0:00	0:00	0:00	1:00:00:00	0								
Dallas_MCN-queue1->EMEA_RCN-queue2	0:00	0:00	0:00	---	0:00	0:00	1:00:03:45	1:00:03:45	0:00	0	---	0	0
EMEA_RCN-queue2->Dallas_MCN-queue1	0:00	0:00	0:00	0:00	0:00	---	1:00:03:45	1:00:03:45	---	0	0	0	---
Virtual Path Dallas_MCN-Newyork	1:00:00:00	1:00:00:00	0:00	0:00	8								
Dallas_MCN-WL-2->Newyork-WL-2	0:00	0:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
Dallas_MCN-queue1->Newyork-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
Newyork-WL-2->Dallas_MCN-WL-2	0:00	0:00	0:00	0:00	0:00	---	1:00:03:45	1:00:03:45	---	0	0	0	---
Newyork-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:40	1:20	0:00	1:20	---	0:00	0:00	---	8	0	8	---
Virtual Path Dallas_MCN-Texas	1:00:00:00	23:59:42	0:18	0:00	12								
Dallas_MCN-queue1->Texas-queue1	23:58:35	23:58:35	0:00	---	0:00	0:00	0:00	0:00	0:00	2	---	0	2
Texas-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:00	2:00	0:00	2:00	---	0:00	0:00	---	12	0	12	---

WAN Links

	Uptime	Downtime	Incidents
Dallas_MCN-WL-2	0:00	1:00:00:00	1
Dallas_MCN-queue1	1:00:00:00	0:00	No downtime

Rapports de l'appliance

Le rapport Appliance fournit des rapports sur le trafic réseau et l'utilisation du système. Cliquez sur chaque lien pour afficher ou surveiller le graphique de l'appliance par jour, hebdomadaire, mensuel et annuel.



Affichage des statistiques du pare-feu

May 6, 2021

Une fois que vous avez configuré les stratégies de pare-feu et NAT, vous pouvez afficher les statistiques des connexions, des stratégies de pare-feu et des stratégies NAT sous forme de rapports. Vous pouvez filtrer les rapports à l'aide des différents paramètres de filtrage.

Pour plus d'informations sur la configuration des stratégies de pare-feu et NAT, reportez-vous à la section [Prise en charge du pare-feu avec état et NAT](#).

Connexions

Vous pouvez vérifier les statistiques pour Applications pour la stratégie de pare-feu. Cela vous permet de voir toutes les connexions qui correspondent à l'application sélectionnée, d'où elles viennent, où

elles vont et combien de trafic elles génèrent. Vous pouvez voir comment les stratégies de pare-feu agissent sur le trafic de chaque application.

Vous pouvez filtrer les statistiques de connexions à l'aide des paramètres suivants :

- Application - Application utilisée comme critère de filtre pour la connexion.
- Famille - Famille d'applications utilisée comme critère de filtre pour la connexion.
- Protocole IP - Protocole IP utilisé par la connexion.
- Zone source - Zone d'origine de la connexion.
- Zone de destination - Zone d'où provient le trafic répondant.
- Type de service source - Service d'origine de la connexion.
- Instance de service source - Instance du service d'origine de la connexion.
- IP source - Adresse IP d'origine de la connexion, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.
- Port source - Port ou plage de ports d'origine de la connexion. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.
- Type de service de destination - Service à partir duquel provient le trafic répondant.
- Instance de service de destination : instance du service d'où provient le trafic répondant.
- IP de destination - Adresse IP du périphérique répondant, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.
- Port de destination - Port ou plage de ports utilisés par le périphérique répondant. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.

Stratégies de filtrage

Les stratégies vous permettent de spécifier des actions pour les flux de trafic. Le groupe de filtres de pare-feu est créé à l'aide de modèles de stratégie de pare-feu et peut être appliqué à tous les sites du réseau ou uniquement à des sites spécifiques.

Vous pouvez afficher le rapport de statistiques pour toutes les stratégies de filtrage et le filtrer à l'aide des paramètres suivants.

- Objet Application : objet Application utilisé comme critère de filtre dans la stratégie de pare-feu.
- Application : application utilisée comme critère de filtre dans la stratégie de pare-feu
- Famille : famille d'applications utilisée comme critère de filtre dans la stratégie de pare-feu.
- Protocole IP - Protocole IP correspondant à la stratégie de filtre.
- DSCP : balise DSCP correspondant à la stratégie de filtre.
- Action de la stratégie de filtrage - Action effectuée par la stratégie lorsqu'un paquet correspond au filtre.
- Type de service source - Service d'origine de la connexion.
- Nom du service source : instance du service d'origine de la connexion.

- IP source - Adresse IP d'origine de la connexion, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.
- Port source - Port ou plage de ports d'origine de la connexion. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.
- Type de service de destination - Service auquel le trafic de réponse est destiné.
- Nom du service de destination - Le cas échéant, service auquel le trafic de réponse est destiné.
- IP de destination - Adresse IP du périphérique répondant, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.
- Port de destination - Port ou plage de ports utilisés par le périphérique répondant. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.
- Zone source - Zone d'origine correspondant à la stratégie de filtre.
- Zone de destination - Zone de réponse correspondant à la stratégie de filtre.

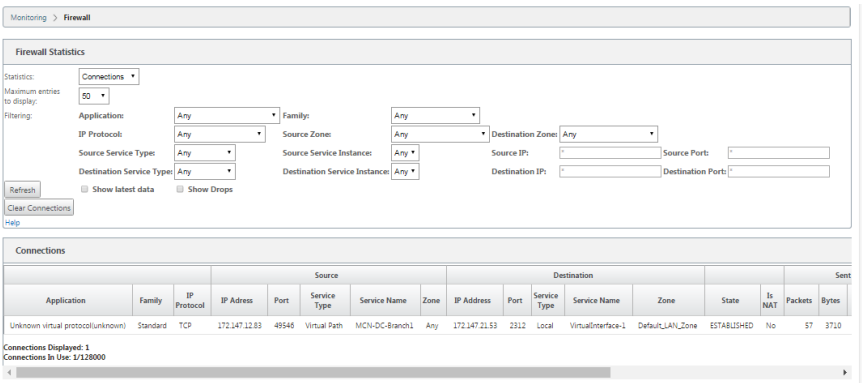
Stratégies NAT

Vous pouvez afficher les statistiques de toutes les stratégies NAT (Network Address Translation) et filtrer le rapport à l'aide des paramètres suivants.

- Protocole IP - Protocole IP correspondant à la stratégie NAT.
- Type NAT - Type de NAT utilisé par la stratégie NAT.
- Type NAT dynamique - Type de NAT dynamique utilisé par la stratégie NAT.
- Type de service : type de service utilisé par la stratégie NAT.
- Nom du service : instance du service utilisé par la stratégie NAT.
- Inside IP - L'adresse IP interne, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.
- Port intérieur- Plage de ports interne utilisée par la stratégie NAT. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.
- IP extérieure - Adresse IP extérieure, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.
- Port externe - Plage de ports externe utilisée par la stratégie NAT. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.

Pour afficher les statistiques du pare-feu :

1. Accédez à **Surveillance > Pare-feu**.
2. Dans le champ Statistiques, sélectionnez **Connexions, Stratégies de filtrage ou Stratégies NAT** selon les besoins.
3. Définissez les critères de filtrage selon les besoins.



4. Cliquez sur **Actualiser**.

Diagnostics

August 31, 2022

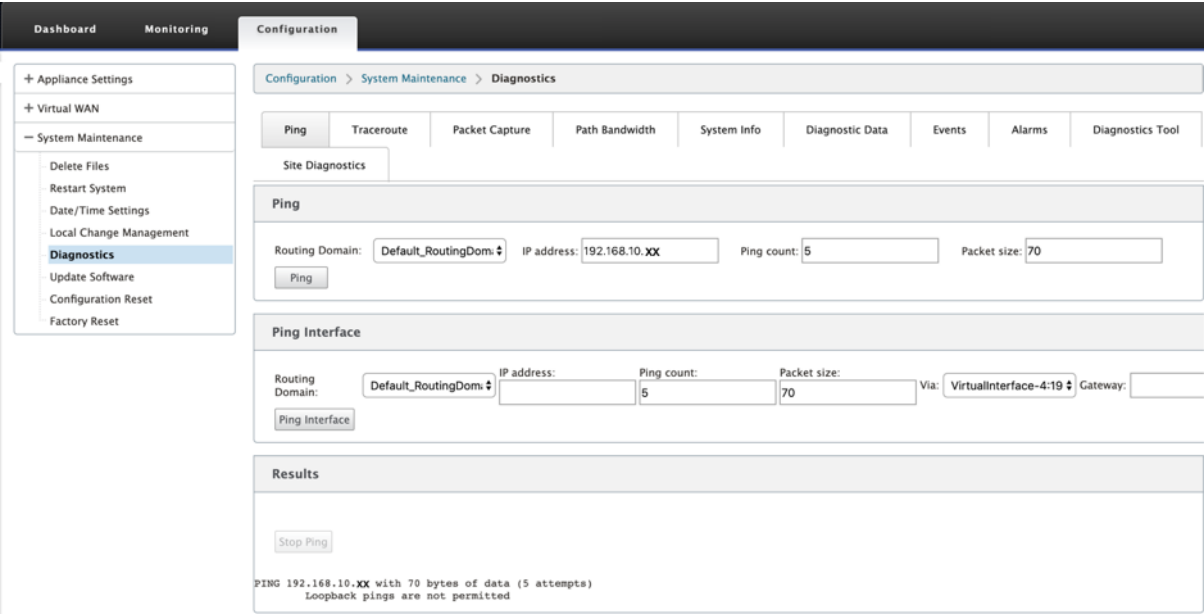
Les utilitaires **Citrix SD-WAN Diagnostics** offrent les options suivantes pour tester et examiner les problèmes de connectivité :

- Ping
- Traceroute
- Capture de paquets
- Bande passante du chemin
- Infos système
- Données de diagnostic
- Événements
- Alarmes
- Outil de diagnostic
- Diagnostics du

Les options de diagnostic du tableau de **bord Citrix SD-WAN** contrôlent la collecte des données.

Ping

Pour utiliser l'option **Ping**, accédez à **Configuration > Diagnostics** et sélectionnez **Ping**. Vous pouvez utiliser Ping pour vérifier l'accessibilité de l'hôte et la connectivité réseau.

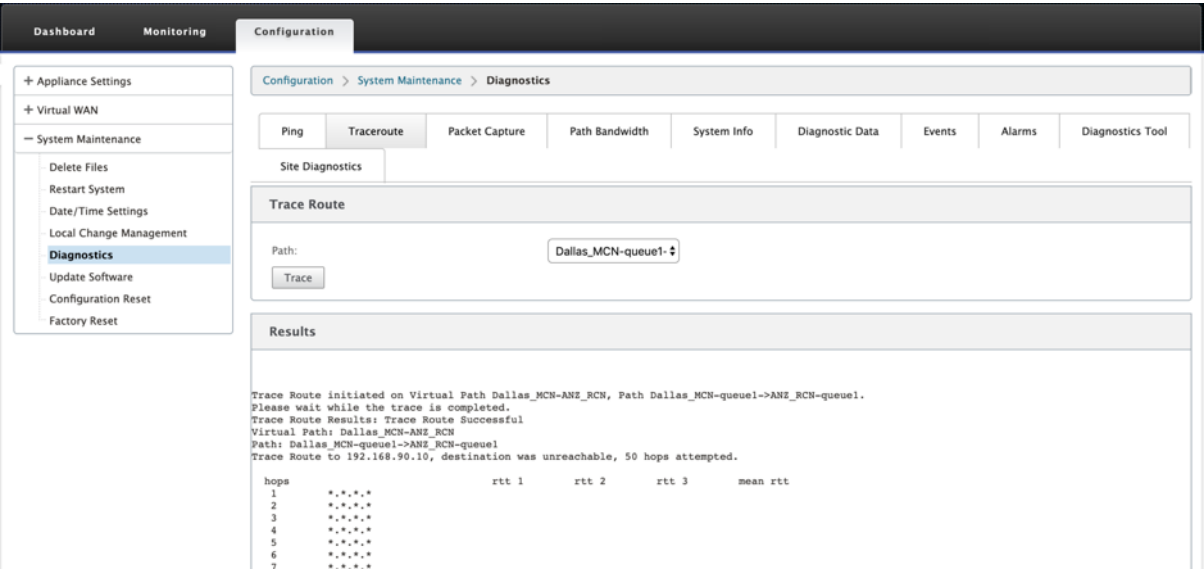


Sélectionnez le domaine de routage. Fournissez une adresse IP valide, un nombre de pings (nombre de fois où la demande ping doit être envoyée) et une taille de paquet (nombre d’octets de données) valides. Cliquez sur **Arrêter le ping** pour arrêter une recherche ping en cours.

Vous pouvez effectuer un ping via une interface spécifique. Sélectionnez le domaine de routage et spécifiez l’adresse IP avec le nombre de ping, la taille du paquet et sélectionnez l’interface virtuelle dans la liste déroulante.

Traceroute

Pour utiliser l’option **Traceroute**, accédez à **Configuration > développez Maintenance du système > Diagnostics** et sélectionnez **Traceroute**.



Traceroute permet de découvrir et d'afficher le chemin ou l'itinéraire vers un serveur distant. Utilisez l'option **Traceroute** comme outil de débogage pour détecter les points de défaillance d'un réseau.

Sélectionnez un chemin dans la liste déroulante, puis cliquez sur **Tracer**. Vous pouvez consulter les détails dans la section **Résultats**.

Capture de paquets

Vous pouvez utiliser l'option **Capture de paquets** pour intercepter le paquet de données en temps réel qui traverse l'interface active sélectionnée présente sur le site sélectionné. La capture de paquets vous aide à analyser et à résoudre les problèmes de réseau.

Dashboard

Monitoring

Configuration

+ Appliance Settings

+ Virtual WAN

- System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Factory Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Site Diagnostics

Packet Capture

Interfaces:

X 1/1 X 1/2 X 1/4 X 1/6

Duration (seconds):

30

Max # of packets to view:

5000

Capture Filter (Optional):

Capture

Note: Capture file size will not exceed 575 MB. Once the packet capture file reaches this size, packet capturing will be stopped. Atleast 1 interface needs to be selected to trigger a packet capture.

Gathering Requested Data

Generating packet capture information...

Packet Capture Successful

Packet Capture File

A binary file containing the packet data captured during the last successful packet capture. This file can be opened in Wireshark for analysis.

The downloaded Packet capture file displays internal labels for interface names. Here are the mappings for this platform:
MGMT -> tn-mgt0
1/1 -> dpdk-1_1
1/4 -> dpdk-1_4
1/2 -> dpdk-1_2
1/6 -> dpdk-1_6

Download

Packet View

#	Interface Name	Protocol	Time	Length	Source	Destination	Src
1.	1/2	UDP	May 8, 2019 06:06:30.415518572 UTC	1442	172.168.1.10	152.168.1.10	4980
2.	1/2	UDP	May 8, 2019 06:06:30.415524972 UTC	1442	152.168.1.10	172.168.1.10	4980
3.	1/2	UDP	May 8, 2019 06:06:30.415628324 UTC	1442	152.168.1.10	172.168.1.10	4980
4.	1/2	UDP	May 8, 2019 06:06:30.415648675 UTC	1442	172.168.1.10	152.168.1.10	4980
5.	1/2	UDP	May 8, 2019 06:06:30.415858329 UTC	1442	152.168.1.10	172.168.1.10	4980
6.	1/2	UDP	May 8, 2019 06:06:30.415873459 UTC	1442	172.168.1.10	152.168.2.10	4980
7.	1/2	UDP	May 8, 2019 06:06:30.416073413 UTC	1442	172.168.1.10	152.168.2.10	4980
8.	1/2	UDP	May 8, 2019 06:06:30.416232216 UTC	1442	152.168.1.10	172.168.1.10	4980
9.	1/1	TCP	May 8, 2019 06:06:30.321504133 UTC	1384	152.168.1.51	172.168.1.52	80
10.	1/2	UDP	May 8, 2019 06:06:30.416266227 UTC	1442	152.168.1.10	172.168.1.10	4980
11.	1/2	UDP	May 8, 2019 06:06:30.416435190 UTC	1442	172.168.1.10	152.168.1.10	4980
12.	1/2	UDP	May 8, 2019 06:06:30.416525402 UTC	114	172.168.1.10	152.168.2.10	4980
13.	1/1	TCP	May 8, 2019 06:06:30.321511153 UTC	54	152.168.1.52	172.168.1.51	2307
14.	1/2	UDP	May 8, 2019 06:06:30.416529932 UTC	114	172.168.1.10	152.168.2.10	4980
15.	1/1	TCP	May 8, 2019 06:06:30.321514773 UTC	54	152.168.1.52	172.168.1.51	2163
16.	1/2	UDP	May 8, 2019 06:06:30.416651685 UTC	1442	152.168.1.10	172.168.1.10	4980
17.	1/2	UDP	May 8, 2019 06:06:30.416693075 UTC	1442	152.168.1.10	172.168.1.10	4980
18.	1/2	UDP	May 8, 2019 06:06:30.416783167 UTC	1442	172.168.1.10	152.168.2.10	4980
19.	1/2	UDP	May 8, 2019 06:06:30.416881149 UTC	1442	172.168.1.10	152.168.2.10	4980
20.	1/2	UDP	May 8, 2019 06:06:30.417039802 UTC	1442	152.168.1.10	172.168.1.10	4980
21.	1/2	UDP	May 8, 2019 06:06:30.417127644 UTC	114	172.168.1.10	152.168.2.10	4980
22.	1/2	UDP	May 8, 2019 06:06:30.417132114 UTC	114	172.168.1.10	152.168.1.10	4980
23.	1/2	UDP	May 8, 2019 06:06:30.417135804 UTC	1442	172.168.1.10	152.168.2.10	4980
24.	1/1	TCP	May 8, 2019 06:06:30.321517954 UTC	54	152.168.1.52	172.168.1.51	6265
25.	1/2	UDP	May 8, 2019 06:06:30.417178605 UTC	114	172.168.1.10	152.168.1.10	4980
26.	1/1	TCP	May 8, 2019 06:06:30.321648046 UTC	1384	172.168.1.51	152.168.1.52	80

Fournissez les entrées suivantes pour l’opération de capture de paquets :

- **Interfaces** - Des interfaces actives sont disponibles pour la capture de paquets pour l’apppliance SD-WAN. Sélectionnez une interface ou ajoutez des interfaces dans la liste déroulante. Au moins une interface doit être sélectionnée pour déclencher une capture de paquets.

