Citrix SD-WAN 11.5

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 pour Citrix SD-WAN version 11.5

November 16, 2022

Ce document de notes de version décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour Citrix SD-WAN 11.5.

Remarques

Ce document de notes de publication 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

Les améliorations et modifications disponibles dans la version SD-WAN 11.5.

Divers

Spécifications de la version 11.5 de Citrix SD-WAN

- Citrix SD-WAN 11.5.0 est une version à disponibilité limitée, recommandée et prise en charge uniquement pour des clients/déploiements de production spécifiques.
- La version SD-WAN 11.5.0 ne prend pas en charge les déploiements Advanced Edition (AE), Premium Edition (PE) et WAN Optimization.
- Le SD-WAN 11.5.0 prend uniquement en charge les plates-formes mentionnées dans les modèles de plate-forme SD-WAN et les packages logiciels.
- SD-WAN 11.5.0 ne prend pas en charge Citrix SD-WAN Center ou Citrix SD-WAN Orchestrator pour les environnements locaux.
- Le microprogramme SD-WAN 11.5.0 n'est pas disponible sur la page Téléchargements de Citrix.
- La version SD-WAN 11.5.0 est disponible uniquement via le service Citrix SD-WAN Orchestrator et uniquement sur certains points de présence géographiques.
- Assurez-vous d'obtenir les approbations et les conseils requis de la part de Citrix Product Management/Citrix Support avant de déployer la version 11.5.0 sur un réseau de production.

[NSSDW-38486]

Le**service Citrix SD-WAN Orchestrator remplace** l'**éditeur de configuration SD-WAN** :

À partir de la version 11.5 de Citrix SD-WAN, l'éditeur de configuration SD-WAN et le SD-WAN Center sont remplacés par le service Citrix SD-WAN Orchestrator. Le service Citrix SD-WAN Orchestrator prend en charge toutes les configurations actuellement effectuées via l'éditeur de configuration SD-WAN. Pour plus de détails sur le service Citrix SD-WAN Orchestrator, consultez la section Service Citrix SD-WAN Orchestrator.

[NSSDW-33528]

Prise en charge IPv6 :

À partir de la version 11.5.0 de Citrix SD-WAN, les fonctionnalités de plan de données suivantes des appliances Citrix SD-WAN prennent en charge l'adresse IPv6 :

- Itinéraires d'application
- Optimisation des services Citrix Cloud et Gateway
- Classification d'application basée sur un nom de domaine
- Personnalisation dynamique des fichiers PAC
- Routage dynamique
- Paramètres par défaut du pare-feu
- Multidiffusion
- Optimisation d'Office 365
- PPPoE
- Rapports de site - Protocoles de routage
- VRRP

Après avoir configuré les fonctionnalités répertoriées ci-dessus, si vous désactivez le protocole IPv4 ou IPv6, les fonctionnalités ne fonctionnent pas comme prévu.

[SDW-23397, NSSDW-29150, NSSDW-29152, NSSDW-29154, NSSDW-29155, NSSDW-29156, NSSDW-29468, NSSDW-1940, NSSDW-1995]

Améliorations du monitoring :

Les tableaux de bord de surveillance suivants sont améliorés et disponibles sur la nouvelle interface utilisateur de l'appliance :

- Redirecteur DNS transparent
- Connexions du pare-feu, filtre de pare-feu, NAT du pare-feu
- IGMP, proxy IGMP, statistiques IGMP
- IKE, IPsec

- Groupe de multidiffusion, source du groupe de multidiffusion, destination du groupe de multidiffusion
- Sessions PPPoE
- VRRP

[NSSDW-33763]

Plateforme et systèmes

Matériel de référence - bibliothèque de signatures d'application

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

[NSSDW-38209]

Problèmes résolus

Les problèmes résolus dans la version SD-WAN 11.5.

Divers

L'état de l'interface de gestion de certaines appliances SD-WAN était affiché comme Down sur la page **Ethernet Interface Settings** de l'interface utilisateur. Ce problème se produisait lorsque certaines appliances dont la gestion intrabande était prise en charge, l'option d'utilisation hors bande était disponible. Par conséquent, les appliances utilisaient une interface de gestion hors bande pour accéder au service SD-WAN Orchestrator.

[NSSDW-37028]

Problèmes connus

Les problèmes qui existent dans la version SD-WAN 11.5.

En cas de déploiement à l'échelle lors d'un changement de configuration sur un site ou une liaison WAN, le redémarrage du moteur de routage entraîne l'interruption des sessions BGP.

[SDWANHELP-2594]

Une appliance SD-WAN s'est bloquée de manière inattendue. Ce problème s'est produit lorsque :

- Le trafic de multidiffusion IPv6 circulait lors d'une mise à niveau logicielle.

- Le trafic de multidiffusion IPv6 a été généré à l'aide d'un tunnel GRE Intranet et a été répliqué vers plusieurs branches via le chemin virtuel à l'aide de la configuration proxy MLDV2.

Solution : désactivez le trafic de multidiffusion IPv6 pendant la mise à niveau logicielle et activez-le une fois la mise à niveau réussie.

[NSSDW-38495]

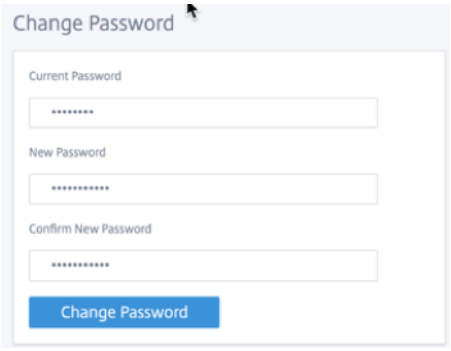
Nouvelle interface utilisateur pour les appliances SD-WAN

August 31, 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]>`.

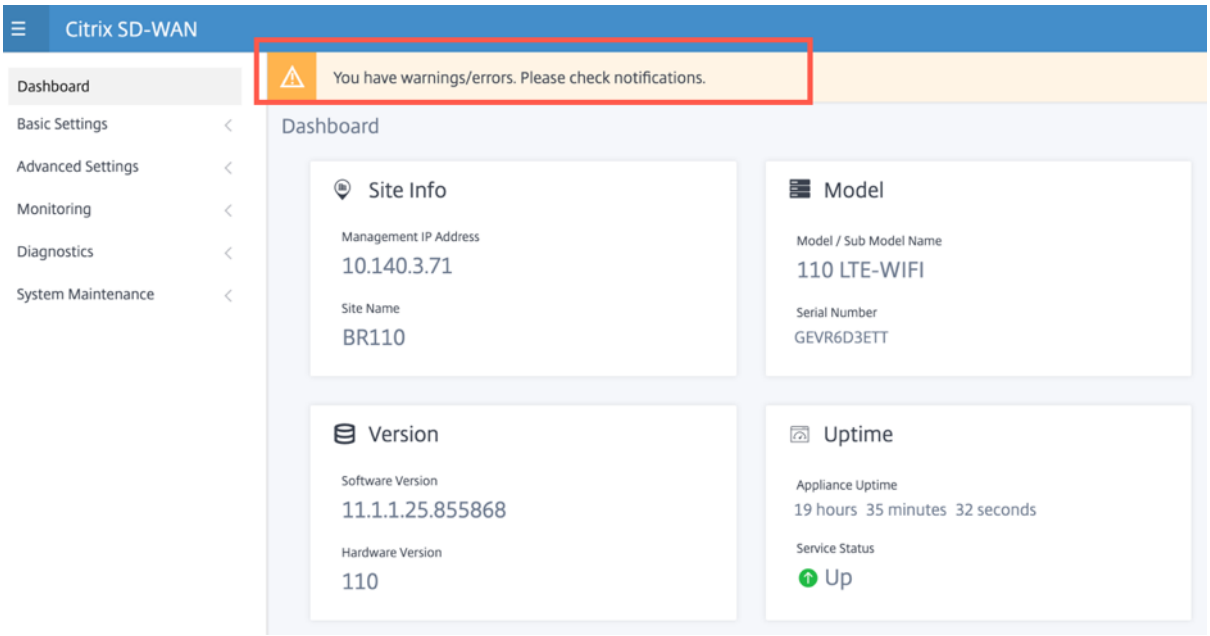
   Exemple : `https://[fd73:xxxx:yyyy:26::9]`

> **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.

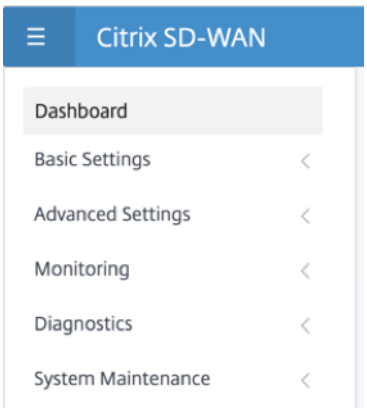
Une fois que vous êtes connecté, vous pouvez voir que le panneau de navigation se trouve sur le côté gauche. En outre, vous pouvez voir une bannière de notifications sur le tableau de bord s'il y a des avertissements ou des erreurs.



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.

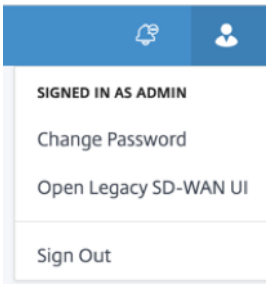
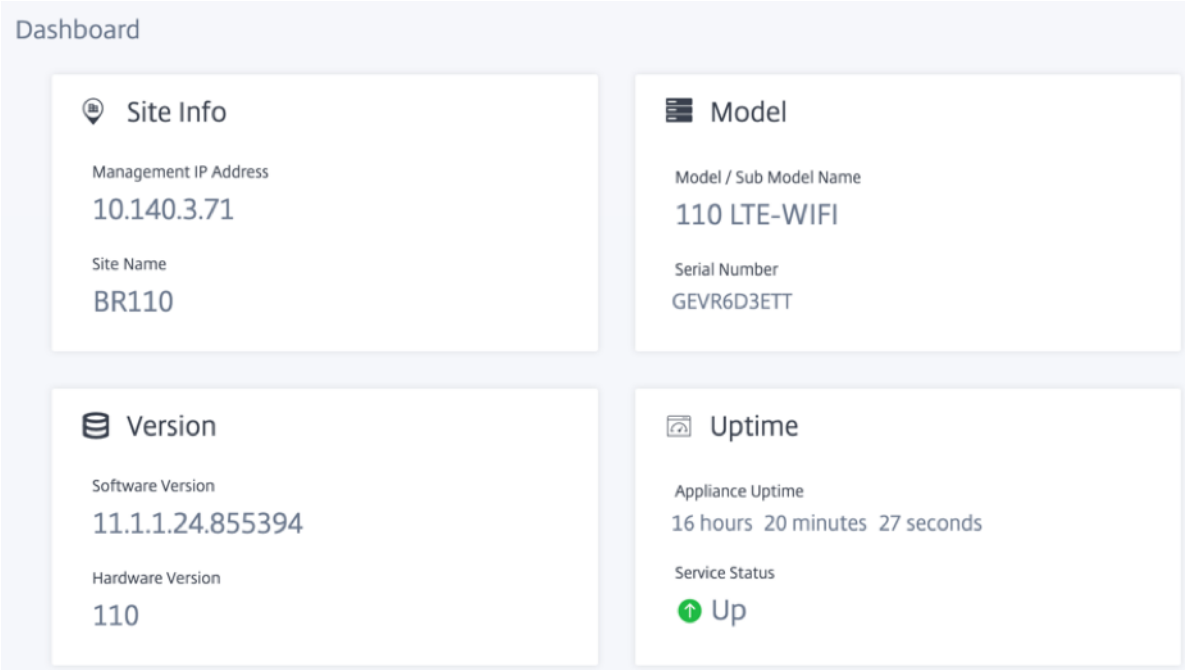


Tableau de bord

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 lenuméro de série**
- **Version** —Affiche la version **logicielleet 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.

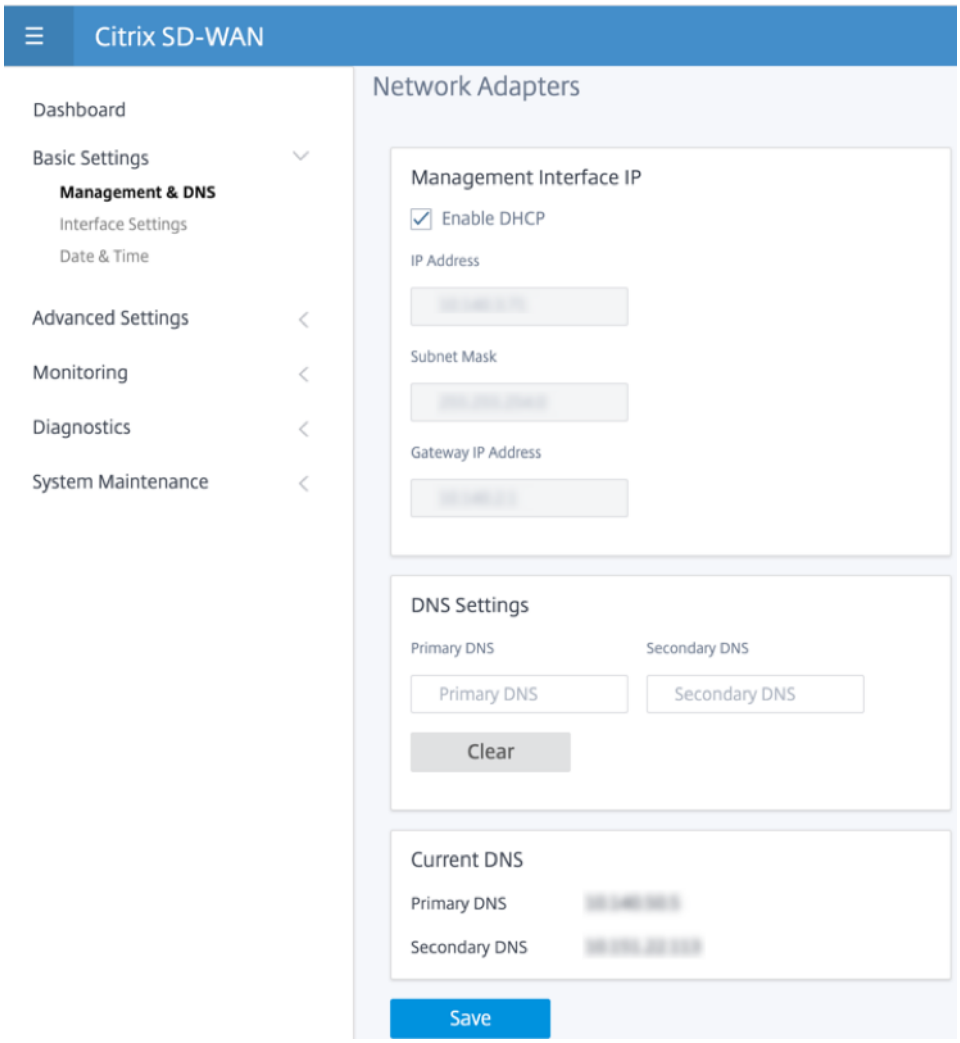
- Gestion et DNS
- Paramètres de l'interface
- Groupe LAG LACP
- Date et heure
- Serveur RADIUS
- Serveur TACACS+

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.

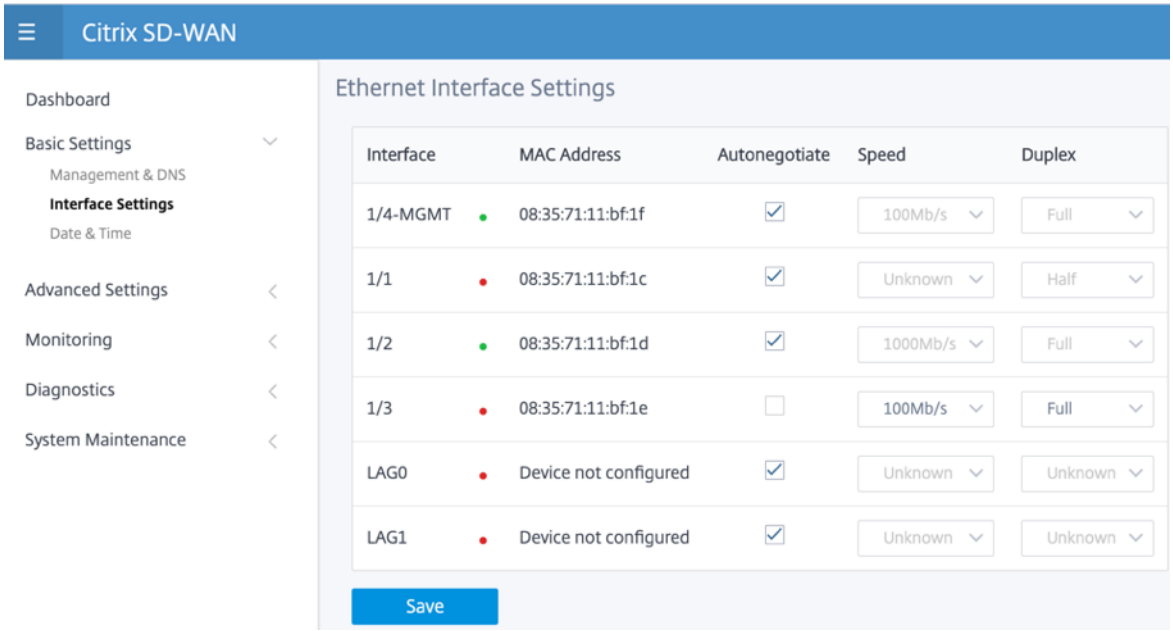
Pour ajouter ou supprimer une adresse IPv4 à la liste autorisée, vous devez accéder à l'interface de gestion de l'appliance SD-WAN à l'aide d'une adresse IPv4 uniquement. De même, pour ajouter ou supprimer une adresse IPv6 à la liste autorisée, vous devez accéder à l'interface de gestion du matériel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



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.



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.

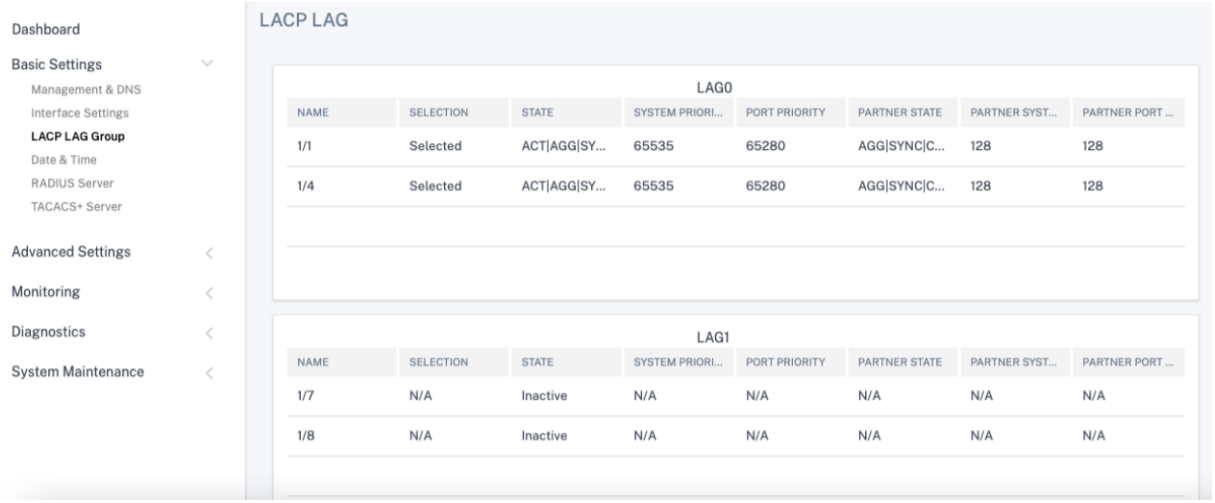
Vous pouvez créer un maximum de 4 LAG avec un maximum de 4 ports regroupés dans chaque LAG sur les appliances Citrix SD-WAN.

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.

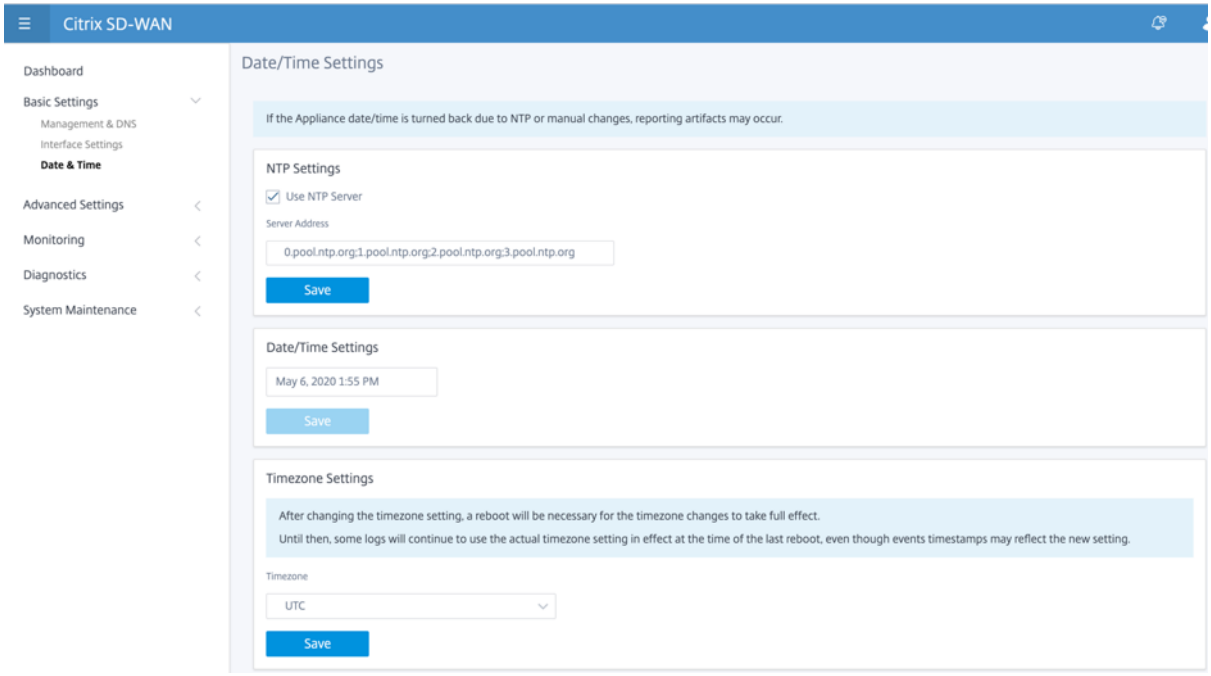
Pour afficher les détails du LAG, accédez à **Paramètres de base** > **Groupe LAG LACP**.

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.



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.



Serveur RADIUS

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

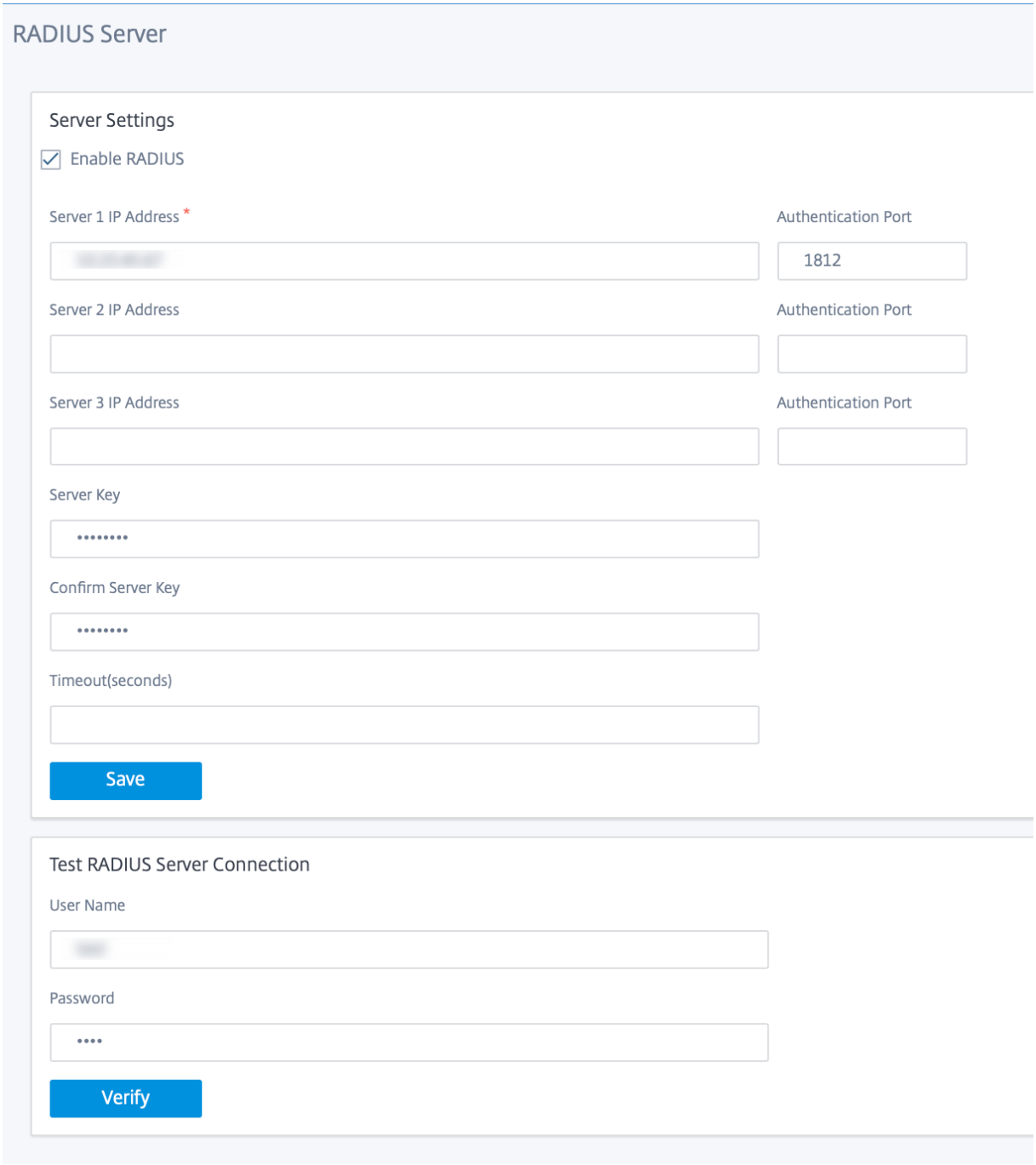
Pour configurer le serveur RADIUS :

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 **Enregistrer**.

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



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.

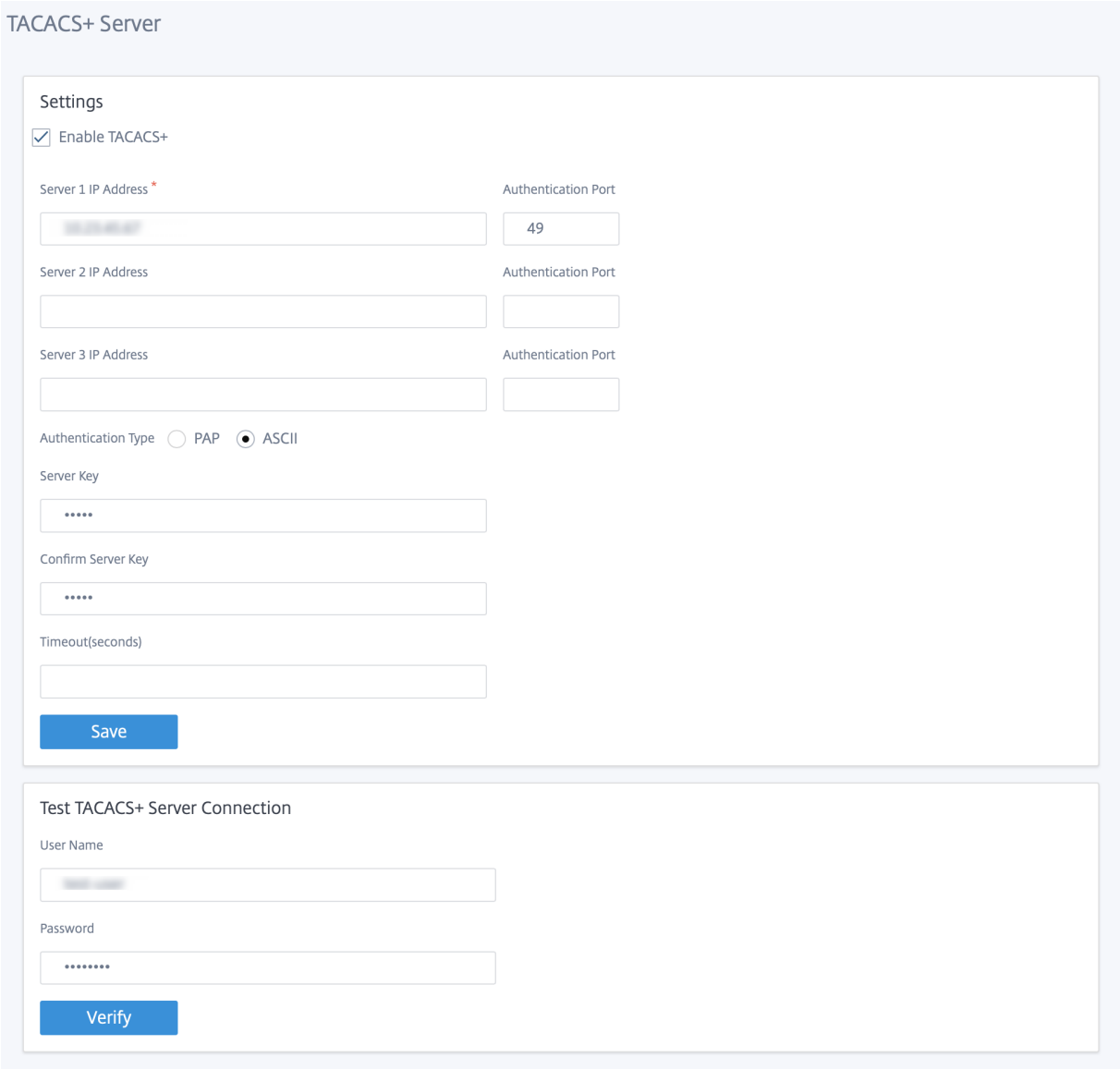
Pour configurer le serveur TACACS+ :

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 **Enregistrer**.

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



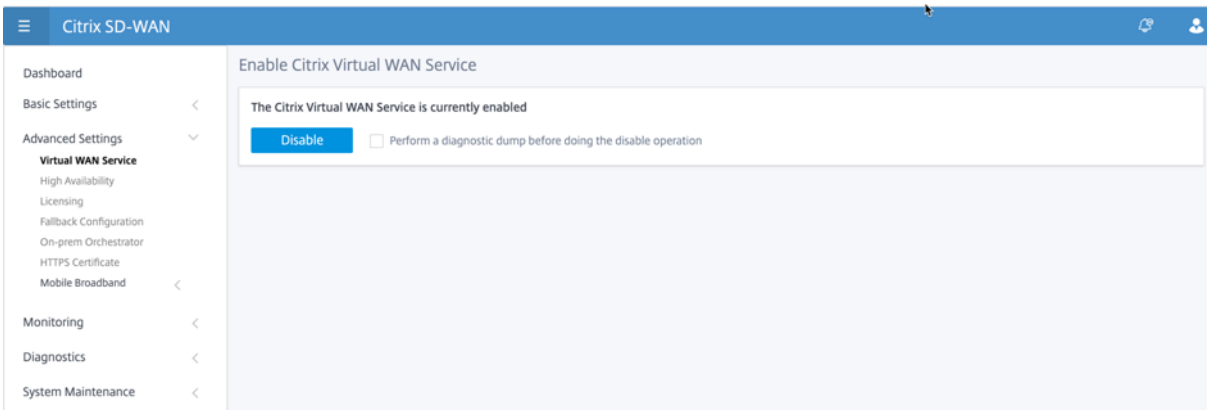
Paramètres avancés

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

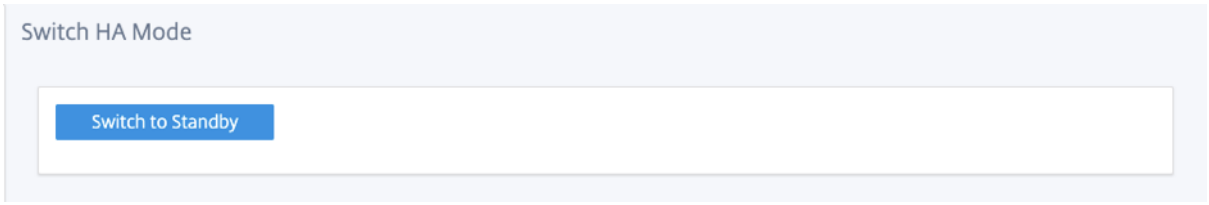
Citrix Virtual WAN Service

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.

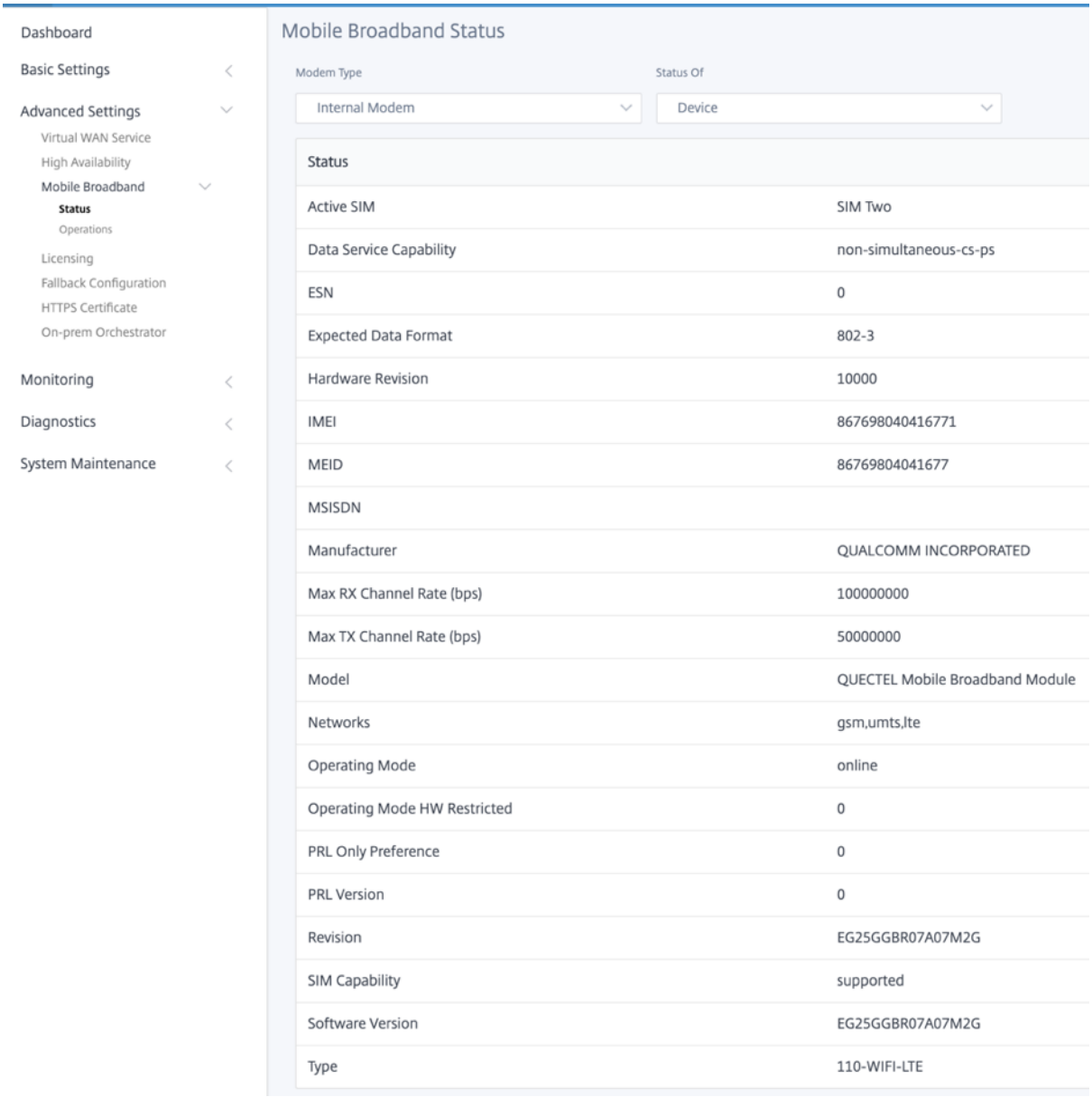
Exigences pour modem LTE externe :

- 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.



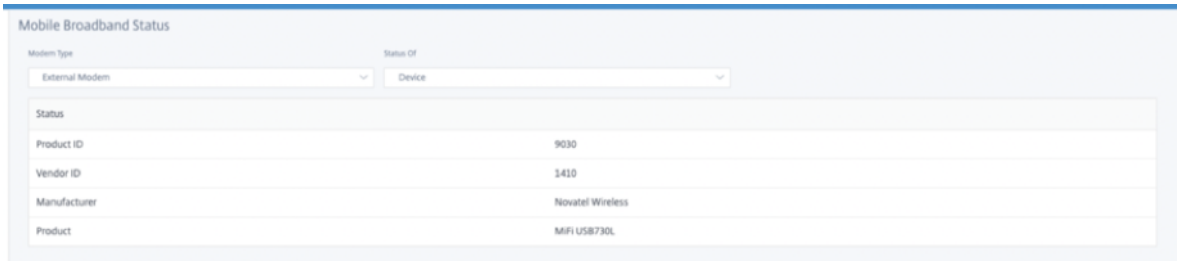
Voici quelques informations d'état utiles :

- **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.

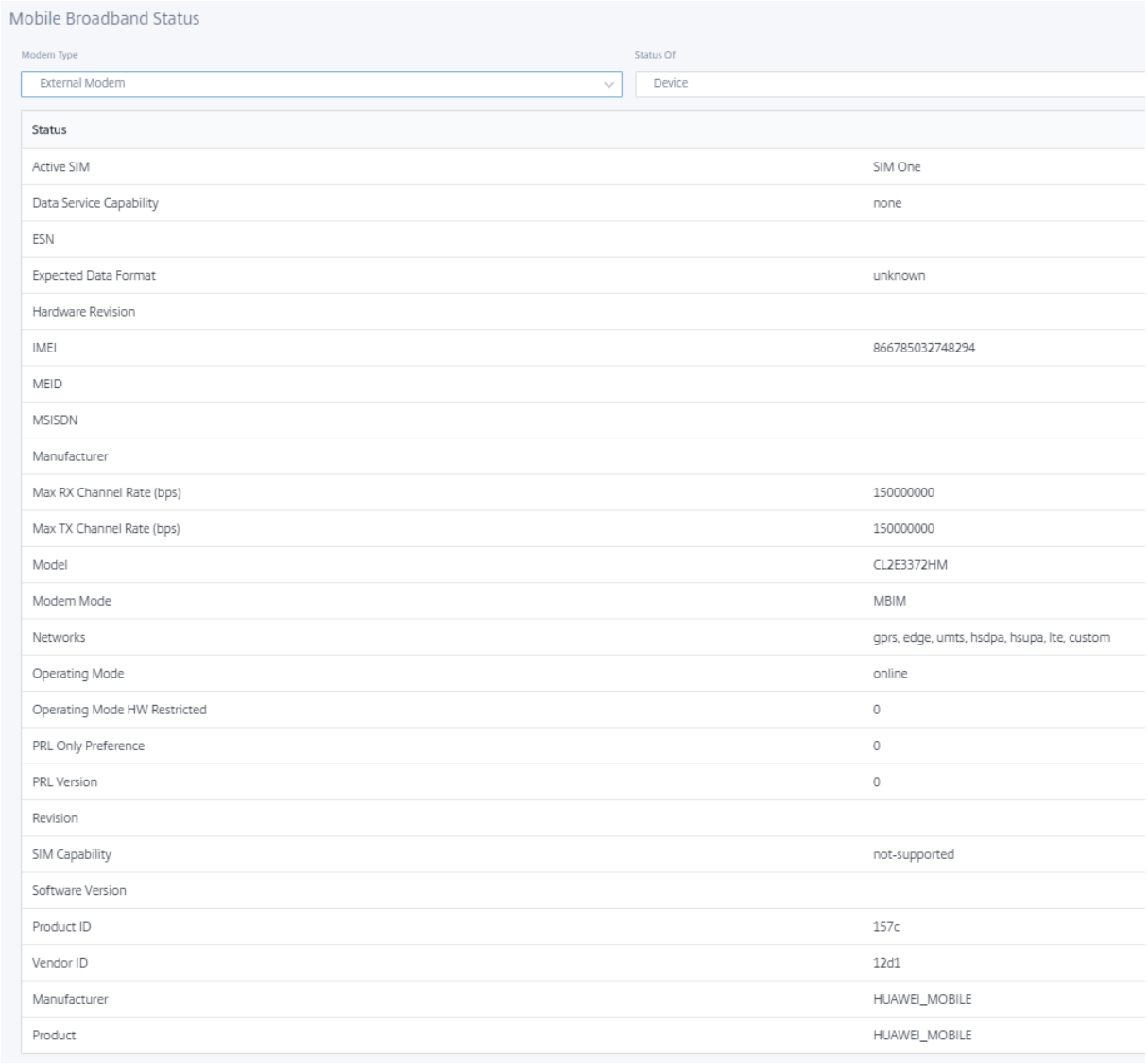
- **Capacités SIM** : indique si la carte SIM est prise en charge ou non.
- **Modèle** : affiche le nom du module haut débit mobile.

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**.

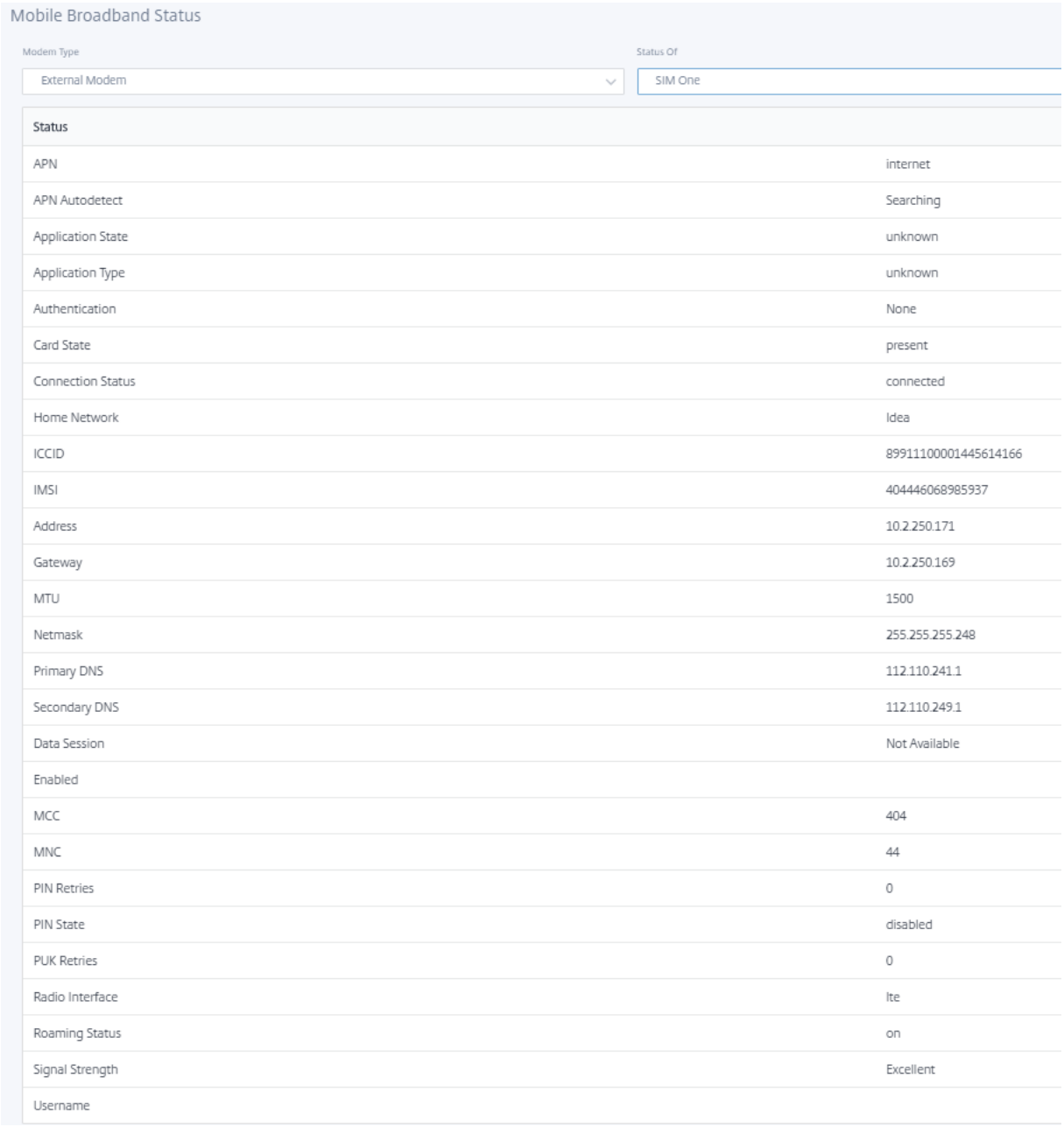
Détails du périphérique pour le modem externe Ethernet CDC.



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



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



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

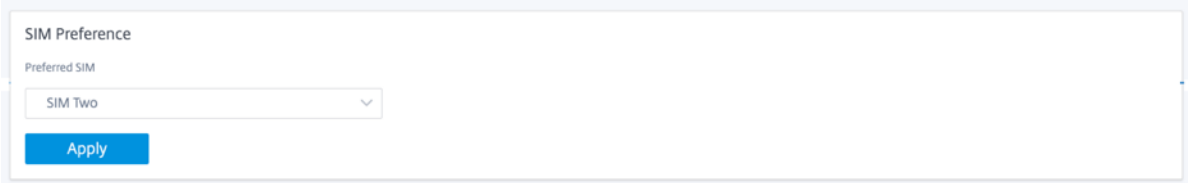
Opérations	Modem interne	Modem externe - CDC Ethernet	Modem externe - MBIM et NCM
Préférence SIM	Oui - Pour les appliances prenant en charge la double SIM	Non	Non

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.

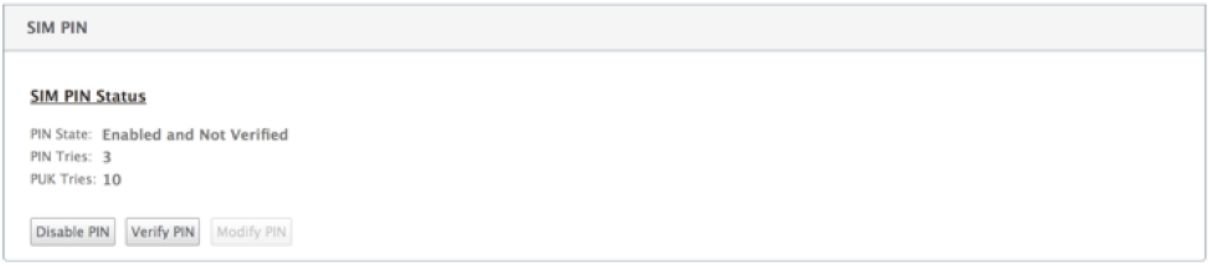
> **Remarque**
>
> L'option Préférence SIM n'est pas disponible pour l'appliance Wi-Fi Citrix SD-WAN 210-SE LTE car elle ne possède qu'un seul emplacement pour carte SIM.



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**.



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 débloquant la carte SIM. Contactez le fournisseur de services de l'opérateur pour

> obtenir une nouvelle carte SIM.

Paramètres APN

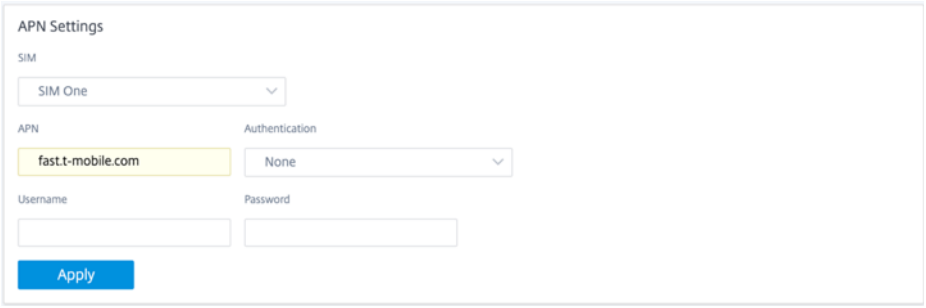
1. Pour configurer les paramètres APN, accédez à **Paramètres avancés > Haut débit mobile > Opérations** et accédez à la section **Paramètres APN**.

   > **Remarque**
   >
   > Obtenez les informations APN auprès du transporteur.

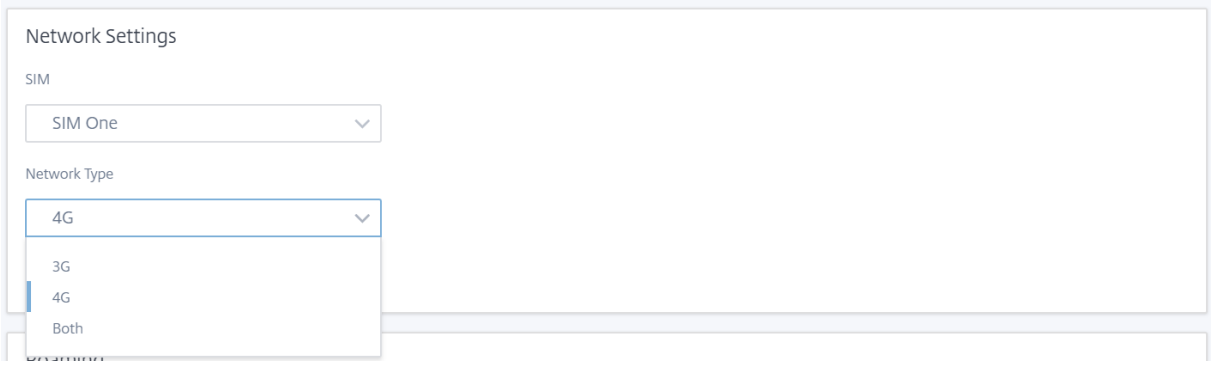
2. Sélectionnez la carte SIM, saisissez l'**APN, le nom d'utilisateur, le mot de passe** et **l'authentification** fournis par l'opérateur. Vous pouvez choisir parmi les protocoles d'authentification PAP, CHAP, PAPCHAP. Si le transporteur n'a fourni aucun type d'authentification, définissez-le sur **Aucun**.

   > **Remarque**
   >
   > Tous ces champs sont facultatifs.

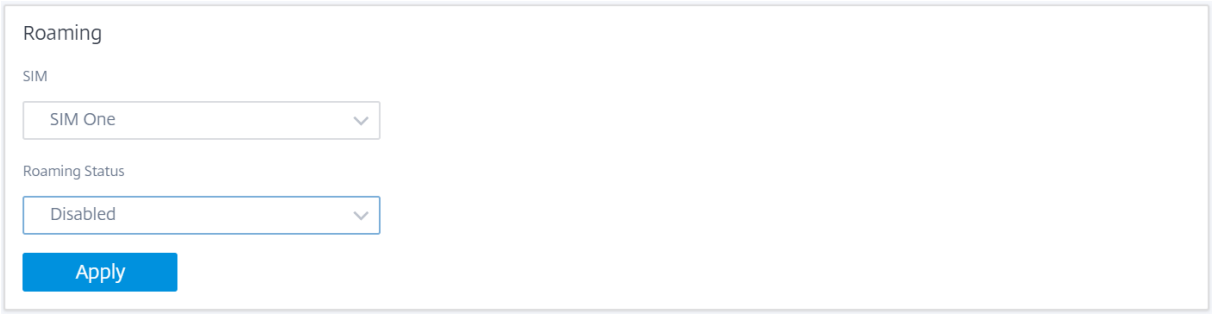
3. Cliquez sur **Appliquer**.



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.



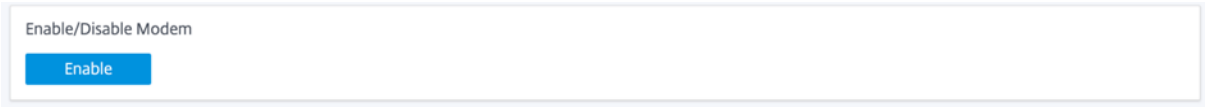
Itinérant L'option d'itinérance est activée par défaut sur vos appliances LTE, vous pouvez choisir de la désactiver.



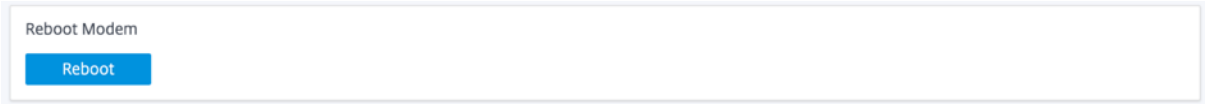
Gérer le firmware

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.

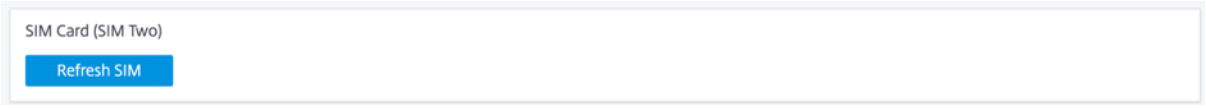


Redémarrer le modem Redémarre le modem. L'opération de redémarrage peut prendre jusqu'à 7 minutes.



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.



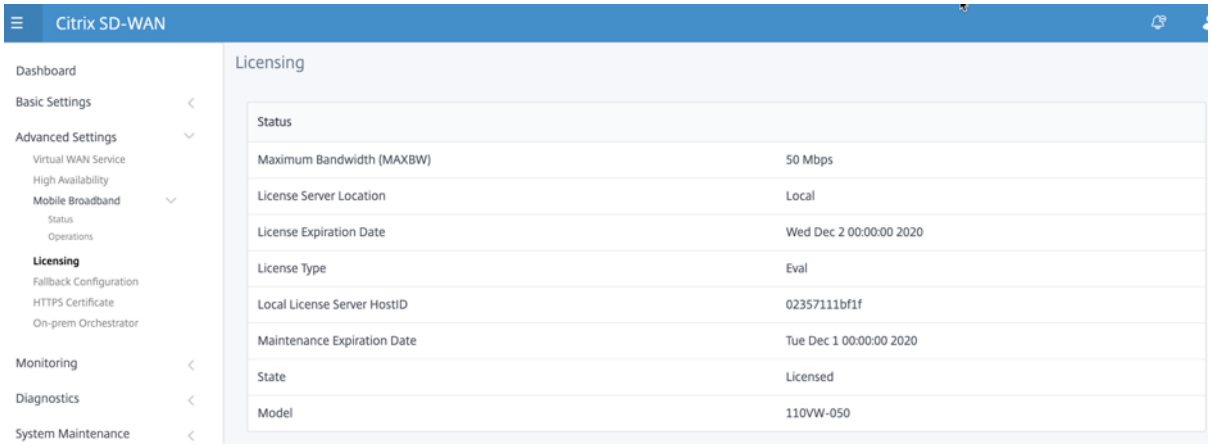
Vous pouvez afficher et gérer à distance tous les sites LTE de votre réseau à l'aide du Centre Citrix SD-WAN. Pour plus d'informations, reportez-vous à la section Gestion de sites LTE distants.

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

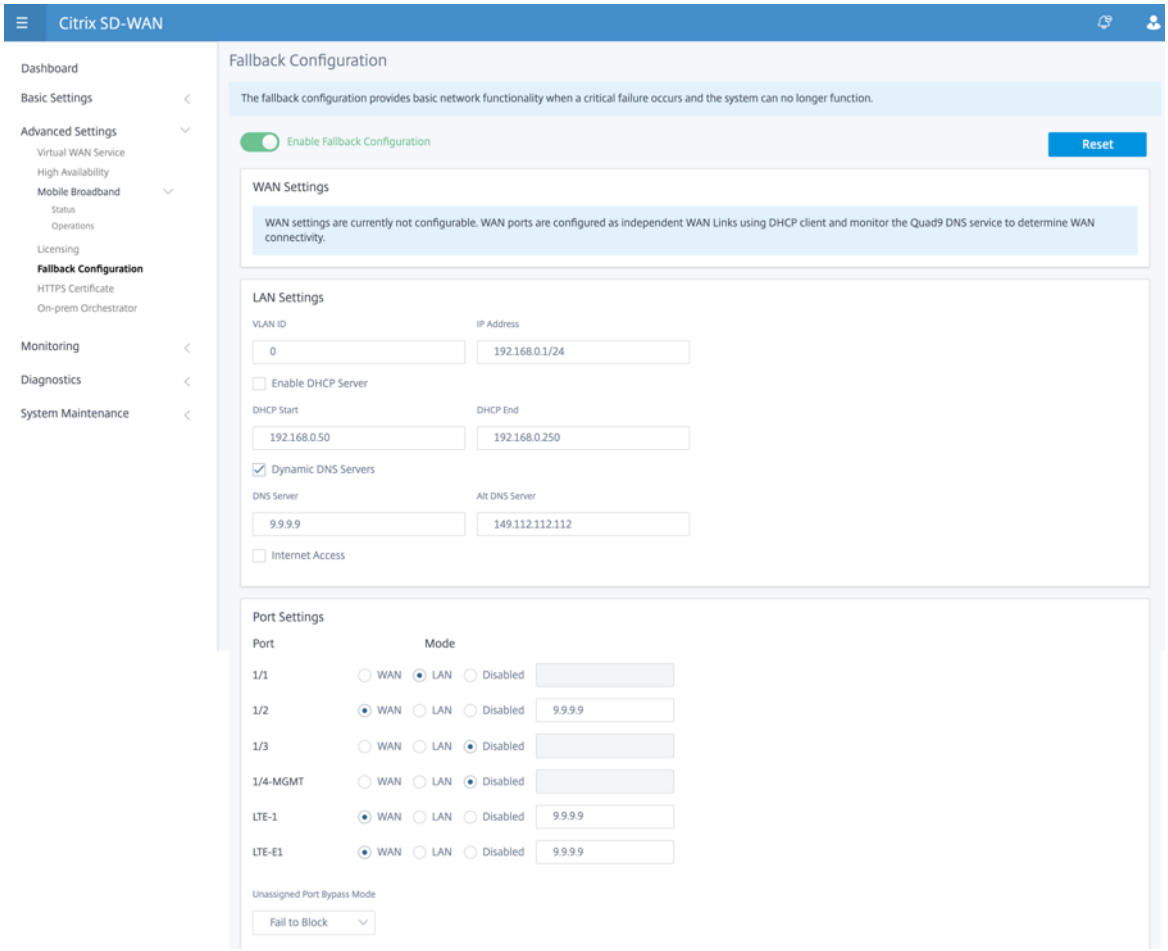
La page **Licence** affiche les détails de licence tels que l'emplacement du serveur, le modèle, le type de licence, etc.



> **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**.

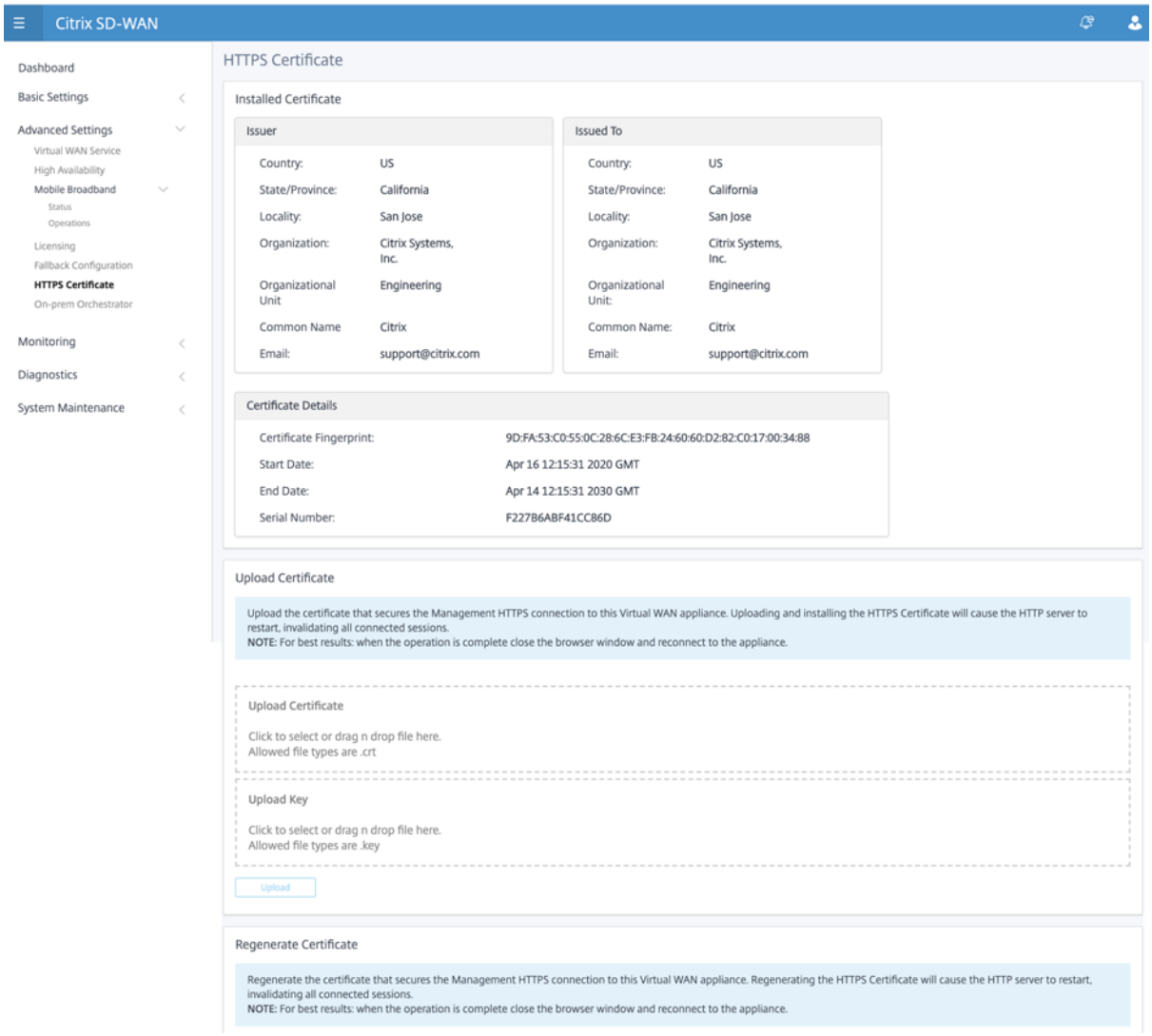


> **Remarque**
>
> Les interfaces LTE ne peuvent pas être configurées avec une adresse IP statique.

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.

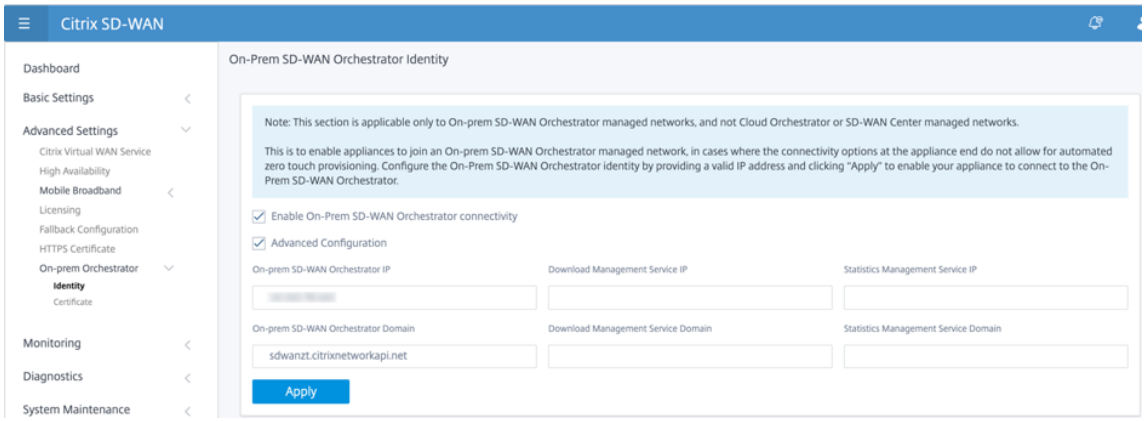
Vous pouvez établir une connexion entre votre appliance Citrix SD-WAN et Citrix On-Prem SD-WAN Orchestrator en activant la connectivité Orchestrator et en spécifiant l'identité SD-WAN Orchestrator sur site.

> **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 décharger 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 décharger 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 **Appliquer**.

   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 Authentificationunidirectionnelle ou Authentificationbidirectionnelle**.

   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**.

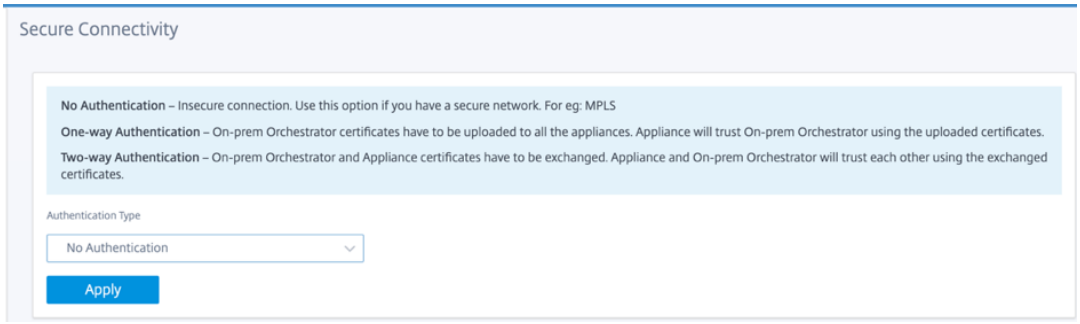
   Lors de la désactivation du **type d'authentification** dans On-Prem Orchestrator de l'état d'activation, les appliances existantes en mode Authentification unidirectionnelle passent à l'état déconnecté. Les clients doivent changer le type d'authentification de l'appliance en authentification bidirectionnelle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

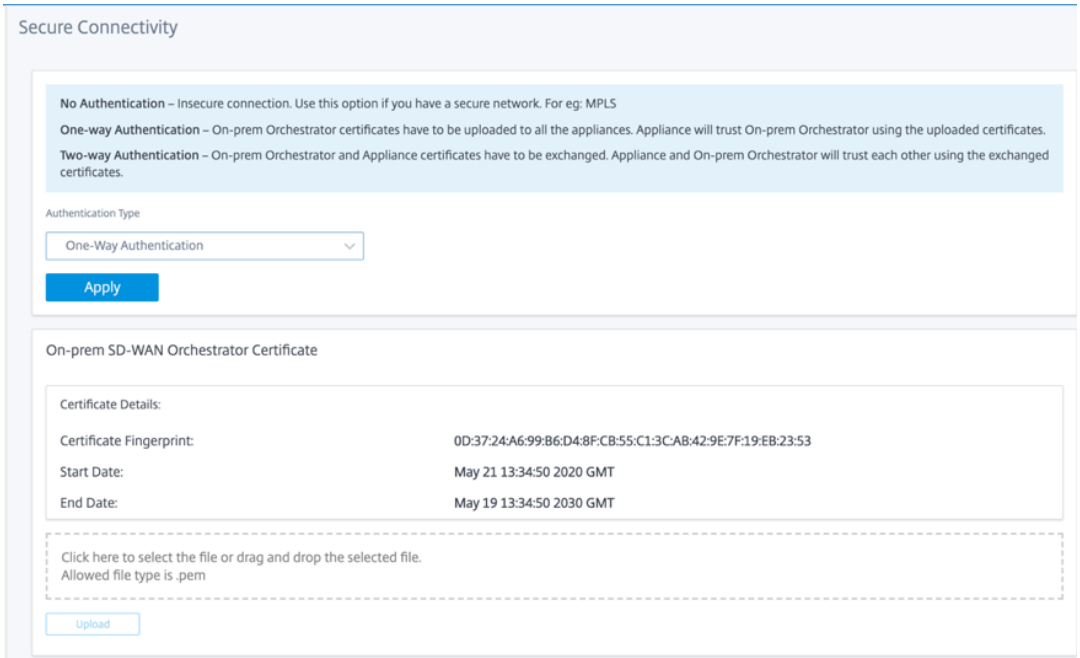
> • Le client doit s'assurer que les certificats sont régénérés et échangés entre On-Prem Orchestrator et l'appliance SD-WAN afin d'éviter la perte de connectivité de l'appliance avec On-Prem Orchestrator.

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

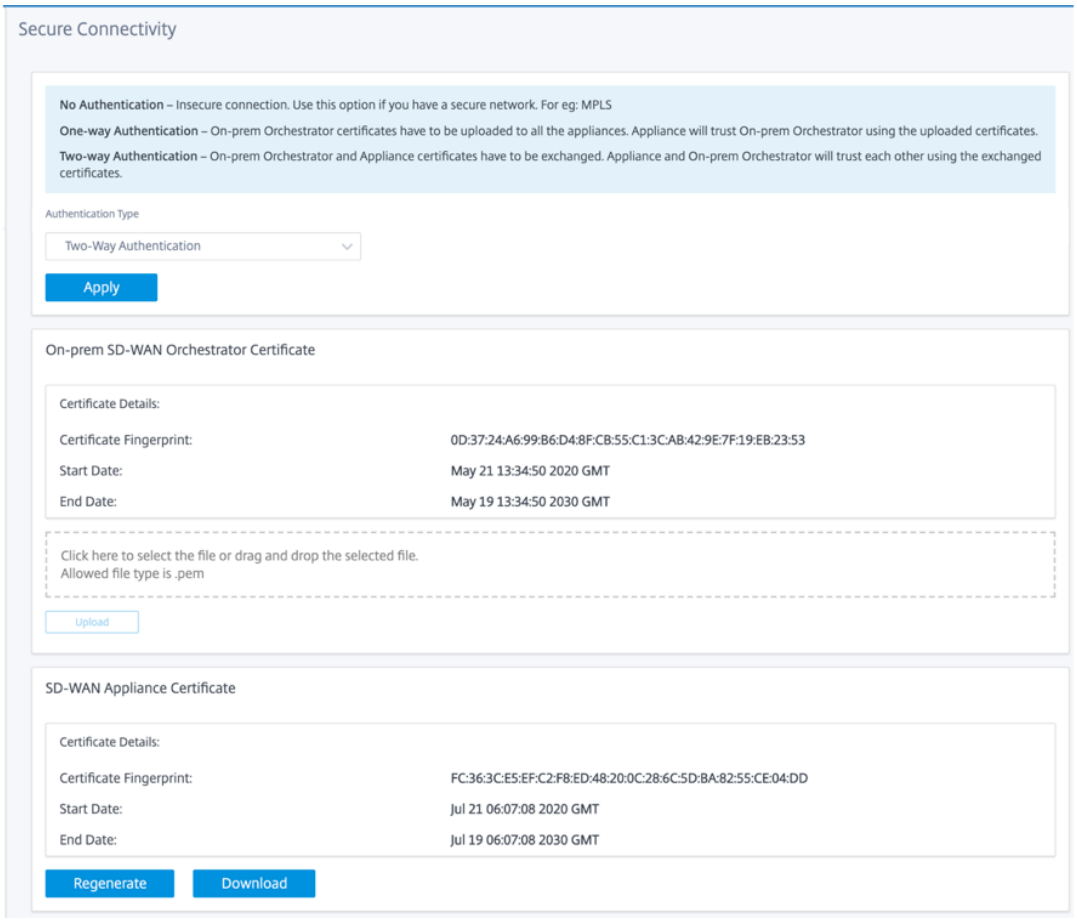
   - **Aucune authentification** : aucune authentification entre l'appliance SD-WAN Orchestrator sur site et le dispositif SD-WAN, et il n'est pas nécessaire d'utiliser l'appliance SD-WAN ou le certificat SD-WAN Orchestrator sur site. Mais vous pouvez utiliser cette option si vous disposez d'un réseau sécurisé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



   - **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'appliance SD-WAN approuve l'Orchestrator On-Prem à l'aide des certificats téléchargés.



- **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.



> **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 Liens**WAN 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

Impact de la mise à niveau vers Citrix SD-WAN 11.5

August 31, 2022

- Citrix SD-WAN 11.5.0 est une version à disponibilité limitée, recommandée et prise en charge uniquement pour des clients/déploiements de production spécifiques.
- La version SD-WAN 11.5.0 ne prend pas en charge les déploiements Advanced Edition (AE), Premium Edition (PE) et WAN Optimization.
- Le SD-WAN 11.5.0 prend uniquement en charge les plates-formes mentionnées dans les modèles de plate-forme SD-WAN et les packages logiciels.
- SD-WAN 11.5.0 ne prend pas en charge Citrix SD-WAN Center ou Citrix SD-WAN Orchestrator pour les environnements locaux.
- Le microprogramme SD-WAN 11.5.0 n'est pas disponible sur la page Téléchargements de Citrix.
- La version SD-WAN 11.5.0 est disponible uniquement via le service Citrix SD-WAN Orchestrator et uniquement sur certains points de présence géographiques.
- Assurez-vous d'obtenir les approbations et les conseils requis de la part de Citrix Product Management/Citrix Support avant de déployer la version 11.5.0 sur un réseau de production.

Configuration système requise

August 31, 2022

Configuration matérielle requise

Les instructions d'installation des appliances SD-WAN sont fournies dans 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

À partir de la version 11.5 SD-WAN, les licences de l'appliance SD-WAN sont gérées via le service Citrix SD-WAN Orchestrator. Pour plus d'informations sur les exigences de licence, consultez la section Licences.

Exigences du navigateur

Les cookies doivent être activés dans les navigateurs et JavaScript doivent être installés et activés.

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

- Mozilla Firefox 49+
- Google Chrome 51+
- Microsoft Edge 13+

Les cookies doivent être activés dans les navigateurs pris en charge, et JavaScript est 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

Plateforme Cloud

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

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

Modèles de plate-forme SD-WAN

September 26, 2023

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
1100-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)

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.

Chemins d'accès

August 31, 2022

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.

Configuration

September 26, 2023

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.

Configuration initiale

Ces procédures doivent être suivies 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 au bon moment. 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 Virtual WAN, 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 de l'appliance.
4. Définissez le seuil de **délai d'expiration 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 de l'exécution d'autres tâches complexes.

5. Téléchargez et installez le fichier de licence du logiciel sur l'appliance.

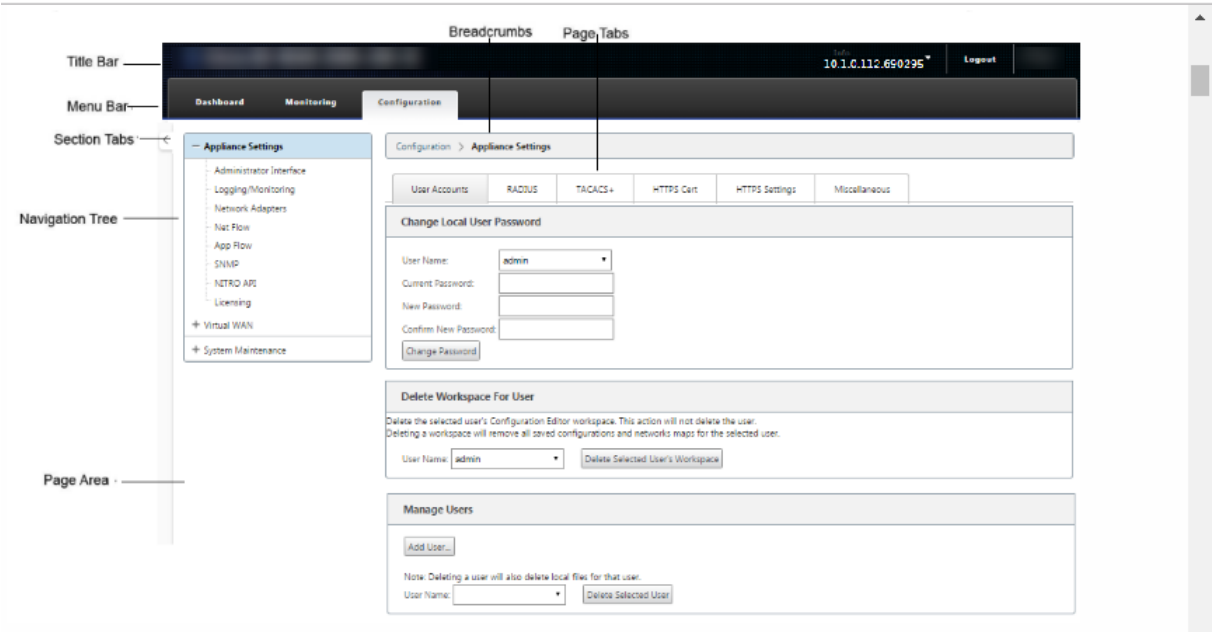
Pour obtenir des instructions sur l'installation d'un dispositif virtuel SD-WAN (SD-WAN VPX), consultez les sections suivantes :

- 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

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.

Navigation de base La figure ci-dessous présente 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** permettant de mettre fin à la session.
- **Barre de menu principale** : il s'agit de la barre affichée sous la barre de titre de 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 formulaires de l'Interface de gestion Web. Chaque section possède sa propre arborescence de navigation pour naviguer dans la hiérarchie des pages de cette section. Cliquez sur l'onglet d'une **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. Cela affiche l'arborescence de navigation d'une section. Cliquez sur l'onglet d'une 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 branche dans l'arborescence pour afficher les pages disponibles pour cette rubrique de branche.
  - 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 branche pour fermer la branche.

- **Breadcrumbs** : affiche le chemin de navigation vers la page actuelle. Les chapelures se trouvent en haut de la zone de la 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 noir.
- **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 davantage de pages enfants pour cette rubrique ou ce formulaire de configuration. Ils sont situés en haut de la zone de la page, juste en dessous de l'affichage de la chapelure. Parfois (comme pour l'assistant **Gestion des modifications**), des 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 augmenter ou réduire la largeur de la zone de page (ou des sections de celle-ci) pour afficher davantage de champs dans un tableau ou un formulaire. Dans ce cas, il y a une barre de redimensionnement verticale grise sur la bordure droite d'un volet de zone de page, d'un formulaire ou d'un tableau. Faites rouler le curseur sur la barre de redimensionnement jusqu'à ce que le curseur devienne une flèche bidirectionnelle. Cliquez ensuite et faites glisser la barre vers la droite ou la gauche pour agrandir ou réduire la largeur de la zone.

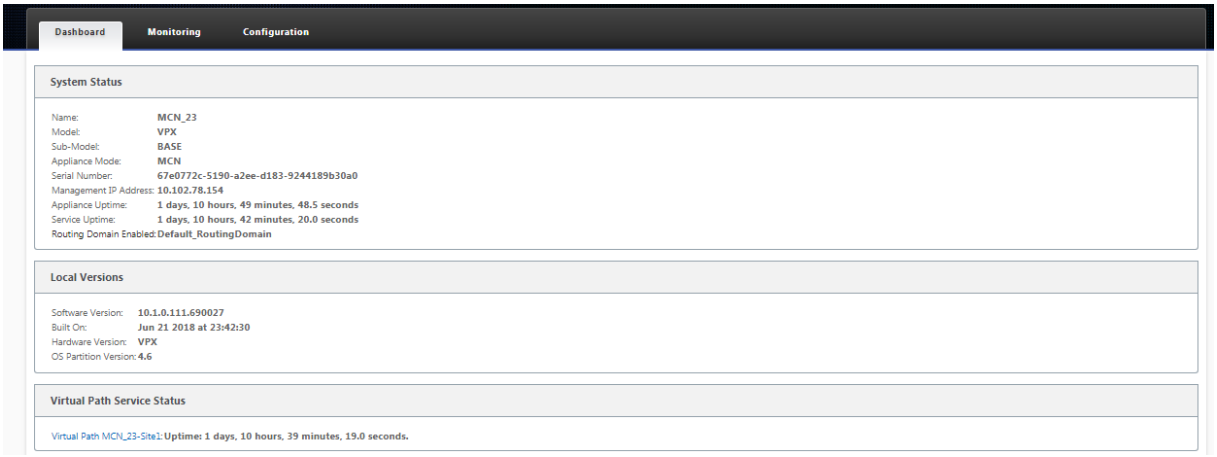
  Si la barre de redimensionnement n'est pas disponible pour une page, vous pouvez cliquer et faire glisser le bord droit de votre navigateur pour afficher la page complète.

Tableau de bord de l'interface Web Cliquez sur l'onglet de la section Tableau de **bord** pour afficher les informations de base relatives à l'appliance locale.

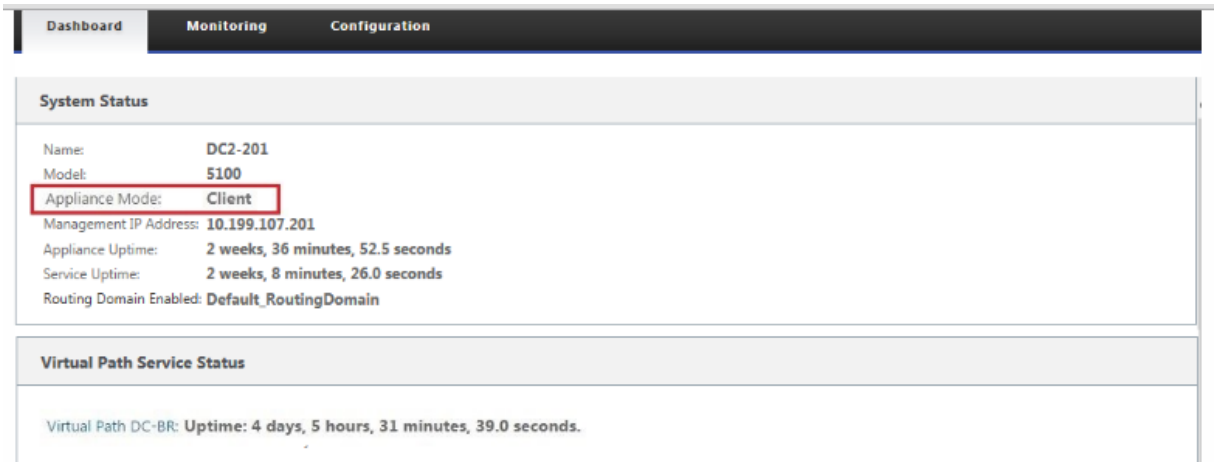
La page **Tableau de bord** affiche les informations de base suivantes concernant l'appliance :

- État du système
- État du service Chemin d'accès virtuel
- Informations sur la version du progiciel local

La figure suivante présente 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 du dispositif client.



Configuration du matériel de l'appliance

Pour configurer le matériel matériel de l'appliance Citrix SD-WAN (appliance 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 sur l'appliance et sur 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 sur l'appliance et sur 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'appliance à un ordinateur personnel.

   Vous devez connecter l'appliance à un PC avant de terminer la procédure suivante, en définissant l'adresse IP de gestion de l'appliance.

   > **Remarque**
   >
   > Avant de connecter l'appliance, assurez-vous que le port Ethernet est activé sur le PC. Utilisez un câble Ethernet pour connecter le port de gestion du matériel SD-WAN au port Ethernet par défaut d'un ordinateur personnel.

Port de gestion SD-WAN VPX-SE L'appliance 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'appliance 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

Pour activer l'accès à distance à une appliance SD-WAN, vous devez spécifier une adresse IP de gestion unique pour l'appliance. Pour ce faire, vous devez d'abord connecter l'appliance à un PC. Vous pouvez ensuite ouvrir un navigateur sur le PC et vous connecter directement à l'interface Web de gestion de l'appliance, 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

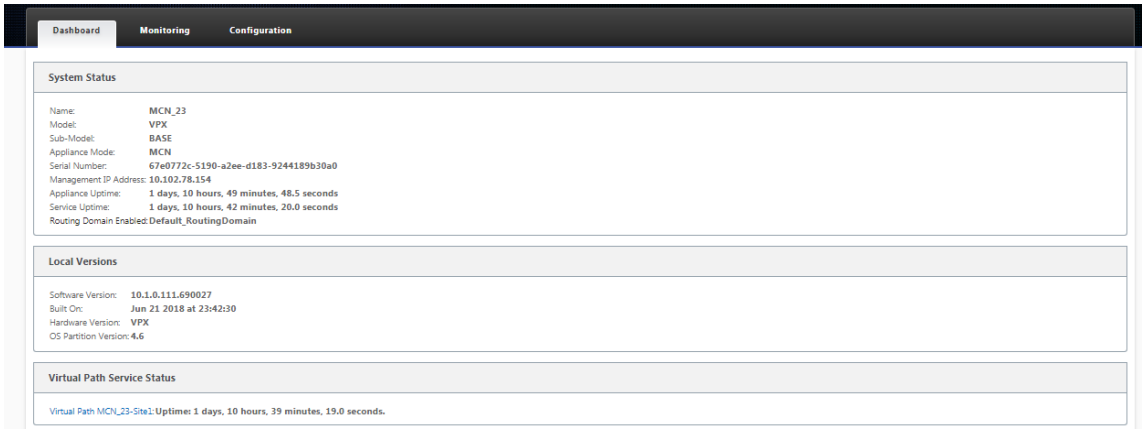
4. Modifiez le paramètre **Masque de sous-réseau** sur votre PC comme suit :
   - 255.255.0.0
5. Sur le PC, ouvrez un navigateur et entrez l'adresse IP par défaut de l'appliance. Entrez l'adresse IP suivante dans la ligne d'adresse du navigateur :
   - 192.168.100.1

   > **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.



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,

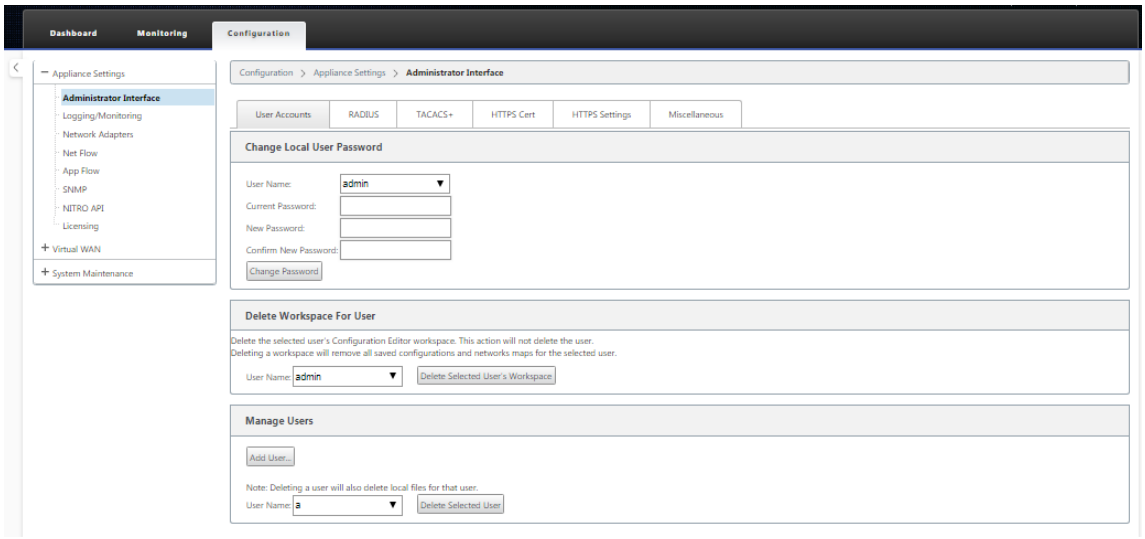
vous pouvez ignorer cette alerte. L'alerte sera résolue après avoir installé la licence et terminé le processus de configuration et de déploiement de l'appliance.

7. Dans la barre de menus principale, sélectionnez l'onglet **Configuration** .

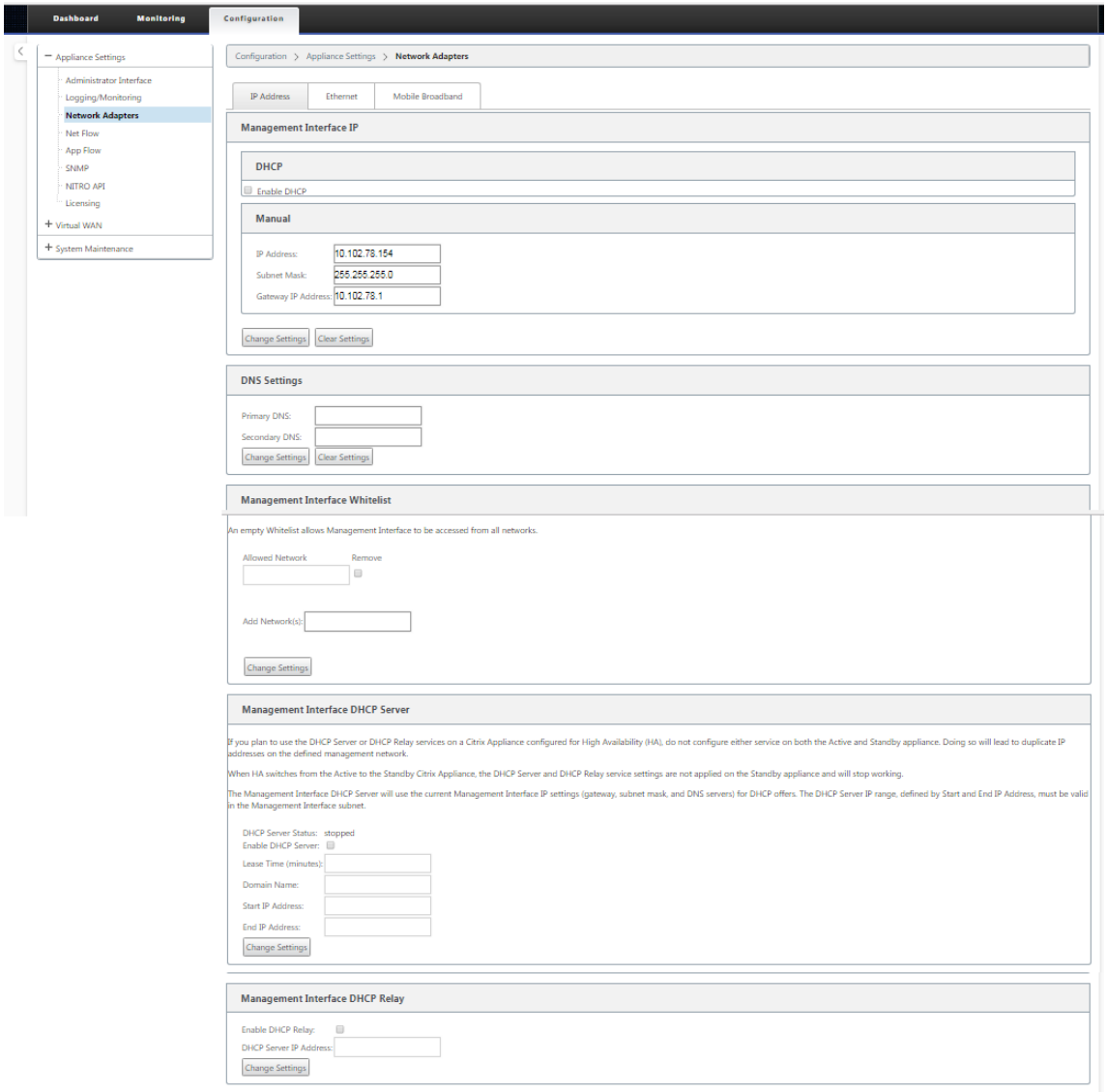
   L'arborescence de navigation **Configuration** s'affiche dans le volet gauche de l'écran. L'arborescence de navigation **Configuration** contient les trois branches principales suivantes :

   - 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.



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.



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 :

     - IP Address
     - 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 :

- IP Address
- 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 IPv6et Activer IPv4** pour activer les protocoles IPv4 et IPv6. Dans de tels scénarios, l'appliance 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]`

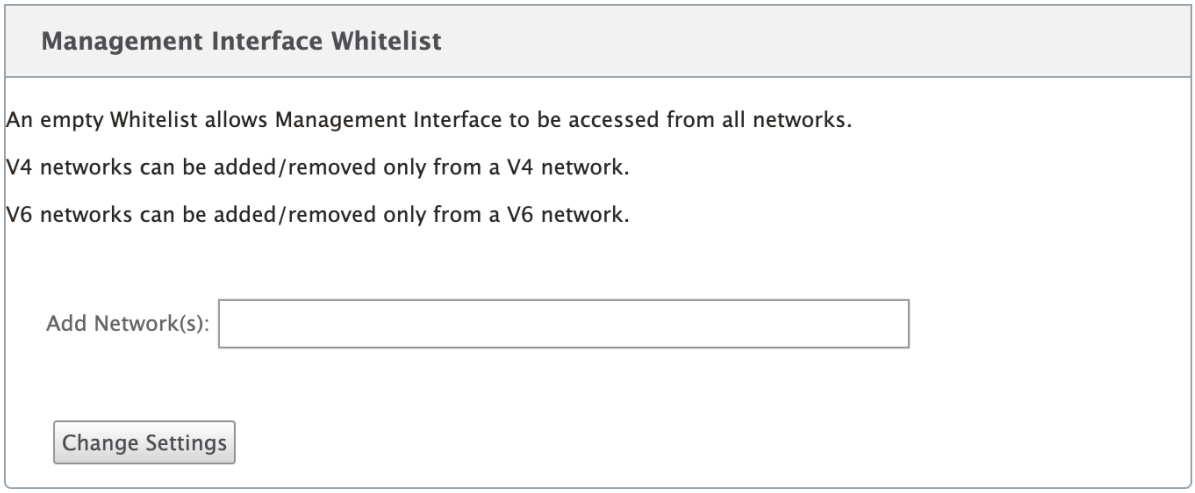
    Si la connexion réussit, l'écran de **connexion** de l'interface Web de gestion SD-WAN de l'appliance que vous avez configurée s'affiche.

    > **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.



Définir la date et l'heure

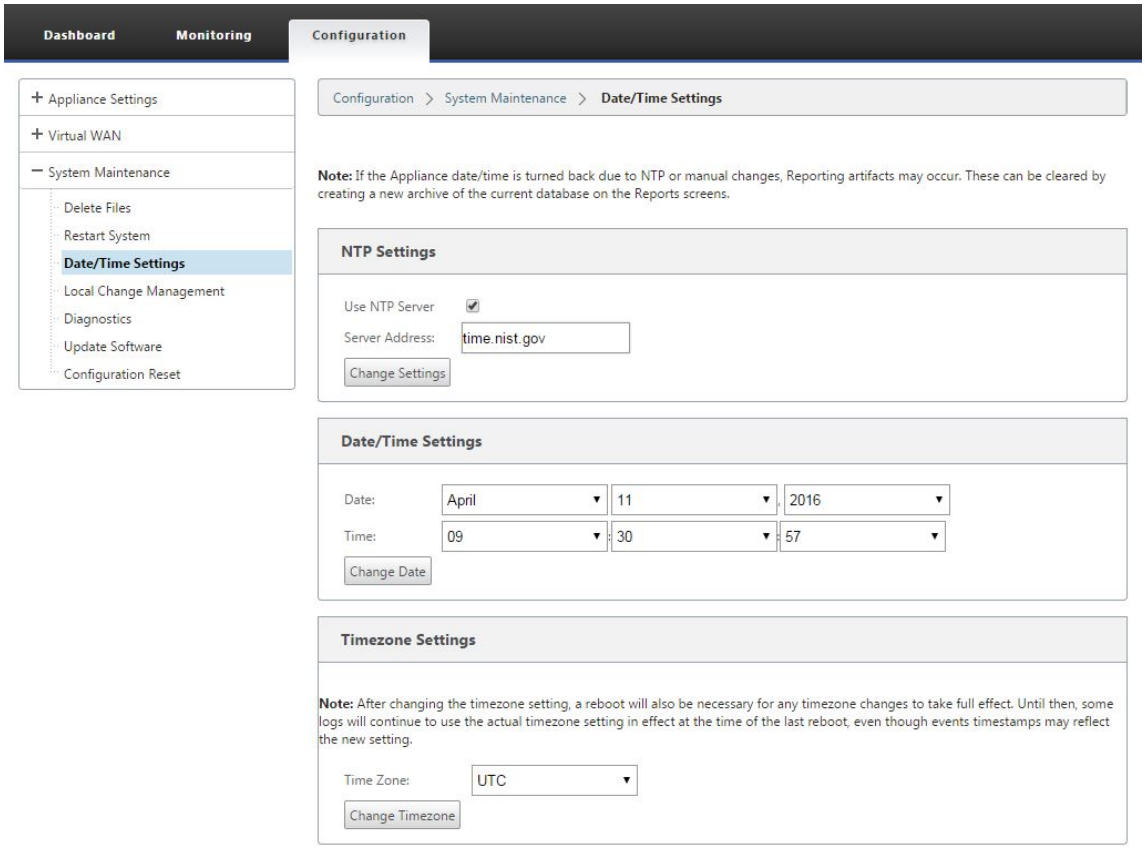
Avant d'installer la licence du logiciel SD-WAN sur une appliance, vous devez définir la date et l'heure sur celle-ci.

> **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. Dans la **branche Maintenance du système, sélectionnez Paramètres de date/heure**. La page **Paramètres de date/heure** s'affiche comme suit.



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 saisis.

6. Cliquez sur **Modifier le fuseau horaire**. Ceci met à jour le fuseau horaire et recalcule la date et l'heure actuelles, en conséquence. 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 d'alerte de succès (coche verte) et un message d'état s'affichent dans la section 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 à la fin de la mise à jour.
8. Sélectionnez le mois, le jour et l'année dans les menus déroulants du champ **Date** .

9. Sélectionnez les heures, les minutes et les secondes dans les menus déroulants du champ **Heure** .
10. Cliquez sur **Modifier la date**.

> **Remarque :**
>
> Ceci met à jour les paramètres 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 d'**expiration de la session de 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 d'expiration, vous pouvez passer directement à la section Chargement 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.

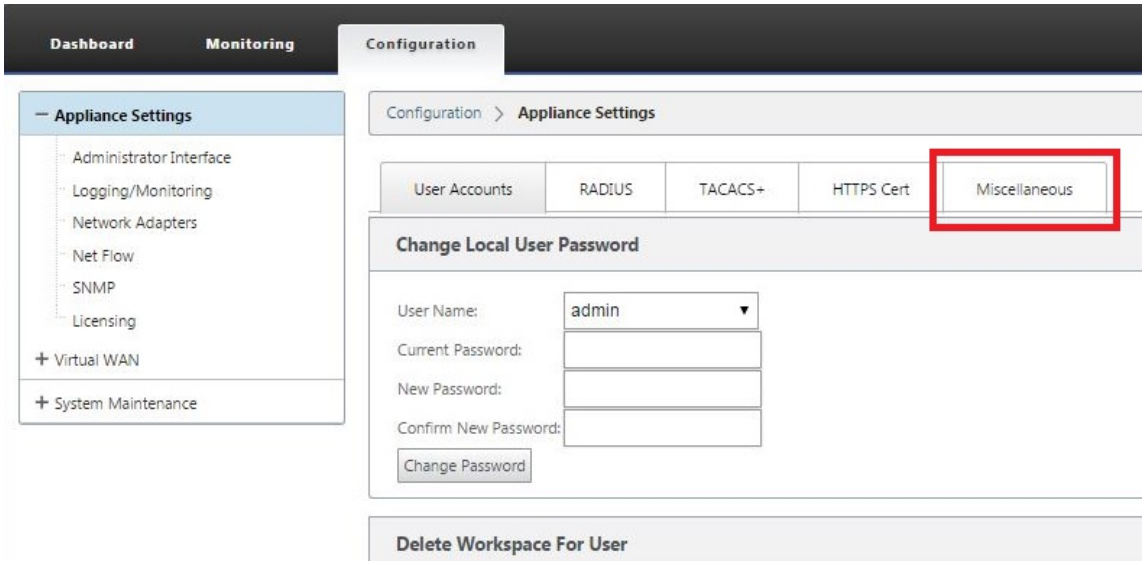
Expiration de session

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 console, procédez comme suit :

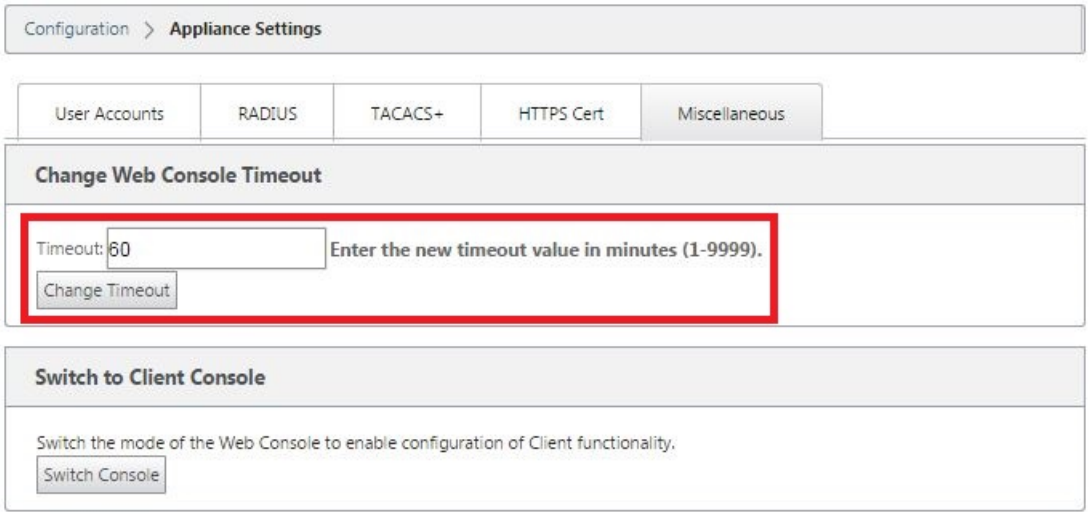
1. Sélectionnez l'onglet **Configuration**, puis la branche **Paramètres du matériel** dans l'arborescence de navigation.

   La page **Paramètres du matériel** s'affiche, avec l'onglet **Comptes d'utilisateurs** présélectionné par défaut.



2. Sélectionnez l'onglet **Divers** (coin le plus à droite).

   L'onglet **Divers** s'affiche.