Remarque :

La possibilité d’exécuter la capture de paquets sur toutes les interfaces simultanément permet d’accélérer la tâche de dépannage.

- **Durée (secondes)** : durée (en secondes) pendant laquelle les données doivent être capturées.
- **Nombre maximal de paquets à afficher** : limite maximale de paquets à afficher dans le résultat de la capture de paquets.
- **Filtre de capture (facultatif)** - Le champ Filtre de capture facultatif accepte une chaîne de filtre utilisée pour déterminer quels paquets sont capturés. Les paquets sont comparés à la chaîne de filtre et si le résultat de comparaison est vrai, le paquet est capturé. Si le filtre est vide, tous les paquets sont capturés. Pour plus d'informations, consultez la section [Filtres de capture](#).

Voici quelques exemples de ce filtre de capture :

- **Ether proto \ ARP** - Capture uniquement les paquets ARP
- **Ether proto \ IP** - Capture uniquement les paquets IPv4
- **VLAN 100** : capture uniquement les paquets avec un VLAN de 100
- **Host 10.40.10.20** - Capture uniquement les paquets IPv4 vers ou depuis l'hôte avec l'adresse 10.40.10.20
- **Net 10.40.10.0 Mask 255.255.255.0** - Capture uniquement les paquets IPv4 dans le sous-réseau 10.40.10.0/24
- **IP proto \ TCP** - Capture uniquement les paquets IPv4/TCP
- **Port 80** : capture uniquement les paquets IP vers ou depuis le port 80
- **Plage de ports 20—30** - Capture uniquement les paquets IP vers ou depuis les ports 20 à 30

Remarque

La taille maximale du fichier de capture est de 575 Mo. Une fois que le fichier de capture de paquets atteint cette taille, la capture de paquets est interrompue.

Cliquez sur **Capturer** pour afficher le résultat de la capture de paquets. Vous pouvez également télécharger un fichier binaire contenant les données de paquets capturées lors de la dernière capture de paquets réussie.

Collecte des données demandées

Vous pouvez voir l'état de la génération d'informations de capture de paquets (si la capture de paquets a réussi ou pas de capture de paquets) dans ce tableau.

Fichier de capture de paquets

Les paquets sont capturés sous forme de données binaires lors de la dernière capture de paquets réussie. Vous pouvez télécharger le fichier binaire pour analyser les informations de paquet hors connexion. Le nom de l'interface est différent dans le fichier téléchargé par rapport à l'interface graphique. Pour afficher le mappage d'interface interne, cliquez sur l'option Aide.

Vous avez besoin de la version 2.4.13 ou supérieure du logiciel **Wireshark** pour ouvrir et lire le fichier binaire.



Bande passante du chemin

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dashboard

Monitoring

Configuration

Appliance Settings

Virtual WAN

System Maintenance

System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Instant Path Bandwidth Testing

Path:MCN-5100-WL-2->BR572

Test

Results

Minimum Bandwidth: 936564 kbps

Maximum Bandwidth: 1213863 kbps

Average Bandwidth: 1109046 kbps

Schedule Path Bandwidth Testing

Add

Path NameFrequencyDay of WeekHourMinute

Apply Settings

History Path Bandwidth Testing Result

Show 50 entriesShowing 1 to 27 of 27 entries

Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 2:01:03 PM	2883972	5099707	4357330
2	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 4:01:03 PM	3109115	3872000	3616157
3	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 6:01:04 PM	3041280	4119960	3518949
4	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 8:01:04 PM	2769377	3700672	3276124
5	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 10:01:04 PM	409245	3574153	2489269
6	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:04 AM	2481756	4001684	3198214
7	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 AM	2548853	3872000	3236546
8	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 AM	3204413	3982628	3642649
9	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 AM	2997677	4672357	3664018
10	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:04 AM	2248258	6288360	3612666
11	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:04 AM	2410236	3372387	2816032
12	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:03 PM	2613600	4401852	3563752
13	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 PM	2324266	4059961	3101910
14	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 PM	2179340	3684970	2929146
15	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 PM	2613600	3588493	3021890
16	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:03 PM	1676056	3499980	2655200
17	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:03 PM	1954093	3558944	2975884
18	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 AM	2161116	3784398	2902068
19	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 AM	2968971	4079765	3821158
20	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:04 AM	3514004	4181760	3893381
21	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 6:01:03 AM	3358843	4059961	3756691
22	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 8:01:03 AM	3216738	4245441	3716351
23	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 10:01:04 AM	3558944	4202773	3932908
24	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 PM	3427672	4267102	3838552
25	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 PM	2674061	4224000	3608676
26	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:03 PM	2816000	6288360	4165337
27	MCN-5100-WL-2	BR572-WL-1	2/19/2018, 5:23:04 PM	936564	1213863	1109046

Showing 1 to 27 of 27 entries

Le test de la bande passante active vous permet d’émettre un test de bande passante de chemin instantané via une liaison WAN Internet publique, ou de planifier des tests de bande passante de connexion WAN Internet publique à effectuer à des moments spécifiques et de façon récurrente.

La fonctionnalité Path Bandwidth (Bande passante de chemin) est utile pour démontrer la quantité de bande passante disponible entre deux emplacements au cours des installations nouvelles et

existantes. Les valeurs de la bande passante du chemin indiquent la bande passante maximale possible. Pour obtenir une bande passante autorisée précise, accédez à **Configuration > Maintenance du système > Diagnostics > Diagnosticsdu site>Test de bande passante**. Pour plus d’informations, consultez la section [Test de bande passante active](#).

Infos système

La page **Informations système** fournit les informations système, les détails des ports Ethernet et l’état de la licence.

Pour afficher les informations système, accédez à **Configuration > développez Maintenance du système > Diagnostics** et sélectionnez **Informations système**.

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

— System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics**
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

System Information

Name: Dallas_MCN

Appliance Mode: MCN

Hardware Model: 4000

Software Version: 11.0.0.72.760315

Built On: Apr 10 2019 at 19:08:49

OS Partition Version: 5.1

Serial Number: HNXCJCRGJX

BIOS version: 4.2a

Hard Disk Usage

Partition	Usage
Active OS	51%
/home	18%

[View Details](#)

Ethernet Ports

0/1:	mgt0	0a:c4:7a:85:ce:62
1/1:	la0	be:0a:f7:be:76:3d
1/2:	wa0	e6:18:31:22:b9:84
1/3:	la1	86:c0:b7:3c:03:5d
1/4:	wa1	8e:4b:f2:fd:86:75
1/5:	la2	da:6c:7c:73:d4:84
1/6:	wa2	be:e3:26:7e:2b:99
1/7:	la3	82:af:6a:d8:74:72
1/8:	wa3	a2:af:76:6f:90:a2
10/1:	la4	96:9a:df:97:77:eb
10/2:	wa4	76:5d:15:d9:f0:26

License Status

State:	Licensed
License Server HostID:	02c47a85ce62
Model:	4000VW-2000
Maximum Bandwidth (MAXBW):	2000 Mbps
License Type:	Retail
Maintenance Expiration Date:	Sun Dec 1 00:00:00 2019
License Expiration Date:	Mon Dec 2 00:00:00 2019

Les **informations système** répertorie tous les paramètres qui ne sont pas définis sur leurs valeurs par défaut. Ces informations sont en lecture seule. Il est utilisé par le support lorsqu’une erreur de configuration est suspectée. Lorsque vous signalez un problème, vous pouvez être invité à vérifier une ou plusieurs valeurs sur cette page.

Données de diagnostic

Les données de diagnostic vous permettent de générer un package de données de diagnostic à des fins d'analyse par l'équipe d'assistance Citrix. Vous pouvez télécharger le package **Fichiers journaux de diagnostic** et le partager avec l'équipe de support Citrix.

Pour afficher les **données de diagnostic**, accédez à **Configuration > développez Maintenance du système > Diagnostics** et sélectionnez **Données de diagnostic**.

Dashboard

Monitoring

Configuration

+ Appliance Settings

+ Virtual WAN

- System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Site Diagnostics

FTP Information

- These fields define the parameters used when connecting to an FTP server in order to Upload either Diagnostic Information packages or Memory Dump packages.
- Upload connections from this appliance to the FTP server are done in passive mode, so the server must support this and be in passive mode.

Note: All fields are required in order to FTP Apply.

Customer:

Username:

Password:

FTP Server:

FTP Apply

Diagnostic Information

NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.

Diagnostic Log Files

- These packages contain important real-time system information you can forward to Citrix Support Representatives. They may be downloaded directly through the browser or uploaded via FTP to the FTP server defined in the FTP Information area above.
- Only 5 diagnostics packages can exist on the system at a time.

Create New...

Filename:

Download Selected

Upload Selected

Delete Selected

Memory Dumps

NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.

System Error Memory Dumps

- Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete any that are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.

There are no memory dumps available for download.

Download

Upload

Delete

Configuration Diagnostic Information

NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.

Configuration Diagnostic Files

- This package contains Configuration Diagnostics information you can forward to Citrix Support Representatives. This is an additional package to the STS captured on Branches. This package contains configuration archive and log files which help debug issues on the Branch. They may be downloaded directly through the browser or uploaded via FTP to the FTP server defined in the FTP Information area above.
- Only 5 Configuration diagnostics packages can exist on the system at a time.

Create New...

Filename:

Download Selected

Upload

Delete Selected

Les **données de diagnostic** incluent :

- **Informations FTP** : indiquez les détails des paramètres FTP, puis cliquez sur **Appliquer FTP**. Informations FTP requises pour connecter un serveur FTP pour télécharger le package d'informations de diagnostic.
- **Informations de diagnostic** : le package de fichiers journaux de diagnostic contient des infor-

mations système en temps réel qui peuvent être téléchargées via le navigateur ou téléchargées via FTP sur le serveur FTP.

Remarque :

Seuls cinq packages de diagnostic peuvent exister sur le système à la fois.

- **Informations de diagnostic de configuration** : dans la version de Citrix SD-WAN 11.0, le fichier de configuration réseau ne sera pas disponible dans les informations de diagnostic collectées pour la succursale. Pour tous les cas de support, fournissez les informations de diagnostic de la branche et les informations de diagnostic de configuration à partir du nœud de contrôle auquel la branche est connectée.

Pour collecter des informations de diagnostic de configuration à partir de l'interface graphique du nœud de contrôle, accédez à **Configuration > Maintenance du système > Diagnostics > Données de diagnostic** > sous **Informations de diagnostic de configuration**, cliquez sur **Créer un nouveau**.

Configuration Diagnostic Information

NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.

Configuration Diagnostic Files

- This package contains Configuration Diagnostics information you can forward to Citrix Support Representatives. This is an additional package to the STS captured on Branches. This package contains configuration archive and log files which help debug issues on the Branch. They may be downloaded directly through the browser or uploaded via FTP to the FTP server defined in the FTP Information area above.
- Only 5 Configuration diagnostics packages can exist on the system at a time.

Create New...

Filename:

Une fois la création des **informations de diagnostic de configuration** terminée, cliquez sur **Télécharger le fichier sélectionné** et fournissez ce fichier au support Citrix OU utilisez l'opération d'application FTP disponible sur la même page pour FTP ce fichier.

- **Dumps mémoire** : vous pouvez télécharger ou télécharger le fichier de vidages mémoire d'erreur système et le partager avec l'équipe de support Citrix. Vous pouvez également supprimer les fichiers si ce n'est pas nécessaire.

REMARQUE :

Par défaut, l'option **Upload** est en mode désactivé. Pour l'activer, configurez les paramètres **DNS** et un **nom de client FTP** pour cette appliance.

Événements

Utilisez la fonctionnalité **Événements** pour ajouter, surveiller et gérer les événements générés. Il permet d'identifier les événements en temps réel, ce qui vous aide à résoudre immédiatement les prob-

lèmes et à maintenir l’appliance Citrix SD-WAN en fonctionnement efficace. Vous pouvez télécharger des événements au format CSV.

Pour ajouter un événement, sélectionnez le type d’objet, le type d’événement et la gravité dans la liste déroulante, puis cliquez sur **Ajouter un événement**.

Pour afficher les **événements**, accédez à **Configuration** développez **Maintenance du système > Diagnostics** et sélectionnez **Événements**.

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

Insert Event

Object Type:USER EVENT

Event type:UNDEFINED

Severity:DEBUG

Add Event

Download Events

There are currently 85 in the Events database, spanning from event 245471 at 2019-03-24 05:35:54 to event 245555 at 2019-04-21 06:23:16. You can download some or all of them in CSV format. You may wish to limit the amount to download because some common spreadsheet programs limit you to 65,536 rows.

Download events starting from2019March24535

54Download (85 events)

Alert Count

Alert Type	Alerts Sent
Emails:	0
Syslog Messages:	0
SNMP Traps:	5

View Events

Quantity:1000

Filter: Object Type = AnyEvent type = AnySeverity = Any

Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
245555	25	License_Alert	LICENSE_EVENT	2019-04-21 06:23:16	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245554	25	License_Alert	LICENSE_EVENT	2019-04-20 06:23:01	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245553	25	License_Alert	LICENSE_EVENT	2019-04-19 06:22:46	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245552	25	License_Alert	LICENSE_EVENT	2019-04-18 06:22:31	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245551	25	License_Alert	LICENSE_EVENT	2019-04-17 06:22:15	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245550	25	License_Alert	LICENSE_EVENT	2019-04-16 06:22:00	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245549	25	License_Alert	LICENSE_EVENT	2019-04-15 06:21:44	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245548	25	License_Alert	LICENSE_EVENT	2019-04-14 06:21:29	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).

Vous pouvez configurer Citrix SD-WAN pour envoyer des notifications d’événements pour différents types d’événements tels que **des e-mails, des interruptions SNMP** ou **des messages Syslog**.

Une fois que les paramètres de notification e-mail, SNMP et syslog sont configurés, vous pouvez sélectionner la gravité des différents types d’événements et sélectionner le mode (e-mail, SNMP, syslog) pour envoyer des notifications d’événements.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

986

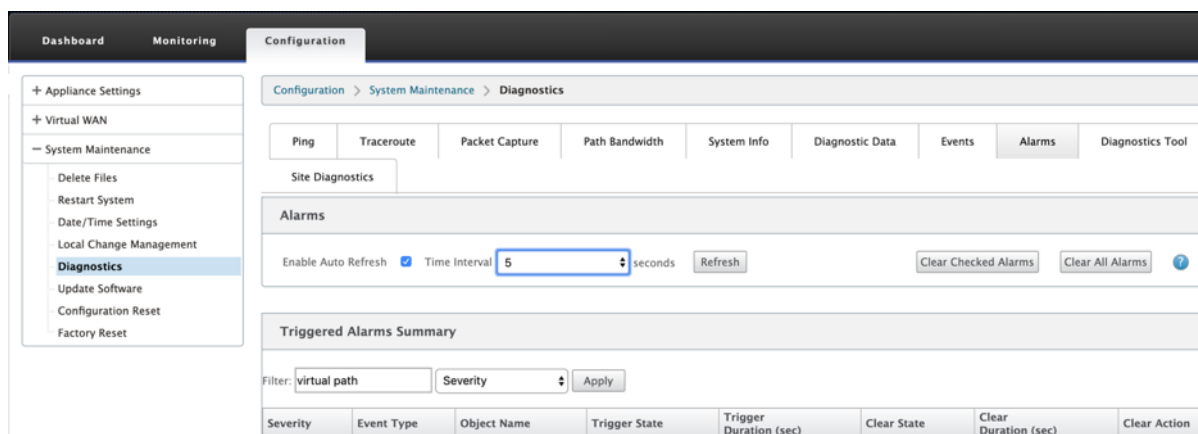
Les notifications sont générées pour les événements égaux ou supérieurs au niveau de gravité spécifié pour le type d'événement.

Vous pouvez afficher les détails des événements sous le tableau **Afficher les événements**. Les détails de l'événement comprennent les informations suivantes.

- **ID :** ID de l'événement.
- **ID de l'objet :** ID de l'objet générant l'événement.
- **Nom de l'objet :** nom de l'objet générant l'événement.
- **Type d'objet :** type de l'objet générant l'événement.
- **Heure :** heure à laquelle l'événement a été généré.
- **Type d'événement :** état de l'objet au moment de l'événement.
- **Gravité :** niveau de gravité de l'événement.
- **Description :** description textuelle de l'événement.

Alarmes

Vous pouvez afficher et effacer l'alarme déclenchée. Pour afficher les **alarmes**, accédez à **Configuration > développez Maintenance du système > Diagnostic** et sélectionnez **Alarmes**.



Sélectionnez les alarmes que vous souhaitez effacer et cliquez sur **Effacer les alarmes vérifiées** ou cliquez sur **Effacer toutes les alarmes** pour effacer toutes les alarmes.

Vous pouvez afficher le résumé suivant de toutes les alarmes déclenchées :

- **Gravité :** la gravité est affichée dans les alertes envoyées lorsque l'alarme est déclenchée ou effacée et dans le résumé des alarmes déclenchées.
- **Type d'événement :** l'appliance SD-WAN peut déclencher des alarmes pour des sous-systèmes ou des objets particuliers du réseau. Ces alarmes sont appelées types d'événements.
- **Nom de l'objet :** nom de l'objet générant l'événement.
- **État du déclencheur :** état de l'événement qui déclenche une alarme pour un type d'événement.