3. Entrez la valeur du **délai d'expiration de** la console.

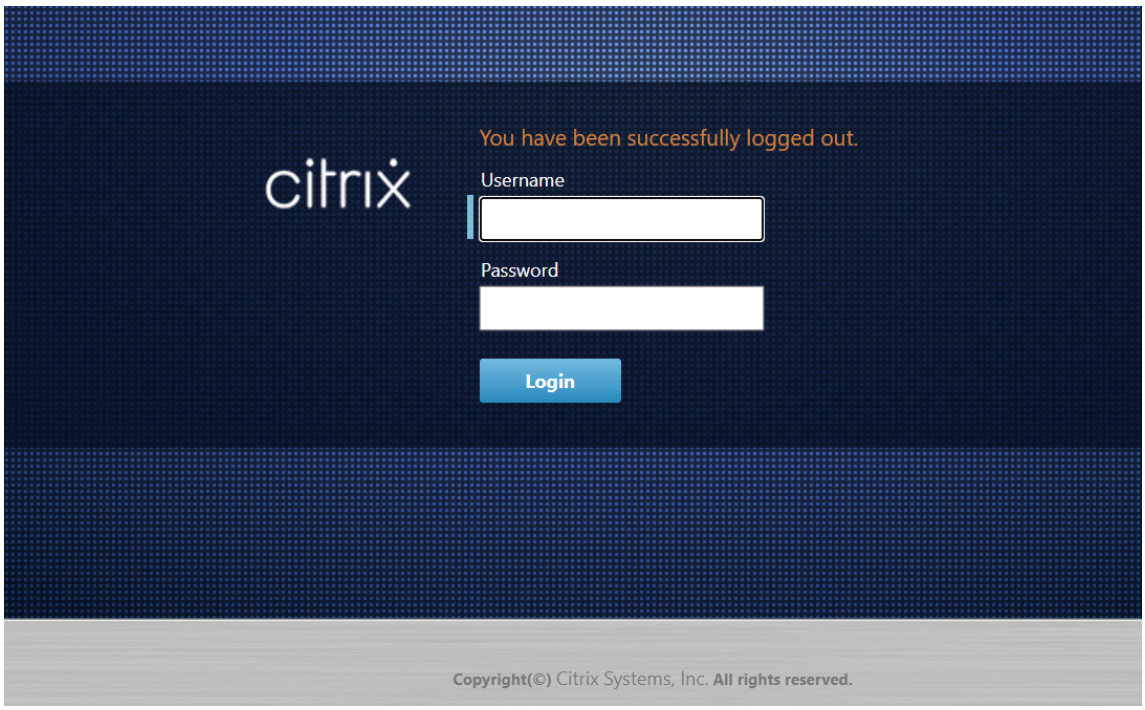
   Dans le champ **Délai** d'expiration de la section **Modifier le délai d'expiration de la console Web**, entrez une valeur supérieure (en minutes) jusqu'à la valeur maximale de 9999. La valeur par défaut est 60, ce qui est beaucoup trop court pour une session de configuration initiale.

   > **Remarque**
   >
   > Pour des raisons de sécurité, assurez-vous de réinitialiser cette valeur à un intervalle inférieur après la fin de la configuration et du déploiement.

4. 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.

Après un bref intervalle (quelques secondes), la session est interrompue et vous êtes automatiquement déconnecté de l'Interface Web de gestion. La page Connexion s'affiche.



5. Entrez le nom d'utilisateur administrateur (*administrateur*) 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

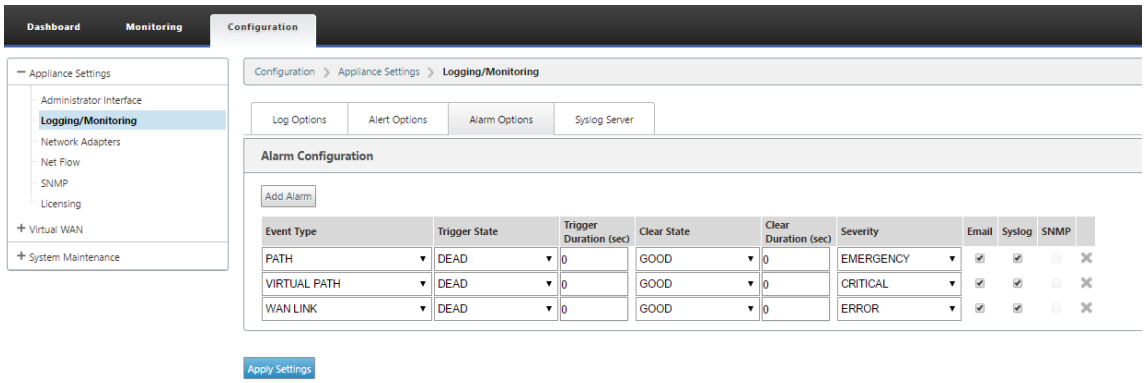
Vous pouvez désormais configurer votre appliance SD-WAN pour identifier les conditions d'alarme en fonction de votre réseau et de vos priorités, générer des alertes et recevoir des notifications par e-mail,

syslog ou SNMP trap.

Une alarme est une alerte configurée composée d'un type d'événement, d'un état de déclenchement, d'un état clair et d'une gravité.

Pour configurer les paramètres d'alarme :

1. Dans l'interface de gestion Web SD-WAN, accédez à **Configuration** > **Paramètres de l'appliance** > **Journalisation/surveillance**, puis cliquez sur **Options d'alarme**.
2. Cliquez sur **Ajouter une alarme pour** ajouter une nouvelle alarme.



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** : Durée en secondes, qui détermine la rapidité avec 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 de durée de déclenchement. Plus d'alarmes sont déclenchées uniquement si un événement persiste plus longtemps que la durée de déclenchement.
   - **État d'effacer** : état d'événement qui efface une alarme pour un type d'événement après le déclenchement de l'alarme. Les options Effacer l'état dépendent de l'état de déclenchement choisi.
   - **Durée d'effacement :** durée en secondes, qui détermine le temps d'attente avant de désactiver 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 clair se produit sur le même objet dans le délai spécifié.

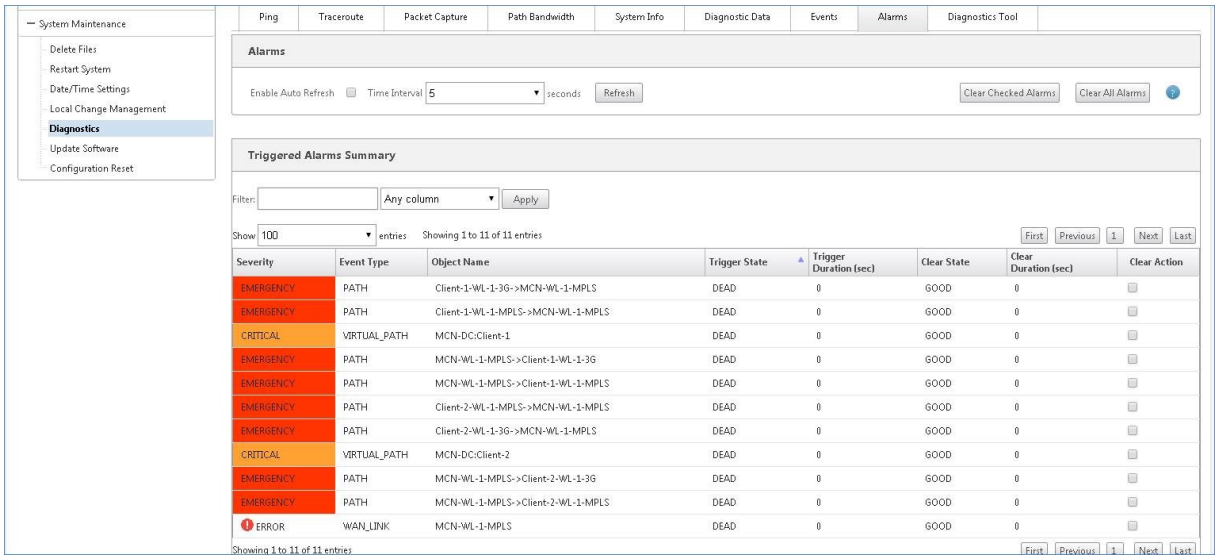
- **Gravité** : champ défini par l'utilisateur qui détermine l'urgence d'une alarme. La gravité est affichée dans les alertes envoyées lorsque l'alarme est déclenchée ou effacée et dans le résumé de l'alarme déclenchée.
- **E-mail** : Les alertes de déclenchement d'alarme et d'effacer les alertes pour le type d'événement sont envoyées par e-mail.
- **Syslog** : les alertes de déclenchement d'alarme et d'effacer 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 une interruption SNMP.

4. Continuez à ajouter des alarmes au besoin.
5. Cliquez sur **Appliquer les paramètres**.

Affichage des alarmes déclenchées **Pour afficher un récapitulatif 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.



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 que vous souhaitez effacer.

3. Cliquez sur **Effacer les alarmes vérifiées**. Vous pouvez également cliquer sur **Effacer toutes les alarmes** pour effacer toutes les alarmes.

Configuration du nœud de contrôle principal

Le **nœud de contrôle principal SD-WAN (MCN)** est l'appliance principale du réseau étendu virtuel. Il s'agit généralement d'une appliance Virtual WAN déployée dans le centre de données. Le MCN sert de point de distribution pour la configuration initiale du système et pour 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.

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.

À partir de la version 11.5 de Citrix SD-WAN, vous pouvez configurer un MCN via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Déploiement et configuration du site.

Connexion des appliances client à votre réseau

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 CBVWSSH. Cette synchronisation entre le compte CBVWSSH et le compte d'administrateur par défaut a lieu chaque fois que vous modifier/mettre 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 CBVWSSH. 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.

Déployer Citrix SD-WAN Standard Edition dans OpenStack à l'aide de CloudInit

Vous pouvez désormais déployer Citrix SD-WAN Standard Edition (SE) dans un environnement OpenStack. 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.

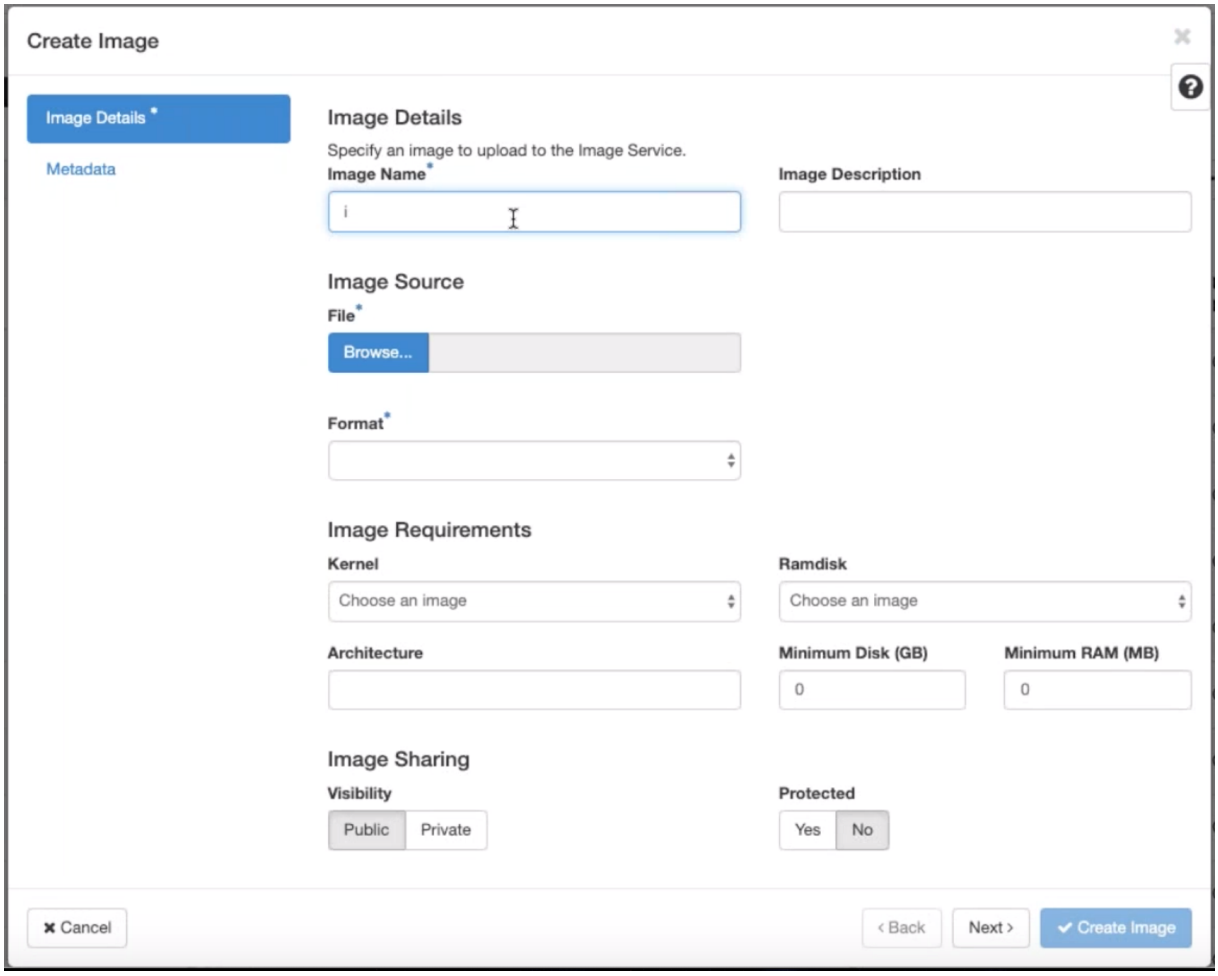
Pour une instance SD-WAN dans OpenStack, les entrées nécessaires pour Management IP, DNS et numéro de série des utilisateurs. Le script Cloudinit analyse ces entrées et provisionne l'instance avec les informations données.

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**.

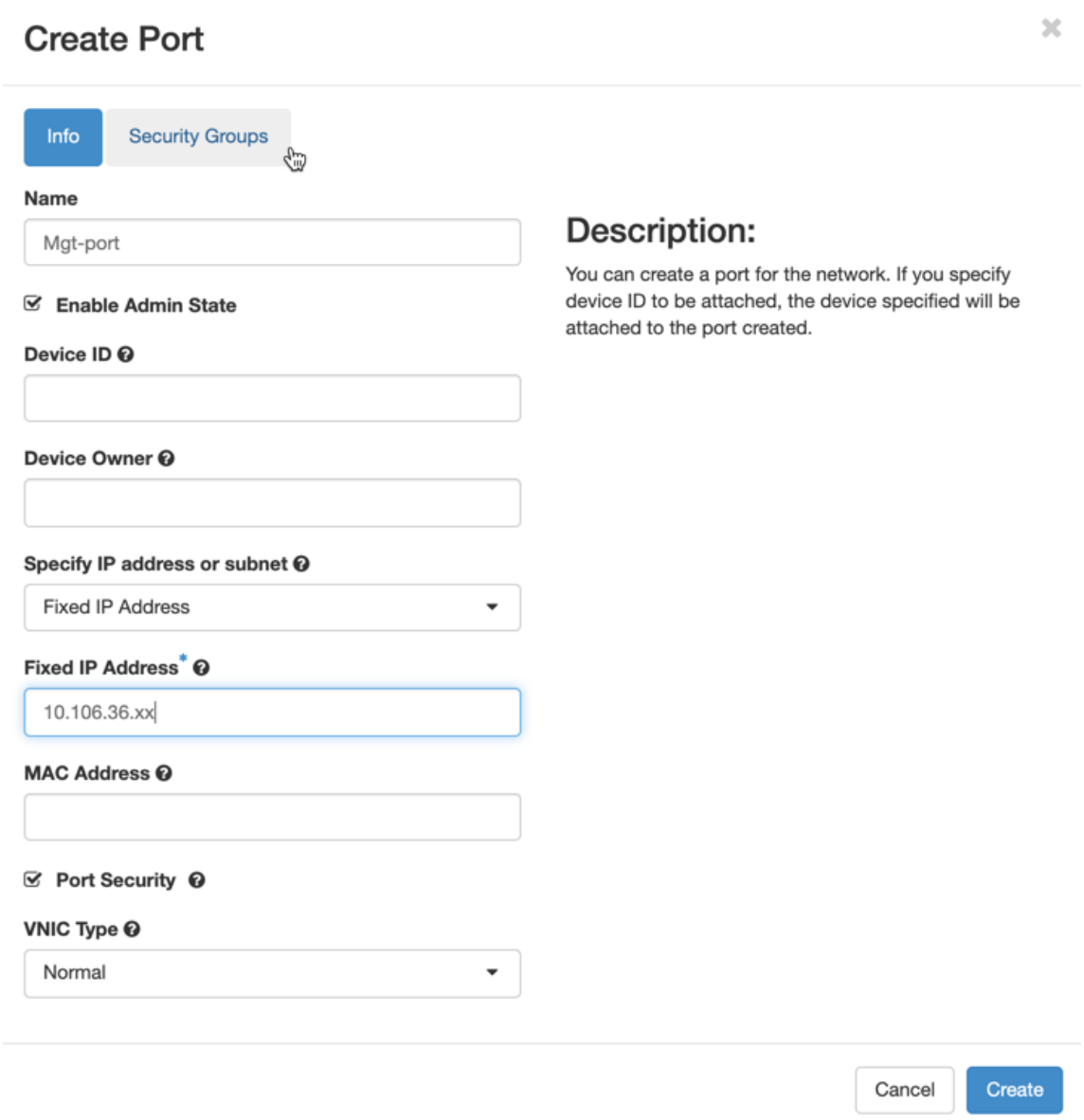


- **Nom de l'image** - Indiquez le nom de l'image.
- **Description de l'image** —Ajoute une description de l'image.
- **Fichier** - Recherchez le fichier image kvm.qcow2 à partir de votre lecteur local et sélectionnez-le.
- **Format** : sélectionnez le format de disque QCOW2 —QEMU Emulator dans la liste 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.

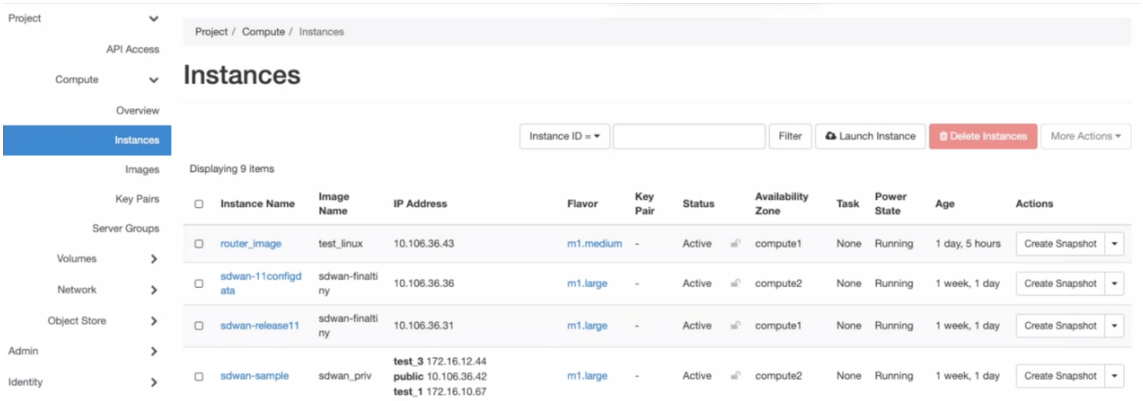


Si vous sélectionnez **Adresse IP fixe**, vous devez fournir l'adresse IP du sous-réseau pour le nouveau port.

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.

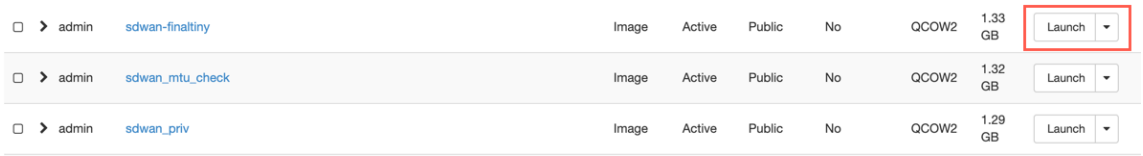
3. Connectez-vous à OpenStack et configurez les instances.



4. Téléchargez le fichier **kvm.qcow2.gz** et décompressez le.

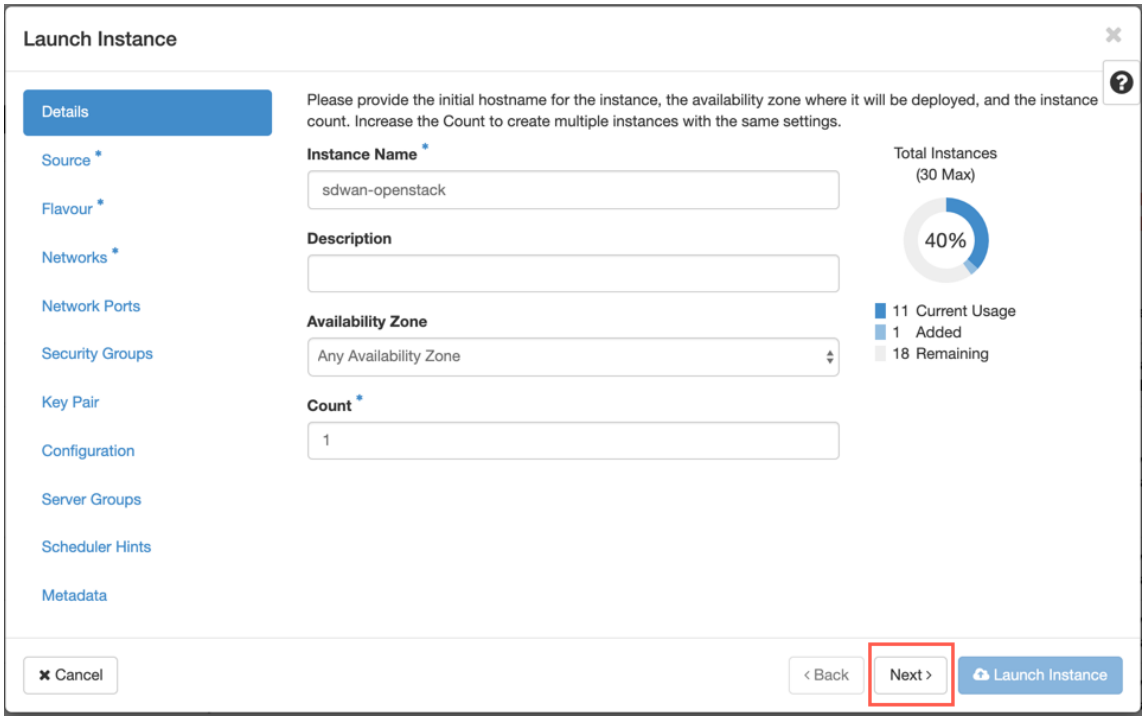
5. Accédez à **Instances** et cliquez sur **Lancer l'instance**.

> **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.

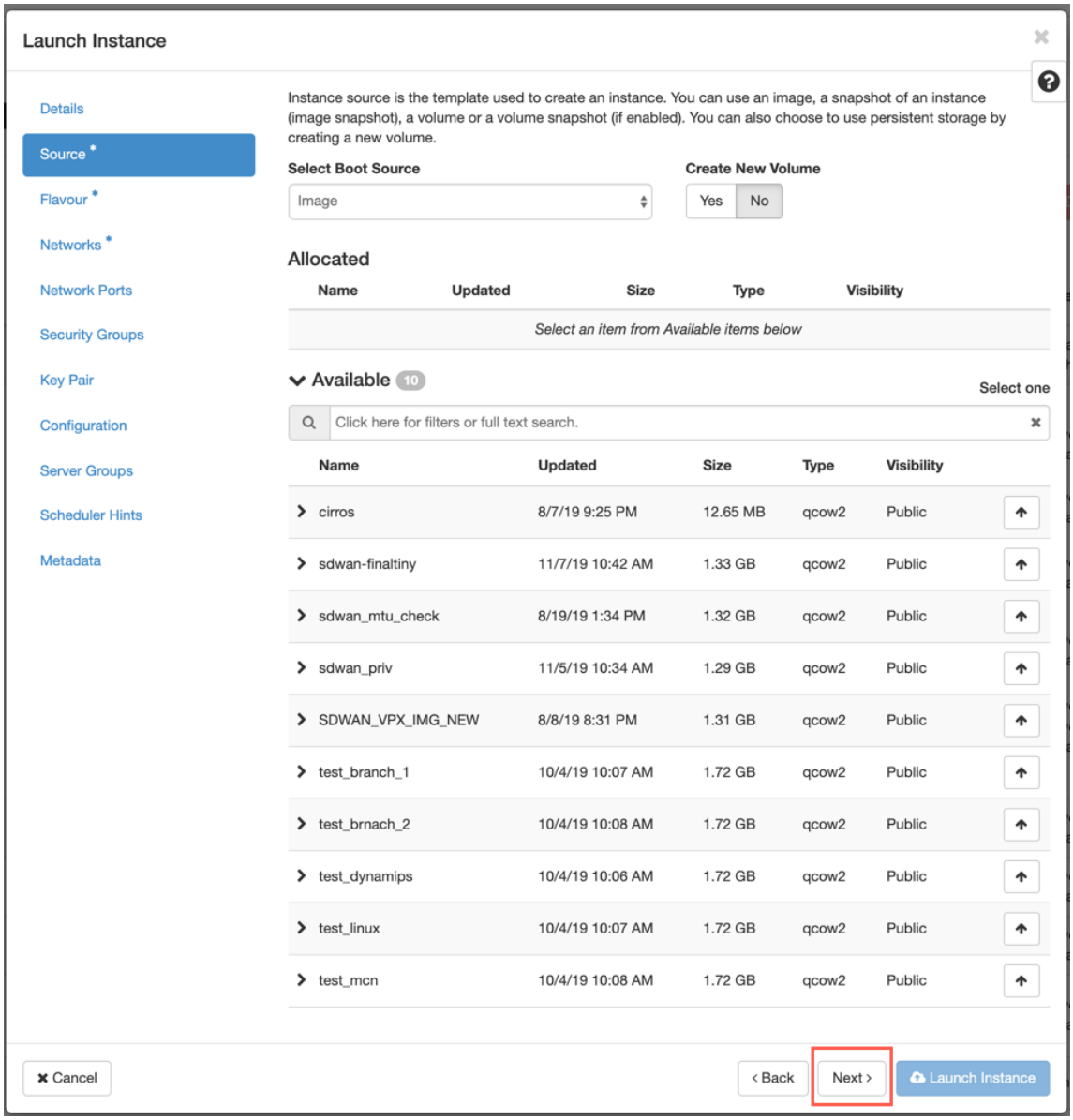


6. Sous l'onglet **Détails**, fournissez les informations suivantes :

   - **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**.



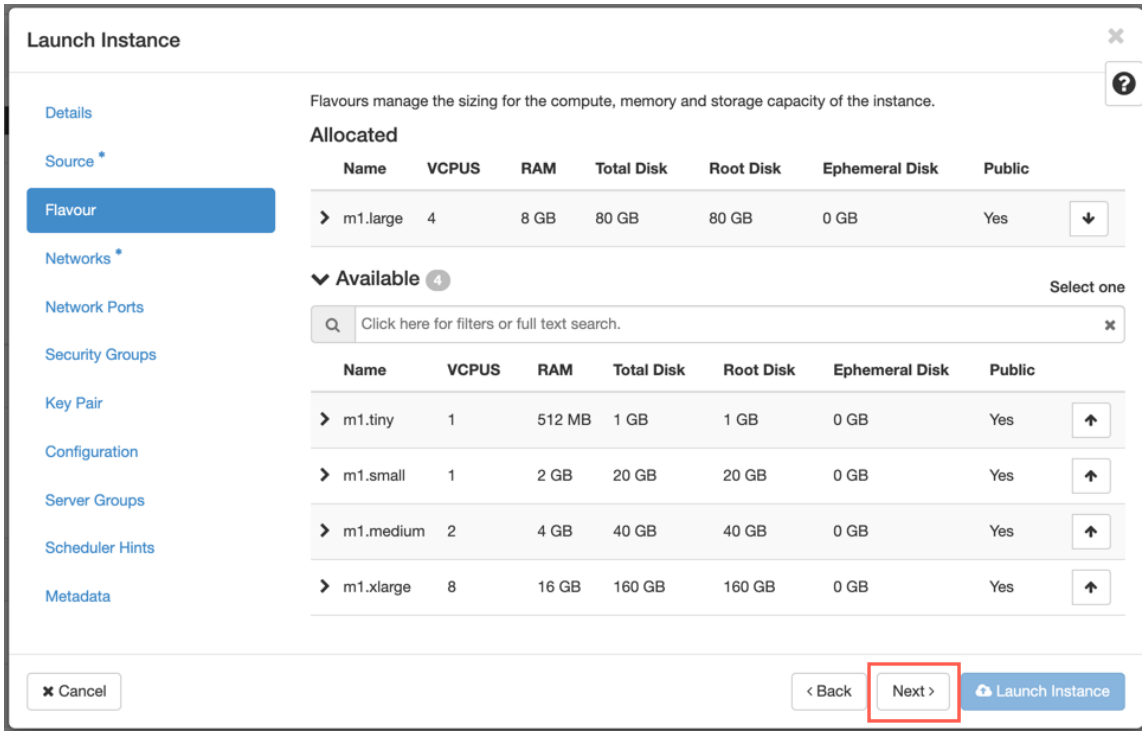
7. Dans l'onglet **Source**, sélectionnez **Non** sous **Créer un nouveau volume**, puis cliquez sur**Suivant**. La source d'instance est le modèle utilisé pour créer une instance.



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.

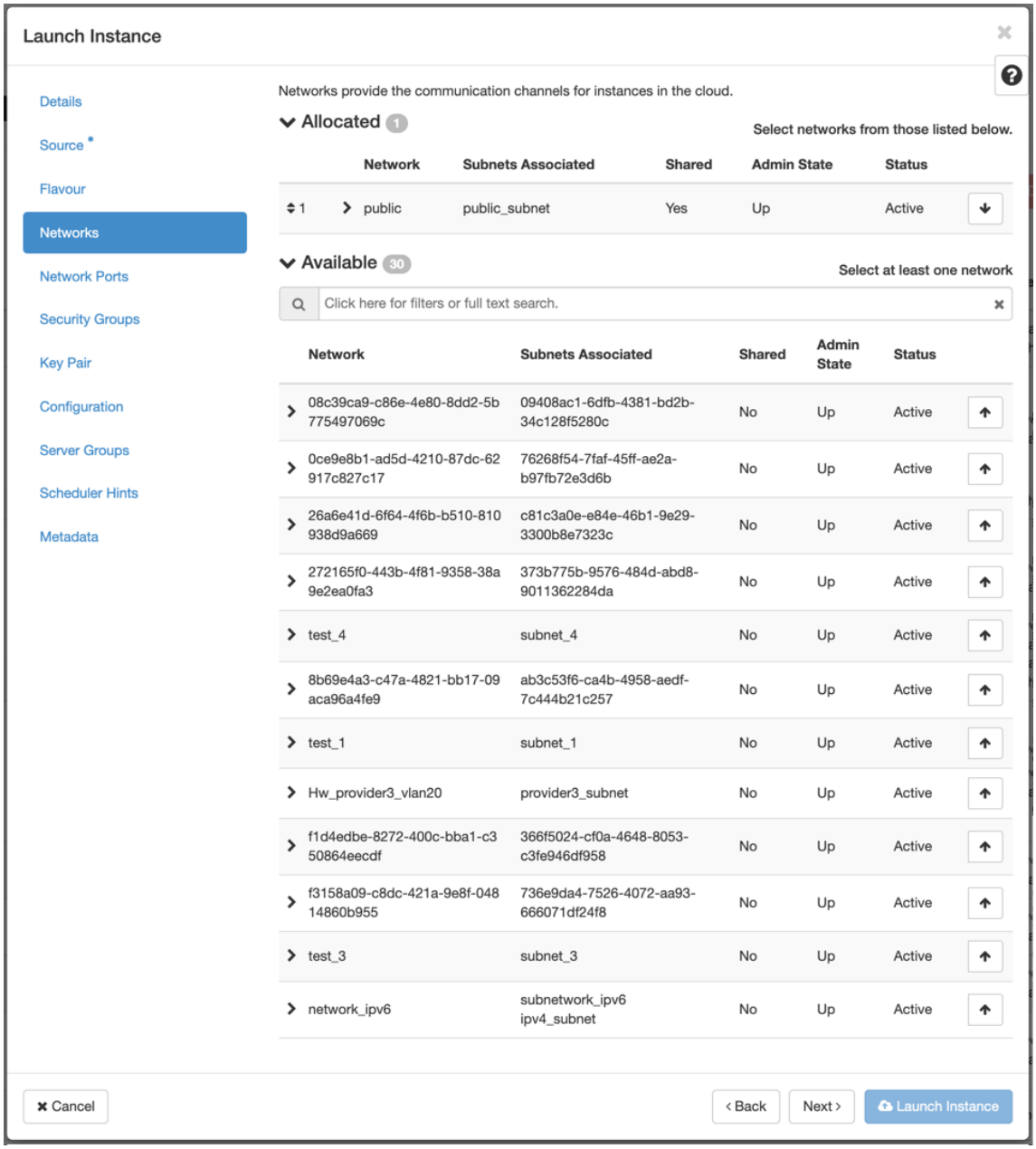
> **REMARQUE**
>
> La version que vous sélectionnez doit disposer de suffisamment de ressources allouées pour prendre en charge le type d'instance que vous essayez de créer. Les versions qui ne fournissent pas suffisamment de ressources pour votre instance sont identifiées sur le tableau disponible avec 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.



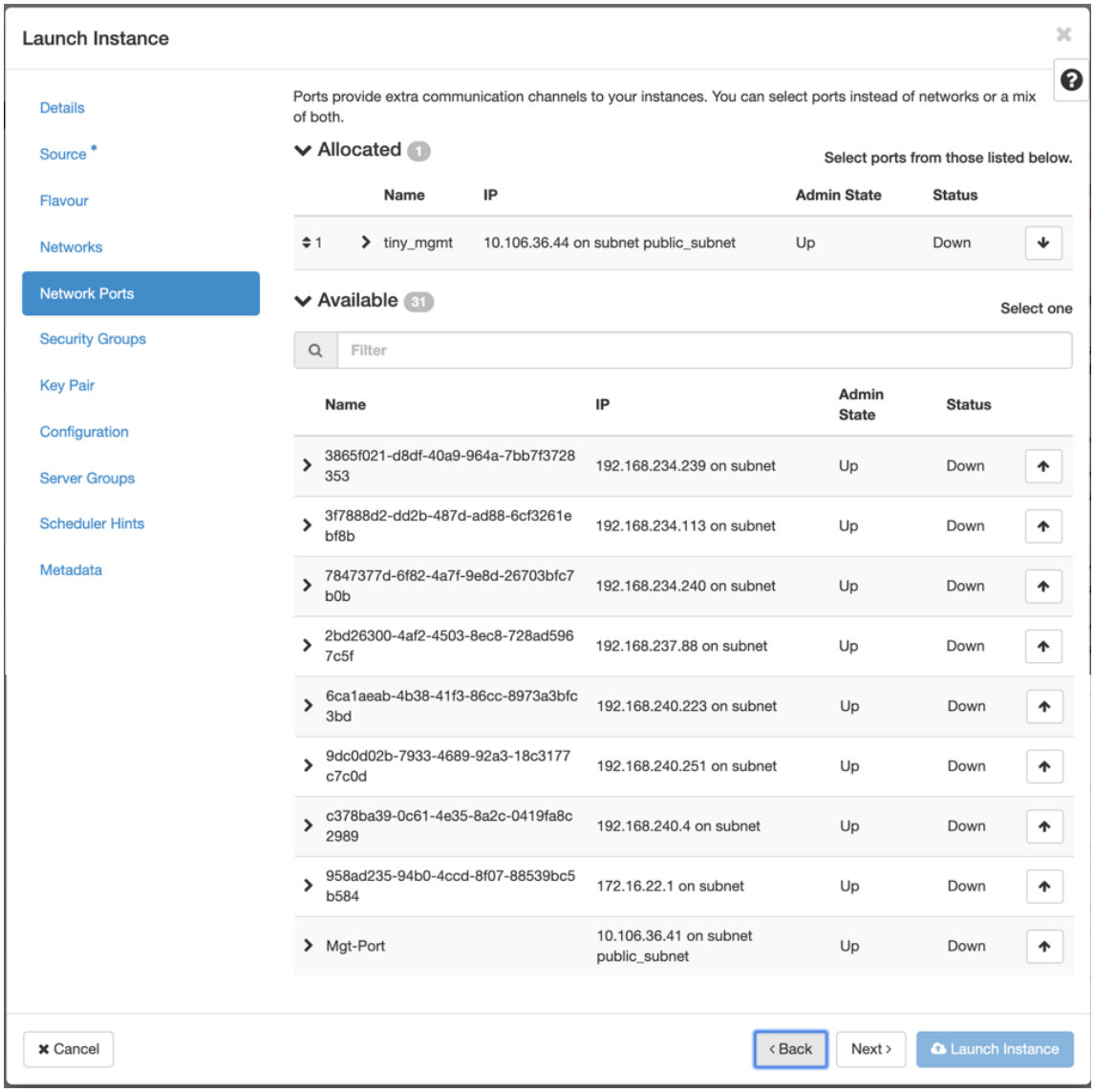
9. Sélectionnez le réseau et cliquez sur **Suivant**. Les réseaux fournissent les canaux de communication pour les instances.

> **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.

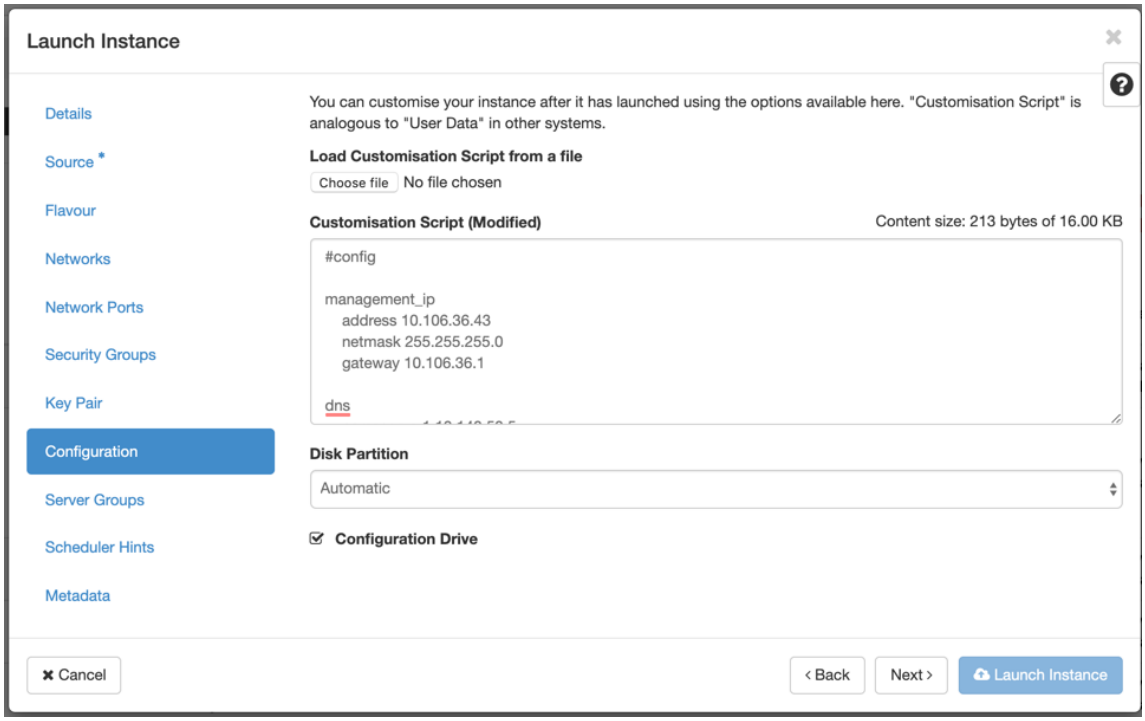


10. Sélectionnez un port réseau pour l'instance et cliquez sur **Suivant**. Les ports réseau fournissent des canaux de communication supplémentaires aux instances.

> **REMARQUE**
>
> Vous pouvez sélectionner des ports au lieu de réseaux ou une combinaison des deux.



11. Accédez à **Configuration** et cliquez sur **Choisir un fichier**. Sélectionnez le fichier user_data . 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.



13. Cliquez sur **Lancer l'instance**.

Configurer la fonctionnalité LTE sur l'appliance 210 SE LTE

August 31, 2022

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. Pour plus d'informations sur la configuration et la gestion des sites LTE de votre réseau, consultez la section Mise à niveau du micrologiciel LTE.

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.

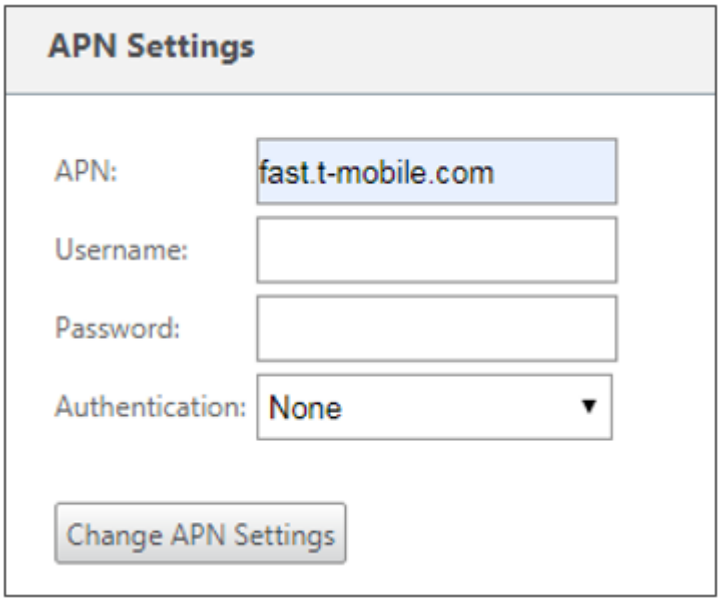
> **Remarque :**
> Seule une carte SIM standard ou 2FF (15 x 25 mm) est prise en charge.

2. Corrigez les antennes sur l'appliance 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'appliance > 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**.

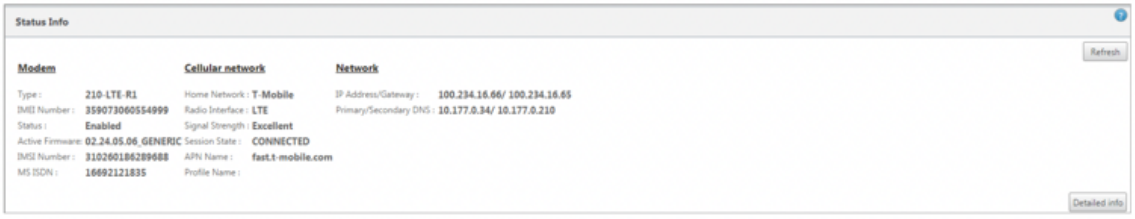
> **Remarque :**
> obtenez les informations APN auprès du transporteur.



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**.

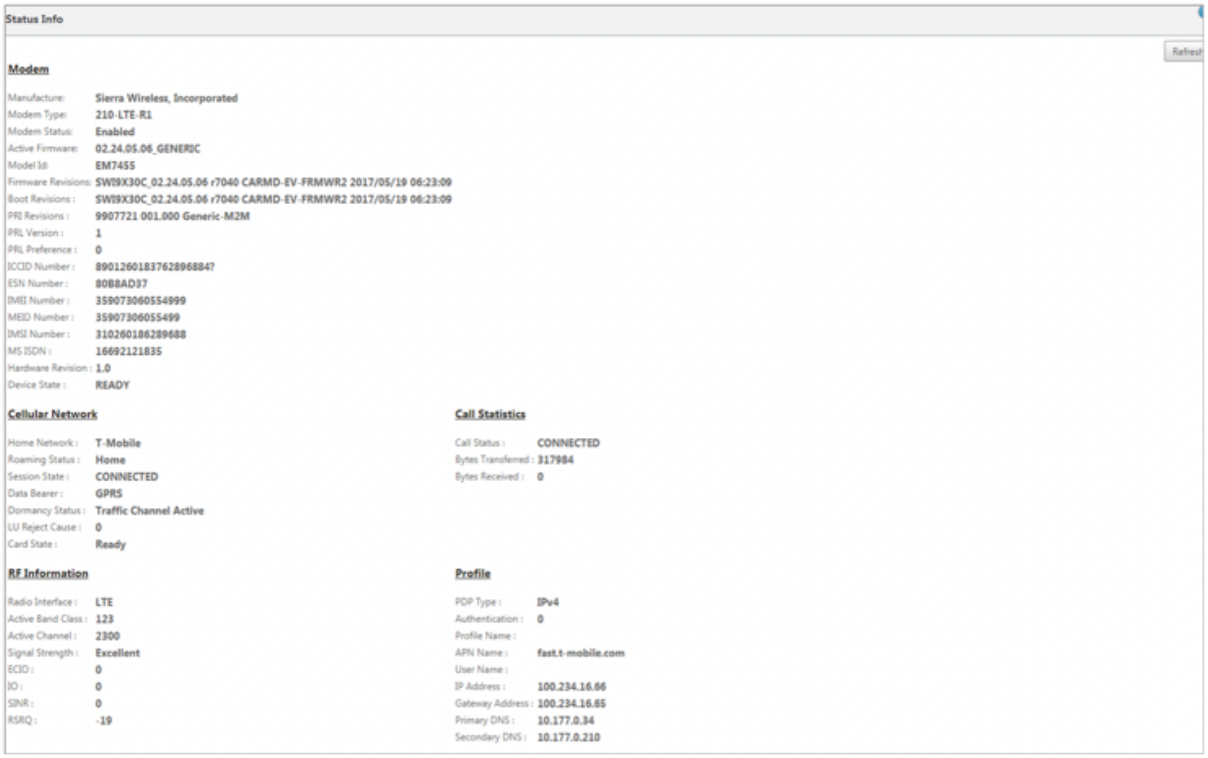
7. Dans l'interface graphique de l'appliance SD-WAN, accédez à **Configuration > Paramètres de l'appliance > Adaptateurs réseau > Haut débit mobile**.

   Vous pouvez afficher les informations d'état des paramètres haut débit mobile.



Voici quelques informations d'état utiles :

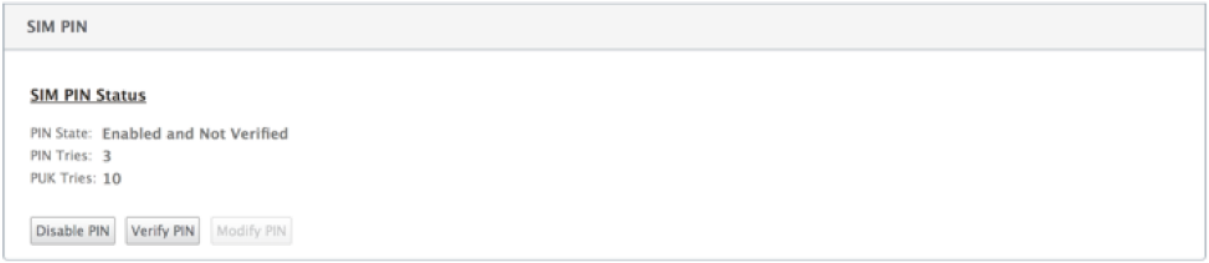
- **Mode de fonctionnement** : affiche l'état du modem.
- **SIM active** : à tout moment, une seule SIM peut être active. Affichage de la carte SIM actuellement active.
- **État de la carte** : Présent indique que la carte SIM est correctement insérée.
- **Force du signal** : Qualité de la force du signal - 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.



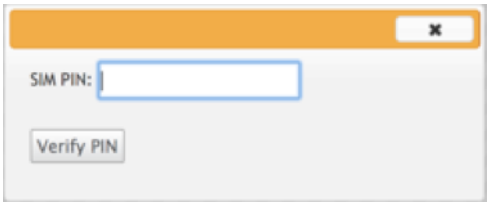
Code PIN de la carte SIM

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'appliance > Cartes réseau > Haut débit mobile > PIN de la carte SIM**.



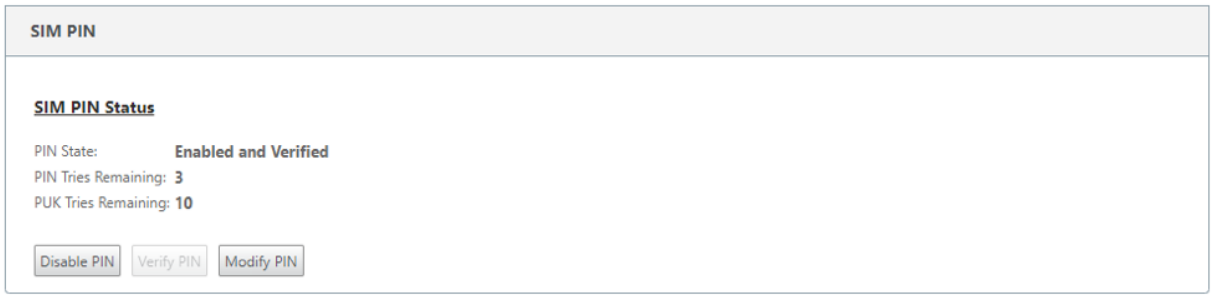
Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.

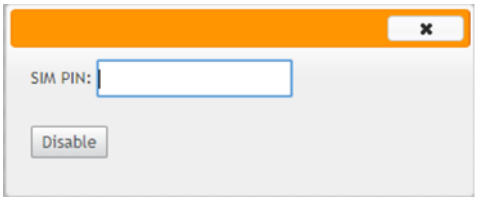


Le statut passe à **Activé et Vérifié**.

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.

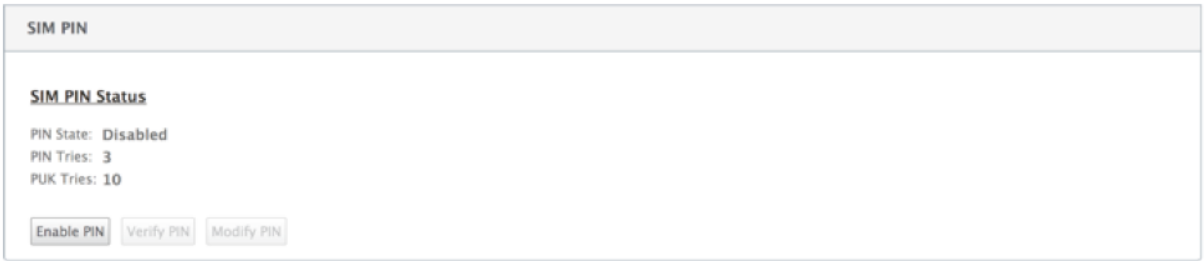




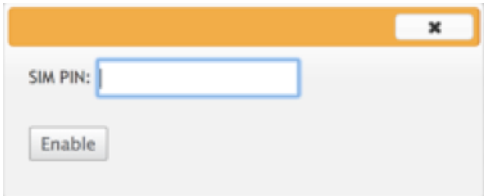
Cliquez sur **Désactiver le code PIN**. Saisissez le **code PIN de la carte SIM** et cliquez sur **Désactiver**

Activer le PIN SIM

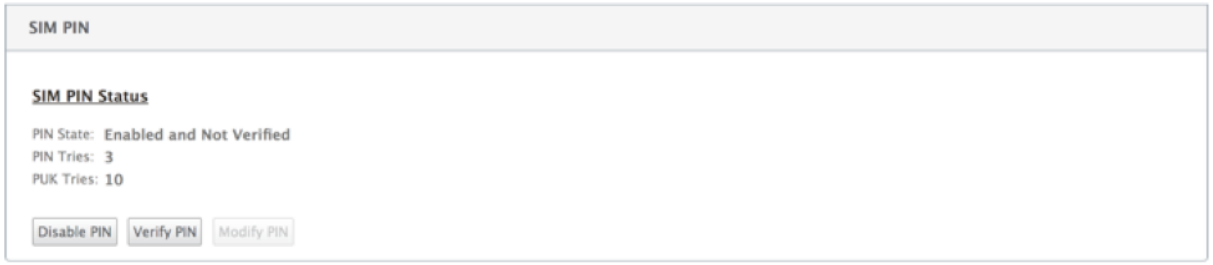
Le code PIN SIM peut être activé pour la carte SIM pour laquelle il est désactivé.



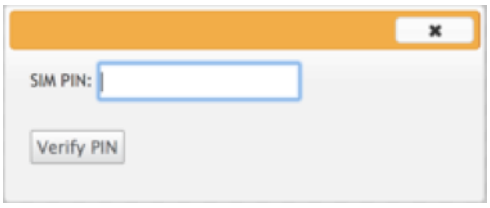
Cliquez sur **Activer le code PIN**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Activer**.



Si l'état du code PIN de la 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.

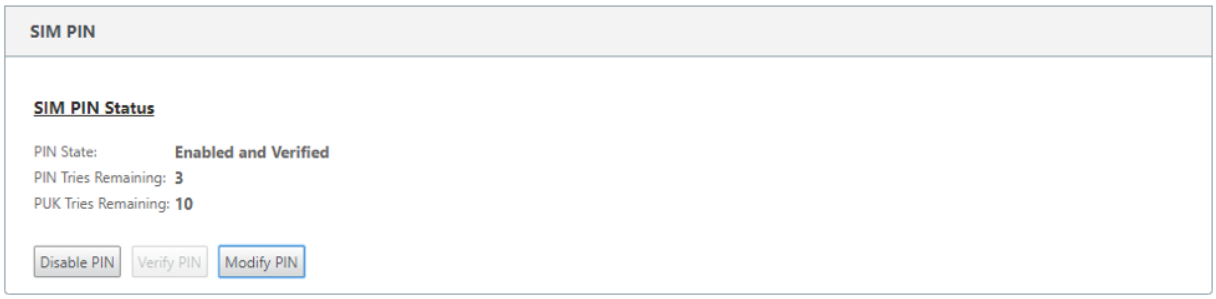


Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.

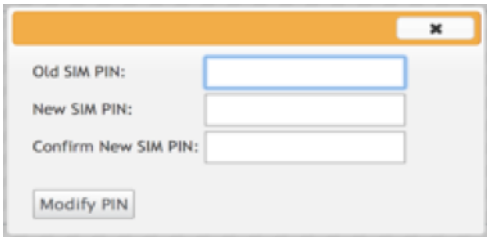


Modifier le code PIN SIM

Une fois que le code PIN est **activé et vérifié**, vous pouvez choisir de le modifier.



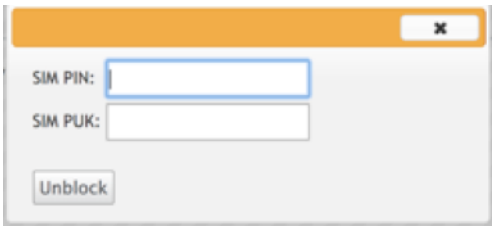
Cliquez sur **Modifier le code PIN**. Entrez le code PIN SIM fourni par le transporteur. Entrez le nouveau code PIN SIM et confirmez-le. Cliquez sur **Modifier le code PIN**.



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.

Pour débloquer une carte SIM, cliquez sur **Débloquer**. Saisissez le **code PIN et le code PUK de la carte SIM** obtenus auprès de l'opérateur, puis cliquez sur **Débloquer**.



> **Remarque :**
> La carte SIM est bloquée de façon permanente avec 10 tentatives infructueuses de PUK, tout en débloquant la carte SIM. Contactez le fournisseur de services de l'opérateur pour obtenir une nouvelle carte SIM.

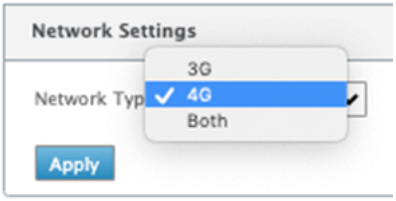
Gérer le firmware

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.

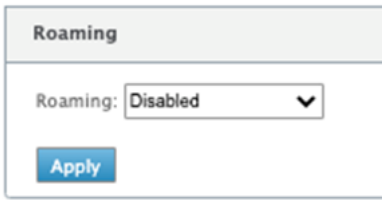
Paramètres réseau

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.



Itinérant

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



Activer/désactiver le modem

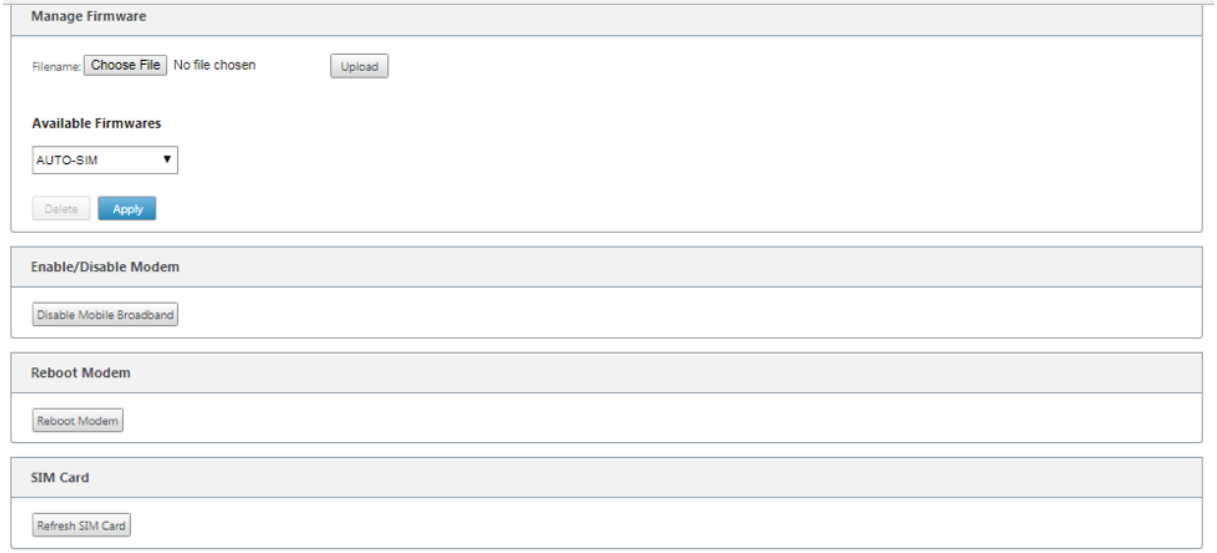
Activez/désactivez le modem en fonction de votre intention d'utiliser la fonctionnalité LTE. Par défaut, le modem LTE est activé.

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.



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'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.

```
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 <unblock> <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

Déploiement sans contact sur LTE

Prérequis pour activer le service de déploiement zéro touche sur LTE

1. Installez l'antenne et la carte SIM de l'appliance 210-SE LTE.
2. Assurez-vous que la carte SIM dispose d'un plan de données activé.
3. 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'appliance.
    - 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'appliance.
4. Assurez-vous que le service Internet est défini pour l'interface LTE dans la configuration de l'appliance 210-SE.

Lorsque l'appliance est mise sous tension, le service de déploiement sans intervention utilise le port

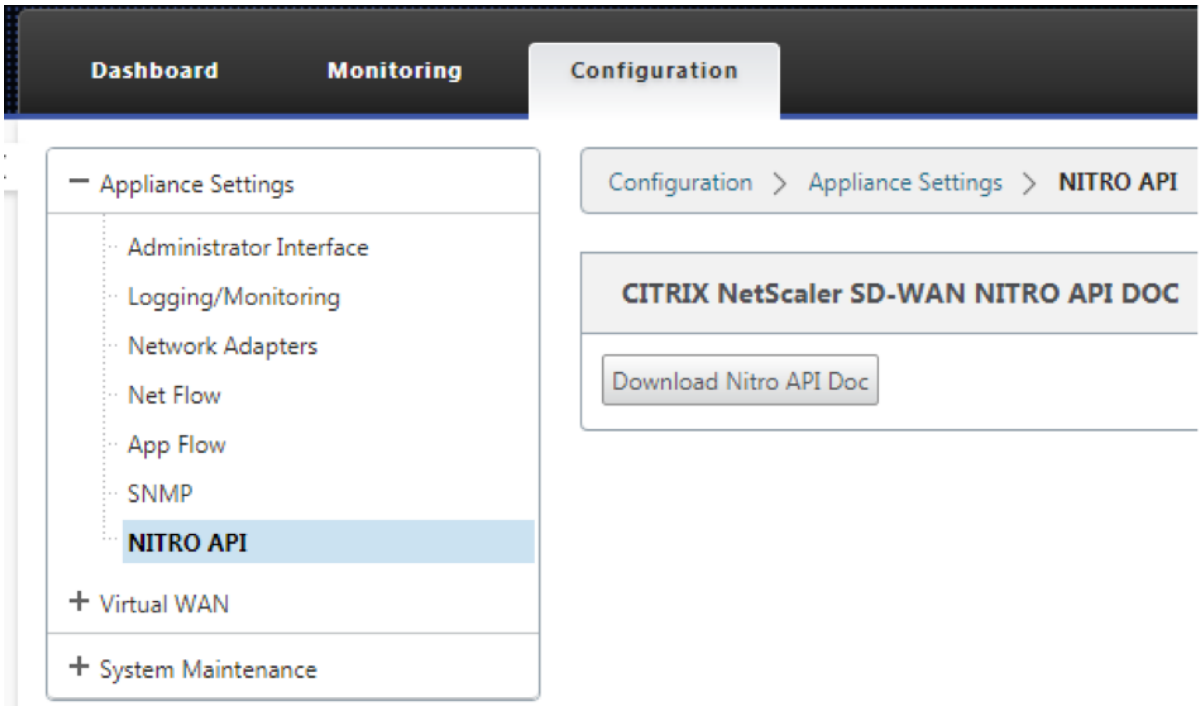
LTE pour obtenir la dernière configuration du logiciel SD-WAN et du SD-WAN uniquement lorsque le port de gestion n'a pas été connecté.

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

August 31, 2022

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.
> - Pour plus d'informations sur la configuration et la gestion de tous les sites LTE de votre réseau, consultez la section Modèle de microprogramme LTE.

Démarrer avec Citrix SD-WAN 110-LTE-WiFi

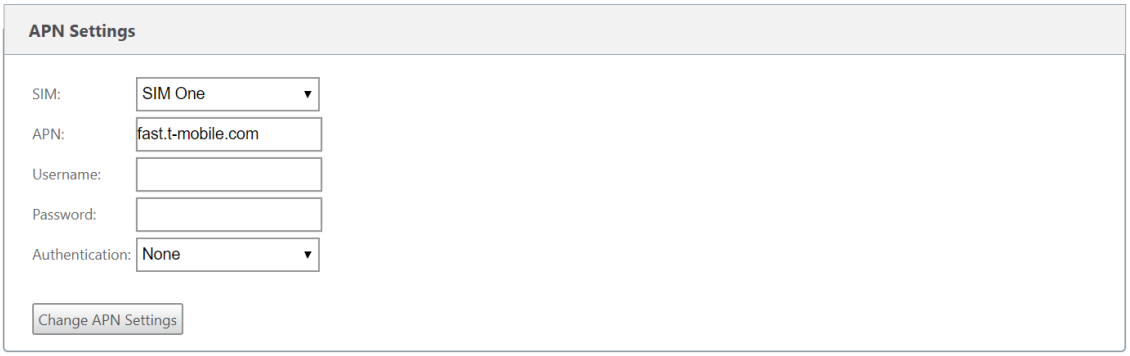
1. Mettez l'appliance sous tension et insérez la carte SIM dans l'emplacement pour carte SIM de l'appliance Citrix SD-WAN 110-LTE-WiFi.

   > **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.

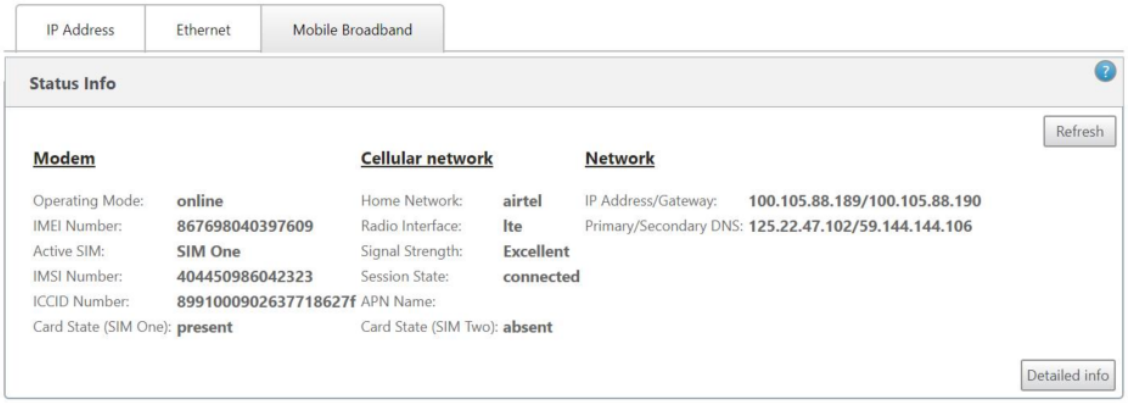


5. Sélectionnez la carte SIM, entrez l'**APN**, le **nom d'utilisateur**, le **mot de passe**et **l'authentification** fournis par l'opérateur. Vous pouvez choisir parmi les protocoles d'authentification PAP, CHAP, PAPCHAP. Si le transporteur n'a fourni aucun type d'authentification, définissez-le sur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

   > **Remarque**
   >
   > Tous ces champs sont facultatifs.

6. Cliquez sur **Modifier les paramètres APN**.
7. Dans l'interface graphique de l'appliance SD-WAN, accédez à **Configuration** > **Paramètres de l'appliance** > **Cartes réseau** > **Haut débit mobile**.

   Vous pouvez afficher les informations d'état des paramètres haut débit mobile.



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** :

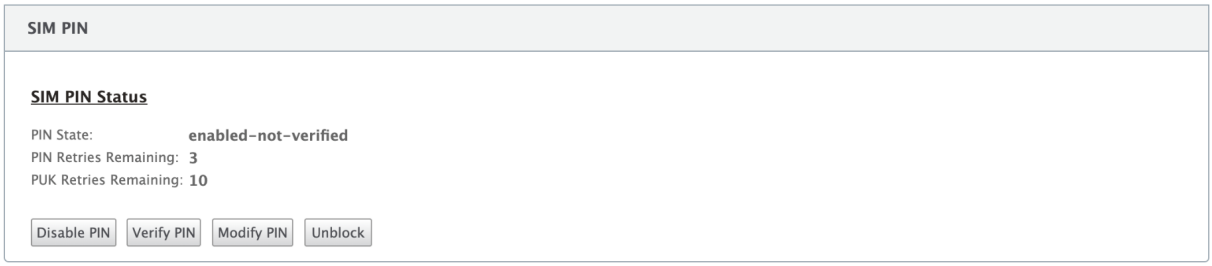
- **SIM One préféré** : si deux cartes SIM sont insérées, au démarrage, le modem LTE utilise SIM One, si disponible. Lorsque le modem LTE est en marche, il utilise la carte SIM (SIM One ou SIM Two) utilisable à ce moment. Il continue à l'utiliser jusqu'à ce que la carte SIM soit active.
- **SIM Two préféré** : 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.

Code PIN de la carte SIM

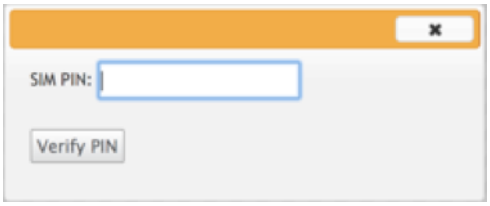
Si vous avez inséré une carte SIM verrouillée avec un code PIN, l'état SIM est **activé, non vérifié**. Vous ne pouvez pas utiliser la carte SIM tant qu'elle n'est pas vérifiée à l'aide du code PIN SIM. Vous pouvez obtenir le code PIN de la carte SIM auprès du transporteur.

> **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**.



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**.

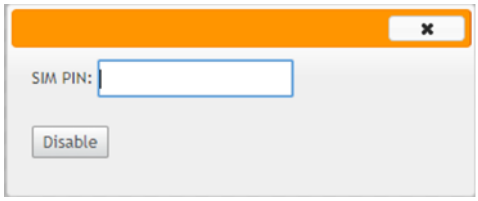


L'état devient **activé vérifié**.

Désactiver le PIN SIM

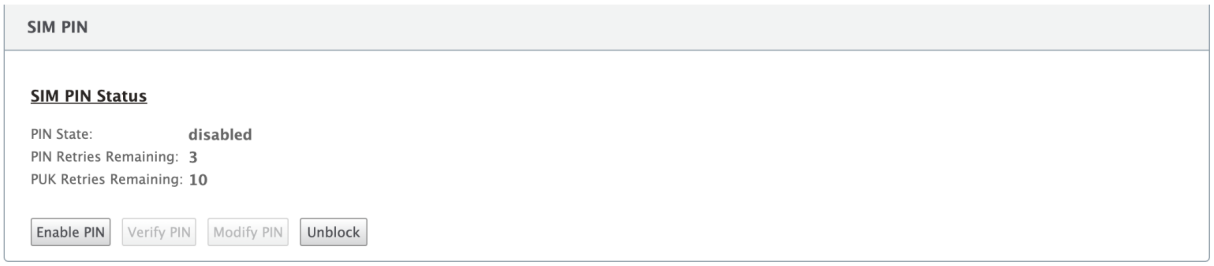
Vous pouvez choisir de désactiver la fonctionnalité PIN SIM pour une SIM pour laquelle le PIN SIM est activé et vérifié.

Cliquez sur **Désactiver le code PIN**. Saisissez le **code PIN de la carte SIM** et cliquez sur **Désactiver**

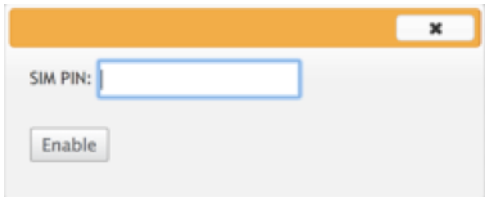


Activer le PIN SIM

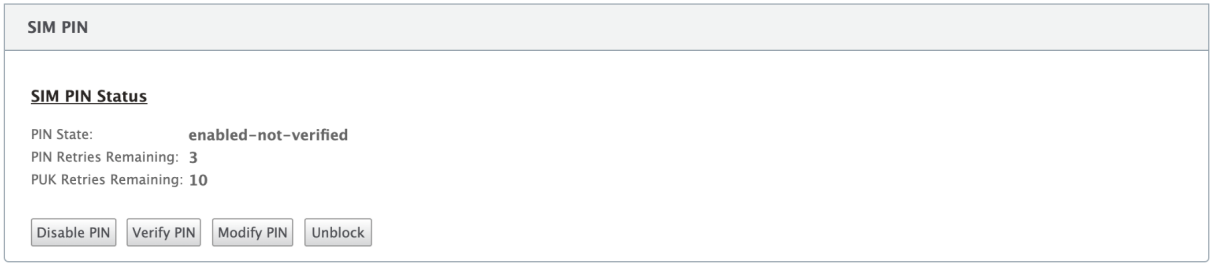
Le code PIN SIM peut être activé pour la carte SIM pour laquelle il est désactivé.



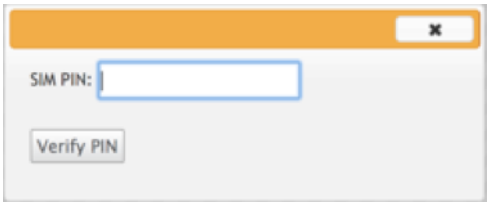
Cliquez sur **Activer le code PIN**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Activer**.



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.



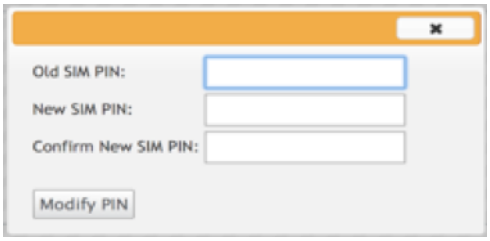
Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.



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.

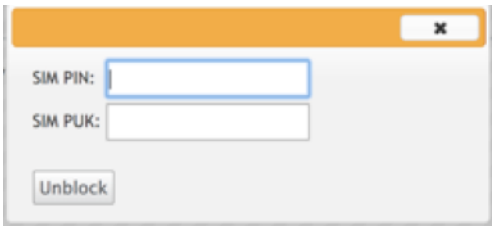
Cliquez sur **Modifier le code PIN**. Entrez le code PIN SIM fourni par le transporteur. Entrez le nouveau code PIN SIM et confirmez-le. Cliquez sur **Modifier le code PIN**.



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.

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**.



> **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.

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.

Itinérant

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

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.

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.

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 <unblock> <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 [1l2] [1l2] {lte>select [1l2] [1l2]}	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

Commande	Description
Reboot {lte>reboot}	Redémarre le modem LTE

> **Remarque**
>
> Les opérations liées au microprogramme ne sont pas prises en charge sur l'appliance 110-LTE-WiFi.

Déploiement sans contact sur LTE

L'appliance 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 :

1. Installez l'antenne, mettez l'appareil sous tension et insérez la carte SIM.
2. Assurez-vous que la carte SIM dispose d'un plan de données activé.
3. 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.
4. Assurez-vous que la configuration de l'appliance 110-LTE-WiFi dispose du service Internet défini pour l'interface LTE.

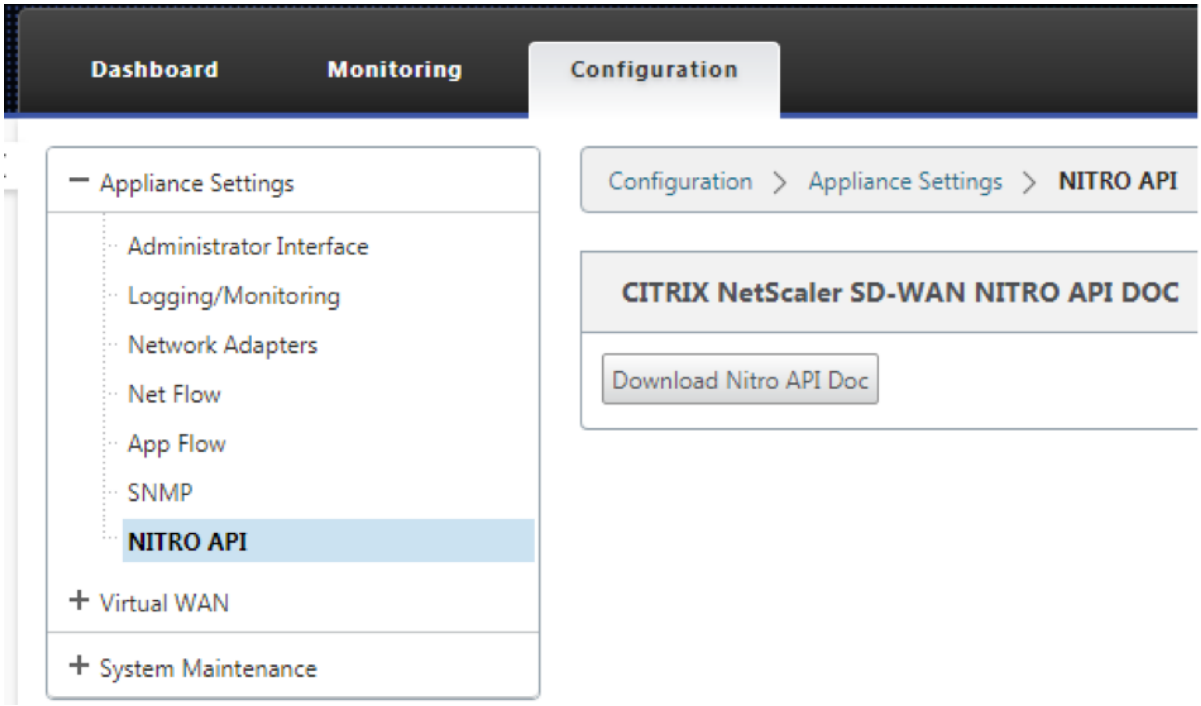
Lorsque l'appliance est sous tension, le service de déploiement zéro touche utilise le port LTE pour obtenir les derniers logiciels SD-WAN et la configuration SD-WAN.

Service de déploiement sans contact sur interface de gestion/données pour l'appliance 110-SE LTE

Connectez le port de gestion/données à Internet et utilisez la procédure de déploiement zéro contact standard prise en charge sur toutes les autres plateformes 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
```

Configurer un modem LTE USB externe

August 31, 2022

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
- 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
- Citrix SD-WAN 2100 SE

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.

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

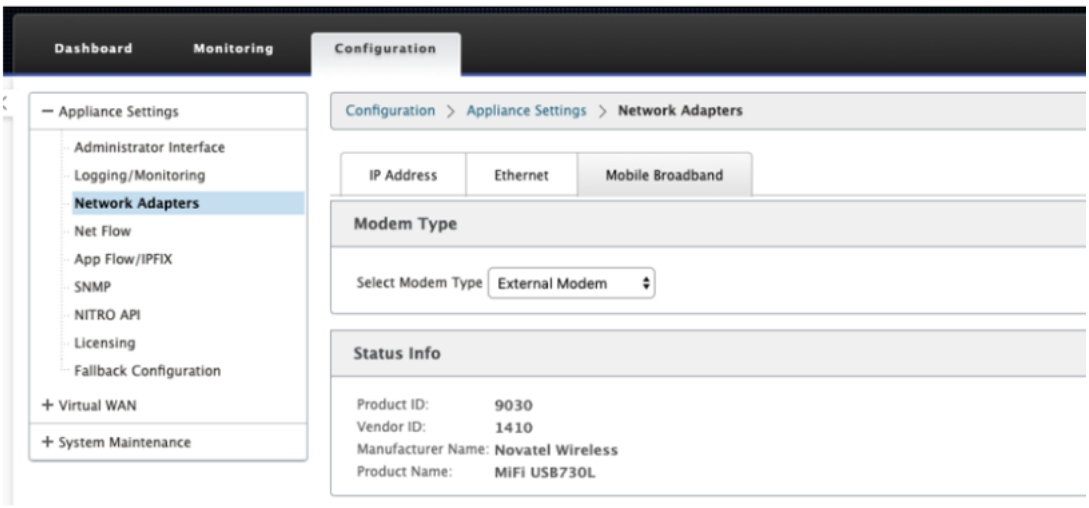
Activez et testez le modem USB conformément aux instructions fournies par votre opérateur sans fil.

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
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

Configurer le modem USB externe

Vous pouvez configurer un site LTE à l'aide d'un modem USB externe via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Mise à niveau du micrologiciel 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.

Pour plus d'informations sur le déploiement sans intervention via le service SD-WAN Orchestrator, consultez la section Déploiement Zero Touch.

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_éther	4G uniquement
États-Unis	AT&T	Modem AT&T Global USB800	cdc_éther	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 **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
```

Déploiements

August 31, 2022

Voici quelques-uns des scénarios de cas d'utilisation implémentés à l'aide d'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
- Déploiement sans intervention
- Déploiement d'une région unique

- Déploiement dans 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 nécessaires au déploiement des éditions standard 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'appliance (un par site)
- Modèle d'appliance 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

August 31, 2022

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 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 la tête de réseau 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).

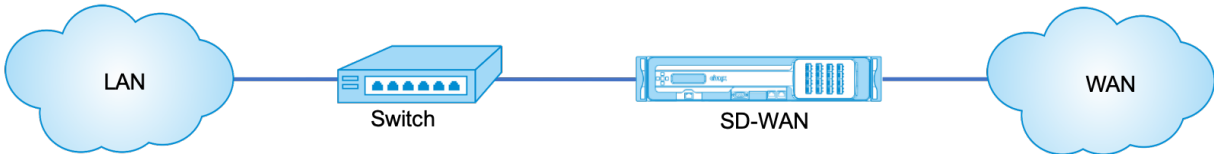
Mode passerelle

August 31, 2022

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 :

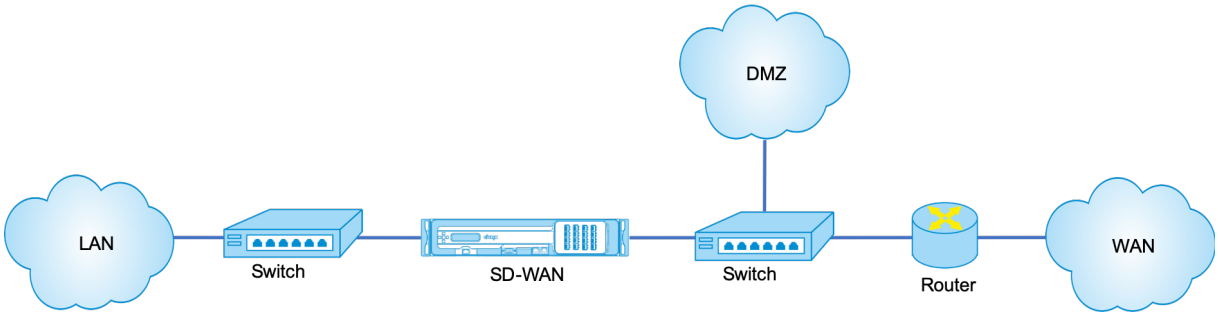
- Pour afficher tout le trafic à destination et en provenance du WAN
- Pour effectuer un routage local

Le mode de déploiement Gateway est pris en charge sur le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Interfaces.



> **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'appliance, la Gateway par défaut du site échoue également, provoquant une panne jusqu'à ce que l'appliance et la Gateway par défaut soient restaurées.

En mode **Inline**, 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. Mode Inline utilisé pour s'intégrer dans des réseaux déjà bien définis.

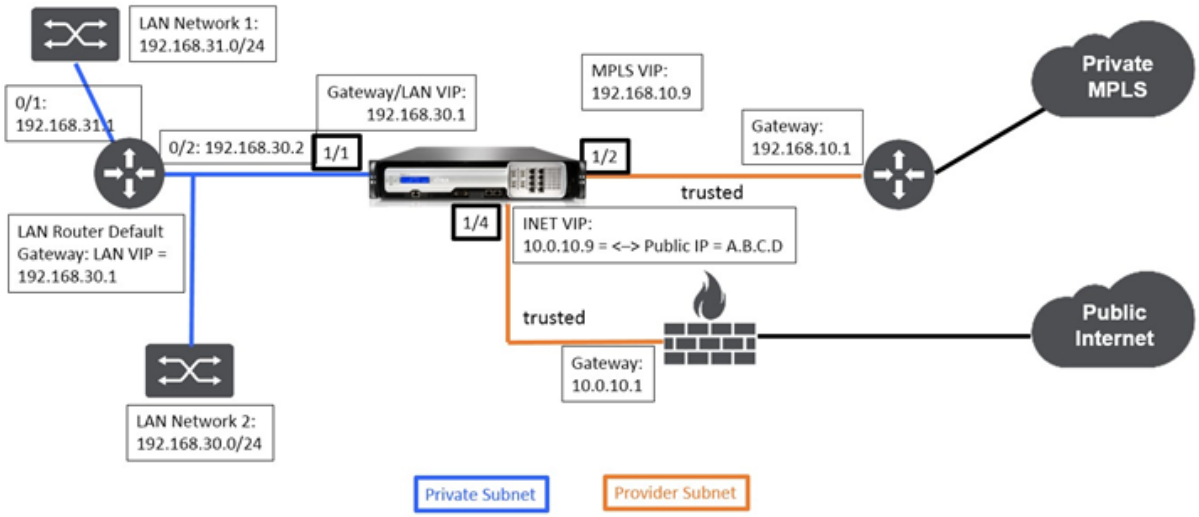


Cet article fournit une procédure étape par étape pour configurer un dispositif SD-WAN en mode passerelle dans un exemple de configuration réseau. Le déploiement en ligne est également décrit pour le côté de la branche pour terminer la configuration. Un réseau peut continuer à fonctionner si un périphérique Inline est supprimé, mais perd tout accès si le périphérique Gateway est supprimé.

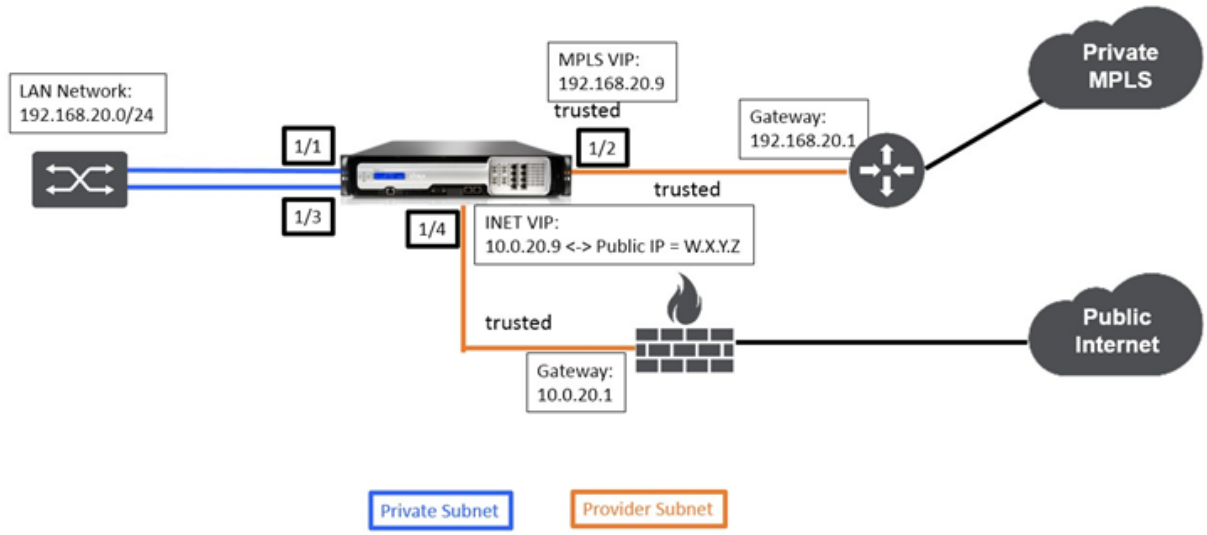
Topologie

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



Configuration du mode Gateway de site du datacenter

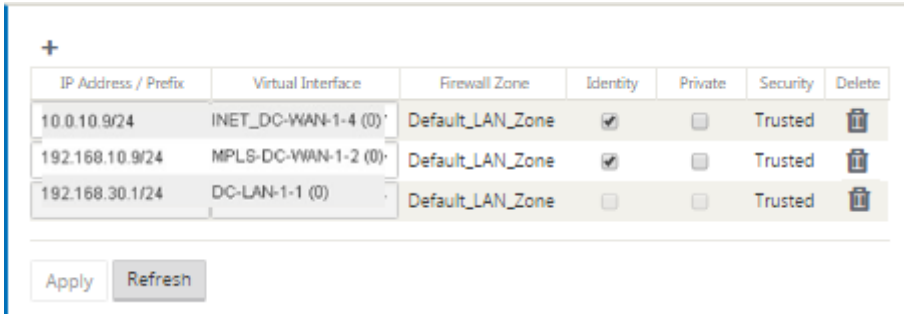
Voici les étapes de configuration de haut niveau pour configurer le déploiement de la passerelle de site de centre de données :

1. Créez un site DC.
2. Remplissez les groupes d'interfaces 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 Routes s'il y a plus de sous-réseaux dans l'infrastructure LAN.

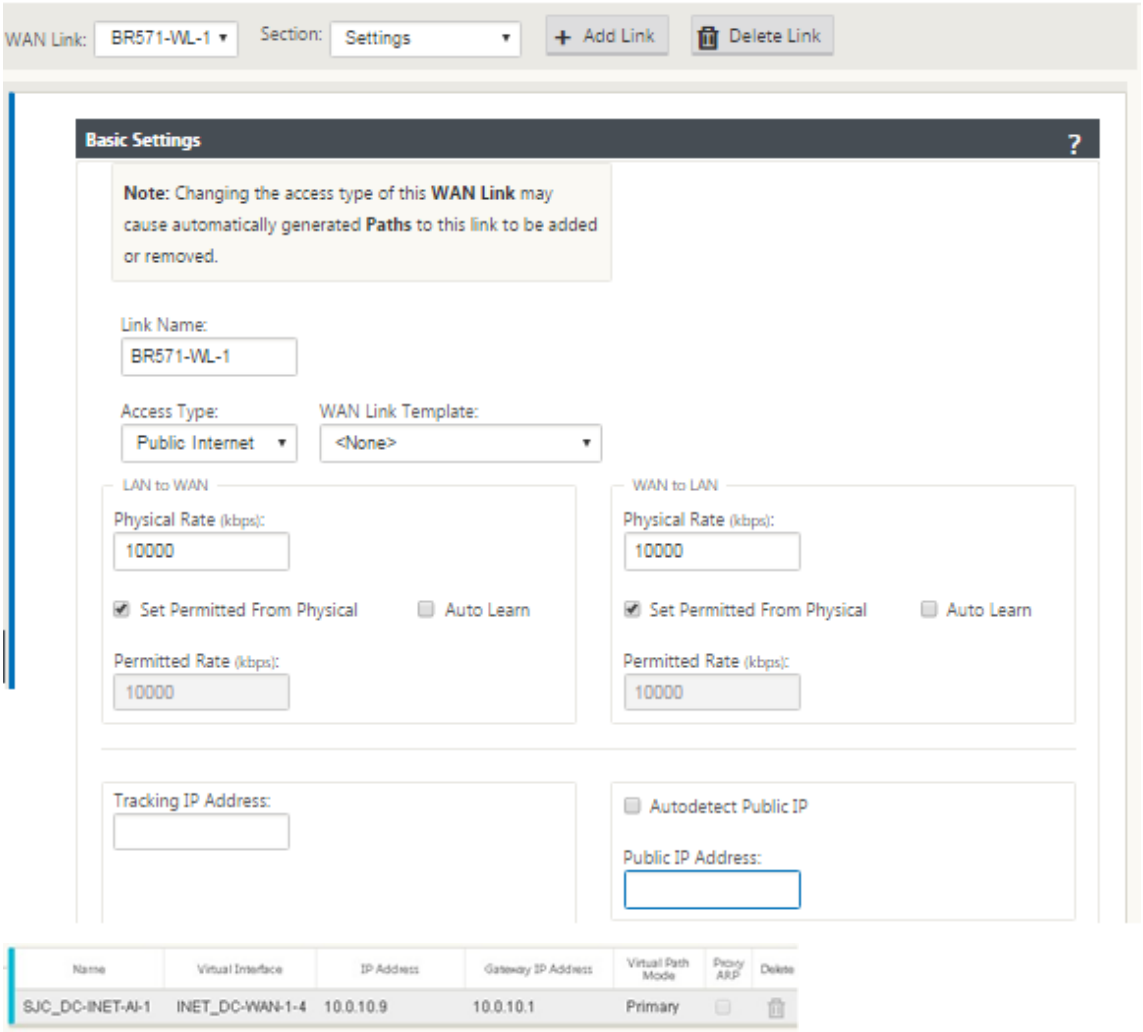
Pour créer une adresse IP virtuelle (VIP) pour chaque interface virtuelle

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.



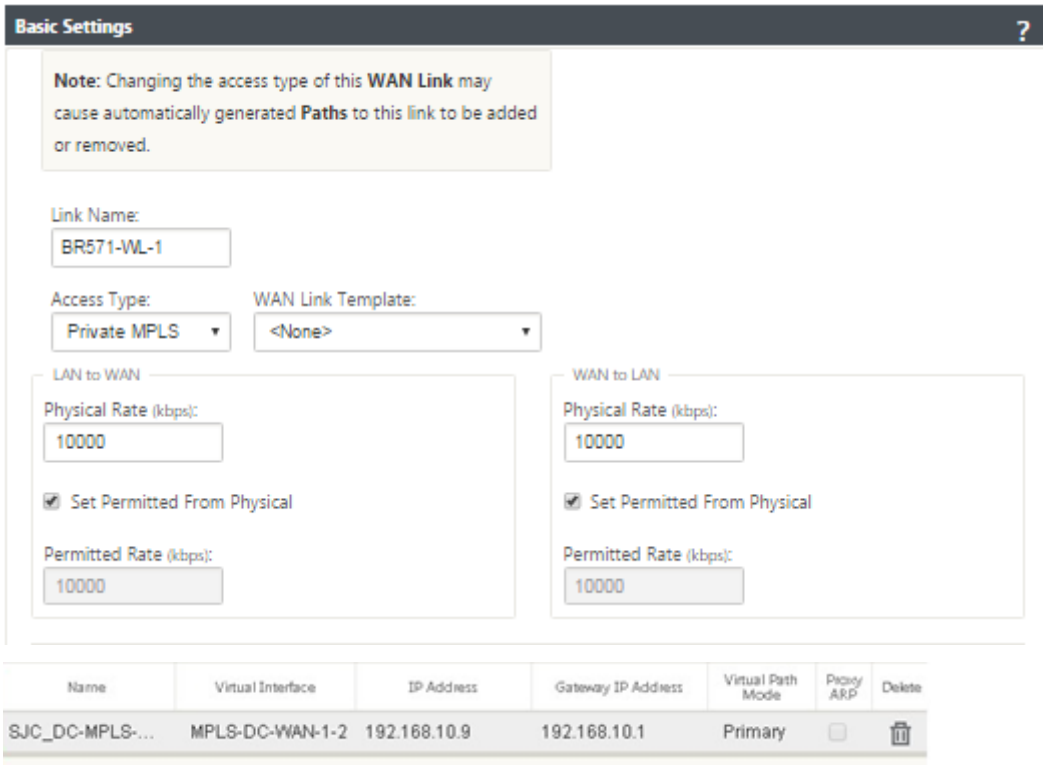
Pour remplir les liens WAN en fonction de la vitesse physique et non de la vitesse de rafale à l'aide de la liaison Internet :

1. Accédez à **Liens WAN**, cliquez sur le **bouton+ Ajouter un lien** pour ajouter un lien WAN pour le lien Internet.
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.



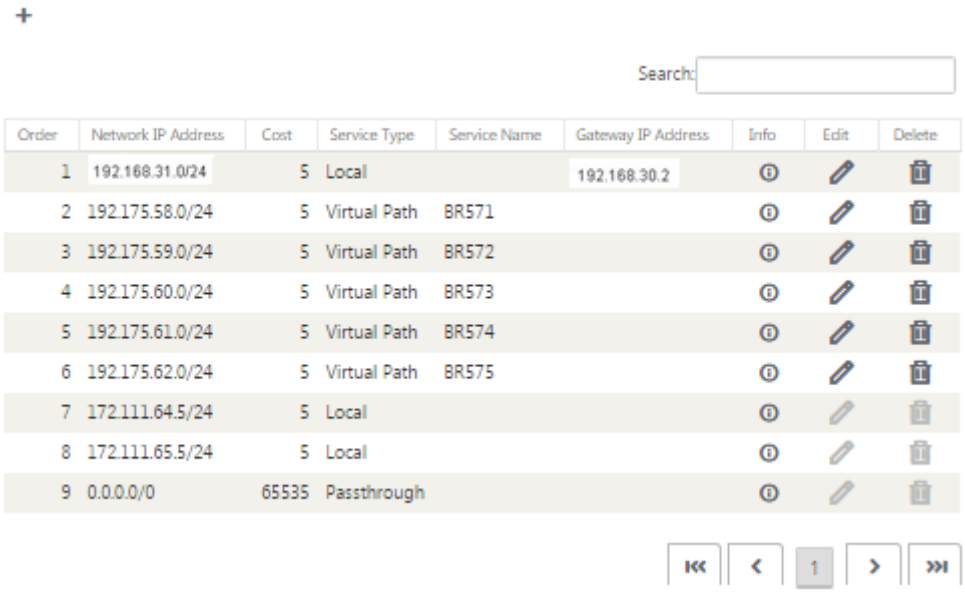
Pour créer un lien MPLS

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 **Access Interfaces**, 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.



Pour remplir les itinéraires

Les itinéraires sont créés automatiquement en fonction de la configuration ci-dessus. L'exemple de topologie DC LAN illustré ci-dessus comporte un sous-réseau LAN supplémentaire qui est **192.168.31.0/24**. Une route doit être créée 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.



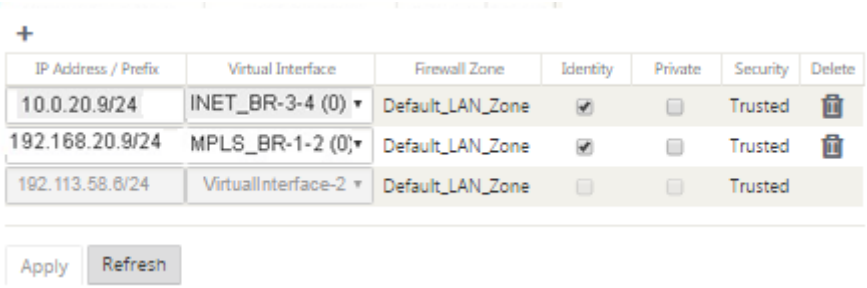
Configuration du déploiement en ligne du site de succursale

Voici les étapes de configuration de haut niveau pour configurer le site de branche pour le déploiement en ligne :

1. Créez un site de succursale.
2. Remplissez les groupes d'interfaces 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 Routes s'il y a plus de sous-réseaux dans l'infrastructure LAN.

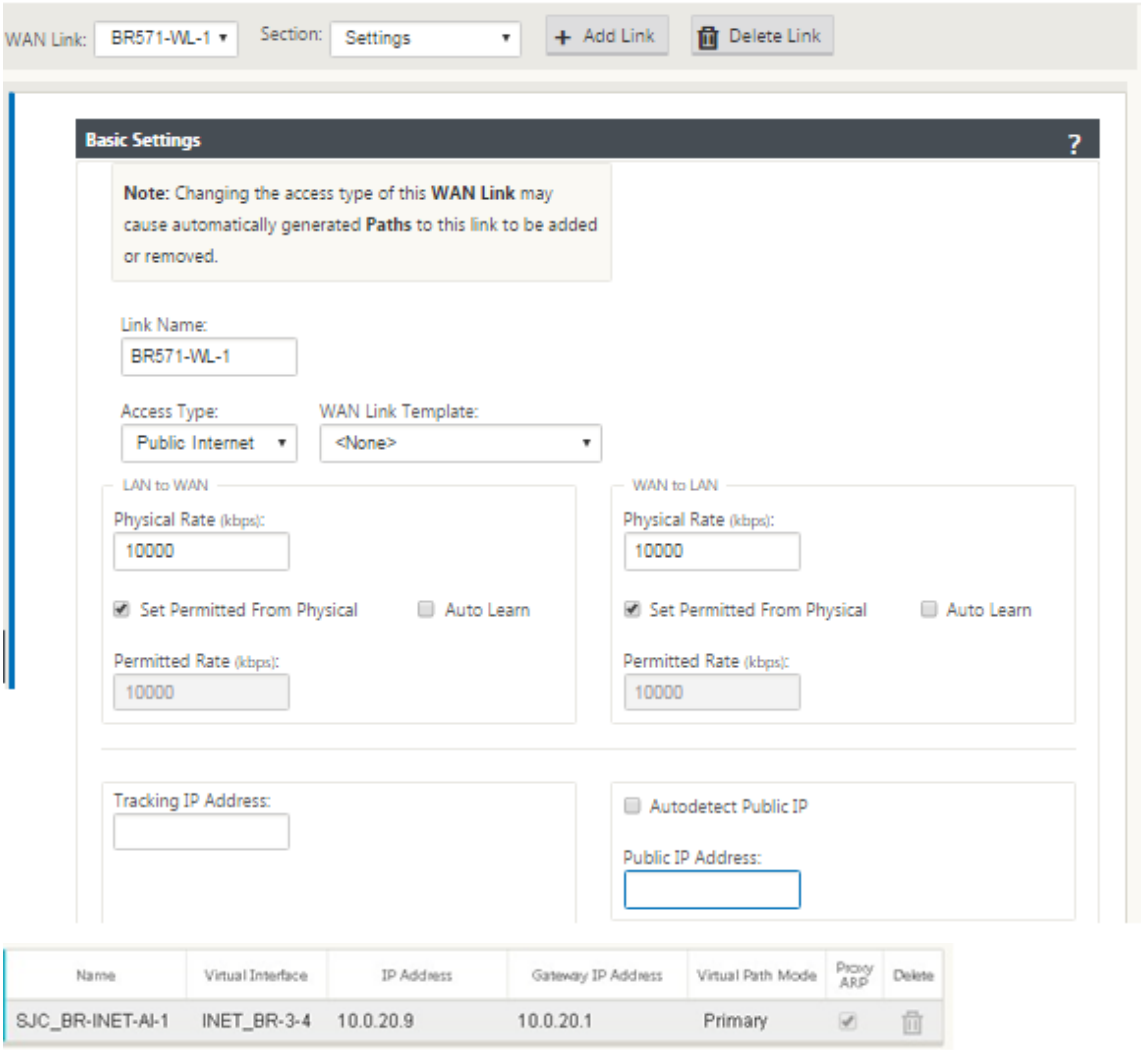
Pour créer une adresse IP virtuelle (VIP) pour chaque interface virtuelle

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.



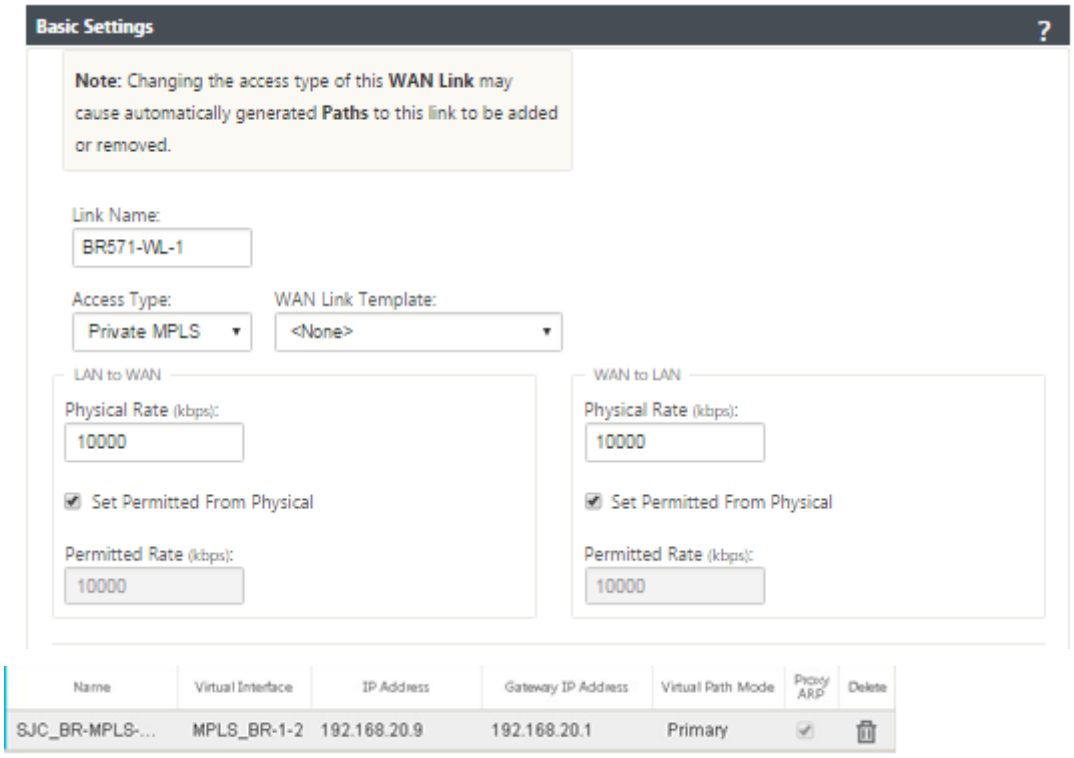
Pour remplir les liens WAN en fonction de la vitesse physique et non de la vitesse de rafale à l'aide de la liaison Internet :

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.



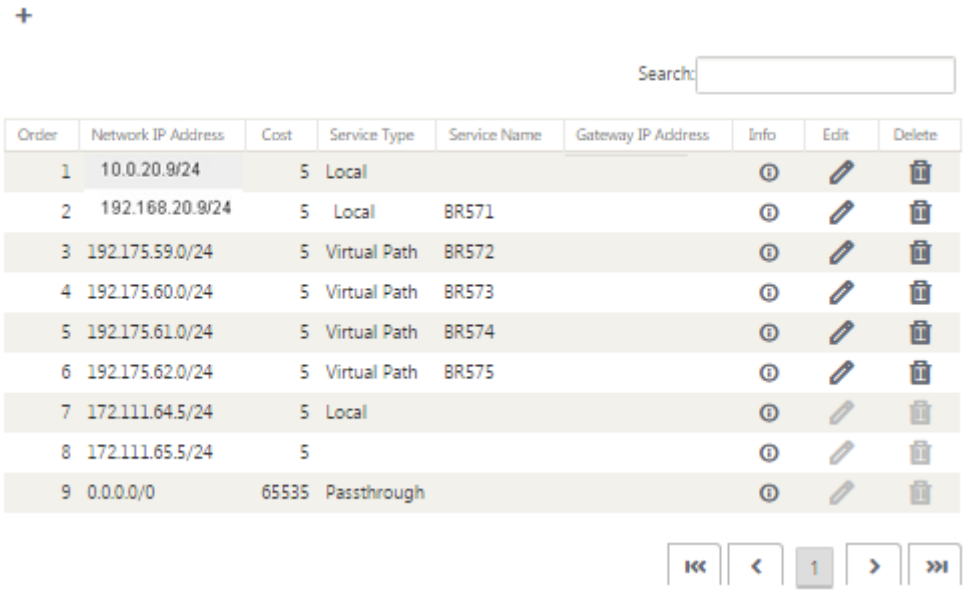
Pour créer un lien MPLS

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.



Pour remplir les itinéraires

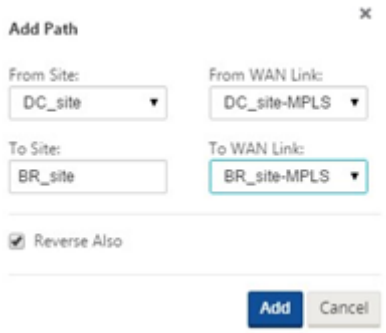
Les itinéraires sont créés automatiquement en fonction de la configuration ci-dessus. Dans le cas où il y a plus de sous-réseaux spécifiques à cette succursale distante, des itinéraires spécifiques doivent être ajoutés pour identifier la Gateway vers le trafic direct pour atteindre ces sous-réseaux back-end.



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 d'accès pour les liaisons WAN définies comme le type d'accès Internet public. Vous devez utiliser la fonction de groupe de chemins 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).



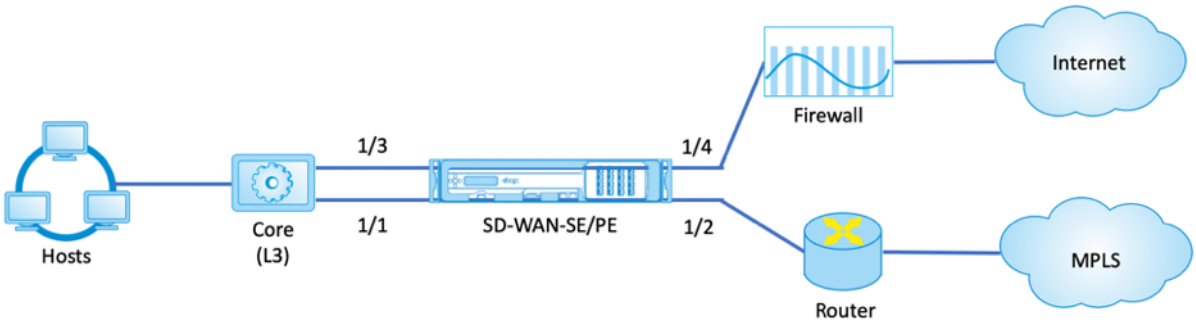
Après avoir effectué toutes les étapes ci-dessus, passez à la section Préparation des packages d'appliance SD-WAN. —>

Mode Inline

August 31, 2022

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. Pour plus d'informations sur le déploiement en mode Inline basé sur les services SD-WAN Orchestrator, consultez Interfaces.



Mode virtuel en ligne

August 31, 2022

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'appliance, et l'appliance 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'appliance SD-WAN afin que l'appliance puisse être contournée en cas de défaillance.
- Le mode virtuel en ligne place l'appliance 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'appliance Citrix SD-WAN doit être configurée pour transmettre le trafic à la Gateway appropriée. Le trafic destiné au chemin virtuel est dirigé vers l'appliance 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

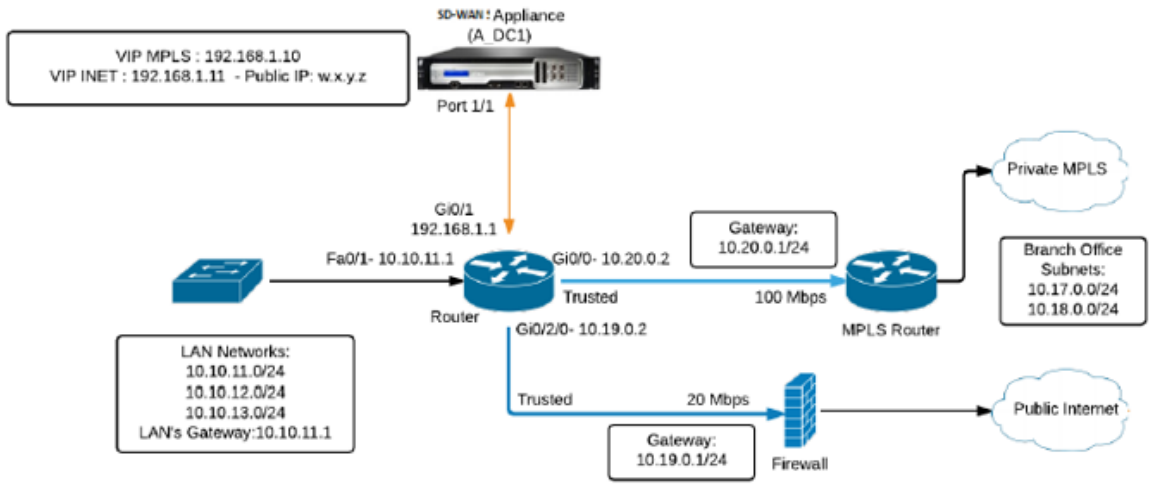
routes et les réseaux locaux virtuels.

- Tableau de déploiement

Pour plus d'informations sur le déploiement du mode Virtual Inline basé sur les services SD-WAN Orchestrator, consultez Interfaces.

Voici un exemple de diagramme de réseau et de table de déploiement :

Topologie du centre de données —Mode virtuel en ligne



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. Résolvez les erreurs d'audit (le cas échéant).

Créer un réseau SD-WAN

August 31, 2022

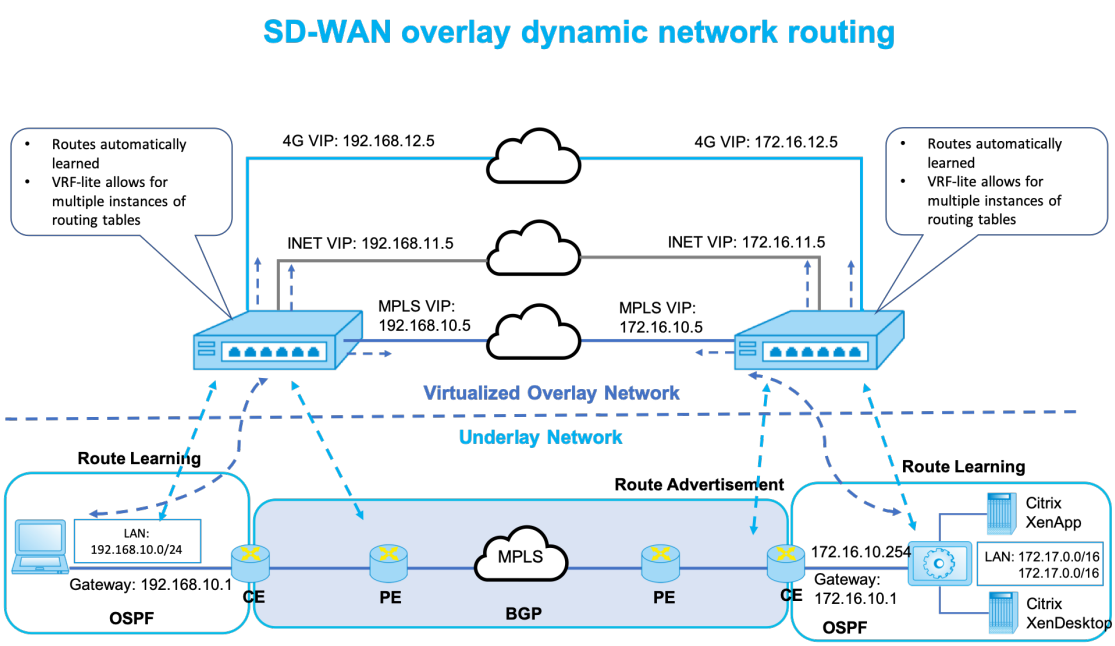
Pour créer un réseau de superposition SD-WAN sans avoir besoin de créer des tables de routage de superposition SD-WAN :

1. Créez un tunnel de chemin WAN 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. Agréger 2, 3 et 4 chemins WAN (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, qui est moins intelligente et peu rentable.

Composants de routage SD-WAN et topologie réseau

- Local —sous-réseau réside sur ce site (annoncé dans l'environnement SD-WAN)
- Chemin virtuel : envoyé via le chemin virtualisé à l'appliance de site sélectionnée
- Intranet : sites sans appliance SD-WAN
- Internet —trafic lié à Internet
- Pass-through —trafic intact, dans une interface de pont à 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.



Haute disponibilité

August 31, 2022

Cette rubrique couvre les déploiements et configurations haute disponibilité (haute disponibilité) pris en charge par les appliances SD-WAN (Standard 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'appliances haute disponibilité se trouve en dehors du chemin de données. Le trafic d'application est redirigé vers la paire d'appliances 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.

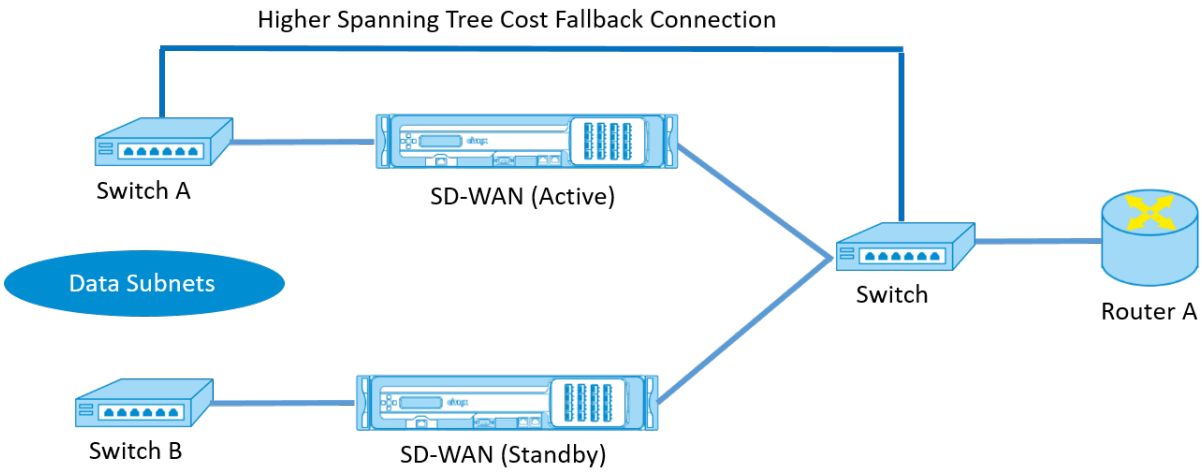
Toutefois, si les deux appliances SD-WAN actif/de secours deviennent inactives, le routeur tente de rediriger le trafic vers les appliances. La surveillance SLA IP peut être configurée au niveau du routeur pour désactiver PBR, si l'appliance suivante n'est pas accessible. Il permet au routeur de revenir en arrière pour effectuer une recherche d'itinéraire et transférer les paquets de manière appropriée.

Mode haute disponibilité parallèle Inline :

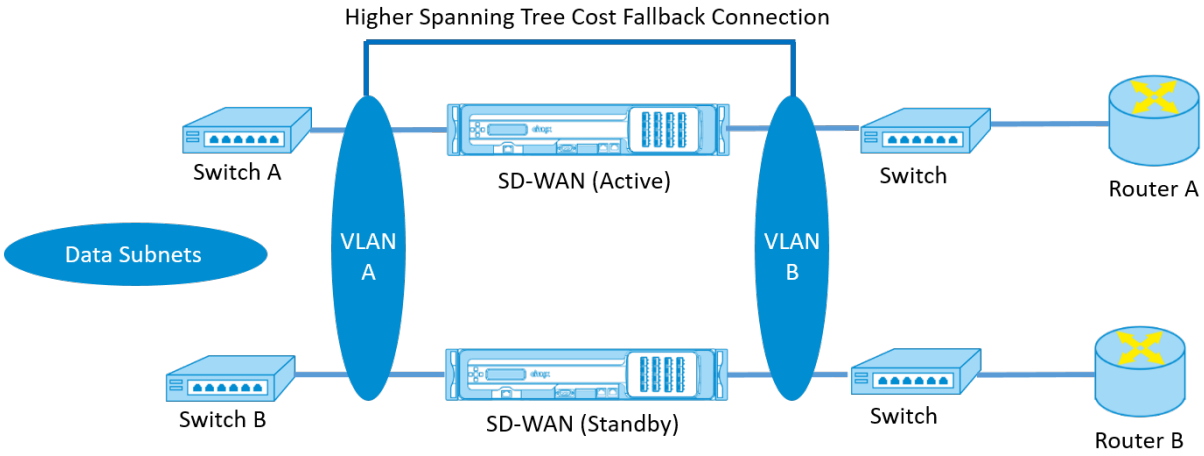
En mode haute disponibilité Parallel Inline, les appliances SD-WAN sont déployées les unes à côté des autres, en ligne avec le chemin de données. Un seul chemin d'accès à l'appliance active est utilisé. Il est important de noter que les groupes d'interface de contournement sont configurés pour être bloqués 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.



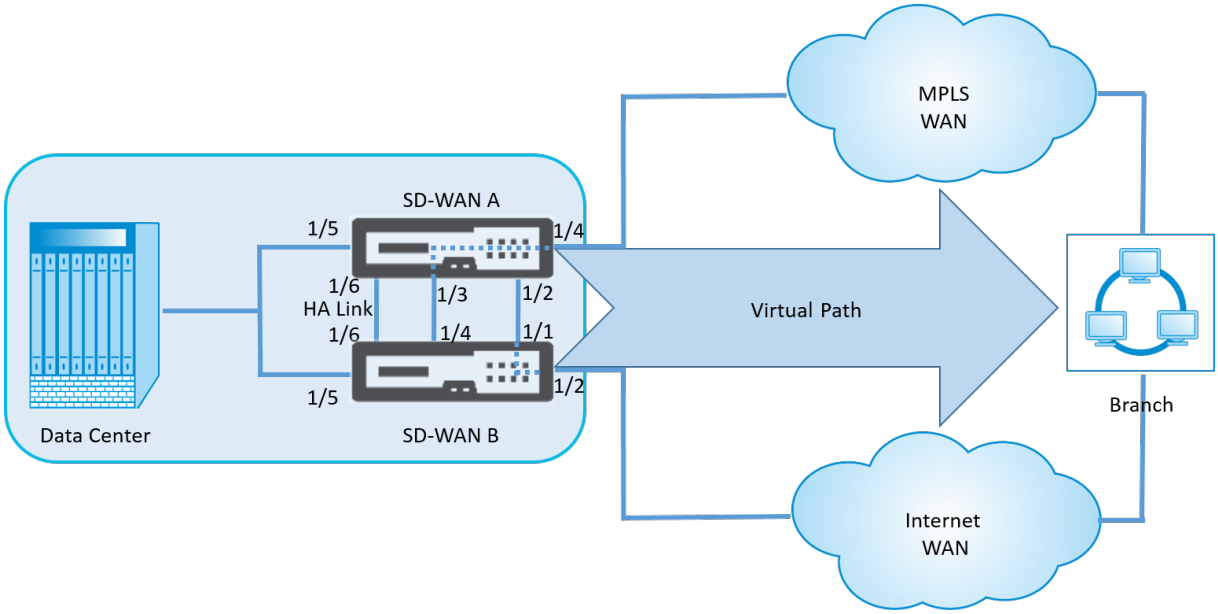
Mode Fail-to-wire :

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'interruption 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.

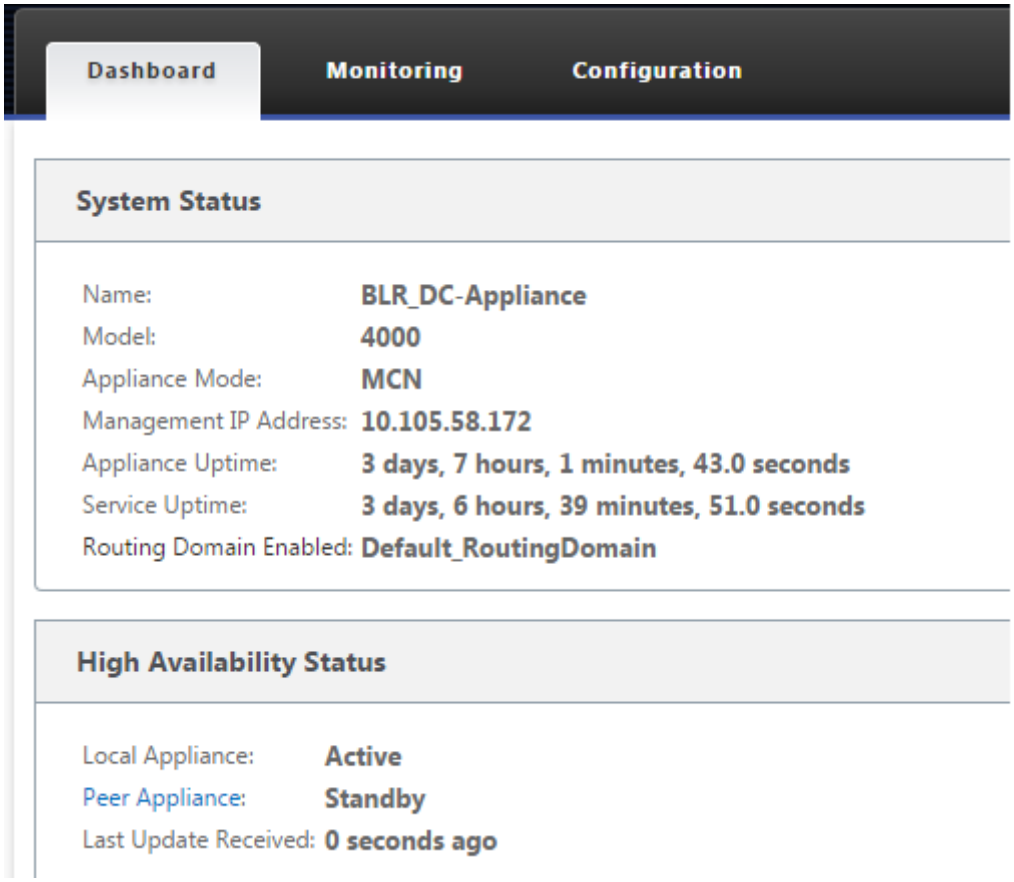
Si une perte de service minimale est acceptable lors d'un basculement, le mode de haute disponibilité Fail-to-Wire est une meilleure solution. Le mode de haute disponibilité Fail-to-Wire protège contre les défaillances de l'appliance et la haute disponibilité parallèle en ligne protège contre toutes 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.

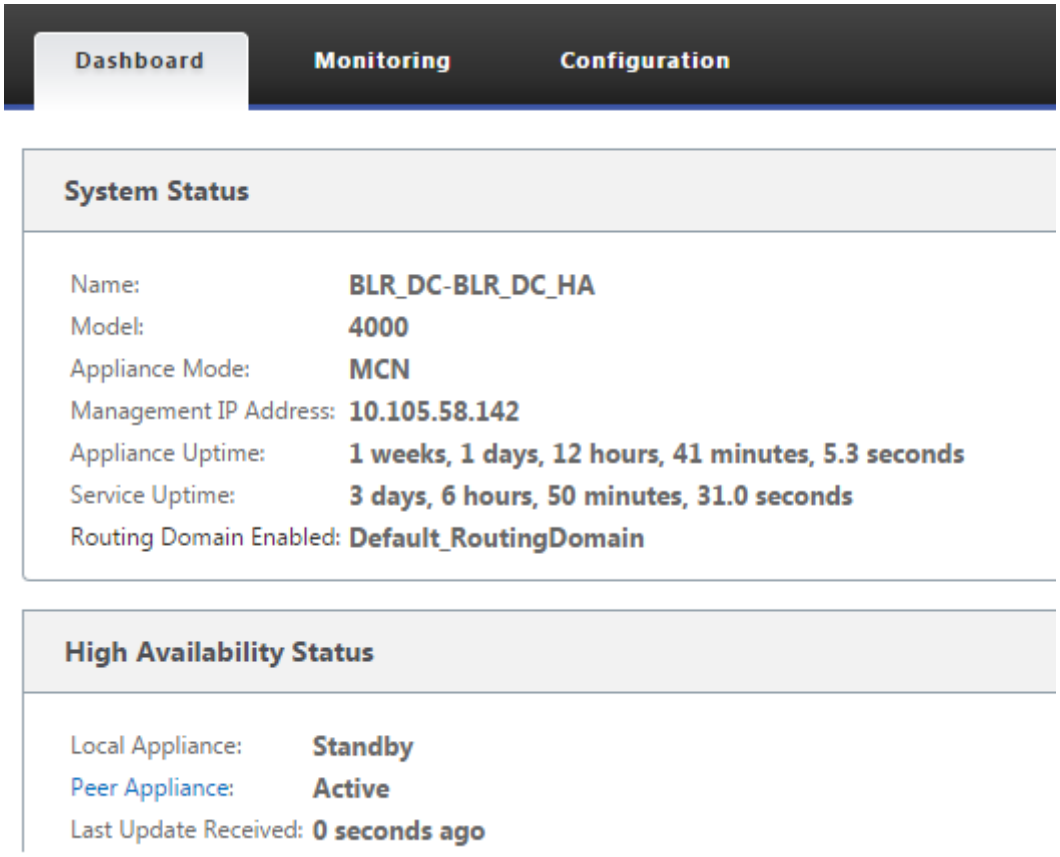
Pour plus d'informations sur le déploiement HA basé sur le service SD-WAN Orchestrator, consultez Détails sur l'appareil.

Surveillance

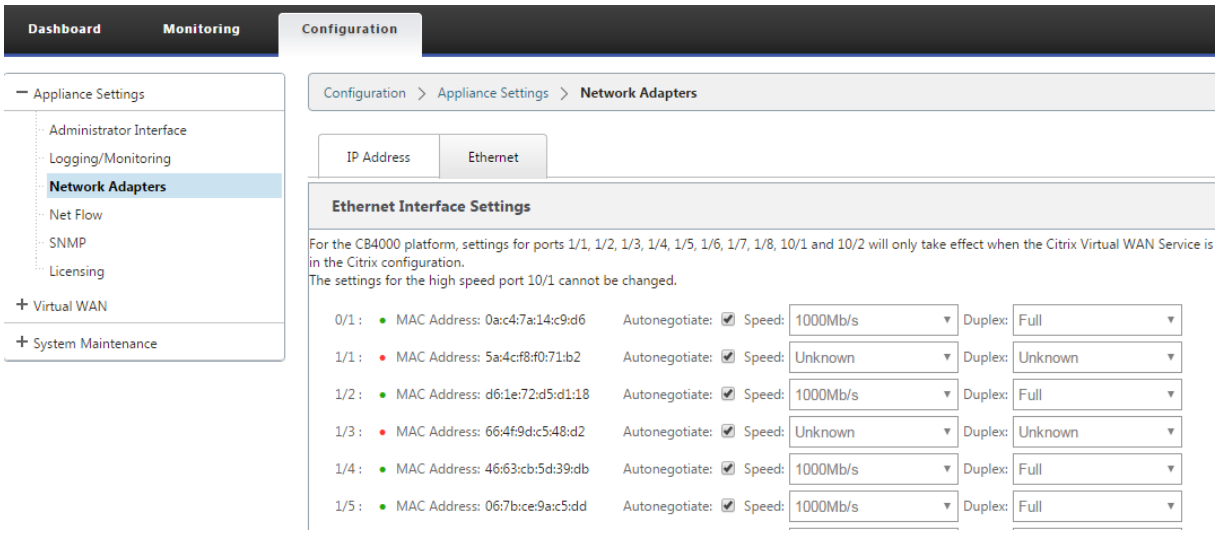
Pour surveiller la configuration de haute disponibilité :

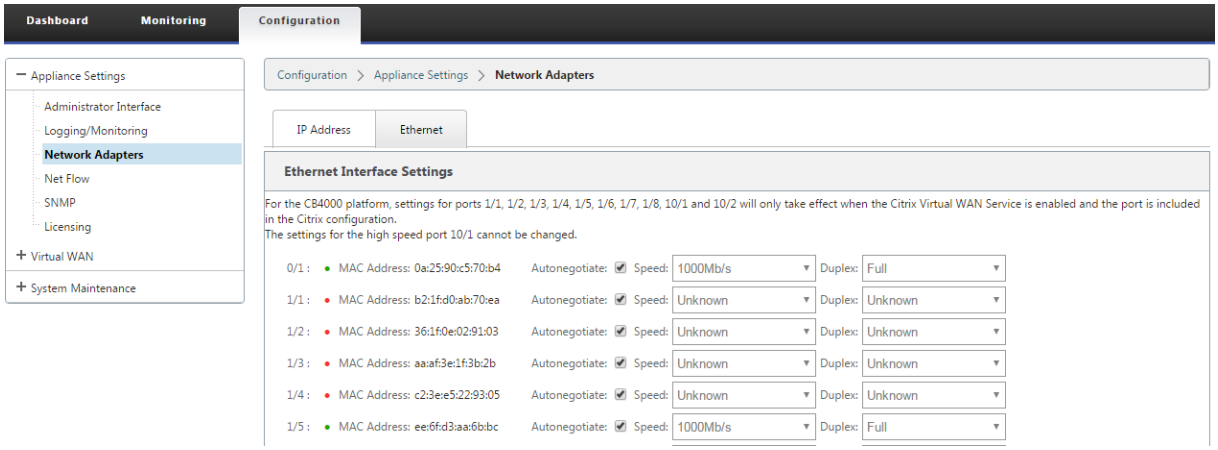
Connectez-vous à l'interface de gestion Web SD-WAN pour les appliances Active et Standby pour lesquelles la haute disponibilité est implémentée. Affichez l'état de la haute disponibilité sous l'onglet Tableau de **bord** .





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** .





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.

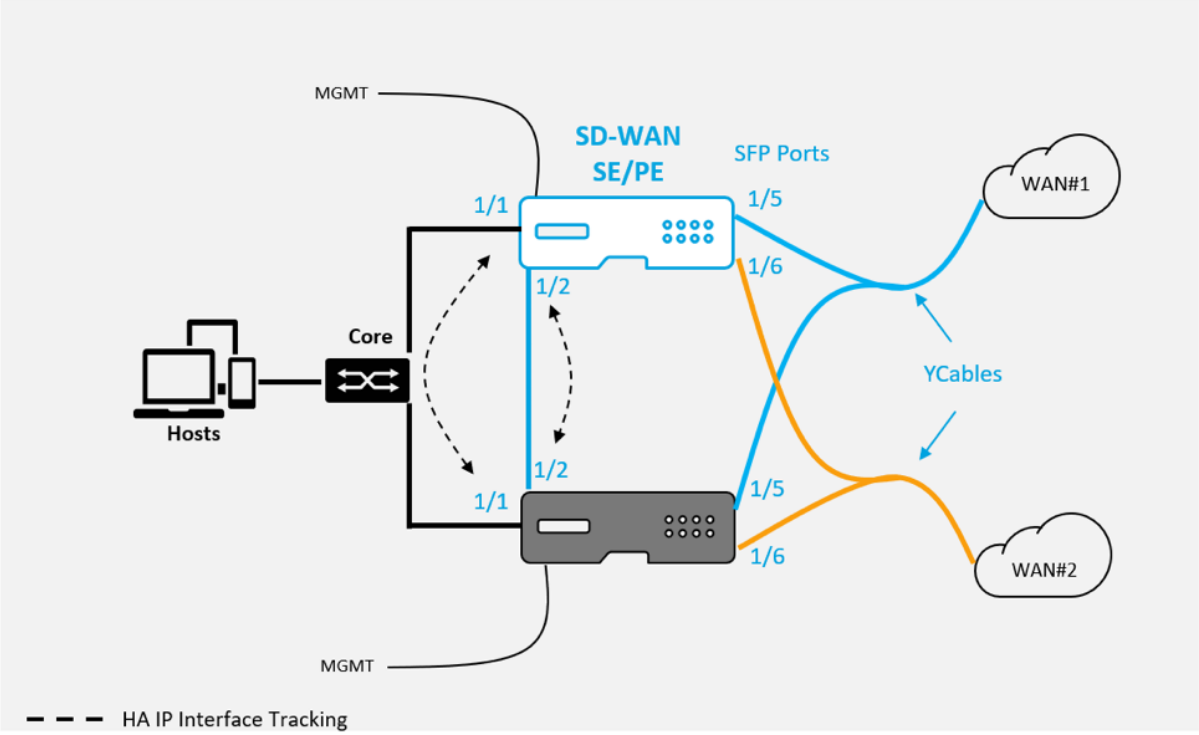
Activer la haute disponibilité en mode Edge à l'aide d'un câble Y à fibre optique

August 31, 2022

> Remarque : Dans la version 10.2 version 2, cette fonctionnalité s'applique uniquement à l'appliance 1100 SE.

La procédure suivante décrit les étapes permettant d'activer la haute disponibilité (HA) sur les appliances 1100 SE déployées en mode Edge où les transferts des fournisseurs de services de liaison WAN se font par fibre optique.
Les ports SFP (Small Form-Factor Pluggable) disponibles sur les appliances 1100 peuvent être utilisés avec des câbles en Y à fibre optique pour activer la fonctionnalité de haute disponibilité pour le déploiement du mode Edge.
Sur l'appliance 1100 SE, l'extrémité divisée du câble répartiteur 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 déployées en paire HA. Le câble séparateur est utilisé pour diviser un signal entrant en plusieurs signaux.

Pour plus d'informations sur le déploiement HA en mode Edge basé sur le service SD-WAN Orchestrator, consultez la section Détails de l'appareil.



Limitations :

- La configuration du mode Fail-to-Wire HA utilisant le 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

August 31, 2022

> **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 1100 Édition Standard
> - SD-WAN 2100 Édition Standard
> - 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).

Les services Cloud de déploiement zéro contact communiquent en toute sécurité avec les services Citrix principaux hébergeant l'identification stockée des clients Citrix qui ont acheté des appareils compatibles Zero Touch (par exemple 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.

Pour plus d'informations, consultez la rubrique Déploiement automatique du service Citrix SD-WAN Orchestrator.

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 :

- Connexion Citrix Cloud pour lancer le service de déploiement sans intervention pour le déploiement de nouveaux nœuds de site.

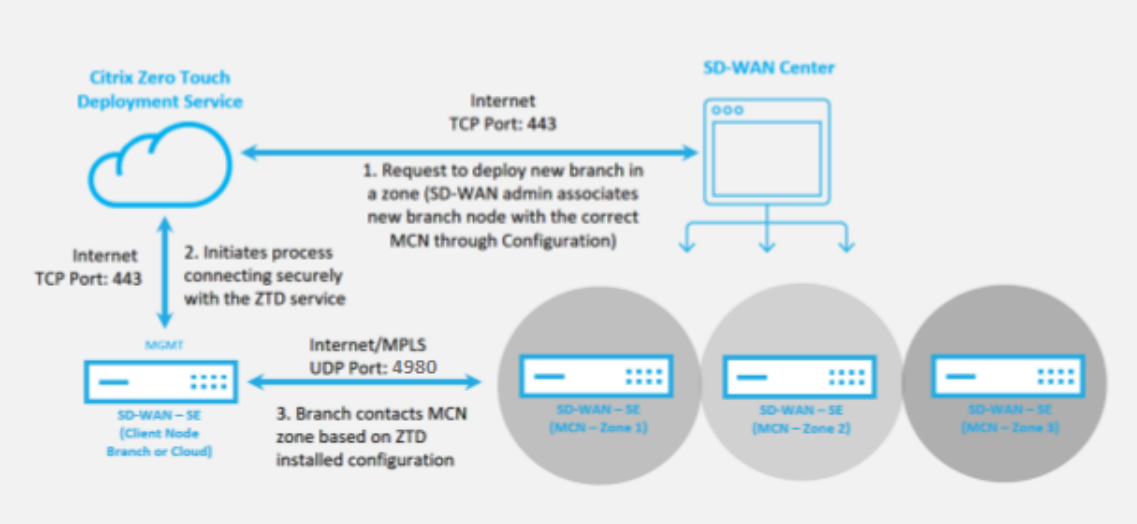
Administrateur réseau : utilisateur responsable de la gestion du réseau d'entreprise (DHCP, DNS, Internet, pare-feu, etc.).

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'appliance Citrix SD-WAN.
- Réimagez 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'appliance pour la connectivité Internet sur l'interface de gestion (par exemple, MGMT ou 0/1).
- Câblez l'appliance 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.

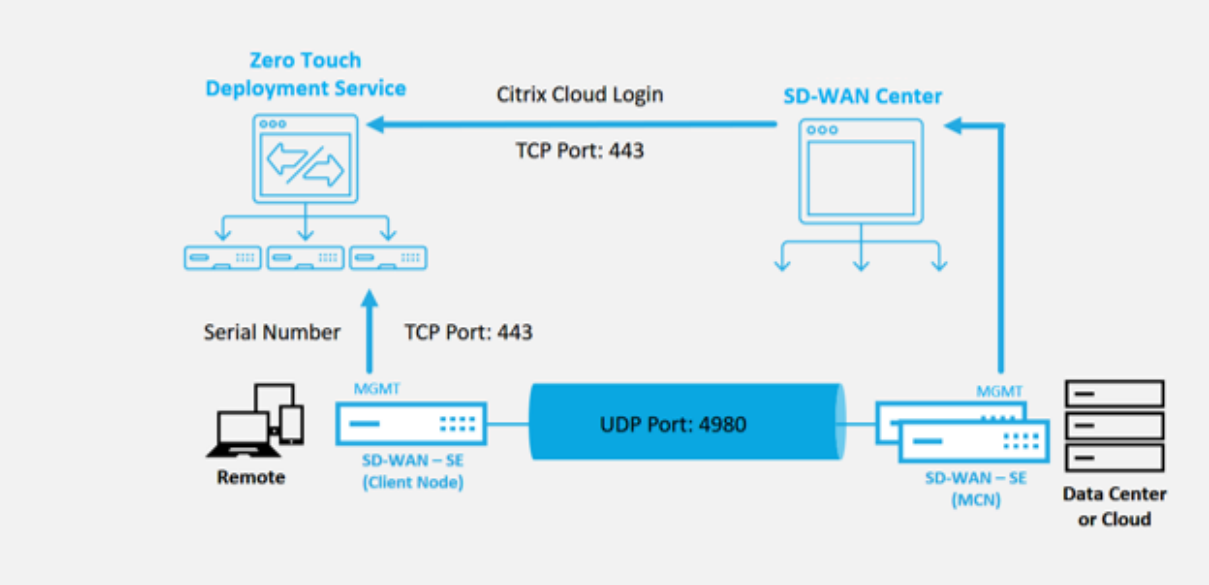


Les conditions préalables suivantes sont requises avant de démarrer un service de déploiement sans intervention :

- Exécution active du SD-WAN promu en MCN (Master Control Node).

- 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 du réseau de gestion (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 fonctionnant dans une succursale en mode client avec une connectivité Virtual Path valide au MCN pour aider à valider l'établissement réussi du chemin sur le réseau sous-jacent existant.

La dernière condition préalable n'est pas obligatoire, mais permet à l'administrateur SD-WAN de valider que le réseau sous-jacent autorise l'établissement de chemins virtuels lorsque le déploiement Zero Touch est terminé avec tout 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 :

Pour utiliser le service de déploiement Zero Touch (ou le service cloud de déploiement zéro contact), un administrateur doit commencer par déployer le premier périphérique SD-WAN dans l'environnement.

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. La connexion au service Zero Touch permet d'authentifier l'ID client associé à l'environnement SD-WAN particulier.

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 Zero Touch Deployment automatise les actions suivantes :

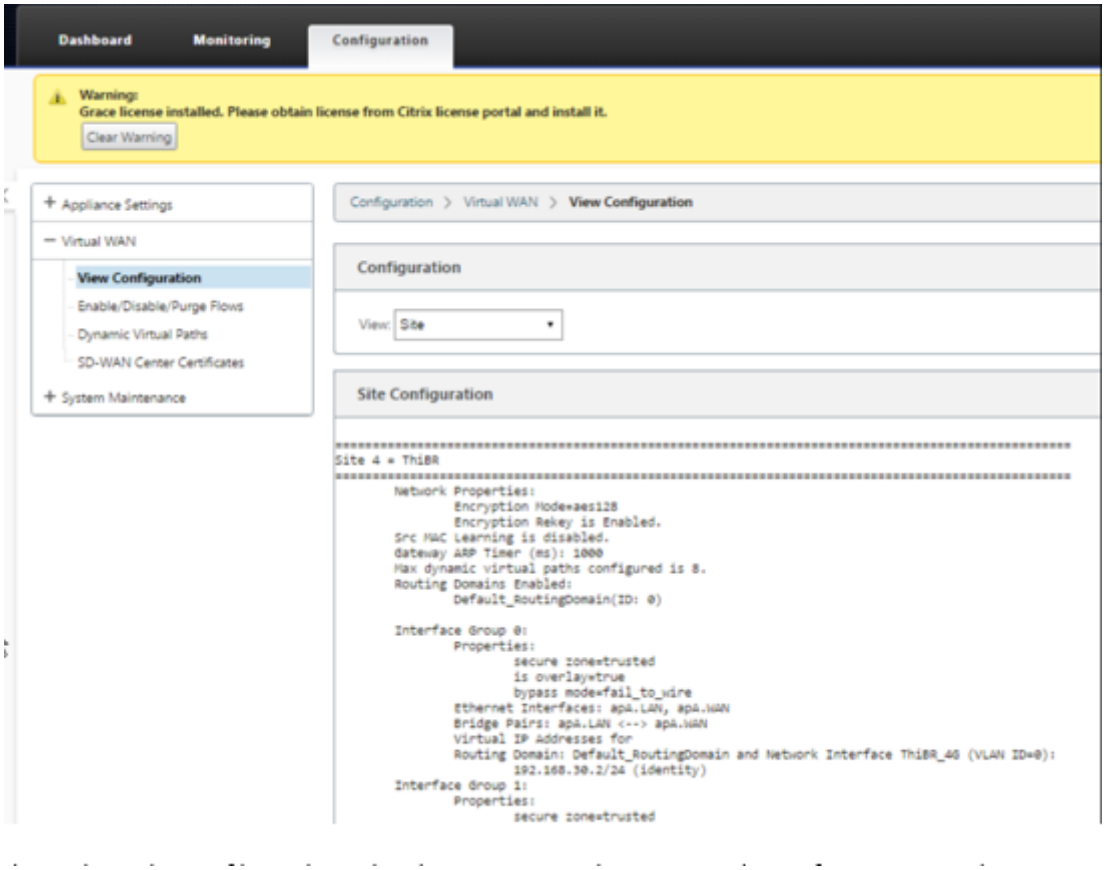
Téléchargez et mettez à jour l'agent de déploiement zéro touche si de nouvelles fonctionnalités sont disponibles sur le dispositif de succursale.

- Authentifiez l'appliance de succursale en validant le numéro de série.
- 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.

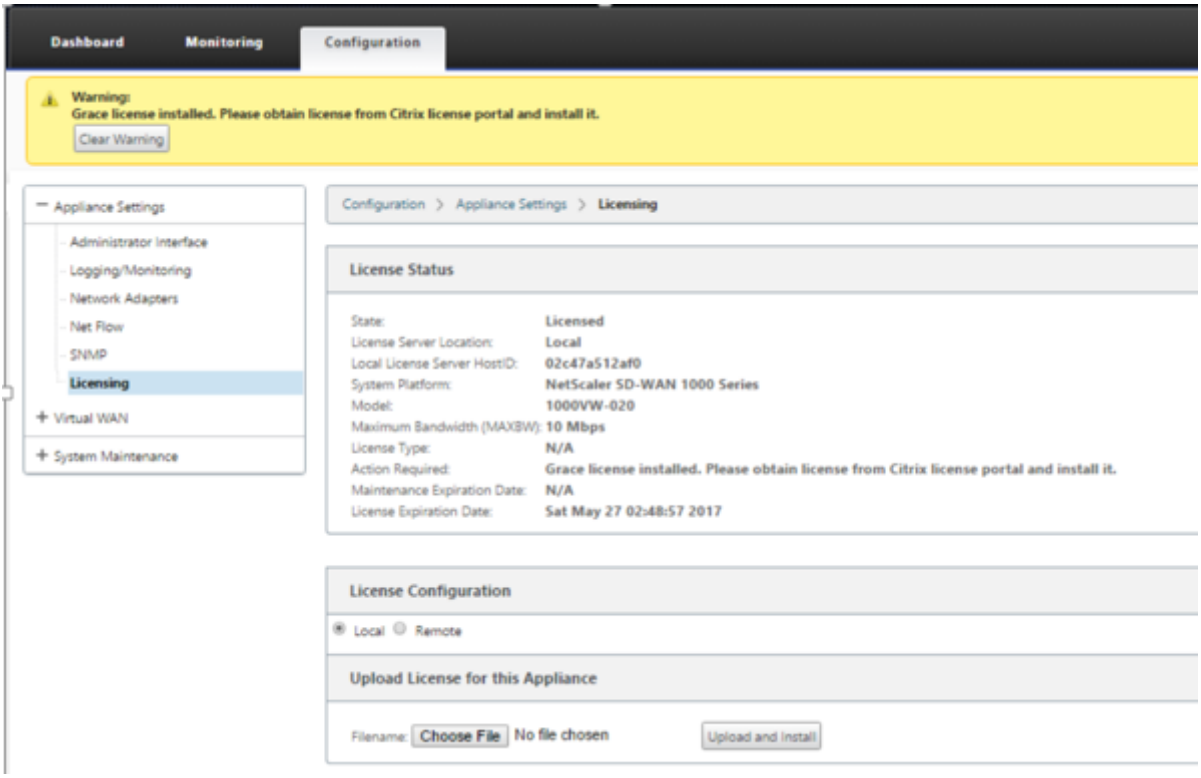
D'autres étapes sont requises pour l'administrateur SD-WAN pour installer un fichier de licence permanent sur l'appliance.

> **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.

La configuration de l'appliance peut être validée à l'aide de la page **Configuration** > **Virtual WAN** > **Afficher la configuration** .



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** .



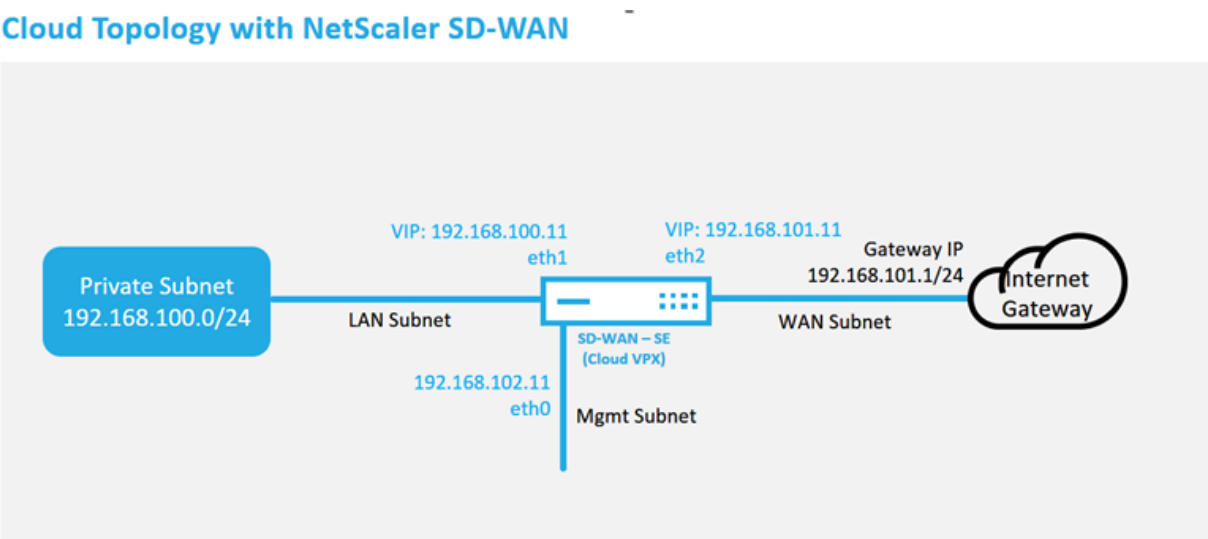
Après le téléchargement et l'installation du fichier de licence permanent, la bannière d'avertissement Grace License disparaît et aucune perte de connectivité avec le site distant ne se produira pendant le processus d'installation de la licence (aucun ping n'est supprimé).

AWS

August 31, 2022

Avec la version 11.5 du SD-WAN, le déploiement sans intervention dans un environnement AWS est pris en charge via le service SD-WAN Orchestrator.

> **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 définis pour obtenir l'adresse IP #.#.#.#.11 des sous-réseaux disponibles dans le VPC.



Il s'agit d'un exemple de déploiement d'un site déployé dans le cloud SD-WAN, le périphérique Citrix SD-WAN est déployé en tant que périphérique périphérique périphérique desservant une seule liaison WAN Internet dans ce réseau cloud. Les sites distants seront en mesure d'exploiter plusieurs liaisons WAN Internet distinctes se connectant à cette même passerelle Internet pour le cloud, offrant ainsi une résilience et une connectivité de bande passante agrégée depuis n'importe quel site de déploiement SD-WAN vers l'infrastructure cloud. Cela fournit une connectivité rentable et hautement fiable au cloud.

Azure

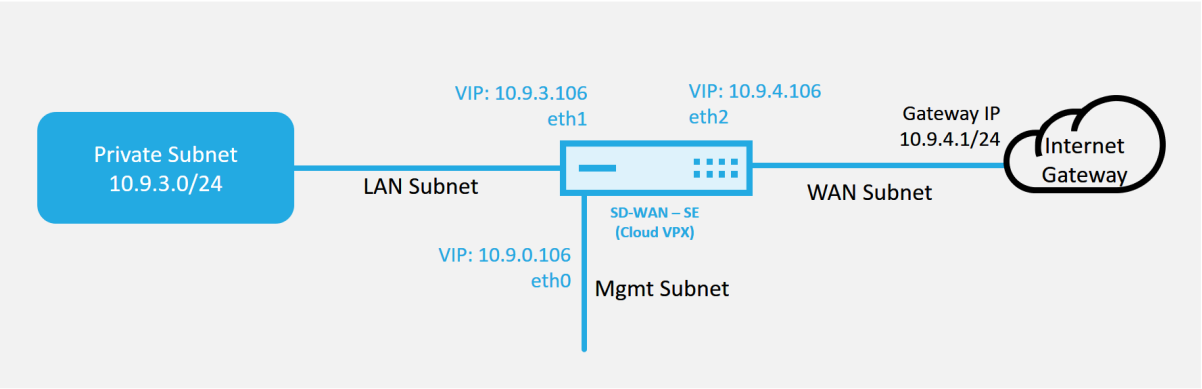
August 31, 2022

Avec la version 11.5 du SD-WAN, le déploiement sans intervention dans un environnement Azure est pris en charge via le service SD-WAN Orchestrator.

> **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 mise en page.

- Le nom du site Azure dans la configuration doit être en minuscules et sans caractères spéciaux (par exemple ztdazure).

Azure Cloud Topology with NetScaler SD-WAN



Il s'agit d'un exemple de déploiement d'un site déployé dans le cloud SD-WAN, l'appareil Citrix SD-WAN est déployé en tant que périphérique desservant une seule liaison WAN Internet dans ce réseau cloud. Les sites distants seront en mesure d'exploiter plusieurs liaisons WAN Internet distinctes se connectant à cette même passerelle Internet pour le cloud, offrant ainsi une résilience et une connectivité de bande passante agrégée depuis n'importe quel site de déploiement SD-WAN vers l'infrastructure cloud. Cela fournit une connectivité rentable et hautement fiable au cloud.

Déploiement sur une région

August 31, 2022

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.

Pour plus d'informations sur le déploiement d'une région unique via le service Citrix SD-WAN Orchestrator, consultez Régions.

Déploiement multi-régions

August 31, 2022

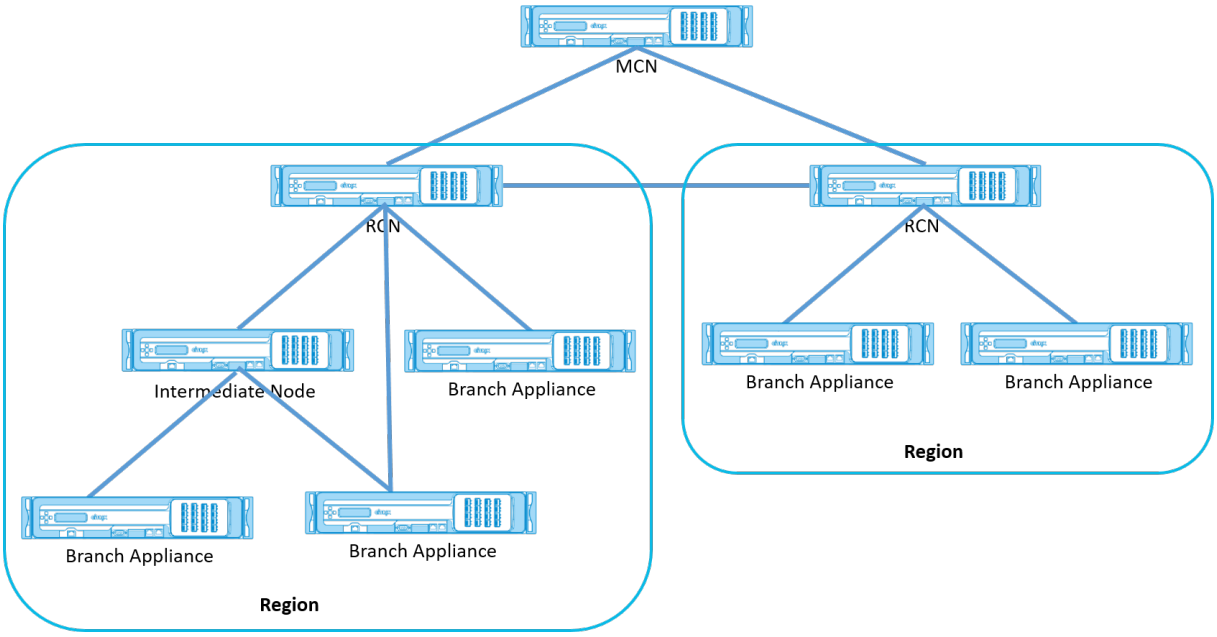
Une appliance SD-WAN configurée en tant que nœud de contrôle principal (MCN) prend en charge le déploiement multi-régions. Le MCN gère plusieurs nœuds de contrôle régionaux (RCN). Chaque RCN, à son tour, gère plusieurs sites clients. Le MCN peut également être utilisé pour gérer directement certains 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.

Pour plus d'informations sur le déploiement multi-régions via le service Citrix SD-WAN Orchestrator, consultez Régions.



Le tableau suivant fournit la liste des plates-formes prises en charge pour la configuration MCN/RCN principale et secondaire.

> **REMARQUE**
>
> 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
1100-SE	Oui	Oui
VPX-SE, VPXL-SE	Oui	Oui
2100-SE, 4100-SE, 5100-SE, 6100-SE	Oui	Oui

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, consultez le 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 multiflux monoport)
  - QoS entre HDX et d'autres trafics
  - HDX QoS Équité entre les utilisateurs

  - QoS de bout en bout

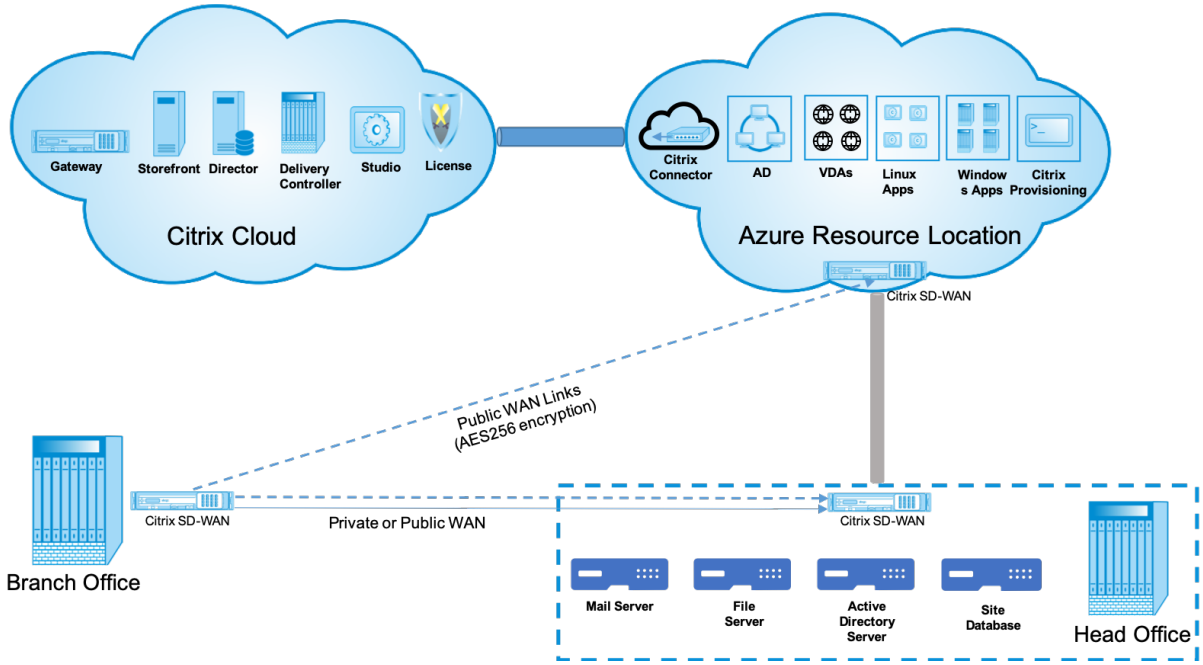
- Le collage de liaison offre plus de bande passante pour des performances plus rapides
- Haute disponibilité avec basculement de lien transparent et redondance SD-WAN sur Azure
- Expérience VoIP optimisée (course de paquets pour une gigue réduite et une perte minimale de paquets, QoS, break-out local 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 multiflux 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 :

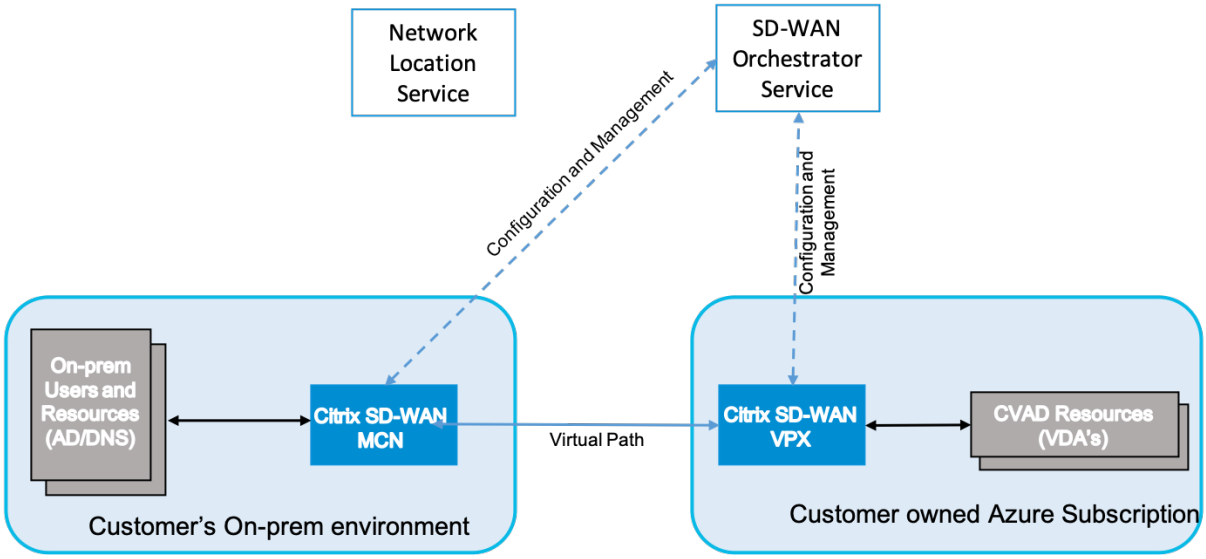
- Emplacement local hébergeant l'appliance SD-WAN qui peut être déployé en mode succursale ou en tant que MCN (Master Control Node). Le mode branche ou MCN contient les machines clientes, Active Directory et DNS. Toutefois, vous pouvez également choisir d'utiliser le DNS et AD d'Azure. Dans la plupart 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 emplace-

ments 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'appliance 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'appliance virtuelle Citrix SD-WAN et les VDA. Les appliances SD-WAN sont gérées via SD-WAN Orchestrator. Une fois que l'appliance SD-

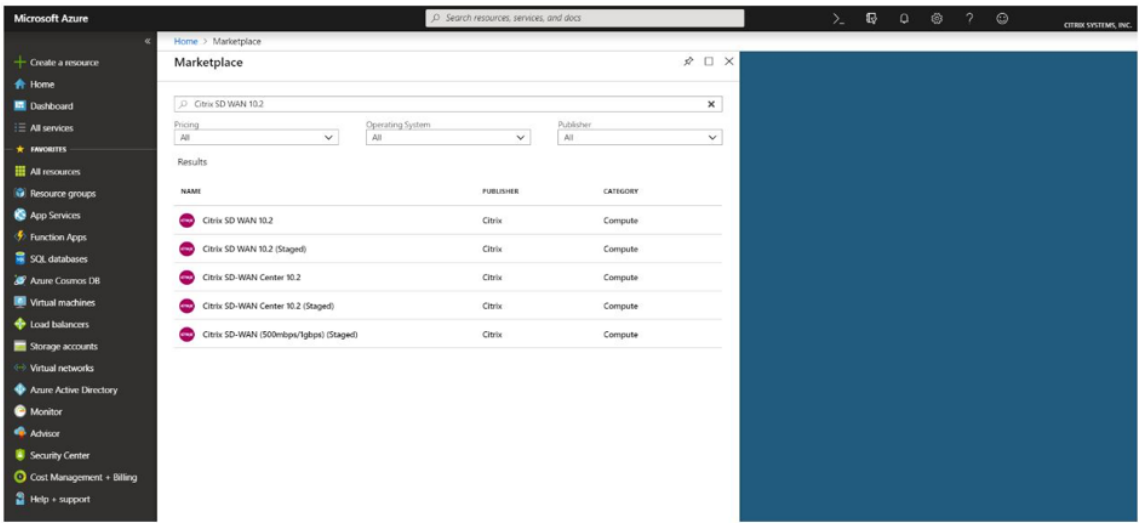
WAN est configurée, elle se connecte au réseau Citrix SD-WAN existant et d'autres tâches telles que la configuration, la visibilité et la gestion sont gérées via SD-WAN Orchestrator.

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, consultez 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. Dans un navigateur Web, accédez au 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.



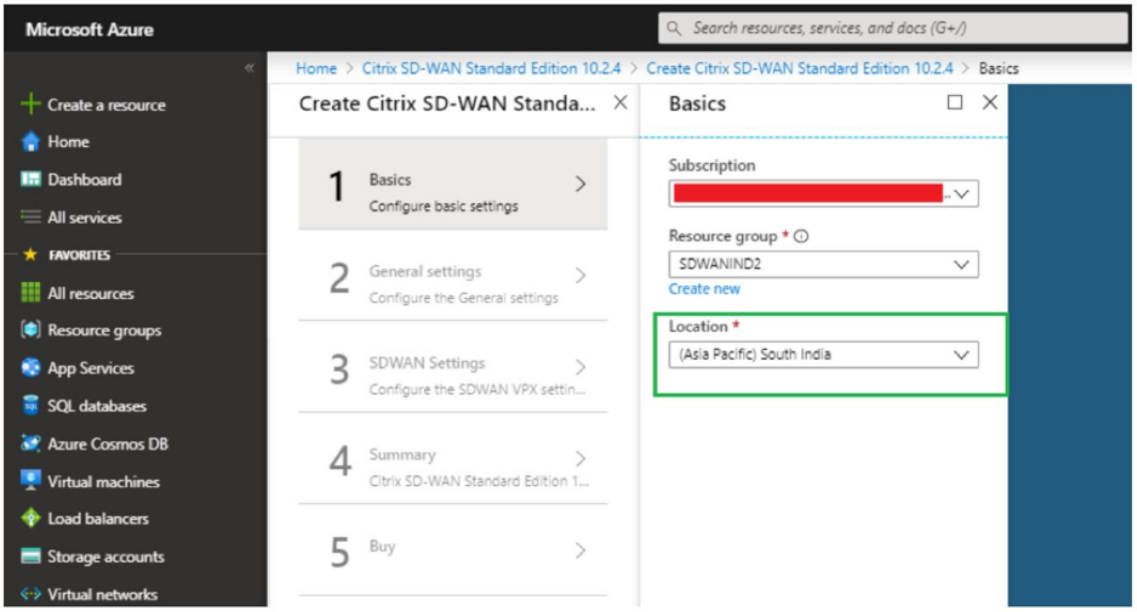
   En cliquant sur **Créer**, un assistant vous invite avec les détails nécessaires pour créer la machine virtuelle.

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 unique-

ment 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.

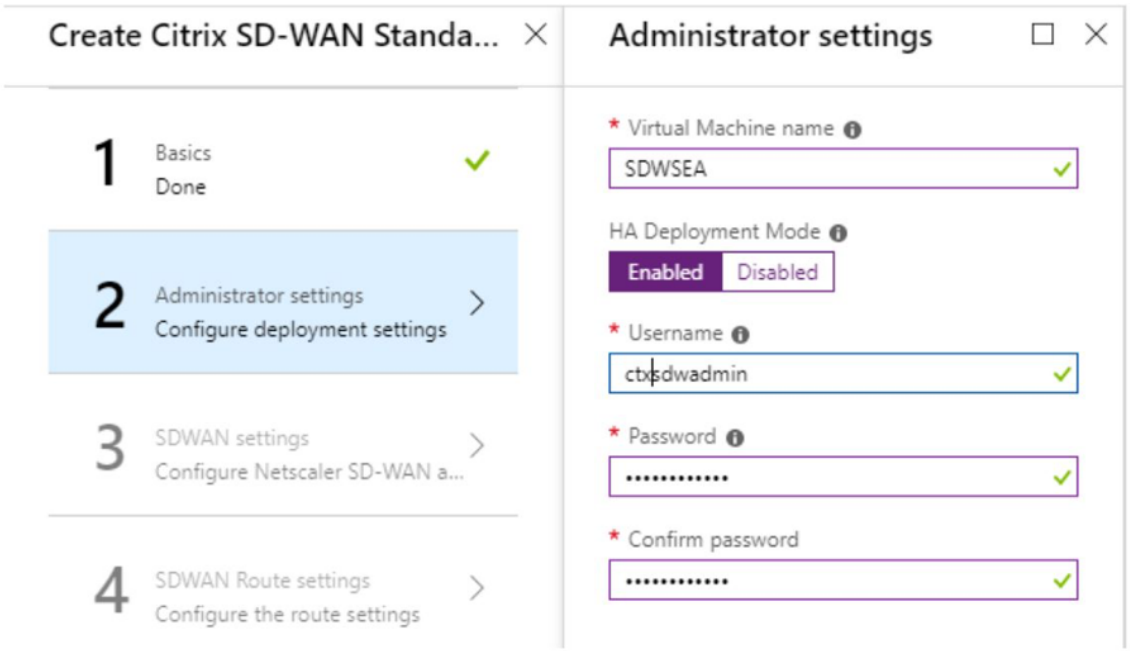
Pour Citrix SD-WAN, il est recommandé que le groupe de ressources que vous choisissez soit vide. De même, sélectionnez la région Azure dans laquelle vous souhaitez déployer l'instance SD-WAN. La région doit être identique à la région dans laquelle vos ressources Citrix Virtual Apps and Desktops sont 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**.

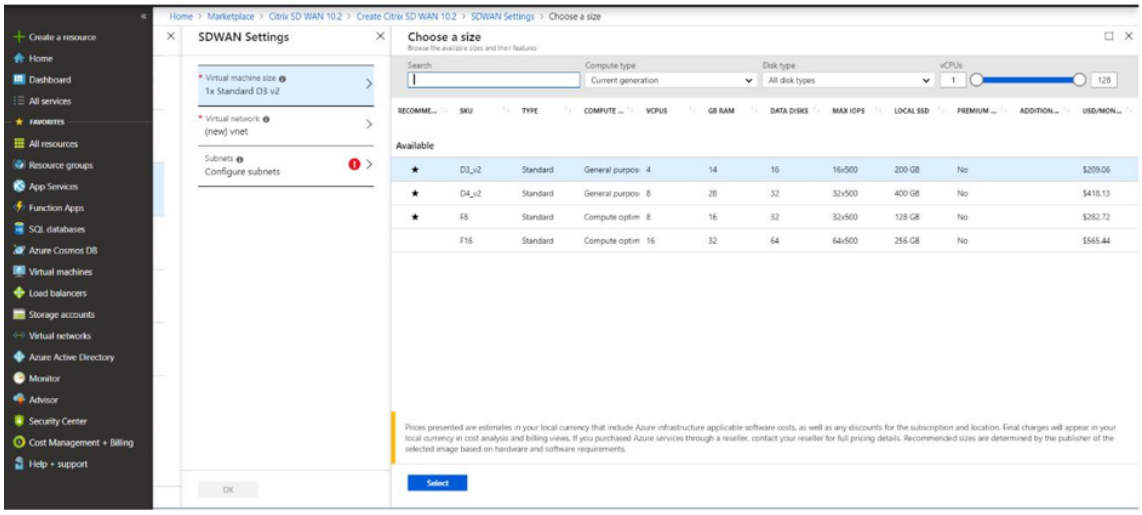
   Ce mot de passe est nécessaire pour vous connecter à l'interface de gestion de l'instance en tant qu'utilisateur invité. Pour obtenir l'accès administrateur à l'instance, utilisez admin comme nom d'utilisateur et le mot de passe créé lors du Provisioning de l'instance. Si vous utilisez le nom d'utilisateur 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.



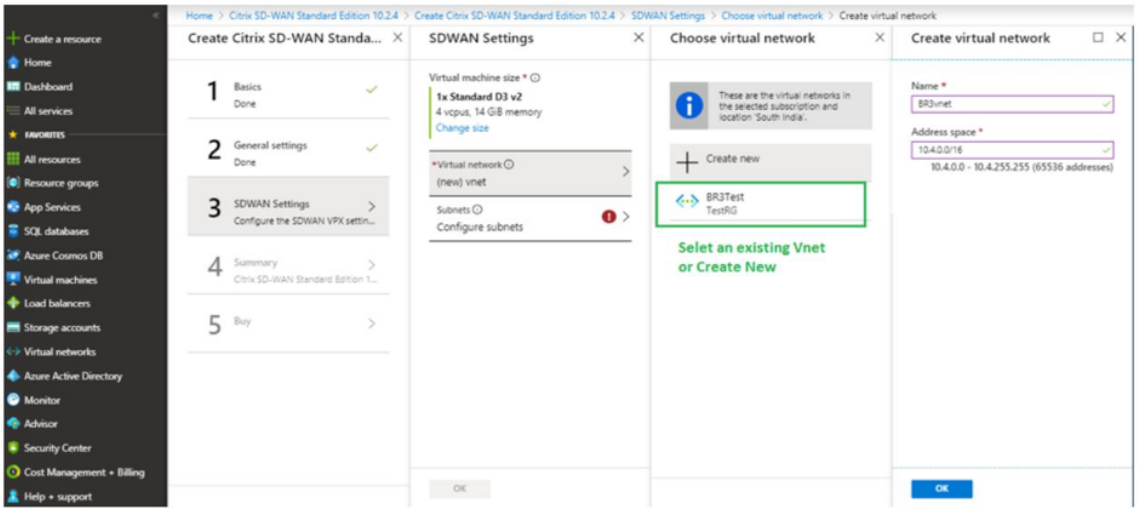
5. Sous la page **Paramètres du SD-WAN**, choisissez l'instance dans laquelle vous souhaitez exécuter l'image. Choisissez le type d'instance suivant selon vos besoins :

   - 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.

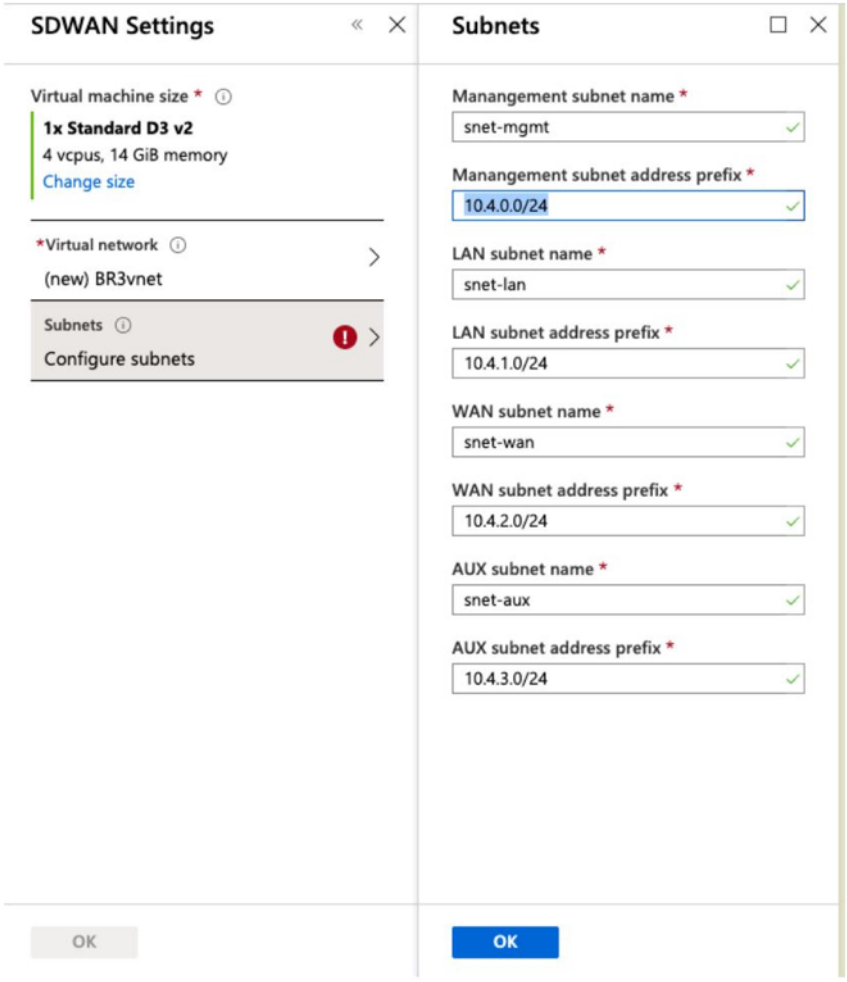


6. Créez un nouveau réseau virtuel (VNet) ou utilisez un réseau virtuel existant. Il s'agit de l'étape

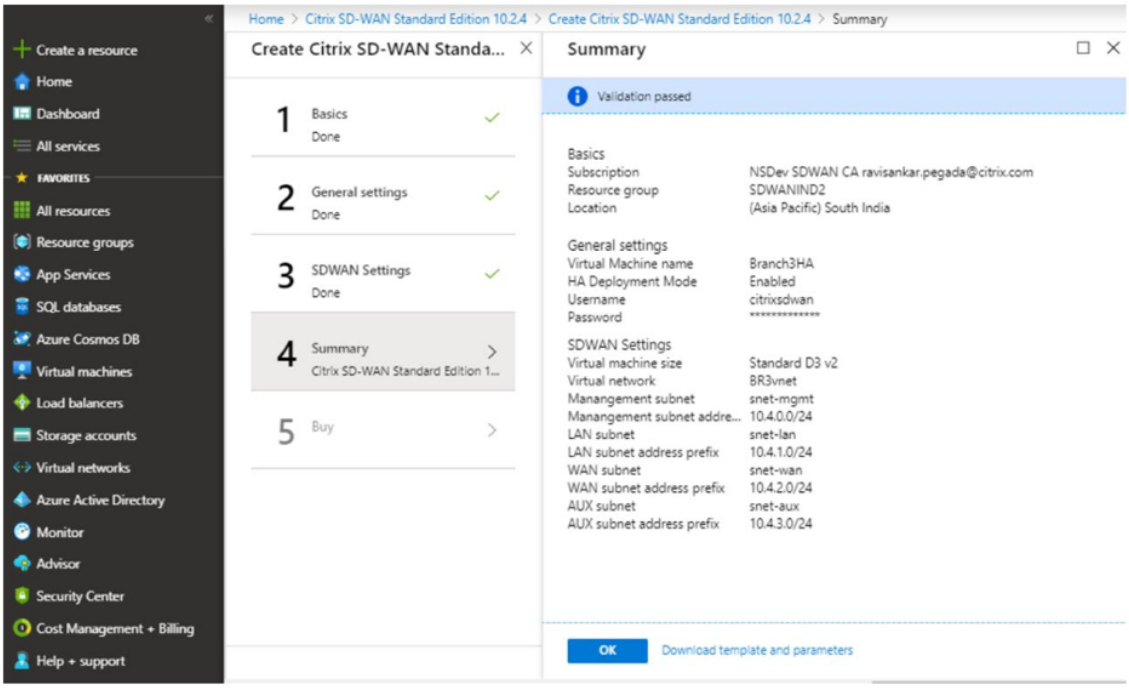
la plus critique pour le déploiement, car cette étape choisit les sous-réseaux à affecter aux interfaces de la machine virtuelle SD-WAN VPX.



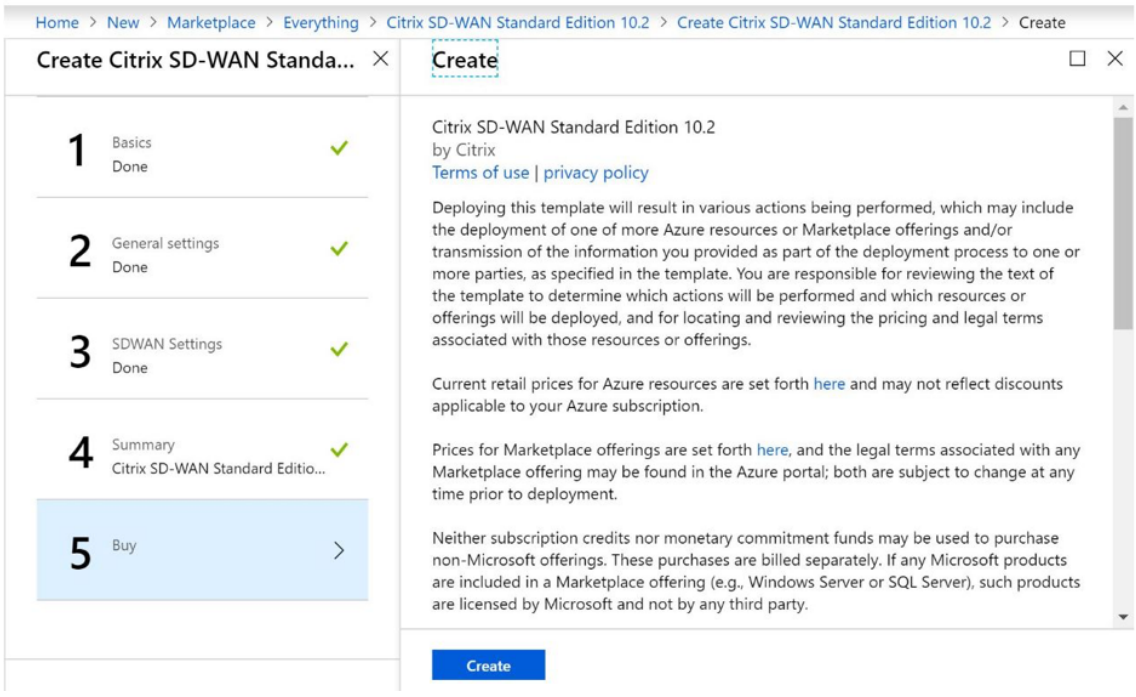
Le sous-réseau auxiliaire n'est nécessaire que lorsque vous déployez les instances en mode HA. Assurez-vous que l'instance SD-WAN est déployée sur le même réseau virtuel que vos ressources Citrix Virtual Apps and Desktops et qu'elle se trouve sur le même sous-réseau que l'interface LAN de l'appliance VPX SD-WAN.



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.

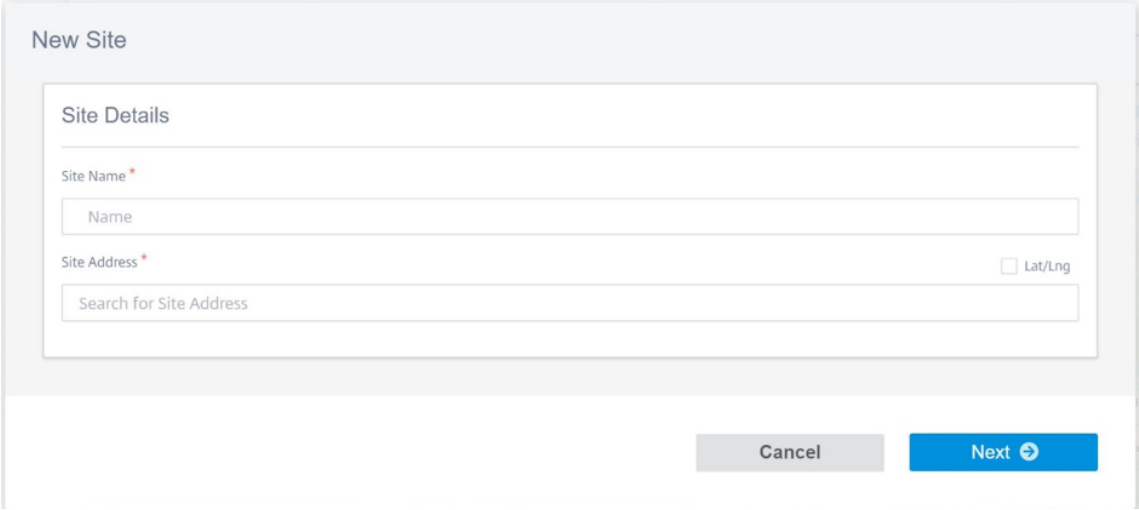


Une fois l'instance créée avec succès, récupère l'adresse IP publique attribuée à l'interface de gestion de l'instance SD-WAN. Elle se trouve dans la section Mise en réseau du groupe de

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, reportez-vous à la section 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, consultez 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).

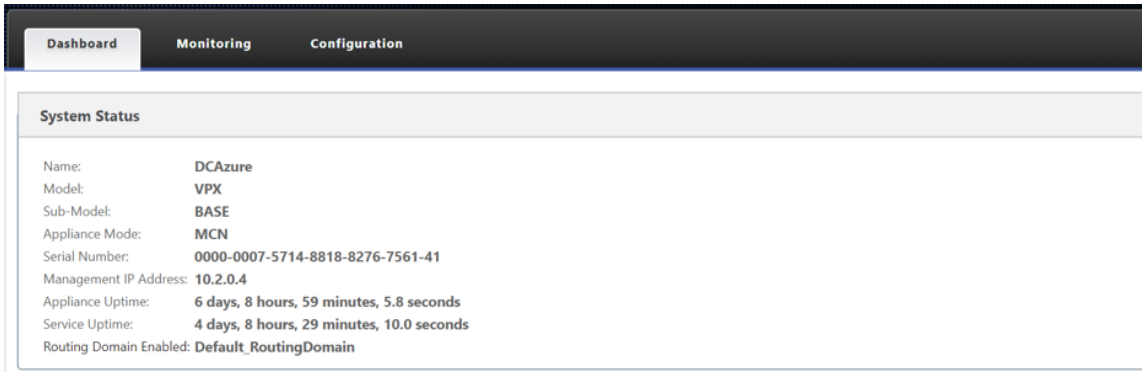


12. Indiquez un nom de site unique et entrez l'adresse en fonction de la région dans laquelle vous provisionnez l'image. Pour configurer l'instance dans Azure, reportez-vous à la section Paramètres de base.

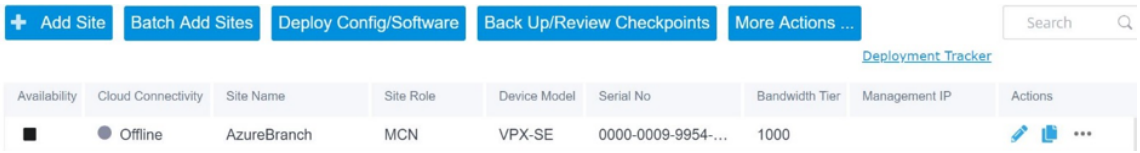
> **Remarque**
>
> Pour récupérer le numéro de série de l'instance dans Azure, connectez-vous à l'instance via l'IP de gestion publique. Vous pouvez voir le numéro de série sur l'écran du tableau de bord. Si vous configurez des instances dans HA, les deux numéros de série doivent être

> 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**.

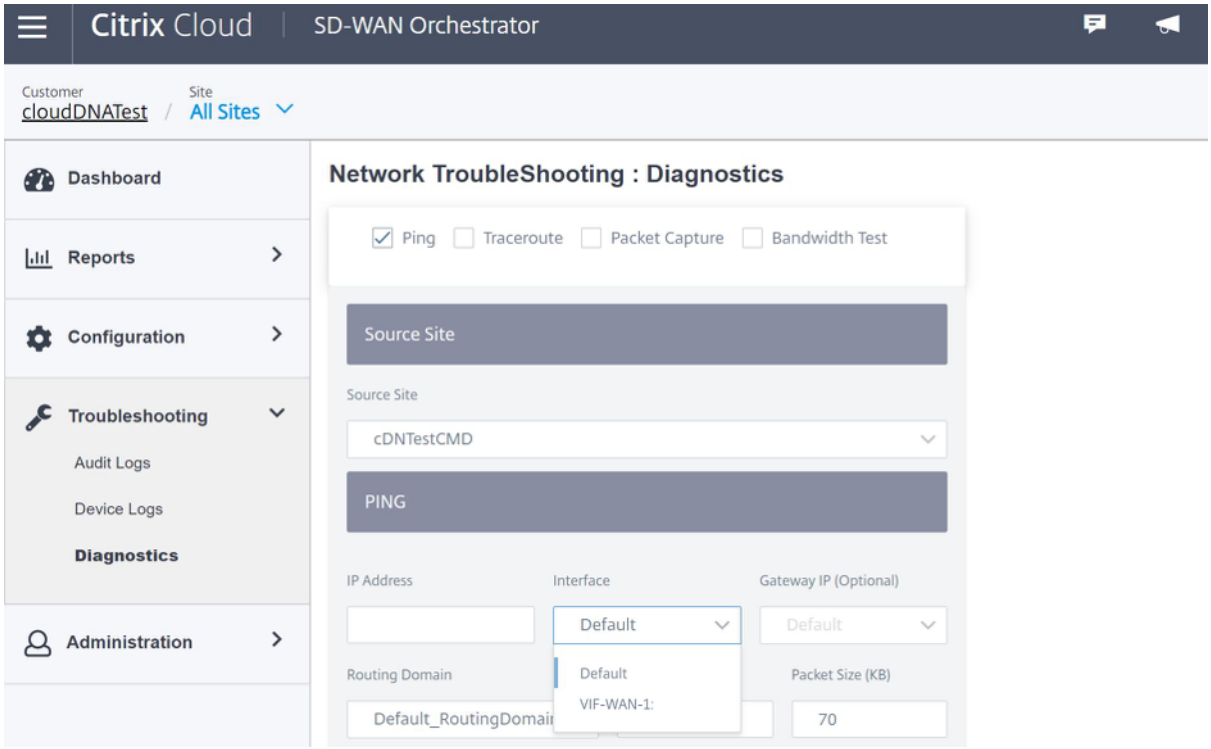


15. S'il n'y a aucun problème et que la configuration est précise, vous devez disposer des chemins virtuels entre l'instance dans Azure et votre MCN une fois le déploiement de configuration exécuté.

Configuration Citrix Virtual Apps and Desktops

Comme indiqué dans la section Déploiement et configuration, l'AD/DNS est présent dans l'emplacement local agissant en tant que contrôleur de domaine et dans un déploiement doté du SD-WAN, il se 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.



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 de **localisation réseau** permet aux utilisateurs internes de contourner la passerelle et de se connecter directement aux VDA, ce qui réduit 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 obtenir des informations détaillées sur la configuration de NLS à l'aide de Citrix SD-WAN Orchestrator, consultez Service de localisation réseau.
- **Module PowerShell du service de localisation réseau fourni par Citrix** : pour obtenir des informations détaillées sur la configuration de NLS à l'aide du module PowerShell, consultez 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

August 31, 2022

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 via le service Citrix SD-WAN Orchestrator 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 plus d'informations sur la configuration du proxy DNS via le service SD-WAN Orchestrator, consultez Proxy DNS.

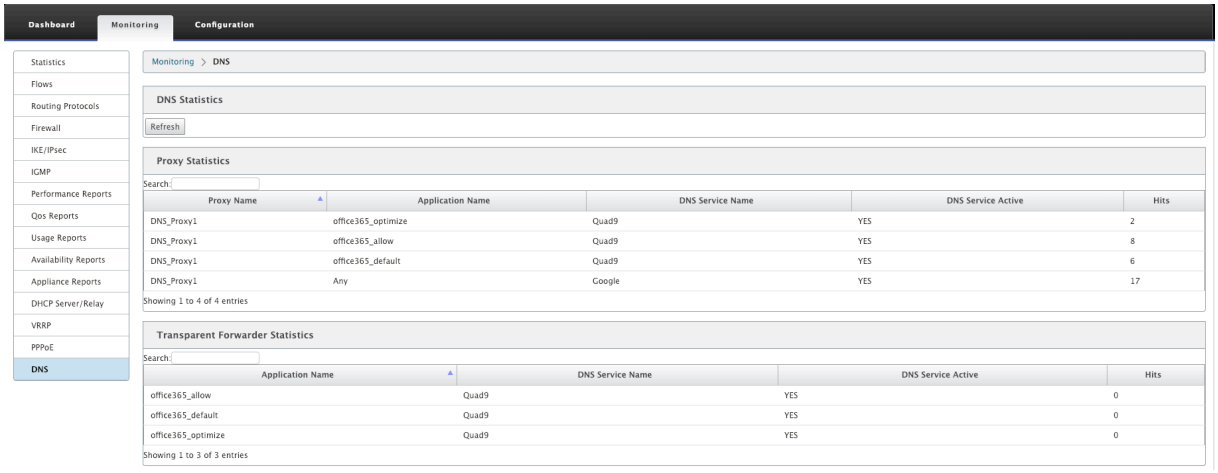
Redirecteur DNS transparent

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 plus d'informations sur la configuration du redirecteur transparent DNS via le service SD-WAN Orchestrator, consultez la section Redirecteurs transparents DNS.

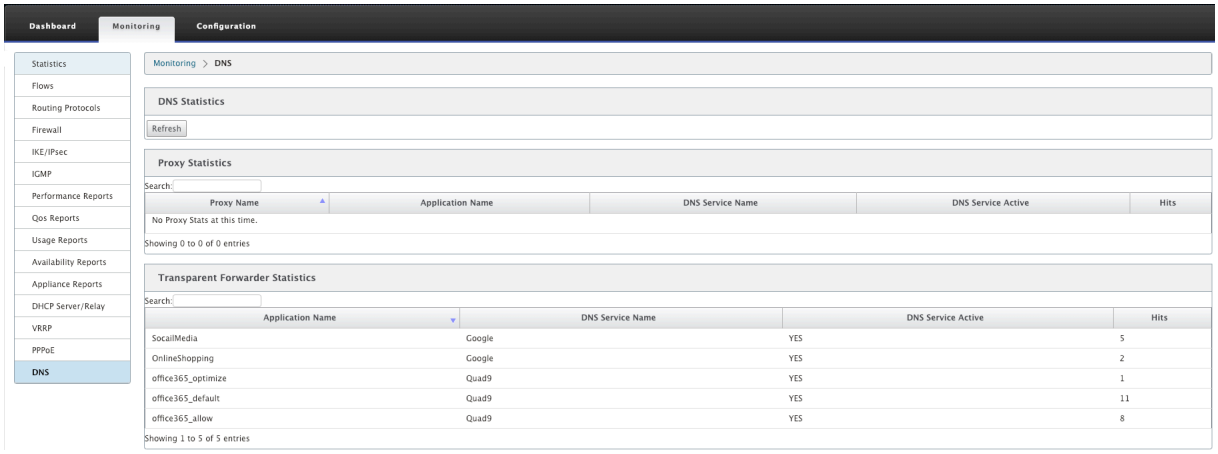
Surveillance

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



Statistiques sur les redirecteurs transparents



DHCP

November 16, 2022

Citrix SD-WAN permet d'utiliser des appliances Standard 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.

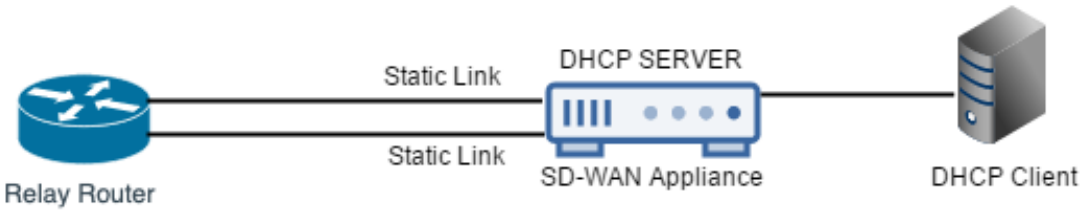
Voici les avantages de l'utilisation du serveur DHCP et des fonctions de relais DHCP :

- 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.

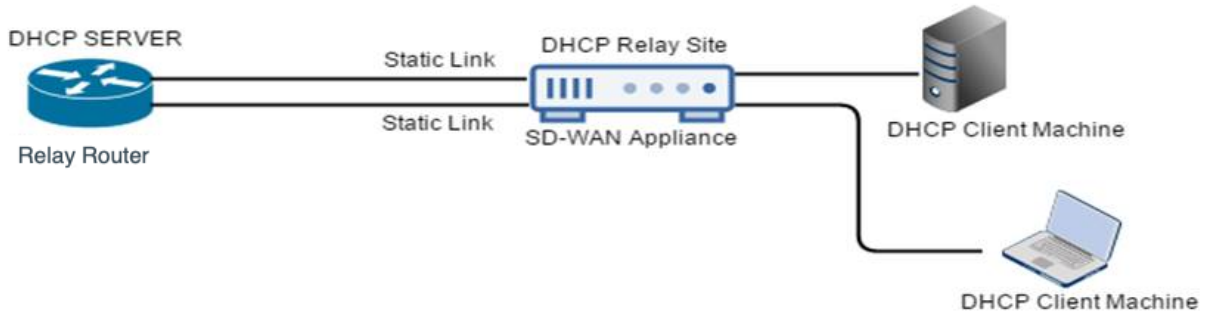
Serveur DHCP

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'acquérir 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.



Apprentissage des adresses IP de liaison WAN via le client DHCP

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.

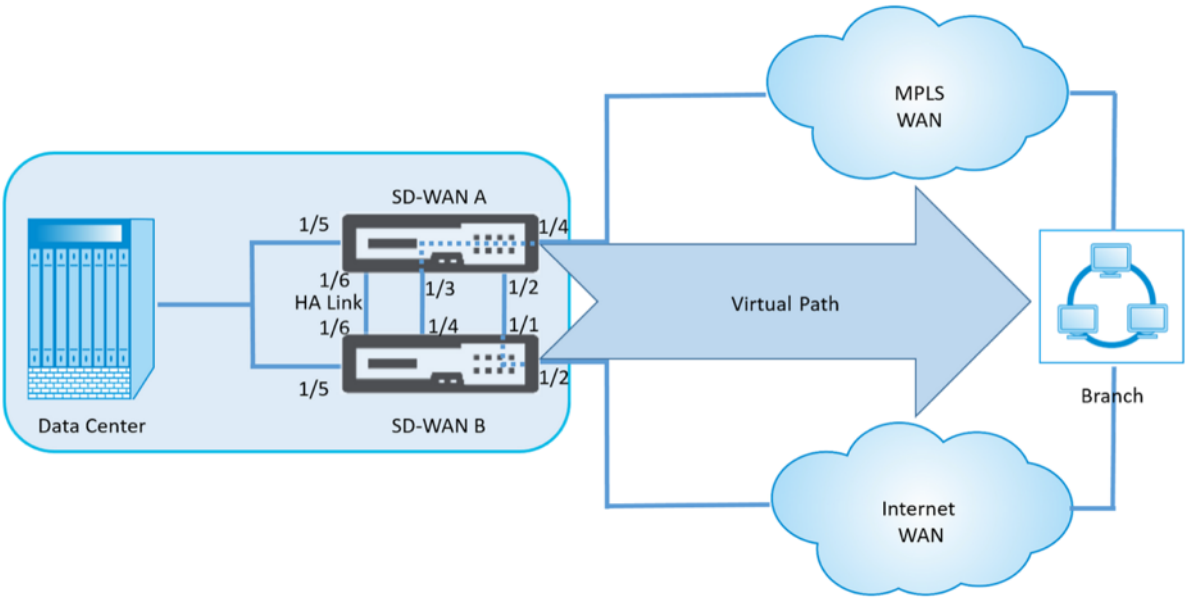
À partir de la version 11.5 de Citrix SD-WAN, vous pouvez configurer DHCP pour une interface virtuelle non approuvée en mode fail-to-block via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez Apprentissage des adresses IP de liaison WAN via le client DHCP.

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 d'un intranet privé**.

Le client DHCP est désormais pris en charge sur le lien intranet privé.



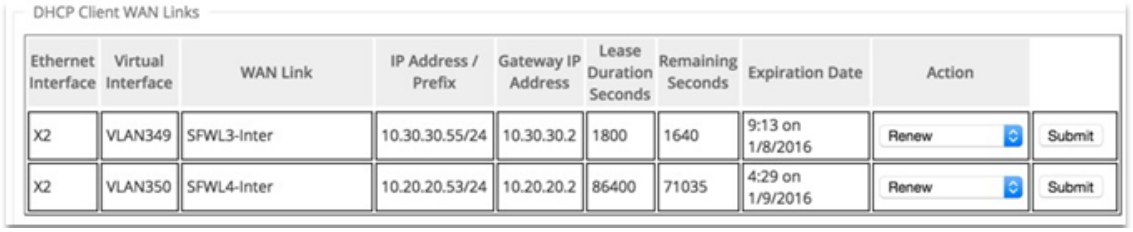
> **Remarque** :
>
> aucune interface LAN ne doit être connectée à la paire fail-to-wire car des paquets peuvent être pontés entre les interfaces.

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.

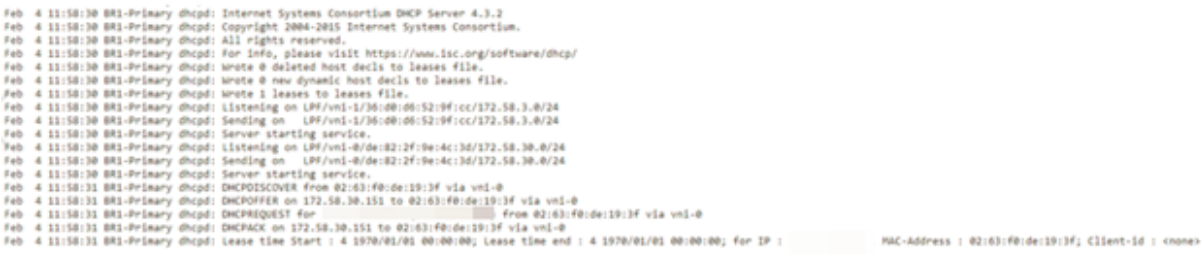

DHCP Client WAN Links

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**.



> **Remarque**
>
> Ces journaux sont générés uniquement lorsque Citrix SD-WAN agit en tant que serveur DHCP.

Personnalisation dynamique des fichiers PAC

August 31, 2022

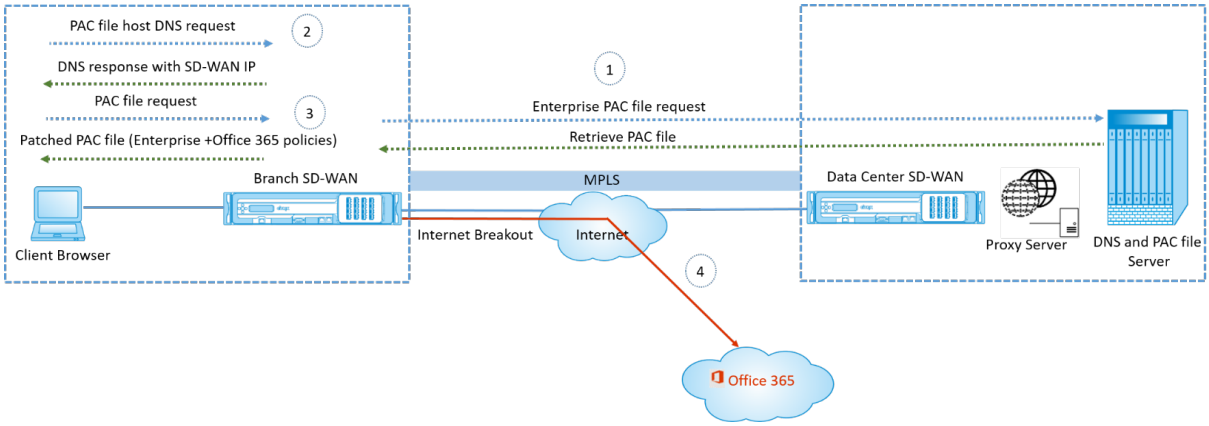
Avec l'adoption croissante d'applications SaaS stratégiques et d'une main-d'œuvre répartie, il devient essentiel de réduire la latence et la congestion. La latence et la congestion sont inhérentes aux méthodes traditionnelles de raccordement du trafic via le centre de données. Citrix SD-WAN permet de router le trafic Internet via le réseau local pour des applications SaaS telles qu'Office 365. Pour plus d'informations, consultez la section Optimisation d'Office 365.

Si des proxys Web explicites sont configurés sur le déploiement d'entreprise, tout le trafic est dirigé vers le proxy Web, ce qui rend difficile la classification et l'accès direct à Internet. La solution consiste à exclure le trafic d'applications 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 du 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 du serveur Web d'entreprise. L'appliance Citrix SD-WAN sert les fichiers PAC personnalisés pour les sites où la panne 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 corrige les URL Office 365 vers le fichier PAC d'entreprise. Le fichier PAC d'entreprise devrait avoir un espace réservé (balise spécifique au SD-WAN) dans lequel les URL Office 365 sont corrigées de façon transparente.
2. Le navigateur client déclenche une requête DNS pour l'hôte de fichier PAC d'entreprise. Citrix SD-WAN intercepte la demande pour le fichier de configuration du proxy FQDN et répond avec le VIP Citrix SD-WAN.
3. Le navigateur client demande le fichier PAC. L'appliance Citrix SD-WAN sert le fichier PAC corrigé localement. Le fichier PAC inclut la configuration du proxy d'entreprise et les stratégies d'exclusion d'URL Office 365.
4. À la réception d'une demande pour l'application Office 365, l'appliance Citrix SD-WAN effectue une panne Internet directe.

Conditions préalables

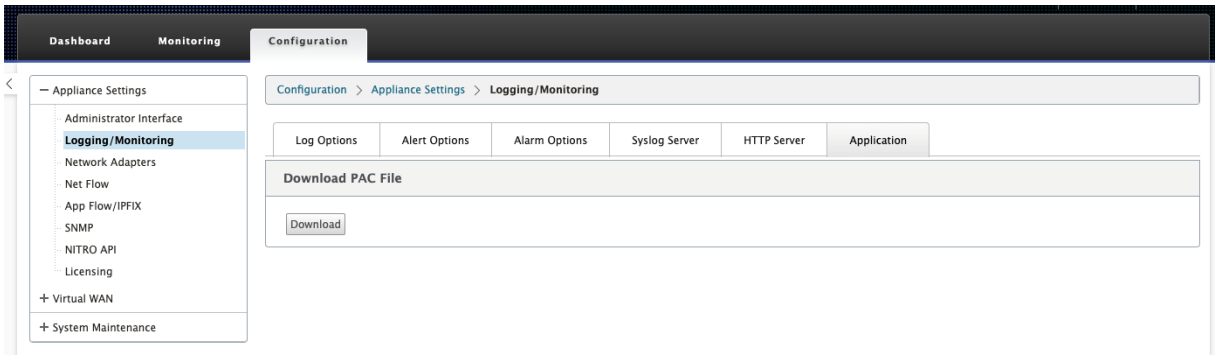
1. Les entreprises devraient avoir un fichier PAC hébergé.
2. Le fichier PAC doit comporter un espace réservé *SDWAN_TAG* ou une occurrence de la fonction *findproxyforurl* pour appliquer des correctifs aux URL Office 365.
3. L'URL du fichier PAC doit être basée sur le domaine et non sur l'IP.
4. Le fichier PAC est servi uniquement sur les VIP d'identité approuvés.
5. L'appliance Citrix SD-WAN doit pouvoir télécharger le fichier PAC d'entreprise sur son interface de gestion.

Configurer la personnalisation des fichiers PAC

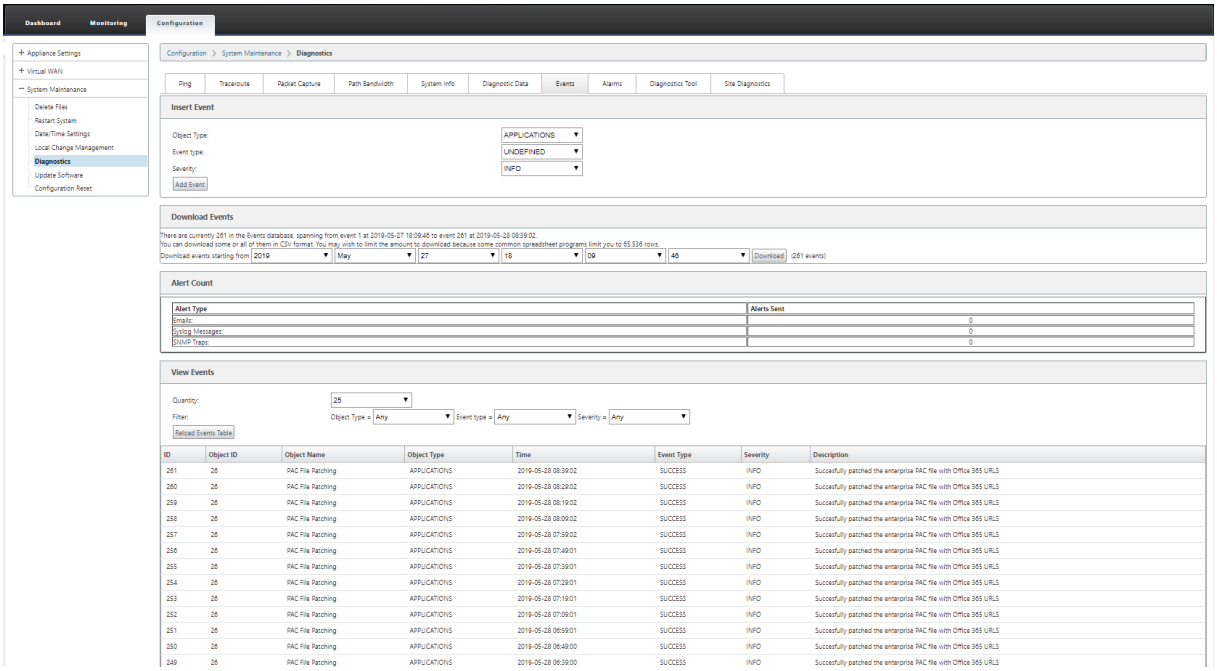
Vous pouvez activer la personnalisation des fichiers PAC à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Configuration automatique du proxy.

Résolution des problèmes

Vous pouvez télécharger le fichier PAC personnalisé à partir de l'appliance Citrix SD-WAN pour le dépannage. Accédez à **Configuration** > **Paramètres du matériel** > **Journalisation/surveillance** > **Application, puis cliquez sur Télécharger**.



Vous pouvez également afficher l'état de l'application des correctifs du fichier PAC dans la section **Événements**, accéder à **Configuration** > **Maintenance du système** > **Diagnostics**, puis cliquez sur l'onglet **Événements** .



Limitations

- Les requêtes du serveur de fichiers PAC HTTPS 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

August 31, 2022

La fonctionnalité de tunnel GRE vous permet de configurer les appliances Citrix SD-WAN pour mettre fin aux tunnels GRE sur le réseau local ou l'intranet.Pour configurer un tunnel GRE à l'aide du service SD-WAN Orchestrator, reportez-vous à la section Service GRE.

Gestion entrante et des sauvegardes

August 31, 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 intrabande pour établir la connectivité au service Citrix SD-WAN Orchestrator via un port de gestion intrabande. 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**
>
> - 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.

À partir de Citrix SD-WAN 11.5, vous pouvez activer la gestion intrabande sur une adresse IP virtuelle uniquement via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Gestion intrabande.

À partir de la version 11.3.1 de Citrix SD-WAN, la gestion in-band prend en charge les paires d'appliances 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.

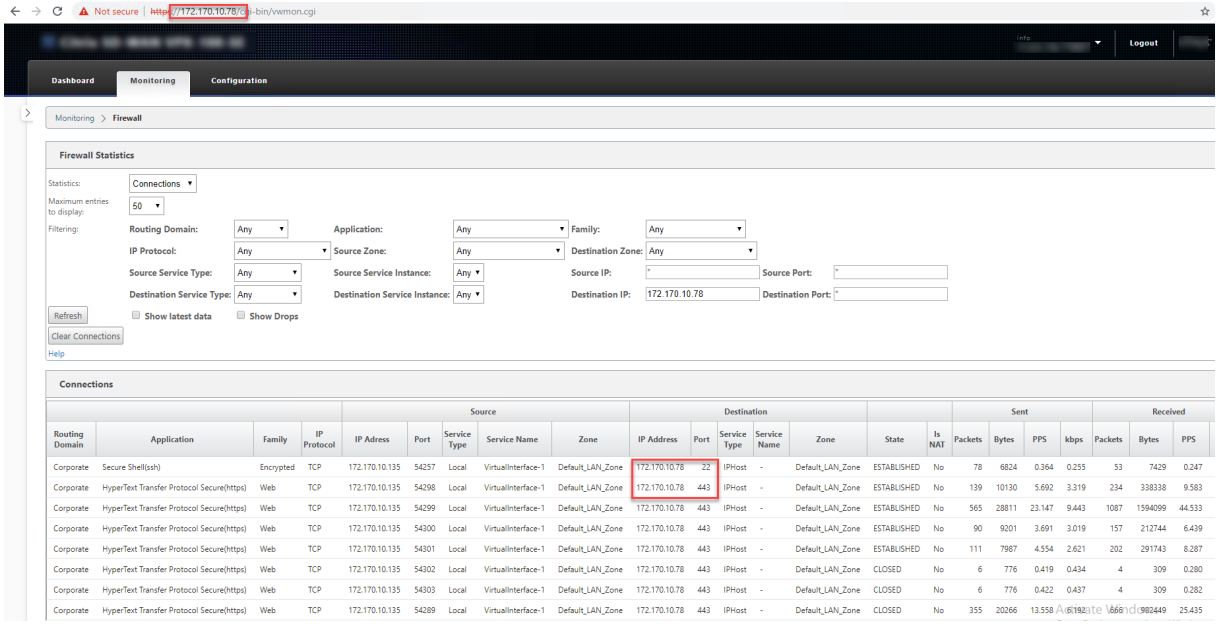
Par exemple, les adresses IP in-band suivantes sont utilisées pour accéder aux appliances :

- Appareil actif - 1.0.1.2
- Appareil principal - 1.0.1.10
- Appareil secondaire - 1.0.1.11

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'interface utilisateur Web accessibles à l'aide de l'IP virtuelle sur les ports 22 et 443 respectivement dans la colonne **Adresse IP de destination** .



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 ges-

tion 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.

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.

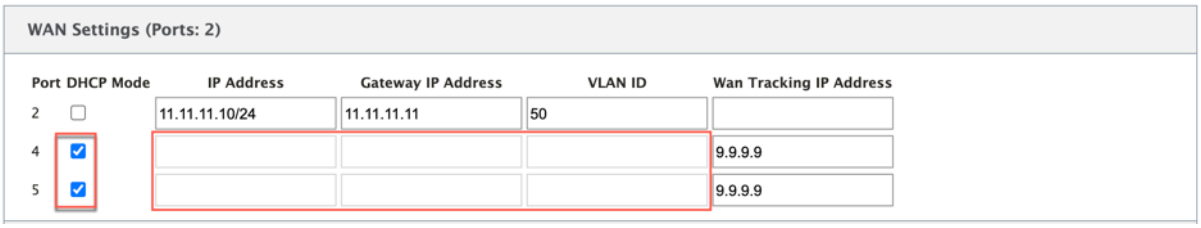
Le tableau suivant fournit les détails des ports WAN et LAN prédésignés pour la configuration de secours sur différentes plates-formes :

Plateforme	Ports WAN	Ports LAN
110	1/2	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
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.



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.

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

Vous pouvez configurer un port de gestion uniquement lorsque la gestion intrabande est activée sur d'autres interfaces approuvées de l'appliance.

Réseau de gestion des sauvegardes

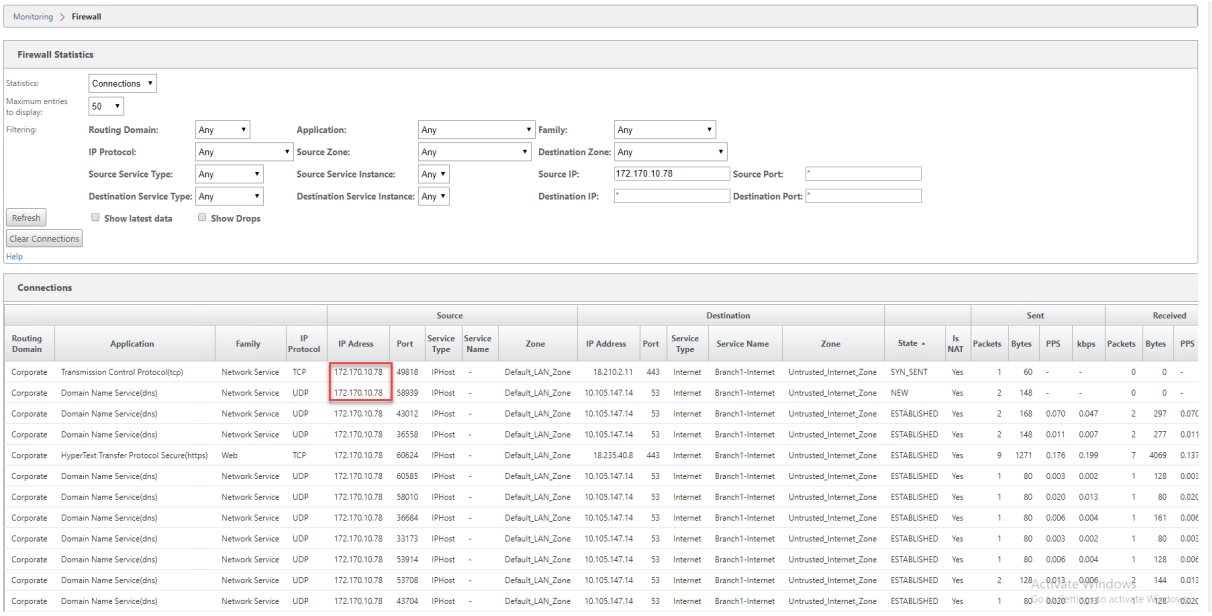
Vous pouvez configurer une adresse IP virtuelle en tant que réseau de gestion de sauvegarde. Il est utilisé comme adresse IP de gestion si le port de gestion n'est pas configuré avec une Gateway par défaut.

> **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.

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.



Accès Internet

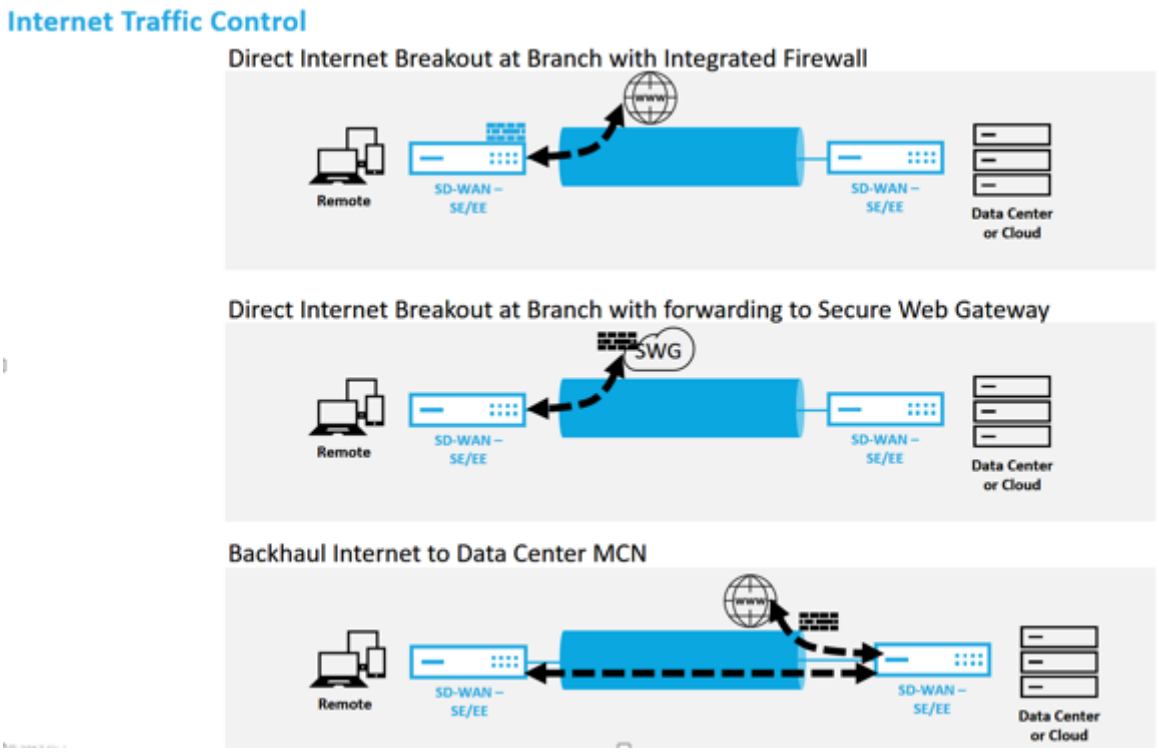
November 16, 2022

Le service Internet est utilisé pour le trafic entre un site d'utilisateur final et des sites sur l'Internet public. Le trafic du service Internet n'est pas encapsulé par SD-WAN et n'a pas les mêmes capacités que le trafic fourni via le service de chemin virtuel. Cependant, il est important de classer et de prendre en compte ce trafic sur le SD-WAN. Le trafic identifié en tant que service Internet permet au SD-WAN de gérer activement la bande passante de liaison WAN en limitant le trafic Internet par rapport au trafic acheminé sur le chemin virtuel et le trafic intranet selon la configuration établie par l'administrateur. En plus des fonctionnalités de provisionnement de bande passante, le SD-WAN a la capacité supplémentaire d'équilibrer la charge du trafic acheminé sur le service Internet à l'aide de plusieurs liaisons WAN Internet ou, en option, d'utiliser les liaisons WAN Internet dans une configuration principale ou secondaire.

Le contrôle du trafic Internet à l'aide du service Internet sur des 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
- Backhaul Internet vers le centre de données MCN

Pour plus d'informations sur la configuration d'un service Internet via le service Citrix SD-WAN Orchestrator, consultez la section Service Internet.



Routage d'Internet direct à la succursale avec pare-feu intégré

Le service Internet peut être utilisé dans les différents modes de déploiement pris en charge par Citrix SD-WAN.

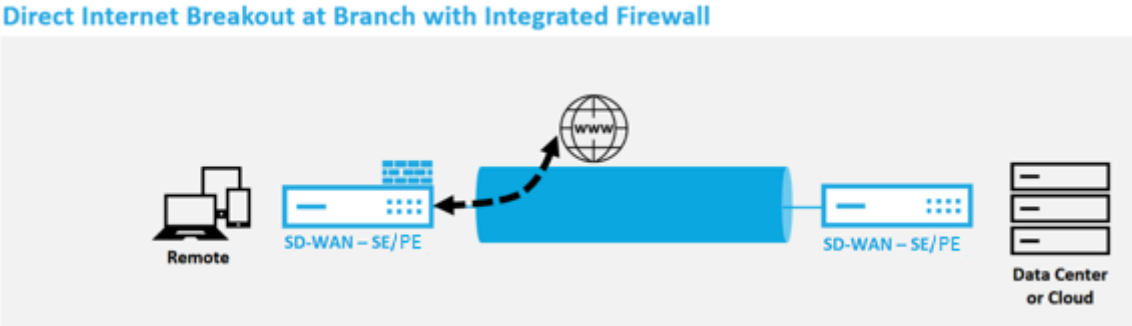
- Mode de déploiement en ligne (superposition SD-WAN)

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 périphériques et/ou des pare-feu existants. Si le SD-WAN est déployé derrière un pare-feu réseau, l'interface peut être configurée comme approuvée et le trafic Internet peut être remis au pare-feu en tant que Gateway Internet.

- Mode Edge ou passerelle

Citrix SD-WAN peut être déployé en tant que périphérique périphérique périphérique, en remplacement des périphériques de routeur Edge et/ou pare-feu existants. La fonctionnalité de pare-feu intégré permet au SD-WAN de protéger le réseau de 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.

Pour plus d'informations sur la configuration d'un service Internet via le service Citrix SD-WAN Orchestrator, consultez la section Service Internet.



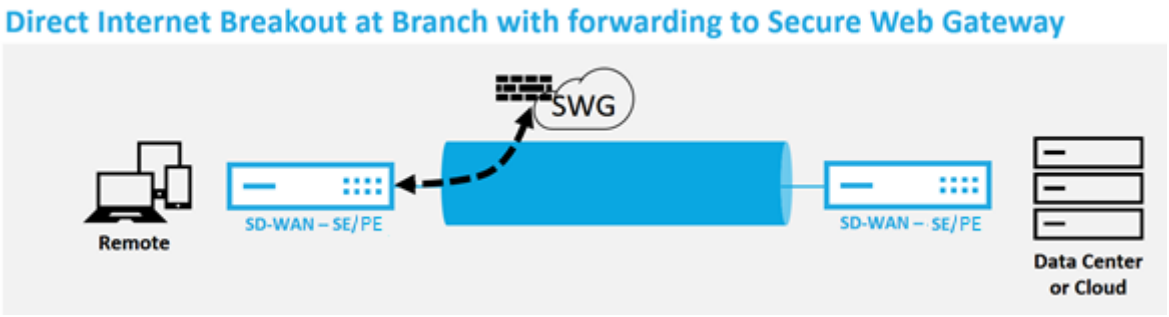
Accès direct à Internet avec Secure Web Gateway

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.

Pour plus d'informations sur la configuration d'un service Internet via le service Citrix SD-WAN Orchestrator, consultez la section Service Internet.



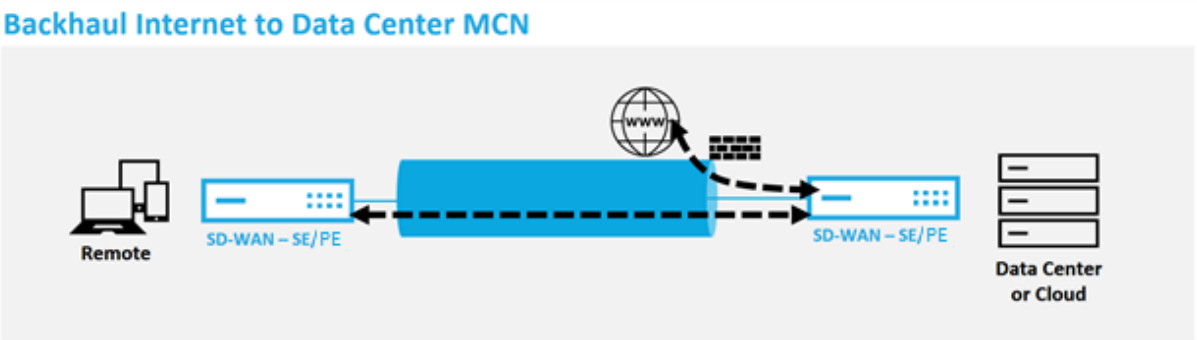
Citrix SD-WAN prend en charge les solutions Secure Web Gateway tierces suivantes :

- Zscaler
- Forcepoint
- Palo Alto
- Citrix Secure Internet Access

Backhauling d'Internet

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.

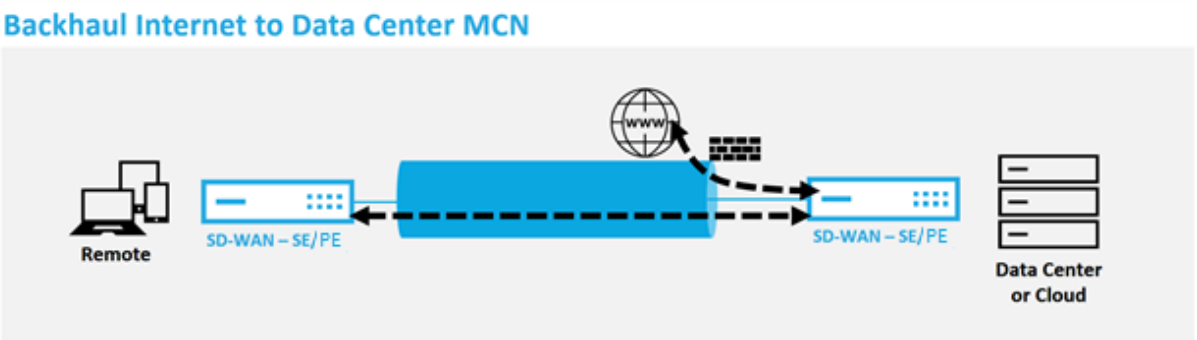


Tous les périphériques Citrix SD-WAN peuvent mettre fin à jusqu'à huit liaisons WAN Internet distinctes en un seul appareil. Les capacités de débit sous licence pour les liaisons WAN agrégées sont répertoriées par appliance respective sur la fiche technique Citrix SD-WAN.

Mode épingle à cheveux

Avec le déploiement de l'épingle à cheveux, vous pouvez implémenter l'utilisation d'un site Remote Hub pour l'accès Internet via backhaul ou en épingle à cheveux lorsque les services Internet locaux ne sont pas disponibles ou connaissent un trafic plus lent. Vous pouvez appliquer un routage à bande passante élevée 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 rationalisée. Vous pouvez utiliser un site Hub distant pour accéder à Internet en cas de besoin et acheminer les flux via le chemin virtuel vers le réseau SD-WAN.



Par exemple, considérez un administrateur disposant de plusieurs sites SD-WAN, A et B. Le site A a un service Internet médiocre. Le site B dispose d'un service Internet utilisable, avec lequel vous souhaitez rediriger le trafic du site A vers le site B. Vous pouvez essayer d'y parvenir sans la complexité des coûts d'itinéraire stratégiquement pondérés 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 d'un déploiement Hairpin. Par exemple, si le trafic est en épingle à cheveux entre le site A et le site B via le site C, seul le site C connaîtrait

les 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 vers WAN.

Lorsque le trafic est transité entre le site A et le site B par 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 intermédiaire C.

Le transfert WAN à 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 de transfert WAN à WAN.

   Le transfert Wan-Wan et le déploiement Hairpin sont mutuellement exclusifs. Un seul d'entre eux peut être configuré à un moment donné dans le temps.

   Les appliances Citrix SD-WAN SE et VPX (virtuelles) prennent en charge le déploiement en épingle à cheveux. Vous pouvez maintenant configurer une route 0.0.0.0/0 vers le trafic en épingle à cheveux entre deux emplacements sans affecter d'autres emplacements. 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 en épingle à cheveux. L'activation du transfert WAN vers WAN pour réaliser la fonctionnalité d'épingle à cheveux n'est plus nécessaire.

Pare-feu hébergés

November 16, 2022

Le service Citrix SD-WAN Orchestrator prend en charge les pare-feux hébergés suivants :

- Réseaux Palo Alto
- Check Point

Intégration du pare-feu Palo Alto Networks sur la plate-forme SD-WAN 1100

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 du pare-feu est intégrée en mode **Virtual Wire** et deux interfaces virtuelles de données y sont connectées. Le trafic requis peut être redirigé vers la machine virtuelle du pare-feu en configurant des stratégies sur SD-WAN.

Pour plus d'informations sur la façon de provisionner la machine virtuelle de pare-feu via le service SD-WAN Orchestrator, consultez la section Pare-feu hébergés.

Avantages

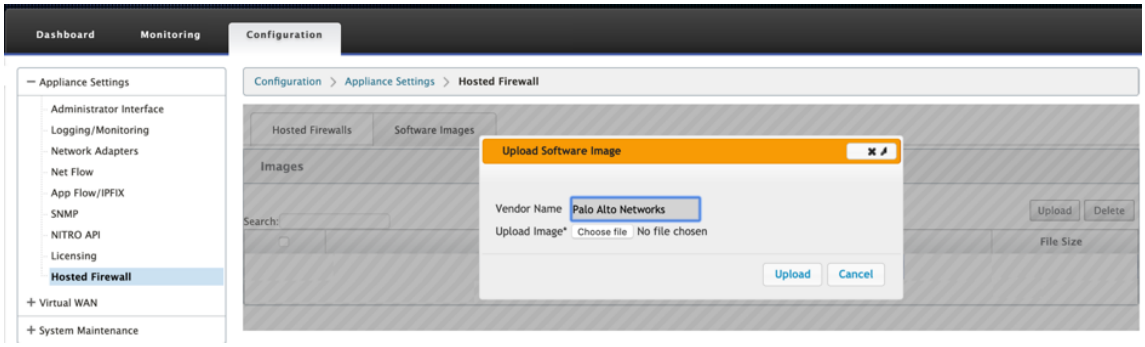
Voici les principaux objectifs ou avantages de l'intégration de Palo Alto Networks sur la plateforme SD-WAN 1100 :

- Consolidation des appareils des succursales : une appliance unique qui assure à la fois le SD-WAN et la sécurité avancée.
- Sécurité des succursales avec pare-feu NGFW (Next Generation Firewall) sur site pour protéger le trafic LAN vers LAN, LAN-to-Internet et Internet-LAN.

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 :

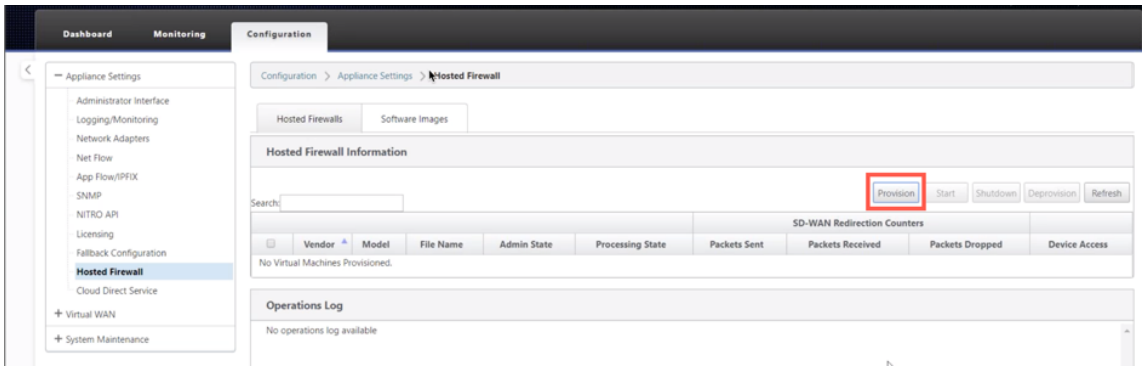
1. Dans l'interface graphique Citrix SD-WAN, accédez à **Configuration >** Développez **Paramètres de l'appliance >** sélectionnez **Pare-feu hébergé** .
2. Téléchargez l'image du logiciel :
    - Sélectionnez l'onglet **Images logicielles** . Sélectionnez le nom du fournisseur en tant que **Palo Alto Networks**.
    - Choisissez le fichier image du logiciel.
    - Cliquez sur **Charger**.



> **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 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 hébergés** et cliquez sur le bouton **Provisioning**.

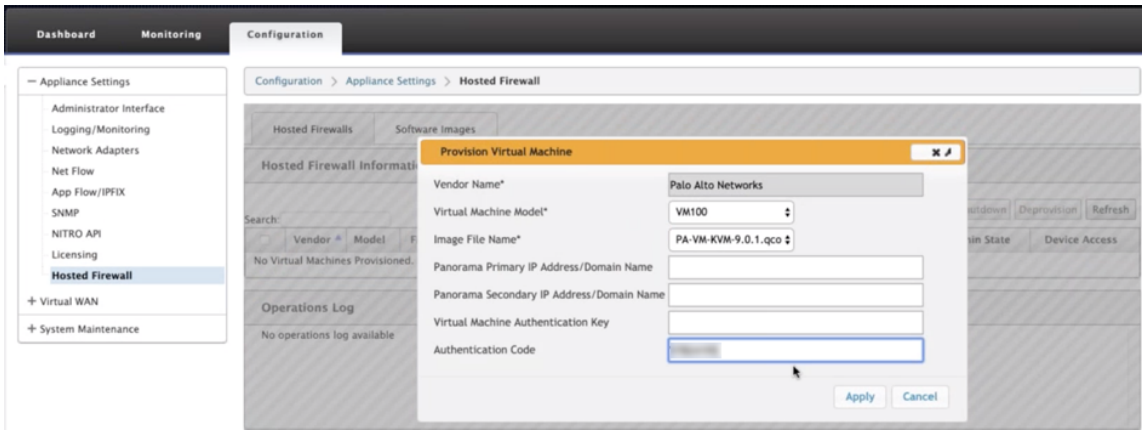


4. Fournissez les détails suivants pour le Provisioning.

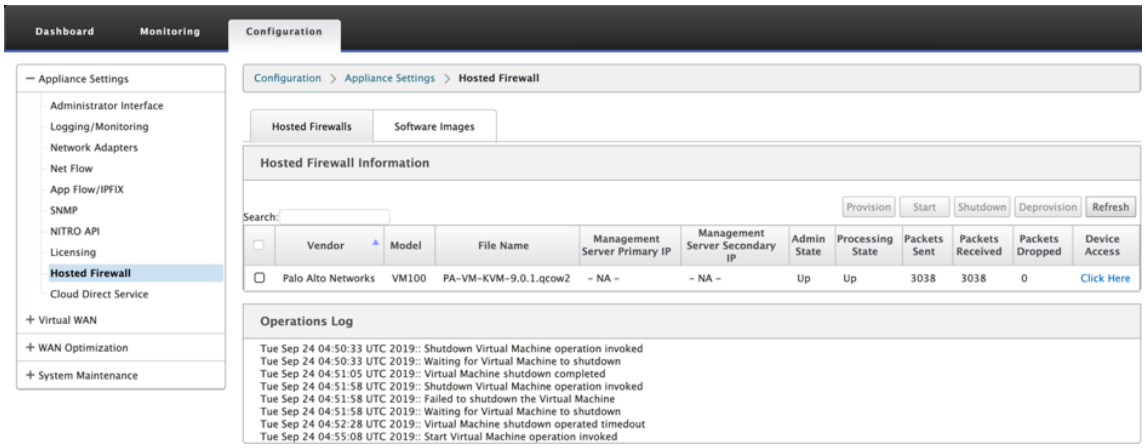
   - **Nom du fournisseur** : sélectionnez le fournisseur comme **Palo Alto Networks**.
   - **Modèle de machine virtuelle** : sélectionnez le numéro de modèle de machine virtuelle dans la liste.
   - **Nom du fichier image** : sélectionnez le fichier image.
   - **Adresse IP principale/nom de domaine Panorama** : indiquez l'adresse IP principale Panorama ou le nom de domaine complet (facultatif).
   - **Adresse IP secondaire Panorama/Nom de domaine** : 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 que la machine virtuelle Palo Alto Networks est complètement démarrée, elle réfléchira 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 Palo Alto Networks ou utilisez 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 de Palo Alto Networks.

Intégration du pare-feu Check Point sur la plate-forme SD-WAN 1100

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** fonctionne comme une machine virtuelle sur la plate-forme SD-WAN 1100 SE. La machine virtuelle du pare-feu est intégrée en mode Bridge et deux interfaces virtuelles de données y sont connectées. Le trafic requis peut être redirigé vers la machine virtuelle du pare-feu en configurant des stratégies sur SD-WAN.

Pour plus d'informations sur la façon de provisionner la machine virtuelle de pare-feu via le service SD-WAN Orchestrator, consultez la section Pare-feu hébergés.

> **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 :

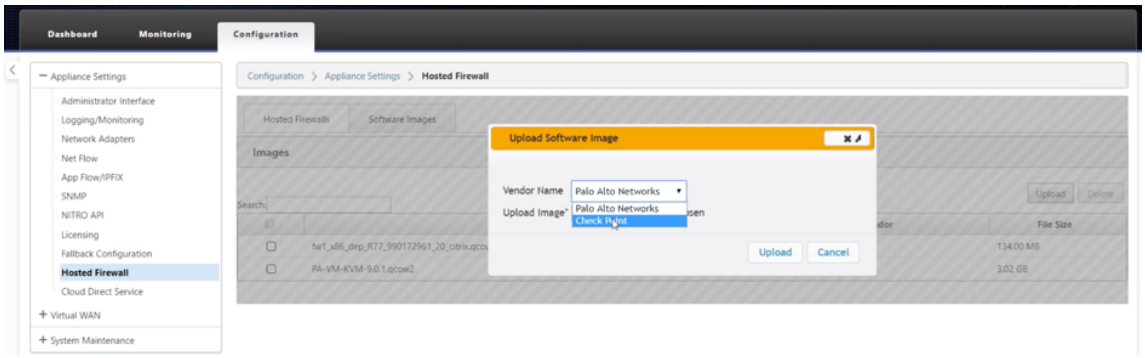
- Consolidation des périphériques de succursale : une appliance unique qui effectue à la fois le SD-WAN et la sécurité avancée
- Sécurité des succursales avec pare-feu NGFW sur site (Next Generation Firewall) pour protéger le trafic LAN à LAN, LAN à Internet et Internet-to-LAN

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 :

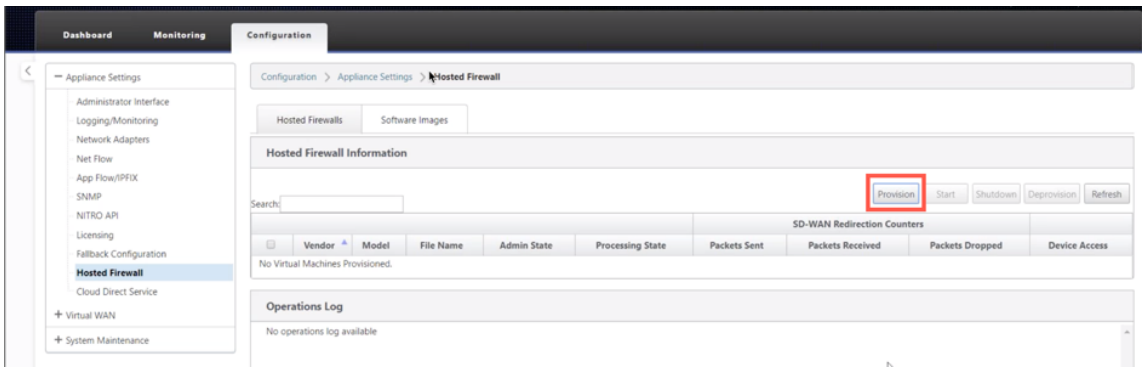
- Sélectionnez l'onglet **Images logicielles** . Sélectionnez le **nom du fournisseur** comme point de contrôle.
- Choisissez le fichier image du logiciel.
- Cliquez sur **Charger**.



> **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.

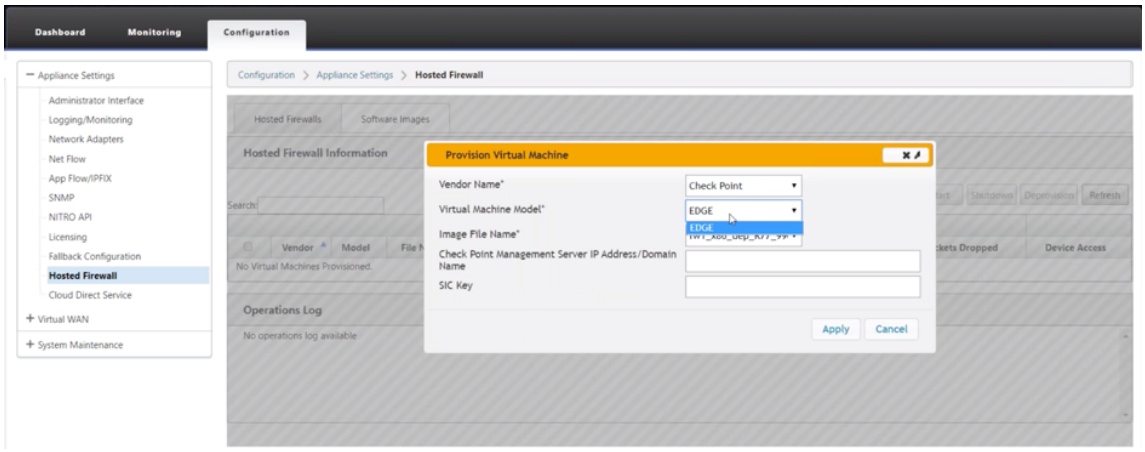
3. Pour le provisioning, sélectionnez l'onglet **Pare-feu hébergé** > cliquez sur le bouton **Provisioning**.



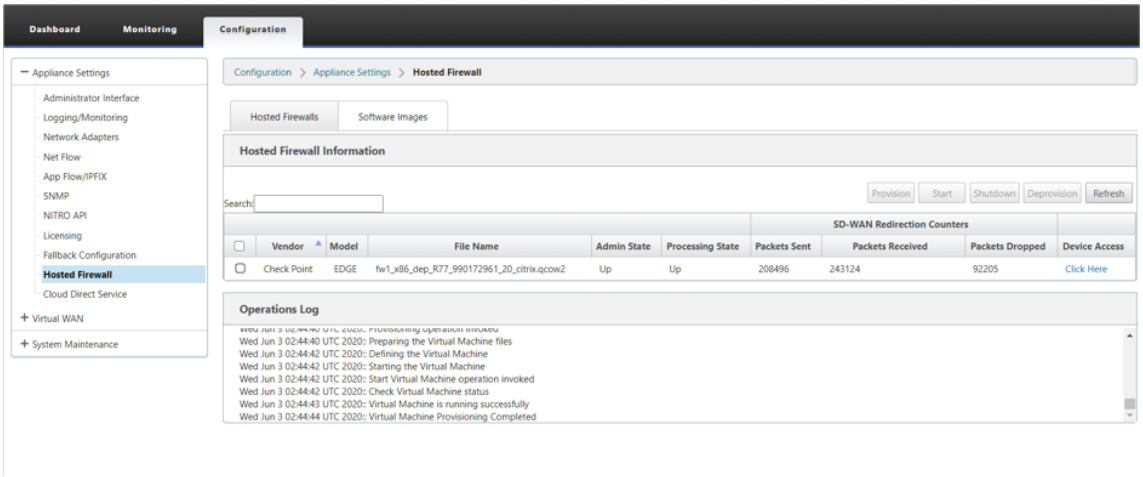
4. Fournissez les détails suivants pour le Provisioning.

- **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 **Appliquer**.



5. Cliquez sur **Actualiser** pour obtenir le dernier état. Une fois que la machine virtuelle Check Point est complètement démarrée, elle réfléchit sur l'interface utilisateur SD-WAN avec les détails du journal des opérations.



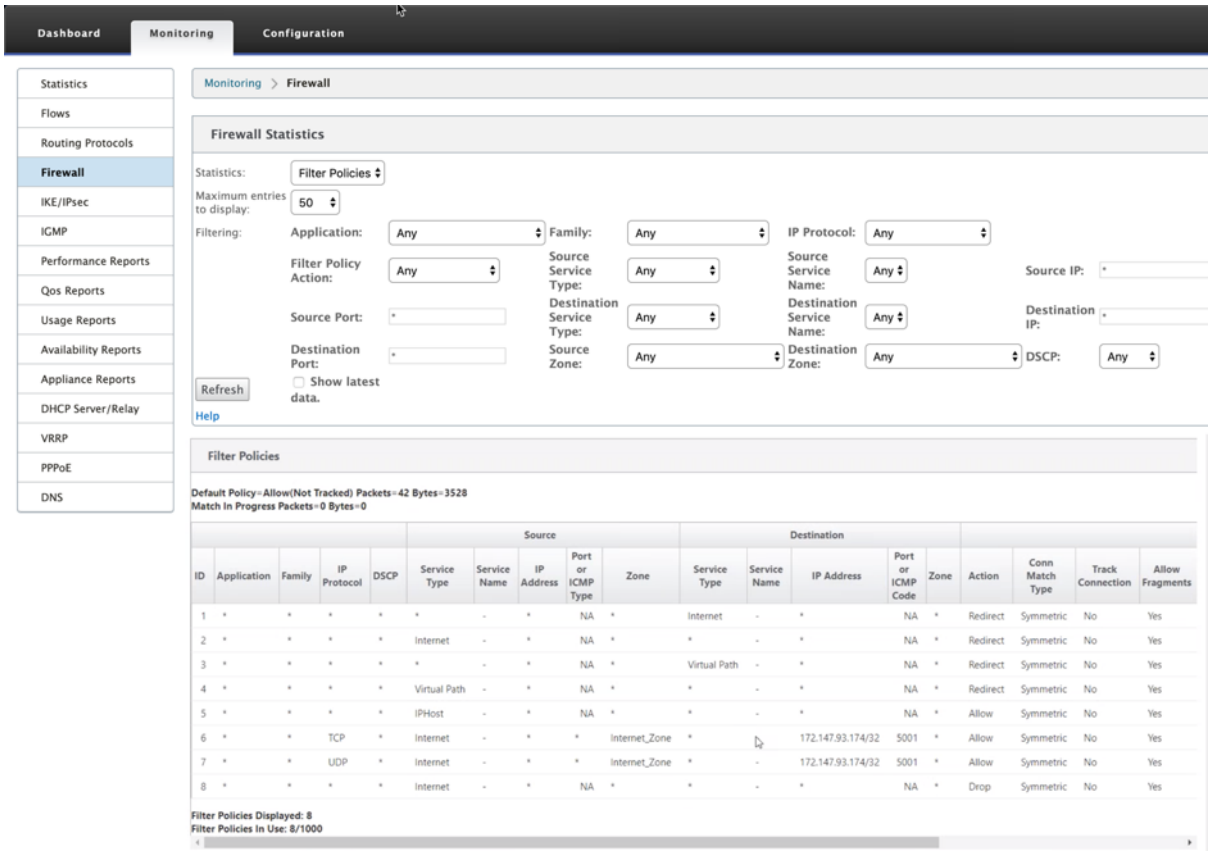
- **État d'administration** : indique si la machine virtuelle est en service ou en panne.
- **État de traitement : état**de traitement du chemin de données de la machine virtuelle.
- **Paquet envoyé** : paquets envoyés depuis le SD-WAN vers la machine virtuelle de sécurité.
- **Paquet reçu** : paquets 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.

Pendant que toute la configuration réseau est en mode opérationnel, vous pouvez surveiller la connexion sous **Surveillance > Pare-feu > Stratégies de filtrage**.



Groupes d'agrégation de liens

August 31, 2022

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 1100 SE
- Citrix SD-WAN 2100 SE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE
- Citrix SD-WAN 6100 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.

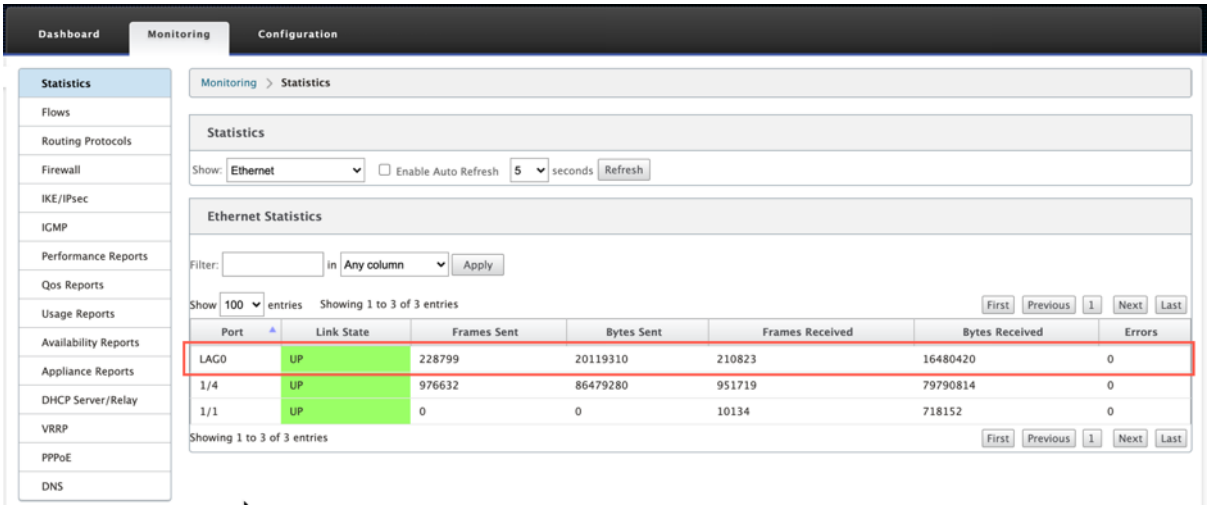
> **Remarque**
>
> - Pour les appliances Citrix SD-WAN 210 SE, vous ne pouvez créer qu'un seul LAG avec un maximum de trois ports regroupés dedans.
> - La fonctionnalité de propagation de l'état de liaison (LSP) n'est pas prise en charge si les

> LAG sont utilisés comme interfaces Ethernet dans les groupes d'interfaces.

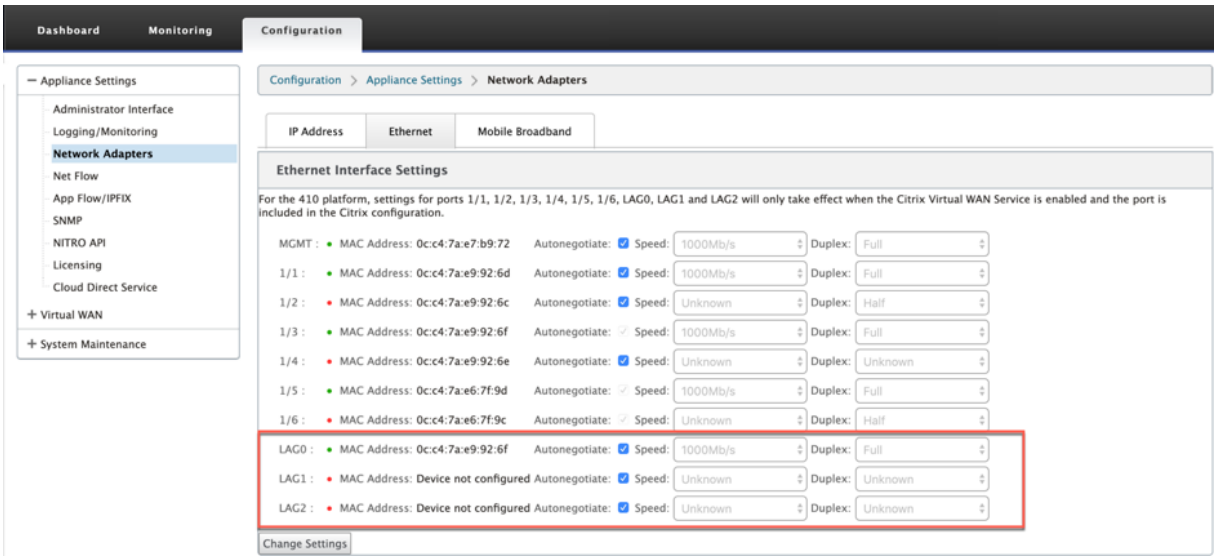
À partir de Citrix SD-WAN 11.5, vous pouvez configurer des groupes d'agrégation de liens via le service SD-WAN Orchestrator. Pour plus d'informations, consultez la section Groupes d'agrégation de liens.

Surveillance et dépannage

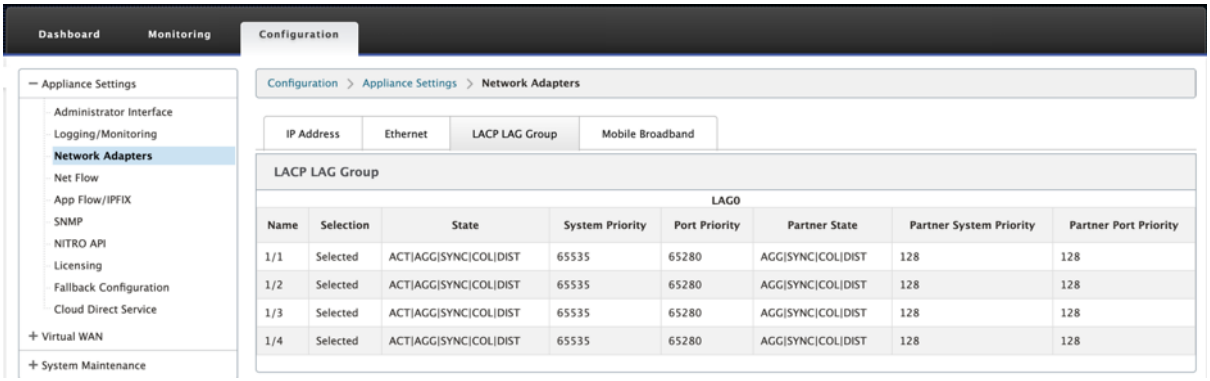
Pour afficher les statistiques ou l'état du lien, accédez à **Surveillance > Statistiques**. Sélectionnez **Ethernet** dans la liste déroulante **Afficher**.



Pour afficher les ports LAG actifs et de secours, accédez à **Configuration** > **Paramètres de l'appliance** > **Cartes réseau** > **Ethernet**.



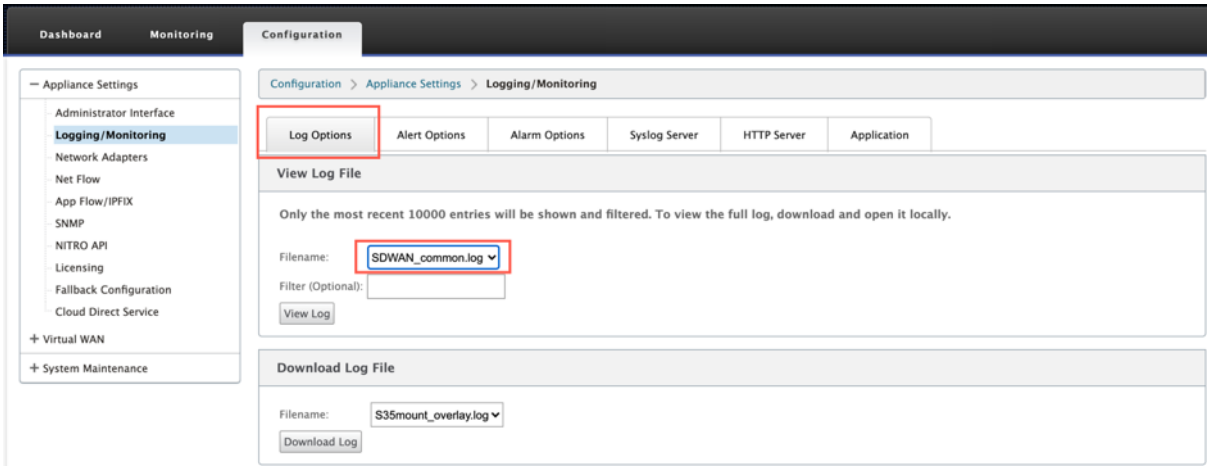
Sélectionnez l'onglet **Groupe de LAG LACP** pour afficher les différents détails relatifs au groupe LAG LACP.



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**.



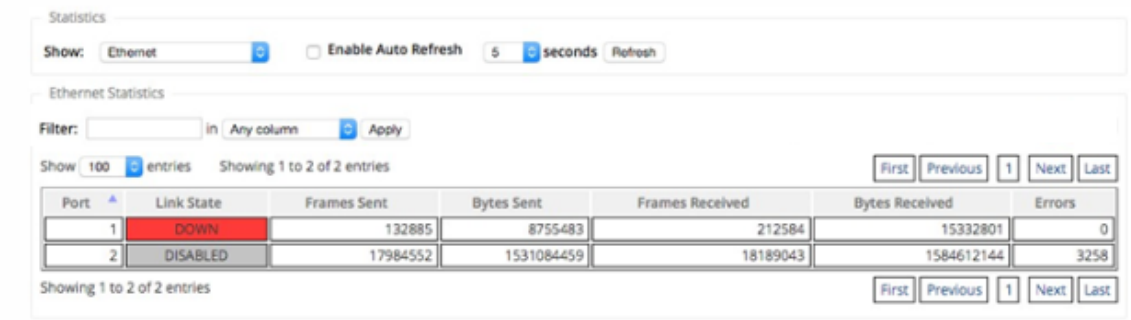
Propagation d'état des liens

August 31, 2022

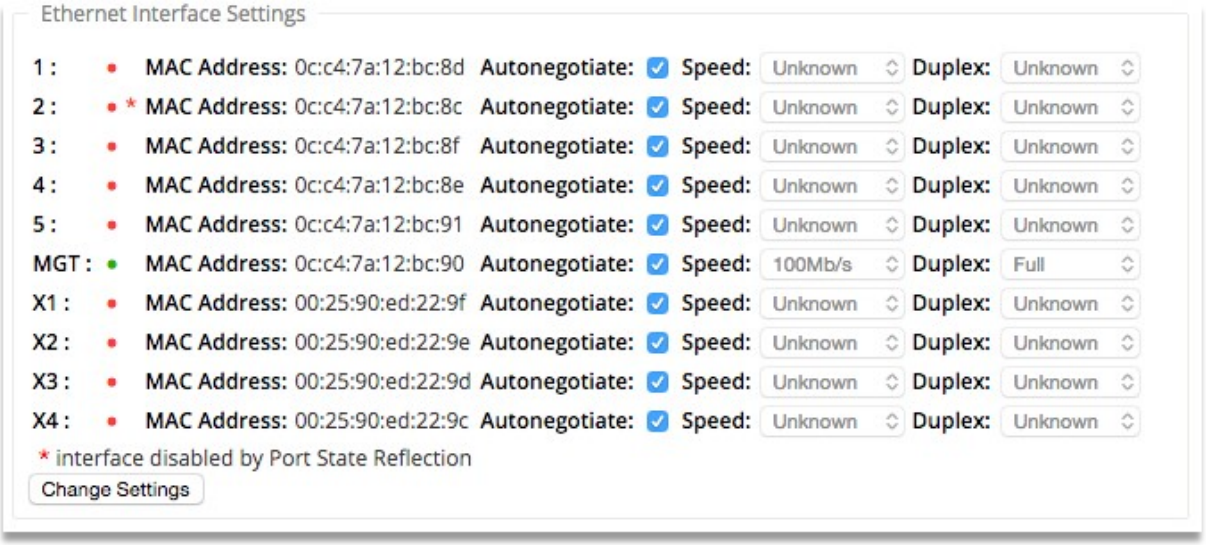
La fonctionnalité de propagation d'état de liaison (LSP) permet aux administrateurs réseau de garder l'état de liaison d'une paire de contournement synchronisé, ce qui permet d'attacher de l'autre côté du lien pour afficher lorsque les liens sont inactifs. Lorsqu'un port d'une paire de dérivation devient inactif, la liaison couplée est désactivée administrativement. Si votre architecture réseau inclut un réseau de basculement parallèle, cela force le trafic à passer à ce réseau. Une fois le lien interrompu restauré, le lien correspondant devient automatiquement actif.

Surveillance des statistiques sur les liens

1. Dans la page **Surveiller > Statistiques**, choisissez **Ethernet dans le menu** déroulant **Afficher** pour afficher l'état de la paire de ports de contournement pour laquelle la propagation de l'état des liens est activée. Observez que la liaison côté LAN est désactivée et plus tard, la liaison côté WAN de la paire de contournement est administrativement désactivée.



2. Accédez à **Configuration > Paramètres du matériel** > **Adaptateurs réseau > onglet Ethernet** . Les ports qui sont en panne sur le plan administratif sont signalés par un astérisque rouge (*) dans la liste des **paramètres de l'interface Ethernet** .



Mesure et liens WAN de secours

November 16, 2022

Citrix SD-WAN prend en charge l'activation des liens mesurés, qui peuvent être configurés de telle sorte que le trafic utilisateur ne soit transmis que sur un lien WAN Internet spécifique lorsque tous les autres liens WAN disponibles sont désactivés.

Les liens mesurés conservent la bande passante sur les liens facturés en fonction de leur utilisation. Avec les liens mesurés, vous pouvez configurer les liens en tant que lien de dernier recours, ce qui n'autorise pas l'utilisation du lien jusqu'à ce que tous les autres liens non mesurés soient en panne ou dégradés. Le paramètre Set Last Resort est généralement activé lorsqu'il existe trois liens WAN vers un site (c'est-à-dire MPLS, Internet haut débit, 4G/LTE) et que l'un des liens WAN est 4G/LTE et peut être trop coûteux pour une entreprise d'autoriser l'utilisation à moins que cela ne soit 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 :

- Bouchon 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

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 mesurée locale est suivie par rapport à la limite de données configurée. 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. 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 l'un des deux modes suivants que la liaison de secours opère

- **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 à la même priorité

Lors de la configuration d'un lien de secours, vous pouvez spécifier la priorité de secours et deux intervalles de pulsation :

- **Intervalle de pulsation actif** : intervalle de pulsation utilisé lorsque le chemin d'accès en veille est actif (50 ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s par défaut)
- **Intervalle de pulsation de veille** : intervalle de pulsation utilisé lorsque le chemin d'accès en veille 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'accès de secours à la demande est formé entre :
  - une liaison non-standby 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 en attente 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 alors qu'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 de secours est en veille.

- Si l'intervalle de pulsation actif est configuré sur les deux liens, la plus grande des deux valeurs est utilisée lorsque le chemin de secours est actif.

Messages de pulsation (garder en vie) :

- Sur un chemin non en attente, 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 de secours 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 attente, les messages de pulsation sont envoyés uniquement lorsqu'il n'y a pas eu de trafic (contrôle ou utilisateur) pour au moins l'intervalle de pulsation actif configuré.
- l'intervalle de pulsation de secours configuré est utilisé lorsque l'état du chemin est BON.
- 1/2 l'intervalle de pulsation de secours configuré est utilisé lorsque l'état du chemin est BAD.

Bien qu'inactifs, les chemins de secours ne sont pas éligibles au trafic utilisateur. Les seuls messages de protocole de contrôle envoyés sur des 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 attente, s'ils sont disponibles, soient favorisés lors de la sélection du chemin de transfert.

L'état du chemin d'accès d'un chemin d'accès de secours avec pulsation désactivé, lorsqu'il est inactif, est supposé être BON et il est affiché comme BON dans le tableau Statistiques de chemin sous **Surveillance**. Lorsqu'il devient actif, contrairement à un chemin non standby qui commence à l'état DEAD jusqu'à ce qu'il entenne 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 l'homologue Virtual Path est rétablie, le chemin devient BAD, puis à nouveau GOOD.

Si ce chemin de secours passe DEAD puis devient inactif, l'état du chemin ne change pas immédiatement en (supposé) GOOD. Au lieu de cela, il est conservé dans l'état DEAD pendant le temps afin

qu'il ne puisse pas être utilisé immédiatement. Ceci permet d'empêcher l'activité d'osciller entre un groupe de chemins de priorité inférieure avec supposés bons chemins DEAD et un groupe de chemins de priorité supérieure avec des chemins réellement GOOD. Cette période de mise en 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 fait la transition entre le mode veille et le mode actif.

À partir de SD-WAN 11.5, vous pouvez configurer des liaisons WAN limitées et de secours à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Metering and Standby WAN Links.

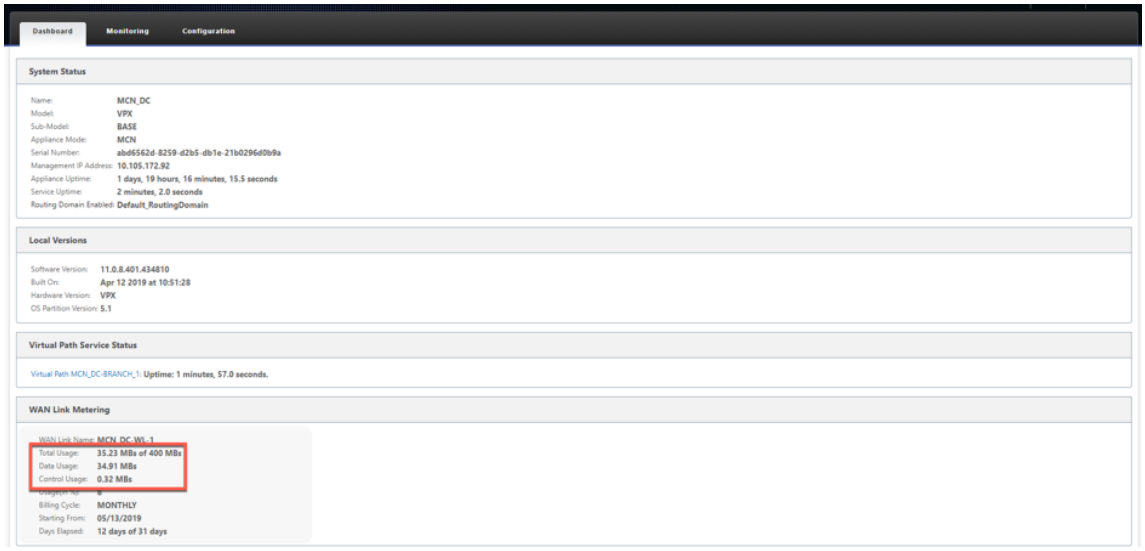
Prérequis de configuration :

- Une liaison 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 Private MPLS ne peut pas être configurée en tant que liaison de secours.
- Au moins un lien non de secours 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 des liens de secours à la demande. Les liens de secours à la demande prennent en charge le service de chemin virtuel uniquement.
- 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.

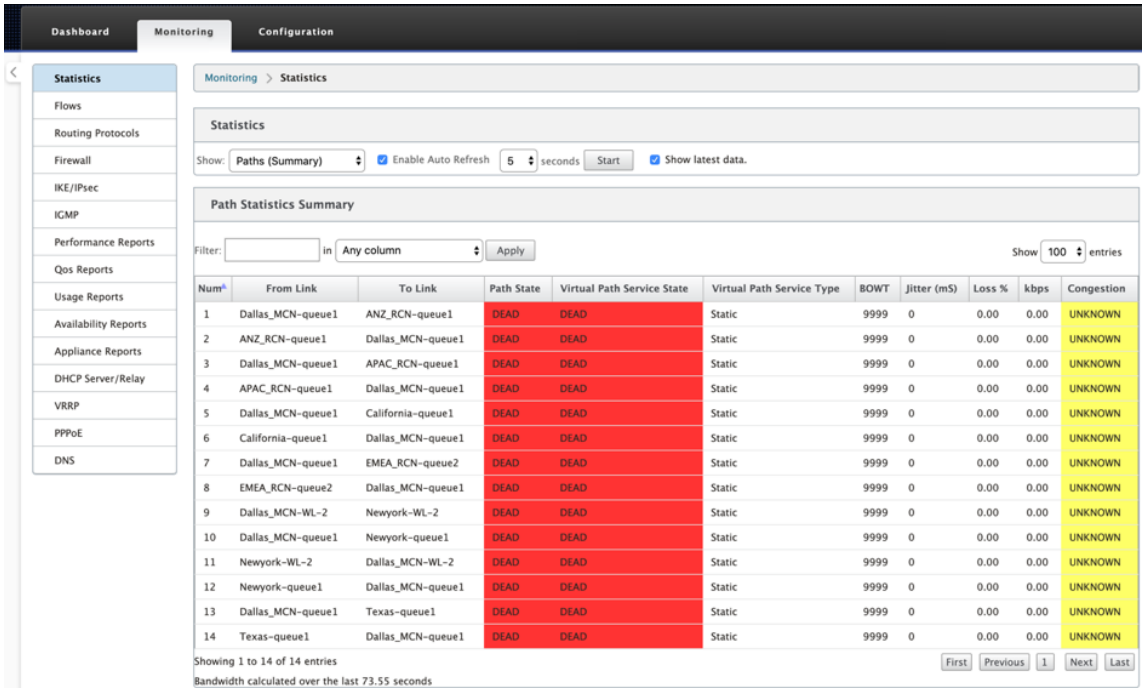
Surveiller les liaisons WAN mesurées et de secours

- La page Tableau de bord fournit les informations suivantes sur la **mesure des liens WAN** 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 donnée+contrôle de l'utilisation).
  - **Utilisation des données** : affiche l'utilisation par trafic utilisateur.

- **Contrôle de l'utilisation** : affiche l'utilisation par trafic de contrôle.
- **Utilisation (en %)** : affiche la valeur du plafond de données utilisées en pourcentage (utilisation totale/limite de données) x 100.
- **Cycle de facturation** : 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)

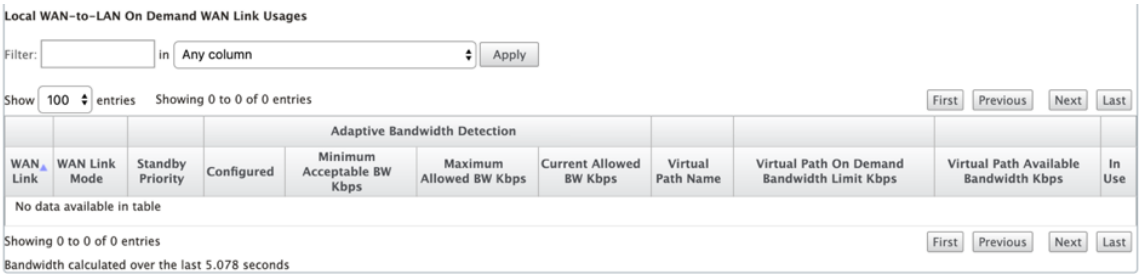


- Lorsque les statistiques de chemin (**Surveillance > Statistiques > Chemins**) sont affichées, les liens mesurés et les liens de secours sont marqués comme indiqué dans la capture d'écran.

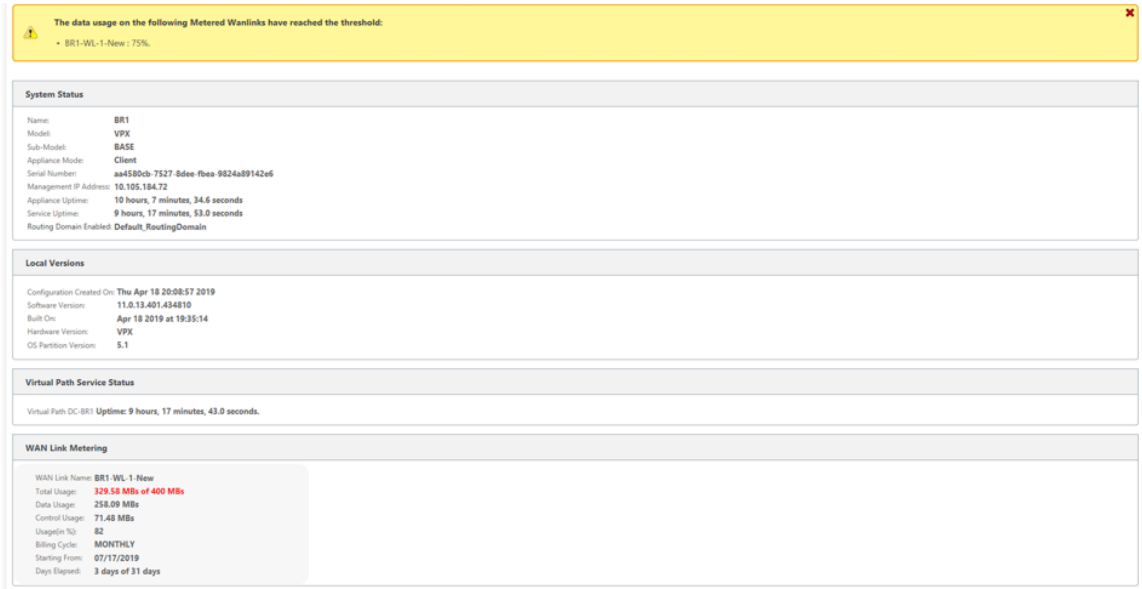


- Si l'appliance dispose d'un chemin virtuel doté d'un lien de secours local ou distant à la de-

mande, lorsque les statistiques d'utilisation du lien WAN sont affichées, un tableau supplémentaire indiquant la bande passante à la demande s'affiche en bas de la page (**Surveillance > Statistiques > Utilisation du lien WAN**).

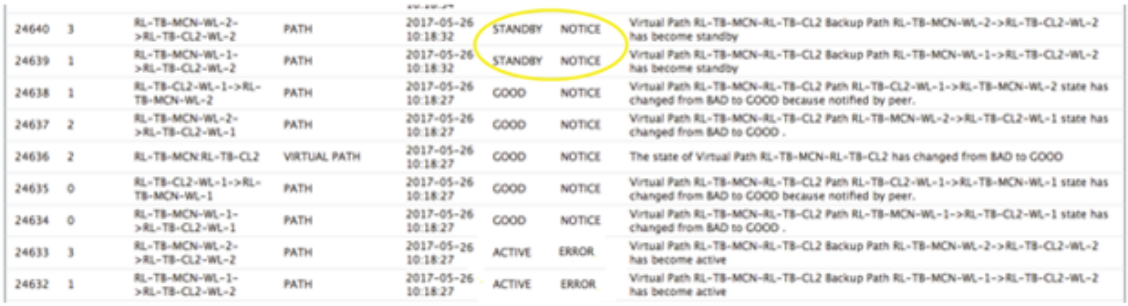


- Lorsque l'utilisation sur un lien mesuré dépasse 50 % de la limite de données configurée, une bannière d'avertissement s'affiche en haut du tableau de bord. En outre, si l'utilisation dépasse 75 % de la limite de données configurée, les informations de mesure numérique vers le bas du tableau de bord sont mises en surbrillance.



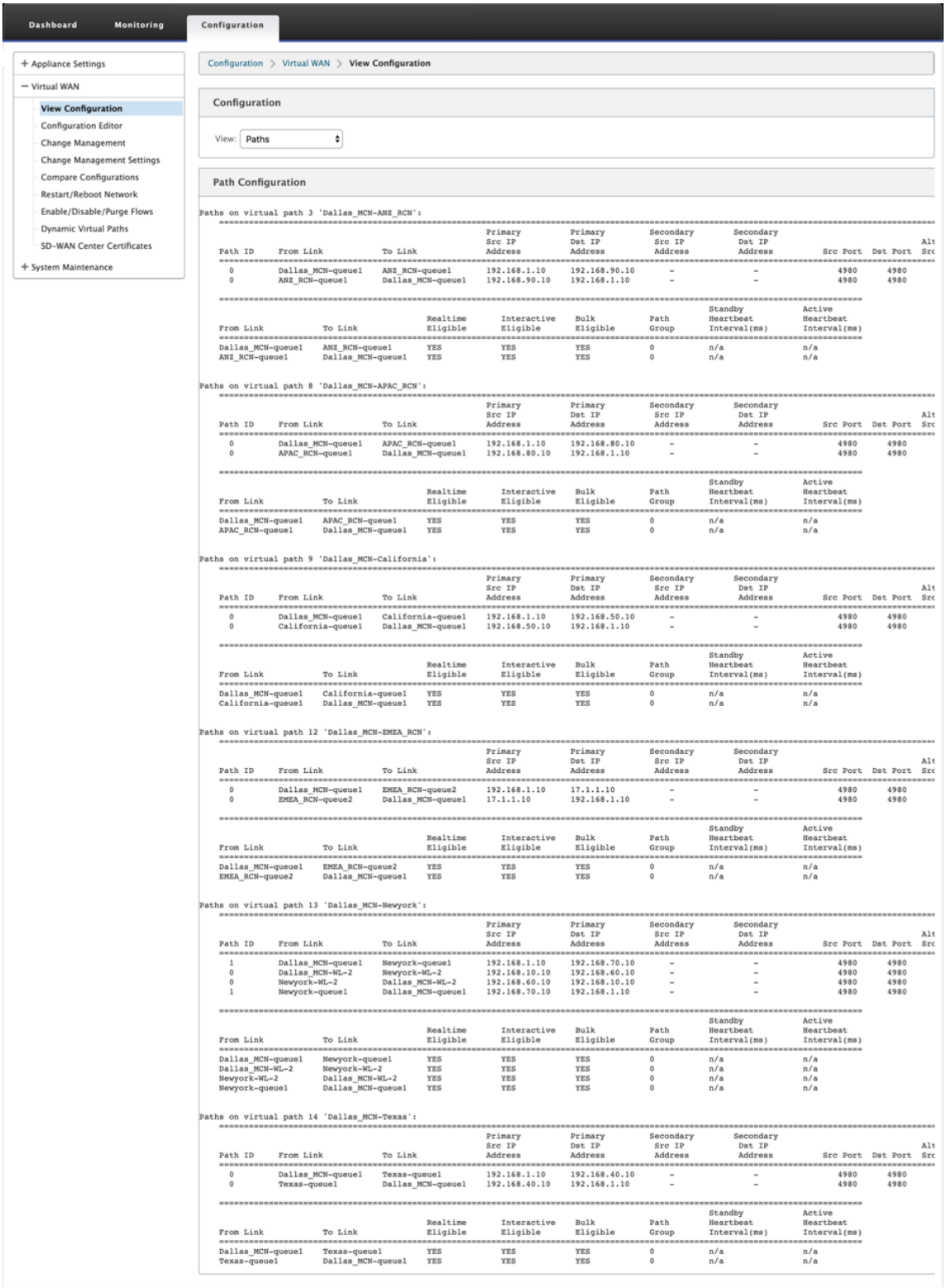
Un événement d'utilisation de liaison WAN est également généré au niveau de l'appliance lorsque l'utilisation dépasse 50 %, 75 % et 90 % du plafond de données configuré.

1. Lorsqu'un chemin de secours passe entre l'état de veille et l'état actif, un événement est généré par l'appliance.



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** .



Optimisation d'Office 365

November 16, 2022

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 Optimize 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 :