- **Durée du déclenchement (sec)** : la durée en secondes détermine la rapidité avec laquelle l'appareil déclenche une alarme.
- **Effacer l'état** : état de l'événement qui efface une alarme pour un type d'événement après le déclenchement de l'alarme.
- **Durée d'effacement (sec)** : la durée en secondes détermine le temps d'attente avant d'effacer une alarme.
- **Effacer l'action** : action effectuée lors de la suppression des alarmes.

Outil de diagnostic

L'**outil de diagnostic** est utilisé pour générer un trafic de test qui vous permet de résoudre les problèmes réseau susceptibles d'entraîner :

- Changement fréquent dans l'état du chemin de Bon à Mauvais.
- Mauvaise performance des applications.
- Perte de paquets plus élevée

Le plus souvent, ces problèmes se posent en raison de la limitation de débit configurée sur le pare-feu et le routeur, des paramètres de bande passante incorrects, de la faible vitesse de liaison, de la file d'attente prioritaire définie par le fournisseur de réseau, etc. L'outil de diagnostic vous permet d'identifier la cause première de ces problèmes et de les résoudre.

L'outil de diagnostic supprime la dépendance à l'égard d'outils tiers tels que iPerf qui doit être installé manuellement sur les hôtes du centre de données et de la branche. Il permet de mieux contrôler le type de trafic de diagnostic envoyé, la direction dans laquelle le trafic de diagnostic circule et le chemin sur lequel le trafic de diagnostic circule.

L'outil de diagnostic permet de générer les deux types de trafic suivants :

- **Contrôle** : génère du trafic sans aucune QoS/planification appliquée aux paquets. Par conséquent, les paquets sont envoyés sur le chemin sélectionné dans l'interface utilisateur, même si le chemin n'est pas le meilleur à ce moment. Ce trafic est utilisé pour tester des chemins spécifiques et aide à identifier les problèmes liés aux FAI. Vous pouvez également l'utiliser pour déterminer la bande passante du chemin sélectionné.
- **Données** : simule le trafic généré par l'hôte avec le traitement du trafic SD-WAN. Étant donné que la QoS/ordonnancement est appliquée aux paquets, les paquets sont envoyés sur le meilleur chemin disponible alors. Le trafic est envoyé sur plusieurs chemins si l'équilibrage de charge est activé. Ce trafic est utilisé pour résoudre les problèmes liés à la QoS/Scheduler.

Remarque

Pour exécuter un test de diagnostic sur un chemin, vous devez démarrer le test sur les appliances aux deux extrémités du chemin. Démarrez le test de diagnostic en tant que serveur sur une ap-

pliance et en tant que client sur l'autre appliance.

Pour utiliser l'outil de diagnostic :

1. Sur les deux solutions matérielles-logicielles, cliquez sur **Configuration > Maintenance du système > Diagnostics > Outil de diagnostic**.

The screenshot shows the 'Diagnostics Tool' interface. At the top, there are three dropdown menus: 'Tool Mode' set to 'Server', 'Traffic Type' set to 'Data', and 'Port' set to '10'. Below these, there is a text input field for 'Iperf:' and a dropdown for 'WAN to LAN Paths' showing 'DC-INET-1->BR1-INET-1'. A 'Start' button is located below the 'Iperf:' field. The bottom section is titled 'Results' and contains a 'stop' button. Below the 'stop' button, there is a dashed line followed by the text 'Server listening on TCP port 10' and 'TCP window size: 85.3 KByte (default)', followed by another dashed line.

2. Dans le champ **Mode outil**, sélectionnez **Serveur** sur un matériel et sélectionnez **Client** sur l'appliance résidant à l'extrémité distante du chemin sélectionné.
3. Dans le champ **Type de trafic**, sélectionnez le type de trafic de diagnostic (**Contrôle** ou **Données**). Sélectionnez le même type de trafic sur les deux appliances.
4. Dans le champ **Port**, spécifiez le numéro de port **TCP/UDP** sur lequel le trafic de diagnostic est envoyé. Spécifiez le même numéro de port sur les deux appliances.
5. Dans le champ **Iperf**, spécifiez les options de ligne de commande IPERF, le cas échéant.

Remarque

Vous n'avez pas besoin de spécifier les options de ligne de commande IPERF suivantes :

- -c : l'option de mode client est ajoutée par l'outil de diagnostic.
- -s : l'option de mode serveur est ajoutée par l'outil de diagnostic.
- -B : La liaison IPERF à une IP/interface spécifique est effectuée par l'outil de diagnostic en fonction du chemin sélectionné.
 - -p : Le numéro de port est fourni dans l'outil de diagnostic.
- -i : intervalle de sortie en secondes.
- -t : Durée totale du test en secondes.

6. Sélectionnez les chemins WAN vers LAN sur lesquels vous souhaitez envoyer le trafic de diagnostic. Sélectionnez le même chemin d'accès sur les deux appliances.

7. Cliquez sur **Démarrer** sur les deux appliances.

Le résultat affiche le mode (client ou serveur) de l’appliance sélectionnée et le port TCP ou UDP sur lequel le test est exécuté. Il affiche périodiquement les données transférées et la bande passante utilisée pendant l’intervalle spécifié jusqu’à ce que la durée totale du test soit atteinte.

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

Diagnostics Tool

Tool Mode: ClientTraffic Type: DataPort: 10

Iperf:LAN to WAN Paths: MCN_184_78-Broadband

Start

Results

stop

Client connecting to 172.16.31.10, TCP port 10
Binding to local address 172.16.21.10
TCP window size: 112 KByte (default)

[3] local 172.16.21.10 port 39993 connected with 172.16.31.10 port 10

[ID]	Interval	Transfer	Bandwidth
[3]	0.0~ 1.0 sec	10.1 MBytes	84.9 Mbits/sec
[3]	1.0~ 2.0 sec	11.9 MBytes	99.6 Mbits/sec
[3]	2.0~ 3.0 sec	13.4 MBytes	112 Mbits/sec
[3]	3.0~ 4.0 sec	15.1 MBytes	127 Mbits/sec
[3]	4.0~ 5.0 sec	14.5 MBytes	122 Mbits/sec
[3]	5.0~ 6.0 sec	14.5 MBytes	122 Mbits/sec
[3]	6.0~ 7.0 sec	15.1 MBytes	127 Mbits/sec
[3]	7.0~ 8.0 sec	15.1 MBytes	127 Mbits/sec
[3]	8.0~ 9.0 sec	15.6 MBytes	131 Mbits/sec
[3]	9.0~10.0 sec	16.0 MBytes	134 Mbits/sec
[3]	0.0~10.0 sec	141 MBytes	118 Mbits/sec

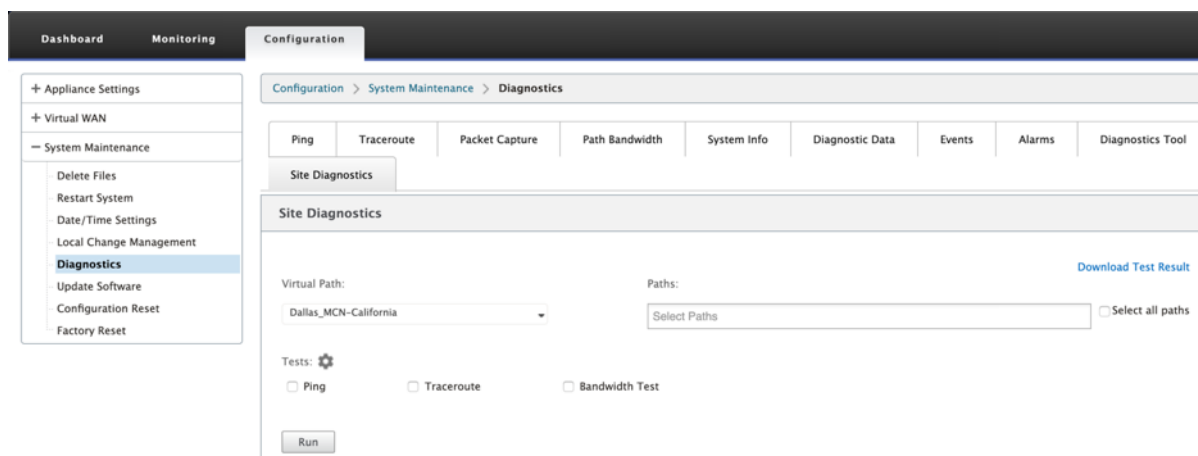
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

990

Diagnostics de

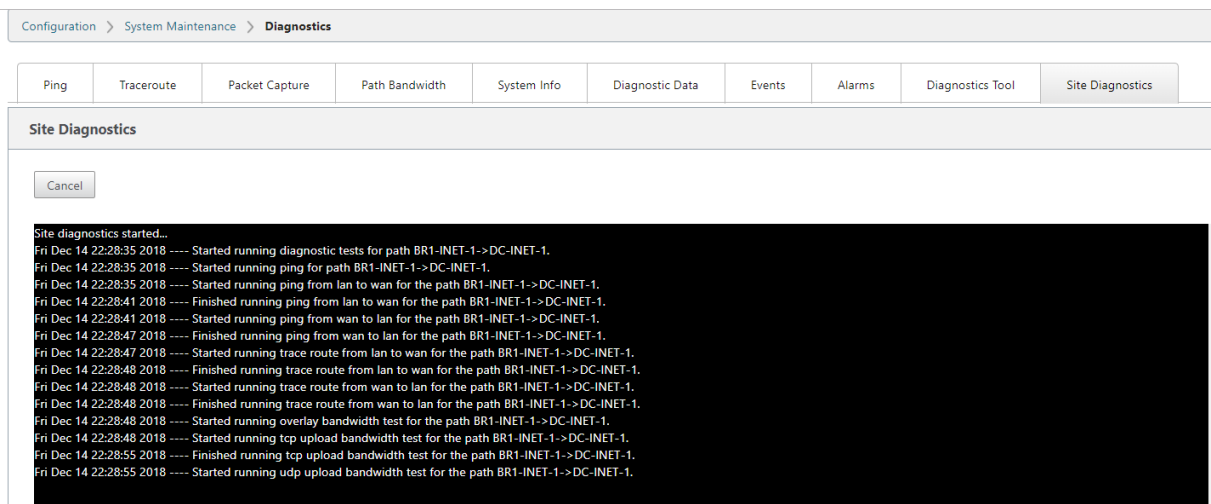
Vous pouvez tester l'utilisation de la bande passante, ping et effectuer un traceroute pour les liens WAN configurés sur différents sites du réseau Citrix SD-WAN. Il fournit des informations qui aident à résoudre les problèmes liés à la configuration existante.

Pour utiliser les **diagnostics de site**, accédez à **Configuration** développez **Maintenance du système** > **Diagnostics** et sélectionnez **Outil de diagnostic**.



La section des résultats affiche les informations suivantes :

- **État de l'interface** : fournit le nom de l'interface, le nombre de zones de pare-feu associées à l'interface, l'ID du VLAN et les ports associés.
- **État du chemin** : fournit les détails de l'adresse IP privée cible, de l'adresse IP de la passerelle, de l'adresse IP publique cible, de l'adresse IP du partenaire et du partenaire. Il affiche également l'état de l'ARP de la passerelle et du MTU du chemin.
- **Résultat du ping** : fournit la direction, l'état, le nombre (y compris le nombre de tentatives et d'échecs) et le temps de réponse rapide du ping.
- **Résultat Traceroute** : fournit la direction, l'état, le nombre de sauts et l'adresse IP ou le RTT des sauts.
- **Résultat de la bande passante** : fournit l'état de TCP et UDP ainsi que la bande passante utilisée (en Kbits/s) pour le réseau de superposition et de sous-couche. Par rapport à UDP, la bande passante utilisée par TCP est supérieure, car UDP est basé sur la bande passante et utilise donc uniquement la bande passante configurée. TCP est un protocole de montée en puissance ; en fonction de la configuration réseau sous-jacente, l'utilisation peut signaler une bande passante supérieure à la bande passante configurée.



Amélioration du mappage des chemins et de l'utilisation de la bande passante

May 6, 2021

Les améliorations du mappage des chemins et de l'utilisation de la bande passante sont implémentées dans l'onglet Surveillance pour afficher les flux de trafic. Par exemple, lorsqu'un seul chemin virtuel sert une connexion réseau et si ce chemin virtuel devient inactif, un nouveau chemin est choisi et le chemin initial devient le dernier meilleur chemin. Ce scénario est implémenté lorsque la demande de bande passante est inférieure et lorsqu'un seul chemin est choisi

Lorsque plusieurs chemins virtuels servent une connexion, vous remarquez un meilleur chemin actuel et le meilleur chemin suivant, le cas échéant. Si un seul chemin existe pour traiter le trafic, en supposant qu'il y ait plus de deux chemins de traitement du trafic et que la table des chemins est mise à jour avec deux chemins, l'onglet Surveillance de l'interface graphique SD-WAN pour les flux affichera le meilleur chemin actuel comme premier chemin et le chemin séparé par la virgule suivant comme dernier chemin. Ce scénario est implémenté lorsqu'il y a un besoin de plus de chemins avec la demande de bande passante.

Surveillance des informations d'application DPI dans l'interface graphique SD-WAN

Le nom de l'objet d'application PPP sur le flux de surveillance est stocké et affiché dans la page **Surveillance** de l'interface graphique SD-WAN -> **Flux** . Une info-bulle s'affiche pour identifier l'application PPP.

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Monitoring > Flows

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows Toggle Columns

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps
172.16.14.99	172.16.19.167	LAN to WAN	80	2189	TCP	default	41572	Virtual Path	DC-BR	LOCAL	758	41571	14527110	2.072	6.337	0.8
172.16.14.99	172.16.19.162	LAN to WAN	80	3161	TCP	Override = NO Demote on Large Packets = NO Separate TCP ACK Class = NO Packet Sequence Inorder = YES Inorder Holdtime: 900 Late Packet Action = DISCARD					361	41525	14427708	2.099	6.488	0.8
172.16.14.99	172.16.19.161	LAN to WAN	80	6310	TCP						60	41827	14468200	2.115	6.341	0.8
172.16.14.99	172.16.19.170	LAN to WAN	80	10844	TCP						360	41863	14393387	2.110	6.285	0.8

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Both LAN to WAN and WAN to LAN Flows Toggle Columns

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps
172.16.14.99	172.16.19.167	LAN to WAN	80	2189	TCP	default	41572	Virtual Path	DC-BR	LOCAL	758	41571	14527110	2.072	6.337	0.8
172.16.14.99	172.16.19.162	LAN to WAN	80	3161	TCP	Override = NO Demote on Large Packets = NO Separate TCP ACK Class = NO Packet Sequence Inorder = YES Inorder Holdtime: 900 Late Packet Action = DISCARD					361	41525	14427708	2.099	6.488	0.8
172.16.14.99	172.16.19.161	LAN to WAN	80	6310	TCP						60	41827	14468200	2.115	6.341	0.8
172.16.14.99	172.16.19.170	LAN to WAN	80	10844	TCP						360	41863	14393387	2.110	6.285	0.8
172.16.14.99	172.16.19.164	LAN to WAN	80	3387	TCP	Packet Duplication = NO Persistent Paths = NO Reliable = YES					358	41798	14472656	2.070	6.284	0.8
172.16.14.215	172.16.19.99	LAN to WAN	9321	80	TCP	TCP Standalone ACKs = NO Check Flow TOS = NO					14	43483	2592802	2.145	1.022	0.8
172.16.14.99	172.16.19.167	LAN to WAN	80	4200	TCP	IP/TCP/UDP Header Compression = NO GRE Header Compression = NO Packet Aggregation = NO					112	41705	14426227	2.114	6.348	0.8
172.16.14.99	172.16.19.169	LAN to WAN	80	3161	TCP	Deep Packet Inspection = NO					356	40970	14508376	2.054	6.299	0.8
172.16.14.218	172.16.19.99	LAN to WAN	3371	80	TCP	TCP Termination = NO Rule ID = 1					407	42980	2552820	2.043	0.967	0.8
172.16.14.99	172.16.19.166	LAN to WAN	80	1116	TCP	VLAN ID = 0					113	41286	14568312	2.047	6.220	0.8
172.16.14.213	172.16.19.99	LAN to WAN	17082	80	TCP	App Rule ID = N/A					161	42915	2556999	2.114	1.006	0.8
172.16.14.217	172.16.19.99	LAN to WAN	4090	80	TCP	DPI Application = http					364	42530	2540882	2.059	0.983	0.8

Surveillance des informations de chemin pour le flux de trafic dans l'interface graphique SD-WAN

Il est possible qu'en fonction du débit de trafic entrant exigeant la bande passante, un ou plusieurs chemins soient nécessaires pour traiter le trafic.

Pour déterminer comment le mappage des chemins est effectué, examinez les scénarios suivants :

Mode de transmission à charge équilibrée :

La figure suivante illustre le scénario lorsque le trafic est initié et que tous les chemins sont bons, un meilleur chemin est choisi car la demande de bande passante est suffisante pour être desservie par un seul chemin. Vous remarquerez qu'un seul chemin **DC-MCN-Internet -> BR1 -VPX-Internet** est choisi et que le type de transmission est affiché en tant que **charge équilibrée**.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
DC-MCN-BR1-VPX	LOCAL	3	291	435918	85.373	1023.106	36.881	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

La figure suivante illustre lorsque le trafic circule et que les attributs WAN du chemin sont dégradés, vous remarquez qu’un nouveau chemin est choisi pour traiter le trafic sans interruption. Dans ce cas, la fonction de mappage de chemin vous permet d’indiquer que le meilleur chemin actuel qui traite le trafic est **DC-MCN-Internet2 -> BR1-VPX-Internet** et que le dernier meilleur chemin qui a traité le trafic est **DC-MCN-Internet -> BR1-VPX-Internet** .