```
- Teams Realtime
- Exchange Online
- 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 :

```
- Teams TCP Fallback
- Exchange Mail
- SharePoint Allow
- 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

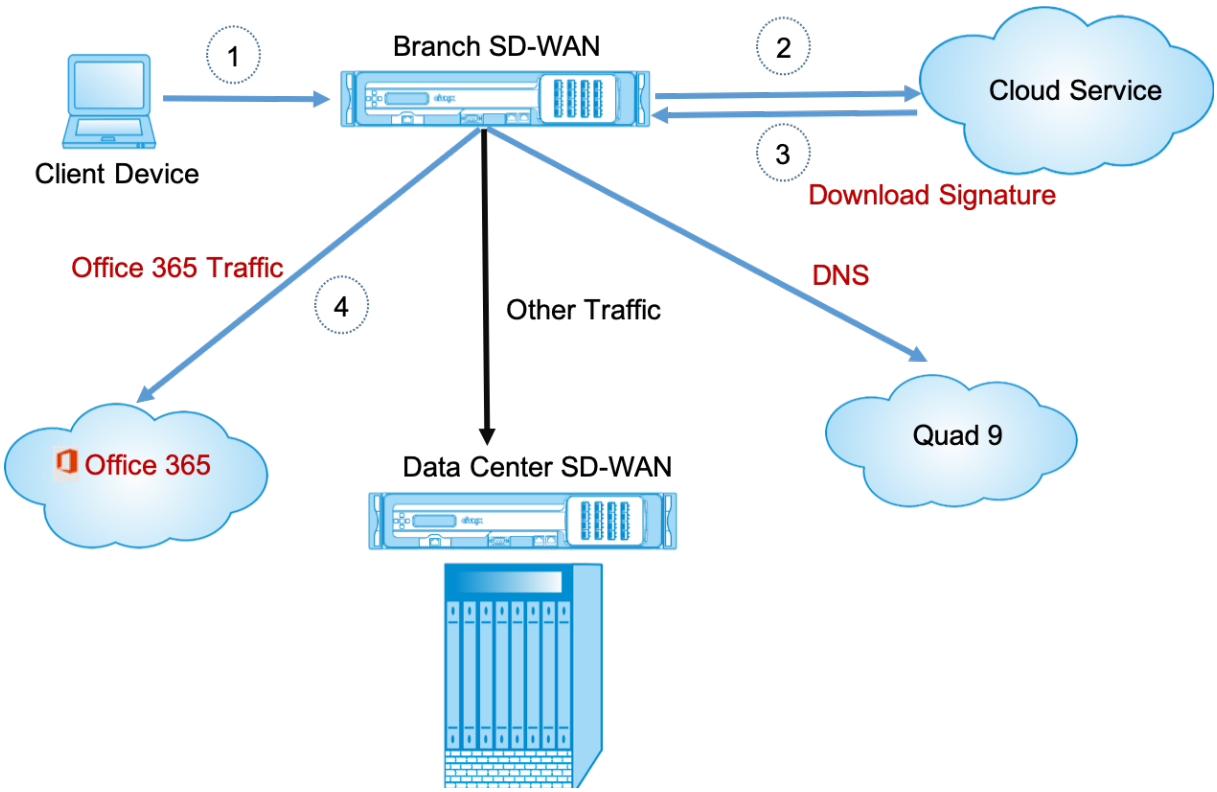
365. Par conséquent, il est recommandé de désactiver cette option lors de l'activation de la répartition Office 365 dans votre réseau.

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).

À partir de Citrix SD-WAN 11.5, vous pouvez configurer le breakout Office 365 à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Optimisation d'Office 365.

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.

Considérations importantes pour la mise à niveau

Optimiser et autoriser les catégories

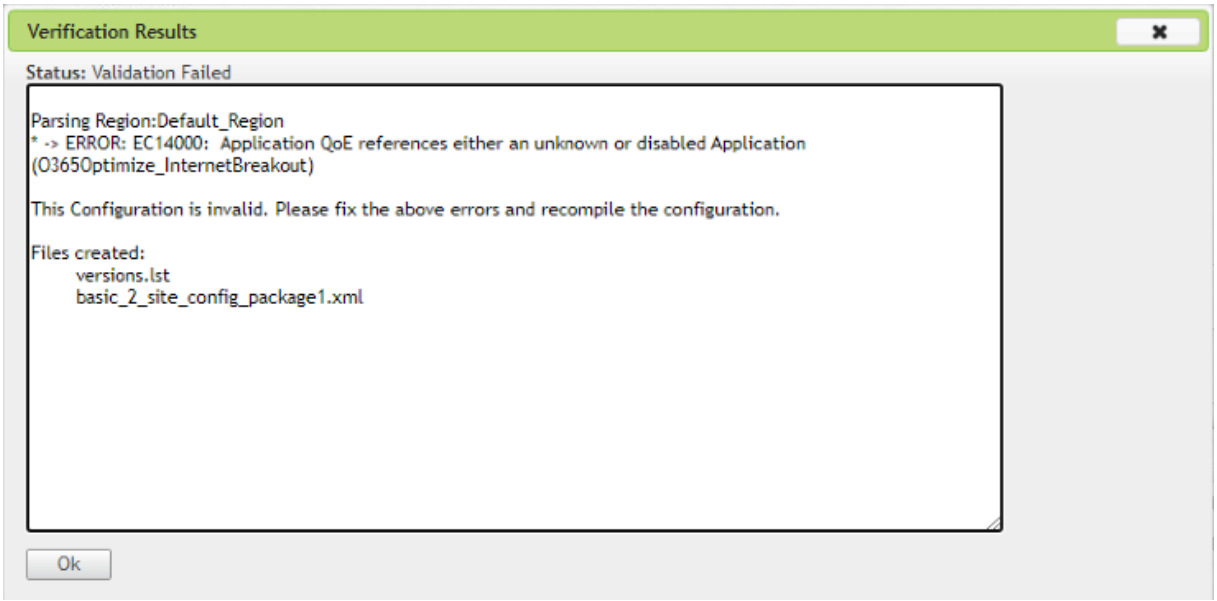
Si vous avez activé la stratégie de répartition Internet pour les catégories **Optimiser** et **Autoriser** Office 365, Citrix SD-WAN active automatiquement la stratégie de déclassement Internet pour les sous-catégories correspondantes lors de la mise à niveau vers Citrix SD-WAN 11.4.0.

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_InternetBreakoutet 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 :



> **Remarque**
>
> Cette mise à niveau n'est pas requise pour les règles/itinéraires créés automatiquement. Elle s'applique uniquement aux règles/itinéraires que vous avez créés.

DNS

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.

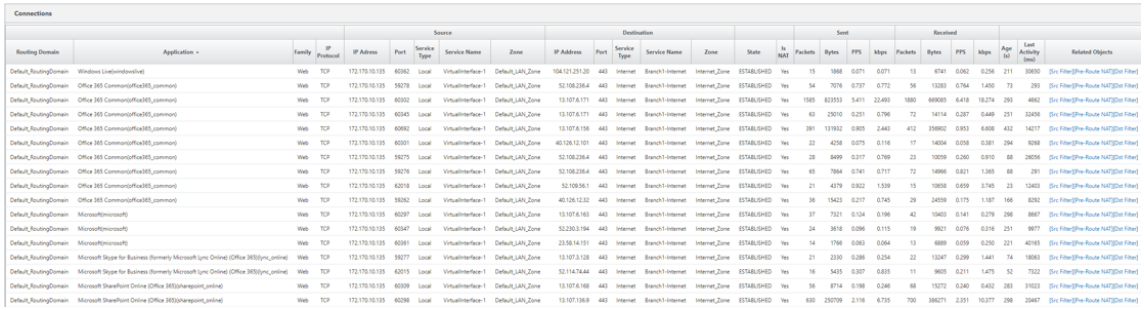
Si vous procédez à la mise à niveau Citrix SD-WAN 11.4.0 sans supprimer les anciennes règles de proxy DNS ou de redirecteur transparent, vous ne voyez aucune erreur et la mise à niveau réussit également. Toutefois, les règles de proxy DNS et les règles de transfert transparentes ne prennent pas effet dans Citrix SD-WAN 11.4.0.

> **Remarque**
>
> Cette activité ne s'applique pas aux règles DNS créées automatiquement. Elle s'applique uniquement aux règles DNS que vous avez créées.

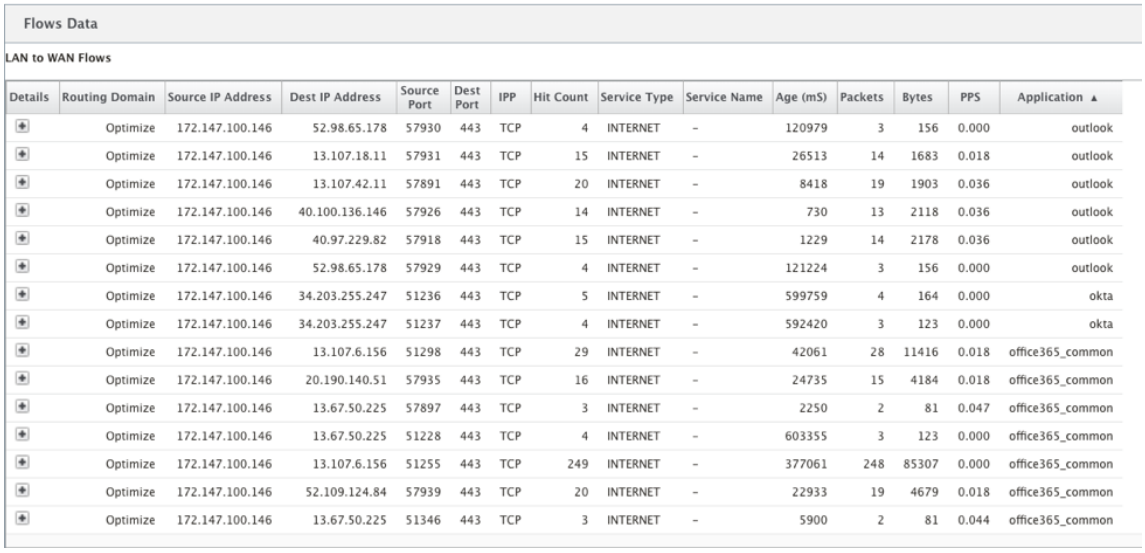
Surveillance

Vous pouvez surveiller les statistiques de l'application Office 365 dans les rapports de statistiques SD-WAN suivants :

- Statistiques de pare-feu



- Flux

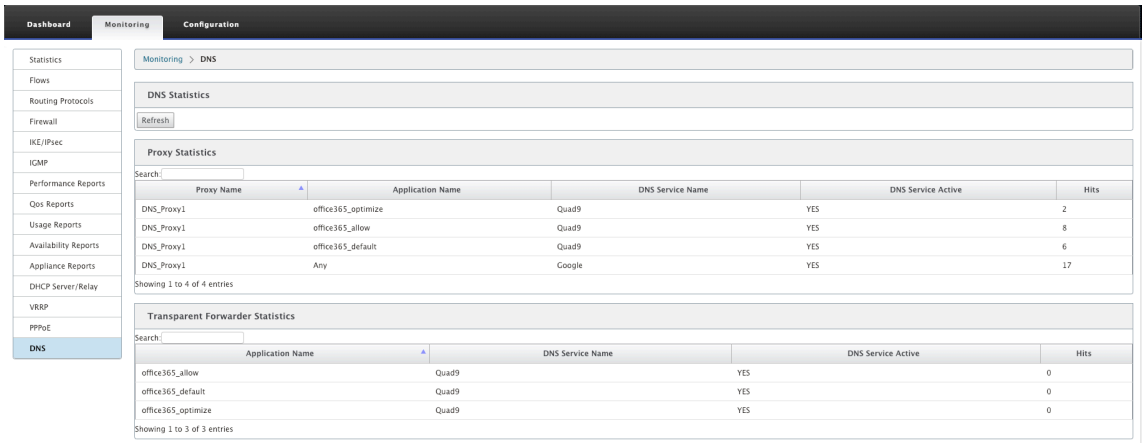


Flows Data

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
Flows
Routing Protocols
Firewall
IKE/IPsec
IGMP
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
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

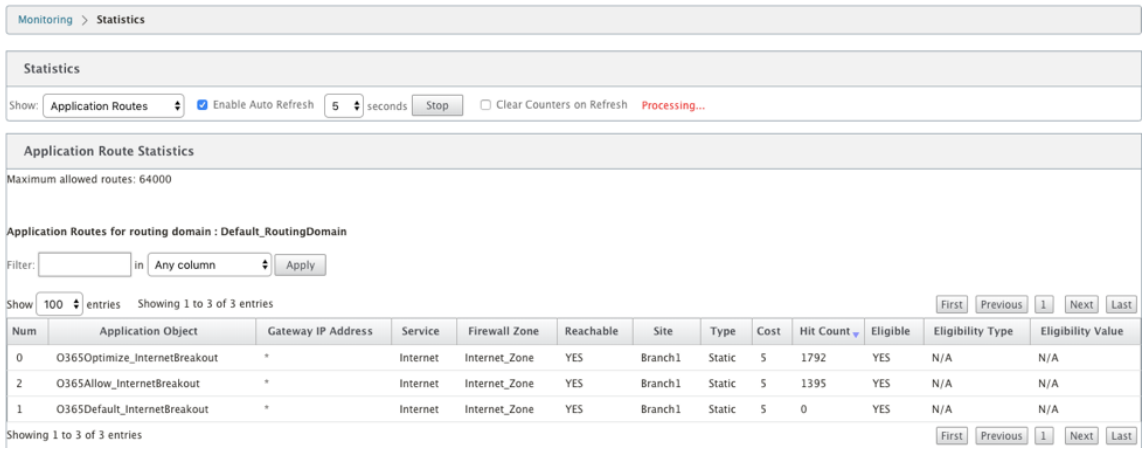
Transparent Forwarder Statistics

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 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

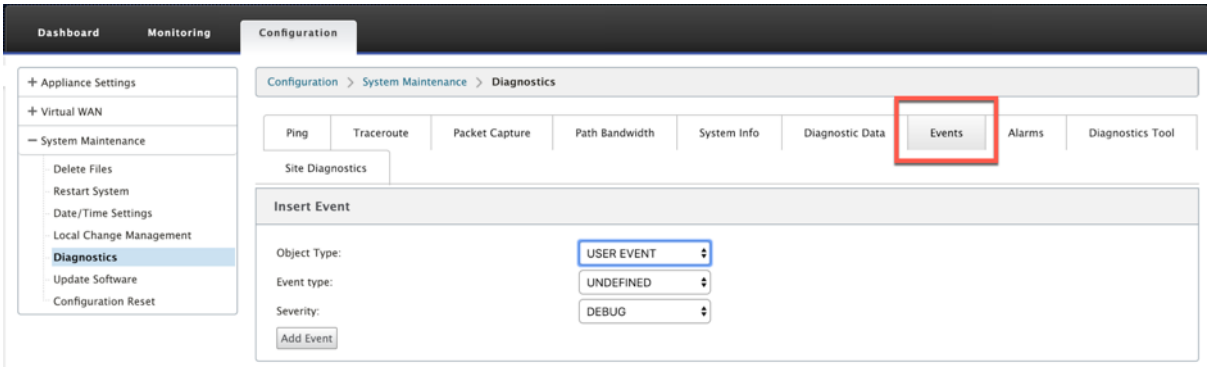
Showing 1 to 3 of 3 entries

First Previous 1 Next Last

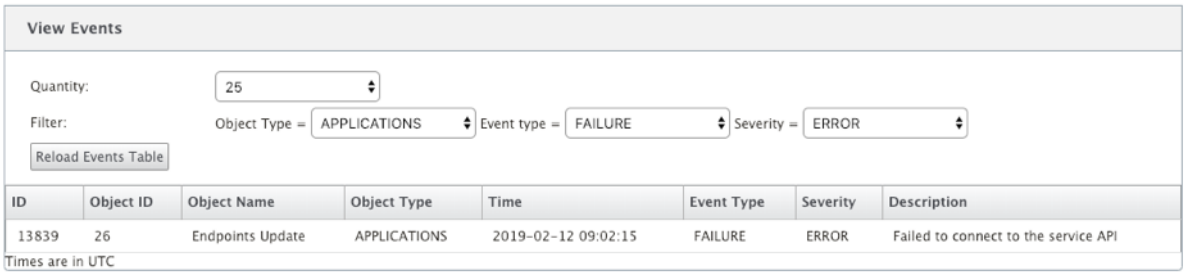
Résolution des problèmes

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**.

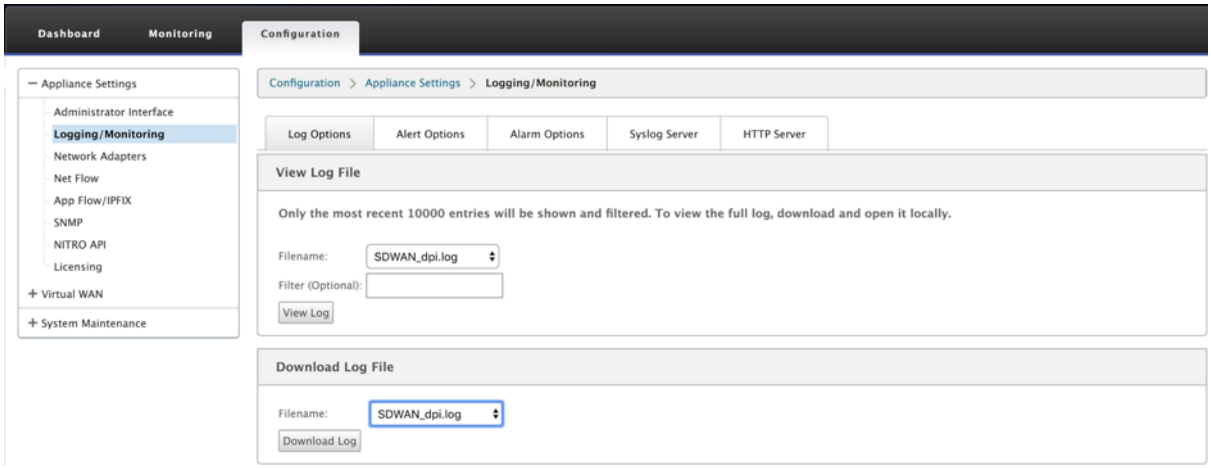


S'il y a un problème lors de la connexion au service Citrix (sdwan-app-routing.citrixnetworkapi.net), le message d'erreur se reflète sous la table **Afficher les événements**.



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

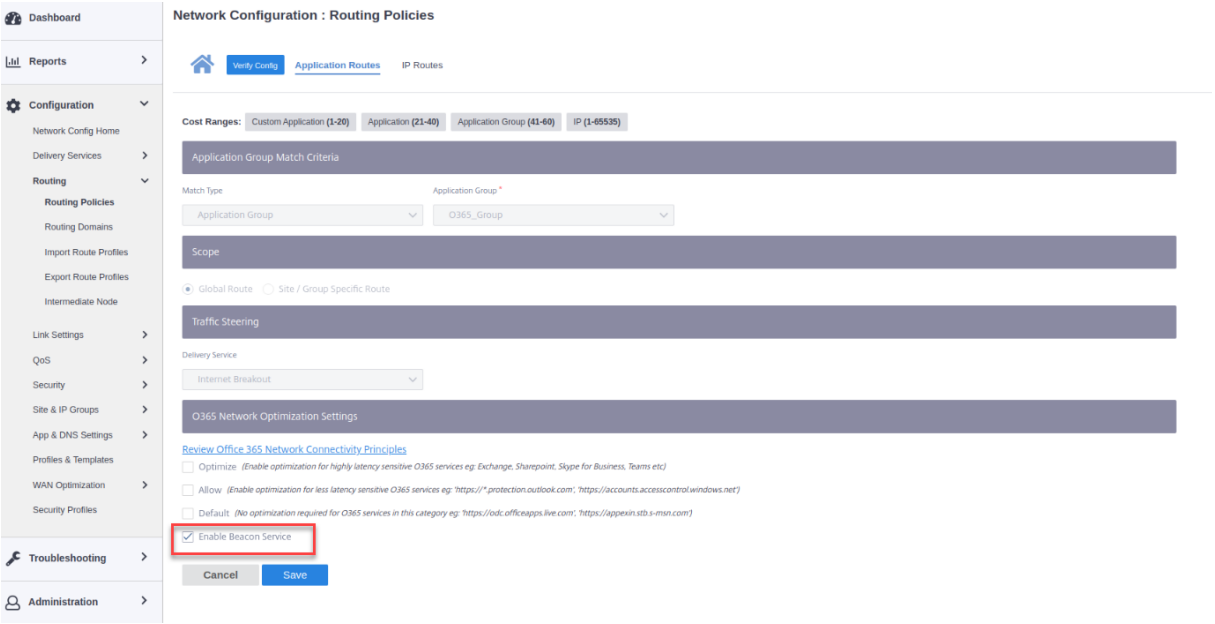
Microsoft fournit le service de balise Office 365 pour mesurer l'accessibilité d'Office 365 via les liens WAN. Le service de balise est essentiellement une URL - sdwan.measure.office.com/apc/trans.png, qui est analysée à intervalles réguliers. Le sondage est effectué sur chaque appliance pour chaque 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 liaison 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.

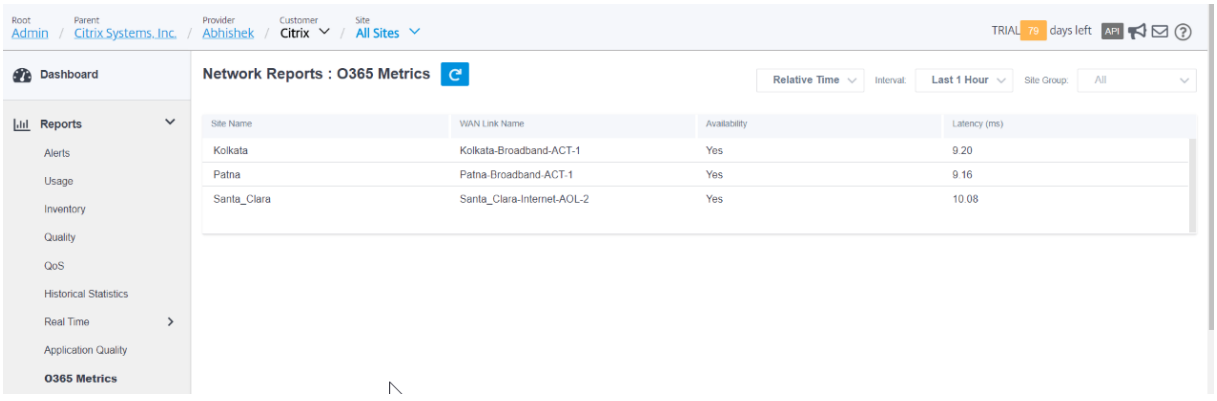
> **Remarque**
>
> L'exploration de balises Office 365 n'est pas activée sur les liens mesurés.

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.

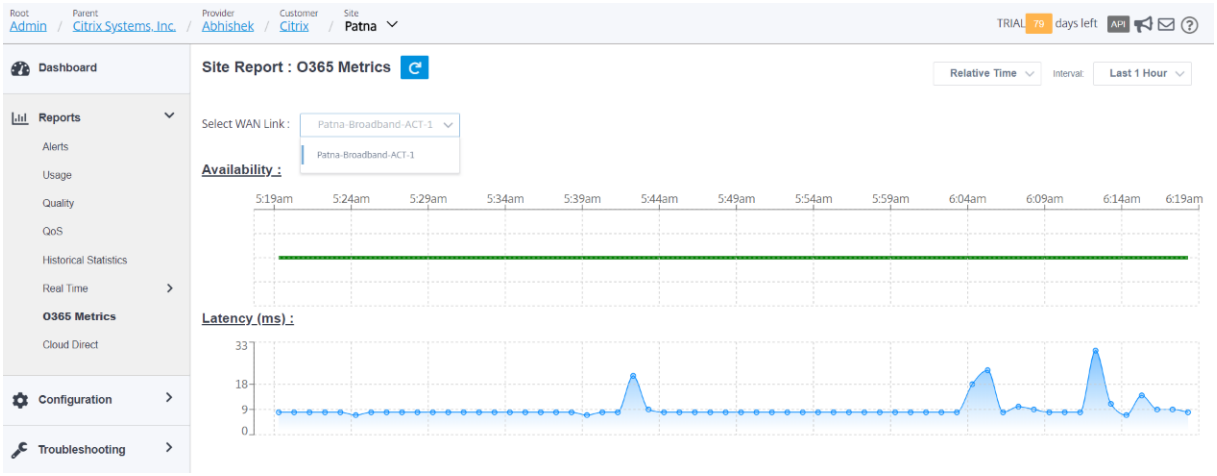
Pour désactiver le service de balise Office 365, dans SD-WAN Orchestrator, au niveau du réseau, accédez à **Configuration** > **Routage** > **Stratégies de routage** > **Paramètres d'optimisation réseau O365** et **désactivez Activer le service Beacon**.



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.

Catégories Citrix Cloud et Gateway Service

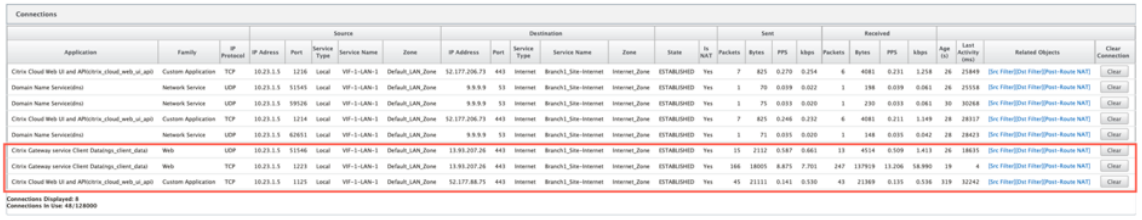
Voici les catégories de trafic utilisées à des fins de classification et d'optimisation :

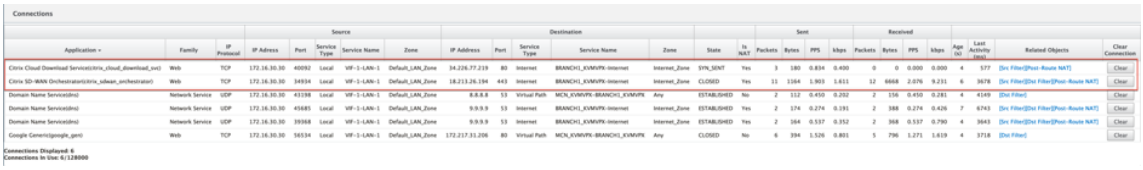
- **Citrix Cloud** : permet de détecter et d'acheminer le trafic destiné à l'interface utilisateur Web et aux API Citrix Cloud.
  - Citrix SD-WAN Orchestrator et services critiques dépendants :
    - **Citrix SD-WAN Orchestrator** : permet une sortie directe sur Internet du rythme cardiaque et d'autres 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

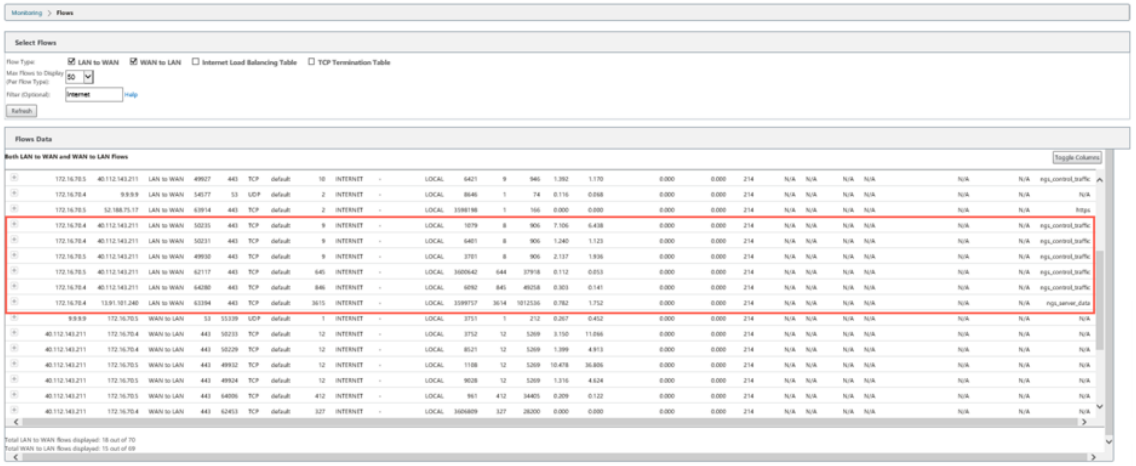
Vous pouvez surveiller les statistiques du service de passerelle dans les rapports de statistiques SD-WAN suivants :

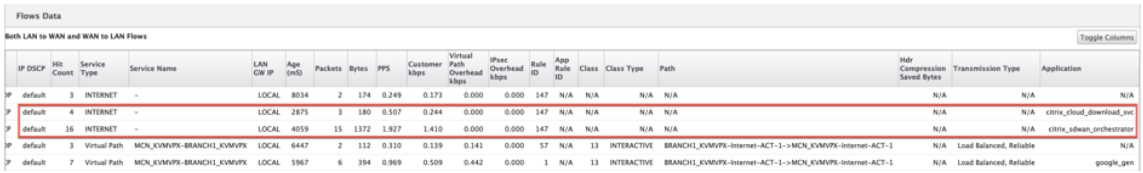
- Statistiques de pare-feu



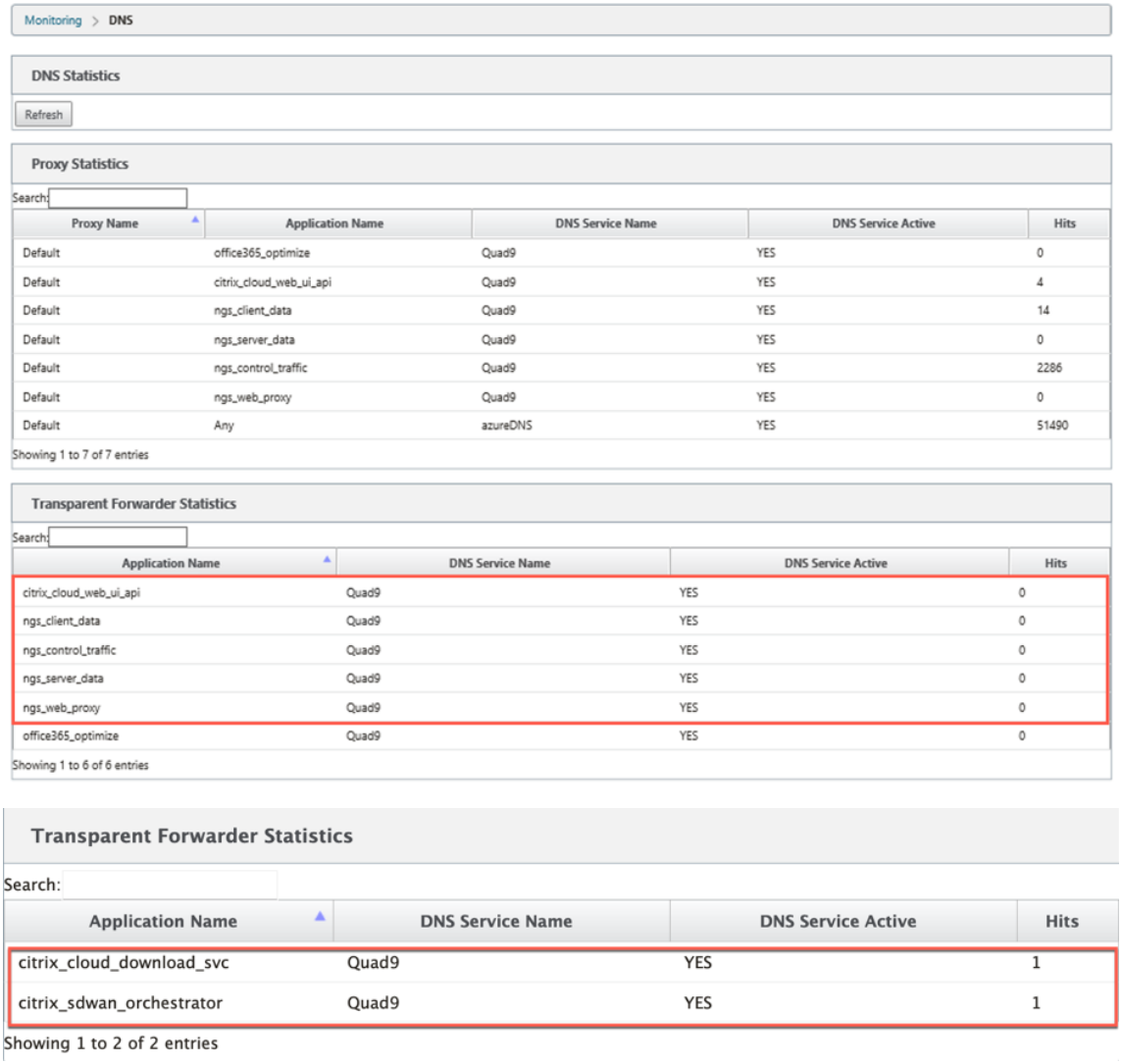


- Flux

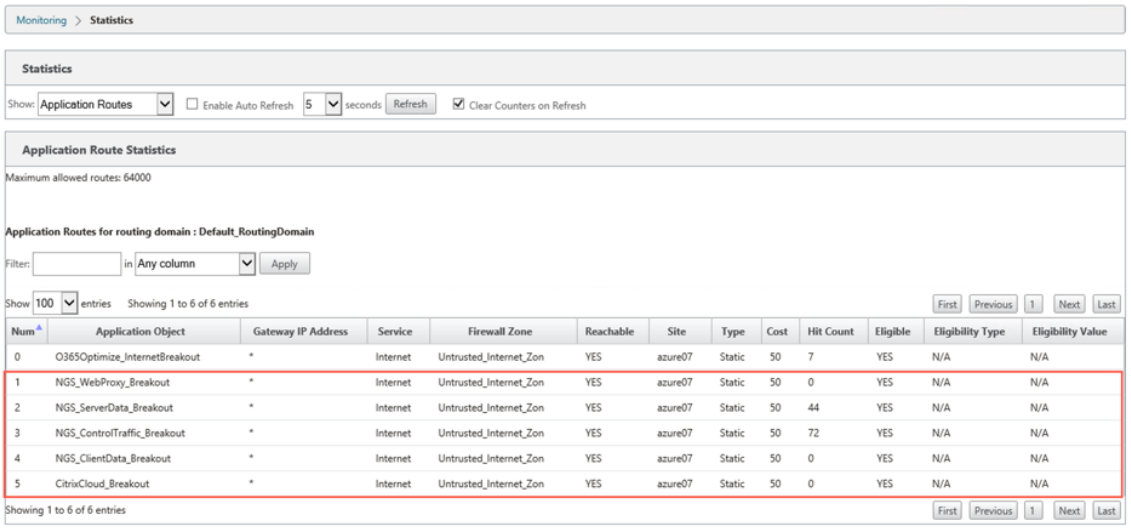


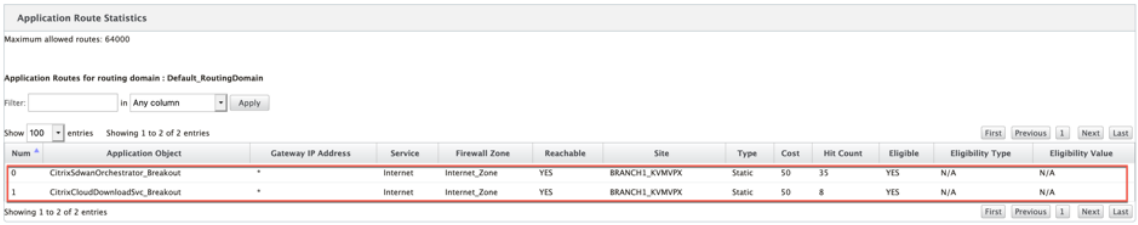


- Statistiques DNS



- Statistiques des itinéraires d'application

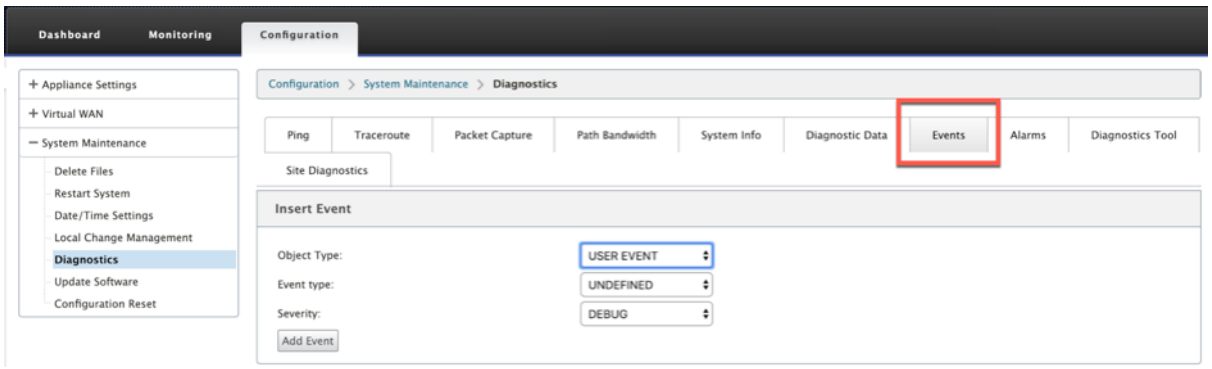




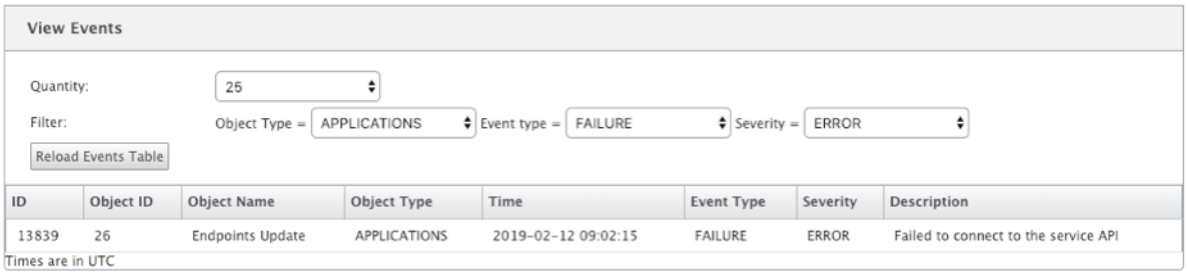
Résolution des problèmes

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**.

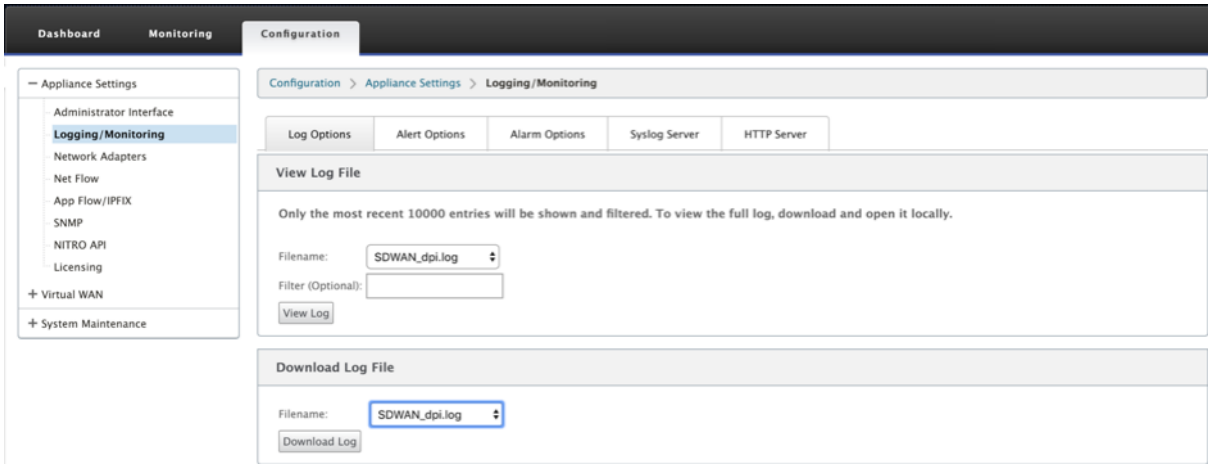


S'il y a un problème lors de la connexion au service Citrix (sdwan-app-routing.citrixnetworkapi.net), le message d'erreur se reflète sous la table **Afficher les événements**.



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** .



Sessions PPPoE

August 31, 2022

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 permettre aux fournisseurs de services Internet (FAI) d'avoir des connexions DSL continues et continues et par modem câble contrairement aux connexions commutées. PPPoE fournit à chaque session de site utilisateur distant pour apprendre les adresses réseau de l'autre par le biais d'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 sur des lignes DSL à l'aide d'Ethernet et de PPPoE.

Citrix SD-WAN agit 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 :

- Configurer l'interface réseau virtuel (VNI).
- Informations d'identification uniques pour créer une session PPPoE.
- Configurer le lien WAN. Chaque VNI ne peut avoir qu'un seul lien WAN configuré.

- 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 d'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 une adresse 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.

> **Remarque** :
>
> plusieurs VNI sont autorisés à créer avec la même balise 802.1Q >VLAN.

Limitations 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.
- Dégonfler la compression.
- Négociation de compression de champ de protocole
- Protocole de contrôle de compression.
- Compression BSD Compresser.
- Protocoles IPX.
- PPP Multi-Link.
- Compression d'en-tête TCP/IP de style Van Jacobson.
- Option de compression de l'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.

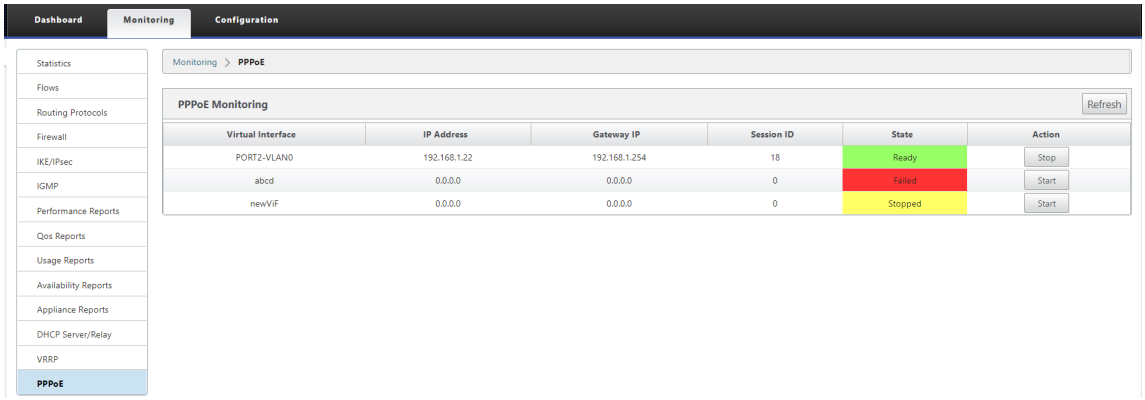
Pour plus d'informations sur la configuration de PPPoE via le service Citrix SD-WAN Orchestrator, consultez Interfaces.

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 et d'arrêter manuellement les sessions à des fins de dépannage à partir du service Citrix SD-WAN Orchestrator.

- Si le VNI est opérationnel et prêt, les colonnes **IP et IP de 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.



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.
Numérotation	Jaune	Une fois qu'un VNI est configuré, l'état de la 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
Session	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 VNI et le lien WAN associé sont prêts à l'emploi.
Échec	rouge	La session PPP/PPPoE est terminée. La raison de l'échec peut être due à une configuration non valide 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	Un état intermédiaire se terminant pour 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, lorsqu'il y a un problème lors de l'établissement d'une session PPPoE :

- Le pointeur de la souris sur l'état Échec indique la raison de l'échec récent.
- Pour créer 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'est pas démarrée manuellement et qu'une modification de configuration n'est pas activée, ou que le service n'est pas 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 d'AC ou nom de service incorrect).
- Échec de l'ouverture du port série en raison d'une erreur du système d'exploitation.
- Aucune réponse reçue pour les paquets echo (le lien est mauvais ou le serveur ne répond pas).
- Il y a eu plusieurs sessions de numérotation infructueuses continues avec en une minute.

Après 10 échecs consécutifs, la raison de l'échec est observée.

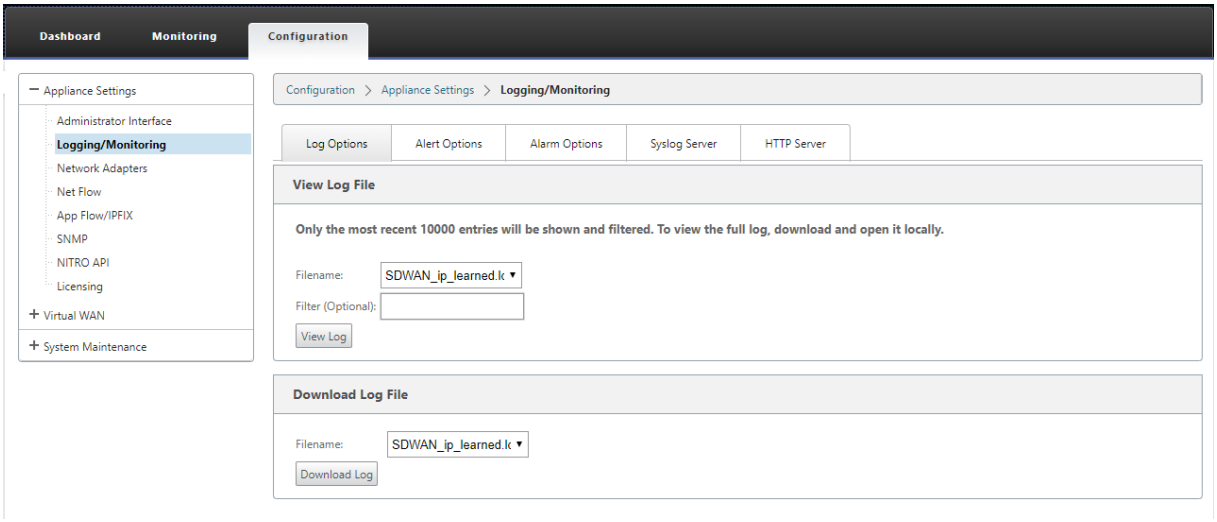
- Si l'échec est normal, il redémarre immédiatement.
- Si l'échec est une erreur, le redémarrage revient pendant 10 secondes.
- Si l'échec est fatal, le redémarrage revient pendant 30 secondes avant le redémarrage.

Les paquets de requête LCP Echo sont générés à partir du SD-WAN toutes les 60 secondes et le défaut de recevoir 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 du matériel** > **Journalisation/surveillance** > **Options de 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.

À partir de la version SD-WAN 11.5, les fonctionnalités QoS sont configurables via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Qualité de service.

Classes

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.

Le service Citrix SD-WAN Orchestrator prend en charge 13 classes. Pour plus d'informations, consultez la section Classes.

Voici les différents types de classes :

- Temps**réel** : utilisé pour un trafic à faible latence, à faible bande passante et soumis à des contraintes de 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 faibles à moyennes et des exigences de bande passante faibles à moyennes. 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'interférence 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.

Règles par adresse IP et numéro de port

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)".

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.

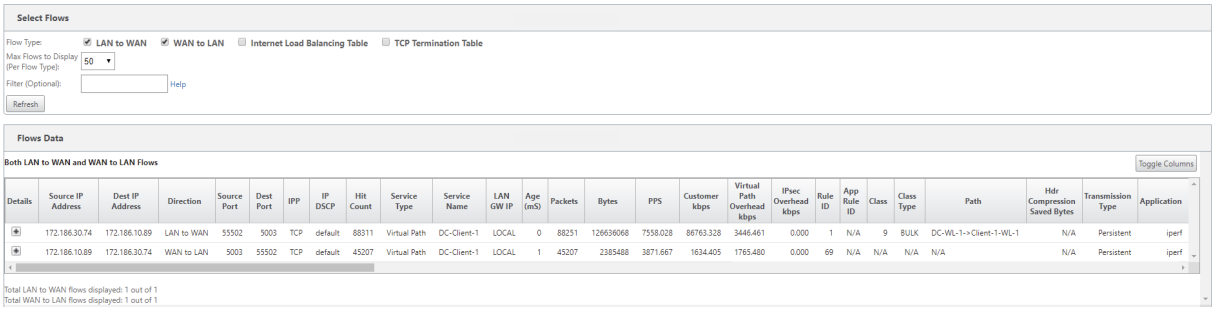
À partir de la version 11.5 de Citrix SD-WAN, vous pouvez créer des règles IP à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Règles IP.

Vérifier les règles

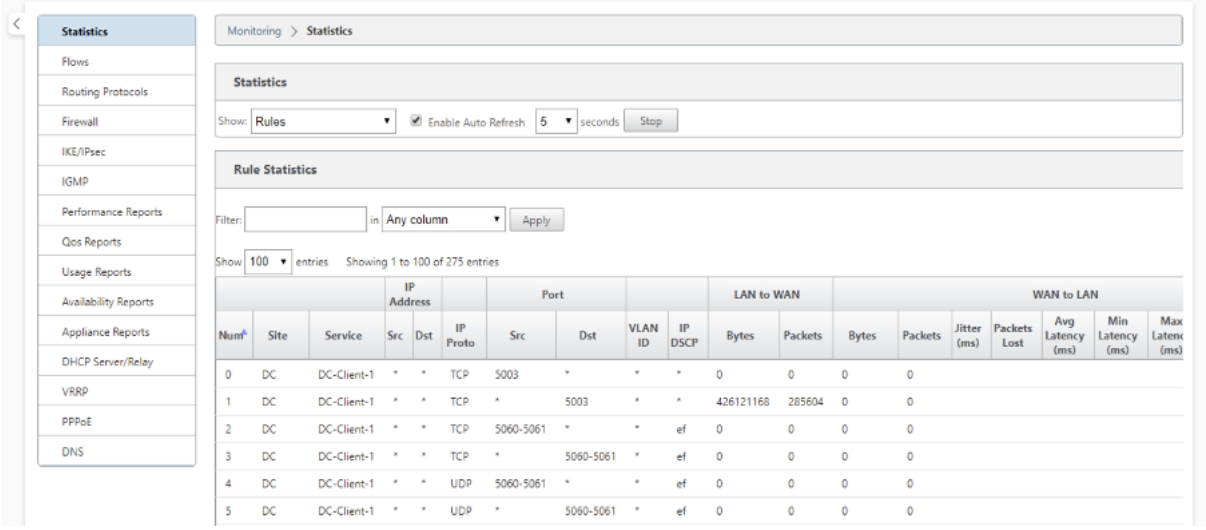
Accédez à **Surveillance > Flux**. Sélectionnez le champ **Type de flux** situé dans la section **Sélectionner des flux** en haut de la page **Flux**. En regard du champ **Type de flux**, une ligne de cases à cocher permet de sélectionner les informations de flux que vous souhaitez afficher. Vérifiez 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.



Accédez à **Surveillance > Statistiques** et vérifiez les règles configurées.



Règles par nom d'application

La fonctionnalité de classification des applications permet à l'appliance Citrix SD-WAN d'analyser le trafic entrant et de le classer comme appartenant à une application ou 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'applications, de familles d'applications ou d'objets 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 IP, consultez Règles par adresse IP et numéro de port.

Pour chaque règle d'application, vous pouvez spécifier le mode de transmission. Les modes de transmission disponibles sont les suivants :

- **Chemin d'équilibrage de charge** : le trafic applicatif du 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 de l'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 :

Rule	Classe	Mode de transmission	Retransmettre les paquets perdus	Activer la mise en réception de paquets	Activer le réséquençage des paquets	Temps de blocage de la réséquence (ms)	Rejeter les paquets de réséquence tardif	Limite de charge (ms)	Profondeur de dépôt (octets)	Activer RED	Désactiver la limite (ms)	Désactiver la profondeur (octets)
HDX_Priority_0 (HDX_priority_tag_0)	0	Chemin équilibrage de charge	Vrai	Faux	Vrai	250	Vrai	350	30000	Vrai	0	128000
HDX_Priority_1 (HDX_priority_tag_1)	1	Chemin équilibrage de charge	Vrai	Faux	Vrai	250	Vrai	350	30000	Vrai	0	128000
HDX_Priority_2 (HDX_priority_tag_2)	2	Chemin équilibrage de charge	Vrai	Faux	Vrai	250	Vrai	350	30000	Vrai	0	128000

Rule	Classe	Mode de transmission	Retransmettre les paquets perdus	Activer l'atténuation de paquets	Activer le réséquençage des paquets	Temps de blocage de la réséquence (ms)	Rejeter les paquets de réséquence tardif	Limite de charge (ms)	Profondeur de dépôt (octets)	Activer RED	Désactiver la limite (ms)	Désactiver la profondeur (octets)
HDX_Priority_3 (HDX_priority_tag_3)	3	Chemin d'équilibrage de charge	Vrai	Faux	Vrai	250	Vrai	350	30000	Vrai	0	128000
HDX	11 (interactive_high_class)	Chemin d'équilibrage de charge	Vrai	Faux	Vrai	250	Vrai	350	30000	Vrai	0	128000

Comment les règles d'application sont appliquées ?

Dans le réseau SD-WAN, lorsque les paquets entrants atteignent l'appliance SD-WAN, les quelques paquets initiaux ne subissent pas la classification DPI. 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.

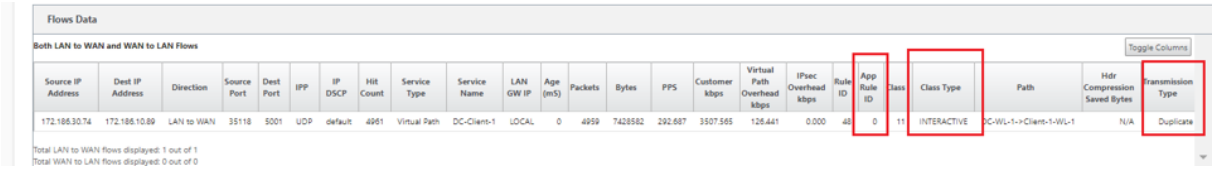
Les règles IP ont plus d'attributs que les règles d'application. La règle d'application remplace seulement quelques attributs de règle IP, le reste des attributs de règle IP reste traité sur les paquets.

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. L'ensemble 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.

Pour créer des règles d'application à l'aide de Citrix SD-WAN Orchestrator, consultez la section Règles d'application.

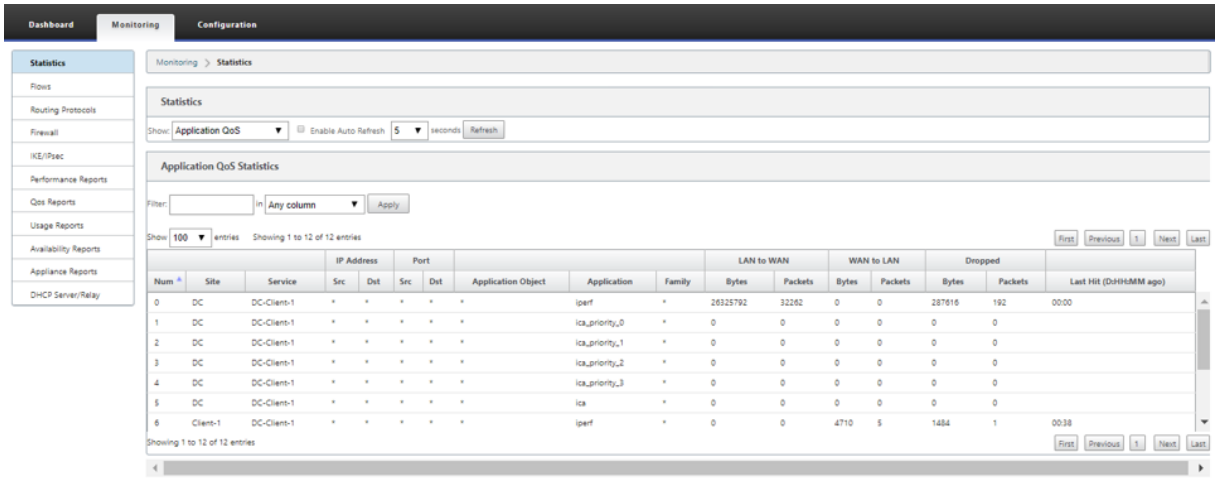
Pour vérifier si les règles d'application sont appliquées au flux de trafic, accédez à **Surveillance** > **Flux**.

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.



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 d'application. Vérifiez l'identifiant de la règle d'application obtenu à partir du flux.



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 en tant qu'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.

Classification des demandes

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 DPI sur le service Citrix SD-WAN Orchestrator, consultez la section Classification des bibliothèques DPI.

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 transmis via SSL/TLS ou DTLS n'est pas prise en charge dans SD-WAN Standard 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'appliance 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 Multi-Stream ICA fonctionne correctement, vous devez disposer du SD-WAN Standard Edition 10.1 ou supérieur.
- Pour que les rapports basés sur les utilisateurs HDX soient affichés sur SDWAN-Center, vous devez disposer de SD-WAN Standard 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 multiflux 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_prority_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 sur le service Citrix SD-WAN Orchestrator, consultez la section Classification 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 des noms de domaine sur le service Citrix SD-WAN Orchestrator, consultez la section Classification des applications basée sur le nom de domaine.

> **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.
> - À partir de la version 11.5.0 de Citrix SD-WAN, les enregistrements AAAA sont pris en charge sur le service Citrix SD-WAN Orchestrator.

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 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'appliance 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.

Objets d'application

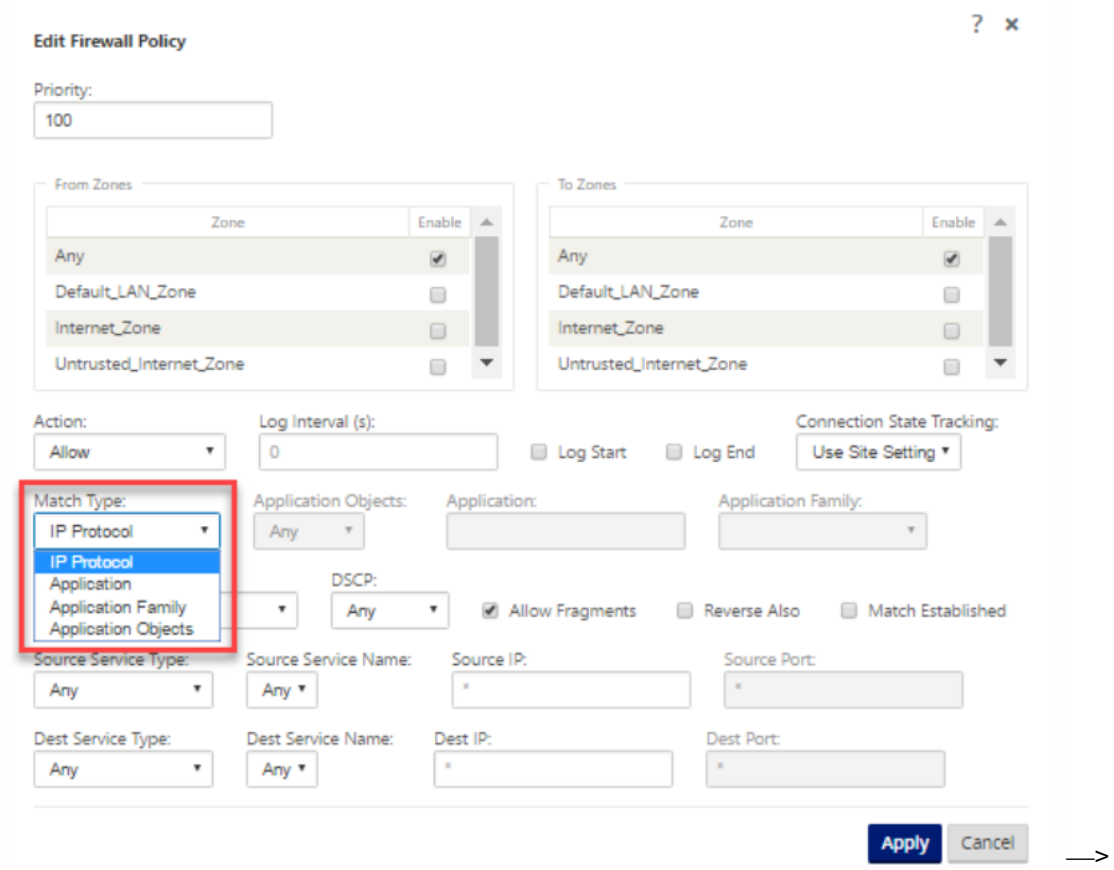
Les objets d'application vous permettent de regrouper différents types de critères de correspondance en un seul objet qui peut être utilisé dans les stratégies de pare-feu et la direction d'application. Le protocole IP, l'application et la famille d'applications sont les types de correspondance disponibles.

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

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.

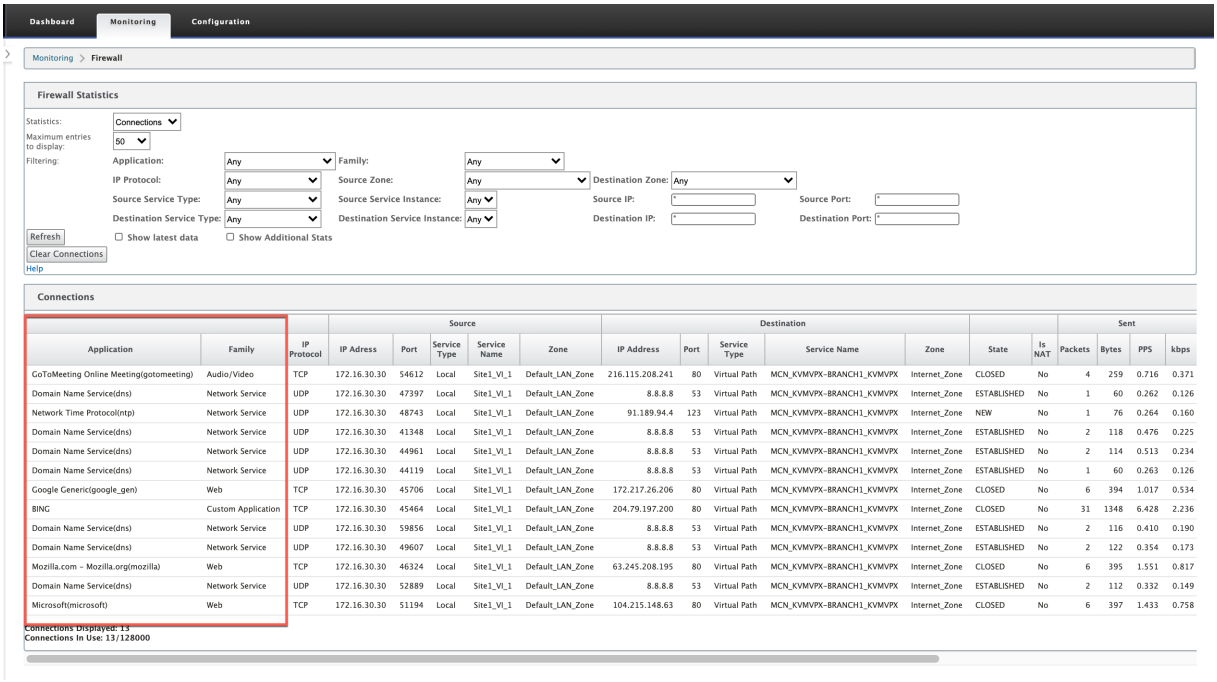


Affichage de la classification des applications

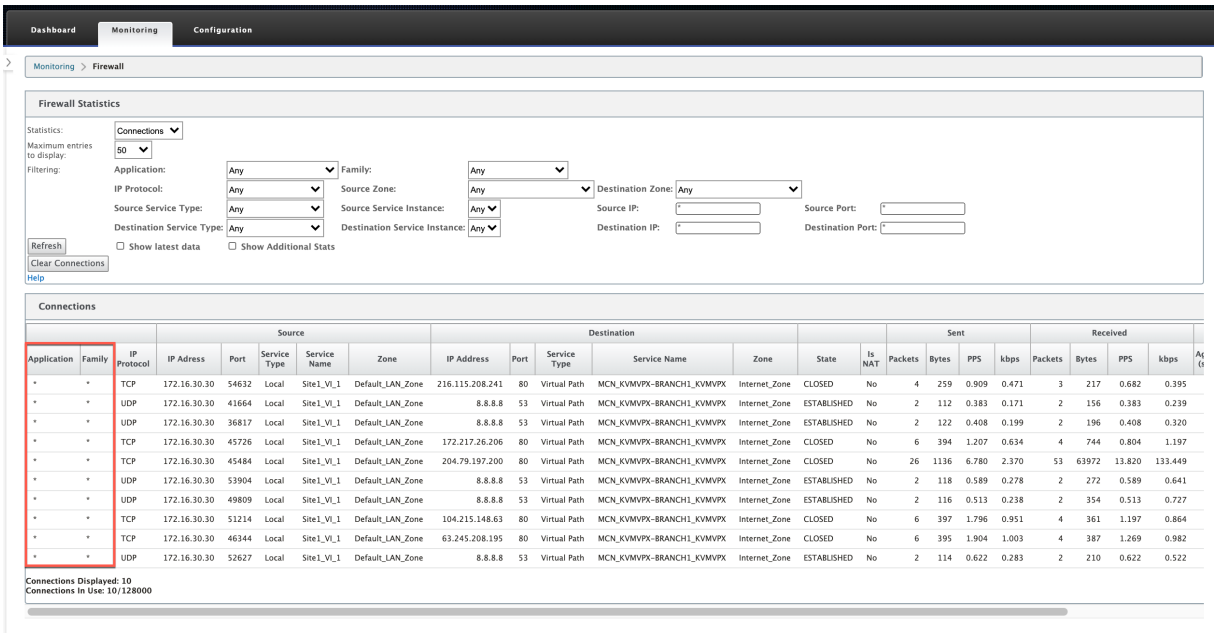
Après avoir activé la classification de l'application, vous pouvez afficher le nom de l'application et les détails de la famille d'applications dans les rapports suivants :

- Statistiques de connexion au pare-feu
- Informations sur les flux
- Statistiques relatives aux applications

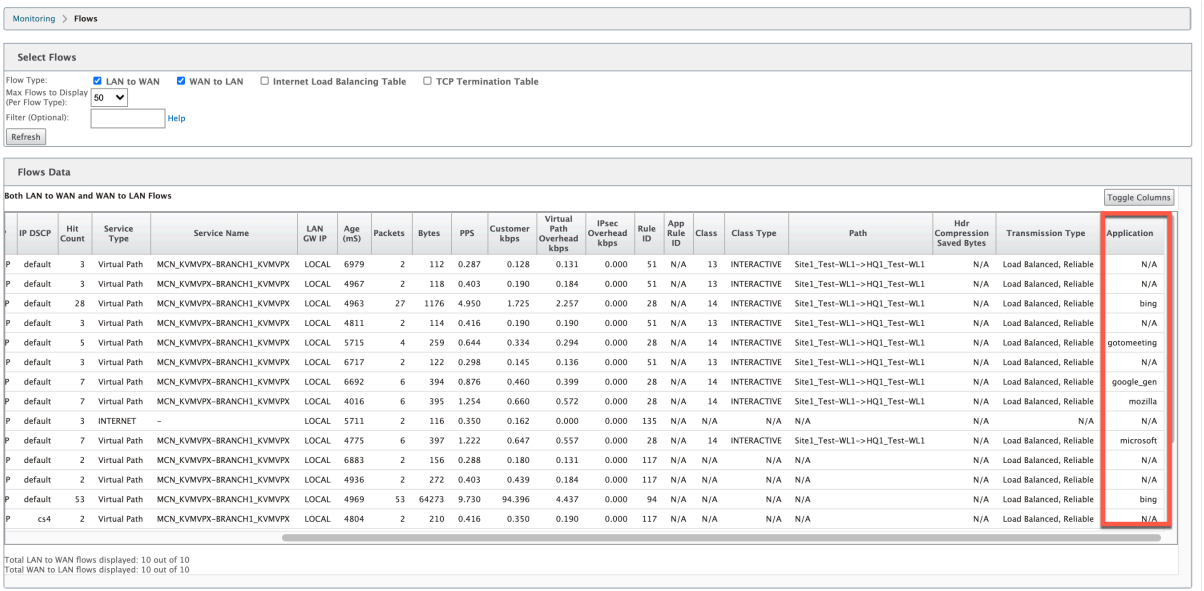
Statistiques de connexion au pare-feu Accédez à **Surveillance > Pare-feu**. Sous la section **Connexions**, les colonnes **Application** et **Famille** répertorient les applications et la famille associée.



Si vous n'activez pas la classification des applications, les colonnes **Application** et **Famille** n'affichent aucune donnée.



Informations sur les flux Accédez à **Surveillance > Flux**. Sous la section **Données de flux**, la colonne **Application** répertorie les détails de l'application.



Statistiques relatives aux applications Accédez à **Surveillance > Statistiques**. Sous la section **Statistiques d'application**, la colonne **Application** répertorie les détails de l'application.

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)

La fonction d'équité QoS améliore l'équité de plusieurs flux de chemins virtuels en utilisant des classes QoS et la détection précoce aléatoire (RED). Un chemin virtuel peut être attribué à l'une des 16 classes différentes. Une classe peut être l'un des trois types de base suivants :

- Les classes en temps réel servent les 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 en temps réel, mais ont une priorité absolue sur le trafic en masse.

- 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 masse.

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 Hierarchical Fair Service Curve (HFSC) pour atteindre l'équité entre les classes.

Classes de services HFSC dans l'ordre du 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 supprimés au lieu d'être mis dans la file d'attente (queue abandonnée).

Pourquoi TCP provoque-t-il la mise en file d'attente ?

TCP ne peut pas contrôler la rapidité avec laquelle le réseau peut transmettre des données. Pour contrôler la bande passante, TCP implémente le concept d'une fenêtre de bande passante, c'est-à-dire la quantité de trafic non reconnu qu'il autorise dans le réseau. Il commence initialement 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 du réseau en détectant les paquets abandonnés. 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 peut 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 paquet est détectée, et augmente la bande passante autorisée d'un paquet pour chaque accusé de réception. TCP alterne donc entre la pression ascendante sur la bande passante et la sauvegarde. Malheureusement, si le temps d'attente atteint 800 ms au moment où la perte de paquet est détectée, la réduction de la bande passante entraîne un retard de transmission.

Impact sur l'équité QoS

En cas de retard de transmission TCP, fournir n'importe quel type de garantie d'équité au sein d'une classe de chemin virtuel est difficile. Le planificateur de chemins virtuels doit appliquer un comportement de chute de queue pour éviter de contenir d'énormes quantités de trafic. La nature des connexions TCP est telle qu'un petit nombre de trafic circule pour remplir le chemin virtuel, ce qui rend difficile pour une nouvelle connexion TCP d'obtenir une part équitable de la bande passante. Le partage équitable 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 de provoquer des actions de dépose de queue. 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.

Pour plus d'informations sur l'utilisation et l'activation de RED, consultez Comment utiliser RED.

Files d'attente MPLS

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'un lien WAN. Chaque liaison WAN nécessitait une adresse IP virtuelle (VIP) unique pour créer le lien WAN et une balise DSCP (Differentiated Services Code Point) unique correspondant au schéma de mise en file d'attente du fournisseur. Après avoir défini un lien 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. Pour plus d'informations sur la configuration de MPLS à l'aide du service Citrix SD-WAN Orchestrator, consultez Files d'attente MPLS.

> **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.

Affecter un groupe de chemin automatique au lien de chemin d'accès WAN virtuel

Le groupe de chemin automatique défini est le même pour le MCN et le dispositif client. Cela permet au système de créer automatiquement les chemins. Sur le site MCN, vous pouvez également développer le lien WAN associé au chemin virtuel.

Afficher le taux et la congestion autorisés pour les liaisons WAN

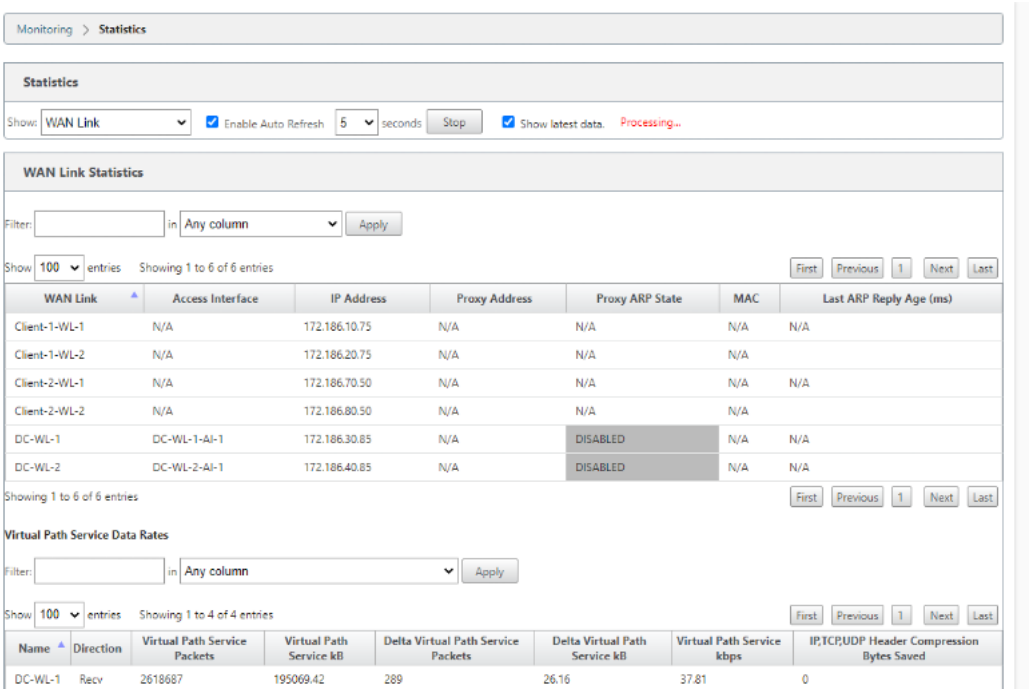
L'interface Web SD-WAN vous permet désormais d'afficher le taux autorisé pour les utilisations des liaisons WAN et WAN et de savoir si un lien WAN, un chemin ou un chemin virtuel est encombré. Dans les versions précédentes, ces informations n'étaient disponibles que dans les fichiers journaux SD-WAN

et via l'interface de ligne de commande. Ces options sont maintenant disponibles dans l'interface Web pour faciliter le dépannage.

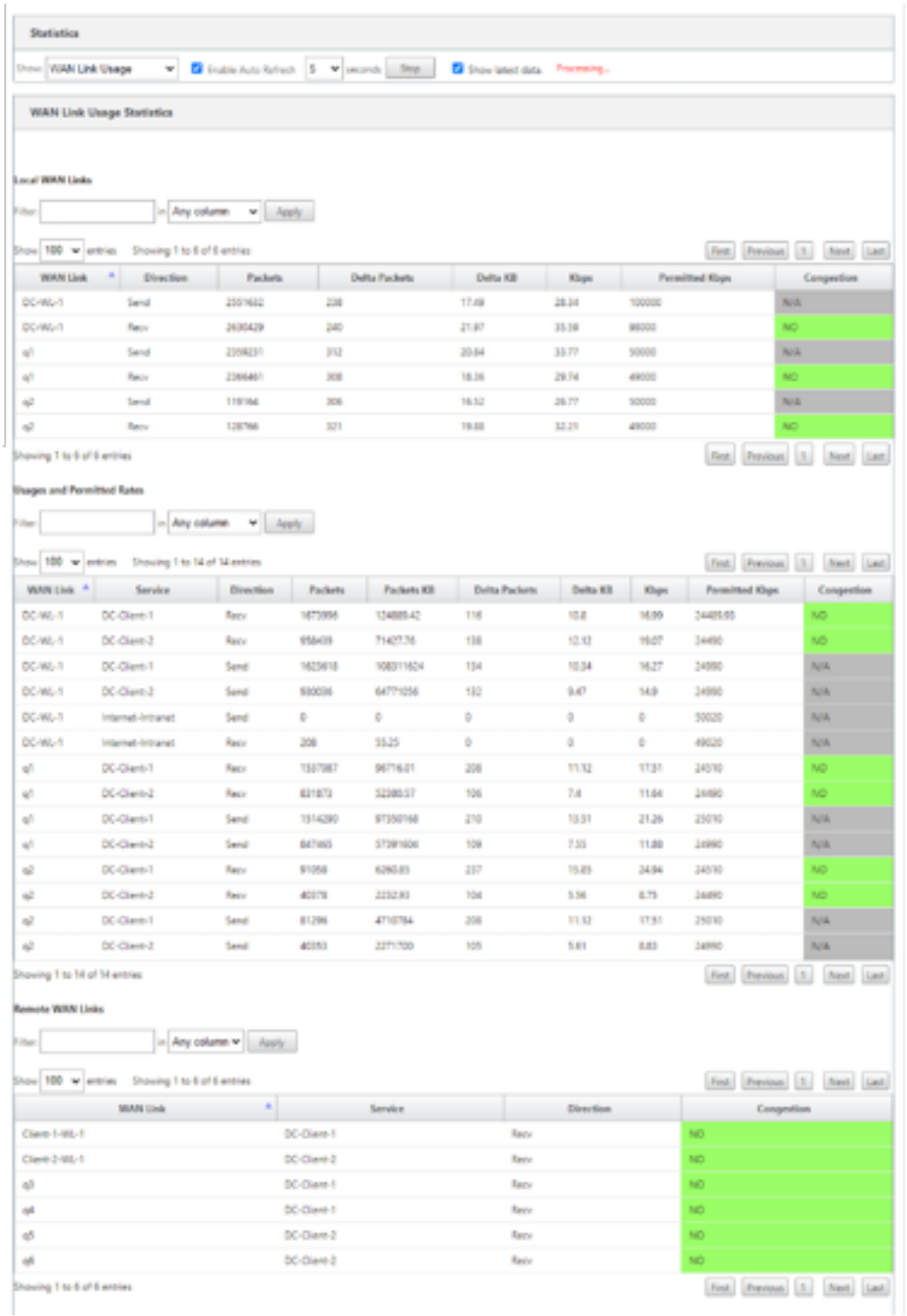
Afficher le tarif autorisé Taux autorisé est la quantité de bande passante qu'un lien WAN, un service de chemin virtuel, un service intranet ou un service Internet particulier est autorisé à utiliser à un moment donné dans le temps. Le débit autorisé pour une liaison WAN est statique et est défini explicitement 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 fonction de la congestion, de la demande des utilisateurs et des partages équitables, 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** .

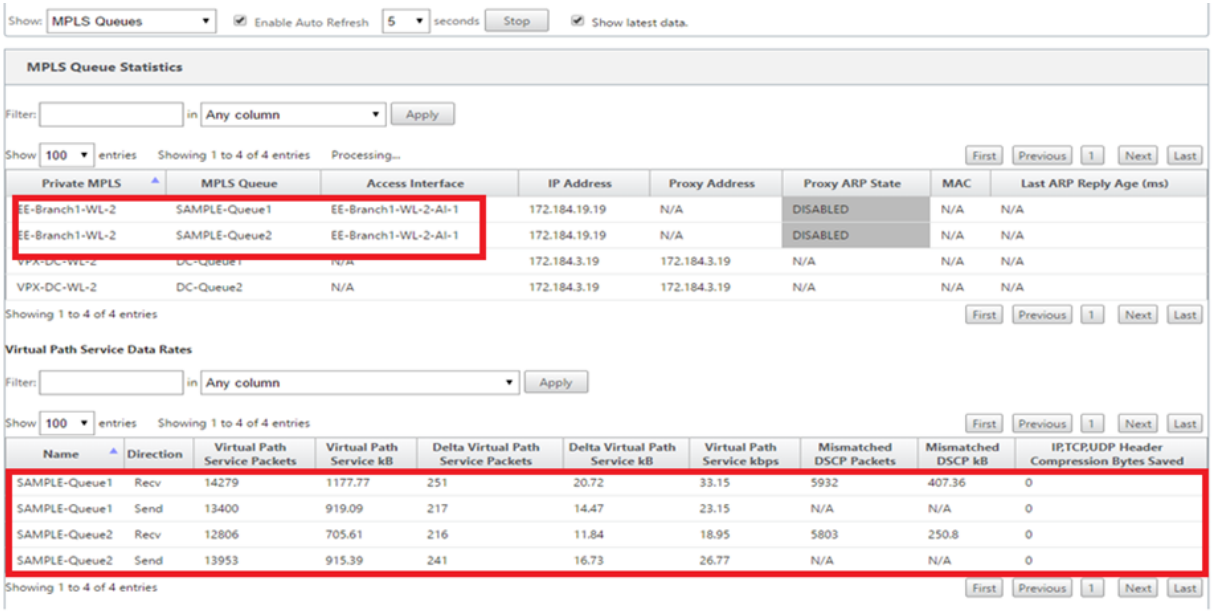


Accédez à **Moniteur > Statistiques**, puis sélectionnez **Utilisation du lien WAN** dans la liste déroulante **Afficher** .



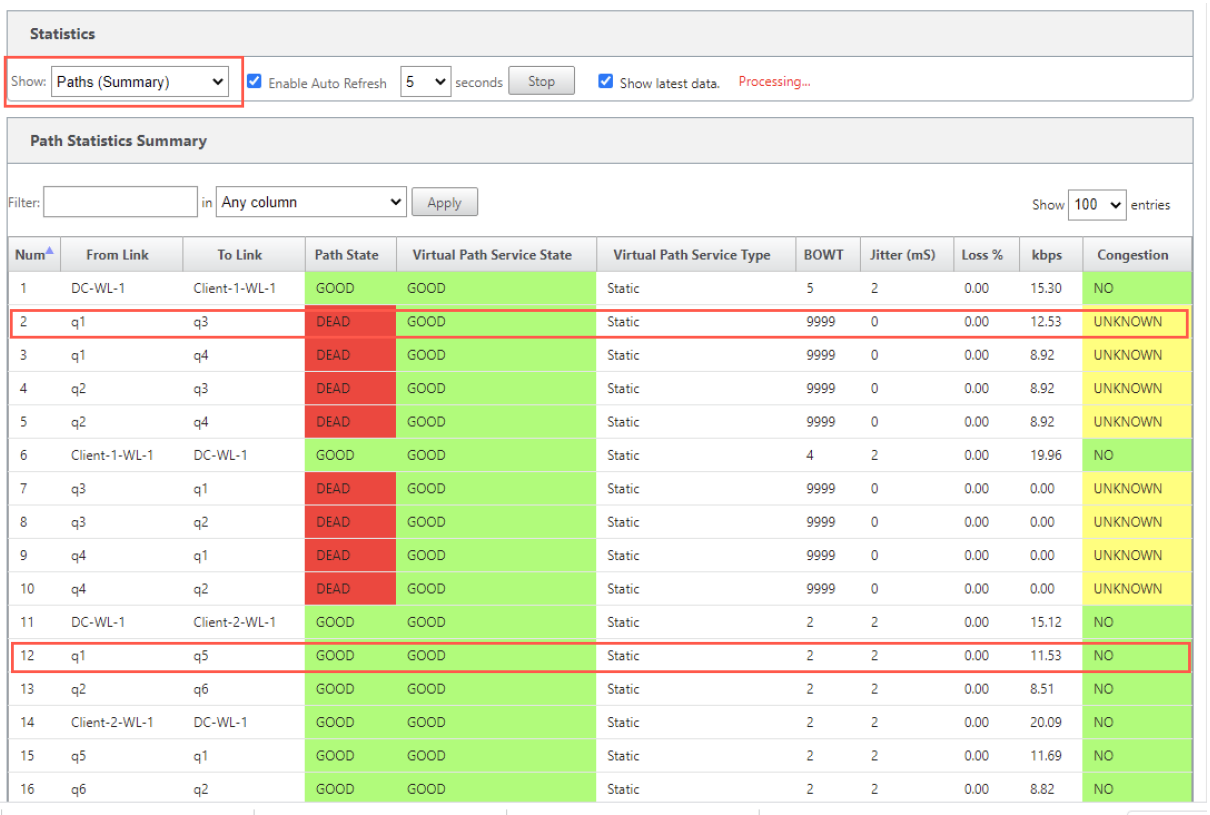
Surveillance des files d'attente MPLS

Accédez à **Moniteur Statistiques**, puis sélectionnez Files d'**attente MPLS** dans la liste déroulante **Afficher**.



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.

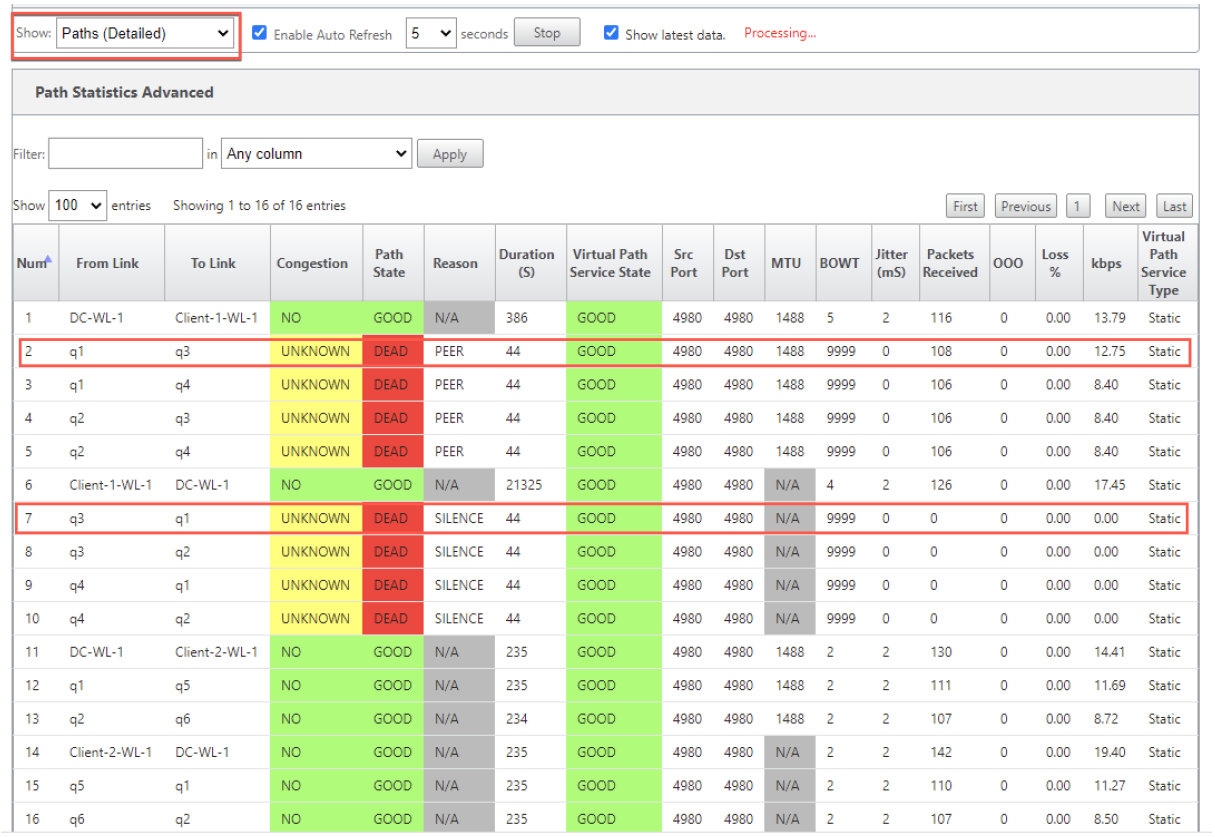


Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	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 (Détaillés)** 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 signalement que le chemin est BAD



Show: Paths (Detailed) | Enable Auto Refresh 5 seconds | Stop | Show latest data. Processing...

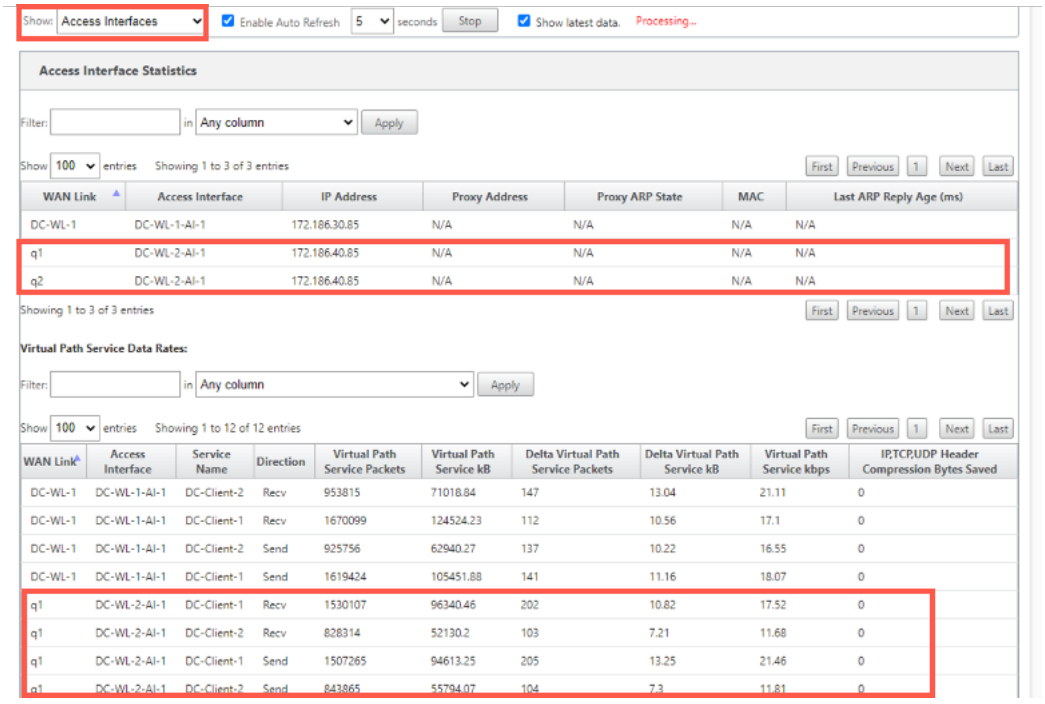
Path Statistics Advanced

Filter: in Any column | Apply

Show 100 entries Showing 1 to 16 of 16 entries | First | Previous | 1 | Next | Last

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 | First | Previous | 1 | Next | Last

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 | First | Previous | 1 | Next | Last

Virtual Path Service Data Rates:

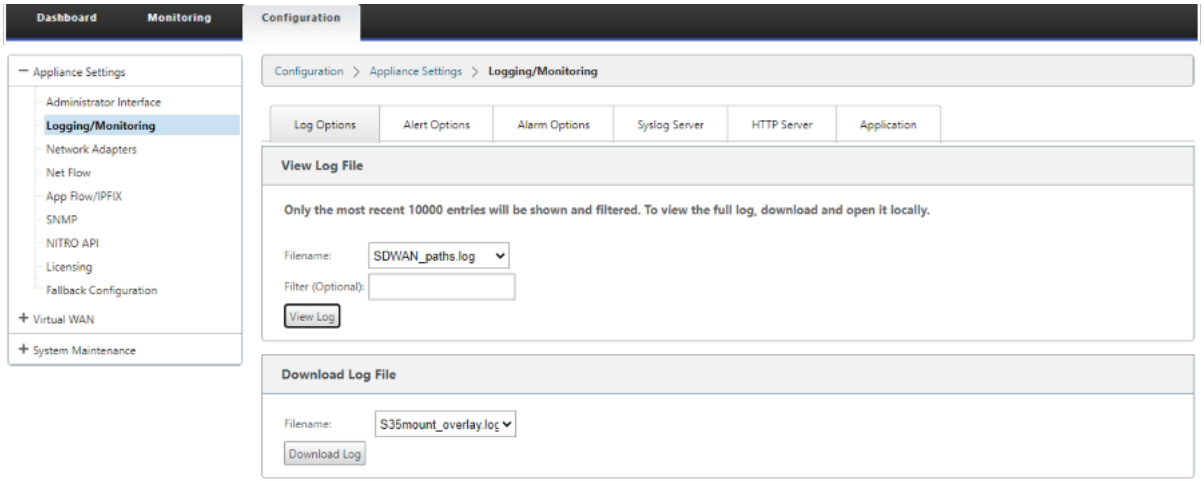
Filter: in Any column | Apply

Show 100 entries Showing 1 to 12 of 12 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
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	11.81	0

Vous pouvez télécharger les fichiers journaux pour un dépannage ultérieur. Accédez à **Configura-**

tion > Logging/Monitoring et sélectionnez **SDWAN_paths.log** ou **SDWAN_common.log** dans l'onglet **Options du journal**.



Rapports

November 16, 2022

QoE des applications

La**QoE des applications** est une mesure de la qualité d'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 se trouve détermine la qualité d'une application.

Qualité	Gamme
Good	8–10
Fair	4–8
Poor	0–4

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, et mapper ces profils avec des applications ou des objets d'applications.

> **Remarque**
>
> Pour surveiller la QoE des applications, il est essentiel d'activer l'inspection approfondie des paquets. Pour plus d'informations, consultez la section Classification des applications.

QoE des applications en temps réel

Le calcul de la QoE des applications en temps réel utilise une technique innovante Citrix, 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.

> **Remarque**
>
> La valeur QoE peut être égale à zéro si les conditions du réseau sont en dehors des seuils configurés pour le trafic en temps réel.

Application interactive QoE

La QoE des applications pour les applications interactives utilise une technique innovante Citrix basée sur les seuils de perte de paquets et de taux de rafale.

Les applications interactives sont sensibles à la perte de paquets et au débit. 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 :

- Pourcentage de perte de paquets.

- Pourcentage du taux d'éclatement prévu par rapport au taux d'éclatement d'entrée.

Les valeurs de seuil par défaut sont les suivantes :

- Seuil de perte de paquets : 1%
- Taux d'éclatement : 60%

Un flux est de bonne qualité si les conditions suivantes sont remplies :

- Le pourcentage de perte pour un flux est inférieur au seuil configuré.
- Le taux de rafale de sortie est au moins le pourcentage configuré du taux de rafale 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 un trafic interactif en temps réel et mapper jusqu'à 10 applications ou objets d'application avec des profils QoE.

Pour créer des profils QoE personnalisés via le service Citrix SD-WAN Orchestrator, consultez la section Profils QoE des applications.

QoE HDX

Les paramètres réseau tels que la latence, la gigue et la perte de paquets affectent l'expérience utilisateur des utilisateurs HDX. La qualité d'expérience (QoE) est introduite 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 ajuster les règles et la stratégie pour améliorer la QoE.

La QoE est une valeur numérique comprise entre 0 et 100, plus la valeur est élevée, plus l'expérience utilisateur est bonne. 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
Good	80–100
Fair	50–80
Poor	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 plus d'informations sur la configuration de HDX QoE à l'aide du service Citrix SD-WAN Orchestrator, consultez Tableau de bord et rapports HDX.

> **Remarque**
>
> - *Ne vous attendez pas à ce que la latence, la gigue et la perte de paquets de liaison WAN correspondent toujours à la latence, à la gigue et à la perte de paquets de l'application. La perte de liaison WAN est corrélée à la perte réelle de paquets WAN, tandis que la perte d'application survient après la retransmission, ce qui est inférieur à la perte de liaison WAN.*
> - *La latence de liaison WAN affichée dans l'interface graphique est BOWT (Best One Way Time). Il s'agit des meilleures mesures du lien comme un moyen de mesurer l'état du lien. La QoE de l'application suit et calcule la latence totale et moyenne de tous les paquets de cette application. Souvent, cela ne correspond pas au lien BOWT.*
> - *Lorsqu'une session MSI démarre, pendant l'établissement de liaison ICA, la session peut être temporairement comptée comme 4 SSI 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 SSI.*
> - *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.*

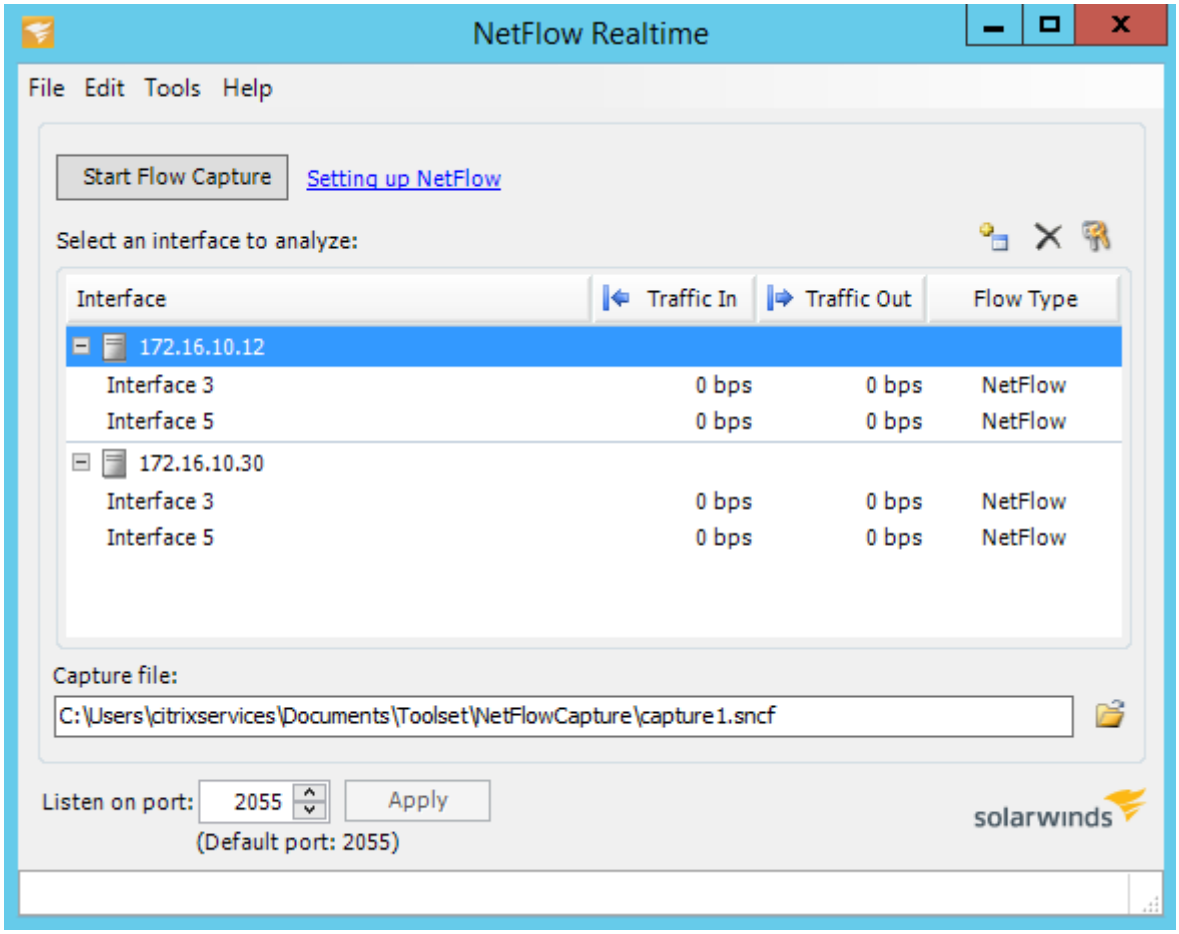
Collecteurs de flux net multiples

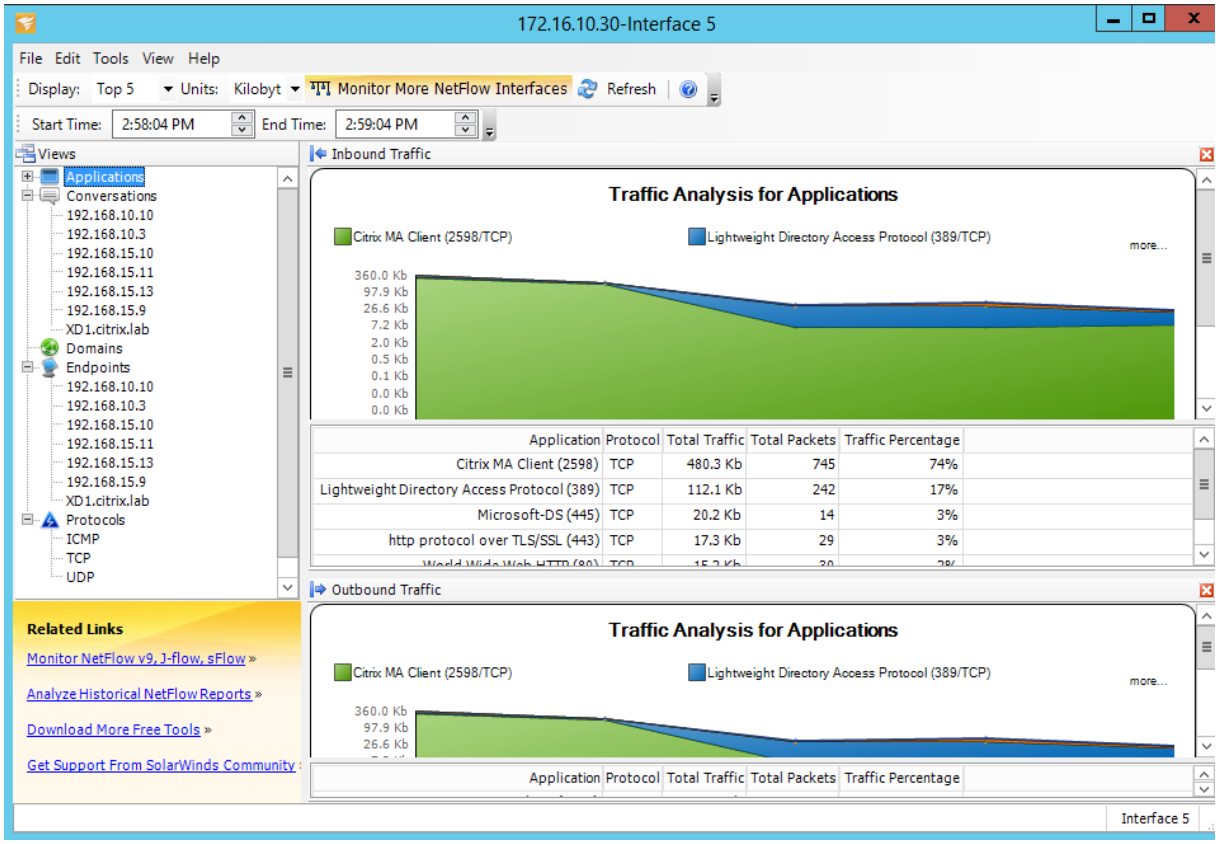
Net Flow collectors collectent le trafic réseau IP lorsqu'il entre ou quitte une interface SD-WAN. En analysant les données fournies par Net Flow, vous pouvez déterminer la source et la destination du trafic, la classe de service et les causes de la congestion du trafic. Les périphériques Citrix SD-WAN 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 Edition.

Pour plus d'informations sur la configuration des hôtes Net Flow à l'aide du service Citrix SD-WAN Orchestrator, consultez la section Paramètres de l'hôte Netflow.

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, voir SNMP.



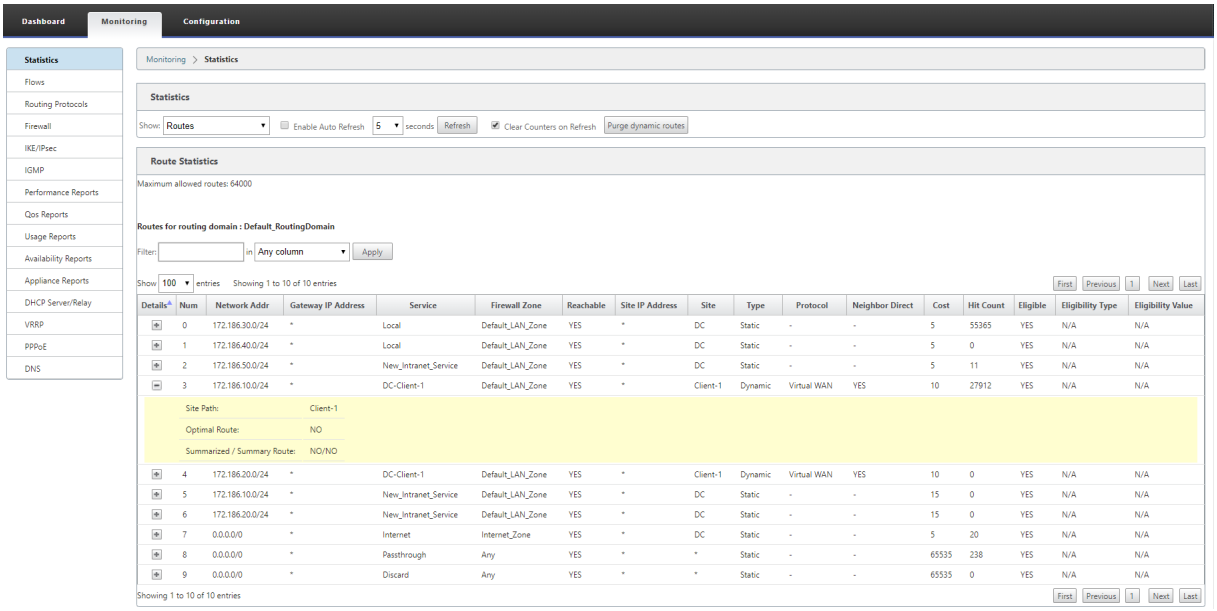


Limitations de NetFlow

- Lorsque Netflow est activé sur les appliances SD-WAN Standard Edition, les données Virtual Path sont diffusées en continu 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

Pour afficher les statistiques d'itinéraire de vos appliances SD-WAN, dans l'interface graphique SD-WAN, accédez à **Monitoring** > **Statistics** > **Itinéraires**.



Vous pouvez afficher les paramètres suivants :

- **Adresse réseau : adresse**réseau et masque de sous-réseau de l'itinéraire.
- **Détails** : cliquez sur + pour afficher les informations suivantes.
  - **Chemin**d'accès au site : Le chemin d'accès au 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 de ces préfixes sont reçus et les administrateurs sont en mesure de juger les attributs du préfixe en affichant le chemin du site.

    Par exemple, considérez une topologie simple de Branch1, Branch2 et MCN avec un MCN Geo. Branch1 a un préfixe 172.16.1.0/24 et doit se rendre à Branch2. Geo MCN et MCN ont le transfert WAN vers WAN activé.

    Le préfixe 172.16.1.0/24 peut atteindre 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 leur métrique de chemin d'accès au site. La mesure du chemin d'accès du site indique l'origine du préfixe d'itinéraire et le coût nécessaire pour accéder à Branch2.
  - **Itinéraire**optimal : L'itinéraire optimal indique si l'itinéraire est l'itinéraire optimal pour atteindre ce sous-réseau par rapport à tous les autres itinéraires. Cette route optimale est exportée vers d'autres sites.

  - **Itinéraire récapitulé/récapitulatif** : une route récapitulative est une route configurée explicitement par un administrateur pour résumer plusieurs préfixes qui se trouvent dans le superréseau. Les itinéraires résumés sont les préfixes qui relèvent de la route récapitulative.

    Par exemple, supposons que nous avons une route sommaire 172.16.0.0/16. Il s'agit d'une route récapitulative uniquement et non d'une route résumée. Un itinéraire récapitulatif a un résumé « OUI » et un résumé « NON ». 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 résumées. Une route résumée a résumé « OUI » et « NON » récapitulatif.

- **Adresse IP de la passerelle** : adresse IP de la passerelle/route utilisée pour atteindre cette route.
- **Service** : type de service Citrix SD-WAN.
- **Zone de pare-feu** : zone de pare-feu utilisée par l'itinéraire.
- **Reachable** : 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 routes du côté LAN et les routes saisies manuellement pendant la configuration sont des routes statiques. Les routes apprises auprès 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.
  - **Virtual WAN** : préfixes apportés par les appliances SD-WAN homologues.
  - **OSPF** : préfixes apportés par le pair de routage dynamique OSPF.
  - **BGP** : préfixes apportés par l'homologue de routage dynamique BGP.
- **Neighbor 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'une route a été atteinte 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 atteint pendant le traitement du trafic.
- **Type d'éligibilité** : Les deux types d'éligibilité suivants sont disponibles.

  - **Éligibilité**de la passerelle : détermine si la passerelle est accessible ou non.
  - **Admissibilité du chemin** : détermine si le chemin est DEAD ou NOT DEAD.

- **Valeur d'éligibilité** : valeur sélectionnée pour la passerelle ou le chemin d'accès dans la configuration lors de la création de l'itinéraire dans le système. Par exemple, un itinéraire peut être appelé éligible sur la base d'un chemin MCN-WL-1->BR1-WL-2. Donc, la valeur d'éligibilité pour cette route dans la section itinéraires est la valeur MCN-WL-1->BR1-WL-2.

Routage

November 16, 2022

> **Remarque**
>
> À partir de la version SD-WAN 11.5, toutes les configurations de routage sont prises en charge uniquement via le service Citrix SD-WAN Orchestrator. Pour plus d'informations sur les configurations de routage du service Citrix SD-WAN Orchestrator, consultez Routage.

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 annonce de route unique, réduisant ainsi le nombre de liens entre les routeurs. Il économise 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 CLI 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

August 31, 2022

Citrix SD-WAN fournit une connectivité résiliente et robuste 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 du réseau permettant 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

Le SD-WAN autorise des entrées de route statiques pour des sites spécifiques et des entrées de route apprises du réseau sous-jacent 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 Virtual Interface (crée automatiquement des itinéraires locaux) et toute route locale définie dans la table de routage (avec un saut suivant local). La route est annoncée pour d'autres appliances SD-WAN qui ont un chemin virtuel vers ce site local où cette route est configurée lorsqu'elle est approuvée en tant que partenaire.

> **Remarque**
>
> Soyez prudent lorsque vous ajoutez des itinéraires par défaut et des itinéraires récapitulatifs en tant qu'itinéraires locaux, 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 cette route (sous-réseau) est classé comme intranet pour cette appliance en vue de sa remise à un site ne disposant pas d'une 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** : similaire à l'intranet, mais il est utilisé pour définir le trafic circulant vers des liens WAN Internet publics plutôt que vers des liens WAN privés. 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. Une route Internet par défaut est créée lorsque le service Internet est activé (il est désactivé par défaut). Tout trafic correspondant à cette route (sous-réseau) est classé comme Internet pour cette appliance en vue de sa remise aux ressources Internet publiques.

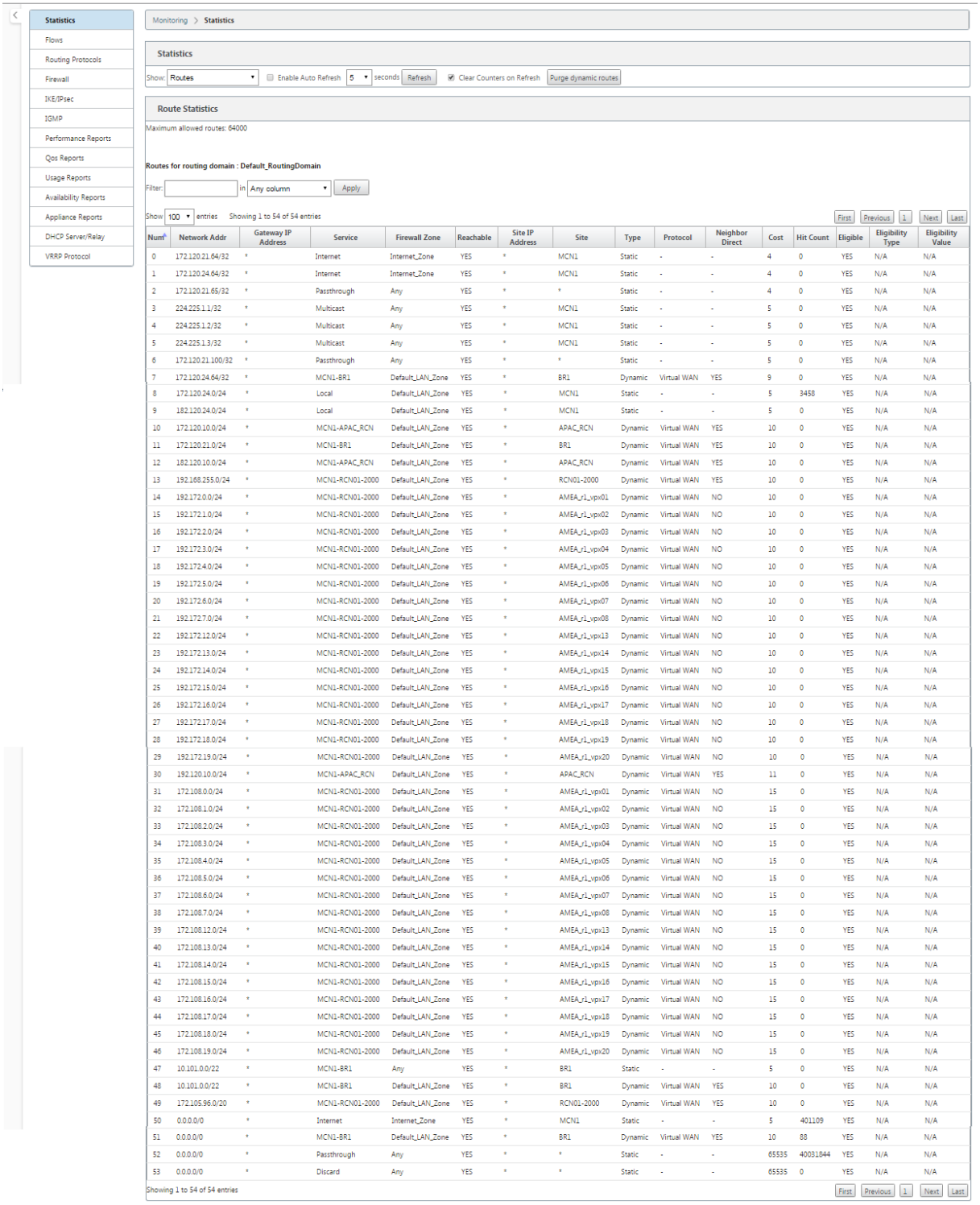
> **Remarque**
>
> Les routes de service Internet peuvent être publiées sur les autres appliances SD-WAN ou ne pas être exportées selon que vous utilisez ou non l'accès Internet via les chemins virtuels.

- **Passthrough** : ce service agit en dernier recours ou en remplacement lorsqu'une appliance est en mode en ligne. Si une adresse IP de destination ne correspond pas à une autre route, l'appliance SD-WAN la transmet simplement sur le saut suivant du lien WAN. Un itinéraire par défaut : le coût 0.0.0.0/0 de 16 itinéraires pass-through est créé automatiquement. Passthrough ne fonctionne pas lorsque l'appliance SD-WAN est déployée hors chemin ou en mode Edge/-Gateway. 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).

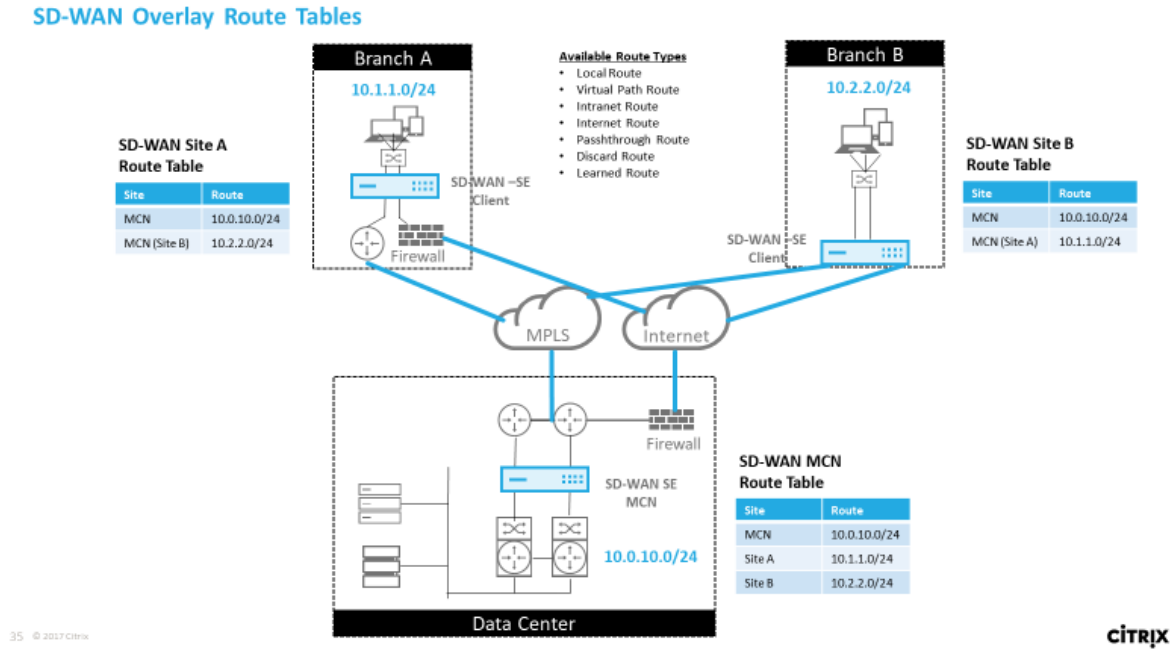
La table de routage du nœud client local peut être surveillée sur la page **Surveillance** > **Statistiques** avec Itinéraires sélectionnées dans la liste déroulante **Afficher**.



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.



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 se fait dans l'ordre suivant :

1. Correspondances de préfixe les plus longues
2. Coût
3. Service

Par conséquent, un itinéraire /32 précède toujours un itinéraire /31. Pour deux routes /32, un itinéraire Coût 4 précède toujours un itinéraire Coût 5. Pour deux /32 coût 5 routes, les routes sont choisies 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 de 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 de trafic WAN vers LAN (chemin virtuel) :
    1. Le trafic de chemin virtuel est reçu par SD-WAN à partir du tunnel et est traité.
    2. l'appliance compare l'adresse IP source pour vérifier si la source est locale.
        - Si oui, alors éligible au WAN et faites correspondre la destination IP à la table de route/-chemin virtuel.
        - Si non, alors la vérification du transfert WAN vers WAN est activée.
    3. (Transfert WAN vers WAN désactivé) 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 introduit les protocoles de routage OSPF et BGP dans la configuration. L'introduction de protocoles de routage au SD-WAN a facilité l'intégration du 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 le service SD-WAN Orchestrator, 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 communication directe avec les routeurs périphériques clients existants à l'aide du 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.

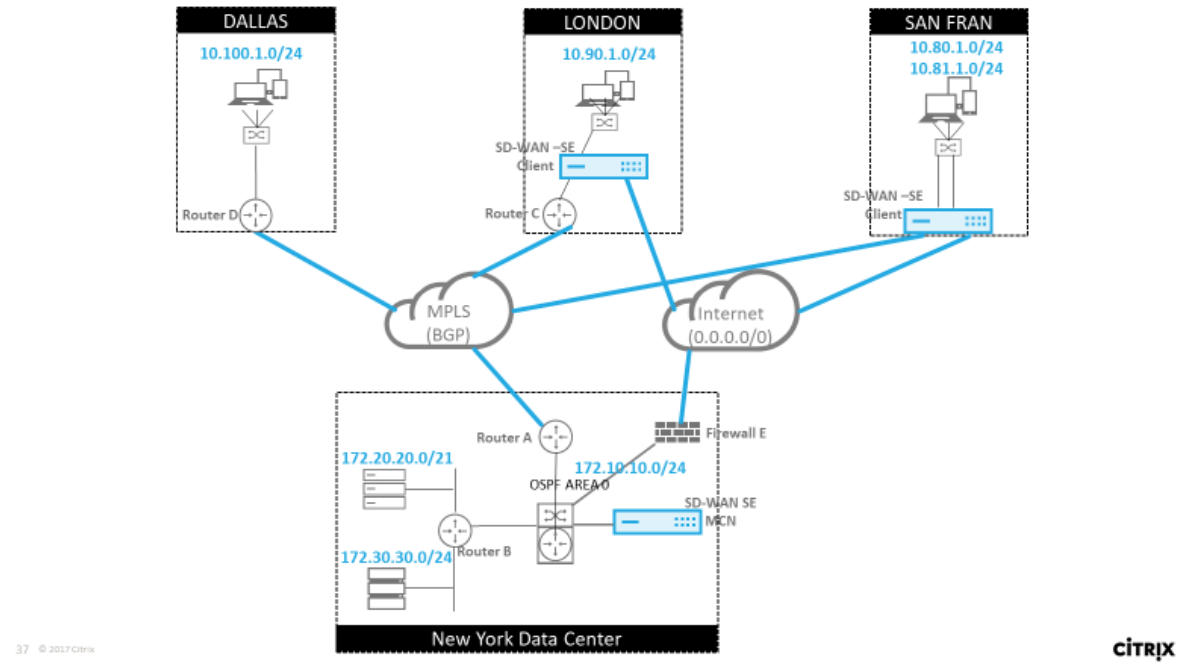
> **Important**
>
> Il est facile de fuir la route indésirable, si vous n'êtes pas prudent.

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.

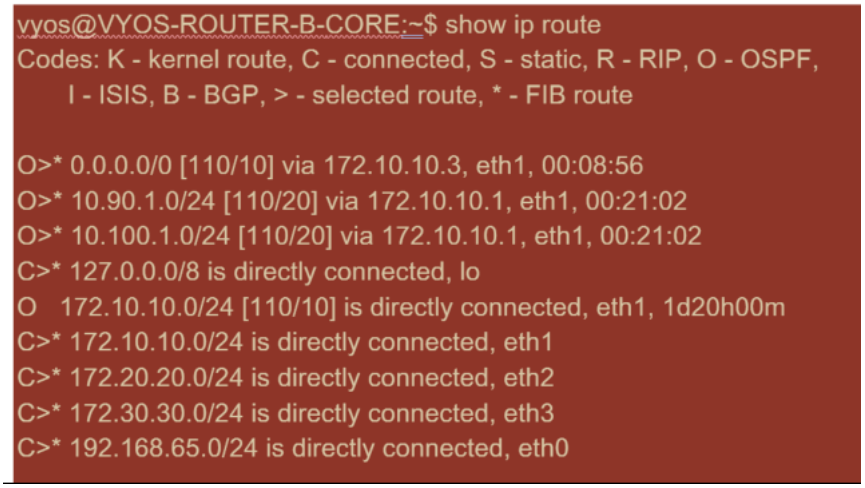
Le site de San Francisco doit également être noté pour ne pas avoir de routeur. Le SD-WAN est déployé en mode Edge/Gateway, cette appliance étant la Gateway par défaut pour le sous-réseau de San Francisco et participant également à l'eBGP vers le MPLS.

- Avec le centre de données de New York, notez que le SD-WAN est déployé en mode Virtual Inline. L'intention est de participer au protocole de routage OSPF existant afin de transférer le trafic vers l'appliance en tant que Gateway préférée.
- Le site de Londres est déployé en mode traditionnel en ligne. Le routeur WAN (C) en amont sera toujours la Gateway par défaut pour le sous-réseau London.

- Le site de San Francisco est un site nouvellement introduit à ce réseau et le SD-WAN est prévu pour être déployé en mode Edge/Gateway et servir de Gateway par défaut pour le nouveau sous-réseau de San Francisco.

Passez en revue certaines tables de routage de sous-couche existantes avant de mettre en œuvre le SD-WAN.

Routeur Core de New York B :



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 Londres (10.100.1.0/24) sont disponibles via 172.10.10.1 (MPLS Router A). Les coûts de la route 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 le 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
```