Le dernier meilleur chemin dans cet exemple est un indicateur du chemin qui a servi la connexion précédemment.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
728	1090544	0.983	11.778	0.425	0.000	52	N/A	15	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

La figure suivante illustre que lorsque le trafic est en cours et que plusieurs chemins sont choisis pour le traitement du trafic en raison de la demande en bande passante, comme indiqué ci-dessous, plusieurs chemins sont choisis lors de l’envoi du trafic. Contrairement au cas ci-dessus, ici il peut y avoir plus de deux chemins desservant également le trafic, mais dans l’interface graphique, seuls les deux meilleurs chemins qui servent actuellement le trafic sont affichés.

Observez **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-Internet2->BR1-VPX-Internet**étant les deux chemins indiqués dans le tableau **Flux de données**.

Remarque

Comme indiqué, seuls deux chemins maximum dans la table des flux sont affichés.

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☐ Internet Load Balancing Table

☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

ets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
155	1280790	318.598	3818.082	137.634	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

La figure suivante illustre que lorsque le trafic continue à circuler, si le meilleur chemin actuel qui est **DC-MCN-Internet->BR1-VPX-Internet** est indisponible/inactif/dégradé dans les attributs WAN, le meilleur chemin actuel choisi apparaîtra en premier dans la section chemin de la table **Flux Data** suivi du dernier meilleur chemin qui dessert le trafic.

Comme le **DC-MCN-Internet->BR1-VPX-Internet** n’était plus le meilleur, le système a choisi un nouveau meilleur chemin actuel comme **DC-MCN-MPLS->BR1-VPX-MPLS**, et le dernier meilleur chemin qui sert activement la connexion avec le meilleur chemin actuel est **DC-MCN-Internet2->BR1-VPX-Internet** car les deux sont nécessaires pour la demande actuelle de trafic de bande passante.

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☐ Internet Load Balancing Table

☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

ackets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2764	4140472	170.434	2042.476	73.627	0.000	52	N/A	15	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

Mode de transmission dupliqué

Le mode général de duplication des paquets garantit que deux chemins sont initialement utilisés pour le traitement des paquets de la même connexion afin d’assurer une distribution fiable en dupliquant les paquets sur deux chemins distincts.

Pour le mappage de chemins, vous remarquez que deux chemins sont pris dans la section chemin de la table de flux tant qu’il existe deux chemins pour traiter les flux par duplication.

La figure suivante illustre que le trafic wen circule, on peut remarquer que deux chemins sont montrés pour traiter le trafic. Contrairement à tout autre mode, même si le trafic demande moins de bande passante qui peut être fournie par un seul chemin, ce mode dupliquera toujours le trafic sur deux chemins pour une livraison fiable des applications.

Vous remarquez dans la figure ci-dessous, deux chemins dans la section chemin de la table **Flux Data** : **DC-MCN-Internet2->BR1-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS** .

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☐ Internet Load Balancing Table

☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

Flow ID	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
3	551	32640	88.836	42.100	38.377	0.000	0	N/A	9	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Duplicate, Reliable	iperf
4	1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable	iperf

La figure suivante illustre que lorsque le trafic circule, si l’un des meilleurs chemins actuels devient inactif, un autre chemin est choisi et il y a toujours deux chemins dans la section de chemin dans la table **Flux Data** .

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☐ Internet Load Balancing Table

☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

IN / IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
CAL	10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Duplicate, Reliable
CAL	0	34213	49055970	267.264	3066.058	115.458	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable

Mode de transmission du chemin persistant

Le mode de transmission de chemin persistant permet de conserver les paquets d’un flux basé sur l’impédance de latence de chemin.

La figure suivante illustre un seul chemin qui est le meilleur chemin qui gère actuellement les flux et ses paquets. Il n’y a pas de demande de bande passante et un chemin sert tout cela. Actuellement, il n’y a qu’un seul meilleur chemin qui est **DC-MCN-Internet->BR1-VPX-Internet**.

Flows Data

Toggle Columns

Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
Local Path	DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

La figure suivante illustre que si le chemin **DC-MCN-Internet->BR1-VPX-Internet** devient sujet à la latence ou est désactivé, vous remarquez que le nouveau chemin prend effet et que le chemin courant **DC-MCN-Internet->BR1-VPX-Internet** devient le dernier meilleur chemin.

Ainsi, la nouvelle section de chemin affiche **DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet**.

Flows Data															
Toggle Columns															
IN / IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
ICAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

En mode persistant, plusieurs chemins peuvent être choisis pour traiter le trafic. Dans ce cas, l’interface graphique affiche à la fois les chemins avec le meilleur et le suivant meilleur dans la section chemin de la table de flux depuis le début du flux de trafic.

La figure suivante illustre que le flux n’a initialement besoin que de plus de deux chemins et qu’ils restent persistants tant qu’il n’y a pas de croisement d’impédance de latence de chemin (50 ms). Les deux chemins empruntés sont indiqués comme : **DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS**.

Flows Data

Toggle Columns

	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
L	51	6368	367504	128.449	59.303	55.490	0.000	2	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Persistent	iperf
L	1	9694	13894396	195.491	2241.576	84.452	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Supposons que l’un des meilleurs chemins **DC-MCN-Internet** va dans une latence élevée ou est dés-activé. Cela fait apparaître un nouveau chemin et le nouveau chemin peut être le meilleur chemin ou pourrait être le deuxième meilleur chemin basé sur la décision de sélection de chemin à ce moment de temps.

Flows Data														
Toggle Columns														
Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2	79540	4709572	147.475	73.223	63.709	0.000	2	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Persistent	iperf
0	119720	171655210	195.634	2233.531	84.514	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Résolution des problèmes de gestion IP

May 6, 2021

Voici les scénarios possibles que vous pourriez rencontrer lors de la configuration de l’adresse IP DHCP.

Il inclut également les meilleures pratiques et les recommandations pour la configuration de l'adresse IP de gestion DHCP lors du déploiement d'appliances SD-WAN.

Ces recommandations s'appliquent à tous les modèles de plates-formes SD-WAN ; Standard Edition, WANOP et Premium (Enterprise) Edition - Appliances physiques et virtuelles.

Remarque

Tous les modèles matériels des appliances SD-WAN sont livrés avec une adresse IP de gestion par défaut. Assurez-vous de configurer l'adresse IP DHCP requise pour l'appliance pendant le processus d'installation.

Tous les modèles virtuels d'appliances SD-WAN (modèles VPX) et d'appliances pouvant être déployés dans un environnement AWS n'ont pas d'adresse IP par défaut attribuée.

Les appliances s'allument sans serveurs DHCP accessibles :

- Causes :
 - Câble de gestion Ethernet déconnecté
 - Le service DHCP est en panne pour le réseau connecté
- Comportement attendu
 - Les appliances dont le service DHCP est activé réessaieront la requête DHCP toutes les 300 secondes (valeur par défaut). L'intervalle réel est d'environ 7 minutes
 - Par conséquent, les appliances dont le service DHCP est activé acquièrent des adresses DHCP dans les 7 minutes suivant la disponibilité des serveurs DHCP. Le délai varie de 0 à 7 minutes

l'adresse DHCP attribuée expire :

- Comportement attendu :
 - Les appliances dont le service DHCP est activé tenteront de renouveler le bail avant l'expiration de l'adresse
 - Les appliances démarrent avec une nouvelle découverte DHCP si le renouvellement échoue

Les appliances dont le service DHCP est activé passent d'un sous-réseau DHCP à un autre sous-réseau :

- Causes : les appliances passent d'un sous-réseau DHCP affecté à un autre sous-réseau DHCP
- Comportement attendu :
 - Une attribution d'adresse IP DHCP à bail permanent peut nécessiter le redémarrage des appliances pour acquérir une adresse IP à partir du nouveau serveur DHCP.

- À l'expiration du bail DHCP, les appliances peuvent relancer le protocole de découverte DHCP si le serveur DHCP actuel n'est pas accessible.
- Les appareils acquièrent de nouvelles adresses IP avec un délai de 8 minutes. L'adresse IP de la Gateway n'est pas modifiée dans l'interface graphique et l'interface de ligne de commande. Il est mis à jour une fois le processus de redémarrage terminé.

Recommandation :

- Affectez toujours un bail permanent pour les adresses DHCP attribuées aux appliances Citrix SD-WAN (physique/virtuelle). Cela permet aux appliances d'avoir une adresse IP de gestion prévisible.

Notifications HTTP basées sur la session

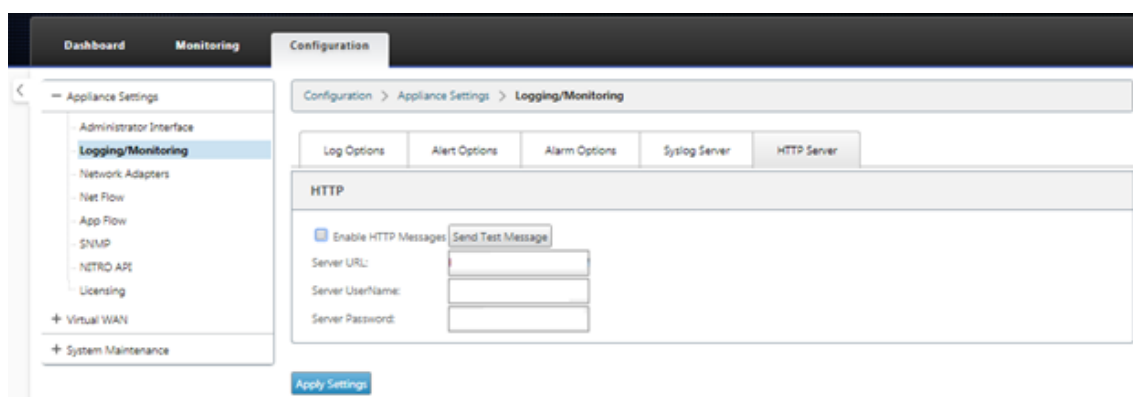
May 6, 2021

Vous pouvez désormais configurer les rapports d'événements et d'alarme pour les demandes de service d'API HTTP POST génériques dans l'interface graphique du dispositif Citrix SD-WAN. La configuration d'alarme HTTP et de notification d'événement est similaire aux événements de messagerie électronique et SNMP pour les événements et les alarmes pris en charge par SD-WAN.

La notification HTTP Post basée sur une session est envoyée à un service externe, tel que Service Now. Les notifications d'événements pour le serveur HTTP peuvent être configurées dans l'interface graphique de l'appliance Citrix SD-WAN et Citrix SD-WAN Center.

Pour configurer les notifications HTTP POST dans l'interface graphique du dispositif Citrix SD-WAN :

1. Accédez à **Configuration > Logging/Monitoring > Serveur HTTP**.



2. Cliquez sur **Activer les messages HTTP**.
3. Entrez l'**URL** du serveur HTTP pour lequel vous souhaitez recevoir des notifications. Entrez le **nom d'utilisateur** et le mot de **mot de passe du serveur**.

Configuration > Appliance Settings > Logging/Monitoring

Log OptionsAlert OptionsAlarm OptionsSyslog ServerHTTP Server

HTTP

☒ Enable HTTP Messages Send Test Message

Server URL:

Server UserName:

Server Password:

Apply Settings

4. Cliquez sur **Appliquer les paramètres**. La page s’actualise après l’application des paramètres de notifications du serveur HTTP.

Remarque

Utilisez l’option **Envoyer un message de test** pour vérifier que la connexion au serveur HTTP est réussie.

Pour ajouter une notification d’alarme pour une session de serveur HTTP :

1. Dans la page **Enregistrement/Surveillance**, accédez à la page de l’onglet **Options d’alarme** .
2. Cliquez sur **Ajouter une alarme**.

Configuration > Appliance Settings > Logging/Monitoring

Log OptionsAlert OptionsAlarm OptionsSyslog ServerHTTP Server

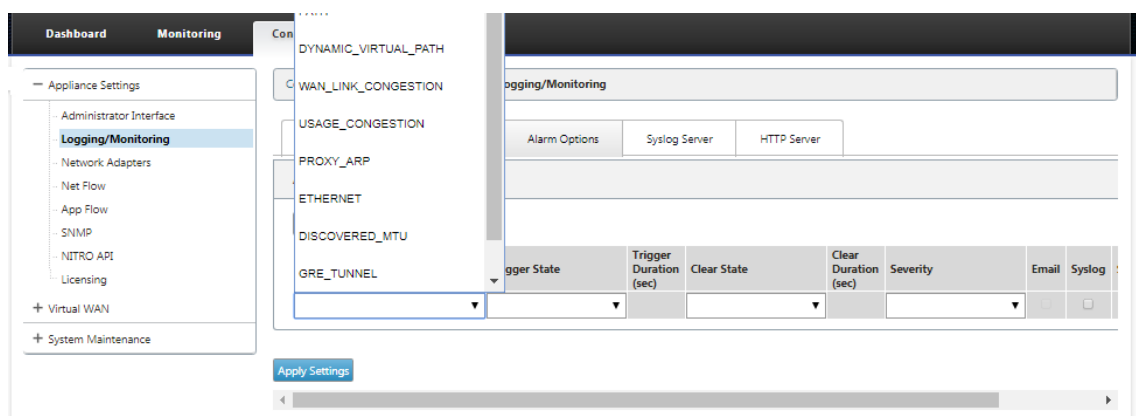
Alarm Configuration

Add Alarm

Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

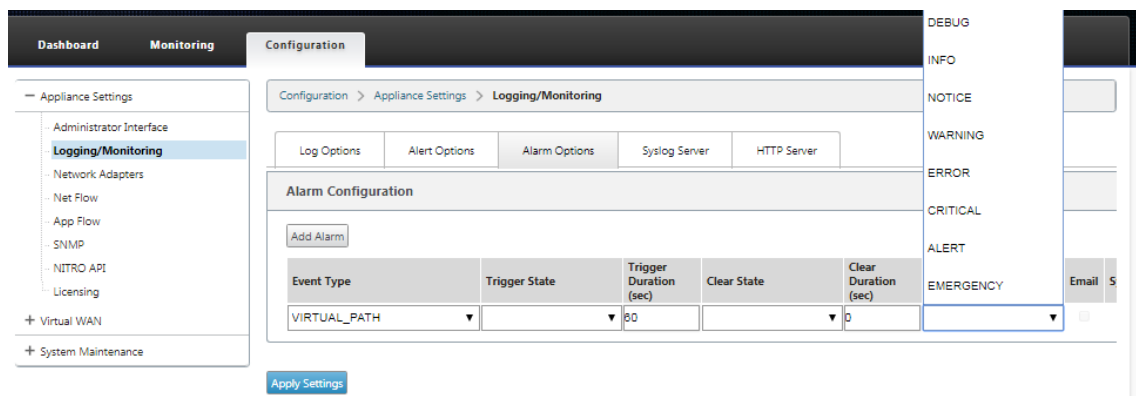
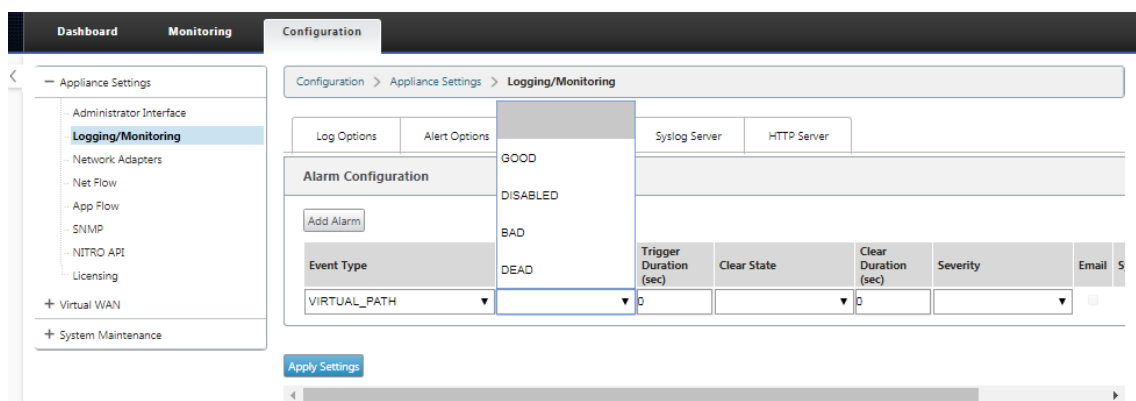
Apply Settings

3. Sélectionnez un **type d’événement** dans la liste déroulante.



4. Sélectionnez les états de notification d'alarme suivants pour le **type d'événement** choisi. L'état de déclenchement et l'état clair changent en fonction du type d'événement sélectionné.

- État de déclenchement —GOOD, DISABLED, BAD, DEAD
- Durée du déclenchement —durée en secondes
- État clair - GOOD, DISABLED, BAD, DEAD
- Effacer la durée —temps en secondes
- Gravité —DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, EVENT, EMERGENCY



5. Cochez les cases **Syslog** et **HTTP** pour recevoir des notifications spécifiques aux événements serveur Syslog et HTTP. Cliquez sur **Appliquer les paramètres**.

Configuration > Appliance Settings > Logging/Monitoring

Log OptionsAlert OptionsAlarm OptionsSyslog ServerHTTP Server

Alarm Configuration

Add Alarm?