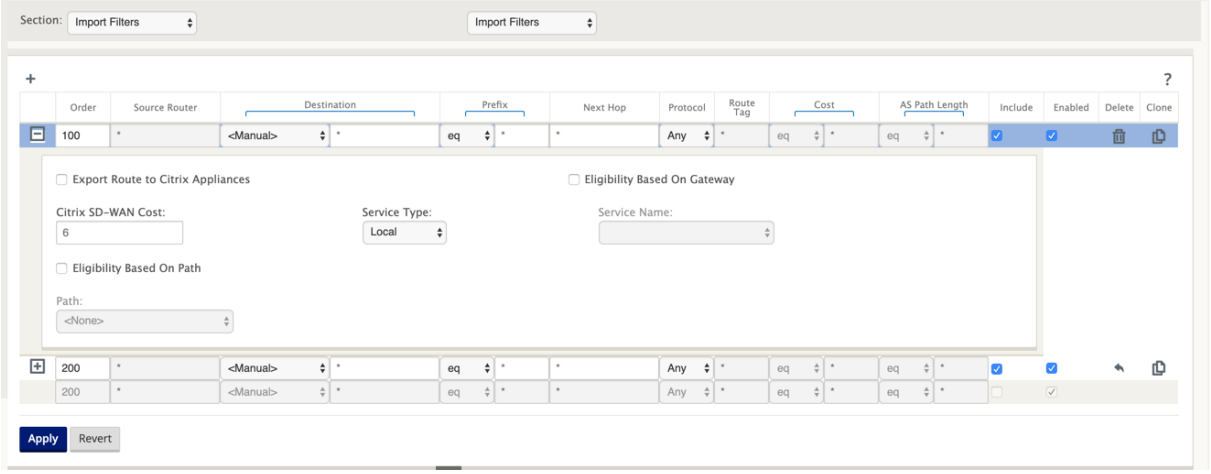
> **Remarque**
>
> Dans cet exemple, vous pouvez ignorer le sous-réseau 192.168.65.0/24. Il s'agit d'un réseau de gestion qui n'est pas pertinent pour l'exemple. Tous les routeurs sont connectés au sous-réseau de gestion, mais ils ne sont annoncés dans aucun protocole de routage.

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

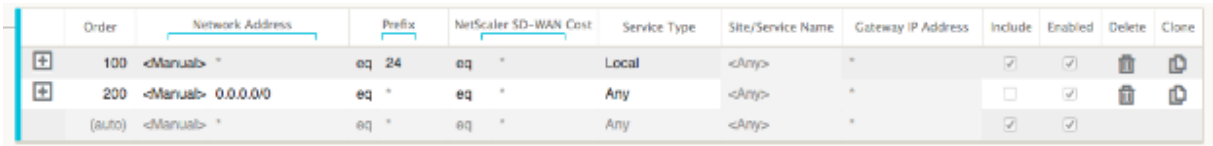
de contrôler ce qui entre et sort de la table de routage. Nous considérons chaque emplacement à tour de rôle.

- 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.



- Exporter des itinéraires locaux vers eBGP

La règle par défaut pour l'exportation consiste à tout exporter. La règle 200 est utilisée pour remplacer la règle d'erreur pour ne pas republier les routes. Toute route correspondant à un préfixe SD-WAN a appris sur les chemins virtuels.



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 les sous-réseaux 10.80.1.0/24 et 10.81.1.0/24 sont vus correctement via eBGP du SD-WAN de San Francisco.

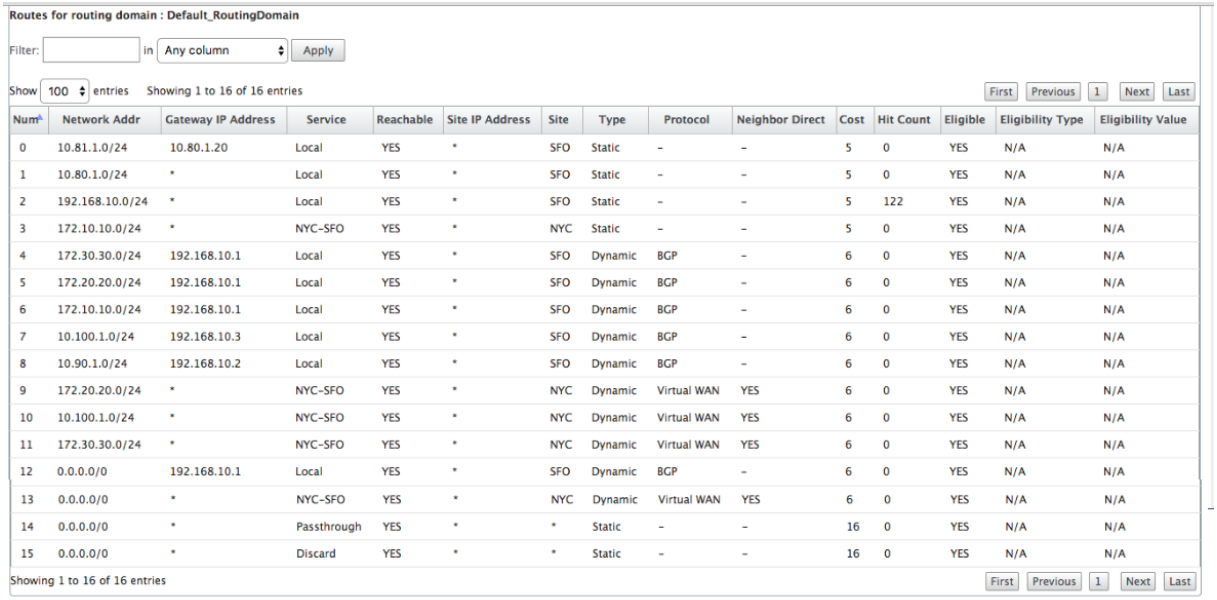
Routeur D de Dallas :


```
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** .

Citrix SD-WAN de San Francisco :



Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 16 of 16 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	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 First Previous 1 Next Last

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 apprise 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 statique 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.

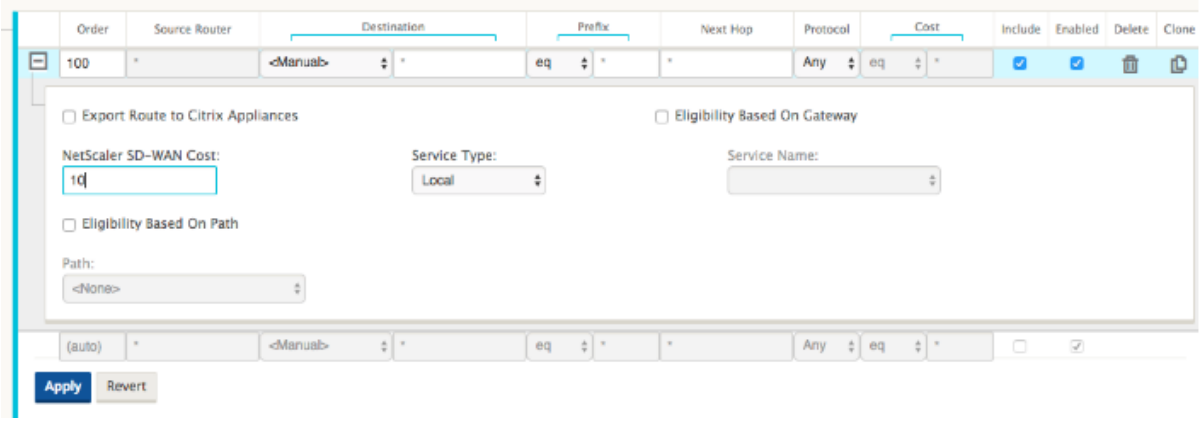
- Comme une route annoncée par BGP (numéro 6), avec un coût de 6. Ceci est maintenant considéré comme une route de secours.

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.

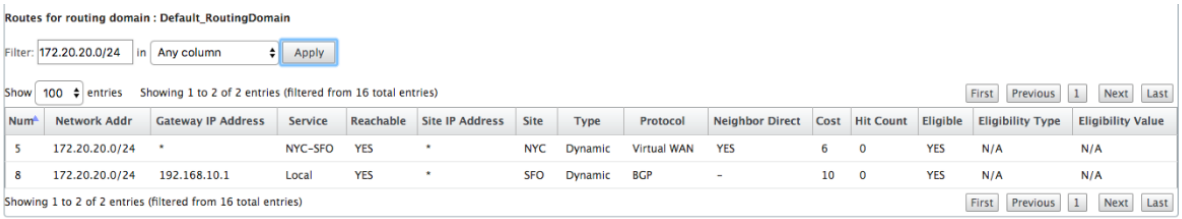
Maintenant, considérons la route 172.20.20.0/24.

- 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'appliance 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.

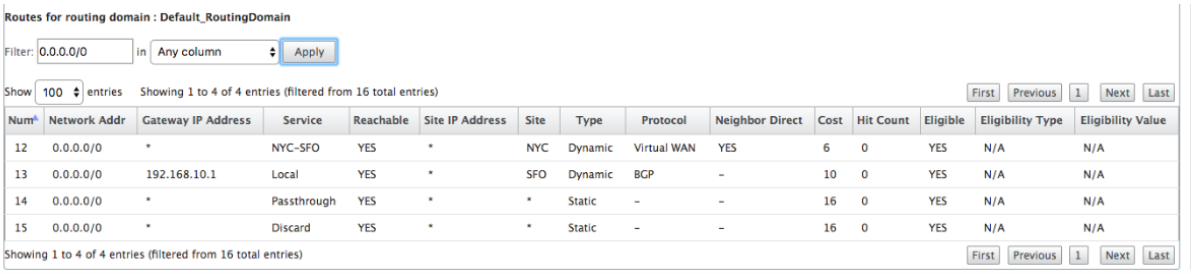


Après avoir effectué l'ajustement, nous pouvons actualiser la table de routage SD-WAN sur l'appliance San Francisco pour voir les coûts d'itinéraire ajustés. Utilisez l'option de filtre pour focaliser la liste affichée.



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) 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
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) First Previous 1 Next Last

Nous voyons également une route de passage et de rejet avec le coût 16. Il s'agit de routes automatiques qui ne peuvent pas être supprimées. Si le périphérique est en ligne, la route passthrough est utilisée en dernier recours, donc si un paquet ne peut pas être mis en correspondance avec 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 passthrough, auquel cas SD-WAN supprime le paquet en utilisant la route de rejet par défaut. Le nombre d'accès indique le nombre de paquets qui atteignent chaque route, ce qui peut être utile lors du dépannage.

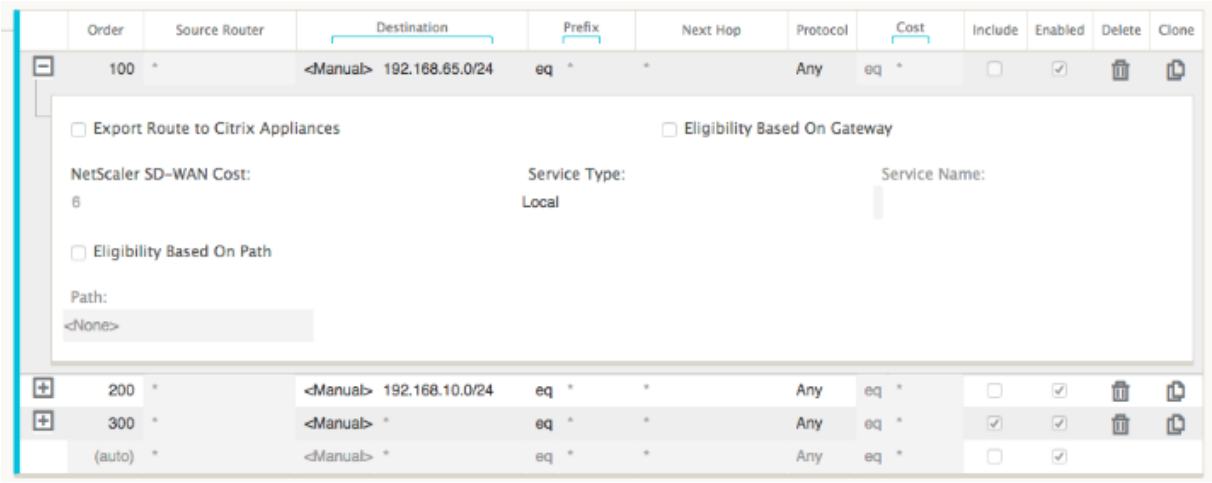
Maintenant, nous nous concentrons sur le site de New York, nous voulons que le trafic destiné aux sites distants (Londres et San Francisco) soit dirigé vers l'appliance SD-WAN lorsque le chemin virtuel est actif.

Il existe plusieurs sous-réseaux disponibles sur le site de New York :

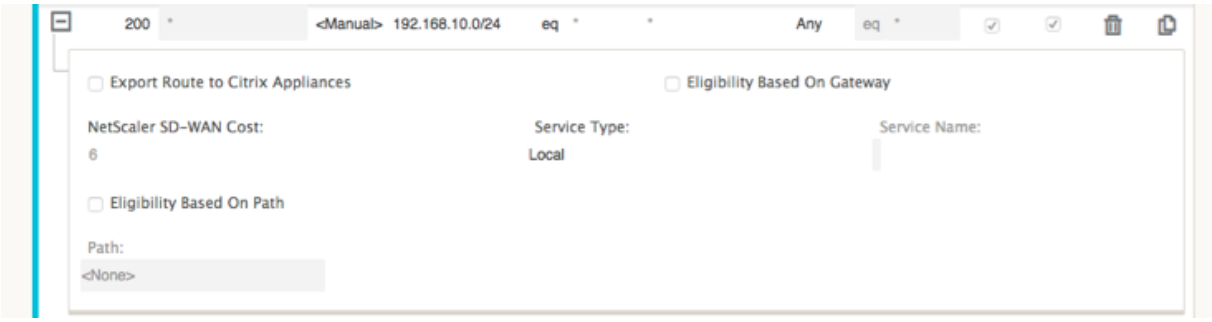
- 172.10.10.0/24 (directement connecté)
- 172.20.20.0/24 (annoncé via OSPF à partir du routeur principal B)
- 172.30.30.0/24 (annoncé via OSPF à partir du routeur principal B)

Nous sommes également tenus de fournir le flux de trafic vers Dallas (10.100.1.0/24) via MPLS.

Enfin, nous voulons tout le trafic lié à Internet vers le pare-feu E à travers 172.10.10.3 comme un prochain saut. 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 :

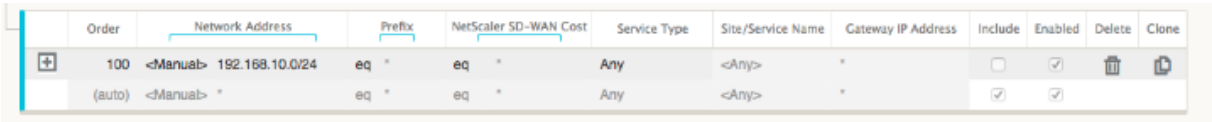


Le site SD-WAN de New York importe toutes les routes du réseau de gestion. Cela peut être ignoré. On peut se concentrer sur le filtre 200.



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.

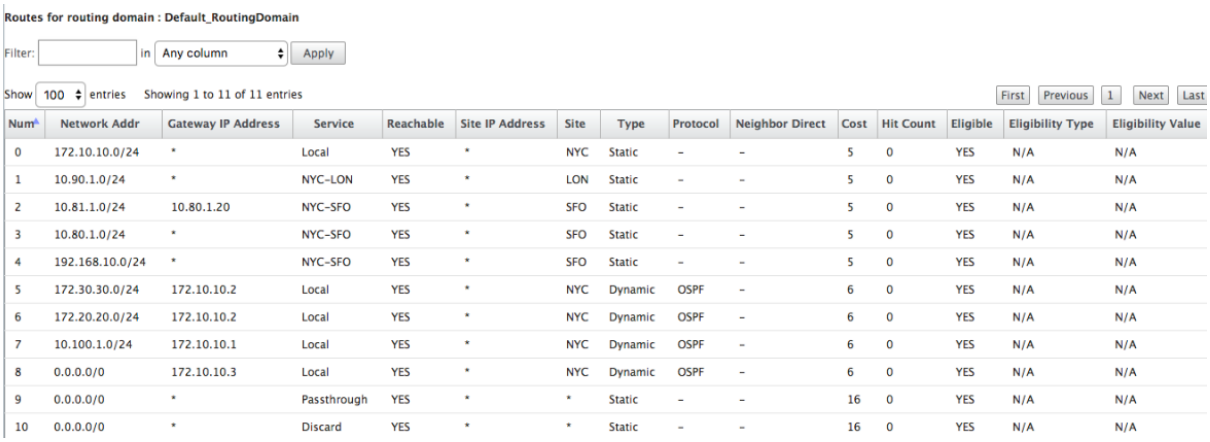
Routeur de New York B :


```
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 du routeur MPLS A. Passons en revue la table de routage 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 route pour ajuster le coût AD/métrique afin qu'il y ait une préférence de route de la route provenant de 172.10.10.10 plutôt que de la route apprise via eBGP.

Alternativement, une route « backdoor » peut être configurée pour forcer le routeur à préférer la route OSPF à 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 un itinéraire pour le 10.90.1.0/24 annoncé 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 à lui-même.

Chemins virtuels dynamiques

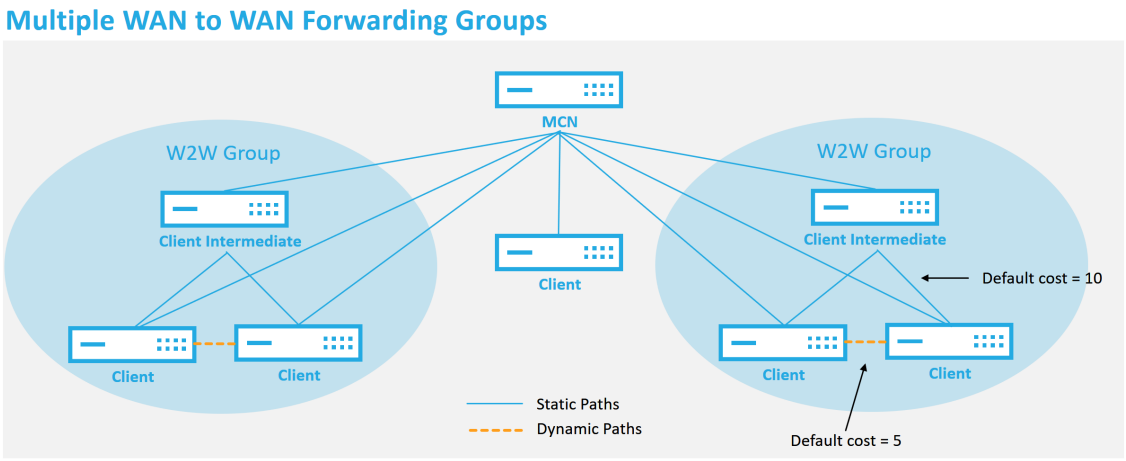
Les chemins virtuels dynamiques peuvent être autorisés entre deux nœuds clients pour créer des chemins virtuels à la demande pour une communication directe entre les deux sites. L'avantage d'un chemin virtuel dynamique est que le trafic peut circuler directement d'un nœud client au second sans avoir 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 comme étant des paquets par seconde (pps) ou de la bande passante (kbps). Cette fonctionnalité active une topologie de superposition SD-WAN à maillage complet dynamique.

Une fois que les seuils pour les chemins virtuels dynamiques sont atteints, les nœuds clients créent dynamiquement leur chemin virtualisé les uns vers les autres en utilisant tous les chemins WAN disponibles entre les sites et en tirent pleinement parti de la manière suivante :

- Envoyez des données en vrac s'il y en a et vérifiez qu'aucune perte, puis
- Envoyez des données interactives et vérifiez aucune perte, puis
- Envoyer des données en temps réel une fois que les données Bulk et Interactive sont considérées comme stables (pas de perte ou de 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.

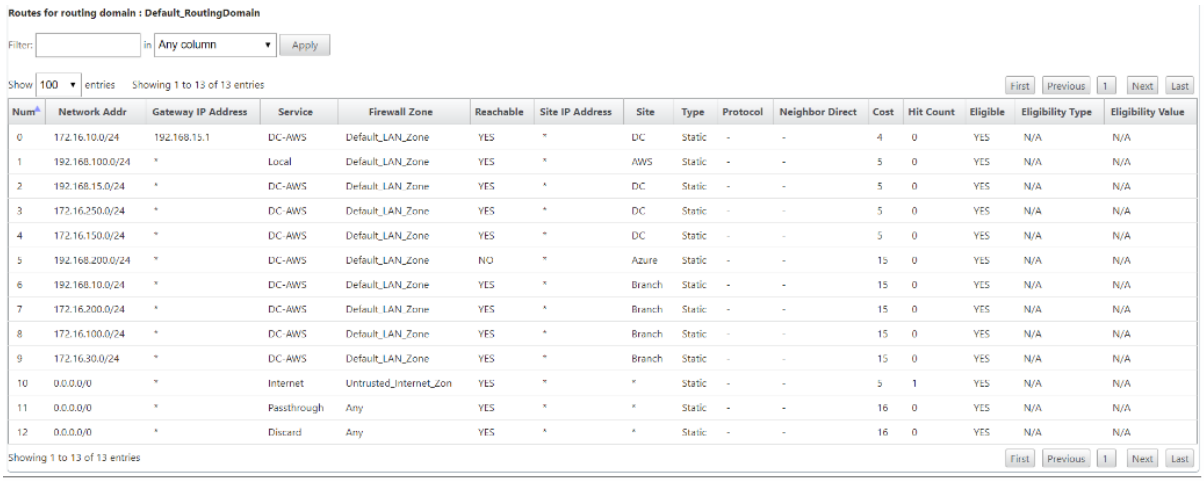
Plusieurs groupes de transfert WAN vers WAN sont autorisés dans le SD-WAN, ce qui permet un contrôle total de l'établissement du chemin entre certains nœuds clients et pas d'autres.



Chaque périphérique SD-WAN possède sa propre table de routage unique avec les détails suivants définis pour chaque itinéraire :

- Num —ordre de route de cette appliance basé sur le processus de correspondance (Num le plus bas traité en premier)
- Adresse réseau —adresse de sous-réseau ou d'hôte
- Passerelle si nécessaire
- Service —quel service est appliqué pour cette route
- Zone de pare-feu —classification de la zone de pare-feu de l'itinéraire
- Reachable —Identifie si l'état du chemin virtuel est actif pour ce site
- Site —Nom du site sur lequel l'itinéraire doit exister
- Type —Identification du type d'itinéraire (statique ou dynamique)
- Voisin Direct
- Coût - coût de l'itinéraire spécifique
- Nombre de coups —combien de fois la route a été utilisée par paquet. Cela serait utilisé pour vérifier qu'une route est touchée correctement.
- Admissibles
- 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 Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries First Previous 1 Next Last

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 First Previous 1 Next Last

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 des différents états du service (le chemin virtuel étant désactivé 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'une route locale 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'une route partagée vers un autre nœud client qui est partagée par le MCN avec un état d'accessibilité de Non en raison du chemin virtuel vers le bas entre ce site et le MCN.
- Route 6—9 —Ces routes existent sur un autre site client. Pour cette route, une route de chemin virtuel est créée pour correspondre au trafic d'entrée WAN 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 existantes. 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'acheminement direct par défaut —5
- Routes générées automatiquement —5
- Chemin virtuel —5
- Local —5
- Intranet —5
- Internet —5
- Passthrough —5
- Facultatif : la route est 0.0.0.0/0 définie en tant que 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 divisés en flux suivants :

- LAN vers WAN (chemin virtuel) —Trafic entrant dans le tunnel de superposition SD-WAN
- WAN to LAN (chemin virtuel) —Trafic existant dans le tunnel de superposition SD-WAN
- Trafic de chemin non virtuel —Trafic acheminé vers le réseau de sous-couche

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 route 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 relais, les éléments suivants sont pris en compte lors de la conception :

- 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
- Nombre maximal d'interfaces virtuelles par zone OSPF : 255
- Filtres d'importation maximum d'apprentissage d'itinéraire par site : 512
- Filtres d'exportation maximum d'apprentissage par route par site : 512
- Stratégies de routage BGP maximales : 255
- Nombre maximal d'objets de chaîne de communauté BGP : 255

Domaine de routage

August 31, 2022

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 des protocoles de routage OSPF et BGP pour les domaines de routage afin de contrôler et de segmenter 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 quel endroit 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
  - 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 une liaison Internet publique, une seule interface d'accès primaire 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.

Configuration du domaine de routage

August 31, 2022

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.

Avec la version 11.0.2, **le routage de domaines sans IP virtuelles (VIP) routables** est autorisé avec les fonctionnalités suivantes :

- Autoriser un périphérique à avoir un domaine de routage pour des interfaces non fiables 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.

Utiliser CLI pour accéder au routage

August 31, 2022

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.

```
dynamic_routing?
<!--NeedCopy-->
```

Routage dynamique

August 31, 2022

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.

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.

> **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).

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.

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'appliance 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

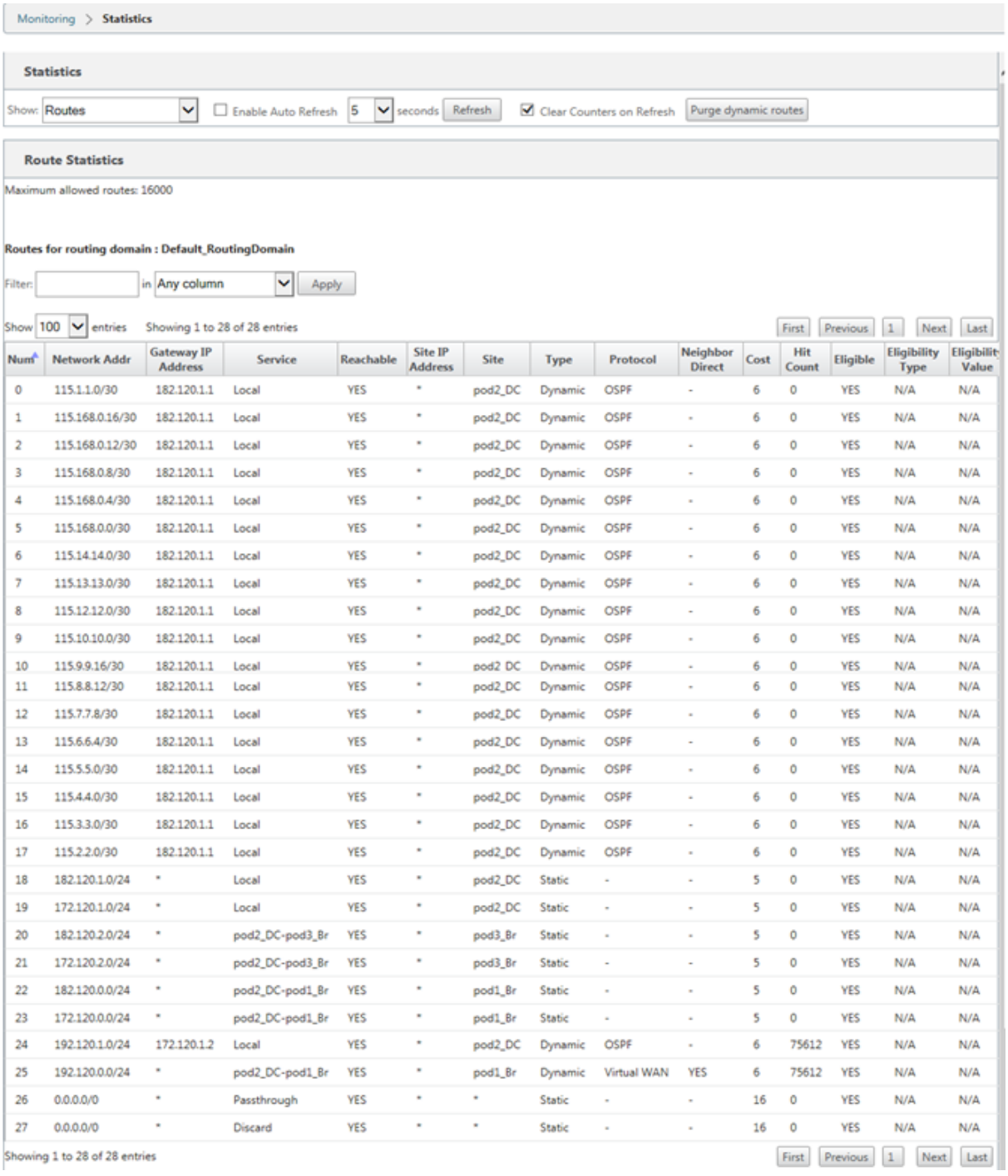
Le protocole BGP utilise l'attribut de **longueur de chemin AS** pour déterminer le meilleur itinéraire. La longueur du chemin AS indique le nombre de systèmes autonomes traversés dans un itinéraire. Citrix SD-WAN utilise l'attribut de **longueur de chemin BGP AS** pour filtrer et importer des itinéraires.

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.

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 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	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 First Previous 1 Next Last

OSPF

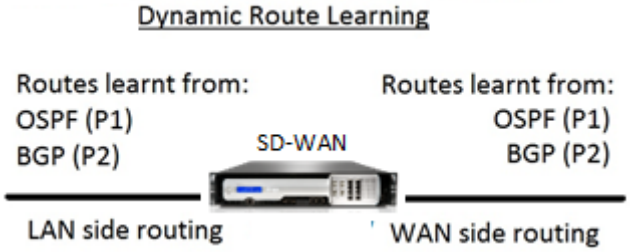
August 31, 2022

Côté LAN : apprentissage dynamique des itinéraires

OSPF s'exécutant sur le port LAN de l'appliance Citrix SD-WAN déployé 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 zone AREA définie comme une zone STUB en limitant l'apprentissage de type 5 AS-External 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 la connectivité entre les sites à travers le réseau en évolution.

Modes de déploiement OSPF

Dans les versions précédentes, les routes acquises par instance OSPF à partir du SD-WAN étaient traitées comme des routes externes avec LSA de type 5 uniquement. Ces routes ont été annoncées à ses routeurs voisins en LSA externe de type 5. Il en résulte que les routes SD-WAN sont moins préférées selon l'algorithme de sélection des chemins OSPF.

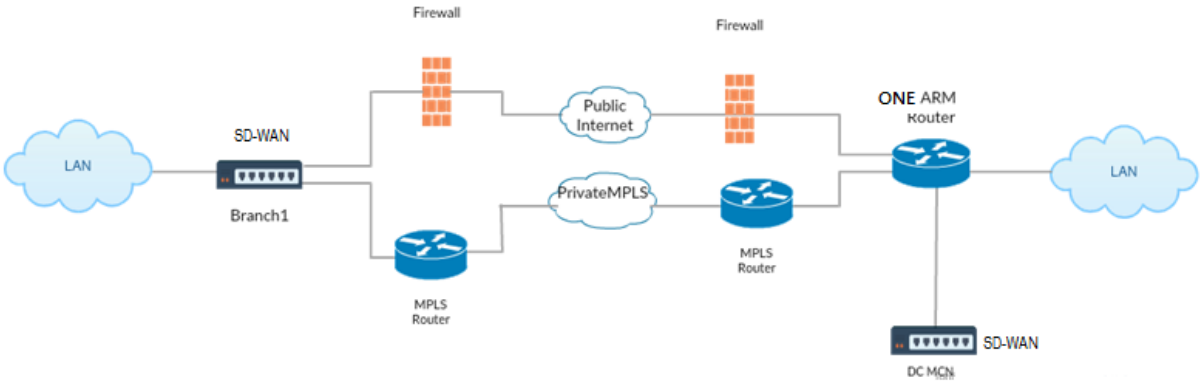
Avec la dernière version, SD-WAN peut désormais annoncer des itinéraires en tant qu'itinéraires intra-zone (LSA Type 1) pour obtenir la préférence en fonction de son coût d'itinéraire à l'aide de l'algorithme de sélection de chemin OSPF. Le coût de l'itinéraire peut être configuré et annoncé au routeur voisin. Cela permet de déployer l'appliance SD-WAN dans un mode à bras unique décrit ci-dessous.

Implémentation d'OSPF dans la topologie à bras unique

Dans une configuration à bras unique, le routeur a besoin d'une configuration PBR ou WCCP compliquée 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'appliance 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.

Pré-requis :

- 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.

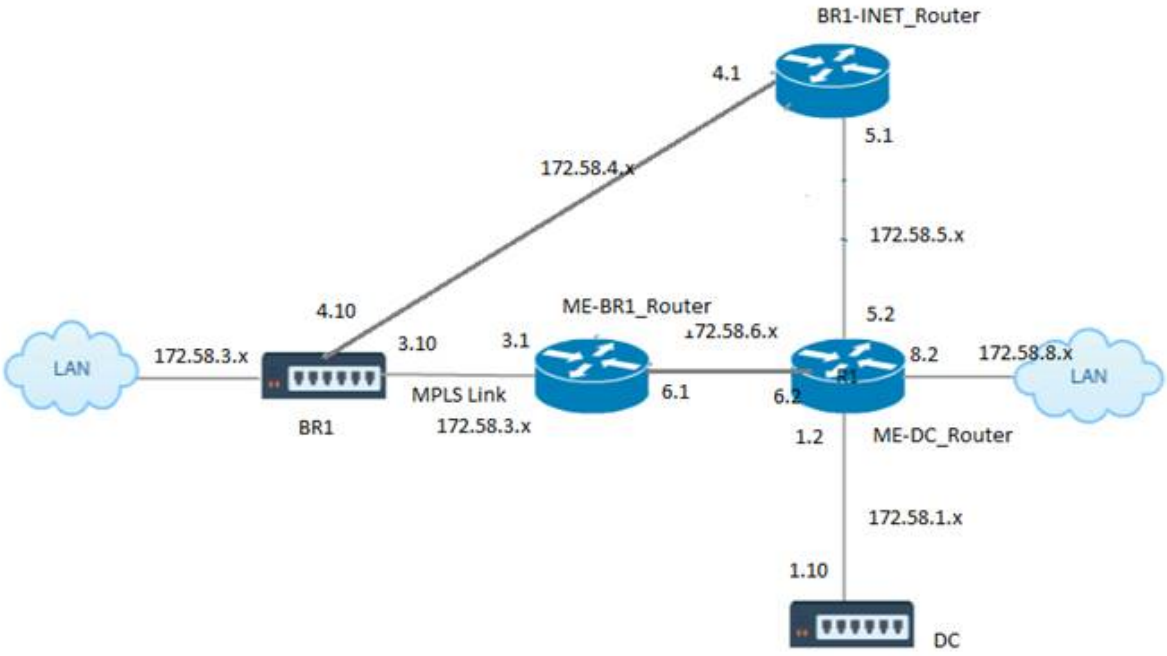


Comme le montre l'illustration ci-dessus, le MCN DC est déployé en topologie à bras unique. Lorsque le site DC est actif, le routeur à bras unique transfère tout le trafic du réseau local vers d'autres sites, tels que le réseau local local de la succursale dont l'adresse IP de destination se trouve dans le même sous-réseau vers le SD-WAN, puis l'appliance 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'appliance 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'appliances SD-WAN. L'illustration ci-dessous décrit l'implémentation du réseau MPLS standard.



Dans l'illustration ci-dessus :

- OSPF est configuré entre le routeur *ME-BR1_et le routeur**ME-DC_Router* dans la zone 0.
- OSPF est configuré entre *Me-DC_Router* et *DC* dans la zone 0.

Configuration recommandée :

- DC VW and ME-DC_Router on area0
- ME-BR1_Router and ME-DC_Router on area0
- BR1 VW and ME-BR1_Router on area0

Sur le routeur ME-DC_routeur :

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'appliance 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'appliance 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.

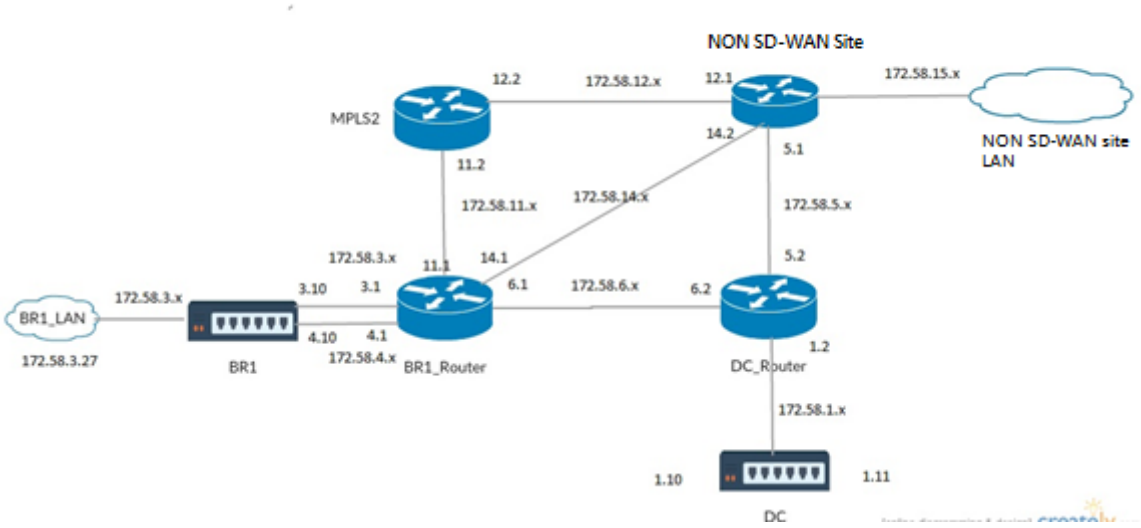
Cela garantit également qu'en cas de défaillance du dispositif SD-WAN DC, la route alternative permettant d'utiliser ME-BR1_router comme Gateway préférée suivante garantit un flux de trafic ininterrompu.

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 amont étant conscient du sous-réseau LAN après la décapsulation. Si DC SD-WAN tombe en panne, l'infrastructure de routage héritée aiderait le routeur ME-BR1_Router à utiliser le routeur ME-DC_Router comme prochain saut pour atteindre le réseau 172.58.8.x.

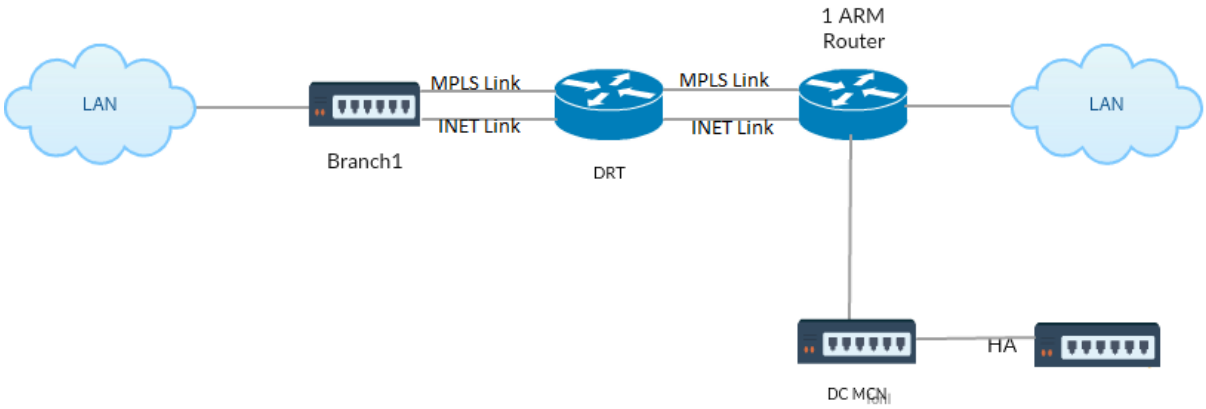
Déploiement d'appliances SD-WAN et tierces (non SD-WAN)

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.



Le flux de trafic peut être observé dans l'interface graphique SD-WAN sous **Monitoring** > **Flux** .

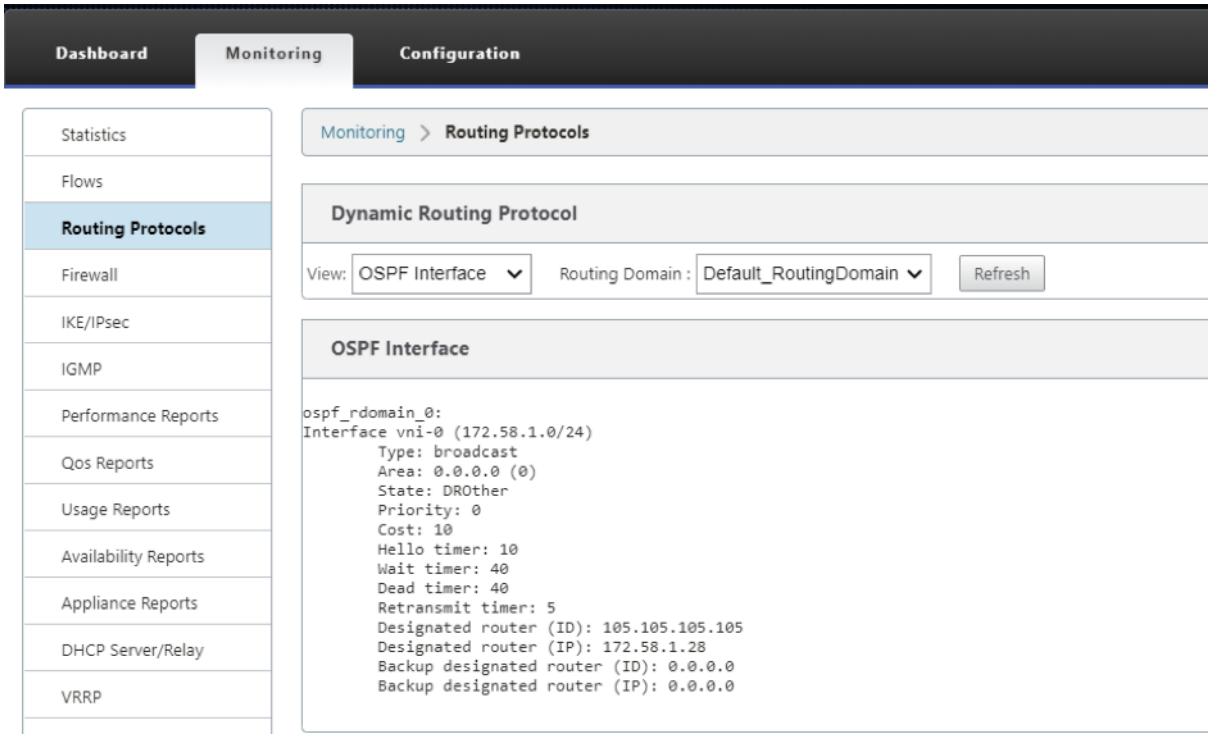
Mise en œuvre d'OSPF avec le réseau SD-WAN dans la configuration haute disponibilité

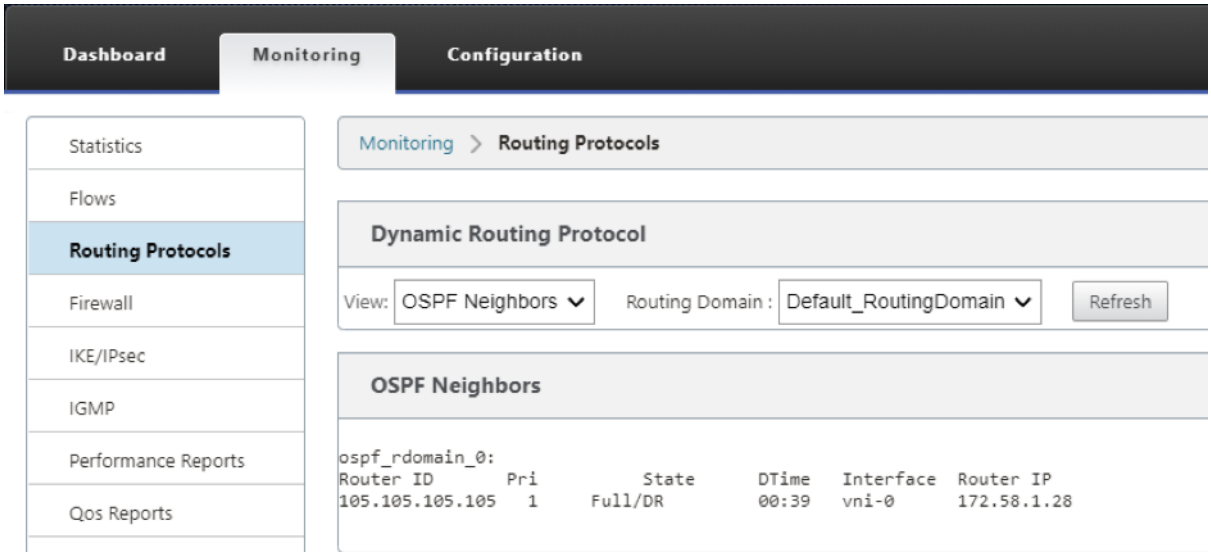


OSPF Type5 à Type1 avec des sites haute disponibilité pendant le basculement vers l'appliance de secours et déployé dans une configuration haute disponibilité :

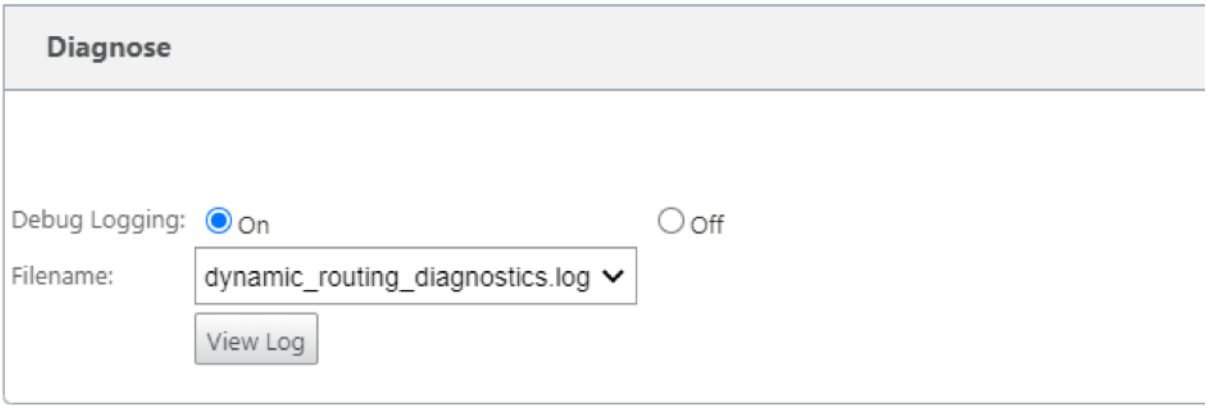
Résolution des problèmes

Vous pouvez afficher les paramètres OSPF sous **Surveillance >Protocoles de routage**.





Vous pouvez également observer les journaux de routage dynamique pour voir s'il y a un problème avec la convergence OSPF.



BGP

August 31, 2022

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 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 d'itinéraire et d'ACL pour correspondre à certaines routes 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.

1. 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 **Surveiller** > **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 peut être consulté à partir de la surveillance des protocoles de routage.

Reconfiguration logicielle BGP

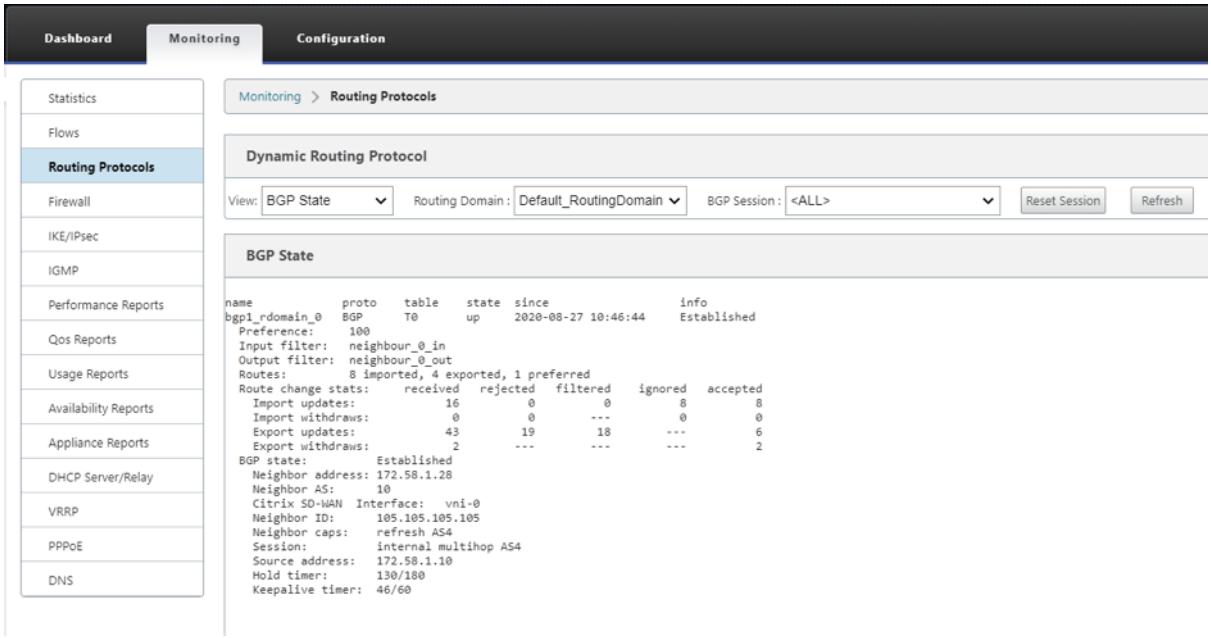
Les stratégies de routage pour homologue BGP incluent des configurations telles que la carte de routage, la liste de distribution, la liste de préfix-list et la liste de filtres qui peuvent avoir un impact sur les mises à jour de tables de routage entrantes ou sortantes. En cas de modification de la 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.

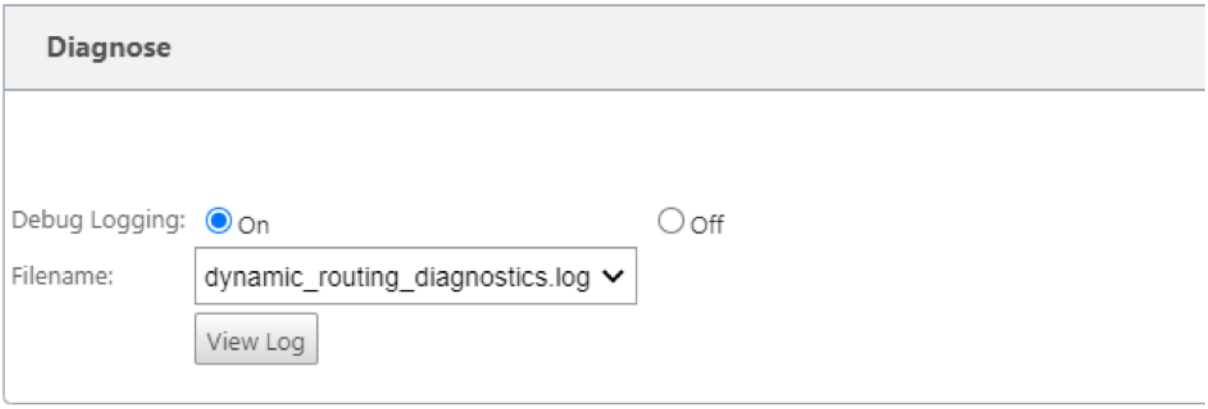
La fonctionnalité BGP Soft Reset Enhancement fournit une prise en charge automatique de la réinitialisation dynamique dynamique des mises à jour de la table de routage BGP entrantes qui ne dépendent pas des informations de mise à jour de la table de routage stockées.

Résolution des problèmes

Pour afficher les paramètres BGP, accédez à **Surveillance > Protocoles de routage** > sélectionnez **État BGP** dans le champ **Affichage**.



Vous pouvez observer les journaux de routage dynamique pour voir s'il y a un problème avec BGP Convergence.



iBGP

August 31, 2022

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 maillés avec Citrix SD-WAN.

Limitations:

- Les attributs AS-path prepend, 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 toutes les routes (ou) aucune des routes apprises par OSPF sont annoncées aux pairs du 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

August 31, 2022

Site SD-WAN communiquant avec un site non SD-WAN via eBGP :

Lorsqu'un site sans appliance SD-WAN communique avec un autre site avec une appliance SD-WAN (Site-A) sur un seul chemin WAN (seul Internet est disponible), et si le site avec une 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). Le Site-B achemine le trafic du site sans dispositif SD-WAN vers le Site-A.

Communication entre les sites SD-WAN à l'aide du chemin virtuel et de l'eBGP :

Fournit l'apprentissage de la route de sous-couche pour communiquer avec les sous-réseaux locaux du site distant lorsque le chemin virtuel est en panne entre deux sites alors que l'appliance Virtual WAN est toujours en service et en cours d'exécution.

Route de l'application

August 31, 2022

Dans un réseau d'entreprise typique, les succursales accèdent aux applications du datacenter local, du datacenter cloud ou des applications SaaS. La fonction 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 essaie 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 d'abord.

Citrix SD-WAN vous permet de définir les itinéraires d'application pour les services suivants :

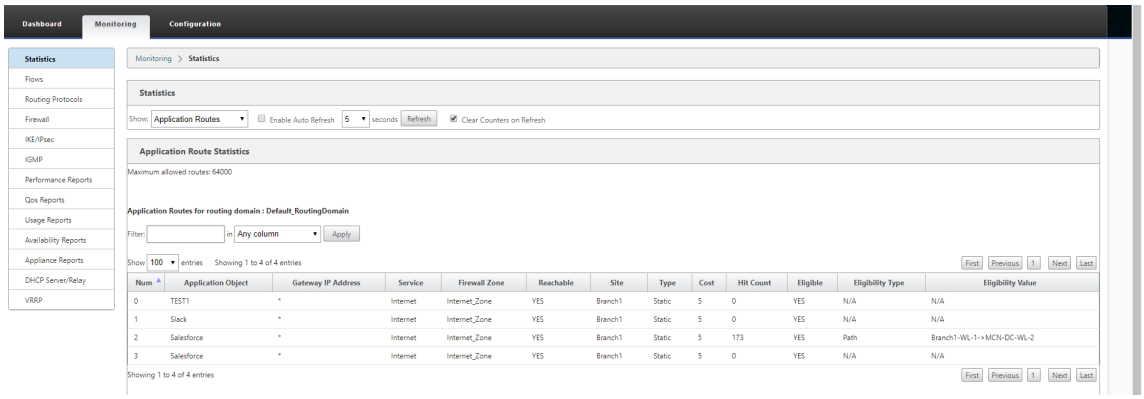
- **Chemin virtuel** : ce service gère le trafic sur les chemins virtuels. Un chemin virtuel est un lien logique entre deux liens WAN. Il comprend un ensemble de chemins WAN combinés pour fournir une communication de niveau de service élevé entre deux nœuds SD-WAN. L'appliance SD-WAN mesure le réseau par chemin d'accès et s'adapte à l'évolution de la demande des applications et des conditions WAN. Un chemin virtuel peut être statique (existe toujours) ou dynamique (existe uniquement 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 l'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 via un chemin virtuel. Le trafic intranet n'est pas encapsulé. Le SD-WAN gère la bande passante en limitant le débit de ce trafic par rapport aux autres types de service en période de congestion. Dans certaines conditions, et si Intranet Fallback est configuré sur le chemin virtuel, le trafic qui circule habituellement via le chemin virtuel peut plutôt 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 de tunnel GRE vous permet de configurer des appliances SD-WAN pour qu'elles terminent les tunnels GRE sur le réseau local. Pour une route avec un tunnel GRE de type service, 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 fonctionnalité Tunnel IPSec LAN vous permet de configurer des appliances SD-WAN pour mettre fin aux tunnels IPSec du 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. Au départ, les paquets passent par la route IP une fois que le trafic est classé et que l'application est connue, la route d'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 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** .



Vous pouvez afficher les statistiques suivantes :

- **Objet Application** : nom de l'objet d'application.
- **Adresse IP de la passerelle : adresse**IP de passerelle utilisée par les objets d'application avec le type de service 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.
- **Joignable** : état de la route de l'application.
- **Site** : Nom du site.
- **Type** : indique si l'itinéraire est statique ou dynamique.
- **Coût** : Priorité de l'itinéraire.
- **Nombre d'accès** : nombre de fois que l'itinéraire de l'application est utilisé pour diriger le trafic.
- **Éligible** : l'itinéraire de l'application est-il éligible pour envoyer le trafic.
- **Type d'éligibilité** : Type de condition d'éligibilité de route appliquée à cet itinéraire. Le type d'éligibilité peut être Chemin, 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

August 31, 2022

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.

Récapitulatif des itinéraires

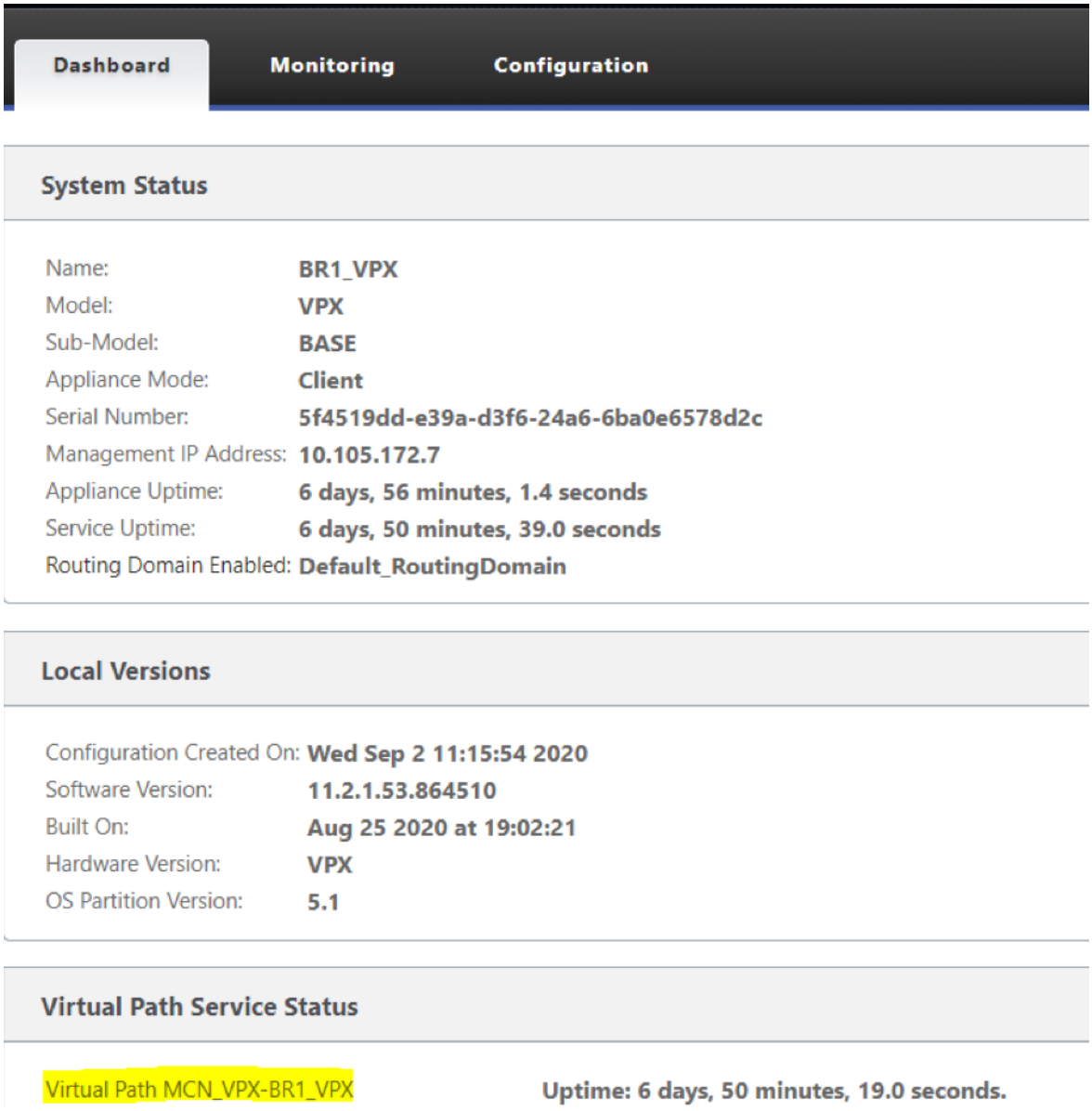
August 31, 2022

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 Rejeter. Cette route récapitulative est annoncée sur les périphériques de saut suivant.

Résolution des problèmes

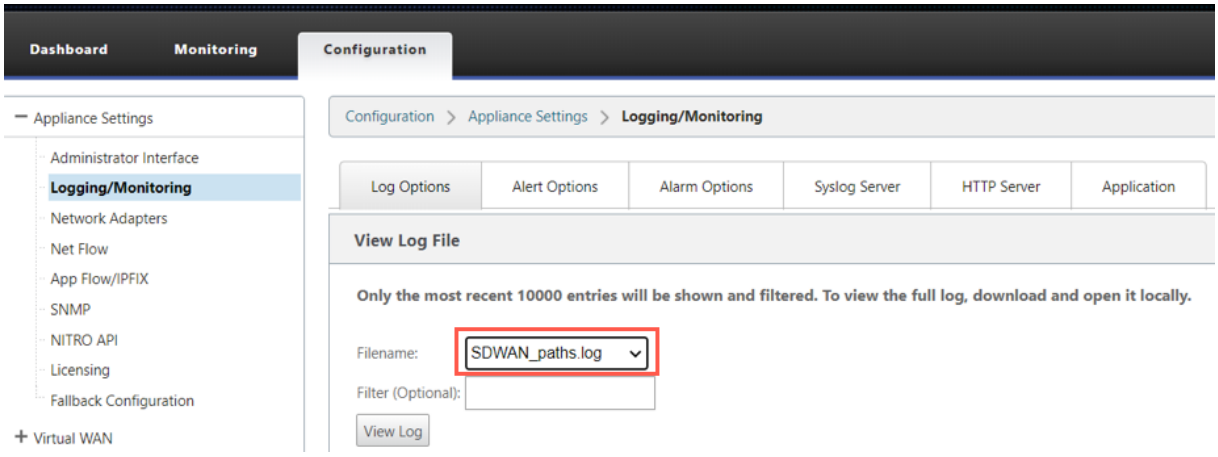
Les routes résumées configurées sur le MCN sont envoyées à la branche via le chemin virtuel. Si vous ne voyez pas les détails du chemin virtuel dans la table de routage de la branche, vérifiez le tableau de bord Branche. Le tableau de bord affiche l'état du chemin virtuel entre le MCN et la branche.



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 du protocole

August 31, 2022

La préférence de protocole est une fonctionnalité spécifique à Citrix SD-WAN, qui est similaire à la distance administrative du routeur. Le protocole avec l'ordre de préférence le plus élevé est le plus préféré. Route utilisant le protocole avec la valeur de préférence de protocole la plus élevée. 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

August 31, 2022

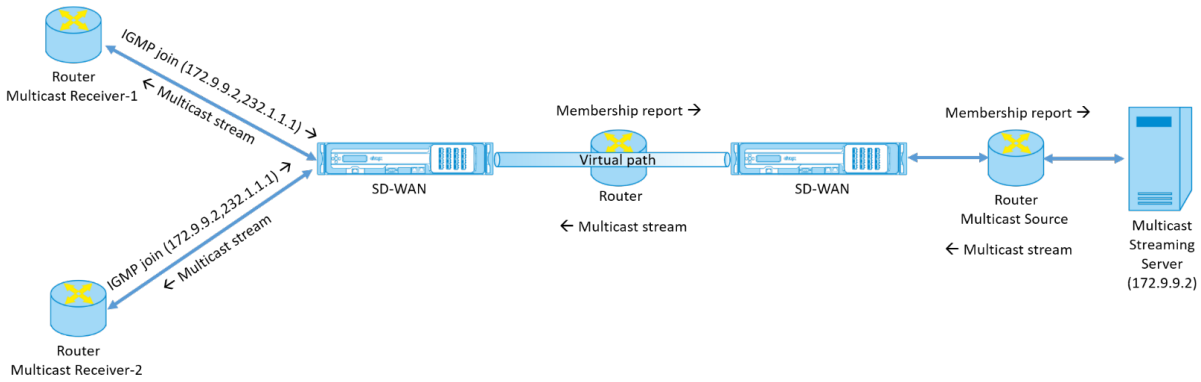
Le routage multidiffusion permet une distribution efficace du trafic un-à-plusieurs. Une source de multidiffusion envoie le trafic de multidiffusion dans un seul flux vers un groupe de multidiffusion. Le groupe de multidiffusion contient des récepteurs tels que des hôtes et des routeurs adjacents qui 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'appliance Citrix SD-WAN, l'appliance 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 spécifique 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'appliance SD-WAN à la source et à la destination.

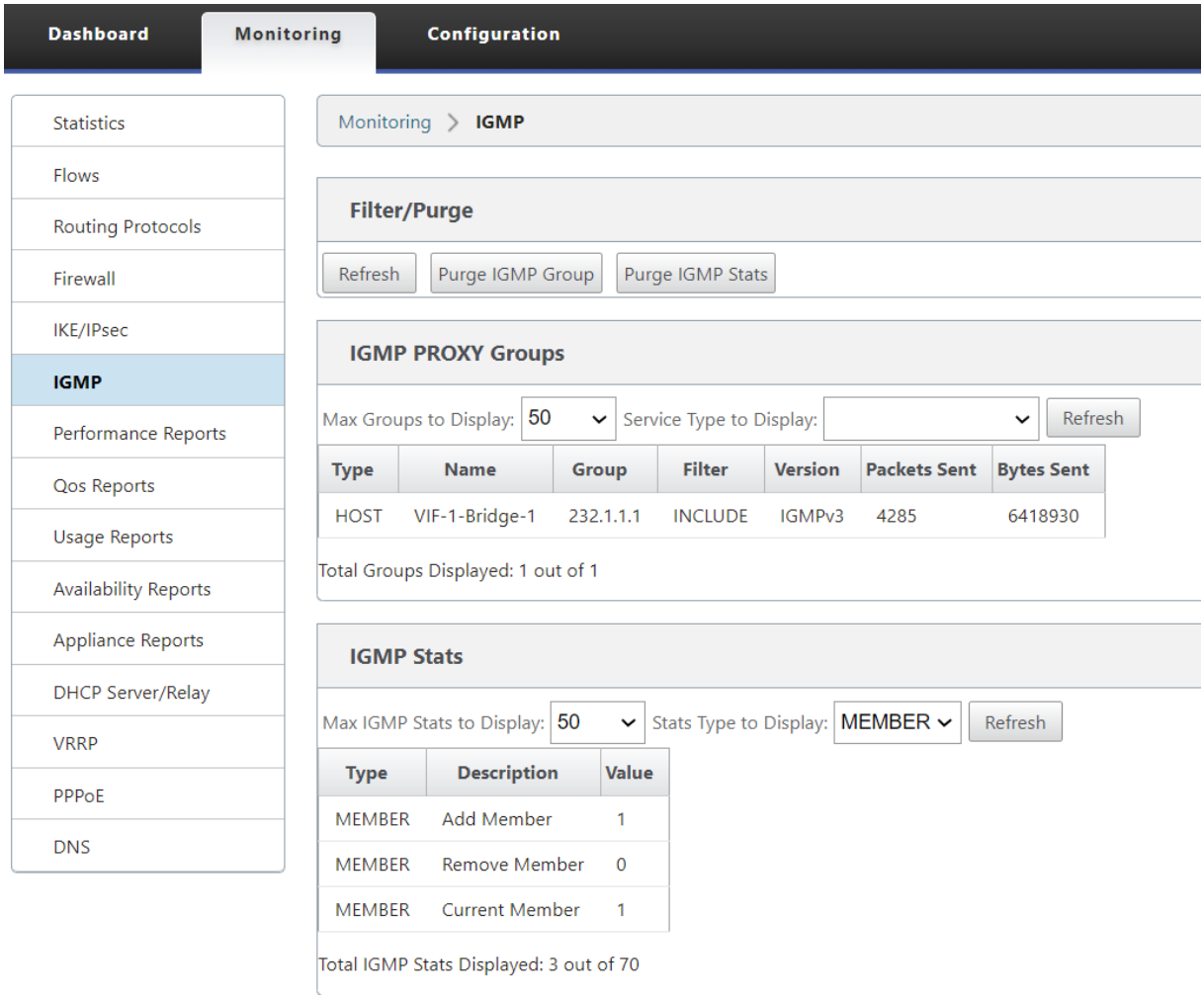
1. Créer un groupe de multidiffusion : indiquez un nom et une adresse IP pour le groupe de multidiffusion. L'IP du groupe de multidiffusion doit se situer dans la plage 232.0.0.0/8 pour la multidiffusion spécifique à la source.
2. Activer le proxy IGMP : vous pouvez configurer l'appliance Citrix SD-WAN 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'appliance 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'appliance à la source et l'appliance à la destination.

Surveillance

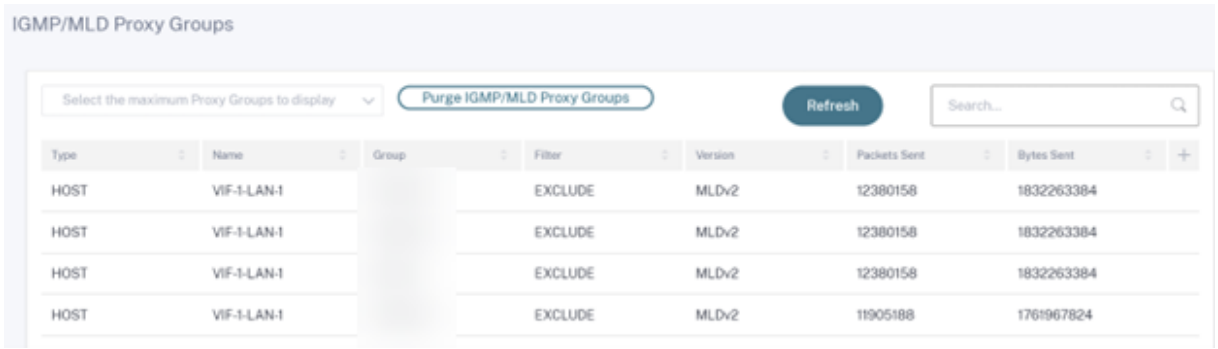
Statistiques IGMP

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 une jointure MLD initiée et le type de message RECV est utilisé pour recevoir des adresses de groupe de multidiffusion. Vous pouvez également consulter les statistiques des messages IGMP/MLD ci-dessous.



L'image suivante présente des informations sur les groupes proxy IGMP/MLD. Vous pouvez également consulter les statistiques du groupe proxy IGMP/MLD et la version utilisée.



Configurer le coût d'itinéraire de chemin virtuel

August 31, 2022

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 branche 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'itinéraires sur un chemin virtuel spécifique au lieu du coût du site par défaut. Avec cela, nous pouvons manipuler quel 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.

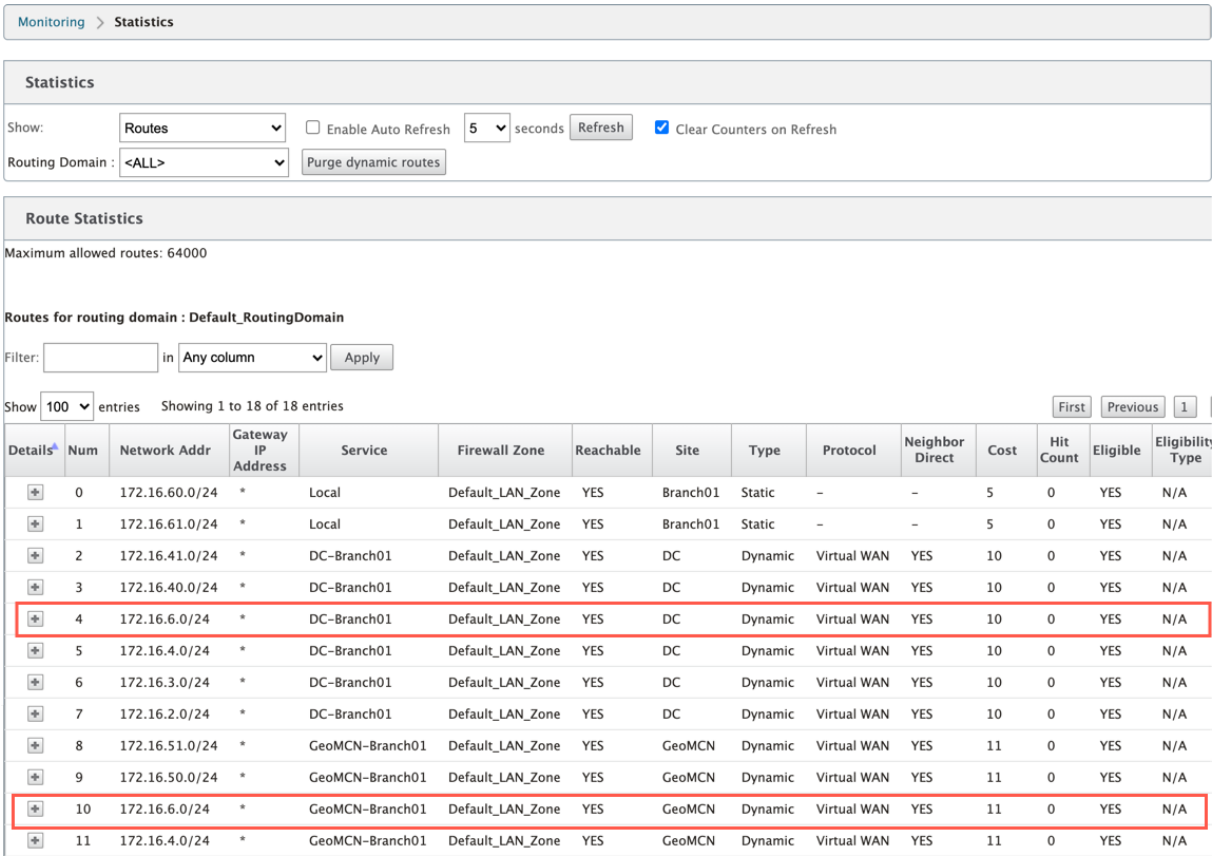
> **Remarque**
>
> Le coût d'acheminement VP déprécie le coût de transfert WAN vers WAN qui existait dans les versions antérieures à la version 10.0. Les décisions de routage basées sur les coûts de transfert WAN vers WAN doivent être réinfluencées par l'utilisation du coût de route VP, car le coût de transfert WAN vers WAN n'a aucune importance lorsque vous migrez vers la version 10.0.

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.



Configurer le protocole de redondance du routeur virtuel

August 31, 2022

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 secours 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 secours. 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.

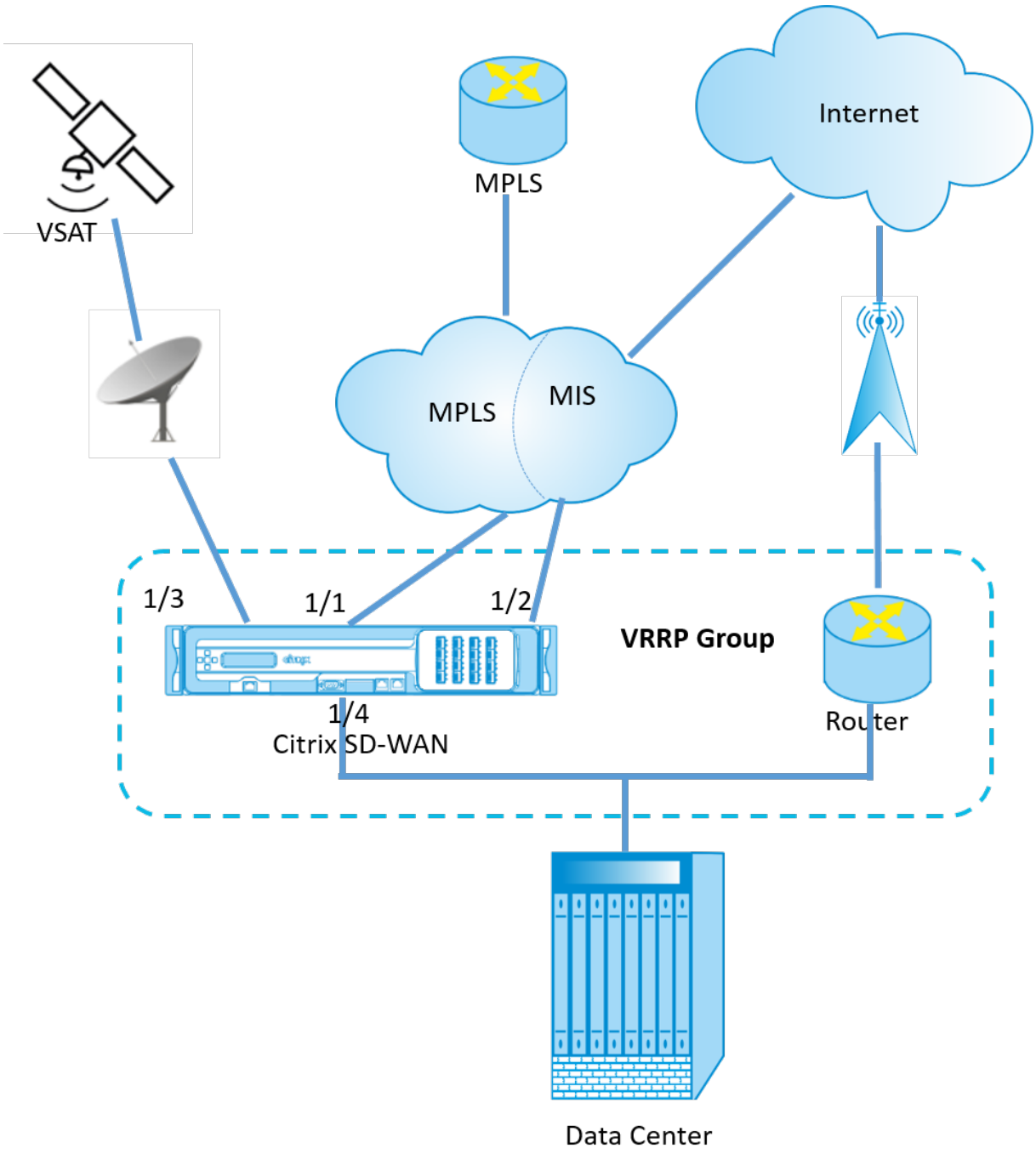
VRRP spécifie un processus d'élection dans lequel, le routeur ayant la priorité la plus élevée devient le maître. Si la priorité est la même parmi les routeurs, le routeur avec l'adresse IP la plus élevée devient

le maître. Les autres routeurs sont en état de sauvegarde. Le processus d'élection est relancé si le maître échoue, si un nouveau routeur rejoint le groupe ou si un routeur existant quitte le groupe.

VRRP garantit un chemin par défaut haute disponibilité sans configurer les protocoles de routage dynamique ou de découverte de routeurs sur chaque hôte final.

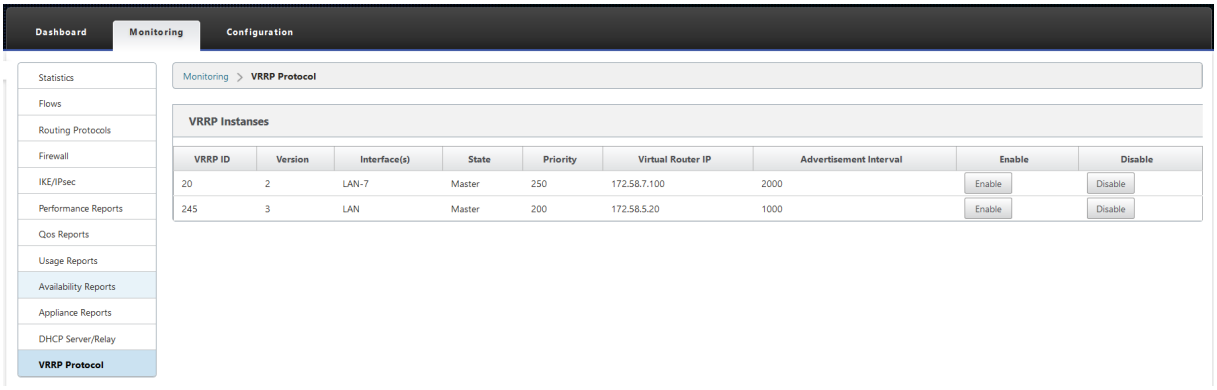
Citrix SD-WAN version 10.1 prend en charge les versions 2 et 3 de VRRP pour interagir avec tous les routeurs tiers. L'appliance SD-WAN agit comme un routeur maître et dirige le trafic vers l'utilisation du service de chemin virtuel entre les sites. Vous pouvez configurer l'appliance SD-WAN en tant que 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 un dispositif Citrix SD-WAN et un routeur configuré 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.



Statistiques VRRP

Vous pouvez consulter les statistiques VRRP sous **Surveillance** > **VRRP**.



Vous pouvez afficher les données statistiques suivantes :

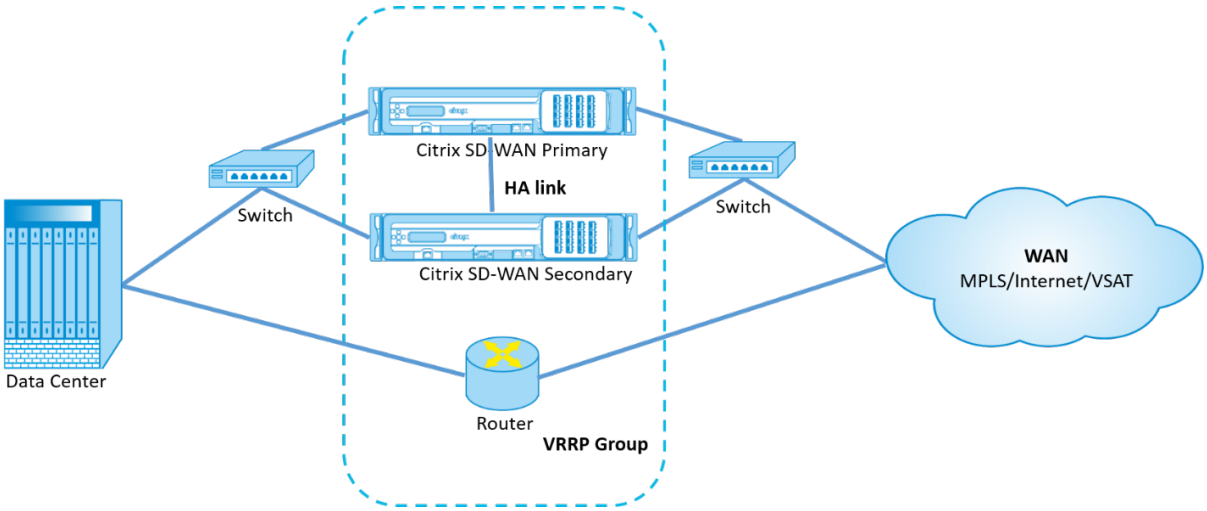
- ID**VRRP : ID** du groupe VRRP
- **Version : version** du protocole VRRP.
- **Interface :** Interface virtuelle utilisée pour le VRRP.
- **État : état** VRRP de l'appliance SD-WAN. Il indique si l'appliance est une solution principale ou une sauvegarde.
- Priorité **: priorité** de l'appliance SD-WAN pour un groupe VRRP
- **IP du routeur virtuel :** adresse IP du routeur virtuel du groupe VRRP.
- **Intervalle publicitaire :** 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 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 exploitant à la fois la haute disponibilité et les fonctionnalités VRRP de votre réseau SD-WAN. Déployez une paire d'appliances Citrix SD-WAN dans des rôles actif/de secours avec 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, consultez la section Haute disponibilité.

Prise en charge du routage pour la segmentation LAN

August 31, 2022

Les appliances SD-WAN Standard Edition implémentent la segmentation LAN sur des sites distincts où l'une ou l'autre des appliances est déployée. Les appliances reconnaissent et conservent un enregistrement des VLAN côté LAN disponibles, et configurent des règles concernant les autres segments

LAN (VLAN) auxquels les autres segments LAN (VLAN) peuvent se connecter sur un site distant avec une autre appliance SD-WAN Standard Edition.

La fonctionnalité ci-dessus est mise en œuvre à l'aide d'une table Virtual Routing and Forwarding (VRF) qui est conservée dans l'appliance SD-WAN Standard Edition, qui permet de suivre les plages d'adresses IP distantes accessibles à un segment LAN local. Ce trafic VLAN vers VLAN traverserait toujours le WAN via le même chemin virtuel préétabli entre les deux appliances (aucun nouveau chemin n'a besoin d'être créé).

Un exemple de cas d'utilisation pour cette fonctionnalité est qu'un administrateur WAN peut segmenter l'environnement de réseau local de succursale 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 cet accès.

Service de domaine d'interroutage

August 31, 2022

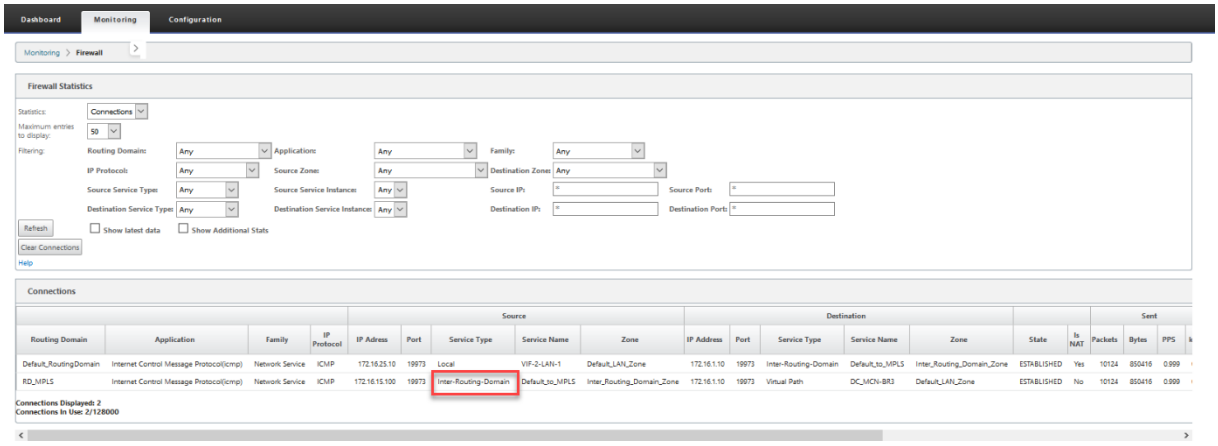
Citrix SD-WAN vous permet de segmenter le réseau à l'aide des domaines de routage, assurant ainsi une sécurité élevée et une gestion facile. Avec l'utilisation du domaine de routage, le trafic est isolé l'un de l'autre dans le réseau de superposition. Chaque domaine de routage conserve sa propre table de routage. 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'interroutage 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'interroutage 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.

Surveillance

Vous pouvez afficher les statistiques de surveillance des connexions qui utilisent des services inter-routing-domaine sous **Surveillance** > **Statistiques de pare-feu** > **Connexions**.



Équilibrage de charge ECMP

August 31, 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 :

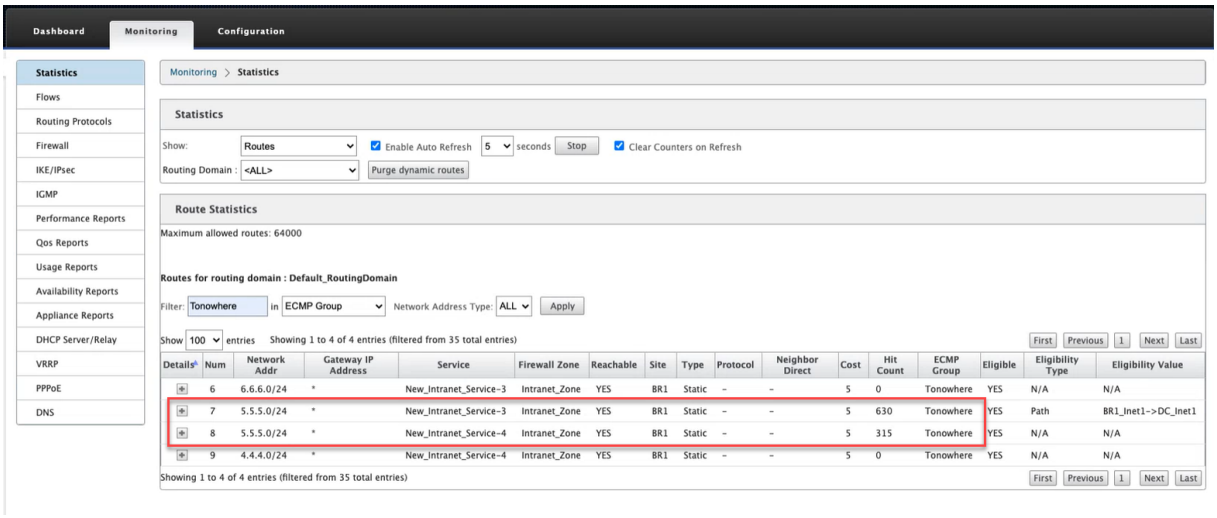
- Répartition du trafic sur plusieurs chemins à coût égal.
- Utilisation optimale de la bande passante disponible.
- Transfert dynamique du trafic vers un autre chemin d'accès membre ECMP, en cas d'échec d'une liaison. ECMP prend en charge les routes statiques sur les tunnels IPsec/GRE.

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 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.



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).

Sécurité

August 31, 2022

Les rubriques de cette section fournissent des conseils de sécurité généraux 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

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 :

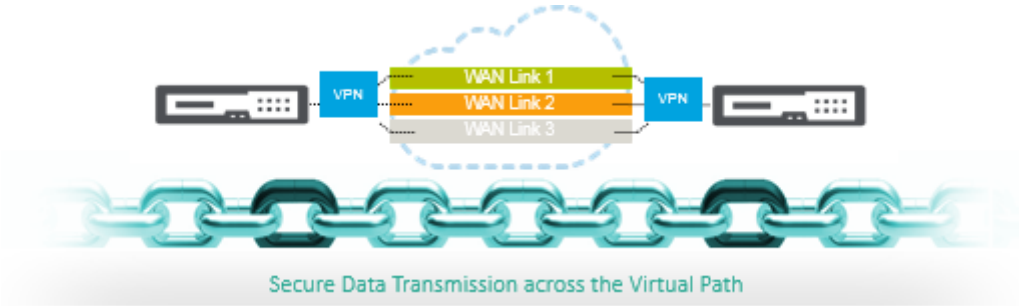
- Tunnels IPSec
- Firewall

Terminaison du tunnel IPSec

August 31, 2022

Citrix SD-WAN prend en charge les chemins virtuels IPSec, permettant aux périphériques tiers de mettre fin aux tunnels VPN IPsec du côté LAN ou WAN d'une appliance Citrix SD-WAN. Vous pouvez sécuriser les tunnels IPSec de 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 tunnel IPsec résilient à l'aide d'un mécanisme de tunnel de chemin virtuel différencié.



> **Remarque importante** :
>
> - À partir de la version SD-WAN 11.5, toutes les configurations de tunnel IPsec et tous les paramètres IKE sont pris en charge uniquement via le service Citrix SD-WAN Orchestrator. Pour plus d'informations sur les configurations IPsec/IKE du service Citrix SD-WAN Orchestrator, consultez la section Service IPSec.
> - Citrix SD-WAN prend en charge la connectivité à Oracle Cloud Infrastructure (OCI) via IPsec.

Intégration de Citrix SD-WAN avec AWS Transit Gateway

November 16, 2022

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).

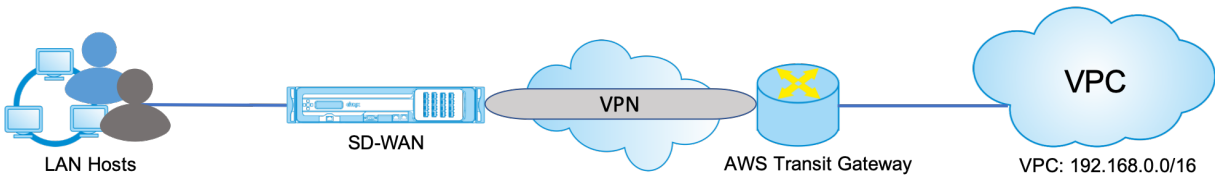
3. Attachez un VPN à la passerelle Transit Gateway configurée où le VPN se trouve avec un site SD-WAN situé sur site Web ou dans n'importe quel cloud (AWS, Azure ou GCP).
4. Établissez l'appairage BGP (Border Gateway Protocol) sur le tunnel IPsec avec AWS Transit Gateway à partir de Citrix SD-WAN pour 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.

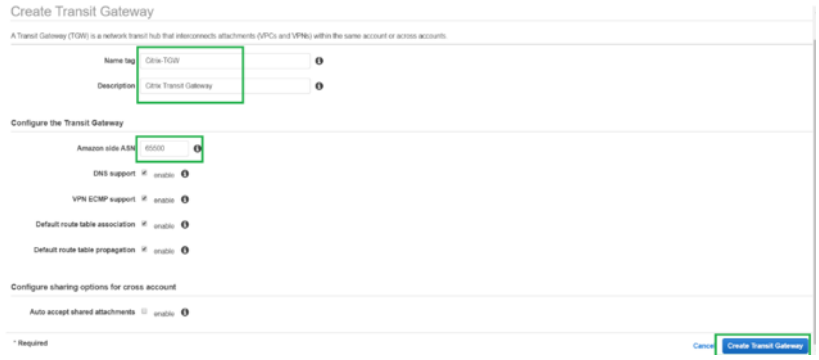
Quelle que soit la méthode choisie, le trafic atteint les VPC connectés à Transit Gateway sans gérer manuellement le routage dans AWS infra.



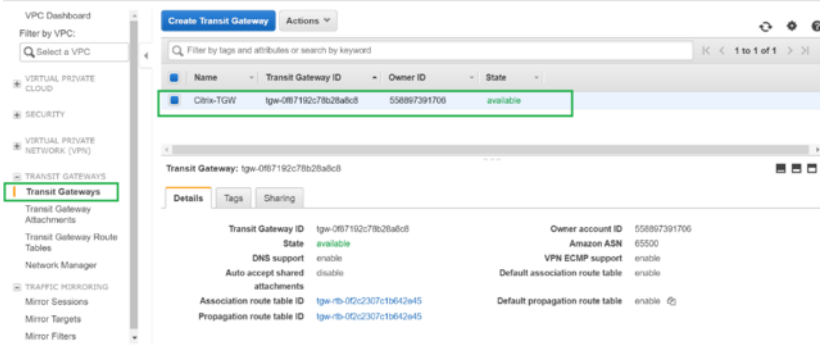
Configuration AWS Transit Gateway

Pour créer **AWS Transit Gateway**, accédez au tableau de bord VPC et accédez à la section **Transit Gateway** .

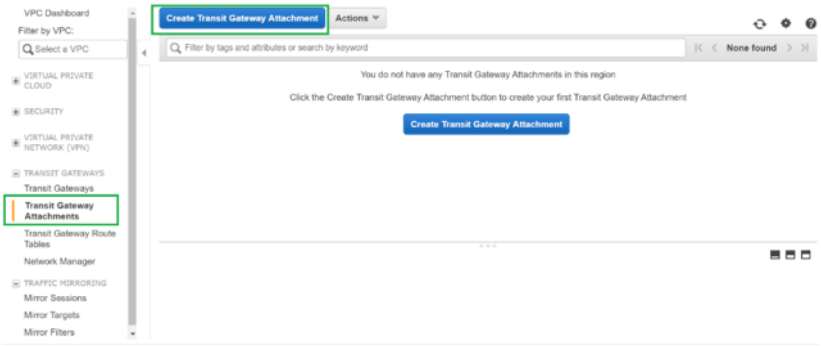
1. Indiquez le nom, la description et le numéro ASN Amazon Transit Gateway comme indiqué dans la capture d'écran suivante, puis cliquez sur **Créer une passerelle de transit**.



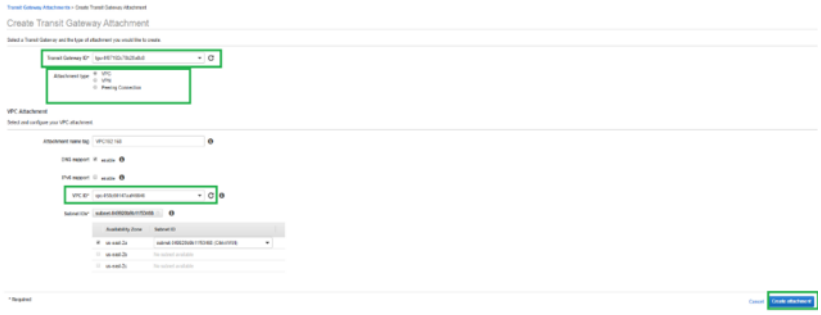
Une fois la création de la passerelle de transit terminée, vous pouvez voir le statut **Disponible**.



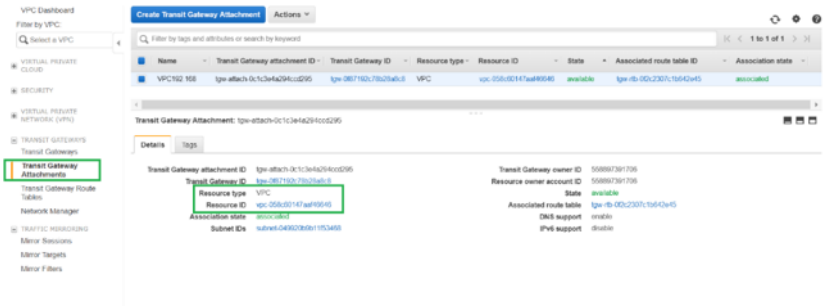
2. Pour créer les **pièces jointes de la passerelle de transit**, accédez à **Passerelles de transit > Pièces jointes de passerelle** de **transit et cliquez sur Créer une pièce jointe de passerelle**de



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.

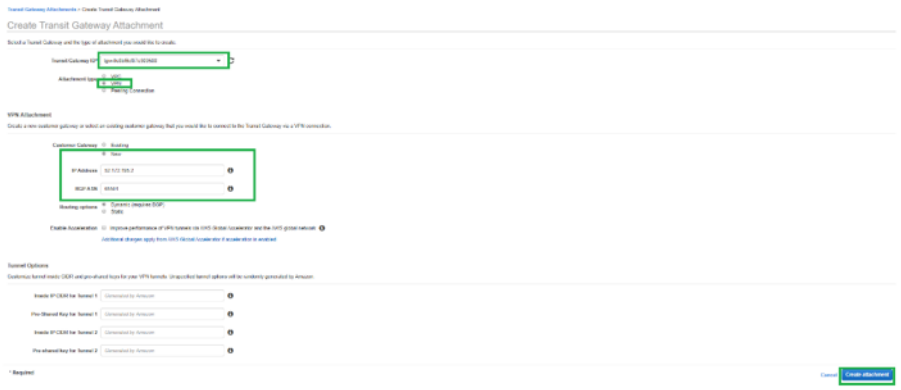


4. Après avoir attaché le VPC à la passerelle de transit, vous pouvez voir que le **type de ressource VPC** a été associé à la passerelle Transit.

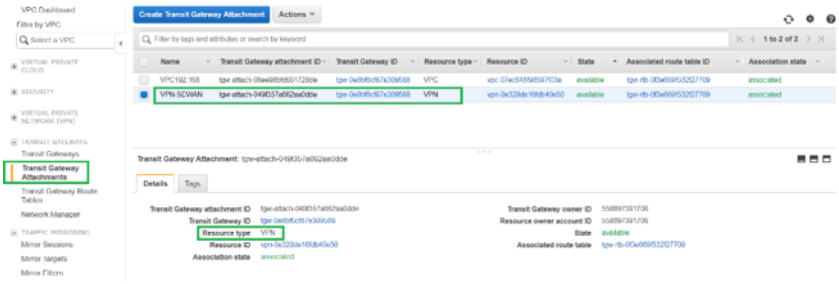


5. Pour attacher le SD-WAN à la passerelle de transit à l'aide du VPN, sélectionnez l'**ID de passerelle Transit** dans la liste déroulante et sélectionnez **Type de pièce jointe** en tant que **VPN**. Assurez-vous de sélectionner le bon ID Transit Gateway.

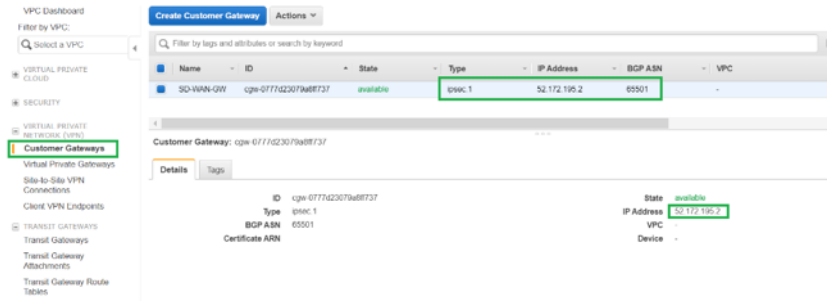
   Joignez une nouvelle passerelle client VPN en fournissant l'adresse IP publique du lien WAN SD-WAN et son numéro ASN BGP. Cliquez sur **Créer une pièce jointe** pour attacher VPN à Transit Gateway.



6. Une fois le VPN attaché à la Transit Gateway, vous pouvez afficher les détails comme indiqué dans la capture d'écran suivante :

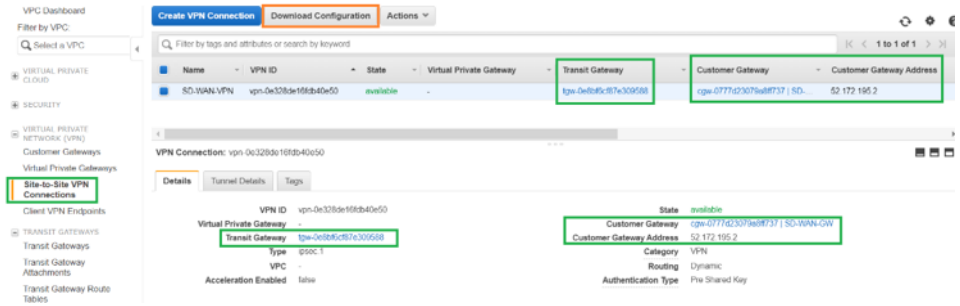


7. Sous **Passerelles client, la passerelle**client SD-WAN et la connexion VPN de site à site sont créées dans le cadre de l'Attachement VPN à Transit Gateway. Vous pouvez voir que la passerelle client SD-WAN est créée avec l'adresse IP de cette passerelle client qui représente l'adresse IP publique de liaison WAN du SD-WAN.

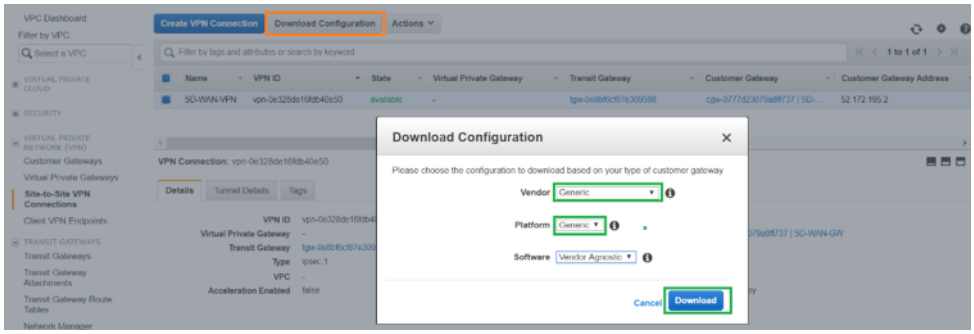


8. Accédez à **Connexions VPN site** à site pour télécharger la **configuration VPN SD-WAN Customer Gateway**. Ce fichier de configuration contient deux détails de tunnel IPsec ainsi que les informations d'homologue BGP. Deux tunnels sont créés à partir du SD-WAN vers Transit Gateway pour la redondance.

   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 :

!Deux tunnels IPSec

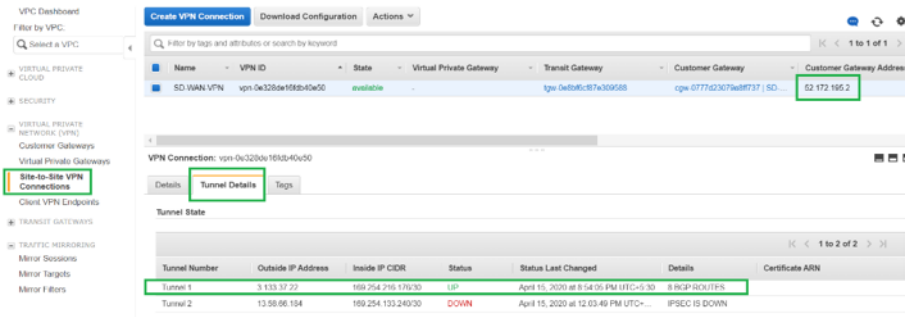
Configurer le service Intranet sur SD-WAN

Pour configurer un service Intranet via le service Citrix SD-WAN Orchestrator, accédez à Delivery Services.

Surveillance et dépannage sur AWS

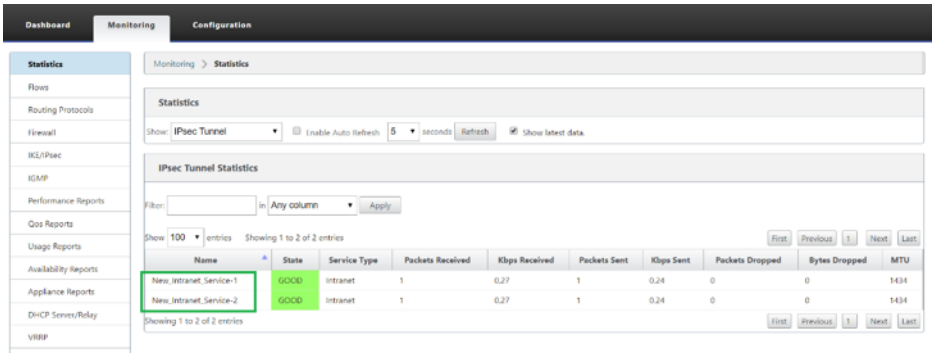
1. Pour vérifier l'état de l'établissement du tunnel IPSec sur AWS, accédez à **RÉSEAU PRIVÉ VIRTUEL (VPN) > Connexions VPN de site à site**. Dans la capture d'écran suivante, vous pouvez observer que l'adresse de passerelle client représente l'adresse IP publique SD-WAN Link à l'aide de laquelle vous 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.

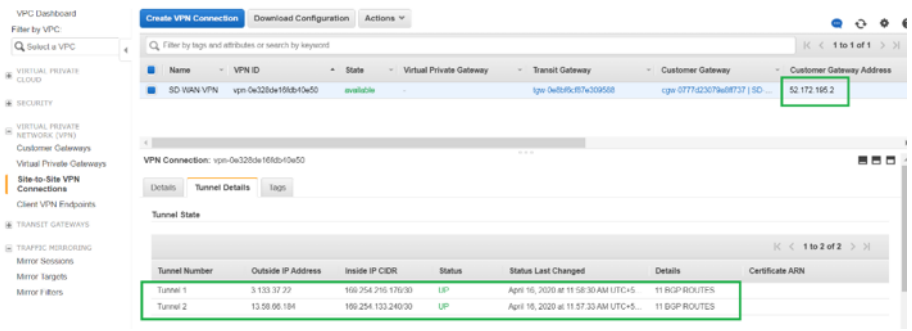


2. Configurez les détails IPsec et BGP relatifs au deuxième tunnel en fonction du fichier de configuration téléchargé sur SD-WAN.

   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 :



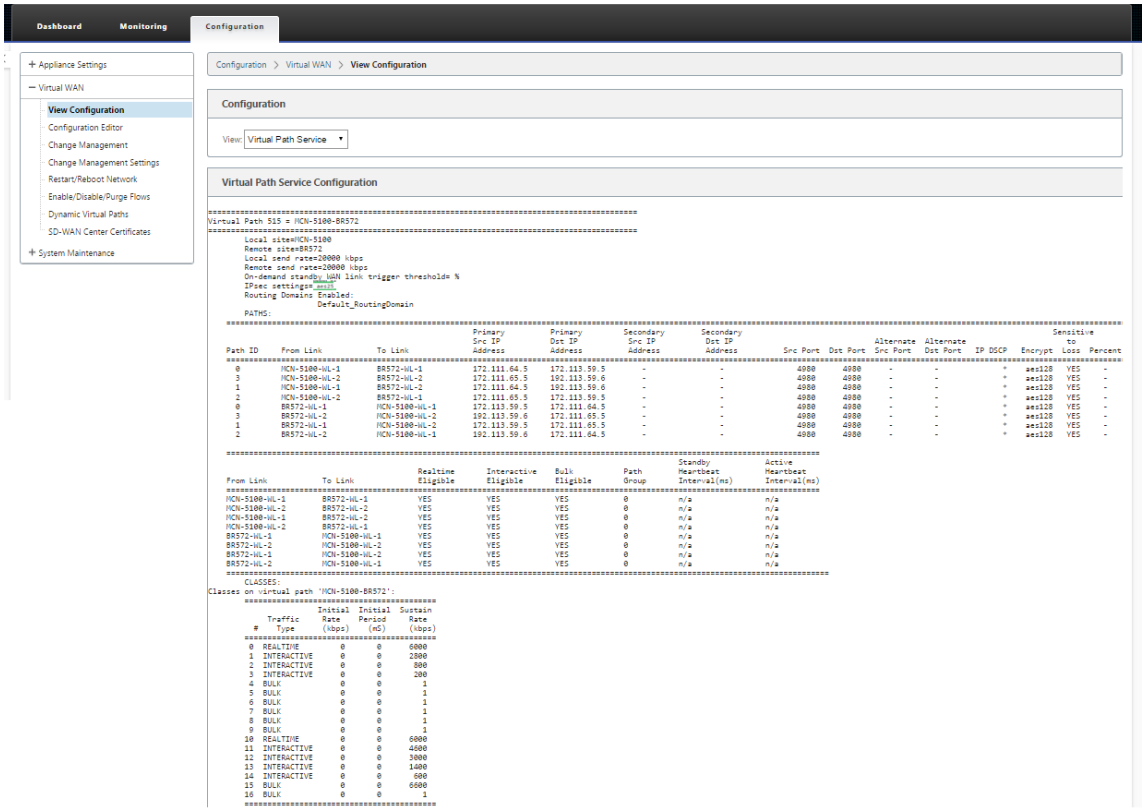
Comment afficher la configuration du tunnel ipsec

August 31, 2022

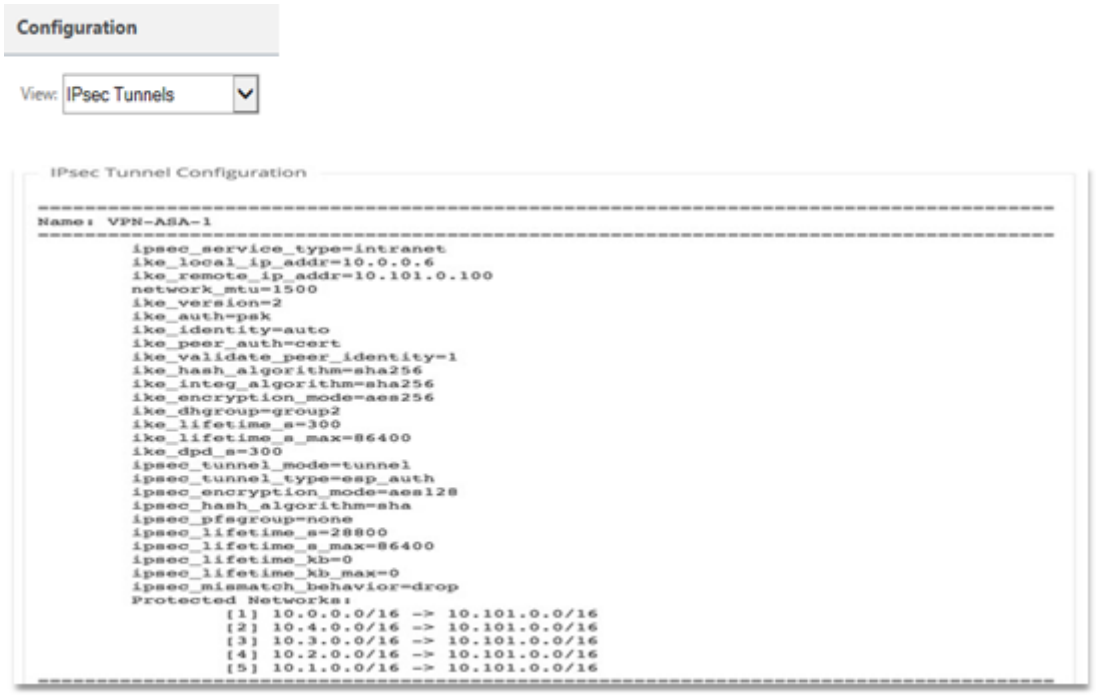
Pour afficher la configuration du tunnel ipsec :

1. Accédez à **Configuration > Virtual WAN** > **Afficher la configuration**.

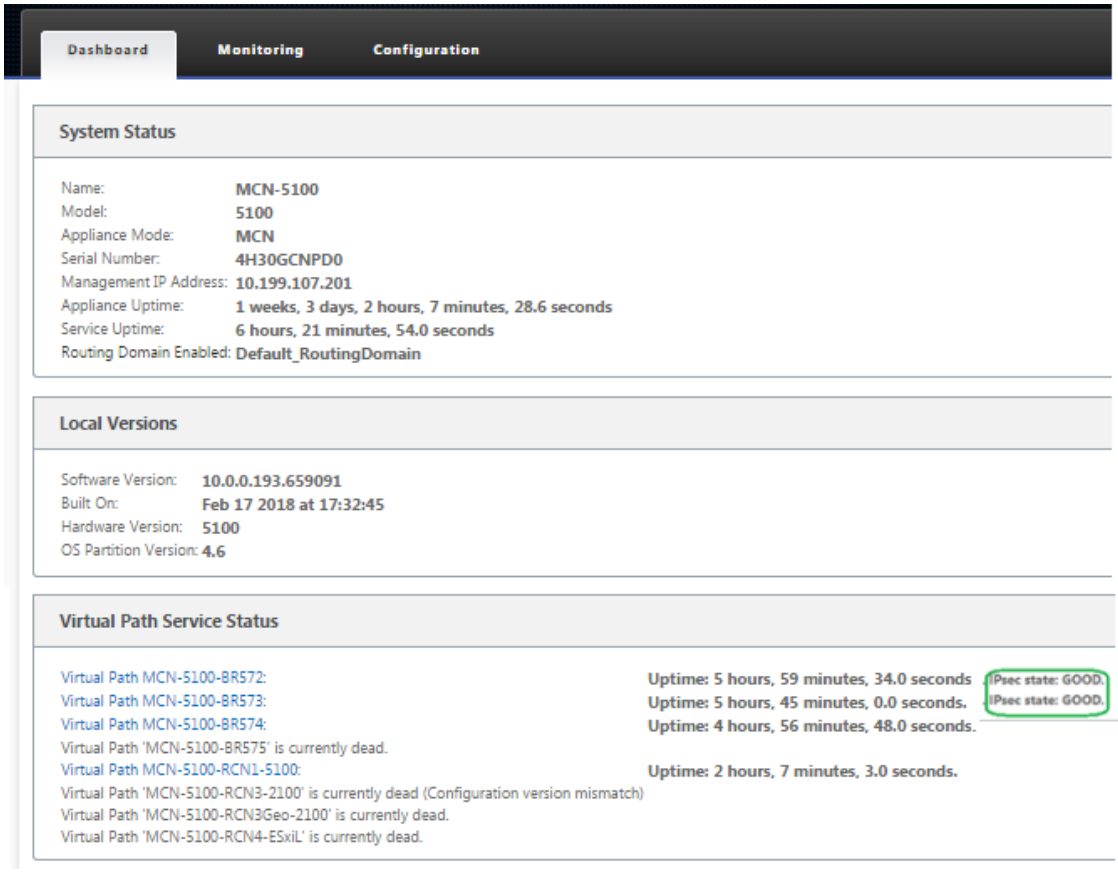
2. Sélectionnez **Virtual Path Service** dans le menu déroulant. Les paramètres IPSec ne s'affichent que si IPsec est activé.