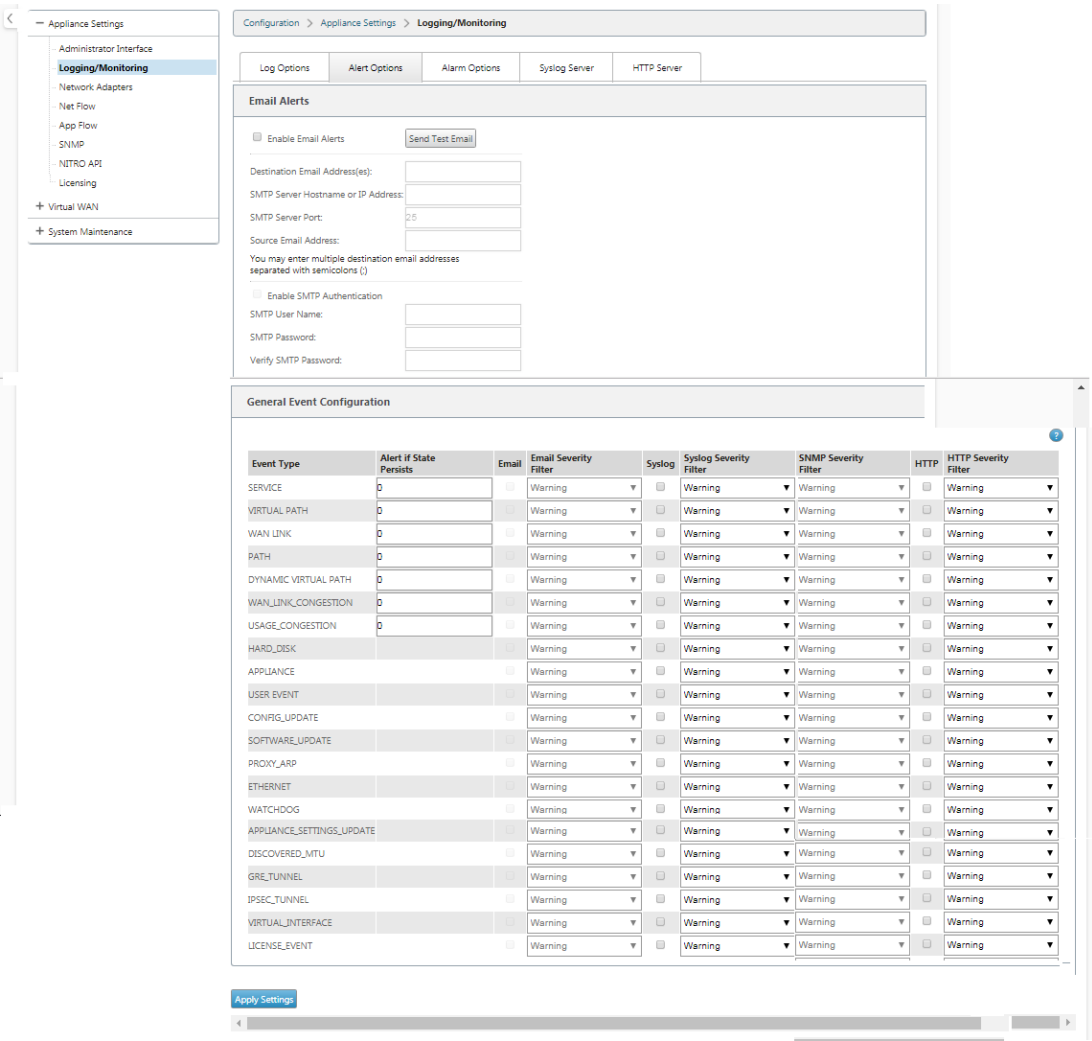
Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog	SNMP	HTTP
VIRTUAL_PATH ▼	DEAD ▼	60	BAD ▼	60	NOTICE ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> ✕

Apply Settings

Pour configurer les options d'événement :

Accédez à la page de l'onglet **Options d'alerte** . Sous la page **Configuration générale des événements**, sélectionnez le filtre de notification du serveur HTTP pour un **type d'événement**, puis cliquez sur **Appliquer les paramètres** .

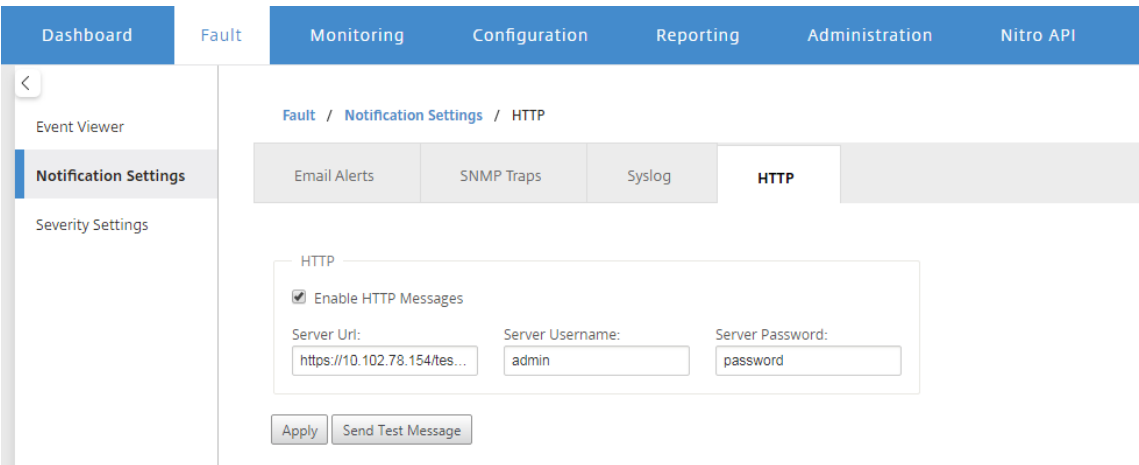
- HTTP
- Filtre de gravité HTTP



Configurer les notifications HTTP dans Citrix SD-WAN Center

Pour configurer les notifications HTTP :

1. Accédez à **Défaillance > Paramètres de notification > HTTP** .



2. Entrez l'**URL du serveur**, le **nom d'utilisateur** du serveur et le **mot de passe** du serveur HTTP.
3. Cliquez sur **Appliquer**

Pour configurer les paramètres de gravité :

1. Accédez à la page **Paramètres de gravité** . Cliquez sur **Activer** pour commencer à surveiller les notifications HTTP pour un type d'événement choisi.

		Email		Syslog		SNMP		HTTP	
Event Type	Alert If State Persists	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter
SERVICE	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WANLINK	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DYNAMIC VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WAN LINK CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USAGE CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼

2. Vous pouvez choisir de surveiller les notifications d'événements Email, Syslog, SNMP et HTTP pour les types d'événements suivants. Cliquez sur **Appliquer**.

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Nitro API

<

Event Viewer

Notification Settings

Severity Settings

Fault / Severity Settings

Event Type	Alert If State Persists	Email		Syslog		SNMP		HTTP	
		Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter
SERVICE	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WANLINK	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DYNAMIC VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WAN LINK CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USAGE CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
HARD DISK		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
APPLIANCE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USER EVENT		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
CONFIG UPDATE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SOFTWARE UPDATE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PROXY ARP		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
ETHERNET		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WATCHDOG		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER SYSTEM		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
APPLIANCE SETTINGS UPDATE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER USER		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER STORAGE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER DATABASE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
CONNECTION TO VIRTUAL WAN		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DISCOVERED MTU		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
GRE TUNNEL		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
IPSEC TUNNEL		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL INTERFACE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
LICENSE EVENT		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼

Apply

Test actif de la bande passante

May 6, 2021

Le test de la bande passante active vous permet d’émettre un test de bande passante de chemin instantané via une liaison WAN Internet publique, ou de planifier des tests de bande passante de connexion WAN Internet publique à effectuer à des moments spécifiques et de façon récurrente. Cette

fonctionnalité est utile pour démontrer la quantité de bande passante disponible entre deux emplacements lors des installations nouvelles et existantes, ainsi que pour tester des chemins pour déterminer le résultat des modifications de paramètres et de confirmation, telles que l'ajustement des paramètres de balise DSCP ou des taux autorisés de bande passante.

Pour utiliser la fonctionnalité de test de bande passante active :

1. Accédez à **Maintenance du système > Diagnostics > Bande passante du chemin**.
2. Sélectionnez le **chemin** souhaité et cliquez sur **Tester**.

The screenshot displays the Citrix SD-WAN 11.4 web interface. The left sidebar shows the navigation menu with 'Diagnostics' selected. The main content area is titled 'Configuration > System Maintenance > Diagnostics'. It features tabs for 'Ping', 'Traceroute', 'Packet Capture', 'Path Bandwidth', 'System Info', 'Diagnostic Data', 'Events', 'Alarms', and 'Diagnostics Tool'. The 'Path Bandwidth' tab is active, showing the 'Instant Path Bandwidth Testing' section. A path is selected as 'MCN-5100-WL-2->BR572-1'. Below this, the 'Results' section shows summary statistics: Minimum Bandwidth: 2883972 kbps, Maximum Bandwidth: 5099707 kbps, and Average Bandwidth: 3109115 kbps. The 'Schedule Path Bandwidth Testing' section includes an 'Add' button and a table for scheduling tests. The 'History Path Bandwidth Testing Result' section shows a table of test results with columns for Num, From Link, To Link, Test Time, Min Bandwidth (kbps), Max Bandwidth (kbps), and Avg Bandwidth (kbps). The table contains 27 entries, showing a range of test times and bandwidth values.

Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	RCN1-S100-WL-1	MCN-5100-WL-1	2/17/2018, 2:01:03 PM	2883972	5099707	4357330
2	RCN1-S100-WL-1	MCN-5100-WL-1	2/17/2018, 4:01:03 PM	3109115	3872000	3616157
3	RCN1-S100-WL-1	MCN-5100-WL-1	2/17/2018, 6:01:04 PM	3041280	4119960	3518949
4	RCN1-S100-WL-1	MCN-5100-WL-1	2/17/2018, 8:01:04 PM	2769377	3700672	3276124
5	RCN1-S100-WL-1	MCN-5100-WL-1	2/17/2018, 10:01:04 PM	409245	3574153	2489269
6	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:04 AM	2481756	4001684	3198214
7	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 AM	2548853	3872000	3236546
8	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 AM	3204413	3982628	3642643
9	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 AM	2997677	4672357	3664018
10	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:04 AM	2248258	6288360	3612666
11	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:04 AM	2410236	3372387	2816032
12	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:03 PM	2613600	4401852	3563752
13	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 PM	2324266	4059961	3101910
14	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 PM	2173340	3684370	2929146
15	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 PM	2613600	3589493	3021690
16	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:03 PM	1670056	3499380	2655200
17	RCN1-S100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:03 PM	1954093	3558944	2975884
18	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 AM	2161116	3784398	2902068
19	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 AM	2986971	4079765	3821158
20	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:04 AM	3514084	4181760	3893381
21	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 6:01:03 AM	3358843	4059961	3756691
22	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 8:01:03 AM	3216738	4245441	3716351
23	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 10:01:04 AM	3558944	4202773	3932908
24	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 PM	3427672	4267102	3838552
25	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 PM	2874061	4224000	3608676
26	RCN1-S100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:03 PM	2816000	6288360	4165337
27	MCN-5100-WL-2	BR572-WL-1	2/19/2018, 5:23:04 PM	936564	1213883	1109046

La sortie affiche la bande passante moyenne utilisée comme valeur à définir comme le taux autorisé pour les résultats de la liaison WAN minimale et maximale de bande passante du test. En plus de la possibilité de tester la bande passante, vous pouvez maintenant modifier le fichier de configuration pour utiliser la bande passante apprise. Ceci est accompli via l'option d'apprentissage automatique qui se trouve sous **Site > [Nom de site] > Liens WAN > [Nom du lien WAN]**

> **Paramètres.** Si cette option est activée, le système utilise la bande passante apprise.

Vous pouvez également planifier des tests récurrents de la bande passante des chemins à intervalles hebdomadaires, quotidiens ou horaires.

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute	
DC_MPLS2->Branch_	every day	Sunday	0	0	X
	every day	Sunday	0	0	↶

Apply Settings

Remarque

Un historique des résultats des tests de bande passante du chemin est affiché au bas de cette page et les résultats sont archivés tous les sept jours.

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute	

Apply Settings

History Path Bandwidth Testing Result

show 50 entries Showing 1 to 14 of 14 entries Search

Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	480818
4	BR_1-MPLS-1	DC_MCN-MPLS-1	3/29/2017, 1:34:00 AM	440056	1083357	725514
5	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:10 AM	506768	786784	638673
6	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:18 AM	462584	1388712	669232
7	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:34:27 AM	380679	727895	533286
8	DC_MCN-MPLS-1	BR_1-MPLS-1	3/29/2017, 1:35:12 AM	26823	35495	30578
9	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:09 AM	350097	733929	591542
10	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:47 AM	476024	789756	639048
11	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:36:56 AM	446292	777674	608533

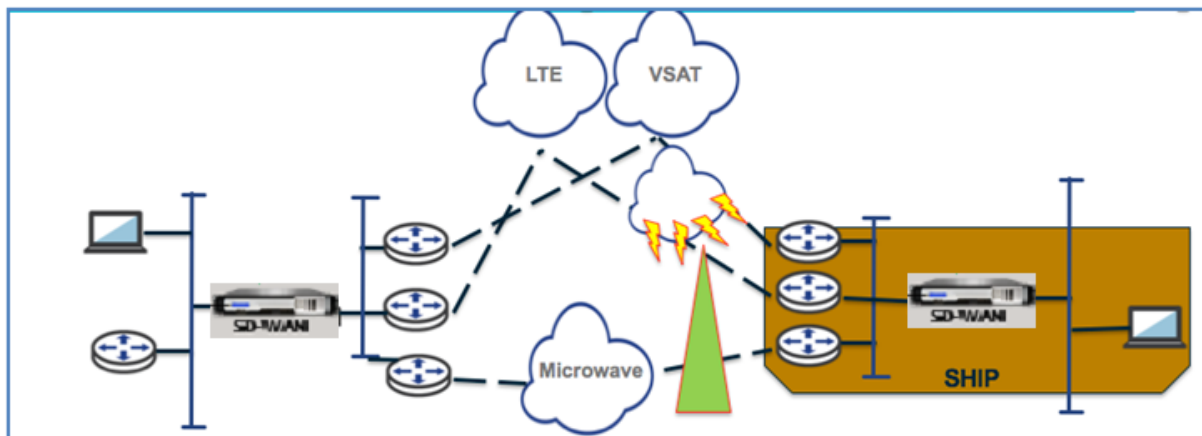
Détection adaptative de la bande passante

May 6, 2021

Cette fonctionnalité s’applique aux réseaux avec des liaisons WAN VSAT, LOS, micro-ondes, 3G/4G/LTE, pour lesquels la bande passante disponible varie en fonction des conditions météorologiques et atmosphériques, de l’emplacement et de la ligne d’obstacles du site. Il permet aux appliances SD-WAN d’ajuster dynamiquement le débit de bande passante sur la liaison WAN en fonction d’

une plage de bande passante définie (débit de liaison WAN minimum et maximum) pour utiliser la quantité maximale de bande passante disponible sans marquer les chemins BAD.

- Plus grande fiabilité de la bande passante (VSAT, micro-ondes, 3G/4G et LTE)
- Prévisibilité accrue de la bande passante adaptative sur les paramètres configurés par l'utilisateur



Pour activer la détection de bande passante adaptative :

Cette fonctionnalité nécessite l'option de sensibilité à la perte incorrecte pour être activée (par défaut/personnalisée) comme condition préalable. Vous pouvez l'activer sous **Global > Groupes Autopath > [Nom du groupe Autopath] > Bad Loss Sensible**.

1. Activez la **détection de bande passante adaptative** sous **Global > Groupes Autopath > [Nom du groupe Autopath] > Bad Loss Sensible**.
2. Accédez à l'**éditeur de configuration > Sites > [Nom de site] > Liens WAN > [Nom du lien WAN] > Paramètres > Paramètres avancés**.

3. Cochez la case **Détection de bande passante adaptative** et entrez une valeur dans le champ **Largeur de bande passante minimale acceptable**.
4. Consultez le tableau **Utilisation et taux autorisés** en accédant à **Surveiller > Statistiques >**

Utilisation du lien WAN > Utilisation et taux autorisés.

Usages and Permitted Rates

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries

FirstPrevious1NextLast

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Recv	5437658	3467411.62	0	0	0	25	NO
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Send	7598365	559484464	118	8.39	12.69	5905	N/A
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Recv	58537274	41745181.34	6562	5203.86	7872.71	8105	NO
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Send	20640095	1497892080	229	17.25	26.1	5880	N/A

Showing 1 to 4 of 4 entries

FirstPrevious1NextLast

Recommandations

May 6, 2021

Les rubriques suivantes fournissent les meilleures pratiques à suivre lors de la conception, de la planification et de l'exécution de la solution Citrix SD-WAN dans votre réseau.

[Sécurité](#)

[Routage](#)

[QoS](#)

[Liens WAN](#)

Sécurité

February 8, 2022

Cet article décrit les meilleures pratiques de sécurité pour la solution Citrix SD-WAN. Il fournit des conseils généraux en matière de sécurité pour les déploiements Citrix SD-WAN.

Directives de déploiement de Citrix SD-WAN

Pour maintenir la sécurité tout au long du cycle de vie du déploiement, Citrix recommande les considérations de sécurité suivantes :

- Sécurité physique
- Sécurité des appareils
- Sécurité du réseau
- Administration et gestion

Sécurité physique

Déployer les appliances Citrix SD-WAN dans une salle de serveurs sécurisée : l'appliance ou le serveur sur lequel Citrix SD-WAN est installé doit être placé dans une salle de serveurs sécurisée ou un centre de données restreint, ce qui protège l'appliance contre tout accès non autorisé. Au minimum, l'accès doit être contrôlé par un lecteur de carte électronique. L'accès à l'appliance est surveillé par CCTV qui enregistre en permanence toutes les activités à des fins d'audit. En cas d'effraction, le système de surveillance électronique doit envoyer une alarme au personnel de sécurité pour une intervention immédiate.

Protégez les ports du panneau avant et de la console contre les accès non autorisés : sécurisez l'appareil dans une grande cage ou un rack grâce au contrôle d'accès par clé physique.