3. Sélectionnez **Tunnels IPsec** dans le menu déroulant pour afficher la configuration du tunnel IPsec.



4. Chaque chemin virtuel affichera son propre statut de tunnel IPSec comme indiqué ci-dessous.

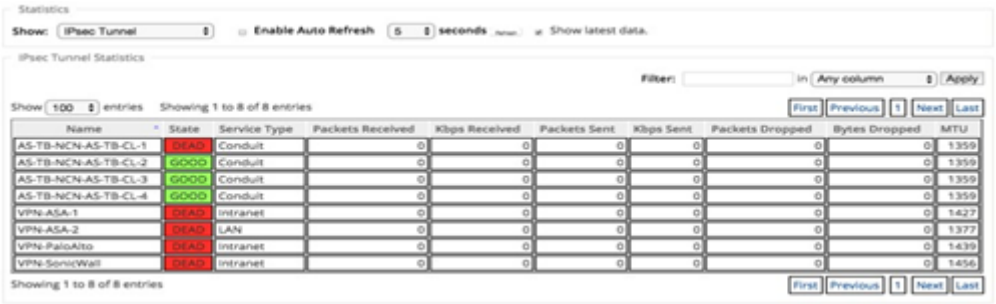


Surveillance et journalisation IPSec

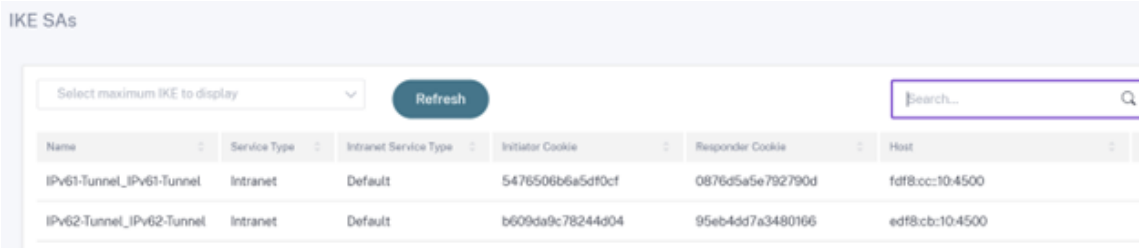
August 31, 2022

Pour surveiller les statistiques IPsec/IKE SA :

1. Accédez à **Surveiller > IPsec**. Choisissez **IPSec SA** :



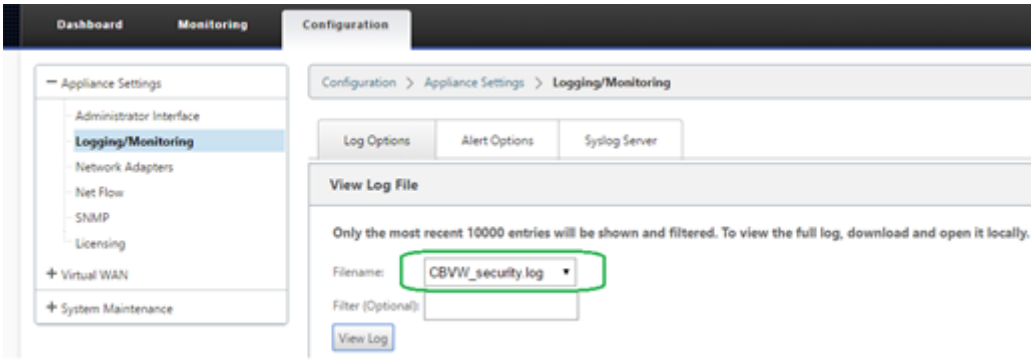
2. Accédez à **Monitor** > **IKE SAs**. Observez les tunnels IPSec configurés, les associations de service IKE et IPSec entre deux points de terminaison VPN ou mode configurés dans le réseau SD-WAN.

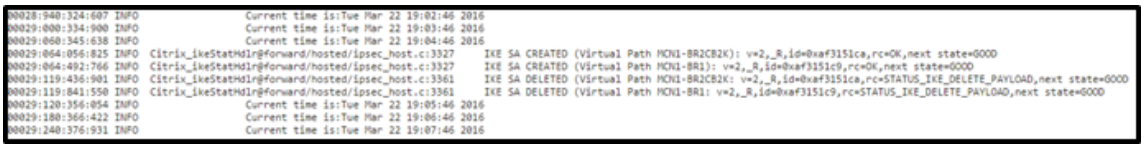


Comment surveiller les journaux IPSec

1. Accédez à **Configuration** > **Paramètres de l'appliance** > **Journalisation/surveillance**. Sélectionnez **Nom de fichier** dans le menu déroulant, puis cliquez sur **Afficher le journal**. Vous pouvez afficher les détails de journal suivants pour le tunnel IPSec :

    - Création et suppression du tunnel IPSec
    - Modification de l'état du tunnel IPSec

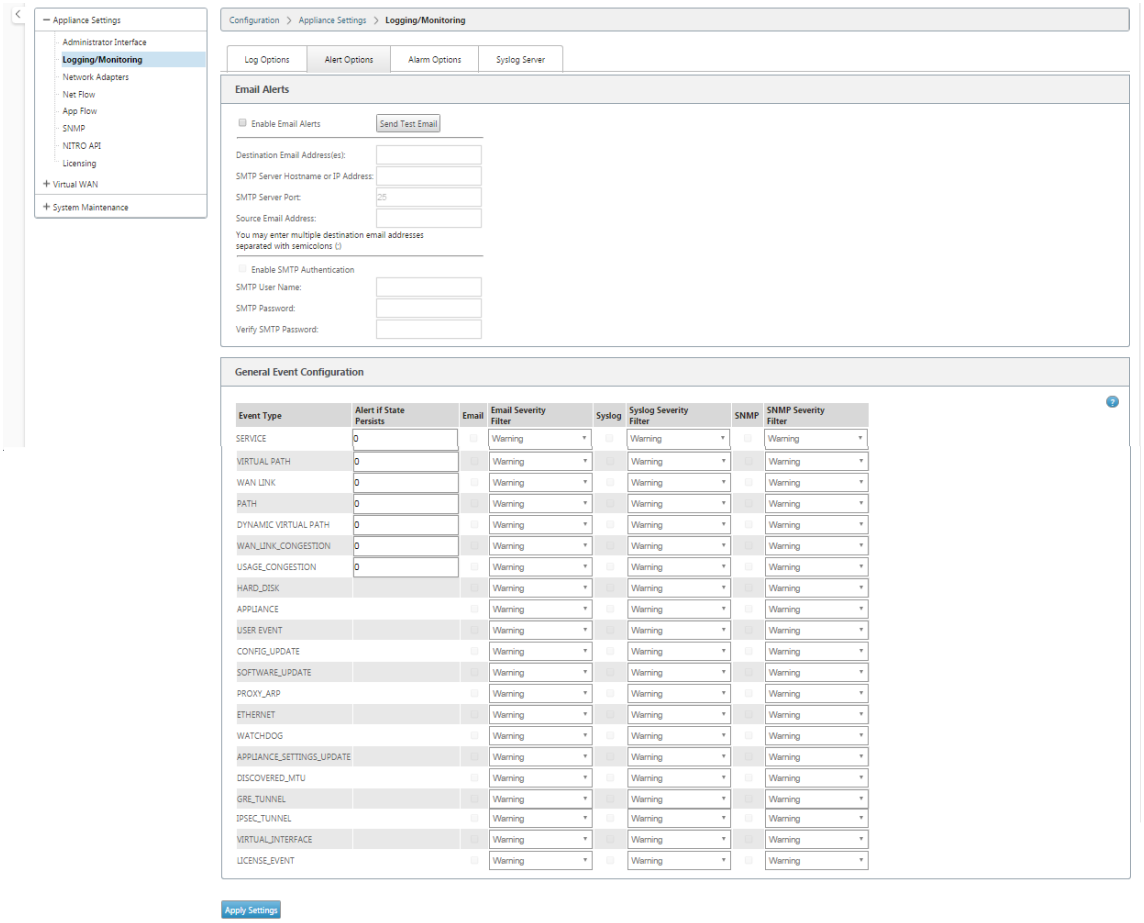




Comment afficher les alertes du tunnel IPSec

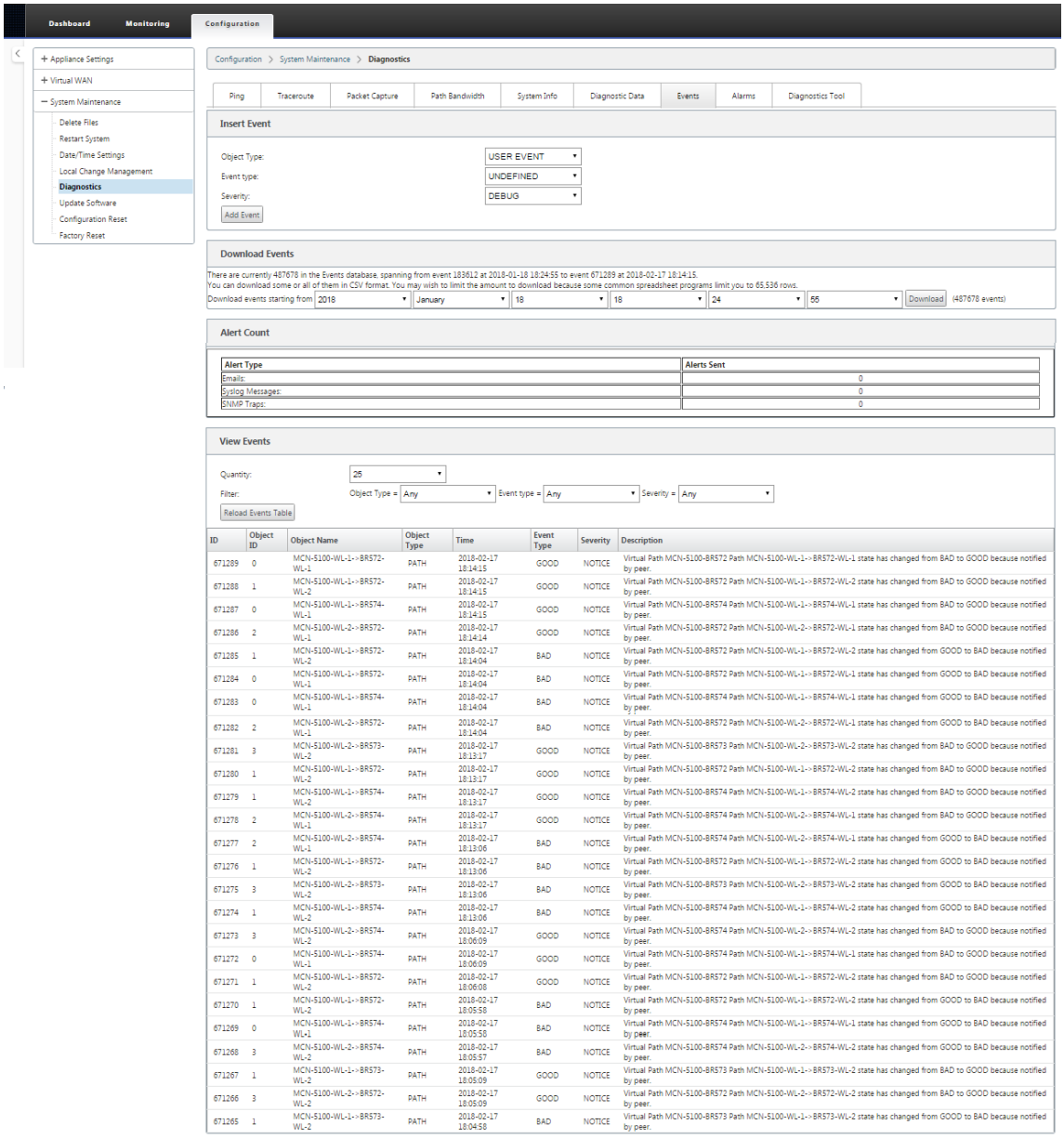
1. Accédez à **Configuration** > **Paramètres du matériel > Journalisation/surveillance** > **Options d'alerte**.
2. Créer des alertes Email et Syslog pour les rapports d'état du tunnel IPSec.

    - Prend en charge IPSEC_TUNNEL comme l'un des types d'événements qui vous permet de configurer les filtres de gravité Email et Syslog.



Comment surveiller les événements du tunnel IPSec

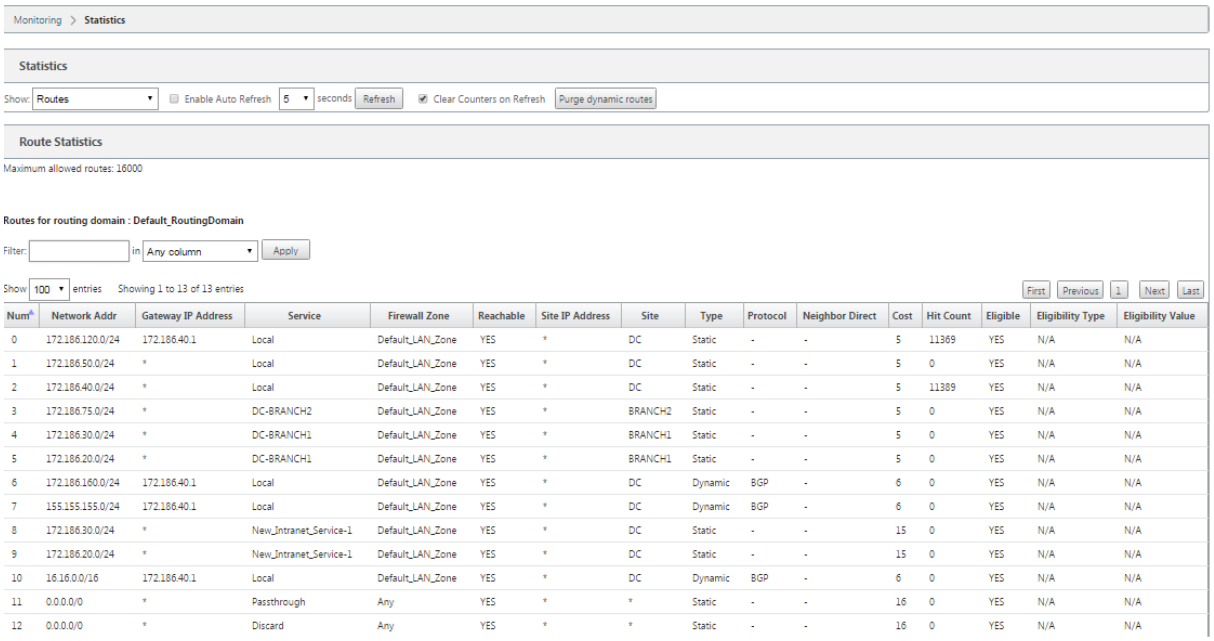
1. Accédez à **Configuration > Maintenance du système** > **Diagnostics** > **Événements** .
2. Ajoutez des événements en fonction du type d'objet **IPSEC_TUNNEL** . Créez des filtres pour tous les événements liés à IPSec.



Admissibilité pour les routes de chemin non virtuels ipsec

August 31, 2022

Dans les versions précédentes, les routes de tunnel ipsec resteraient dans la table de routage, même si le tunnel était indisponible.



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

Conformité aux normes FIPS

August 31, 2022

Dans Citrix SD-WAN, le mode FIPS oblige les utilisateurs à configurer des paramètres conformes à FIPS pour leurs tunnels IPsec et les paramètres IPsec pour les chemins virtuels.

- Affiche le mode IKE conforme à la norme FIPS.
- Affiche un groupe IKE DH conforme à FIPS dans lequel les utilisateurs peuvent sélectionner les paramètres requis pour configurer l'appliance en mode FIPS (2,5,14 —21).
- Affiche le type de tunnel IPSec conforme à FIPS dans les paramètres IPSec pour les chemins virtuels
- Mode Hash IKE et intégrité (IKEV2), mode Auth IPSec.
- Effectue des erreurs d'audit pour les paramètres de vie basés sur FIPS

Pour activer la conformité FIPS à l'aide du service Citrix SD-WAN Orchestrator, consultez la section Mode FIPS.

Passerelle Web sécurisée Citrix SD-WAN

August 31, 2022

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 politiques cohérentes sur l'ensemble des sites. Et si vous avez de nombreuses succursales, la gestion des coûts devient impossible.

Zscaler :

La solution idéale pour renforcer la sécurité sans ajouter de coûts, de complexité ou de latence consiste à acheminer tout le trafic Internet des succursales depuis l'appliance Citrix SD-WAN vers Zscaler Cloud Security Platform. 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 besoin d'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 pas de normes volontaires. FIPS aborde les problèmes suivants :

- Compatibilité entre les 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 :

En utilisant 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 16, 2022

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.

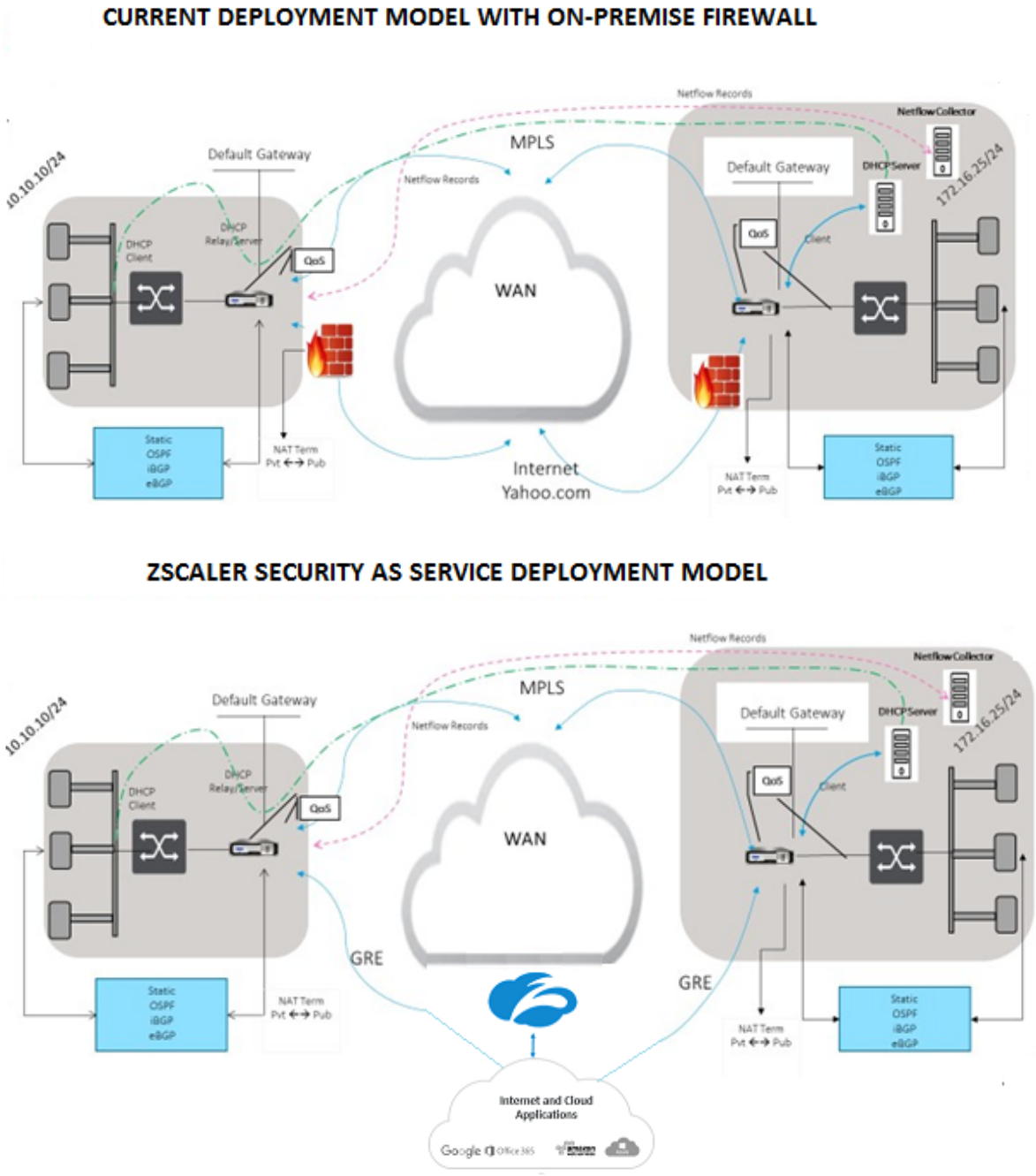
Les appliances Citrix SD-WAN peuvent se connecter à un réseau cloud Zscaler via des tunnels GRE sur le site du client. Un déploiement Zscaler utilisant des appliances SD-WAN prend en charge les fonctionnalités suivantes :

- 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



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

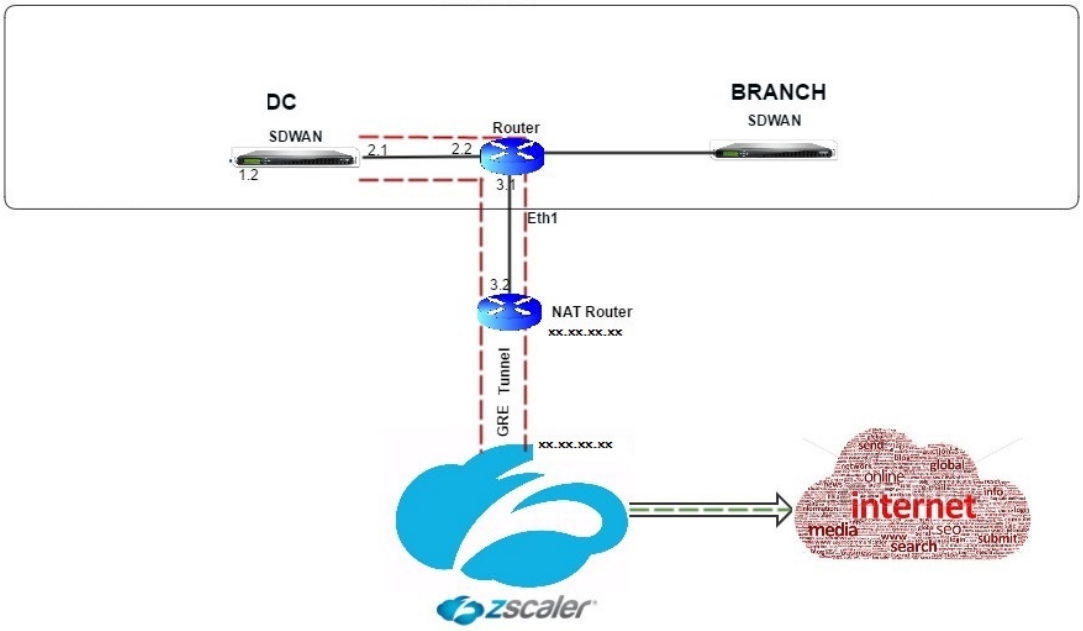
Configuration d'un service Internet

Pour configurer un service Internet via le service Citrix SD-WAN Orchestrator, consultez la section Services de miseà disposition. Pour plus d'informations sur l'activation du service Internet pour un site, consultez Direct Internet Breakout.

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 le tunnel GRE via le service Cirix SD-WAN Orchestrator, reportez-vous à la section 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.

> **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 automatiquement 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.

Pour surveiller les statistiques des tunnels GRE et IPsec :

Dans l'interface Web SD-WAN, accédez à **Surveillance** > **Statistiques** > [**Tunnel GRE**]	**Tunnel IPSec**].

Pour plus d'informations, consultez la rubrique Surveillance des tunnels IPSec et des tunnels GRE .

Prise en charge de la redirection du trafic pare-feu à l'aide de Forcepoint dans Citrix SD-WAN

August 31, 2022

Forcepoint prend en charge les fonctionnalités suivantes, bien que le SD-WAN ne prenne en charge que la fonction de redirection du pare-feu :

- IPsec avec PKI
- IPSec avec PSK
- Chaînage par proxy à l'aide de la configuration de fichier PAC
- Chaînage par proxy avec en-têtes standard
- Chaînage par proxy avec en-têtes propriétaires supprimant la nécessité de configurer la plage IP du client - partenariat/développement
- Redirection du pare-feu (proxy transparent par NAT de destination)

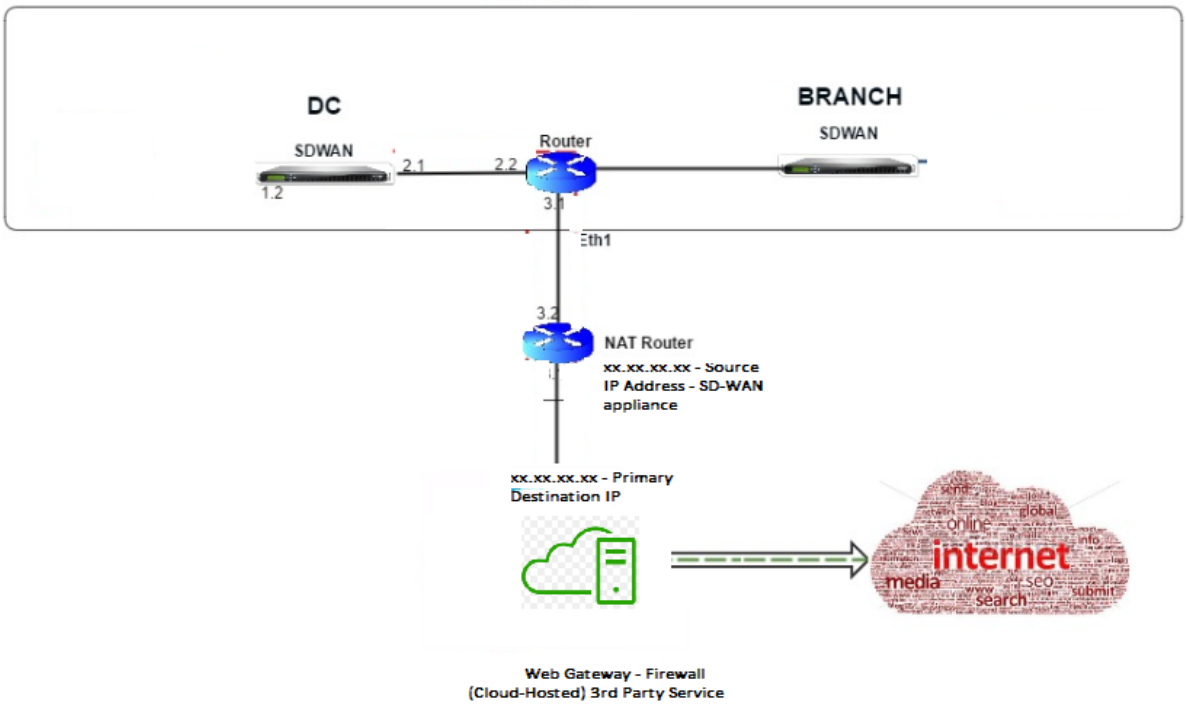
La stratégie NAT de destination permet aux entreprises d'acheminer le trafic Internet via un service de sécurité hébergé dans le cloud à l'aide de ForcePoint.

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 au site du portail Forcepoint. Créez une stratégie en fournissant l'adresse IP publique d'entreprise via laquelle le trafic Internet doit être redirigé vers Forcepoint. Obtenir les adresses IP primaires 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 vers l'adresse IP de destination principale de la passerelle de pare-feu basée sur le cloud avec les ports externes 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.

Vous pouvez configurer NAT à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Traduction d'adresses réseau.

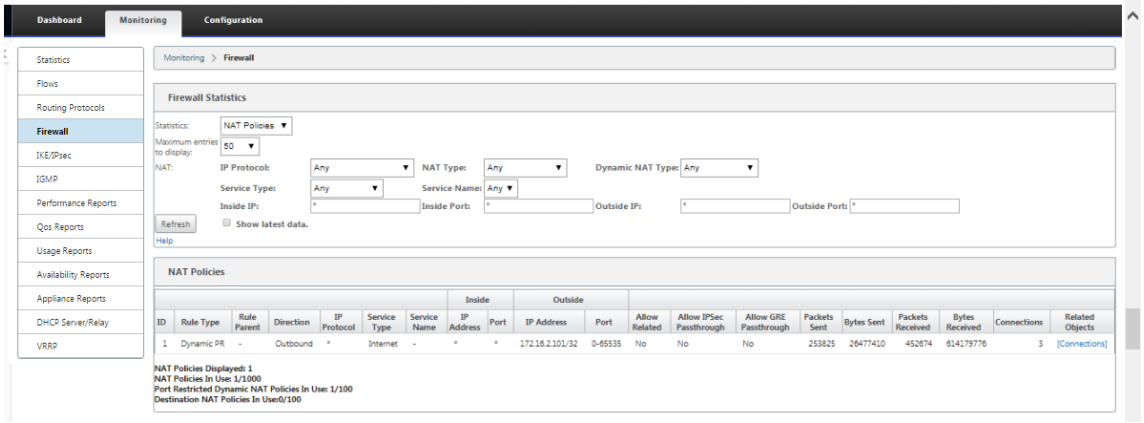


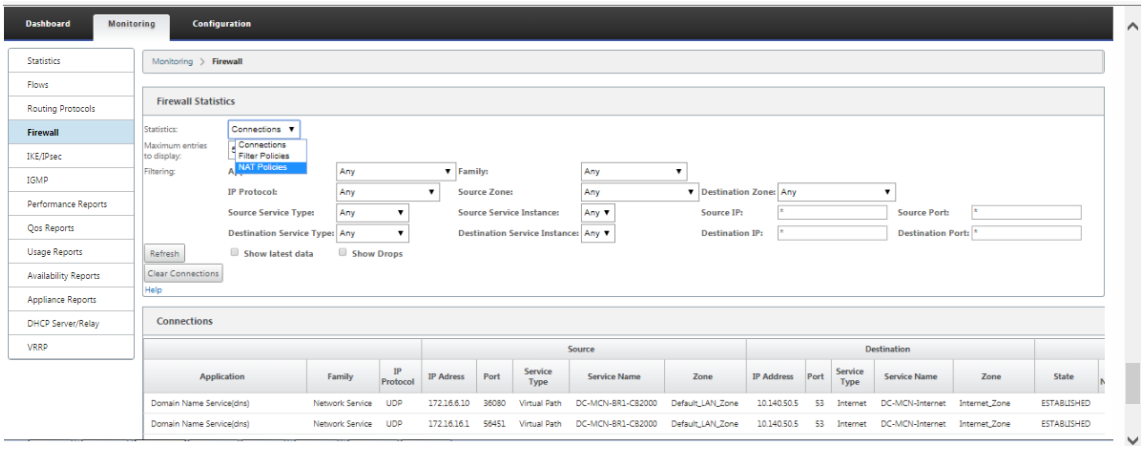
Surveillance d'une stratégie NAT de destination (pare-feu)

Vous pouvez également utiliser l'interface graphique Citrix SD-WAN pour surveiller la configuration actuelle de la stratégie DNAT.

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.





Intégration de Palo Alto à l'aide de tunnels IPsec

August 31, 2022

Les réseaux Palo Alto fournissent une infrastructure de sécurité basée sur le cloud pour la protection des 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 supprime 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 emplacements soient toujours connectés et sécurisés, et il vous permet de gérer les stratégies de manière centralisée à partir de Panorama pour une sécurité cohérente et rationalisée pour votre télécommande emplacements réseau.

Pour connecter vos emplacements réseau distants au service Prisma Access, vous pouvez utiliser le pare-feu de nouvelle génération Palo Alto Networks ou un périphérique tiers compatible IPSec, y compris le
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. Cela est essentiel pour offrir une expérience utilisateur plus fiable et à faible latence, tout en évitant l'introduction d'une pile de sécurité coûteuse dans chaque succursale. Citrix SD-WAN et Palo Alto Net-

works offrent désormais aux entreprises distribuées un moyen plus fiable et sécurisé de connecter les utilisateurs des succursales aux applications du cloud.

Les appliances Citrix SD-WAN peuvent se connecter au réseau du service cloud Palo Alto (Prisma Access Service) via des tunnels IPSec à partir d'emplacements SD-WAN avec une configuration minimale.

Prise en charge du pare-feu dynamique et du NAT

August 31, 2022

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 ports. Plus de fonctionnalités de pare-feu incluent :

- Assurer la sécurité du trafic utilisateur au sein du réseau SD-WAN (Enterprise and Service Providers)
- (Potentiel) Réduction de l'équipement externe (entreprises et fournisseurs de services)
- Utilisation du même espace d'adressage IP pour plusieurs clients : Capabilité 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 au sein d'une zone
- Filtrage du trafic entre les services résidant dans des zones différentes
- Filtrage du trafic entre les services d'un site
- Définition de stratégies de filtrage pour autoriser, refuser ou rejeter les flux
- État de flux de suivi 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 le transfert de port entrant et sortant
- Fournir une traduction d'adresses réseau statique (NAT statique)
- Fournir une traduction dynamique des adresses réseau (NAT dynamique)
- Traduction d'adresses de port (PAT)
- Transfert de ports

> **Remarque**
>
> Il n'est pas recommandé d'utiliser le pare-feu en mode intégré Fail-to-Wire pour des raisons de sécurité.

Paramètres globaux du pare-feu

August 31, 2022

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 Citrix SD-WAN Network. En utilisant les paramètres de pare-feu global, vous pouvez configurer les paramètres de pare-feu global, ces paramètres sont appliqués à tous les sites sur le réseau WAN virtuel.

Paramètres avancés du pare-feu

November 16, 2022

Vous pouvez configurer les paramètres avancés de pare-feu pour chaque site individuellement. Cela remplacera les paramètres globaux.

Pour configurer les paramètres avancés du pare-feu au niveau du site, consultez la section Paramètres du pare-feu.

Zones

August 31, 2022

Vous pouvez configurer des zones dans le réseau et définir des stratégies pour contrôler la façon dont le trafic entre et sort des zones. Par défaut, les zones suivantes sont créées :

- Internet_Zone
  - S'applique au trafic à destination ou en provenance d'un service Internet à l'aide d'une interface de confiance.
- Untrusted_Internet_Zone
  - S'applique au trafic à destination ou en provenance d'un service Internet à l'aide d'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 :

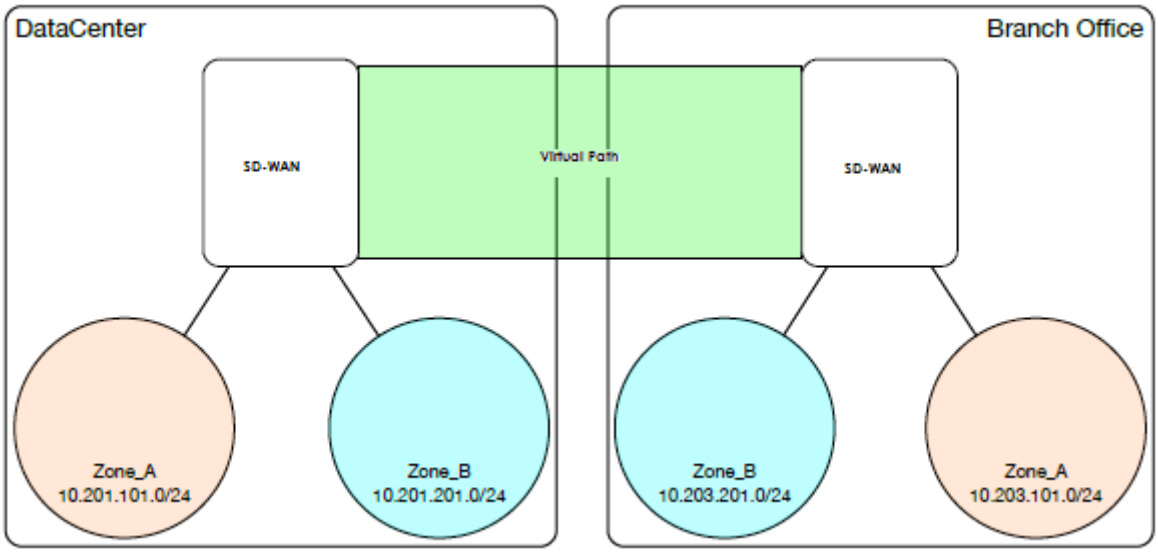
- Interfaces de réseau virtuel (VNI)
- Services Intranet
- Tunnels GRE
- Tunnels IPSec LAN

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 une route, à laquelle une zone lui est assignée.

- Zone source
  - Chemin non virtuel : déterminé par le biais du paquet d'interface réseau virtuel a été reçu le.
  - Chemin virtuel : déterminé par le champ de zone source dans l'en-tête de flux de paquets.
  - Interface réseau virtuel - 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 des informations sur la zone de destination, y compris les itinéraires appris via 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 opérationnelle ou du service.

La fonctionnalité du pare-feu SD-WAN permet à l'utilisateur de filtrer le trafic entre les services dans une seule zone, ou de créer des stratégies qui peuvent être appliquées entre les services dans différentes zones, comme le montre la figure ci-dessous. Dans l'exemple ci-dessous, nous avons Zone_A et Zone_B, chacune ayant une interface réseau LAN Virtual.



Stratégies

August 31, 2022

Les stratégies permettent d'autoriser, de refuser, de rejeter ou de compter et de poursuivre des flux de trafic spécifiques. Vous pouvez configurer les stratégies de pare-feu via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Stratégies de pare-feu.

Traduction d'adresses réseau (NAT)

August 31, 2022

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 (PAT- Translation d'adresses de port)

- NAT dynamique avec règles de transfert de port

> **Remarque**
>
> La fonctionnalité NAT ne peut être configurée que via le service Citrix SD-WAN Orchestrator 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. Pour plus d'informations, consultez la section Traduction d'adresses réseau.

NAT statique

August 31, 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.

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.**

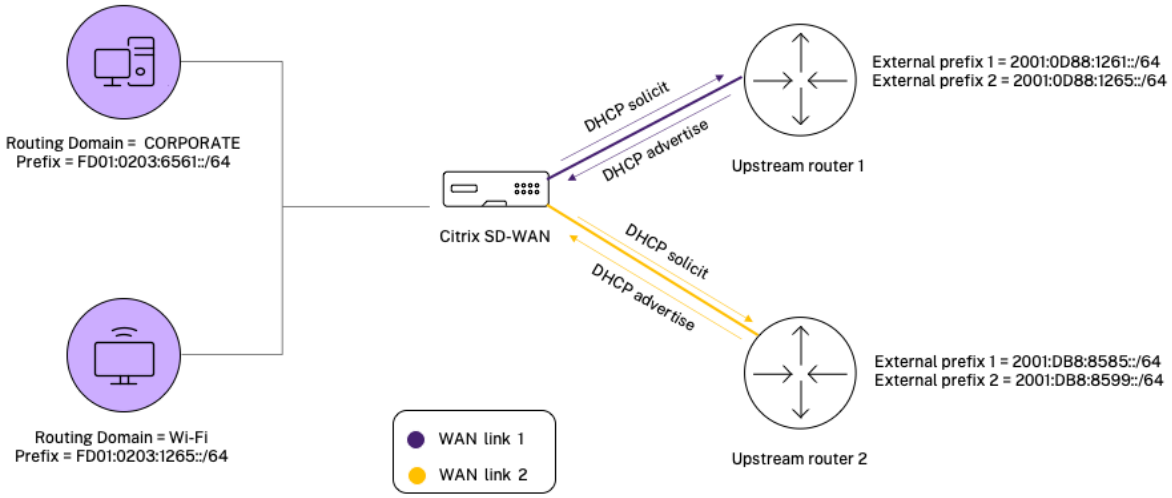
À partir de Citrix SD-WAN version 11.4.0, lors de la création d'une stratégie NAT statique, vous pouvez entrer manuellement l'adresse IP externe ou activer l'**Autolearn via DP**. Lorsque l'**Autolearn via DP** est activé, l'appliance Citrix SD-WAN reçoit des préfixes délégués du routeur délégué en amont 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'appliance 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'appliance 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'appliance 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.

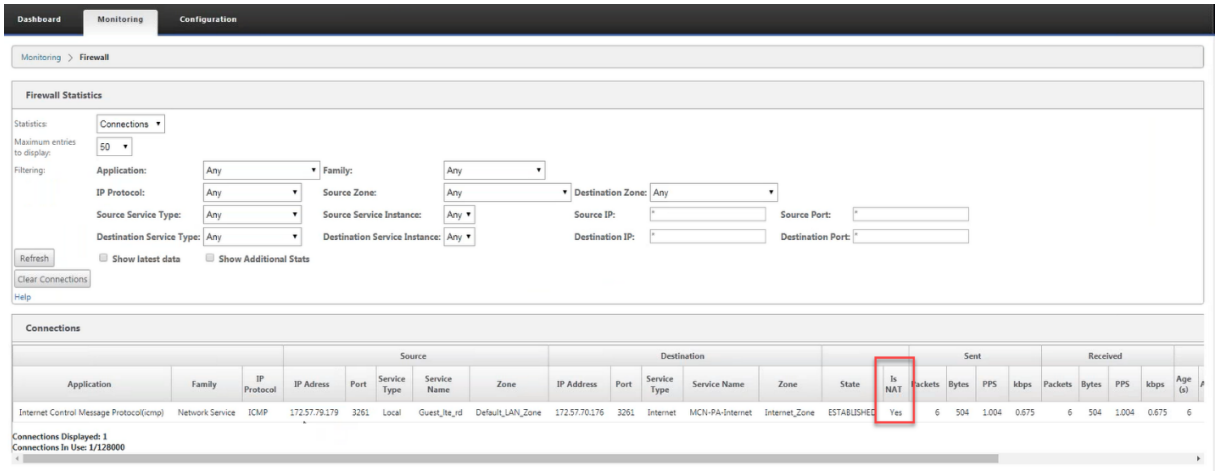


Dans ce scénario, il y a M=2 à l'intérieur des réseaux et des liaisons WAN N=2. Par conséquent, le nombre de stratégies NAT statiques requises pour un déploiement correct du service Internet IPv6 est de 2 x 2 = 4. Ces 4 stratégies NAT statiques spécifient la traduction d'adresse pour :

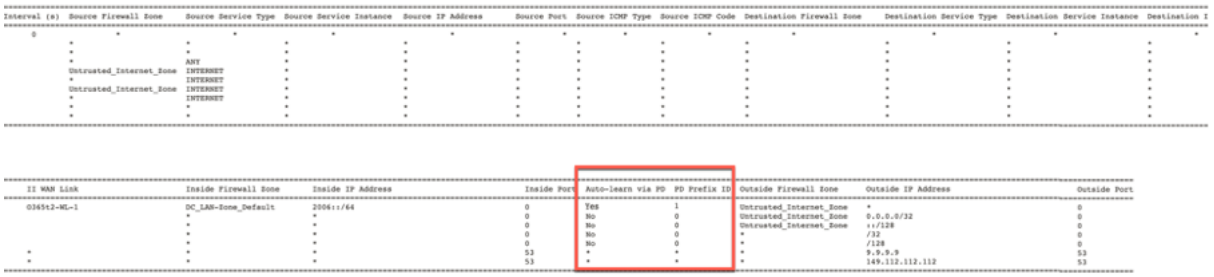
- Réseau interne 1 via la liaison WAN 1
- Réseau interne 1 via la liaison WAN 2
- Réseau interne 2 via la liaison WAN 1
- Réseau interne 2 via la liaison WAN 2

Surveillance

Pour surveiller NAT, accédez à **Surveillance** > **Statistiques du pare-feu** > **Connexions**. Pour une connexion, vous pouvez voir si NAT est fait ou non.

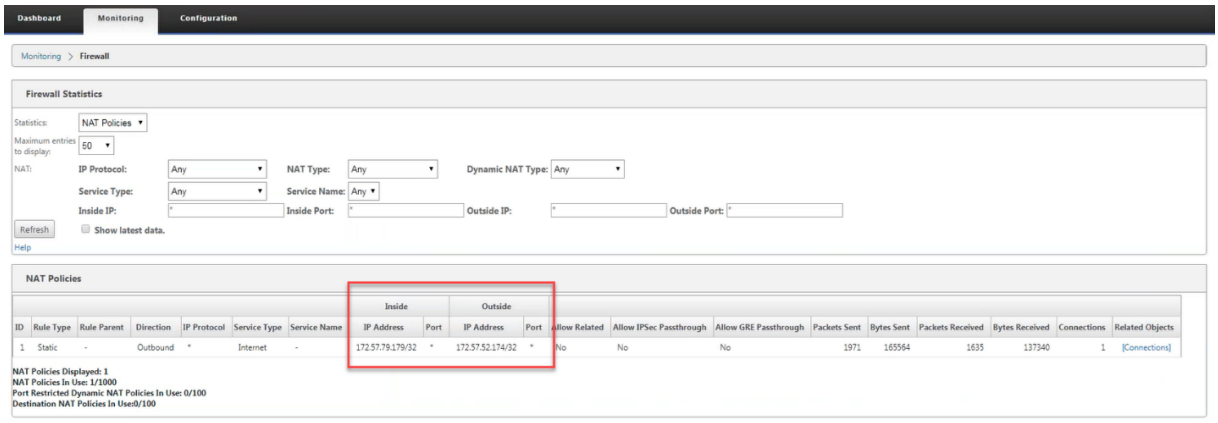


Pour vérifier si l'apprentissage automatique via PD est configuré pour une règle NAT, accédez à **Configuration > Virtual WAN > View Configuration** et choisissez **Pare-feu** dans la liste déroulante **View** . Les colonnes **Auto-learn via PD** et **PD prefix ID** affichent les détails.

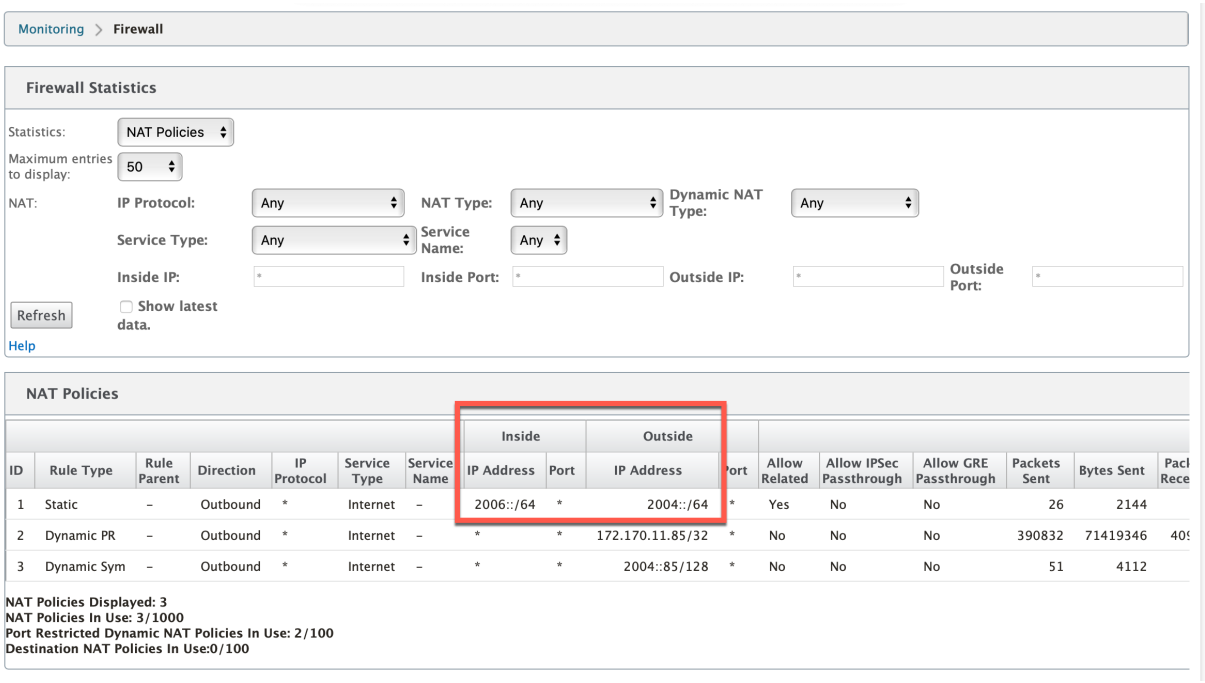


Pour afficher plus en détail le mappage de l'adresse IP interne à l'adresse IP externe, cliquez sur **NAT post-route** sous **Objets associés** ou accédez à **Surveillance** > **Statistiques de pare-feu** > **Stratégies NAT**.

La capture d'écran suivante montre le mappage de l'adresse interne à l'adresse externe dans une stratégie NAT statique IPv4.



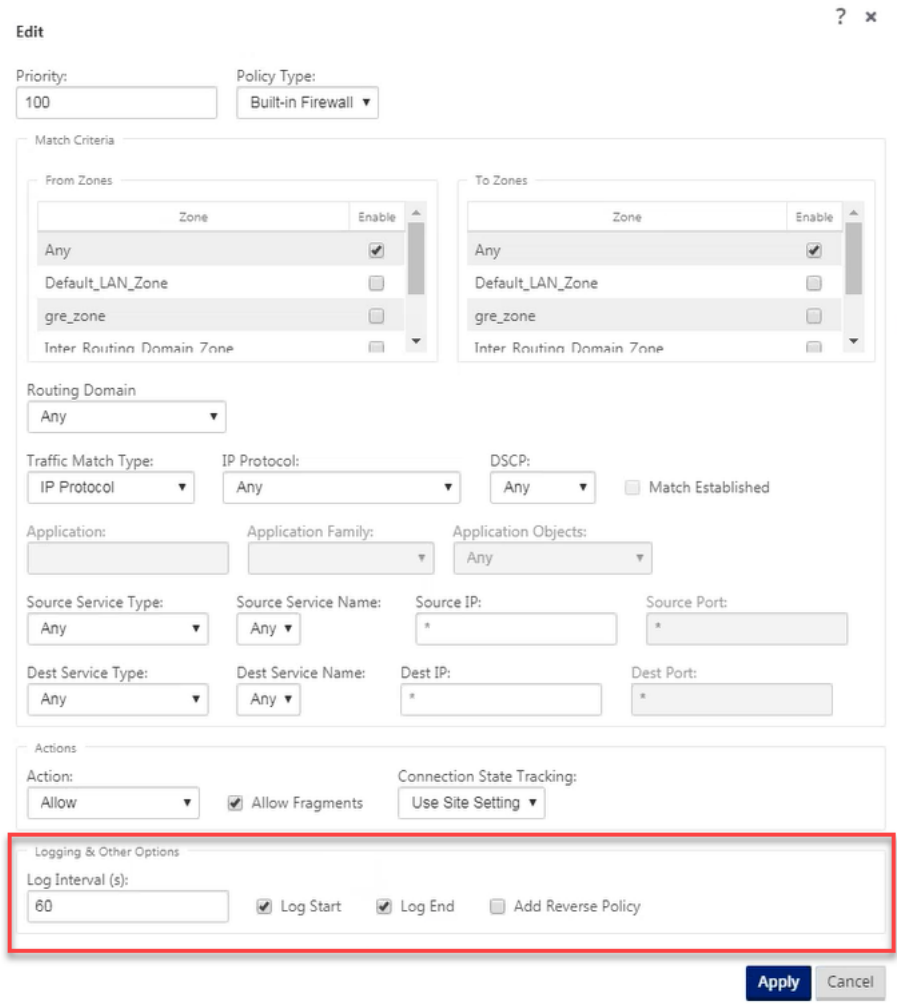
La capture d'écran suivante montre le mappage de l'adresse interne à l'adresse externe dans une stratégie NAT statique IPv6.



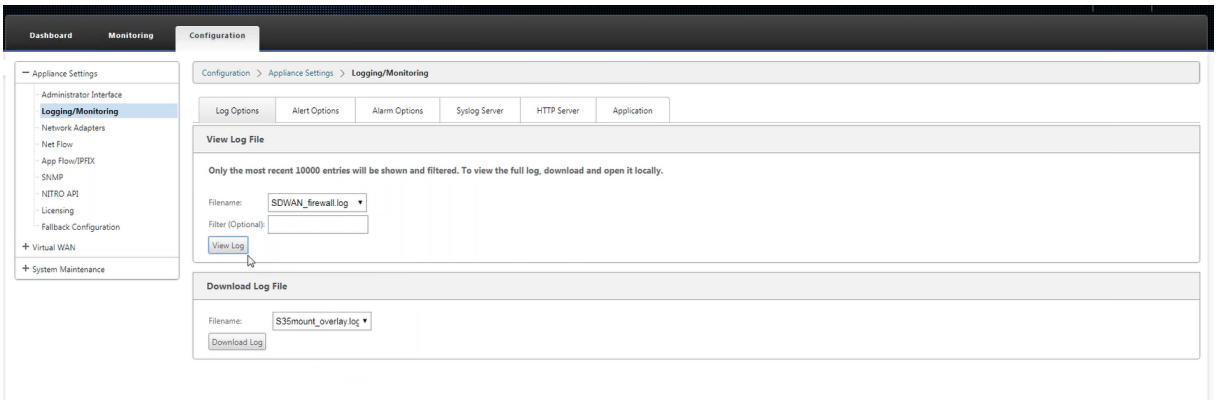
Journaux

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 :

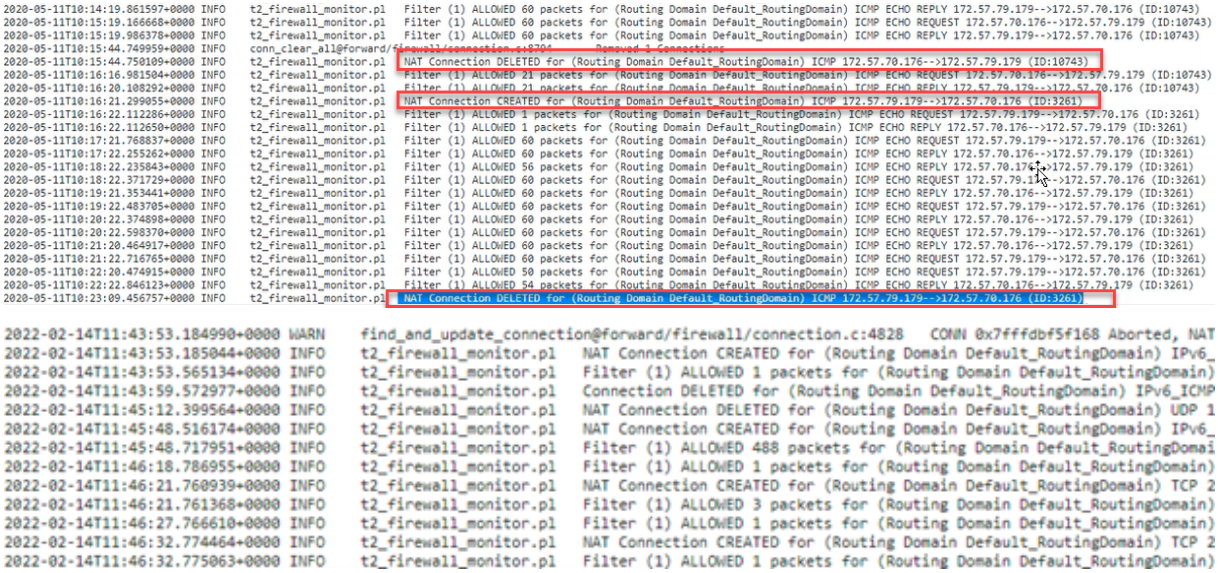
- Date et heure
- Domaine de routage
- Protocole IP
- Port source
- Adresse IP source
- Adresse IP traduite
- Port traduit
- Adresse IP de destination
- Port de destination



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.



NAT dynamique

November 16, 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.

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.

Stratégies NAT dynamiques créées automatiquement

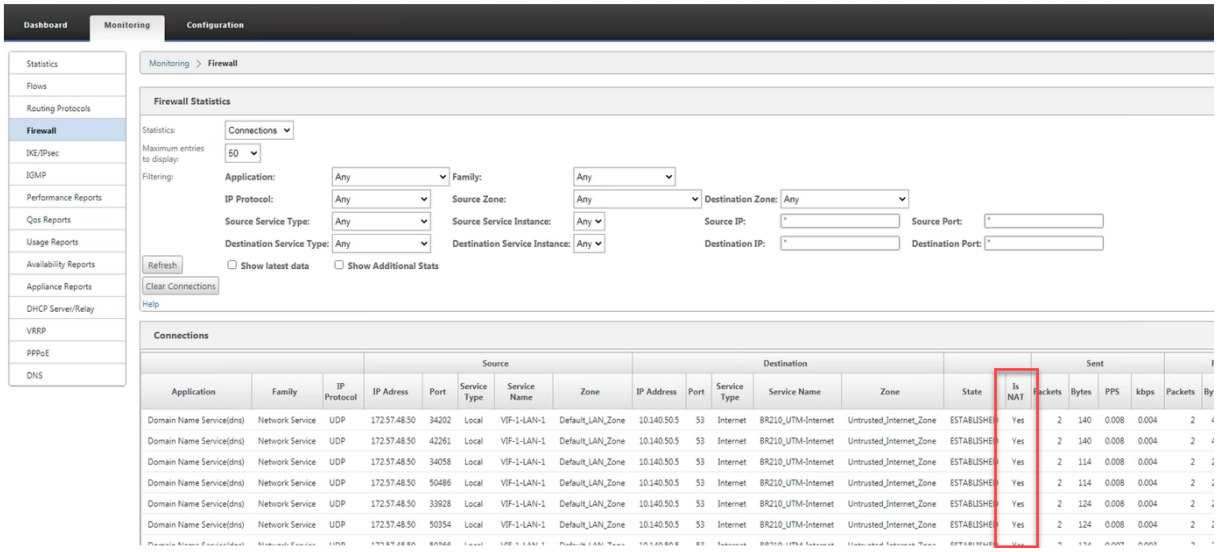
Les stratégies NAT dynamiques pour le service Internet sont créées automatiquement dans les cas suivants :

- Configuration du service Internet sur une interface non approuvée (lien WAN).

- Activation de l'accès à Internet pour tous les domaines de routage sur une seule liaison WAN à l'aide du service Citrix SD-WAN Orchestrator. Pour plus de détails, consultez la section Configurer la segmentation du pare-feu.
- Configuration des redirecteurs DNS ou du proxy DNS sur le service SD-WAN Orchestrator. Pour plus de détails, consultez la section Système de noms de domaine.

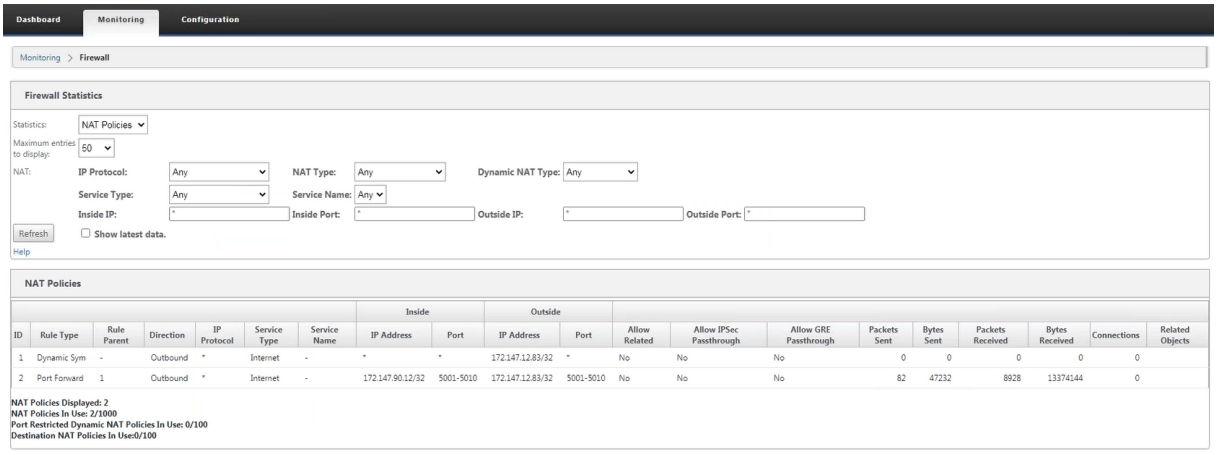
Surveillance

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.

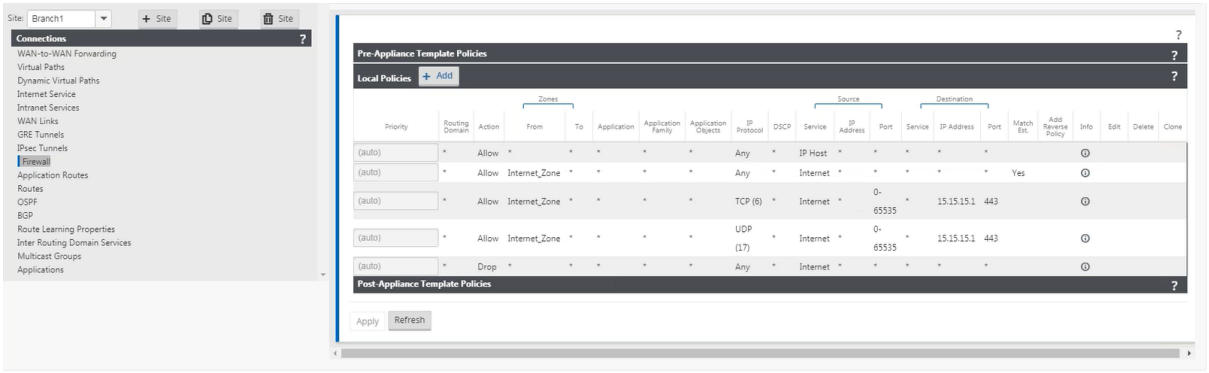


Pour afficher plus en détail le mappage de l'adresse IP interne vers l'adresse IP externe, cliquez sur **NAT pré-itinéraireou NAT post-route**sous**Objets associés**ou accédez à**Surveillance**>**Statistiques de pare-feu**>**Stratégies NAT**.

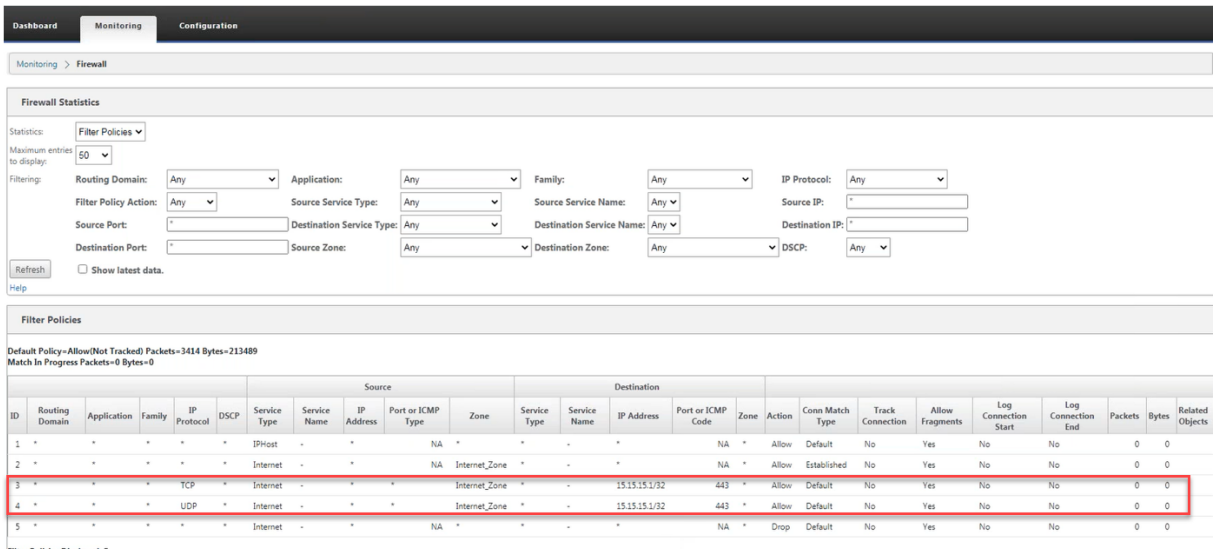
La capture d'écran suivante montre les statistiques de la règle NAT dynamique de type symétrique et de sa règle de transfert de port correspondante.



Lorsqu'une règle de transfert de port est créée, une règle de pare-feu correspondante est également créée.



Vous pouvez afficher les statistiques de stratégie de filtrage en accédant à **Surveillance** > **Statistiques du pare-feu** > **Stratégies de filtrage**.

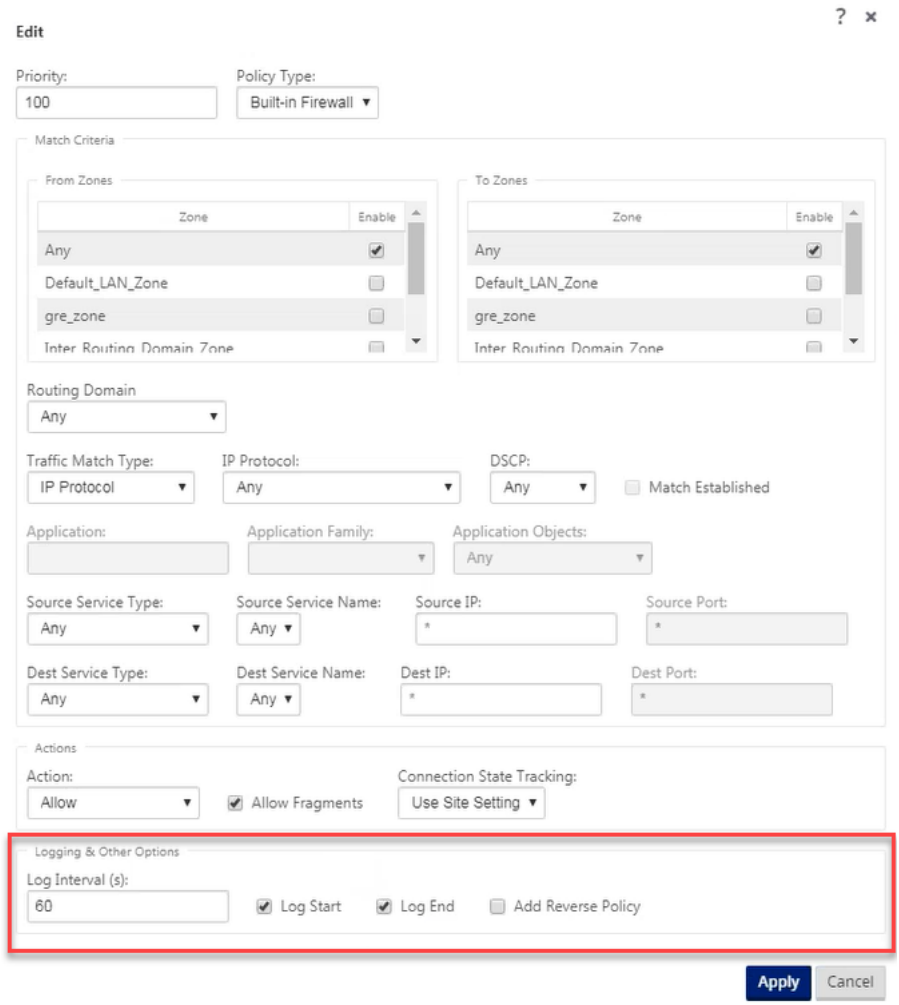


Journaux

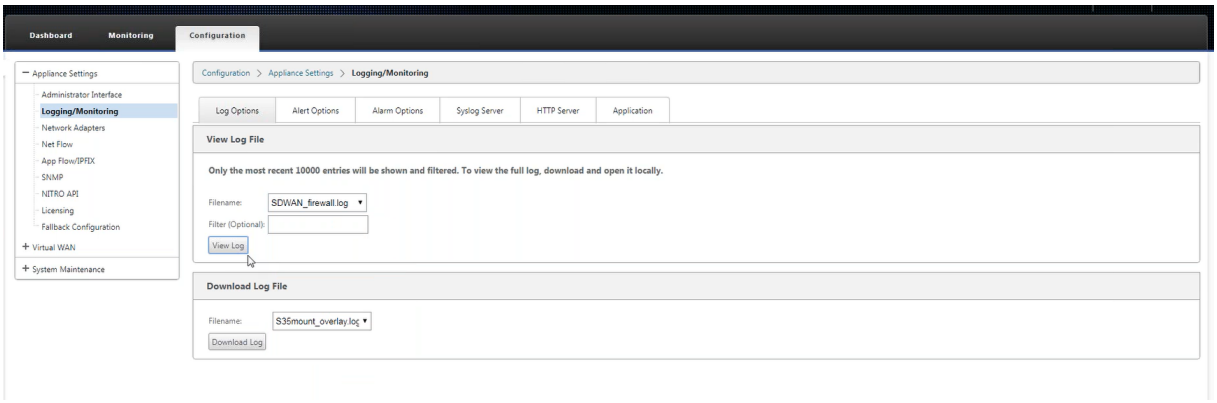
Vous pouvez afficher les journaux liés à NAT dans les journaux de pare-feu. Pour afficher les journaux pour NAT, créez une stratégie de pare-feu qui correspond à votre stratégie NAT et assurez-vous que la journalisation est activée sur le filtre de pare-feu. Les journaux NAT contiennent les informations suivantes :

- Date et heure
- Domaine de routage
- Protocole IP
- Port source
- Adresse IP source

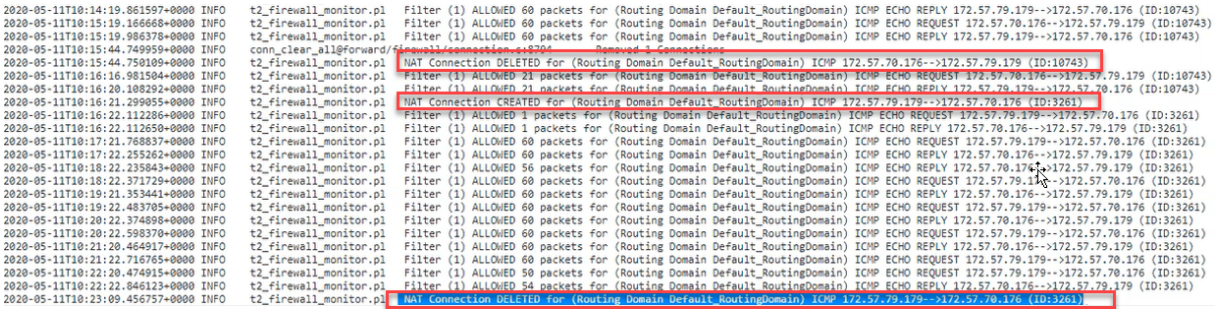
- Adresse IP traduite
- Port traduit
- Adresse IP de destination
- Port de destination



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.



Configurer le service WAN virtuel

August 31, 2022

La configuration Citrix SD-WAN décrit et définit la topologie de votre réseau Citrix SD-WAN. Pour plus d'informations sur la configuration du service WAN virtuel à l'aide du service Citrix SD-WAN Orchestrator, consultez Flux.

Sécurité et chiffrement

L'activation du chiffrement du SD-WAN (pour les chemins virtuels) est facultative. 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.

Authentification entre les fonctions de sites avec la configuration Virtual WAN. La configuration réseau possède une clé secrète pour chaque site. Pour chaque chemin virtuel, la configuration réseau génère une clé en combinant les clés secrètes des sites situés à chaque extrémité du chemin virtuel. L'échange de clés initial qui se produit après la première configuration d'un chemin virtuel dépend de la capacité de chiffrer et de déchiffrer des paquets avec cette clé combinée.

Configurer la segmentation du pare-feu

November 16, 2022

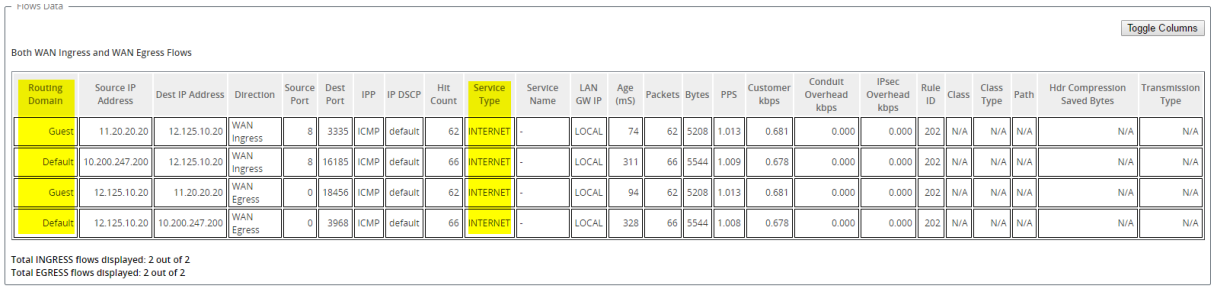
La segmentation du pare-feu VRF (Virtual Route Forwarding) fournit plusieurs domaines de routage accès à Internet via une interface commune, le trafic de chaque domaine étant isolé de celui des autres. Par exemple, les employés et les invités peuvent accéder à Internet via la même interface, sans aucun

accès au trafic de l'autre. À partir de la version 11.5 de SD-WAN, vous pouvez configurer la segmentation du pare-feu à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Segmentation du pare-feu.

- Accès Internet invité-utilisateur local
- Accès à Internet employeur-utilisateur pour des applications définies
- Les employé-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 option fournit la sécurité requise pour chaque groupe d'utilisateurs.

Vous pouvez vérifier que chaque domaine de routage utilise le service Internet en consultant la colonne Domaine de routage dans le tableau Flux de l'interface de gestion Web sous **Surveiller** > **Flux**.


Flows Data

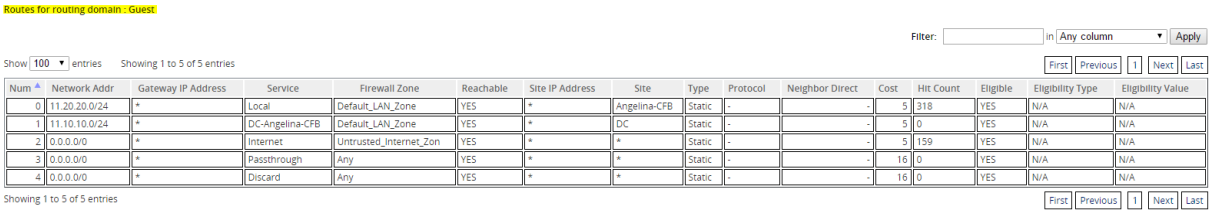
Toggle Columns

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	18456	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

Vous pouvez également consulter la table de routage de chaque domaine de routage sous **Surveiller** > **Statistiques** > **Itinéraires**.


Routes for routing domain : Guest

Filter: in Any column Apply

Show 100 entries Showing 1 to 5 of 5 entries First Previous 1 Next Last

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 First Previous 1 Next Last

Cas d'utilisation

Dans les versions précédentes de Citrix SD-WAN, le routage virtuel et le transfert présentaient les problèmes suivants, qui ont été résolus.

- Les clients ont plusieurs domaines de routage sur un site de succursale sans qu'il soit nécessaire d'inclure tous les domaines du datacenter (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 pare-feu pour que plusieurs domaines de routage puissent accéder à Internet sur un site (au-delà de VRF lite).
- Les clients ont besoin d'une route 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 de segmentation Virtual Forwarding and Routing Firewall, vous pouvez :

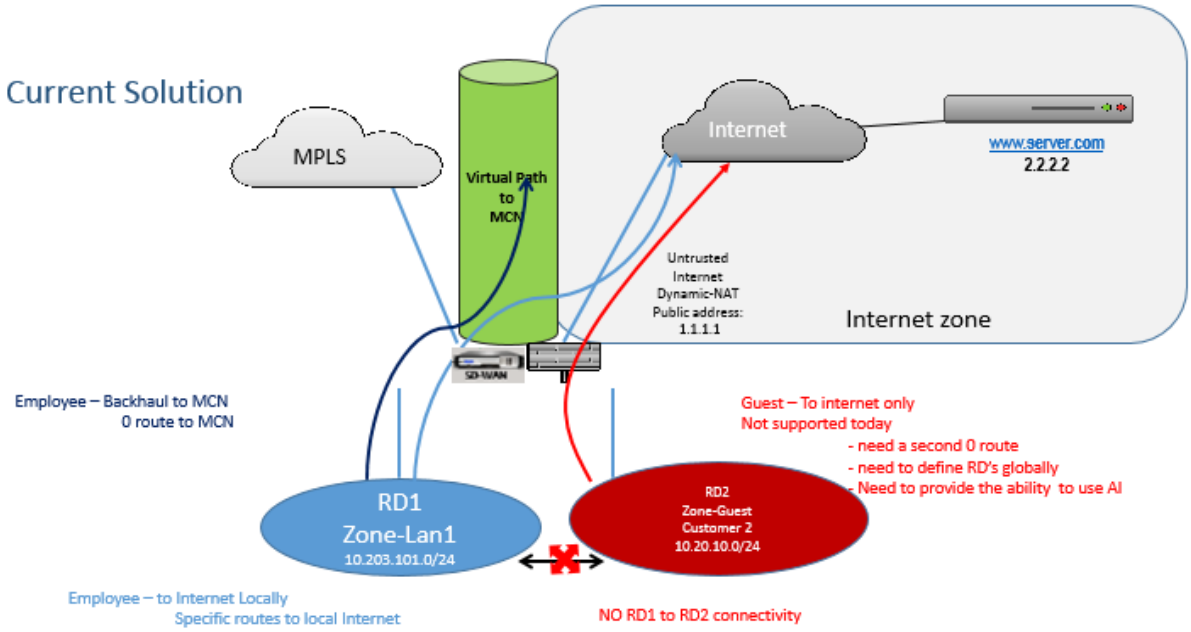
- Fournir une infrastructure, sur le site de la succursale, qui prend en charge la connectivité sécurisée pour au moins deux groupes d'utilisateurs, tels que les employés et les invités. L'infrastructure peut prendre en charge jusqu'à 16 domaines de routage.
- Isolez le trafic de chaque domaine de routage 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 pour l'employé peut être acheminé directement vers l'Internet local (applications spécifiques)
- Le trafic de l'employé peut être acheminé ou rétroacheminé vers le MCN pour un filtrage étendu (route 0)
- Le trafic pour le domaine de routage peut être acheminé directement vers l'Internet local (route 0)
- Prend en charge des itinéraires spécifiques par domaine de routage, si nécessaire
- Les domaines de routage sont basés sur VLAN
- Supprime l'exigence selon laquelle le Bureau à distance doit 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 RD se voit attribuer un itinéraire 0.0.0.0
- Permet d'ajouter des itinéraires spécifiques pour un service RD
- Permet au trafic 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

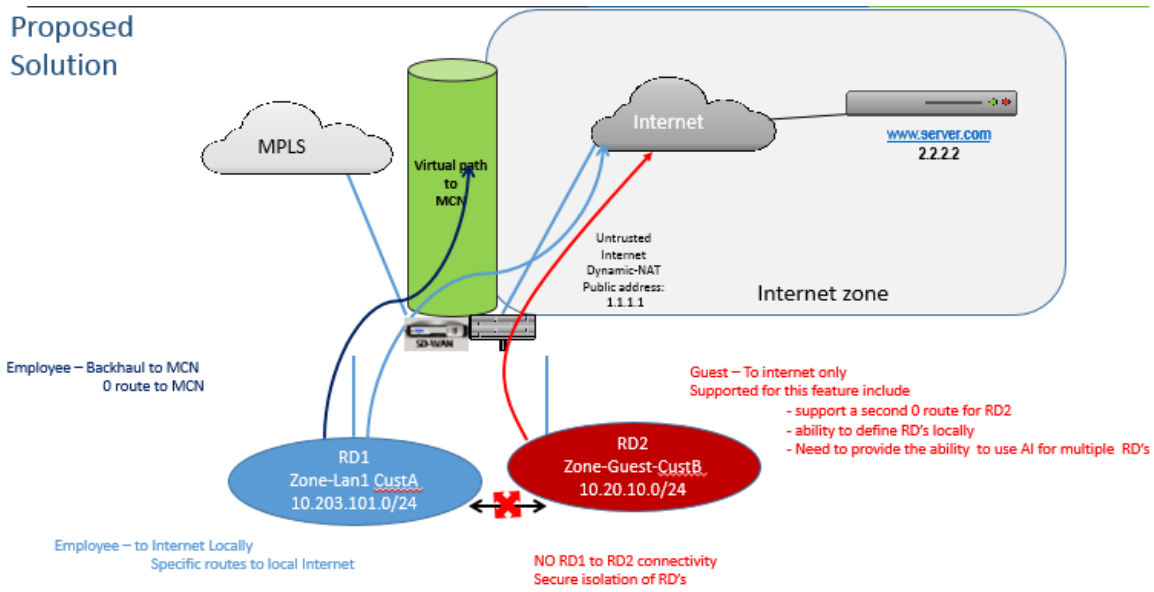
- Doit être des sous-réseaux uniques (les services Bureau à distance sont affectés à un VLAN)
- Chaque Bureau à distance peut utiliser la même zone FW par défaut
- Le trafic est isolé via le domaine de routage
- Les flux sortants ont le Bureau à distance en tant que composant de l'en-tête de flux. Permet au SD-WAN de mapper les flux de retour au domaine de routage correct.

Conditions préalables à la configuration de plusieurs domaines de routage :

- L'accès Internet est configuré et affecté à un lien WAN.
- Pare-feu configuré pour NAT et stratégies correctes appliquées.
- Deuxième domaine de routage ajouté globalement.
- Chaque domaine de routage ajouté à un site.
- Assurez-vous que le service Internet a été correctement défini.

Scénarios de déploiement





Limitations

- Le service Internet doit être ajouté au lien 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 Dynamic-NAT.
- Jusqu'à 16 domaines de routage par site.
- Interface d'accès (AI) : IA unique par sous-réseau.
- Plusieurs AI nécessitent un VLAN distinct pour chaque IA.
- Si vous disposez de deux domaines de routage sur un site et que vous disposez d'un seul lien WAN, les deux domaines utilisent la même adresse IP publique.
- Si l'accès Internet pour tous les domaines de routage est activé, tous les sites peuvent être acheminés 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 liens WAN sont partagés pour l'accès Internet.
- Pas de QOS par domaine de routage ; premier arrivé, premier service.

Authentification du certificat

August 31, 2022

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 réseau et les tunnels IPSec de chemin virtuel. Outre les mesures de sécurité existantes, l'authentification basée sur des certificats est introduite dans Citrix SD-WAN 11.0.2.

L'authentification par certificat permet aux organisations d'utiliser des certificats émis par leur autorité de certification (CA) privée pour authentifier les appliances. Les appliances sont authentifiées avant d'établir les chemins virtuels. Par exemple, si un dispositif de branche tente de se connecter au centre de données et que le certificat de la branche 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.

Vous pouvez activer l'authentification par certificat de votre appliance SD-WAN à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations sur l'authentification par certificat, consultez Authentification par certificat.

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 uniquement les données de niveau de flux pour les connexions HDX/ICA. Vous pouvez activer le TCP uniquement pour le modèle de jeu de données HDX ou le modèle de jeu de données

HDX. Le jeu de données TCP uniquement pour HDX fournit des données à sauts multiples. Le jeu de données HDX fournit des données HDX Insight.

Les collecteurs AppFlow comme Splunk et Citrix ADM disposent de 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	
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	

Info Element (IE)	Nom et ID IE	Type and len	Description
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	IPVersion, 60	Unsigned8, 1	Set to 4.
IP protocol number	protocoldentifier,4	Unsigned8, 1	
Padding	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 lastpkt 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 flow0x01: 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	Réglez sur 0x1E037F.
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|Commentaire|
|-|-|-|-|
|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	protocoldentifier, 4	Non signée8, 1	
Padding	N/A	Non signée16, 2	
Port SRC	SourceTransport	Désigné16, 2			Port
DST	Destination	Transport	Transport	Transport	Désignée16 Désigné16, 2	
Pkt compte	PacketDeltaCount, 2	Unsigned64, 8	
Compte d'octetetetetDeltaCount, 1	Unsigned64, 8			Heure pour la première pkt en microsecondes	FlowStartMicrosecondes,
154	DateTimeMicroseconds, 8			Temps pour lastpkt en microsecondes	FlowendMicroTimSeconds, 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	Commentaire
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	Commentaire
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	IPVersion, 60	Unsigned8, 1	
IP protocol number	protocoldentificateur, 4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: les flux Flowwan-WAN et LAN-LAN sont une possibilité dans SDWAN

Info Element (IE)	Nom et ID IE	Type and len	Commentaire
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	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	

ID de modèle —616 (flux IPv6) |Info Element (IE)|IE name & ID|Type and len|Commentaire|
|-|-|-|-|
|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'octetetetDeltaCount, 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

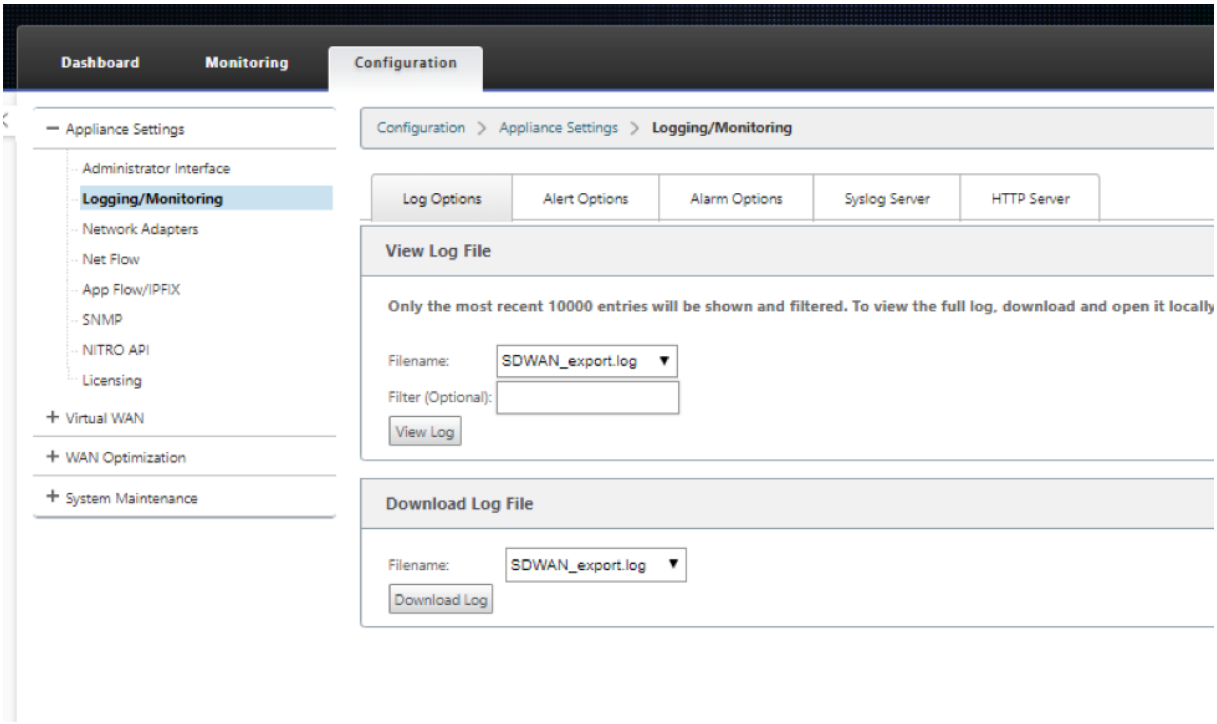
- AppFlow ne prend pas en charge les enregistrements de collecteur et de flux IPv6.
- L'intervalle d'exportation pour le flux net passe de 15 secondes à 60 secondes.
- AppFlow/IPfix flux sont transmis via UDP, en cas de perte de connexion toutes les données ne sont pas retransmises. Si l'intervalle d'exportation est défini sur X minutes, l'appliance ne stocke que 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 localement 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 à l'une des versions précédentes et si AppFlow est configuré sur l'une des appliances, elle sera appliquée globalement à toutes les alliances.

Configuration d'AppFlow/IPFix

Vous pouvez configurer AppFlow/IPFIX uniquement via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez AppFlow et IPFIX.

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

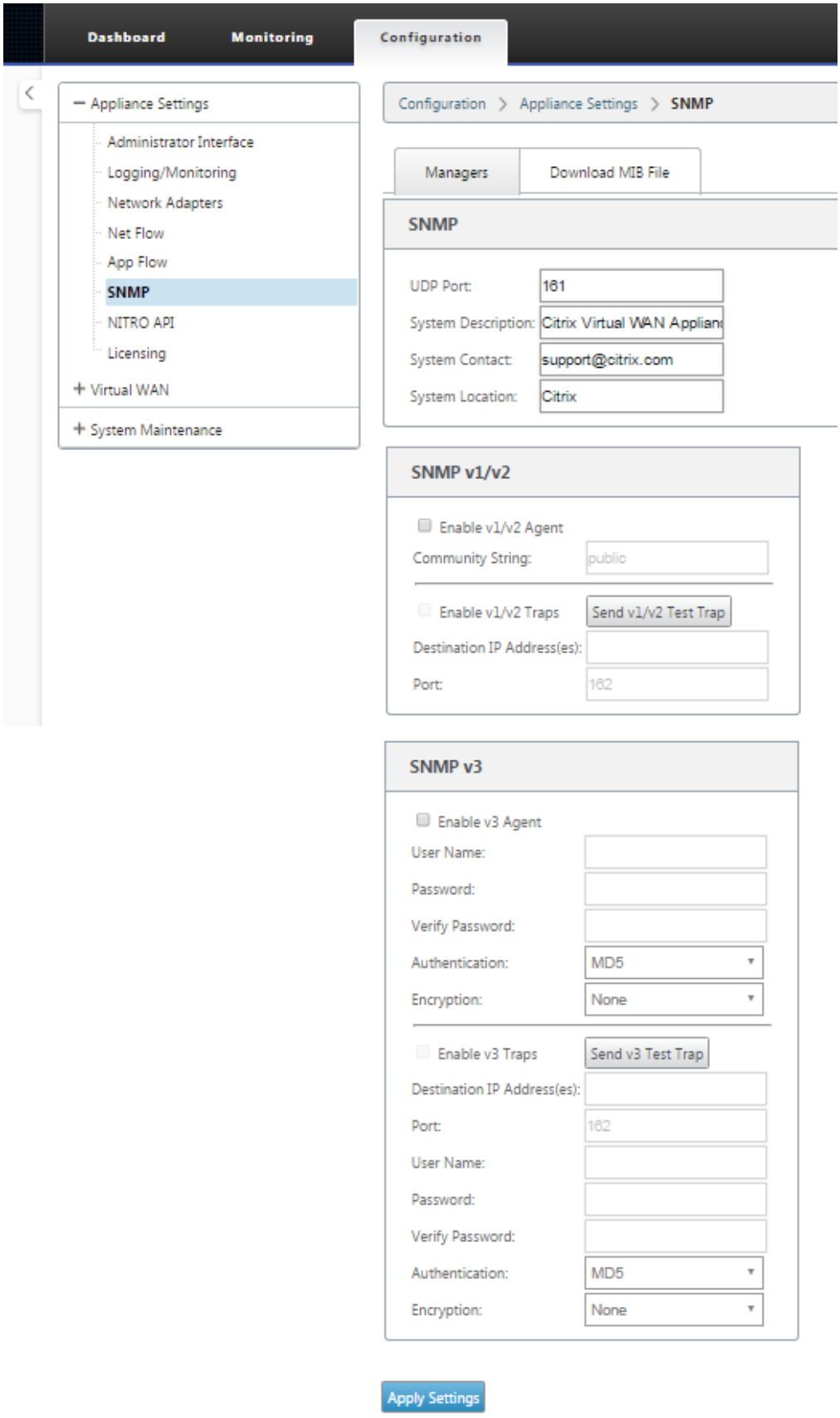
November 16, 2022

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.



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

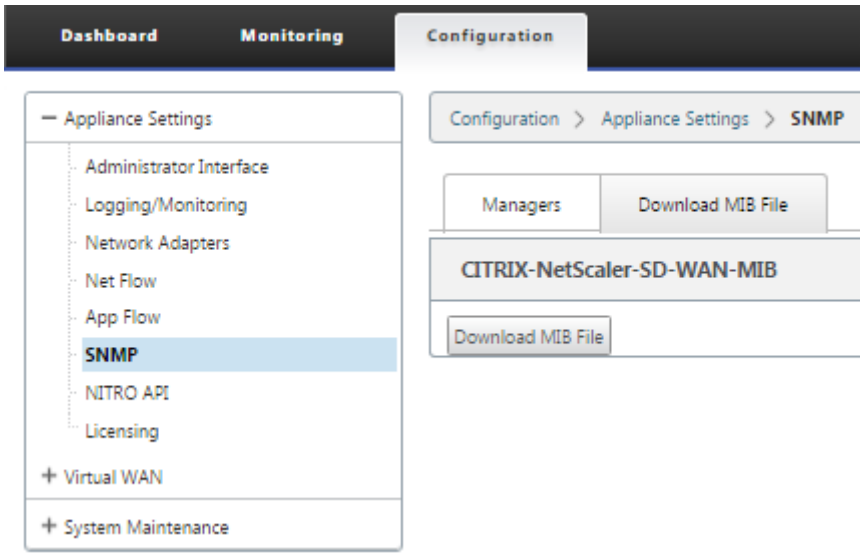
Vous devez télécharger les fichiers SNMP suivants avant de pouvoir commencer à surveiller une appliance Citrix SD-WAN :

- 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, de**sorte 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

August 31, 2022

Vous pouvez gérer et entretenir vos appliances Citrix SD-WAN à l'aide des options d'administration

suivantes à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Paramètres de l'appliance.

- 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'appliance 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.

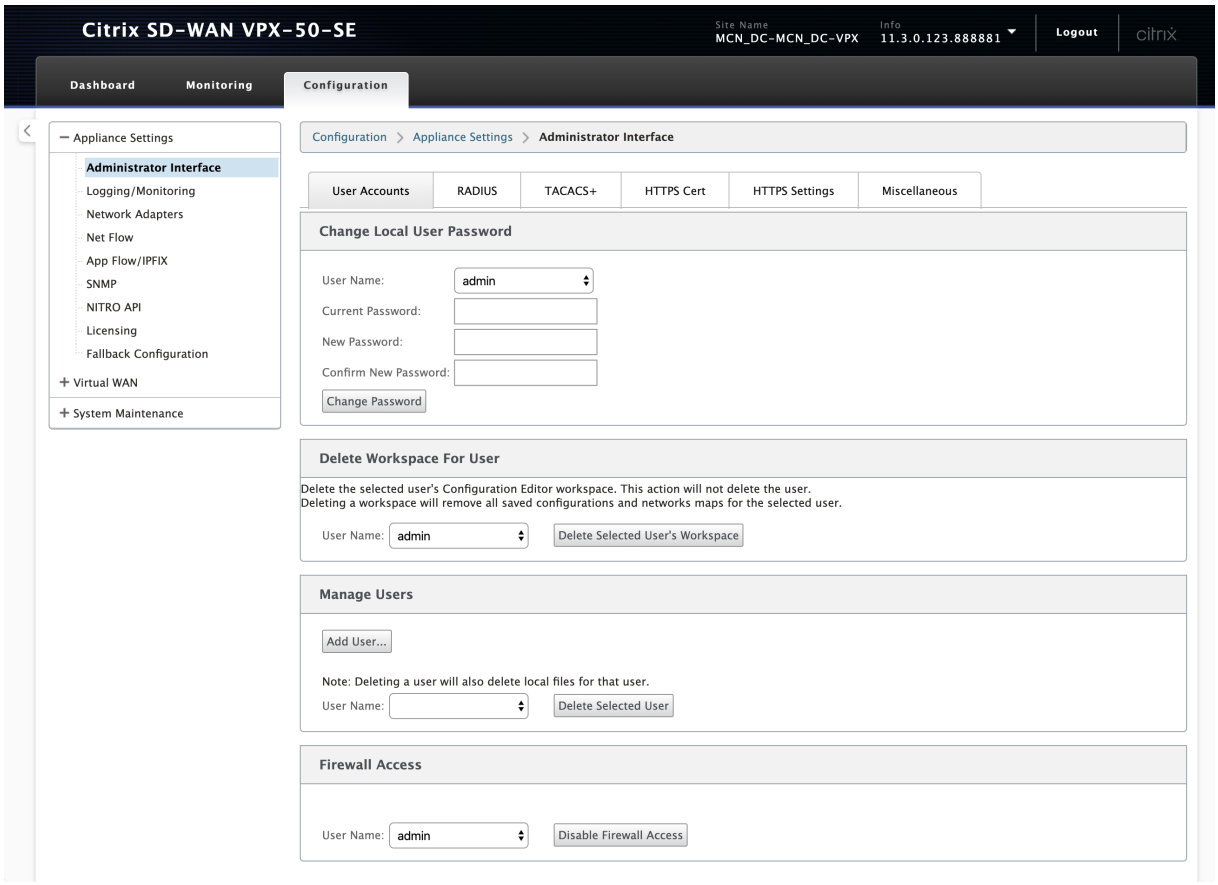
  Un super administrateur (admin) dispose des privilèges suivants :

  - 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 la sécurité** : un administrateur de la sécurité dispose d'un accès en lecture-écriture uniquement pour le pare-feu et les paramètres liés à la sécurité, 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 entièrement provisionner une branche, à l'exception des paramètres liés au pare-feu et à la sécurité. 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.

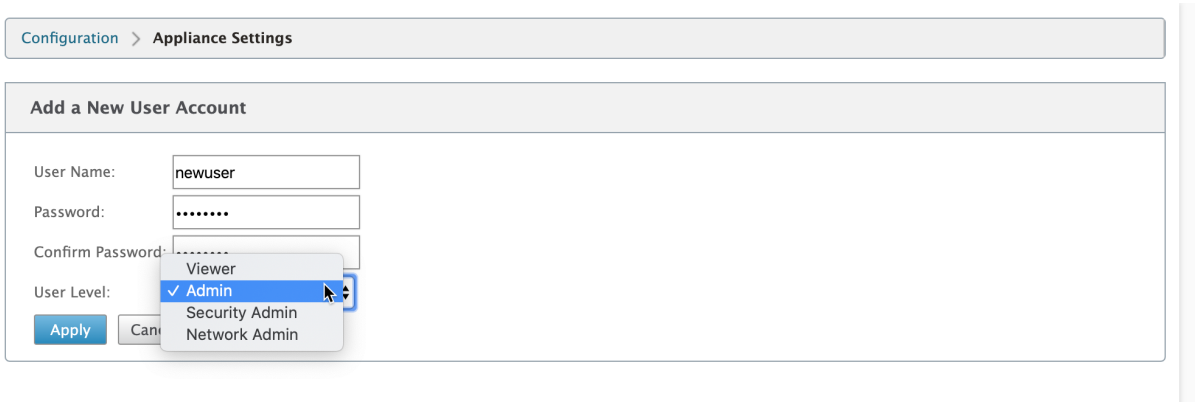
> **REMARQUE**
>
> L'administrateur réseau et l'administrateur de la sécurité ne peuvent pas ajouter ou supprimer des comptes utilisateur. Ils ne peuvent modifier que leurs propres mots de passe de compte.



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**.

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 :

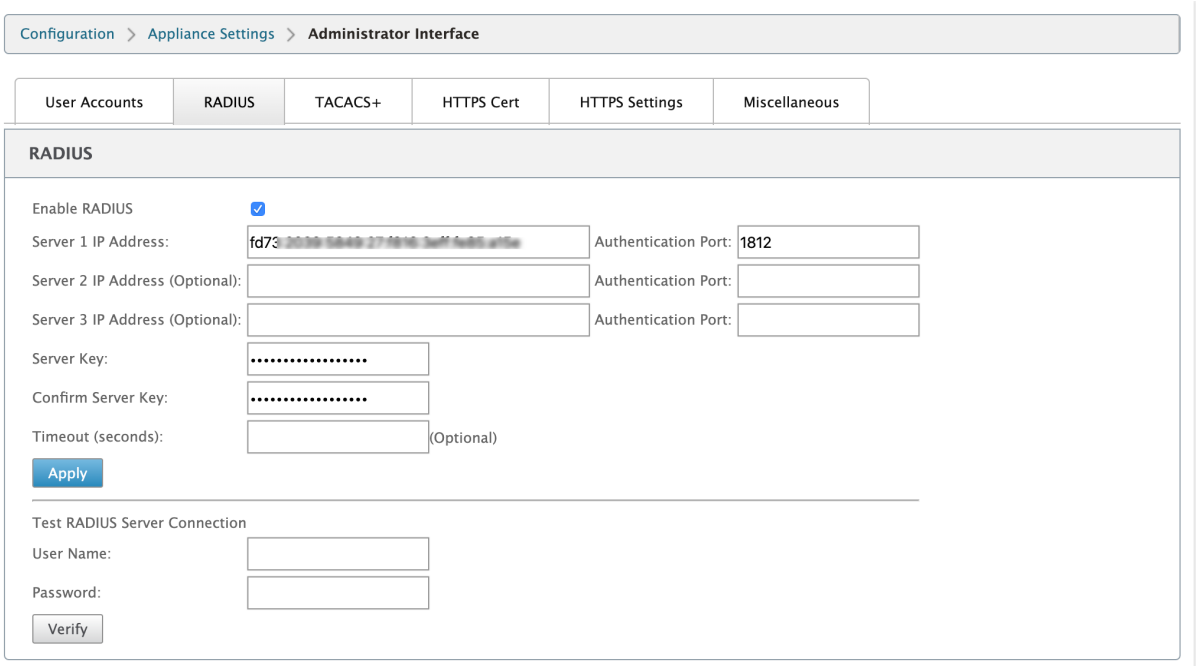
1. Accédez à **Configuration > Paramètres du matériel > Interface Administrateur > RADIUS**.
2. Activez la case à cocher **Activer RADIUS**.
3. Entrez l'**adresse IP du serveur** et le **port d'authentification**. Un maximum de trois adresses IP de serveur peut être configuré.

   > **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 lemot de passe**. Cliquez sur**Vérifier**.



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.

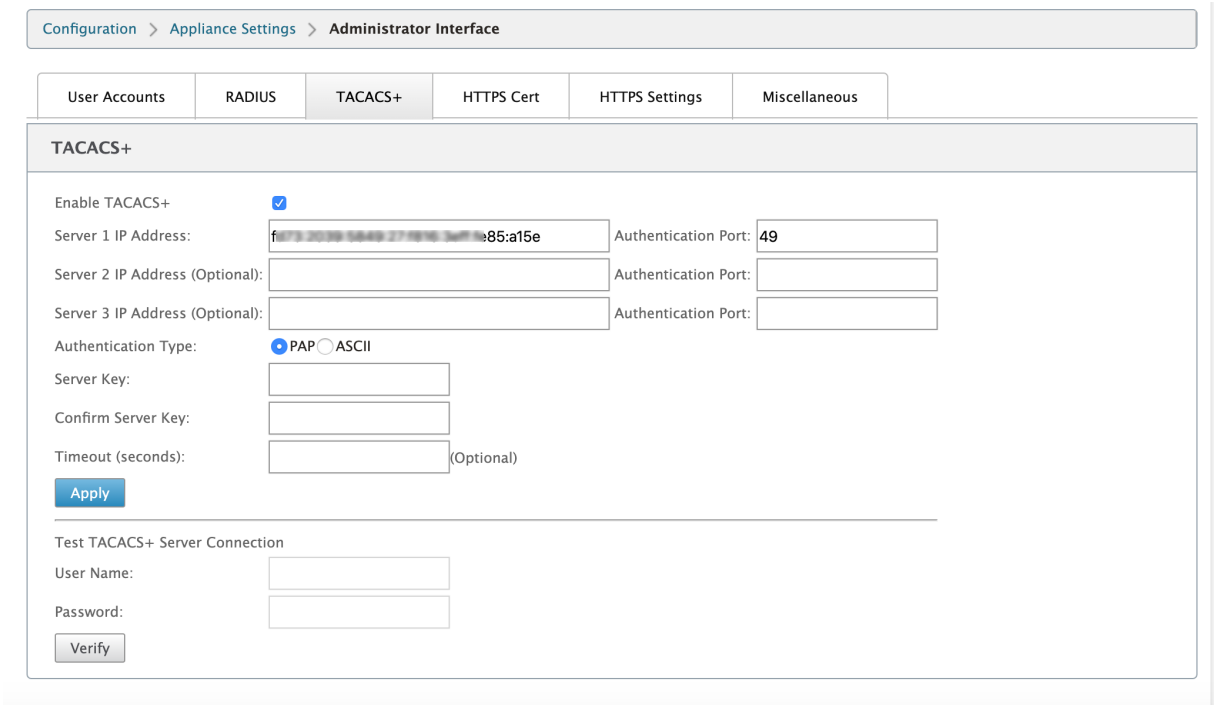
   > **REMARQUE**
   >
   > Pour configurer une adresse IPv6, assurez-vous que le serveur TACACS+ est également configuré avec une adresse IPv6.

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 lemot de passe**. Cliquez sur**Vérifier**.



Annonce de routeur NDP et groupe de délégation de préfixe

November 16, 2022

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.

Vous pouvez configurer l'annonce du routeur NDP à l'aide du service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Annonce du routeur NDP.

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.

Vous pouvez configurer la délégation de préfixes via le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez Groupes de délégations de préfixes.