Protéger l'alimentation - Assurez-vous que l'appareil est protégé par un bloc d'alimentation sans coupure.

Sécurité de l'appliance

Pour la sécurité des appareils, sécurisez le système d'exploitation de tout serveur hébergeant une appliance virtuelle Citrix SD-WAN (VPX), effectuez des mises à jour logicielles à distance et les pratiques de gestion du cycle de vie sécurisées suivantes :

- Sécurisez le système d'exploitation du serveur hébergeant une appliance Citrix SD-WAN VPX - Une appliance Citrix SD-WAN VPX s'exécute en tant qu'appliance virtuelle sur un serveur standard. L'accès au serveur standard doit être protégé par un contrôle d'accès basé sur les rôles et une gestion rigoureuse des mots de passe. Citrix recommande également des mises à jour périodiques sur le serveur avec les derniers correctifs de sécurité pour le système d'exploitation, ainsi que des logiciels antivirus mis à jour sur le serveur.
- Effectuer des mises à jour logicielles à distance : installez toutes les mises à jour de sécurité pour résoudre les problèmes connus. Consultez la page Web des Bulletins de sécurité pour vous inscrire et recevoir des alertes de sécurité à jour.
- Suivez les pratiques de gestion du cycle de vie sécurisé : pour gérer une appliance lors du redéploiement ou du lancement de RMA et de la mise hors service des données sensibles, complétez les contre-mesures de rappel des données en supprimant les données persistantes de l'appliance.
- Déployez l'interface de gestion de l'appliance derrière la zone démilitarisée pour vous assurer qu'il n'y a pas d'accès Internet direct à l'interface de gestion. Pour une protection accrue, assurez-vous que le réseau de gestion est isolé d'Internet et que seuls les utilisateurs autorisés disposant d'applications de gestion approuvées s'exécutent sur le réseau.

Sécurité du réseau

Pour la sécurité du réseau, n'utilisez pas le certificat SSL par défaut. Utilisez le protocole TLS (Transport Layer Security) lors de l'accès à l'interface administrateur, protégez l'adresse IP de gestion non routable de l'appliance, configurez une configuration haute disponibilité et mettez en œuvre des mesures de protection d'administration et de gestion appropriées pour le déploiement.

- Ne pas utiliser le certificat SSL par défaut - Un certificat SSL provenant d'une autorité de certification fiable simplifie l'expérience utilisateur pour les applications Web faisant face à Internet. Contrairement à la situation avec un certificat auto-signé ou un certificat de l'autorité de certification fiable, les navigateurs Web n'exigent pas que les utilisateurs installent le certificat à partir de l'autorité de certification fiable pour initier une communication sécurisée avec le serveur Web.
- Utiliser la sécurité de la couche de transport lors de l'accès à l'interface administrateur - Assurez-vous que l'adresse IP de gestion n'est pas accessible à partir d'Internet ou qu'elle est au moins protégée par un pare-feu sécurisé. Assurez-vous que l'adresse IP LOM n'est pas accessible depuis Internet ou qu'elle est au moins protégée par un pare-feu sécurisé.
- Comptes d'administration et de gestion sécurisés — Créez un autre compte d'administrateur, définissez des mots de passe forts pour les comptes d'administrateur et de visionneuse. Lorsque vous configurez l'accès à un compte distant, envisagez de configurer la gestion administrative des comptes authentifiée en externe à l'aide de RADIUS et TACAS. Modifiez le mot de passe par défaut pour les comptes d'utilisateur administrateur, configurez NTP, utilisez la valeur de délai d'expiration de session par défaut, utilisez SNMPv3 avec authentification SHA et chiffrement AES.

Le réseau de superposition Citrix SD-WAN protège les données traversant le réseau de superposition SD-WAN.

Interface administrateur sécurisée

Pour un accès sécurisé à la gestion Web, remplacez les certificats système par défaut en téléchargeant et en installant des certificats à partir d'une autorité de certification fiable. Accédez à **Configuration > Paramètres de l'appliance > Interface administrateur dans l'interface** graphique de l'appliance SD-WAN.

Comptes d'utilisateurs :

- Modifier le mot de passe utilisateur local
- Gérer les utilisateurs

Certs HTTPS :

- Certificat

- Clé

Divers :

- Expiration de la console Web

The screenshot displays the 'Administrator Interface' for the 'Configuration > Appliance Settings' section. The left sidebar lists various settings categories, with 'Administrator Interface' selected. The main content area is titled 'Installed Certificate' and includes tabs for 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', 'HTTPS Settings', and 'Miscellaneous'. The 'HTTPS Cert' tab is active, showing details for an installed certificate. The 'Issued to' and 'Issuer' fields both list Citrix Systems, Inc. with contact information for support@citrix.com. The 'Certificate Details' section provides the fingerprint, start/end dates (March 2017 to March 2027), and serial number. Below this, the 'Upload HTTPS Certificate Files' section includes fields for 'Certificate Filename' and 'Key Filename', each with a 'Choose File' button. The 'Regenerate HTTPS Certificate' section contains a 'Regenerate HTTPS Certificate' button. A note at the bottom of the regenerate section states: 'NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance.'

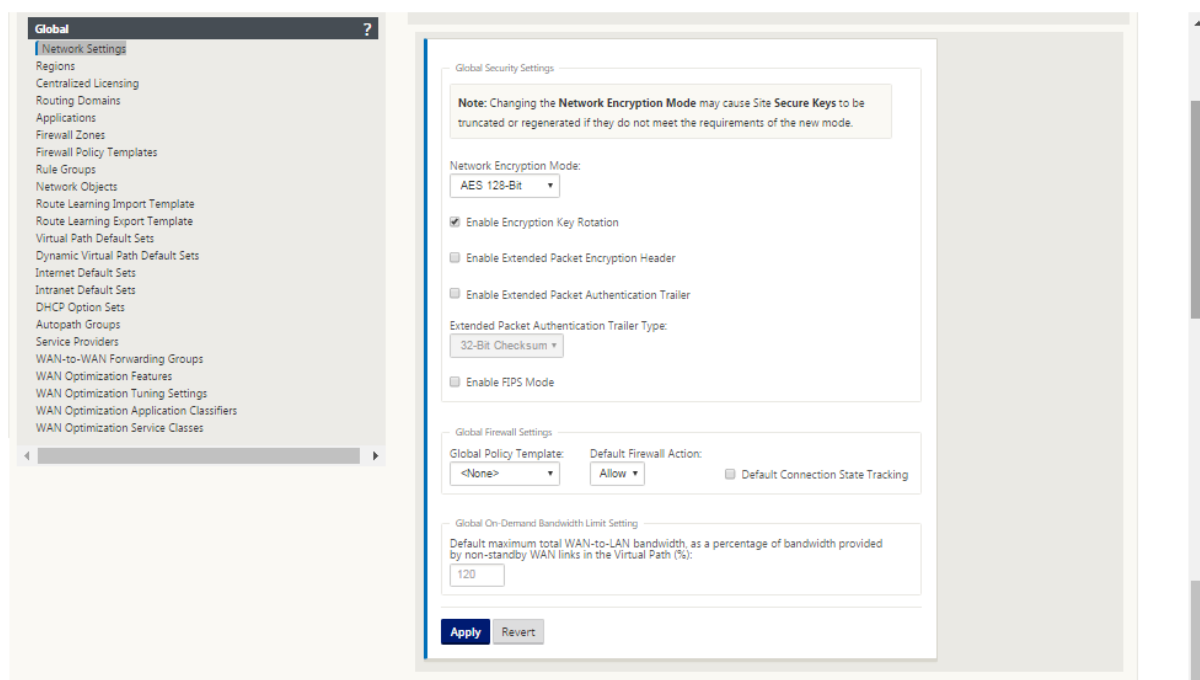
Éditeur de configuration > Global > Paramètres réseau

Paramètres globaux du pare-feu :

- Modèle de stratégie globale
- Actions de pare-feu par
- Suivi des états de connexion par défaut

Paramètres de chiffrement de chemin virtuel global :

- AES 128 bits (par défaut)
- Rotation des clés de chiffrement (par défaut)
- En-tête de chiffrement de paquets étendu
- Bande-annonce d'authentification étendue des paquets



Pensez à utiliser le Citrix Web App Firewall

L'appliance sous licence Citrix ADC fournit un Citrix Web App Firewall intégré qui utilise un modèle de sécurité positif et apprend automatiquement le comportement approprié des applications pour la protection contre les menaces telles que l'injection de commandes, l'injection SQL et les scripts intersites.

Lorsque vous utilisez Citrix Web App Firewall, les utilisateurs peuvent ajouter une sécurité supplémentaire à l'application Web sans modifier le code et avec peu de modifications de configuration. Pour plus d'informations, consultez la section Présentation de [Citrix Web Application Firewall](#).

Paramètres de chiffrement de chemin virtuel global

- Le chiffrement des données AES-128 est activé par défaut. Il est recommandé d'utiliser la protection AES-128 ou plus du niveau de chiffrement AES-256 pour le chiffrement des chemins d'accès. Assurez-vous que « activer la rotation des clés de chiffrement » est défini de manière à garantir la régénération des clés pour chaque chemin virtuel dont le chiffrement est activé à l'aide d'un échange de clés Diffie-Hellman à des intervalles de 10 à 15 minutes.

Si le réseau nécessite l'authentification des messages en plus de la confidentialité (c'est-à-dire la protection contre les falsifications), Citrix recommande d'utiliser le chiffrement des données IPsec. Si seule la confidentialité est requise, Citrix recommande d'utiliser les en-têtes améliorés.

- En-tête de chiffrement de paquets étendu permet d'attribuer un compteur prédéfini aléatoirement au début de chaque message chiffré. Lorsqu'il est chiffré, ce compteur sert de vecteur d'initialisation aléatoire, déterministe uniquement avec la clé de chiffrement. Cela randomise la sortie du cryptage, fournissant un message fort indiscernable. Gardez à l'esprit que lorsqu'elle est activée, cette option augmente la surcharge des paquets de 16 octets
- La remorque d'authentification étendue des paquets ajoute un code d'authentification à la fin de chaque message chiffré. Cette bande-annonce permet de vérifier que les paquets ne sont pas modifiés en transit. Gardez à l'esprit que cette option augmente la surcharge des paquets.

Sécurité du pare-feu

La configuration de pare-feu recommandée est avec une action de pare-feu par défaut comme refuser tout au début, puis ajoutez des exceptions. Avant d'ajouter des règles, documentez et examinez le but de la règle de pare-feu. Utilisez l'inspection Stateful et l'inspection au niveau de l'application lorsque cela est possible. Simplifier les règles et éliminer les règles redondantes. Définissez et respectez un processus de gestion des modifications qui assure le suivi et l'examen des modifications apportées aux paramètres du **pare-feu**. Définissez le pare-feu pour toutes les appliances afin de suivre les connexions via l'appliance à l'aide des paramètres globaux. Le suivi des connexions vérifie que les paquets sont correctement formés et qu'ils sont appropriés à l'état de connexion. Créez des zones appropriées à la hiérarchie logique du réseau ou des zones fonctionnelles de l'organisation. Gardez à l'esprit que les zones sont importantes à l'échelle mondiale et peuvent permettre de traiter des réseaux géographiquement disparates comme la même zone de sécurité. Créez les stratégies les plus spécifiques possibles pour réduire le risque de failles de sécurité, évitez l'utilisation des règles « Tout dans Autoriser ». Configurez et maintenez à jour un modèle de stratégie globale pour créer un niveau de sécurité de base pour toutes les appliances du réseau. Définissez des modèles de stratégie en fonction des rôles fonctionnels des appliances dans le réseau et appliquez-les le cas échéant. Définissez des stratégies sur des sites individuels uniquement lorsque cela est nécessaire.

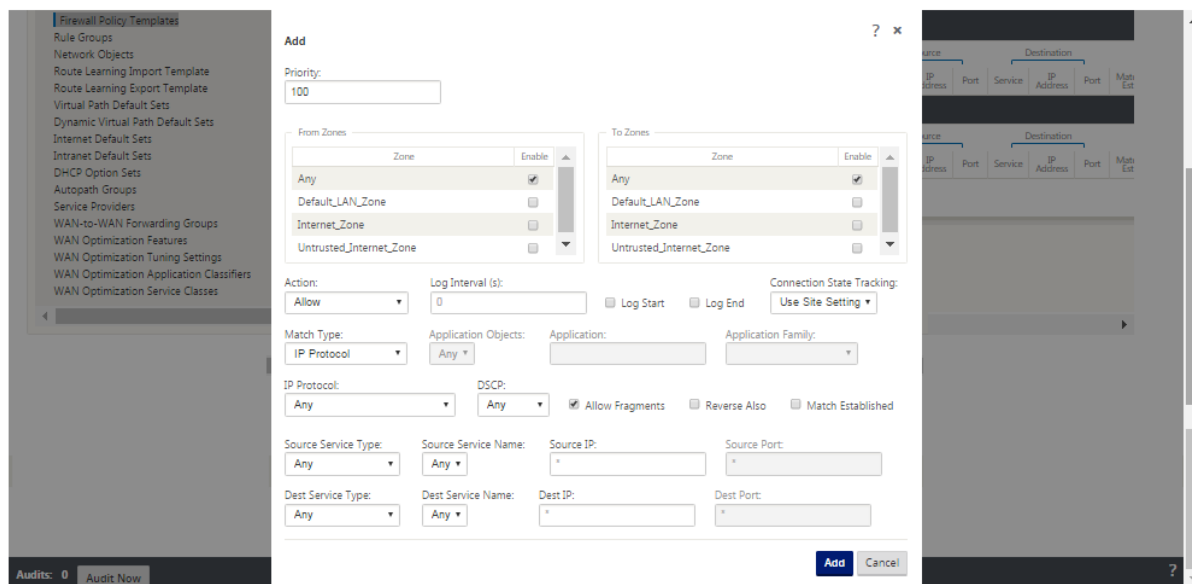
Modèles de pare-feu globaux : les modèles de pare-feu permettent de configurer des paramètres globaux qui ont un impact sur le fonctionnement du pare-feu sur des appliances individuelles fonctionnant dans l'environnement de superposition SD-WAN.

Actions de pare-feu par défaut : Autoriser les paquets ne correspondant à aucune stratégie de filtre sont autorisés. Deny permet que les paquets ne correspondant pas à une stratégie de filtrage soient supprimés.

Suivi de l'état de la connexion par défaut : active le suivi bidirectionnel de l'état des connexions pour les flux TCP, UDP et ICMP qui ne correspondent pas à une stratégie de filtrage ou à une règle NAT. Les flux asymétriques sont bloqués lorsque cela est activé même lorsqu'aucune stratégie de pare-feu n'est définie. Les paramètres peuvent être définis au niveau du site, ce qui remplacera le paramètre global. S'il existe une possibilité de flux asymétriques sur un site, il est recommandé de le faire au

niveau d'un site ou d'une politique et non à l'échelle mondiale.

Zones : les zones de pare-feu définissent le groupe de sécurité logique des réseaux connectés au Citrix SD-WAN. Les zones peuvent être appliquées aux interfaces virtuelles, aux services intranet, aux tunnels GRE et aux tunnels IPSec LAN.



Zone de sécurité de liaison WAN

La zone de sécurité non approuvée doit être configurée sur des liaisons WAN directement connectées à un réseau public (non sécurisé). Non approuvé définira la liaison WAN à son état le plus sécurisé, permettant uniquement le trafic chiffré, authentifié et autorisé à être accepté sur le groupe d'interface. ARP et ICMP à l'adresse IP virtuelle sont les seuls autres types de trafic autorisés. Ce paramètre garantit également que seul le trafic chiffré est envoyé à partir des interfaces associées au groupe Interface.

Domaine de routage

Les domaines de routage sont des systèmes réseau qui incluent un ensemble de routeurs utilisés pour segmenter le trafic réseau. Les nouveaux sires créés sont automatiquement associés au domaine de routage par défaut.

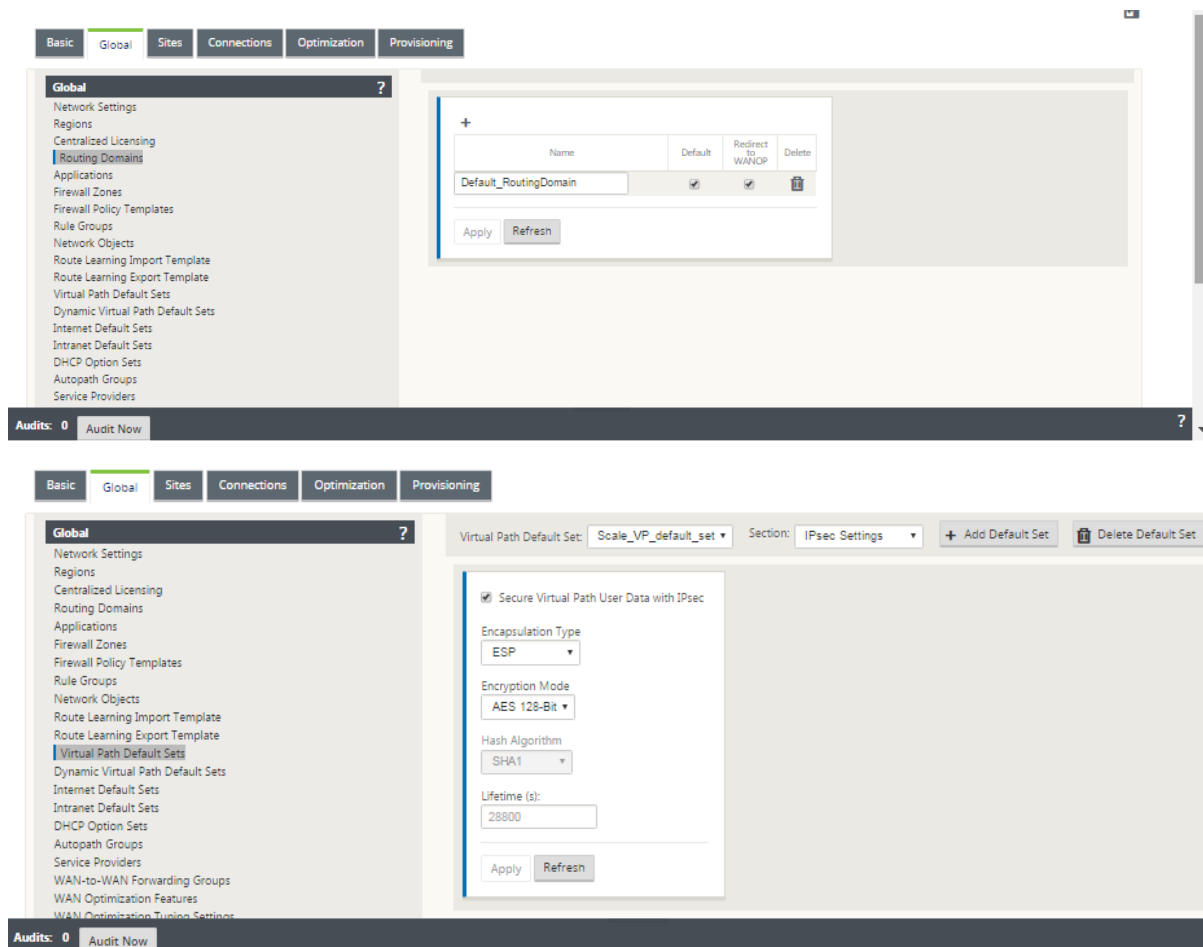
Éditeur de configuration > Global

Domaines de routage

- Default_RoutingDomain

Tunnels IPSec

- Jeux par défaut
- Sécuriser les données utilisateur du chemin virtuel avec IPsec



Tunnels IPsec

Les tunnels IPsec sécurisent à la fois les données utilisateur et les informations d'en-tête. Les appliances Citrix SD-WAN peuvent négocier des tunnels IPsec fixes côté LAN ou WAN avec des homologues non-SD-WAN. Pour les tunnels IPsec sur LAN, un domaine de routage doit être sélectionné. Si le tunnel IPsec utilise un service intranet, le domaine de routage est prédéterminé par le service intranet choisi.

Le tunnel IPsec est établi sur le chemin virtuel avant que les données puissent circuler sur le réseau de superposition SD-WAN.

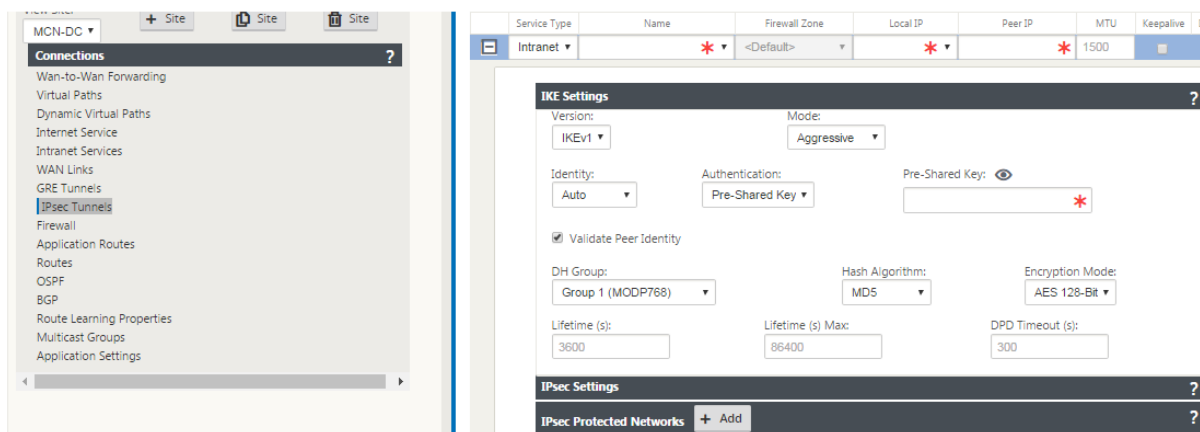
- Les options de type d'encapsulation incluent ESP - les données sont encapsulées et cryptées, ESP+Auth - les données sont encapsulées, cryptées et validées avec un HMAC, AH - les données sont validées avec un HMAC.
- Le mode de chiffrement est l'algorithme de chiffrement utilisé lorsque ESP est activé.

- Hash Algorithm est utilisé pour générer un HMAC.
- La durée de vie est une durée préférée, en secondes, pour qu'une association de sécurité IPsec existe. 0 peut être utilisé pour un nombre illimité.

Paramètres IKE

Internet Key Exchange (IKE) est un protocole IPsec utilisé pour créer une association de sécurité (SA). Les appliances Citrix SD-WAN prennent en charge les protocoles IKEV1 et IKEV2.

- Le mode peut être le mode principal ou le mode agressif.
- L'identité peut être automatique pour identifier le pair, ou une adresse IP peut être utilisée pour spécifier manuellement l'adresse IP du pair.
- L'authentification permet l'authentification ou le certificat de clé pré-partagée comme méthode d'authentification.
- Validate Peer Identity permet de valider l'identité homologue de l'IKE si le type d'ID de l'homologue est pris en charge, sinon n'activez pas cette fonctionnalité.
- Les groupes Diffie-Hellman sont disponibles pour la génération de clés IKE avec le groupe 1 à 768 bits, le groupe 2 à 1024 bits et le groupe 5 à 1536 bits.
- L'algorithme de hachage comprend MD5, SHA1 et SHA-256 a des algorithmes sont disponibles pour les messages IKE.
- Les modes de chiffrement comprennent les modes de chiffrement AES-128, AES-192 et AES-256 sont disponibles pour les messages IKE.
- Les paramètres IKEv2 incluent l'authentification par les pairs et l'algorithme d'intégrité.



Configuration du pare-feu

Les problèmes courants suivants peuvent être identifiés en vérifiant la configuration du routeur et du pare-feu en amont :

- Queues/paramètres QoS MPLS : vérifiez que le trafic encapsulé UDP entre les adresses IP virtuelles SD-WAN ne souffre pas en raison des paramètres de **QoS** sur les appliances intermédiaires du réseau.
- Tout le trafic sur les liaisons WAN configurées sur le réseau SD-WAN doit être traité par l'appliance Citrix SD-WAN à l'aide du type de service approprié (chemin virtuel, Internet, intranet et local).
- Si le trafic doit contourner l'appliance Citrix SD-WAN et utiliser le même lien sous-jacent, des réservations de bande passante appropriées pour le trafic SD-WAN doivent être effectuées sur le routeur. En outre, la capacité de liaison doit être configurée en conséquence dans la configuration SD-WAN.
- Vérifiez que le routeur/pare-feu intermédiaire n'a pas de limites UDP d'inondation et/ou de PPS appliquées. Cela permet de réguler le trafic lorsqu'il est envoyé via le chemin virtuel (encapsulé UDP).

Routage

May 6, 2021

Cet article décrit les meilleures pratiques de routage pour la solution Citrix SD-WAN.

Service de routage Internet/Intranet

Lorsque le service Internet n'est pas configuré pour le trafic lié à Internet et à la place, soit une route **locale** ou une route **passthrough** est configurée pour atteindre le routeur de Gateway. Le routeur utilise les liaisons WAN configurées sur l'appliance SD-WAN, ce qui entraîne un problème de surallocation de liaison.

Si une route Internet est configurée comme **Local** sur le MCN, elle est apprise par tous les sites SD-WAN de la branche et configurée comme **Route de chemin virtuel** par défaut. Cela implique que le trafic lié à Internet au niveau de l'appliance de succursale est acheminé via le chemin virtuel vers MCN.

Priorité de routage

Ordre de priorité du routage :

- Correspondance de préfixe : les préfixes les plus longs correspondent.
- Service : Local, Service de chemin virtuel, Internet, Intranet, Passthrough
- Coût de l'itinéraire

Asymétrie de routage

Assurez-vous qu'il n'y a pas d'asymétrie de routage dans le réseau (l'appliance NetScaler SD-WAN transmet le trafic dans une seule direction). Cela crée des problèmes avec le suivi des connexions au pare-feu et l'inspection approfondie des paquets.

QoS

June 8, 2022

Tenez compte des éléments suivants lors de la configuration de QoS :

- Comprenez vos modèles de trafic réseau et vos besoins. Vous devrez peut-être observer les **statistiques de classe QoS** et modifier la profondeur de la file d'attente et/ou modifier le pourcentage de partage de classe QoS par défaut pour éviter les baisses de queue, comme indiqué dans les statistiques QoS.
- Parfois, l'ensemble du sous-réseau est ajouté à une règle pour faciliter la configuration au lieu de créer des règles pour des adresses IP d'applications spécifiques. L'ajout d'un sous-réseau entier à une règle mappe incorrectement tout le trafic du sous-réseau à une règle. Par conséquent, les classes QoS associées à cette règle peuvent entraîner une chute de queue et une mauvaise performance de l'application ou une expérience utilisateur.

Liens WAN

May 6, 2021

Les plates-formes Citrix SD-WAN prennent en charge jusqu'à 8 connexions Internet publiques et 32 connexions MPLS privées. Cet article décrit les meilleures pratiques de configuration de liaison WAN pour la solution Citrix SD-WAN.

Points à retenir lors de la configuration des liaisons WAN :

- Configurez le débit **autorisé et physique** comme bande passante réelle de la liaison WAN. Dans les cas où la capacité totale de liaison WAN n'est pas censée être utilisée par l'appliance SD-WAN, modifiez le taux **autorisé** en conséquence.
- Lorsque vous n'êtes pas sûr de la bande passante et que les liens ne sont pas fiables, vous pouvez activer la fonctionnalité d'**apprentissage automatique**. La fonction d'apprentissage **automatique apprend** uniquement la capacité de liaison sous-jacente et utilise la même valeur à l'avenir.

- Si le lien sous-jacent n'est pas stable et ne garantit pas une bande passante fixe (par exemple, les liaisons 4G), utilisez la fonction de **détection de bande passante adaptative**.
- Il n'est pas recommandé d'activer l'**apprentissage automatique** et la **détection de bande passante adaptative** sur la même liaison WAN.
- Configurez manuellement le MCN/RCN avec le débit physique d'entrée et de sortie pour tous les liens WAN, car il est le point central de distribution de la bande passante entre plusieurs branches.
- Pour une fiabilité accrue des charges de travail/services importants du datacenter, lorsque l'apprentissage automatique n'est pas utilisé, utilisez des liens fiables avec des SLA qui n'ont pas de variation aléatoire de la capacité.
- Si le lien sous-jacent n'est pas stable, modifiez les paramètres de chemin suivants :
 - Paramètres de perte
 - Désactiver l'instabilité sensible
 - Temps de silence
- Utilisez l'**outil Diagnostic** pour vérifier la santé/capacité du lien.
- Si le SD-WAN est déployé en mode à **un bras**, veillez à ne pas dépasser la capacité physique de la liaison sous-jacente.

Vérification de l'état des liens FAI

Pour les nouveaux déploiements, antérieurs au déploiement SD-WAN et lors de l'ajout d'une nouvelle liaison FAI au déploiement SD-WAN existant :

- Vérifiez le type de lien. Par exemple ; MPLS, ADSL, 4G.
- Caractéristiques du réseau. Par exemple - bande passante, perte, latence et gigue.

Ces informations vous aident à configurer le réseau SD-WAN selon vos besoins.

Topologie réseau

Il est généralement observé que le trafic réseau spécifique contourne les appliances Citrix SD-WAN et utilise la même liaison sous-jacente configurée dans le réseau SD-WAN. Étant donné que le SD-WAN n'a pas une visibilité complète sur l'utilisation des liens, il y a des chances que le SD-WAN suralloue la liaison, ce qui entraîne des problèmes de performances et de PATH.

Provisioning

Points à prendre en compte lors du Provisioning du SD-WAN :

- Par défaut, toutes les succursales et services WAN (Virtual Path, Internet/Intranet) reçoivent une part égale de la bande passante.
- Les sites de provisioning doivent être modifiés lorsqu'il existe une grande disparité en termes d'exigence de bande passante ou de disponibilité entre les sites de connexion.
- Lorsque les chemins virtuels dynamiques sont activés entre les sites disponibles maximum, la capacité de liaison WAN est partagée entre le chemin virtuel statique vers DC et les chemins virtuels dynamiques.

Questions fréquentes

May 6, 2021

Haute disponibilité

Quelle est la différence entre la haute disponibilité et l'appliance secondaire (Geo) ?

- La haute disponibilité garantit la tolérance aux pannes. L'appliance secondaire (Geo) permet la reprise après sinistre.
- La haute disponibilité peut être configurée pour les appliances MCN, RCN et succursales. L'appliance secondaire (Geo) peut être configurée uniquement pour les MCN et les RCN.
- Les appliances haute disponibilité sont configurées sur le même site ou emplacement géographique. Une appliance de succursale située à un emplacement géographique différent est configurée en tant qu'appliance MCN/RCN secondaire (Geo).
- Les appliances primaires et secondaires haute disponibilité doivent être les mêmes modèles de plate-forme. L'appliance secondaire (Geo) peut être le même modèle de plate-forme que le MCN/RCN principal.
- La haute disponibilité a une priorité plus élevée que secondaire (Geo). Si une appliance (MCN/RCN) est configurée avec une appliance haute disponibilité et secondaire (Geo), en cas de défaillance de l'appliance secondaire haute disponibilité devient active. Si les deux appliances haute disponibilité échouent ou si le site du centre de données se bloque, l'appliance secondaire (Geo) devient active.
- En haute disponibilité, le basculement principal/secondaire se produit instantanément ou dans les 10 à 12 secondes suivant le déploiement de haute disponibilité. Le commutateur MCN/RCN principal vers secondaire (Geo) MCN/RCN, se produit après 15 secondes de l'inactivité principale.

- La configuration haute disponibilité vous permet de configurer la réutilisation principale. Vous ne pouvez pas configurer la récupération principale pour l'appliance secondaire (Geo), la récupération principale se produit automatiquement après que l'appliance principale est de retour et que la temporisation de blocage expire.

Mise à niveau en une seule étape

Remarque

WANOP, SVM et XenServer Supplemental/HF sont considérés comme des composants OS.

Dois-je utiliser *.tar.gz*, ou un package *.zip* de mise à niveau en une seule étape pour mettre à niveau vers 9.3.x à partir de ma version actuelle (8.1.x, 9.1.x, 9.2.x) ?

Utilisez les fichiers *.tar.gz* des plates-formes concernées pour mettre à niveau le logiciel SD-WAN vers la version 9.3.x. Une fois le logiciel SD-WAN mis à niveau vers la version 9.3.x, effectuez la gestion des modifications à l'aide du package *.zip* pour transférer/déployer des packages logiciels de composants du système d'exploitation. Après l'activation, le MCN transfère/met en place les composants du système d'exploitation pour toutes les succursales concernées.

Après la mise à niveau vers la 9.3.0 en utilisant le package de mise à niveau en une seule étape (fichier *.zip*) faire, je dois effectuer *.upg* mise à niveau sur chaque appliance ?

Non, la mise à jour/mise à niveau du logiciel du système d'exploitation sera prise en charge par le package *.zip* de mise à niveau en une seule étape et il est installé selon les détails de planification fournis par vous dans les paramètres de gestion des modifications des sites respectifs.

Pourquoi devrais-je utiliser *.tar.gz* suivi du package *.zip* pour mettre à niveau des versions antérieures à 9.3 vers 9.3.x, et pourquoi ne pas utiliser directement le package *.zip* de 9.3.x ?

Le package de mise à niveau Single Step est pris en charge à partir de 9.3.0.161 et sur les versions antérieures (antérieures à la version 9.3), ce package n'est pas reconnu. Lorsque le package *.zip* de mise à niveau en une seule étape est téléchargé dans la boîte de réception de gestion des modifications, le système génère une erreur indiquant que le package n'est pas reconnu. Par conséquent, mettez d'abord à niveau le logiciel SD-WAN vers la version 9.3 ou supérieure, puis effectuez la gestion des modifications à l'aide du package *.zip*.

Comment les composants du système d'exploitation seront-ils installés lors d'une mise à niveau en une seule étape, si *.upg* mise à niveau n'est pas effectuée ?

Le MCN transférera ou déploiera des packages logiciels de composants du système d'exploitation basés sur le modèle de l'appliance, une fois la gestion des modifications terminée à l'aide du package *.zip* de mise à niveau en une seule étape. Après l'activation, le MCN commence à transférer ou à transférer les packages logiciels des composants du système d'exploitation pour les succursales qui en ont besoin pour la mise à jour/mise à niveau planifiée.

Comment installer les composants du système d'exploitation sans planifier les installations ultérieures ?

Définissez la valeur de la **fenêtre de maintenance** sur '0' pour une installation instantanée des composants du système d'exploitation.

Remarque

L'installation démarre uniquement lorsque l'apppliance a reçu tout le package nécessaire pour le site, même lorsque la valeur de la **fenêtre de maintenance** est définie sur « 0 ».

Quelle est l'utilité de l'installation de planification ? Puis-je utiliser les instructions de planification pour mettre à niveau VW seul ?

L'installation planifiée a été introduite dans SD-WAN version 9.3 et s'applique uniquement aux composants du système d'exploitation et non à la mise à niveau logicielle VW. Avec la mise à niveau en une seule étape, vous n'avez pas besoin de vous connecter à chaque appliance pour effectuer la mise à niveau des composants du système d'exploitation et l'option de planification vous permet de planifier l'installation des composants du système d'exploitation à un autre moment que la mise à niveau de la version du logiciel VW.

Pourquoi les informations de planification de la page Paramètres de gestion des modifications affichent-elles la date de planification passée par défaut et qu'est-ce que cela signifie ?

La page **Paramètres de gestion des modifications** affiche les informations de planification par défaut, c'est-à-dire "start" : « 2016-05-21 21:20:00 », « window » : 1, « repeat » : 1, « unit » : « days ». Si la date est une date antérieure, cela signifie que, l'installation planifiée est basée sur l'heure et d'autres paramètres comme la fenêtre de maintenance, la fenêtre de répétition et l'unité, et non sur la date.

Quelle est la date/heure d'installation de planification par défaut définie sur, est-il générique ou dépendant de l'apppliance locale ?

Par défaut, les détails de planification sont définis comme '2016-05-21 à 21:20:00 (fenêtre de maintenance de 1 heure et répétée tous les 1 jour) '. Ce détail dépend du site local de l'apppliance.

Comment puis-je installer les composants OS immédiatement sans attendre la fenêtre de maintenance ou planifiée ?

Définissez la valeur de la **fenêtre Maintenance** sur '0' dans la page **Paramètres de gestion des modifications**, ce qui remplace l'heure d'installation planifiée.

Quel paquet je devrais utiliser pour la mise à niveau lorsque la version actuelle du logiciel est 9.3.x ou supérieure ?

Utilisez le package .zip de mise à niveau en une seule étape pour mettre à niveau vers des versions supérieures lorsque la version actuelle du logiciel 9.3.x ou supérieure.

Quand les fichiers des composants du système d'exploitation sont-ils transférés ou préparé pour être déployé vers les succursales ?

Les fichiers des composants du système d'exploitation sont transférés/transférés vers les succursales concernées après l'activation est terminée lorsque la gestion des modifications est effectuée à l'aide du package .zip de mise à niveau en une seule étape pour mettre à niveau le système.

Quelles sont les appliances qui reçoivent les fichiers des composants du système d'exploitation, dépendent-elles de la plate-forme ou toutes les succursales le reçoivent ?

Les appliances basées sur l'Hypervisor, telles que **SD-WAN —400, 800, 1000, 2000 SE** et **SD-WAN —2100** sous licence EE, recevront les composants du système d'exploitation à mettre à niveau.

Comment fonctionne la planification ?

Par défaut, les détails de la planification sont définis comme *2016-05-21 à 21:20:00 (fenêtre de maintenance de 1 heure et répétée tous les 1 jours)* et cela implique que le système vérifiera si un nouveau logiciel est disponible pour l'installation tous les **jours car la valeur de répétition est définie sur 1** jour et aura d'une **heure** et l'installation sera déclenchée/tentée (si un nouveau logiciel est disponible) à **21:20:00** (heure locale de l'appliance) à compter du **2016-05-21**

Comment puis-je savoir si les composants du système d'exploitation ont été mis à niveau ?

Dans la colonne **État**, vous pouvez voir une graduation verte. En survolant, vous pouvez voir le message **Mise à niveau est réussie**.

Comment planifier l'installation des composants du système d'exploitation pour RCN et ses succursales ?

La planification pour RCN est effectuée à partir de la page **Paramètres de gestion des modifications** MCN. Pour les succursales RNC, vous devez vous connecter au RNC respectif et définir les détails du planning.

D'où puis-je obtenir l'état de l'installation planifiée ?

L'état de l'installation planifiée pour RCN peut être obtenu à partir de la page **Paramètres de gestion des modifications** de MCN. Pour les succursales de la RCN, vous devez vous connecter à la RCN respective pour obtenir le statut.

Comment obtenir l'état de l'installation planifiée ?

Utilisez le bouton Actualiser fourni sur la page **Paramètres de gestion des modifications** pour obtenir l'état de MCN et RCN pour les branches dans la région par défaut et RCN respectivement.

Scheduling Information

Show100▼entries

Search:

Edit Selected

Refresh

<input type="checkbox"/>	Site Name	Scheduling Information	Status	Edit
<input type="checkbox"/>	GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries

Previous

1

Next

Puis-je utiliser le fichier *tar.gz* pour mettre à niveau vers la prochaine version, lorsque la mise à niveau en une seule étape a été utilisée pour la mise à niveau logicielle précédente ?

Vous pouvez utiliser le fichier *tar.gz* pour effectuer la mise à niveau, mais ce n'est pas recommandé car vous pouvez effectuer la mise à niveau logicielle à l'aide de la *upg* fichier. Chargez le fichier pour mettre à niveau le logiciel du composant du système d'exploitation (OS) en vous connectant à chaque appliance applicable. À partir de la version 9.3 1, la page **Mettre à jour le logiciel du système d'exploitation** est amortie. Par conséquent, vous pouvez effectuer la gestion des modifications à l'aide du package *.zip* pour mettre à niveau les composants du système d'exploitation.

Comment pouvons-nous valider les versions en cours d'exécution des composants OS ?

Maintenant, vous ne pouvez pas valider les versions en cours d'exécution des composants du système d'exploitation à partir de l'interface utilisateur. Vous pouvez vous connecter à partir de chaque console ou demander à STS de consulter ces informations.

Quelle différence cela ferait si j'ai des appareils en métal nu dans mon réseau ? La planification a-t-elle un impact sur les appliances virtuelles ou les appareils virtuels ?

Les appareils métalliques nus comme **SD-WAN —410,2100,4100,5100 SD-WAN** exécutent unique-

ment des logiciels SD-WAN. Les appareils en métal nu n'ont pas besoin de packages de composants du système d'exploitation. Ces plates-formes sont traitées sur un pied d'égalité avec les appliances SD-WAN VPX-SE en termes de besoins logiciels. Le MCN ne transfère pas les packages de composants du système d'exploitation vers ces appliances. La définition des informations de planification ne prend pas effet pour ces appliances, car elles ne disposent pas de composants du système d'exploitation nécessitant une mise à niveau.

Comment fonctionne SSU dans l'environnement et le déploiement à haute disponibilité ?

Dans le déploiement de haute disponibilité chez MCN, nous avons une limitation, où le commutateur MCN actif bascule le rôle du MCN principal pendant la gestion des modifications et du MCN Stand-by/Secondaire prend le relais. Dans ce cas, vous pouvez effectuer une nouvelle fois la gestion des modifications avec le package *.zip* sur le MCN actif pour les packages ou vous pouvez revenir à MCN principal en basculant le rôle de MCN actif afin que le MCN principal d'origine puisse assumer le rôle des packages de composants du système d'exploitation à transférer vers d'autres branches.

Comment fonctionne la mise à niveau en une seule étape dans l'environnement et le déploiement à haute disponibilité ?

Lors de la mise à niveau en une seule étape dans le déploiement haute disponibilité, le rôle du MCN principal et du MCN de secours est activé. C'est une limitation. Si cela se produit, effectuez à nouveau la gestion des modifications avec le package *.zip* sur le MCN actif. Vous pouvez également revenir au MCN principal en activant le rôle du MCN actif afin que le MCN principal d'origine puisse préparer le déploiement des packages de composants du système d'exploitation vers les succursales.

La mise à niveau en une seule étape est-elle prise en charge pour un déploiement sans contact pour redémarrer des appliances ?

Oui, elle peut être utilisée.

Puis-je utiliser une mise à niveau en une seule étape pour mettre à niveau mon appliance WANOP autonome ?

Non.

Puis-je utiliser la mise à niveau en une seule étape pour mettre à niveau l'appliance WANOP autonome déployée en mode deux boîtes ?

Non. Seule l'appliance SD-WAN faisant partie du mode boîtier serait mise à niveau et non l'appliance autonome WANOP.

Quel paquet dois-je utiliser pour mettre à niveau vers un réseau à plusieurs niveaux ?

Utilisez le fichier *ns-sdw-sw-<release-version>.zip* du package de mise à niveau en une seule étape lorsque la version actuelle du logiciel est 9.3.x ou supérieure. MCN prend en charge le déploiement du package vers RCN et RCNS stade package logiciel à ses succursales respectives.

Après avoir téléchargé le fichier *ns-sdw-sw-<release-version>.zip*, je ne vois qu'un seul modèle de plate-forme sous le logiciel actuel ?

À partir de la version 10.0, la prise en charge de l'architecture d'échelle est introduite pour accélérer le traitement de la mise à niveau en une seule étape. Vous pouvez voir uniquement le modèle de plate-forme MCN sous le logiciel actuel. Les autres packages de matériel sont listés/affichés/traités lorsque vous cliquez sur le bouton **Vérifier** ou **Stage Appliance**.

Pour les appliances VPX/VPXL/bare metal, quels paquets sont préparé pour être déployé pour RCN ?

Le package est déployé vers les RCN parce que les succursales RCN peuvent être de n'importe quel modèle de plate-forme. Par conséquent, ils ont besoin de tous les paquets.

Comment mon site de succursale derrière le RCN obtient-il des packages de composants du système d'exploitation si RCN est une appliance VPX et que la branche est une appliance qui a besoin de ces packages ?

RCN met en place le package approprié à la branche qui a besoin des packages de composants du système d'exploitation après l'activation du package logiciel SD-WAN VW.

Puis-je choisir Ignorer incomplet pendant la phase intermédiaire et passer à l'étape suivante de la gestion des modifications ? Quel impact cela a-t-il sur les sites qui n'ont pas terminé le déploiement lorsque ce bouton est sélectionné ?

Oui, vous pouvez cliquer sur **Ignorer incomplet**. Ceci active le bouton **Suivant** et la barre de progression s'affiche. Cette option est fournie pour les scénarios dans lesquels le site n'est pas accessible et où la gestion des modifications attend toujours que le déploiement se termine pour ce site, afin que les utilisateurs puissent passer à l'étape suivante en ignorant l'état de déploiement et procéder à l'activation. Une fois le site mis en place, MCN met en place le package après l'activation.

Mise à niveau partielle du logiciel

Qu'est-ce que la mise à niveau partielle du site et comment puis-je l'utiliser ?

La mise à niveau partielle du logiciel de site est une nouvelle fonctionnalité introduite dans la version 10.0. Vous pouvez préparer le déploiement une version plus récente de la version 10.x à partir du MCN et activer la version du logiciel gérée à partir de la page **Gestion des changements locaux** sur les sites/branches sélectionnés. Avant d'activer le logiciel préparé pour être déployé sur le site/branche, assurez-vous que la case à cocher est activée à partir de MCN.

- Cette fonction est désactivée par défaut. Le mécanisme de correction existant permet de synchroniser le réseau. L'utilisateur doit choisir d'autoriser des mises à niveau partielles du site en activant une case à cocher dans la page **Configuration > Paramètres de gestion des modifications**.

- La mise à niveau partielle du logiciel peut être effectuée uniquement sur une succursale ou des RCN et non sur le MCN.

Voici le scénario lorsque la mise à niveau partielle du logiciel du site peut être utilisée :

Valider si un correctif logiciel avec les modifications pertinentes est compatible et fonctionne pour un site spécifique (lorsque la mise à niveau partielle du site est effectuée). Vérifiez que le logiciel mis à niveau fonctionne comme prévu. Cela permet de valider le nouveau logiciel et de corriger sur un site spécifique avant de mettre à niveau l'ensemble du réseau avec le nouveau logiciel.

Puis-je utiliser cette fonctionnalité pour effectuer une mise à niveau à partir de :

- 10.0 à 10.x
- 10.0.x à 10.0.y
- 11.0 à 11.y
- 11.0.x à 11.0.y
- Tout ce qui précède

La mise à niveau partielle du logiciel de site n'est applicable que lorsque l'appliance exécute les versions 10.x et ultérieures et peut être utilisée dans la même version majeure du logiciel. Il peut être utilisé entre les versions 10.0 à 10.0.x/10.x. Uniquement dans le cadre d'une mise à niveau partielle du logiciel de site, la configuration ne peut pas être modifiée.

Puis-je tester une nouvelle fonctionnalité à tester dans le cadre d'une mise à niveau logicielle partielle en les activant depuis la configuration ?

Non, la mise à niveau logicielle partielle nécessite que les configurations Active et Staged soient identiques. Seule la version du logiciel peut changer.

Puis-je désactiver la mise à niveau logicielle partielle pour RCN ?

Non, la mise à niveau logicielle partielle peut être activée ou désactivée à partir de MCN uniquement. Au RCN, la fonctionnalité est en mode lecture seule.

Puis-je utiliser la mise à niveau logicielle partielle lorsque j'ai activé les versions 9.3.x et 10.0.x comme intermédiaires ?

Non, l'appliance doit être exécutée à partir de la version 10.0 en tant que logiciel actif.

Que se passe-t-il lorsque l'option Mise à niveau logicielle partielle est désactivée à partir de MCN, alors que certaines branches sont déjà mises à niveau via cette fonctionnalité ?

MCN envoie une notification à toutes les appliances du réseau indiquant que la fonctionnalité Mise à niveau logicielle partielle est désactivée, puis toutes les appliances du réseau sont corrigées automatiquement par MCN pour qu'elles correspondent à sa version active et intermédiaire. Toutefois, notez que MCN s'attend à ce que l'option Activer la mise en scène soit cliquée à partir de la page Activation

de **Gestion des modifications**. Vous pouvez choisir d'activer le réseau en cliquant sur **Activer intermédiaire** ou en cliquant sur **Modifier la préparation** pour annuler l'état en acceptant la confirmation.

Modification de la gestion des modifications

Qu'est-ce que la fonctionnalité annulée dans le processus de gestion des modifications ?

À partir de la version 9.3, la fonction d'annulation de la gestion des modifications permet de revenir à la configuration de travail lorsque des événements inattendus tels que le plantage de t2-app ou l'état du chemin virtuel deviennent inactifs après une mise à jour de la configuration. Le réseau et les appliances sont surveillés pendant 10 minutes après la mise à jour de la configuration et, pendant cet intervalle, si les conditions suivantes sont remplies (à condition que l'utilisateur ait activé la fonctionnalité), la configuration intermédiaire est activée. Le logiciel actif est restauré en Staged.

Quels sont les critères pour la réinitialisation de la configuration au redémarrage ?

L'annulation se produit si les scénarios suivants sont rencontrés :

1. MCN - Après le changement de config/logiciel, si le service t2_app est désactivé en raison d'un plantage dans un intervalle de 30 min.
2. MCN - Après le changement de configuration ou de logiciel, si le service Virtual Path est en panne pendant 30 minutes ou plus après l'activation. La fonction Rollback est lancée sur les sites.
3. Site : après la modification de la configuration ou du logiciel, si le site perd sa communication avec MCN, la fonction d'annulation est lancée.
4. Site - Après le changement de config/logiciel, le service t2_app est désactivé en raison d'un plantage dans un intervalle de 30 min.

Que se passe-t-il après la restauration ?

Après la restauration de la configuration, la configuration ou le logiciel défectueux est présenté comme logiciel Staged.

Comment les utilisateurs sont-ils informés que la reprise s'est produite ?

Une bannière jaune en haut de l'interface graphique indiquant que Config est annulée en raison d'erreurs respectives s'affiche. En outre, vous pouvez voir qu'il s'agit de la table d'état de gestion des modifications. Il affiche l'**erreur de configuration** ou l'**erreur logicielle** correspondant au site pour lequel la reprise s'est produite.

La configuration et les logiciels sont-ils tous les deux annulés ?

Oui, si la mise à niveau logicielle est également effectuée avec la configuration, et que le scénario de retour arrière est rencontré, le logiciel est également annulé.

Que se passe-t-il s'il y a un problème dans MCN et qu'il se bloque ou perd la connectivité avec tous les sites ?

L'ensemble du réseau est annulé sauf MCN. La notification s'affiche et tous les sites affichent l'état de la reprise dans la section Gestion des modifications. Vous pouvez résoudre le problème manuellement sur MCN.

Peut-on désactiver cette fonctionnalité ?

Oui, nous pouvons désactiver cette fonctionnalité juste avant l'activation. Toutefois, cette fonctionnalité est activée par défaut.

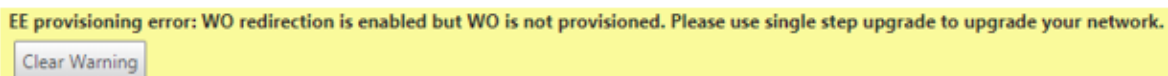
Comment la rétrogradation interagit-elle avec la mise à niveau logicielle partielle lorsque j'ai un réseau à plusieurs niveaux ?

- Si la mise à niveau logicielle partielle est désactivée et si un site d'une région (ou de la RCN) est annulé, la région ayant le problème est annulée et une fois terminée, la restauration se propage jusqu'au MCN. En conséquence, le MCN et le reste du réseau pour revenir en arrière. Le RCN dans la région qui a annulé et le MCN affichent la bannière d'annulation que le MCN ne peut pas fermer automatiquement la bannière d'annulation sur le RCN.
- Si la mise à niveau logicielle partielle est activée et si un site dans une région (ou la RCN) est annulé, seule cette région est annulée. L'événement rollback ne se propage pas vers le MCN. En conséquence, le MCN quitte la région. Le MCN n'affiche pas la bannière d'annulation et ne revient pas lui-même ou le réseau.

Dans ces deux scénarios, la RCN affiche la bannière d'annulation jusqu'à ce qu'elle soit rejetée. Parce que, il ne peut pas être automatiquement rejeté par MCN.

2100 Édition Premium (Entreprise)

Qu'est-ce que le message suivant indique lorsqu'une appliance 2100 EE est mise à niveau vers la version 10.0 ?



L'appliance possède une licence EE ou la redirection WANOP est activée à partir de MCN. Vous pouvez planifier l'installation des composants WANOP pour démarrer le Provisioning des fonctionnalités WANOP sur cette plate-forme.

Informations connexes

- [Déploiement Zéro Touch sur LTE](#)
- [Configurer le MCN secondaire dans HA](#)

Matériel de référence

May 6, 2021

[Bibliothèque de signatures d'application](#)

Liste des applications que les appliances Citrix SD-WAN peuvent identifier à l'aide de l'inspection approfondie des paquets.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).