Comment des articles

August 31, 2022

Les « How-to-Articles » décrivent la procédure de configuration des fonctionnalités prises en charge par Citrix SD-WAN. Ces articles contiennent des informations sur certaines des fonctionnalités importantes suivantes :

Cliquez sur le nom d'une entité ci-dessous pour afficher la liste des articles de procédure relatifs à cette fonctionnalité.

- Routage et transfert virtuels
- Activation de RED pour l'équité QoS
- Configuration
- Routage dynamique
- Serveur DHCP et relais DHCP

- Filtres d'itinéraire
- Résiliation et surveillance IPsec
- Secure Web Gateway
- QoS
- Fonctionnement conforme à FIPS - Tunnel IPsec
- Configuration NAT dynamique
- Détection adaptative de bande passante
- Test de la bande passante active
- Améliorations BGP
- Association de classe de service avec les profils SSL
- Déploiement zéro tactile

Configurer l'interface d'accès

August 31, 2022

Pour configurer l'interface d'accès via le service Citrix SD-WAN Orchestrator, consultez la section Liens WAN.

Configurer les adresses IP virtuelles

August 31, 2022

Pour configurer les adresses IP virtuelles via le service Citrix SD-WAN Orchestrator, consultez la section Liens WAN.

Configurer les tunnels GRE

August 31, 2022

Pour configurer les tunnels GRE à l'aide du service Citrix SD-WAN Orchestrator, consultez la section Service GRE.

Configuration des chemins dynamiques pour la communication de succursale à succursale

November 16, 2022

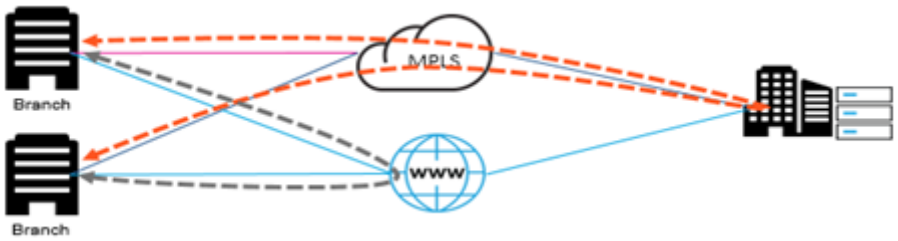
Avec la demande de VoIP et de visioconférence, le trafic se déplace de plus en plus d'un bureau à l'autre. Il est inefficace de configurer des connexions maillées complètes via des centres de données, ce qui peut prendre beaucoup de temps.

Avec Citrix SD-WAN, vous n'avez pas besoin de configurer les 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 de temps sont atteints, un chemin est créé dynamiquement si ce nouveau chemin a de meilleures caractéristiques de performance que le chemin fixe. Le trafic de session est transmis via le nouveau chemin d'accès. Il en résulte une utilisation efficace des ressources. Les chemins d'accès n'existent que lorsqu'ils sont nécessaires et réduisent la quantité de trafic transmis vers et depuis le centre de données.

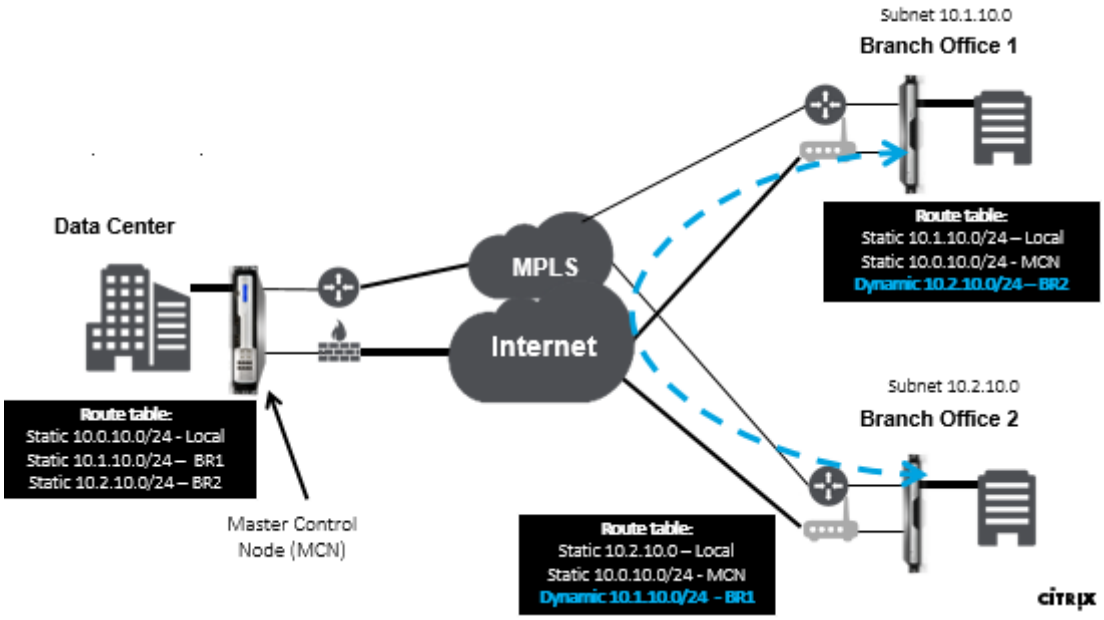
Les avantages supplémentaires du réseau SD-WAN comprennent :

- Seuils de bande passante et de PPS pour autoriser les connexions de branche à branche
- Réduction des besoins en bande passante à l'intérieur et à l'extérieur du centre de données tout en minimisant la latence
- Les chemins créés à la demande dépendent des seuils définis
- Libérer dynamiquement les ressources réseau lorsqu'elles ne sont pas nécessaires
- Réduction de la charge sur le nœud de contrôle maître et de la latence

Communication de branche à branche 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 des chemins virtuels à n'importe quel
- 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 limite la plus basse dynamique, 8 limite la plus basse statique = total 16) qui peuvent être configurés.

Comment activer le chemin virtuel dynamique dans l'interface graphique SD-WAN

Pour activer les chemins virtuels dynamiques à l'aide du service Citrix SD-WAN Orchestrator, consultez Chemins virtuels.

Transfert WAN vers WAN

August 31, 2022

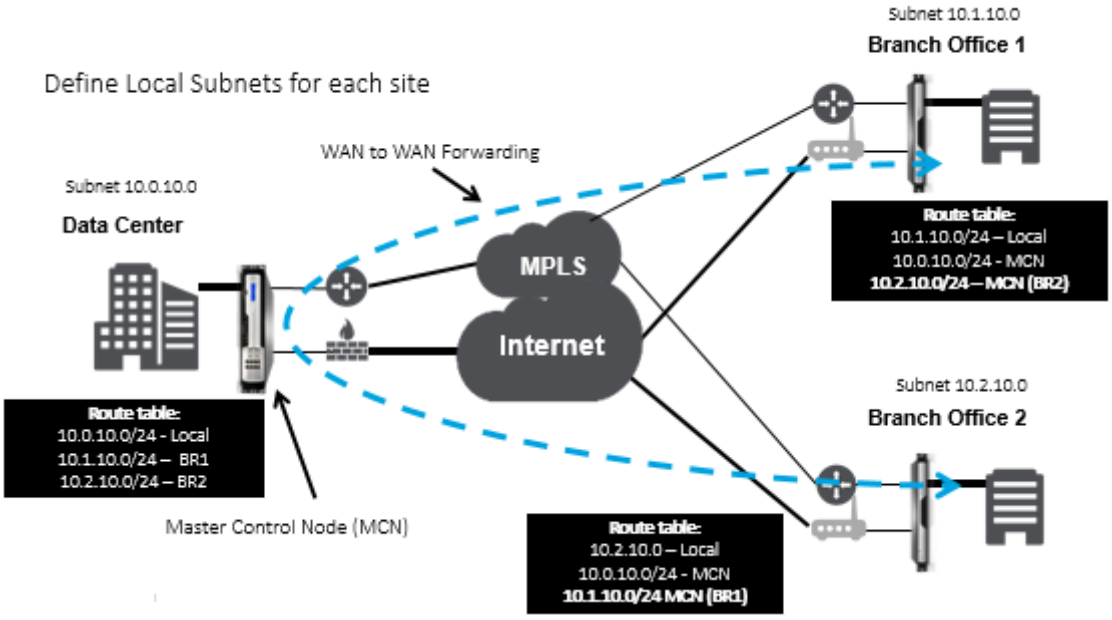
L'activation du transfert WAN vers WAN sur le MCN permet au MCN de publier des itinéraires de site distants.

- Les clients sont au courant des routes locales MCN et d'autres itinéraires de site client

- Du point de vue du client, toutes les routes sont considérées comme des routes MCN

Lorsque le transfert WAN à WAN n'est pas activé sur le MCN, des problèmes de communication de succursale à succursale sont rencontrés dans le réseau client.

Les appliances s'exécutant en mode client ne connaissent pas les autres sous-réseaux de branches tant que le transfert WAN vers WAN n'est pas activé sur le MCN. L'activation de cette option permet aux nœuds SD-WAN de la branche de connaître les autres sous-réseaux de branche. Le trafic destiné à d'autres succursales est transféré à MCN. MCN l'achemine vers la destination correcte.



Surveillance et dépannage

August 31, 2022

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 de surveillance et de 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

Surveillance du réseau étendu virtuel

August 31, 2022

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 de 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 cliente.
- **Adresse IP de gestion :** il s'agit de l'adresse IP de gestion de l'appliance.
- **Temps de disponibilité de l'appliance :** spécifie la durée pendant laquelle l'appliance a été exécutée depuis le dernier redémarrage.
- **Temps de disponibilité du service** : spécifie la durée pendant laquelle le service Virtual WAN a été exécuté depuis le dernier redémarrage.

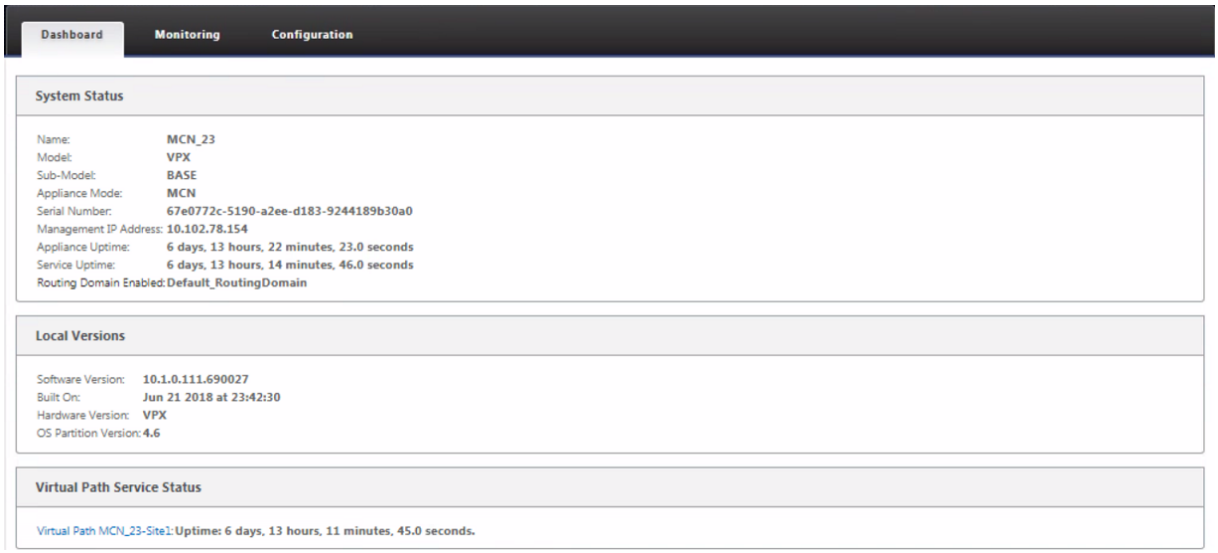
État du service de chemin d'accès virtuel :

Chemin virtuel [nom du site] : affiche l'état de tous les chemins virtuels associés à cette appliance. Si le service WAN virtuel est activé, cette section est incluse sur 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 logicielle :** il s'agit de la version du package logiciel CloudBridge Virtual Path actuellement activé sur l'appliance.
- **Build on** —Il s'agit de la date de création 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 la 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.



Affichage des informations statistiques

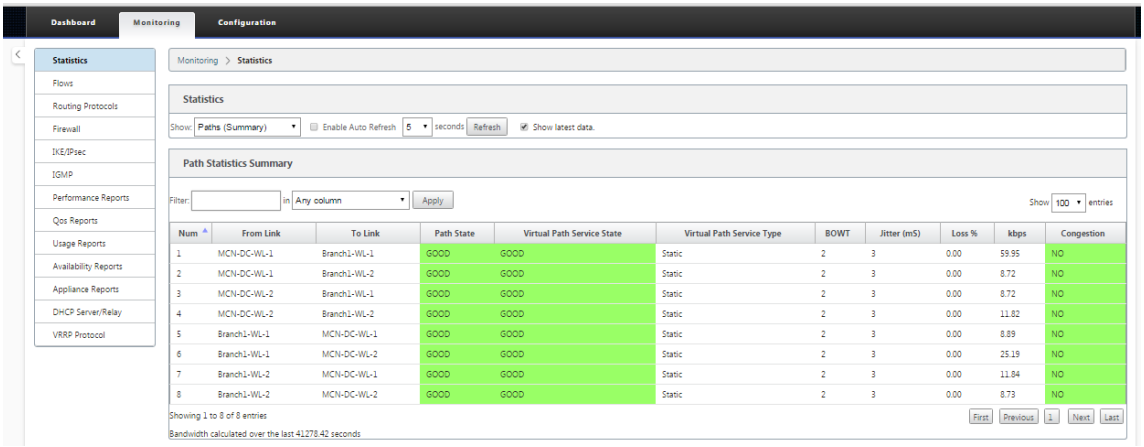
August 31, 2022

Cette section fournit des instructions de base pour afficher les informations de statistiques Virtual WAN.

1. Connectez-vous à l'interface Web de gestion du MCN.
2. Sélectionnez l'onglet **Surveillance** .

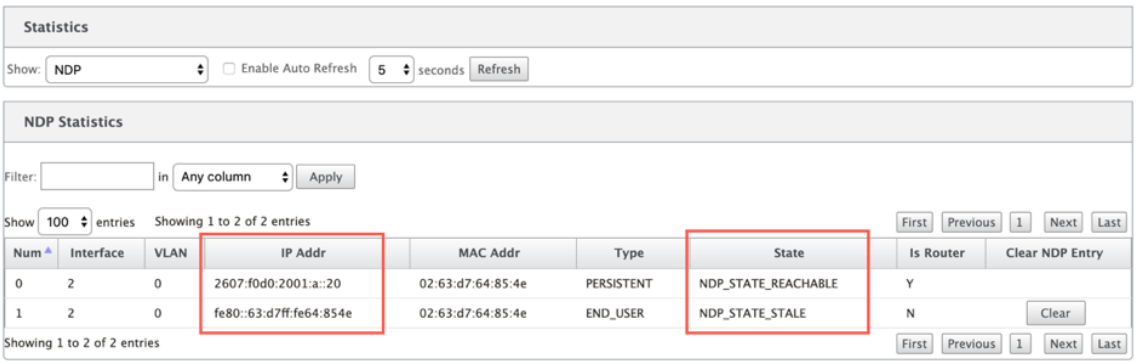
   L'arborescence **de navigation Surveillance** s'ouvre dans le volet gauche. Par défaut, cette option affiche également la page **Statistiques** avec **les chemins** présélectionnés dans le champ **Afficher** . Il contient un tableau détaillé des statistiques de chemin d'accès.

> **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).

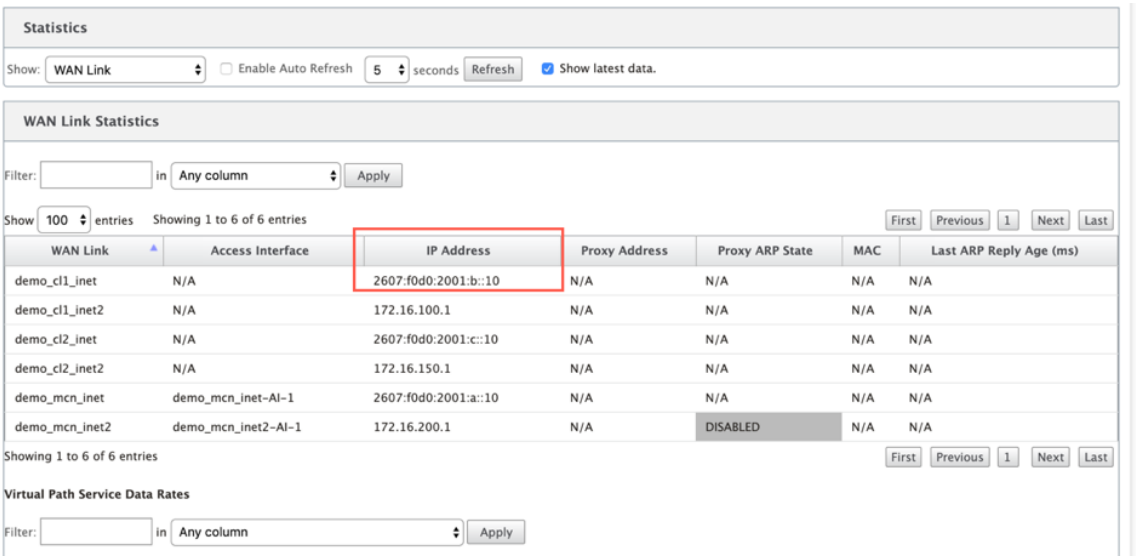


Avec la version 11.1.0, l'option NDP (Neighbor Discovery Protocol) est ajoutée pour le débogage des problèmes de découverte de voisins.

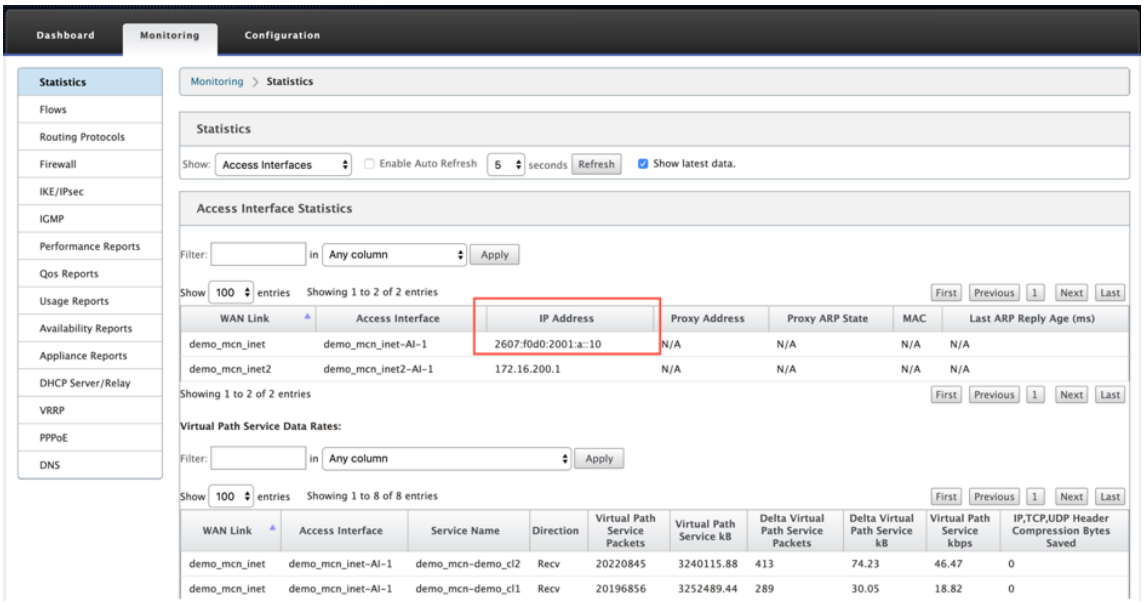
1. Sélectionnez l'option NDP dans le menu déroulant Afficher et vous pouvez afficher l'état de NDP ainsi que les adresses IPv6.



2. Sélectionnez Lien WAN dans le menu déroulant. Vous pouvez également afficher l'adresse IPv6 si vous avez configuré sous l'onglet Adresse IP.

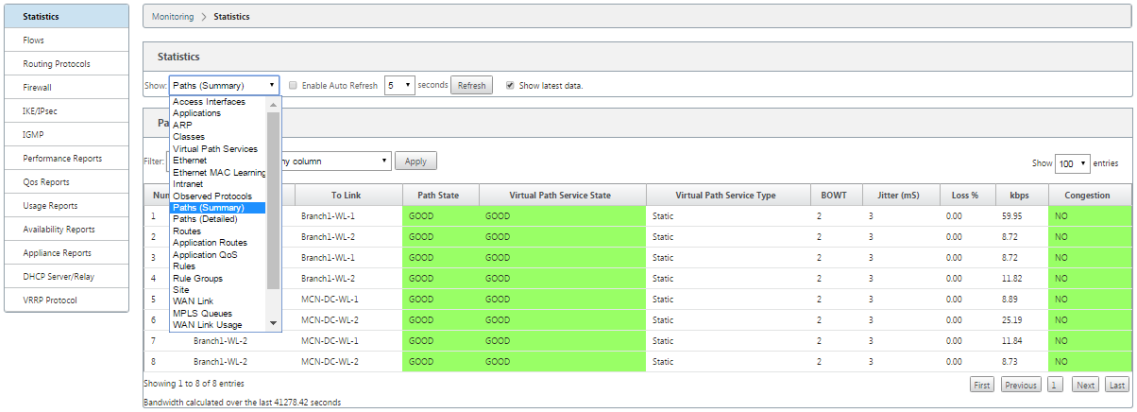


3. Vous pouvez également afficher les statistiques de l'interface d'accès.



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.



Sélectionnez un filtre dans le menu **Afficher** pour afficher un tableau d'informations statistiques pour cette rubrique.

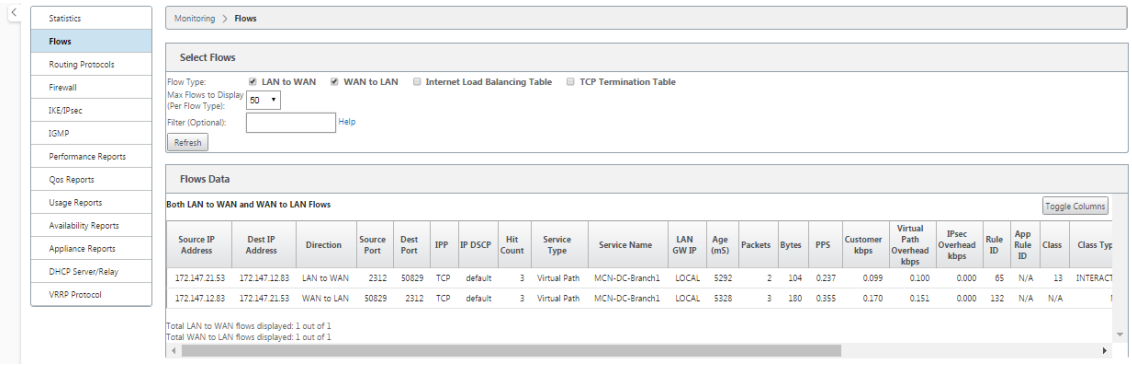
Affichage des informations de flux

August 31, 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**.

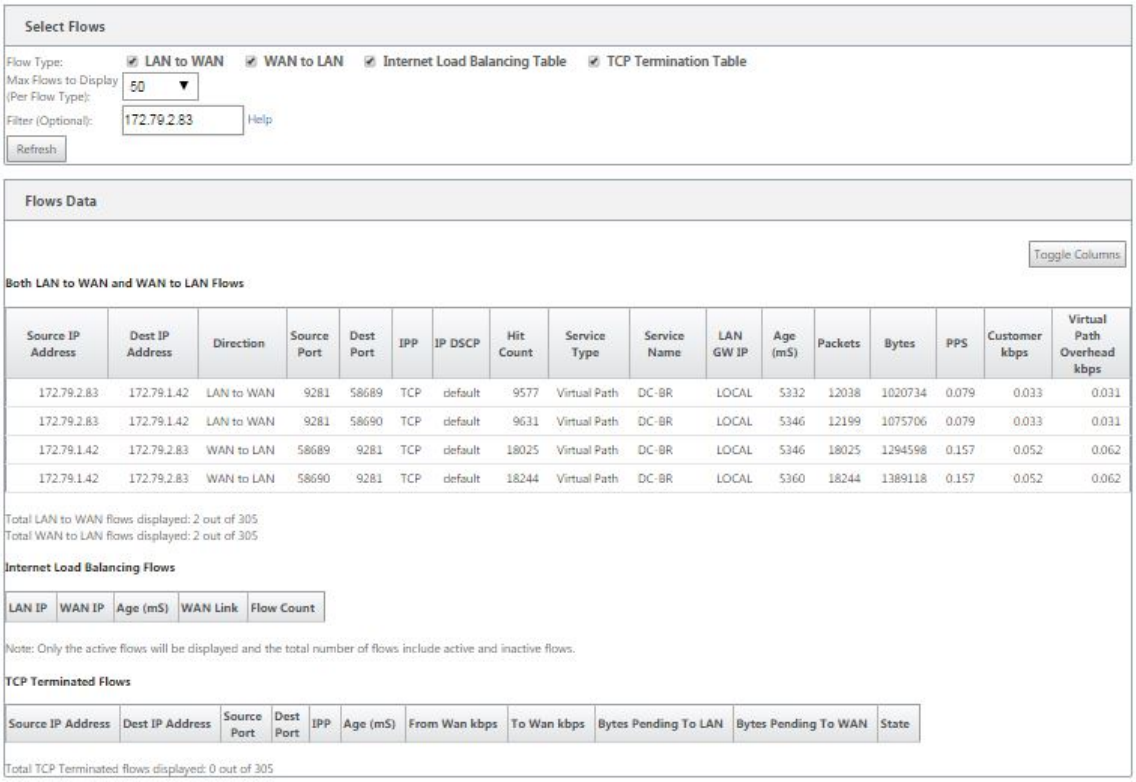


3. Sélectionnez le **type de flux**. Le champ **Type de flux** se trouve dans la section **Sélectionner les flux** en haut de la page **Flux** . En regard du champ **Type de flux** se trouve une ligne d'options de case à cocher permettant de sélectionner les informations de flux que vous souhaitez afficher. 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.

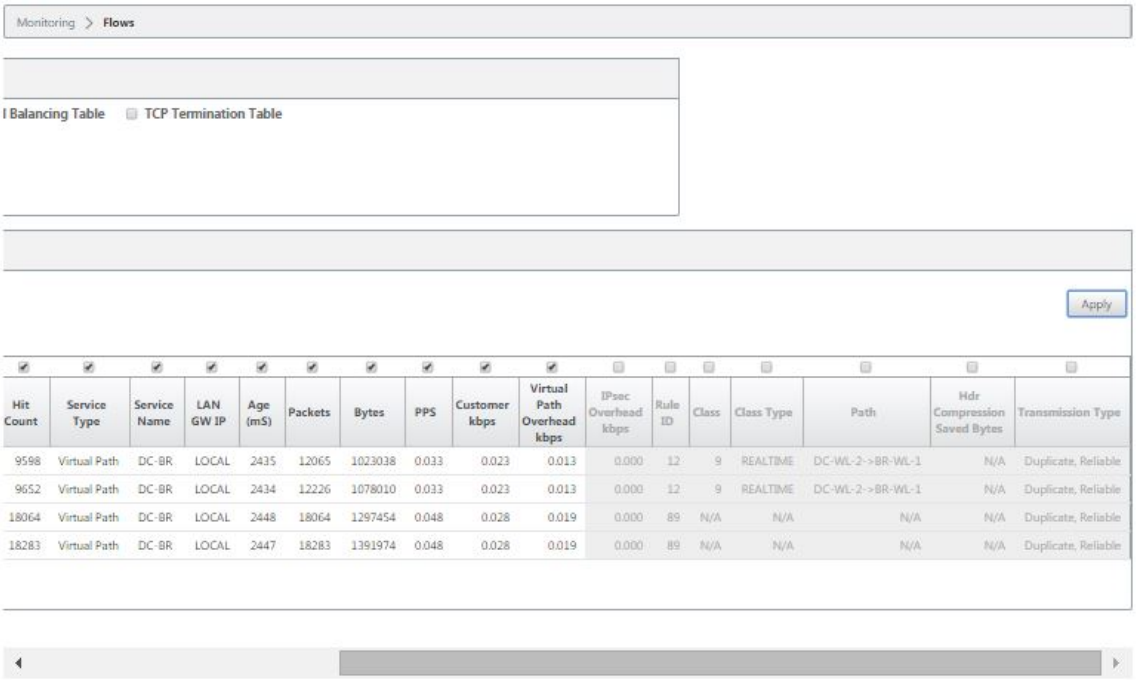
> **Conseil**
>
> Pour obtenir des instructions détaillées sur l'utilisation de filtres pour affiner les résultats de la table de **flux**, cliquez sur **Aide** à droite du champ **Filtre** . Pour fermer l'écran d'aide, cliquez sur **Actualiser** dans le coin inférieur gauche de la section **Sélectionner 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.



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.

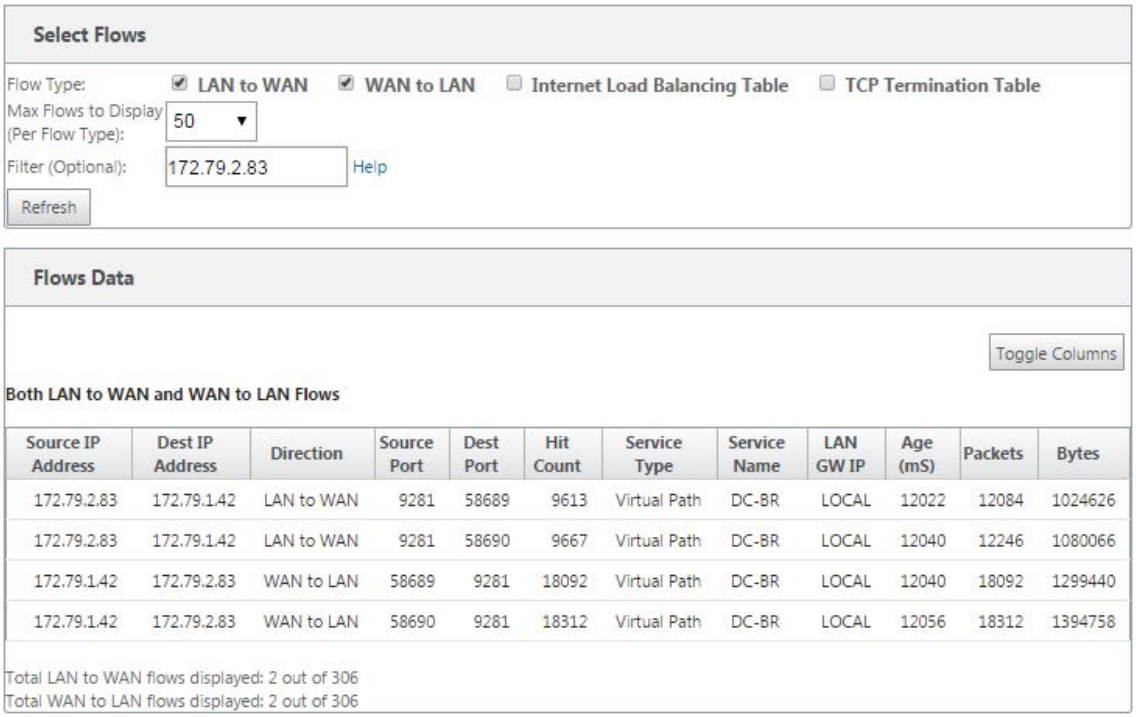


10. Activez une case à cocher pour sélectionner ou désélectionner une colonne.

    - **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.



Applications DPI dans SD-WAN Center

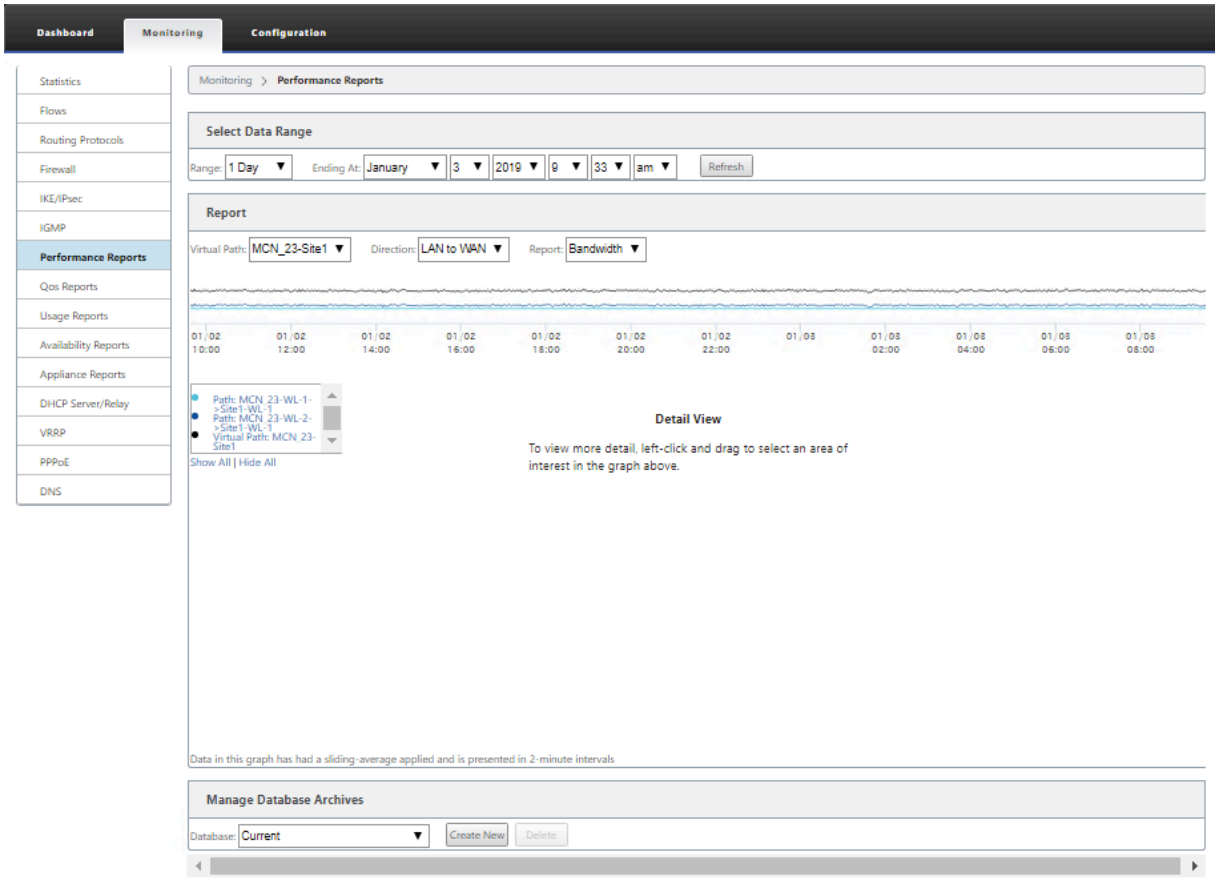
Dans les versions antérieures, environ 4 000 applications et configurées avec 800 services (550 chemins virtuels, 256 services intranet) peuvent être identifiées. Le stockage de ces données aurait un impact sur les performances globales du système (cycles CPU et espace disque requis pour stocker les 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

August 31, 2022

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 étendu virtuel, utilisez l'interface Web Virtual WAN Center.

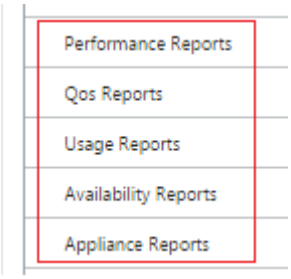
Pour générer et afficher des rapports Virtual WAN, procédez comme suit :

1. Ouvrez une session sur l'interface Web de gestion du MCN, puis sélectionnez l'onglet **Surveillance** .

   L'arborescence **de navigation Surveillance** 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 :

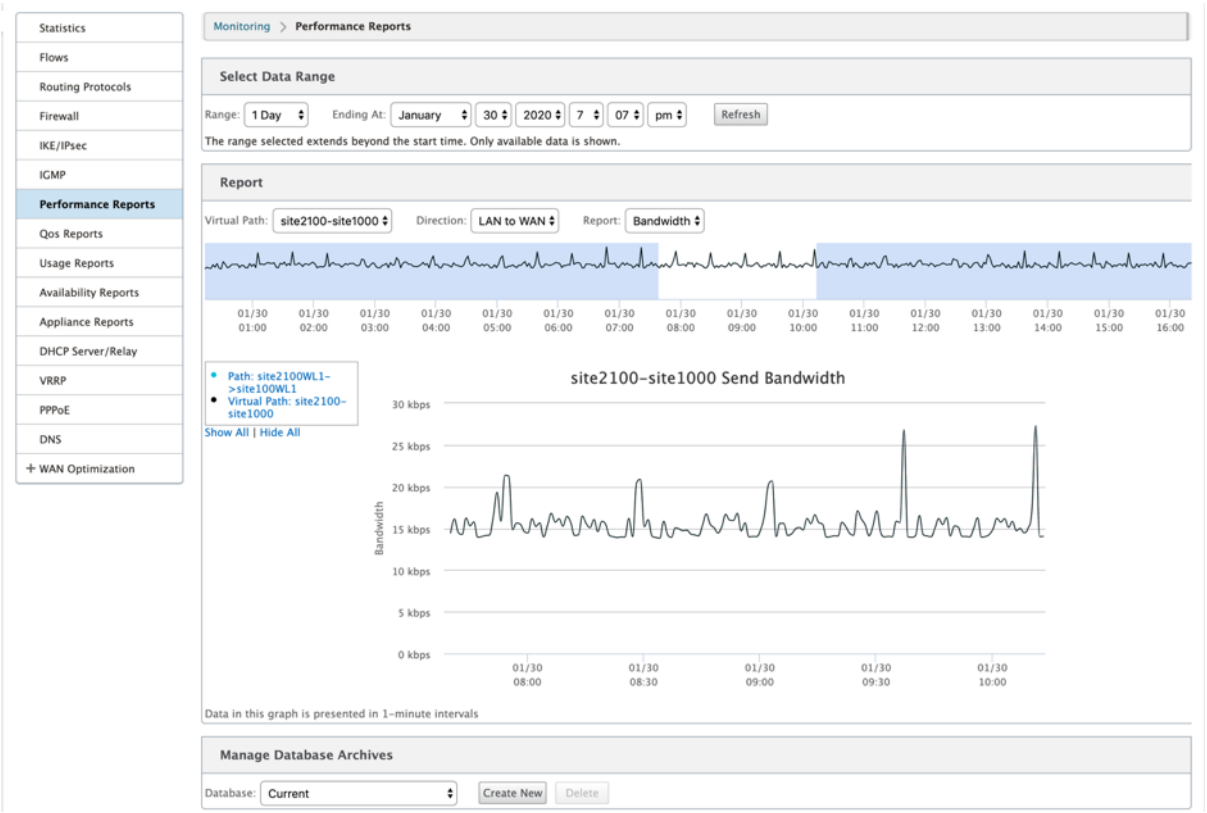
- **Rapports sur le rendement**
- **Rapports QoS**
- **Rapports d'utilisation**
- **Rapports de disponibilité**
- **Rapports de l'appliance**

3. Sélectionnez les options de 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.

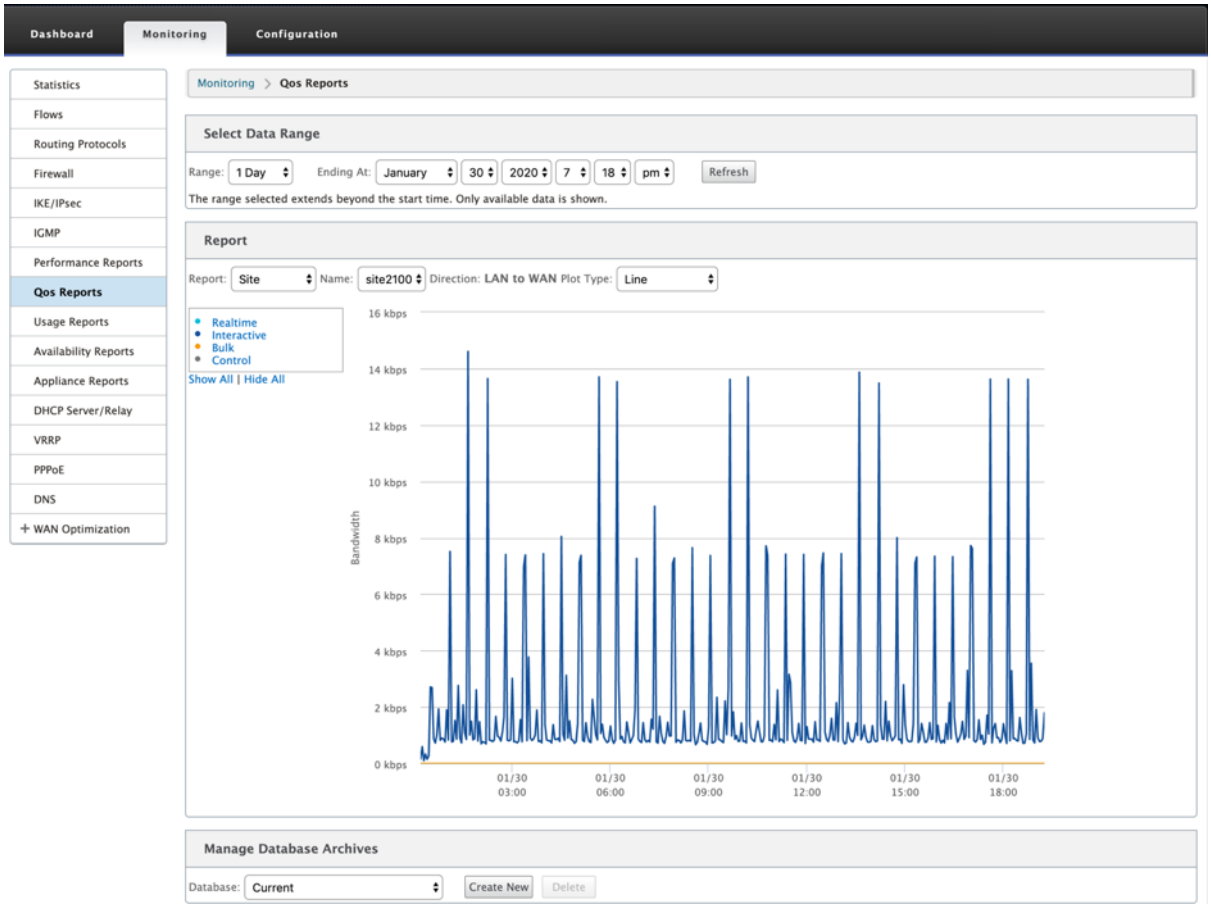


Vous pouvez sélectionner la plage de données selon vos besoins avec les champs suivants pour afficher le rapport de performances :

- **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.

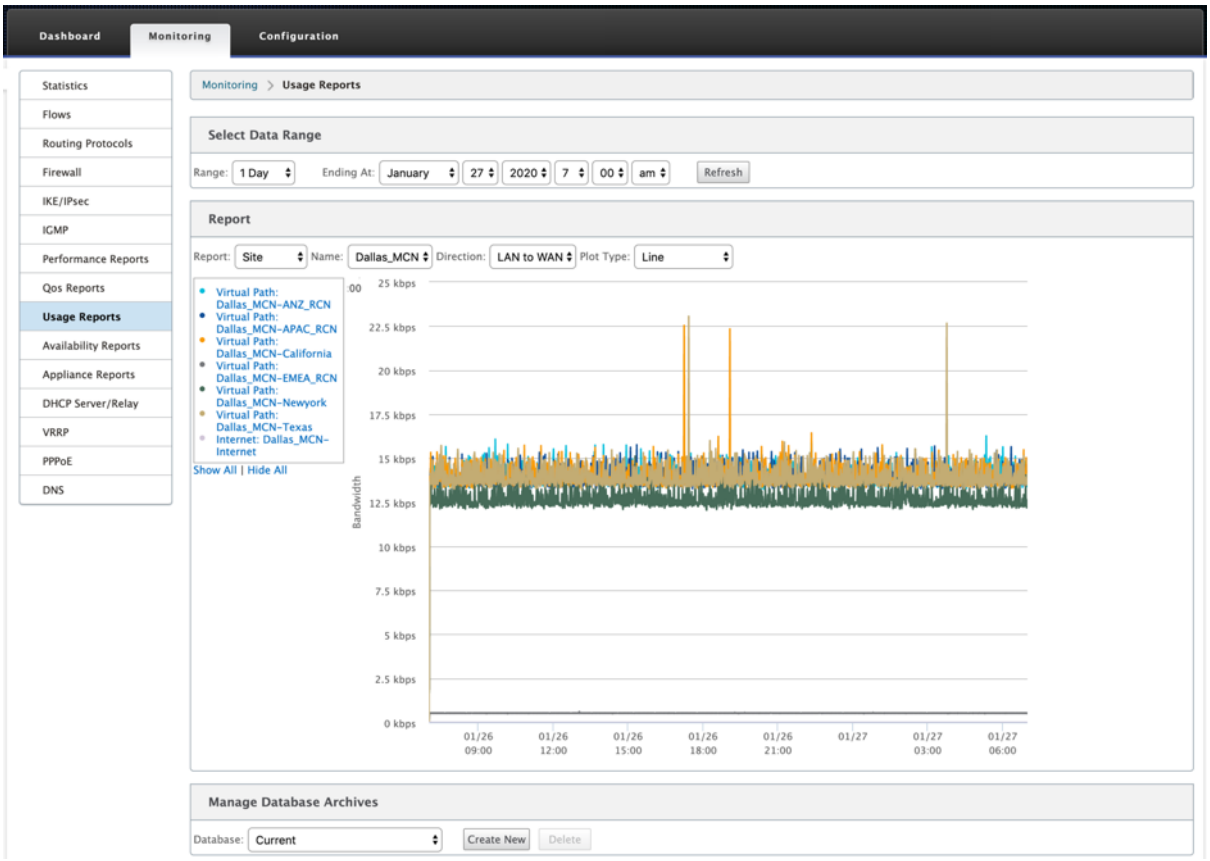


Vous pouvez afficher les mesures suivantes :

- **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

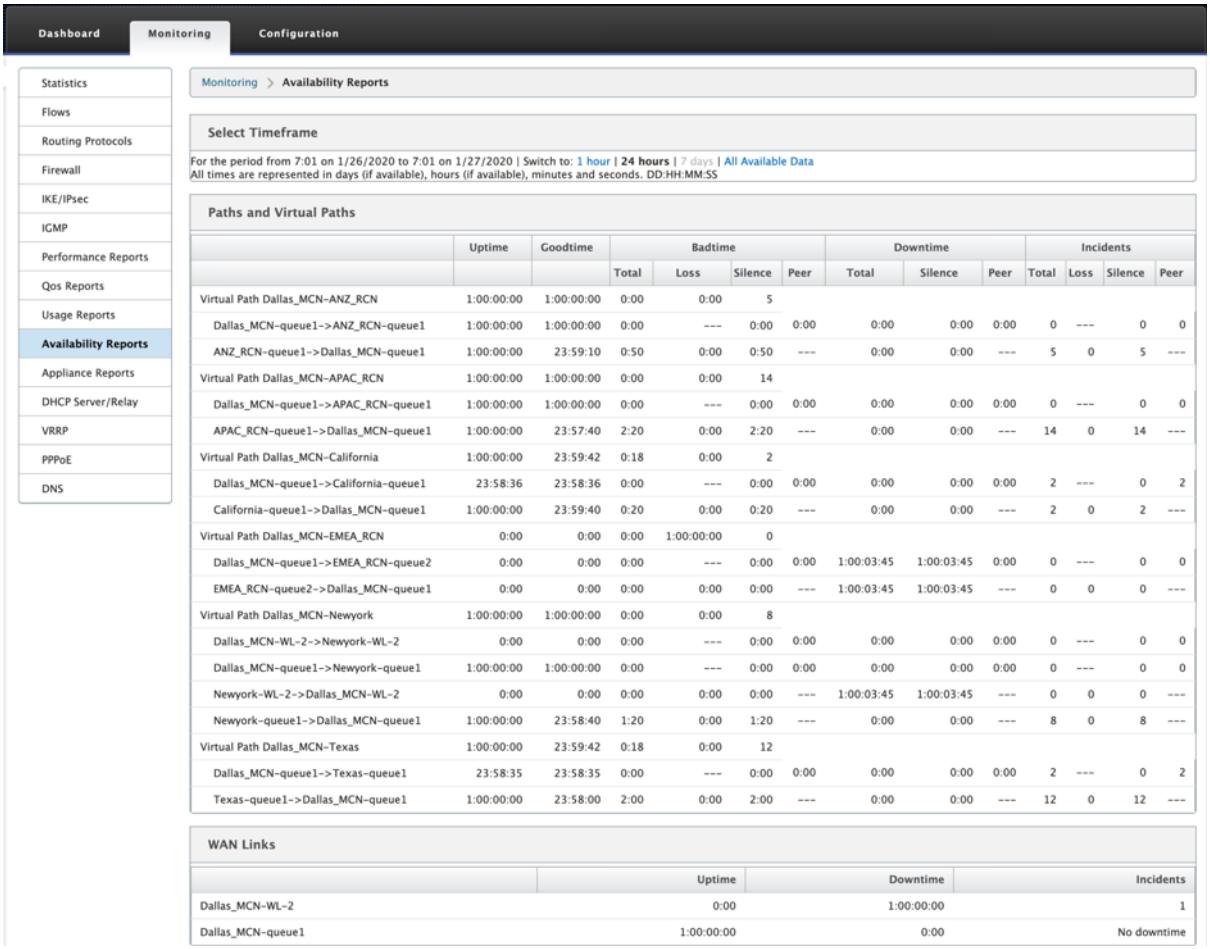
Les rapports d'utilisation fournissent les informations d'utilisation des chemins virtuels.



- **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).

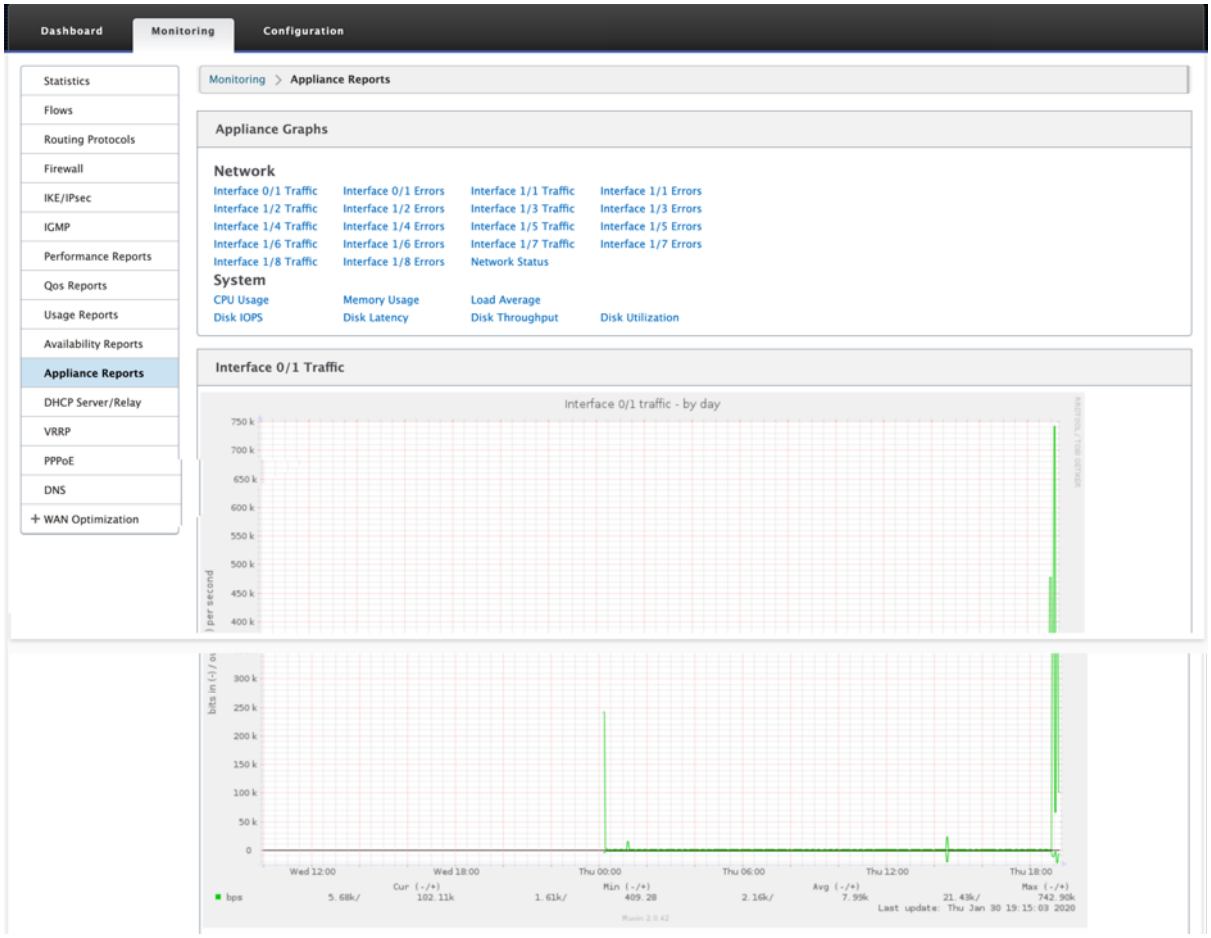
Rapports de disponibilité

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**.



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

August 31, 2022

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 de NAT, consultez la section Pare-feu avec état et prise en charge NAT.

Pour afficher les statistiques du pare-feu :

1. Accédez à **Surveillance** > **Pare-feu.**
2. Sélectionnez **Connexions, Stratégies de filtre ou Stratégies NAT** selon les besoins.
3. Définissez les critères de filtrage selon vos besoins.
4. Cliquez sur **Actualiser**.

Connexions

Vous pouvez vérifier les statistiques relatives aux applications pour la stratégie de pare-feu. Cela vous permet de voir toutes les connexions correspondant à l'application sélectionnée, d'où elles proviennent, d'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 - La famille d'applications utilisée comme critère de filtre pour la connexion.
- IP Protocol - Protocole IP utilisé par la connexion.
- Zone source - Zone d'origine de la connexion.
- Zone de destination - Zone d'origine du 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 d'origine du trafic répondant.
- Instance de service de destination - Instance du service d'origine du trafic répondant.
- Destination IP - 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.

Filtrer les stratégies

Les stratégies vous permettent de spécifier des actions pour les flux de trafic. Les groupes de filtres de pare-feu sont créés à l'aide des modèles de stratégie de pare-feu et peuvent être appliqués 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.
- IP Protocol - Protocole IP correspondant à la stratégie de filtrage.
- DSCP : balise DSCP que la stratégie de filtre correspond.
- Action de stratégie de filtrage - Action prise 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 répondant est destiné.
- Nom du service de destination - Le cas échéant, le service auquel le trafic répondant est destiné.
- Destination IP - 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 filtrage.
- Zone de destination - Zone de réponse correspondant à la stratégie de filtrage.

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.

- IP Protocol : 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.
- IP intérieure - Adresse IP intérieure, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.

- Port intérieur : plage de ports intérieurs utilisée par la stratégie NAT. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.
- IP externe - Adresse IP externe, entrée en notation décimale pointillée avec un masque de sous-réseau facultatif.
- Port extérieur : plage de ports externes utilisée par la stratégie NAT. Un port unique ou une plage de ports utilisant le caractère « - » est accepté.

Diagnostics

August 31, 2022

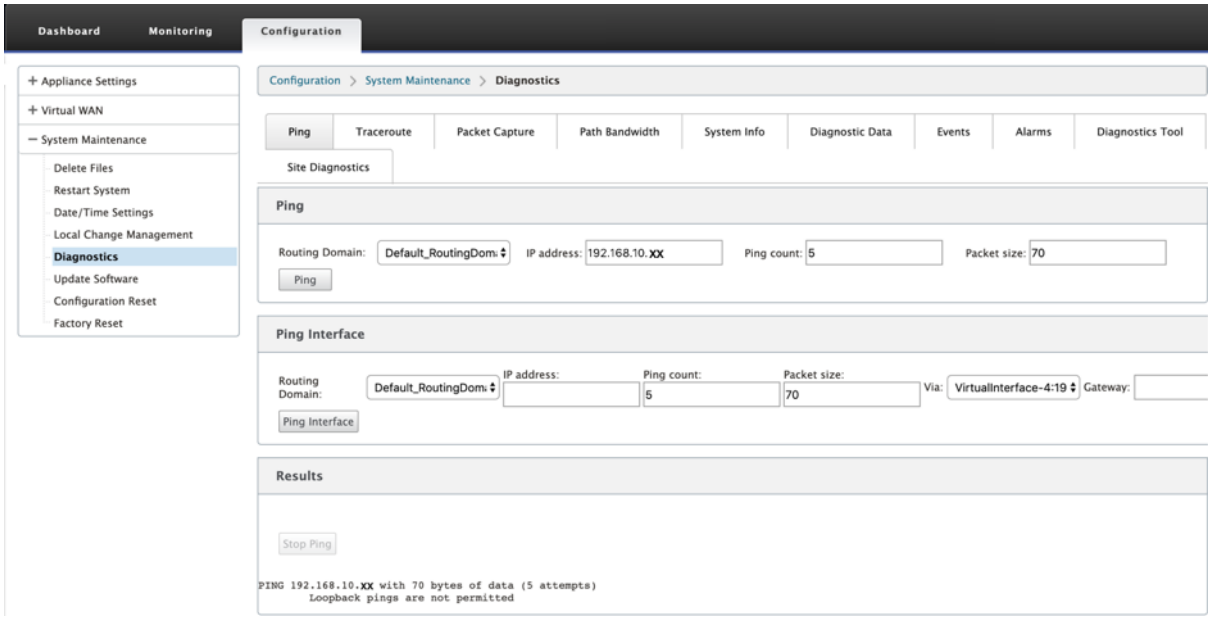
Les utilitaires**Citrix SD-WAN Diagnostics** offrent les options suivantes pour tester et examiner les problèmes de connectivité :

- 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.

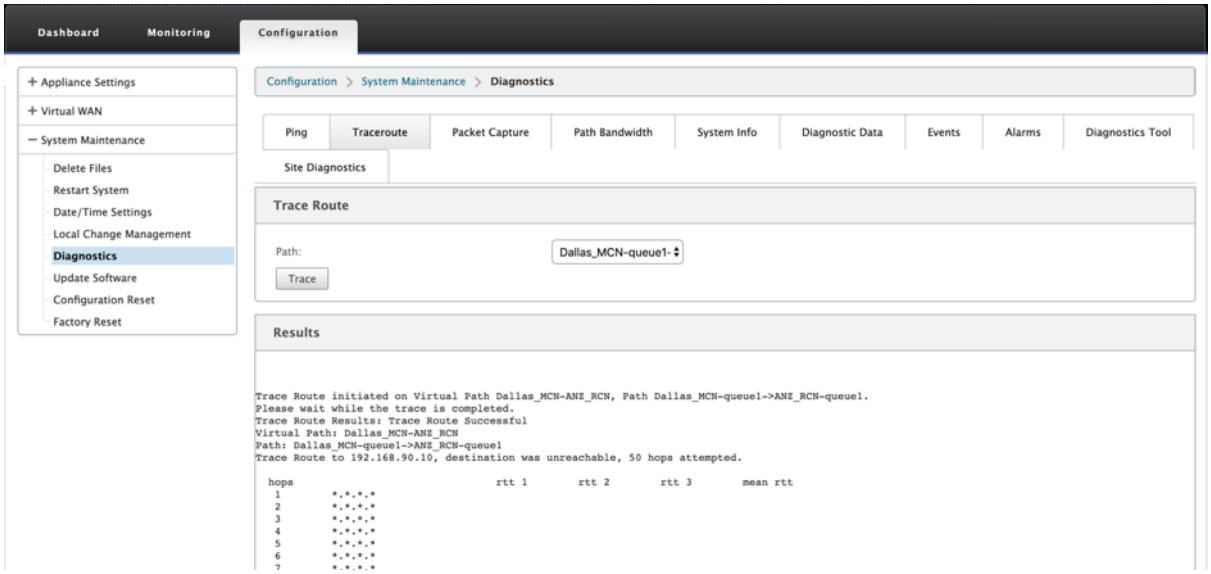


Sélectionnez le domaine de routage. Fournissez une adresse IP valide, un nombre de pings (nombre de fois où la demande ping doit être envoyée) et une taille de paquet (nombre d'octets de données) valides. Cliquez sur **Arrêter le ping** pour arrêter une recherche ping en cours.

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**.

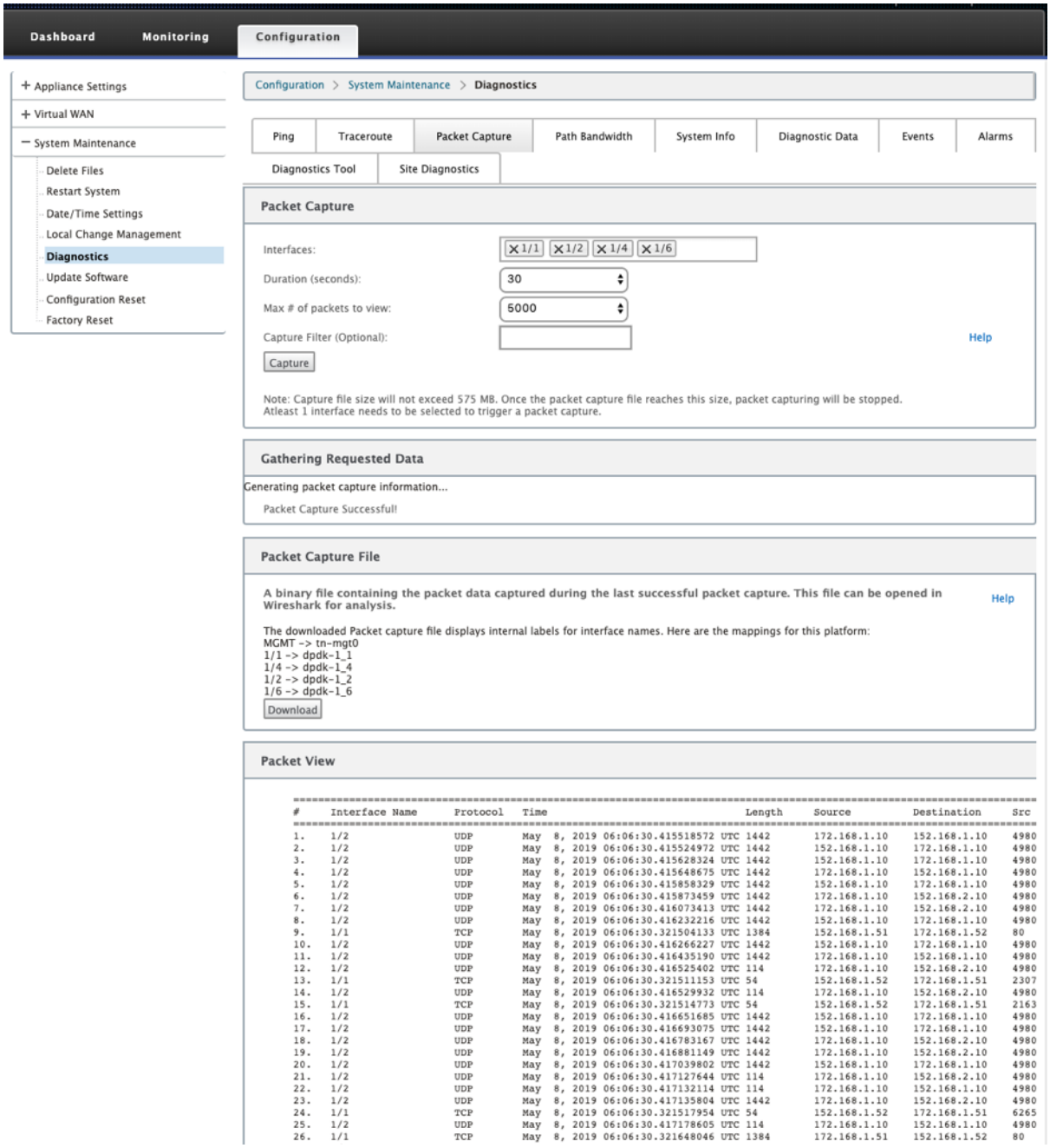


Traceroute permet de découvrir et d'afficher le chemin ou l'itinéraire vers un serveur distant. Utilisez l'option **Traceroute** comme outil de débogage pour détecter les points de défaillance d'un réseau.

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.



Fournissez les entrées suivantes pour l'opération de capture de paquets :

- **Interfaces** - Des interfaces actives sont disponibles pour la capture de paquets pour l'appliance 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 facultatif Filtre de capture 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.

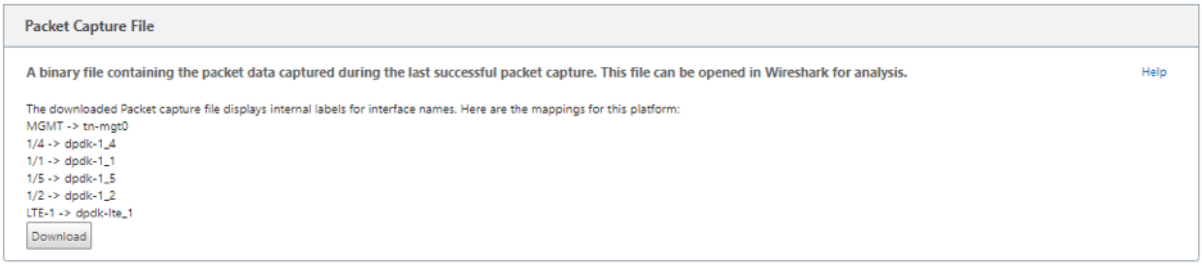
Cliquez sur **Capturer** pour afficher le résultat de la capture de paquets. Vous pouvez également télécharger un fichier binaire contenant les données de paquets capturées lors de la dernière capture de paquets réussie.

Collecte des données demandées

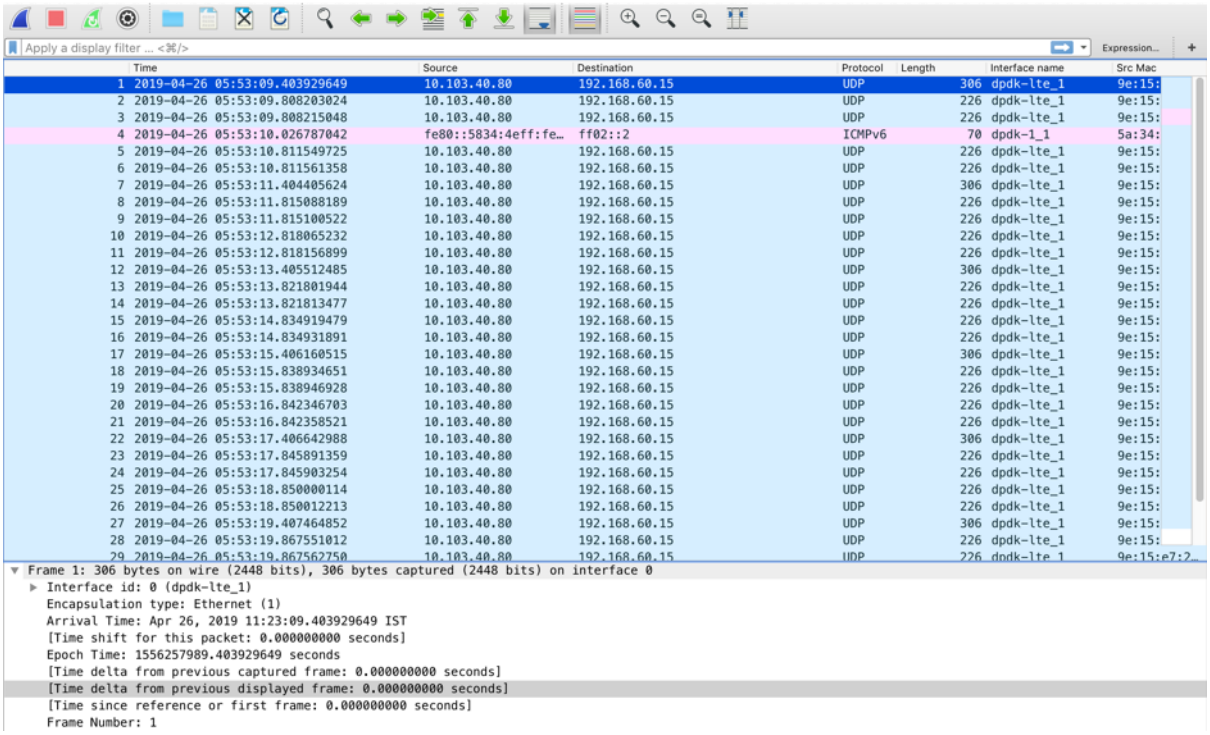
Vous pouvez voir l'état de la génération d'informations de capture de paquets (si la capture de paquets a réussi ou pas de capture de paquets) dans ce tableau.

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.

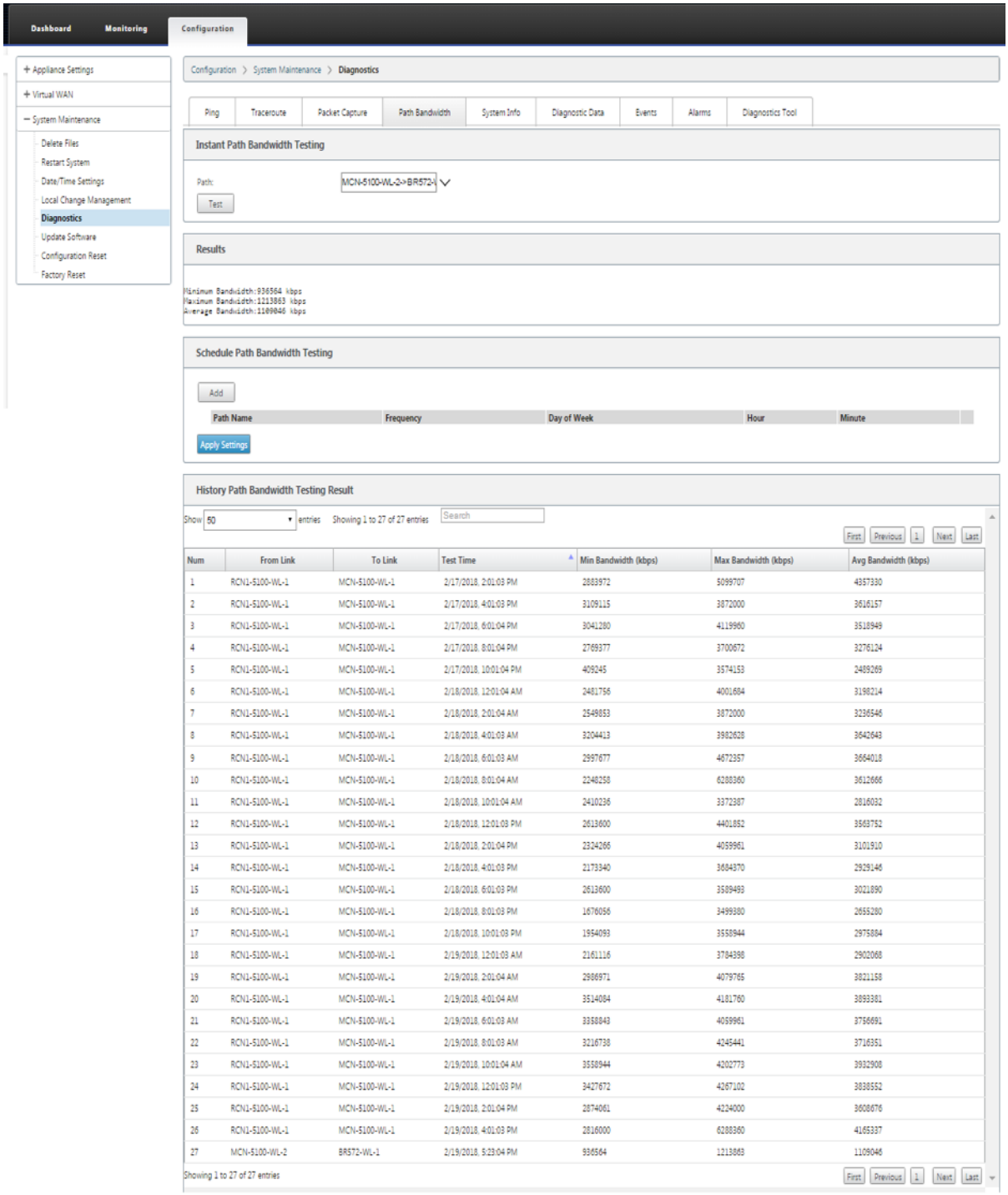


Vue des paquets

Si la taille du fichier de capture de paquets est supérieure, il faut plus de temps pour terminer le processus de rendu de la vue de paquets. Dans ce cas, il est recommandé de télécharger le fichier et d'utiliser **Wireshark** pour l'analyse plutôt que de se fier au résultat de la **vue Paquet** .

Bande passante du chemin

Pour utiliser la fonctionnalité **Bande passante du chemin** d'accès, accédez à **Configuration > développez Maintenance du système > Diagnostics** et sélectionnez **Bande passante du chemin**.



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.

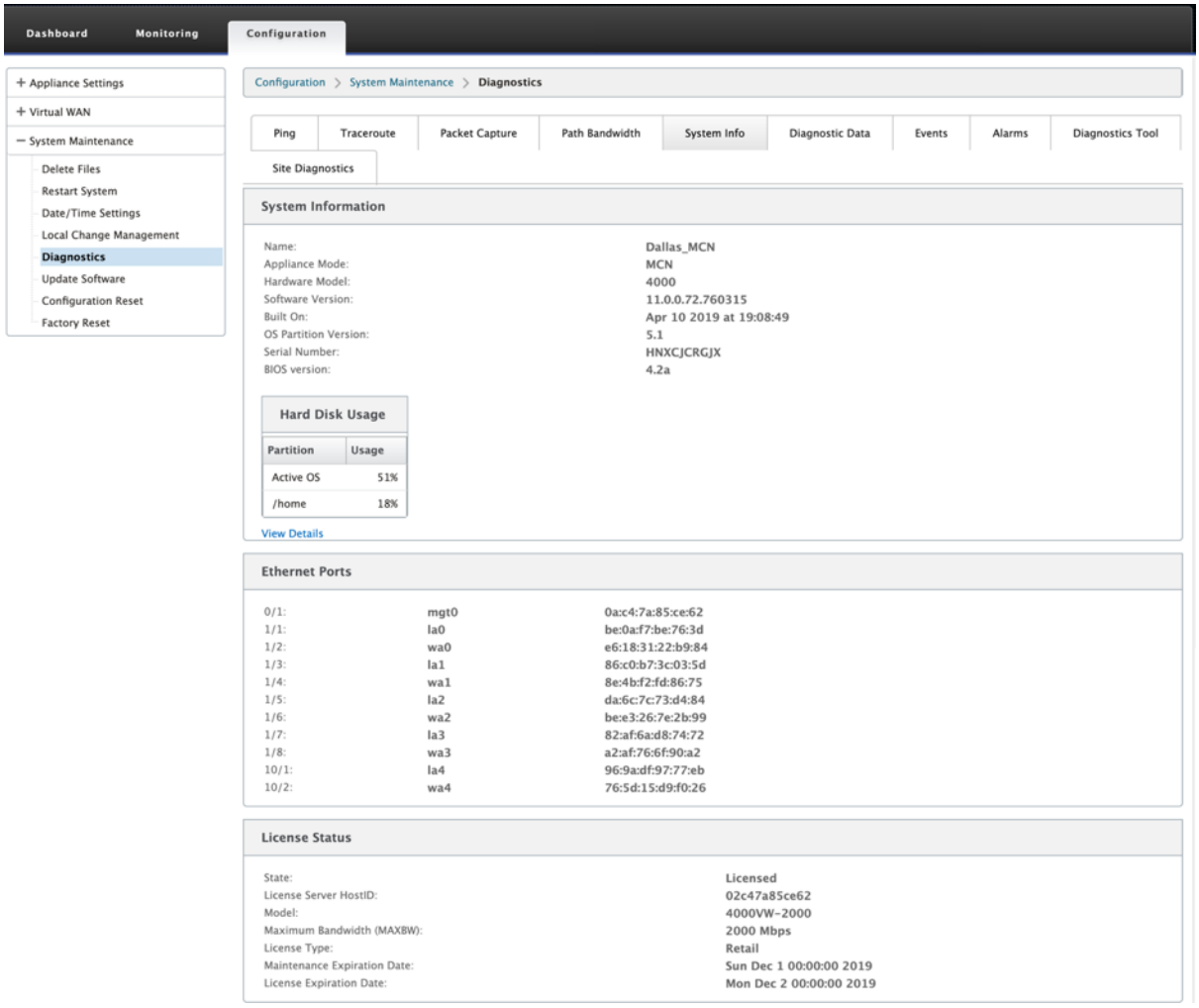
La fonctionnalité Path Bandwidth (Bande passante de chemin) est utile pour démontrer la quantité de bande passante disponible entre deux emplacements au cours des installations nouvelles et

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**.

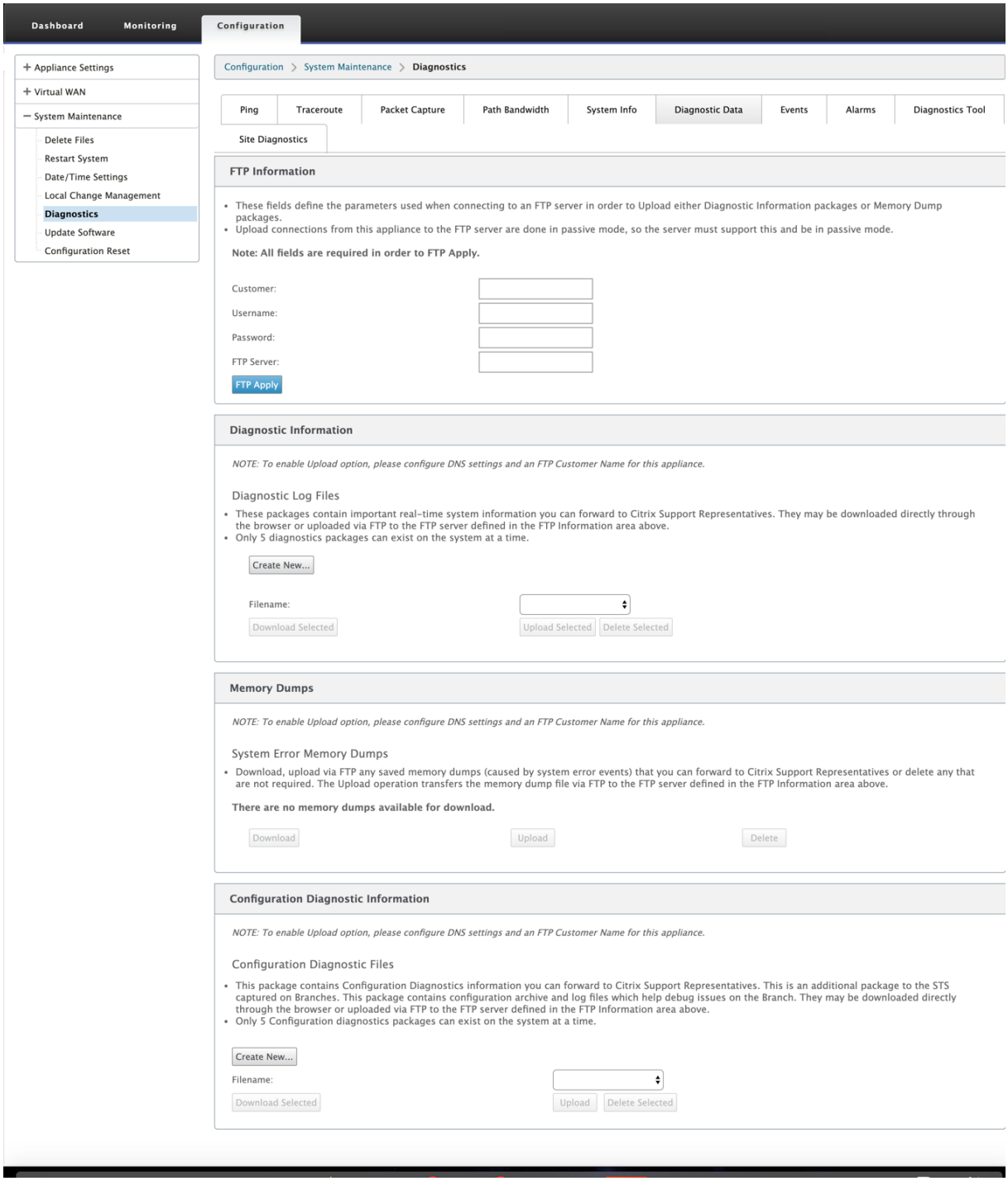


Les **informations système** répertorie tous les paramètres qui ne sont pas définis sur leurs valeurs par défaut. Ces informations sont en lecture seule. Il est utilisé par le support lorsqu'une erreur de configuration est suspectée. Lorsque vous signalez un problème, vous pouvez être invité à vérifier 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**.



Les **données de diagnostic** incluent :

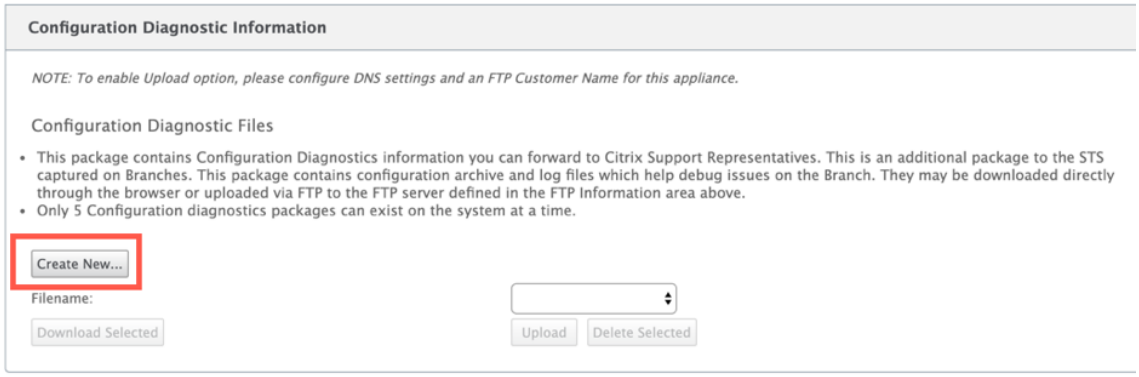
- **Informations FTP** : indiquez les détails des paramètres FTP, puis cliquez sur **Appliquer FTP**. Informations FTP requises pour connecter un serveur FTP pour télécharger le package d'informations de diagnostic.
- **Informations de diagnostic** : le package de fichiers journaux de diagnostic contient 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**.

  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.

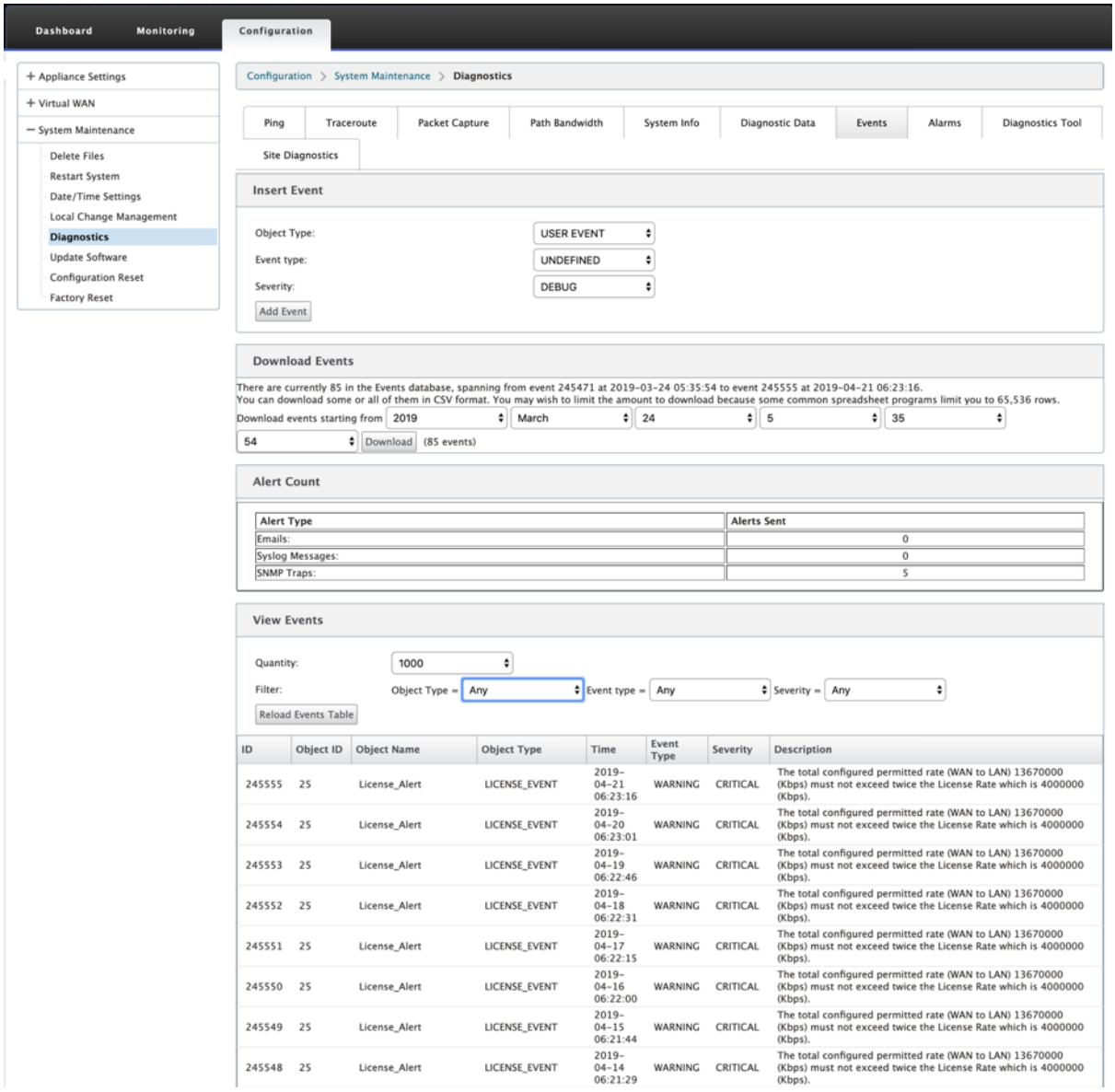
Événements

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**.



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.

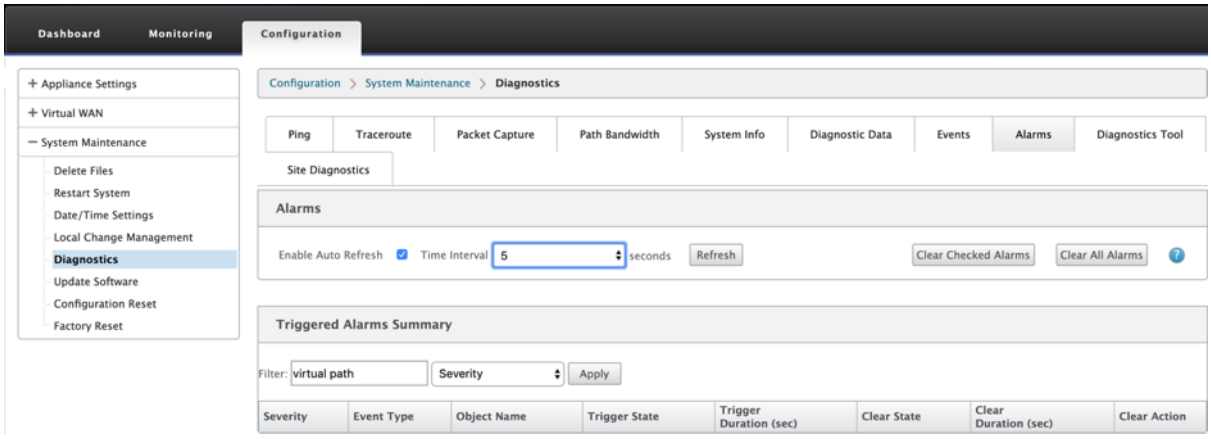
Les notifications sont générées pour les événements égaux ou supérieurs au niveau de gravité spécifié pour le type d'événement.

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 > Diagnostics**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'appliance 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 le 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 :

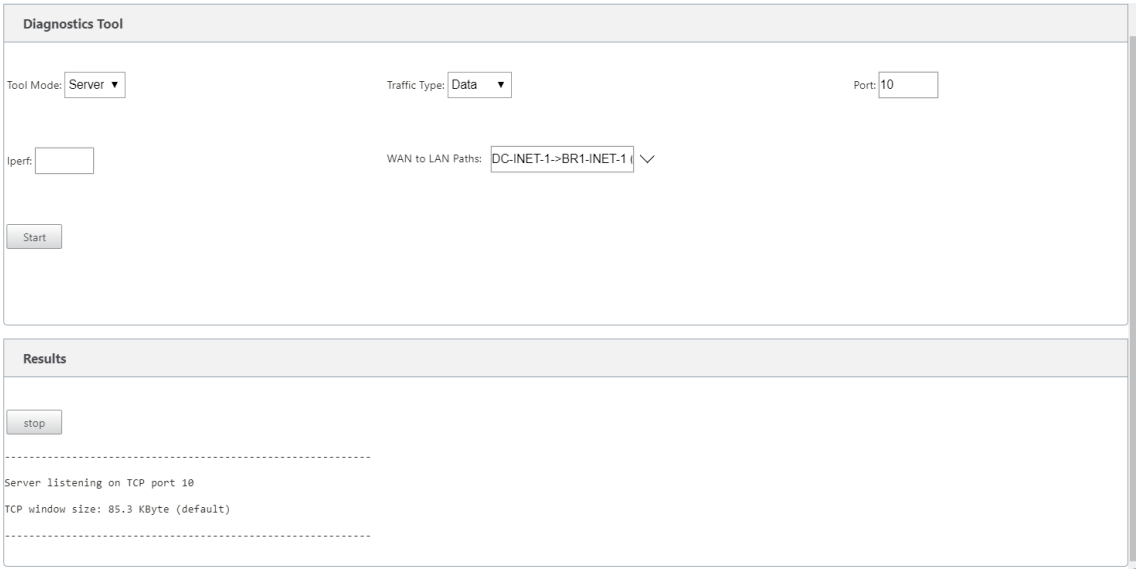
- **Contrôle** : génère du trafic sans aucune QoS/planification appliquée aux paquets. Par conséquent, les paquets sont envoyés sur le chemin sélectionné dans l'interface utilisateur, même si le chemin n'est pas le meilleur à ce moment. Ce trafic est utilisé pour tester des chemins spécifiques et aide 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.



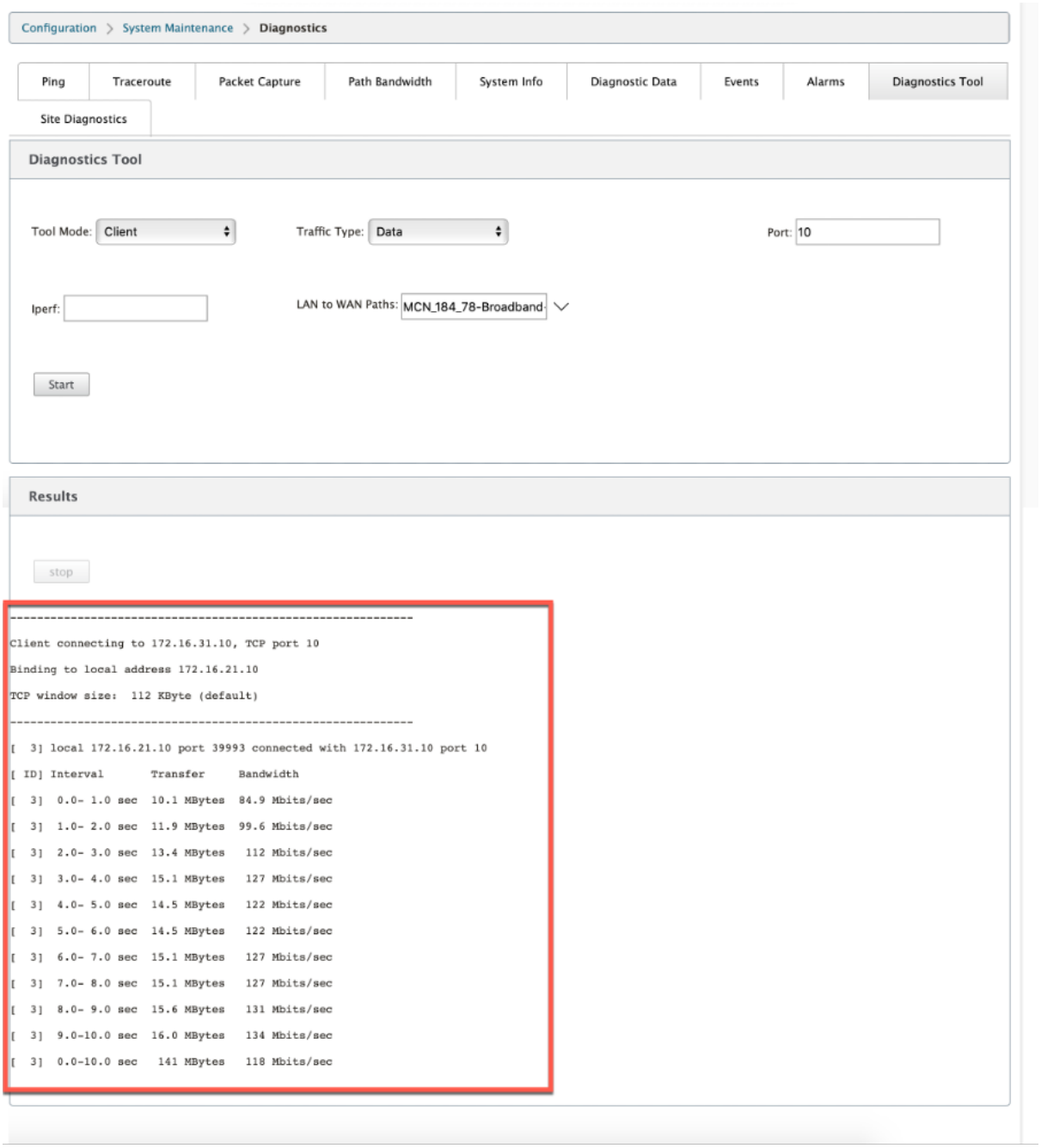
2. Dans le champ **Mode outil**, sélectionnez **Serveur** sur un matériel et sélectionnez **Client** sur l'appliance résidant à l'extrémité distante du chemin sélectionné.
3. Dans le champ **Type de trafic**, sélectionnez le type de trafic de diagnostic (**Contrôle** ou **Données**). Sélectionnez le 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.

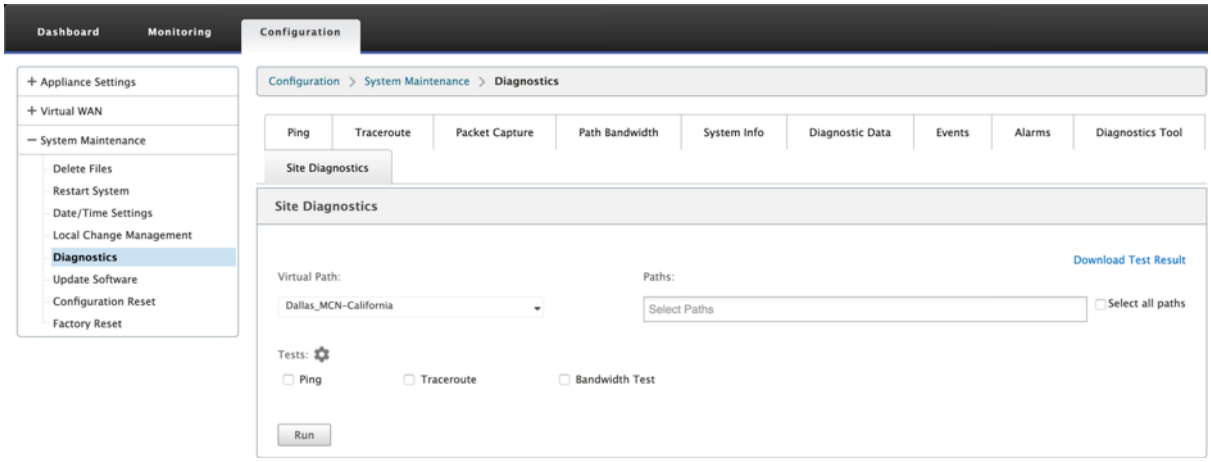
Le résultat affiche le mode (client ou serveur) de l'appliance sélectionnée et le port TCP ou UDP sur lequel le test est exécuté. Il affiche périodiquement les données transférées et la bande passante utilisée pendant l'intervalle spécifié jusqu'à ce que la durée totale du test soit atteinte.



Diagnostics de

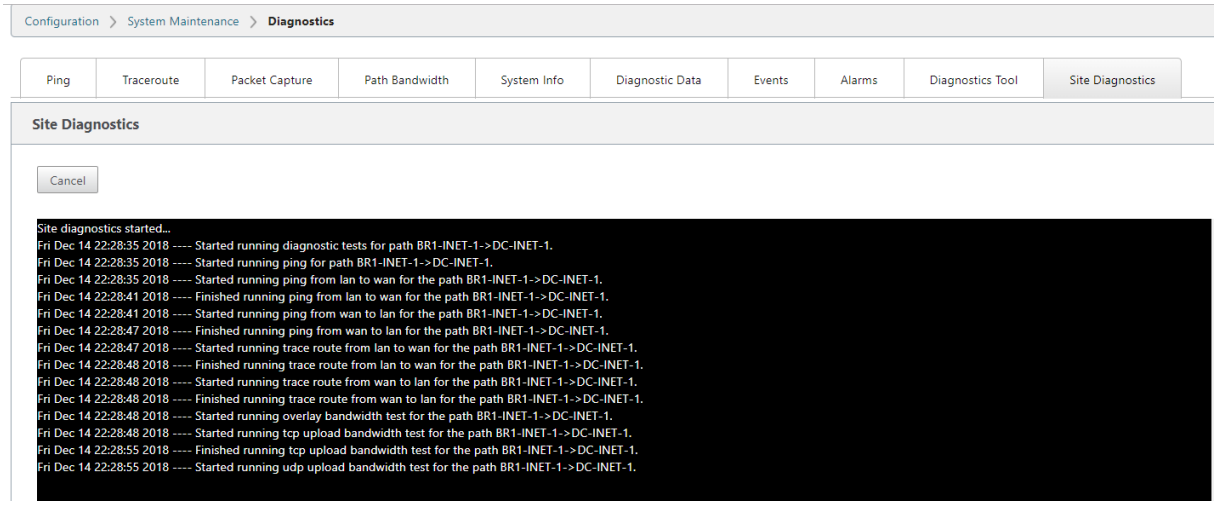
Vous pouvez tester l'utilisation de la bande passante, ping et effectuer un traceroute pour les liens WAN configurés sur différents sites du réseau Citrix SD-WAN. Il fournit des informations qui aident à résoudre les problèmes liés à la configuration existante.

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

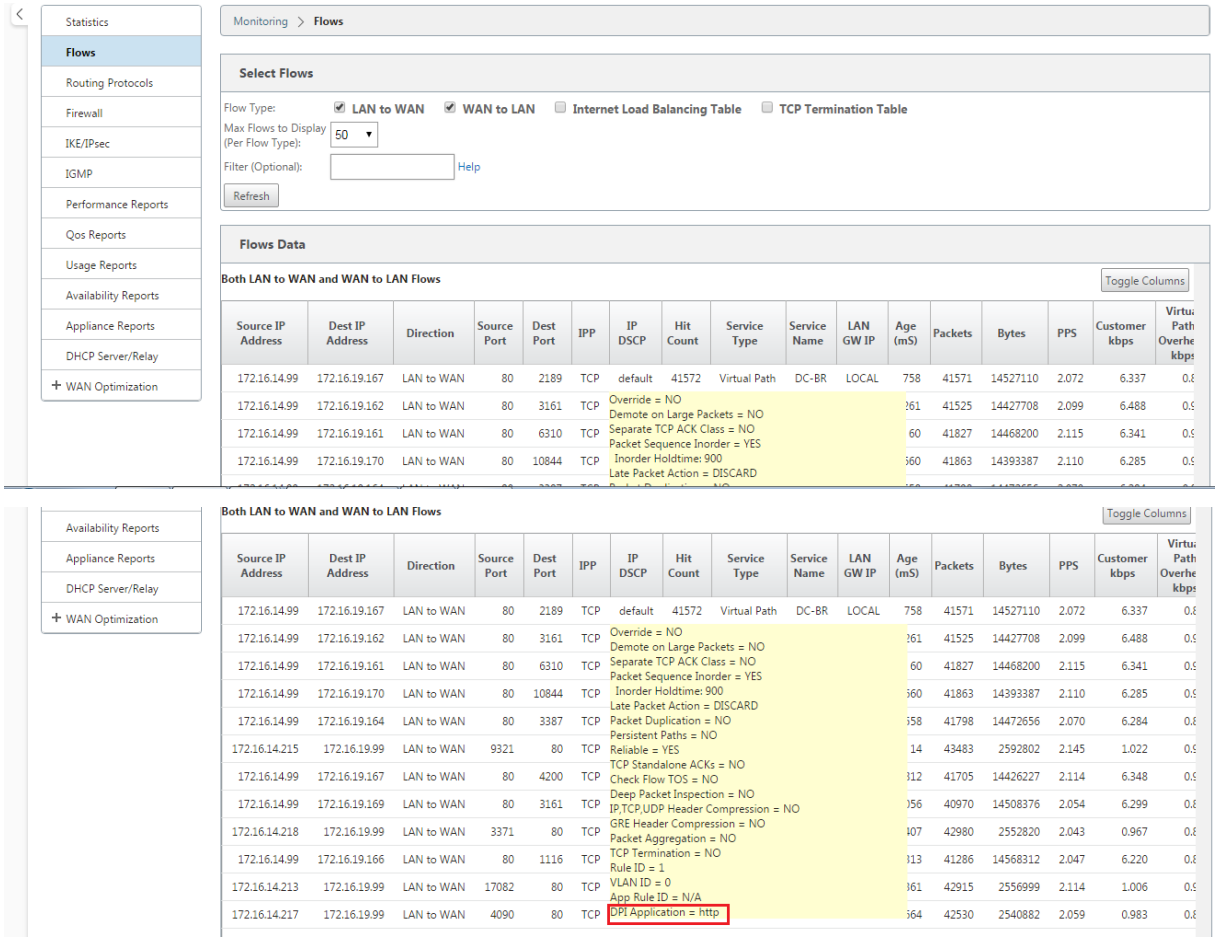
August 31, 2022

Les améliorations apportées au mappage des chemins et à l'utilisation de la bande passante sont mises en œuvre dans l'onglet Surveillance pour afficher les flux de trafic. Par exemple, lorsqu'un seul chemin virtuel sert une connexion réseau et que ce chemin virtuel devient inactif, un nouveau meilleur 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. S'il existe un seul chemin pour traiter le trafic, en supposant qu'il y ait plus de deux chemins de traitement du trafic et que la table de chemin soit 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 virgule suivant comme dernier meilleur chemin. Ce scénario est implémenté lorsqu'il y a un besoin de plus de chemins avec une demande de bande passante.

Surveillance des informations d'application DPI dans l'interface graphique SD-WAN

Le nom de l'objet d'application DPI 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.



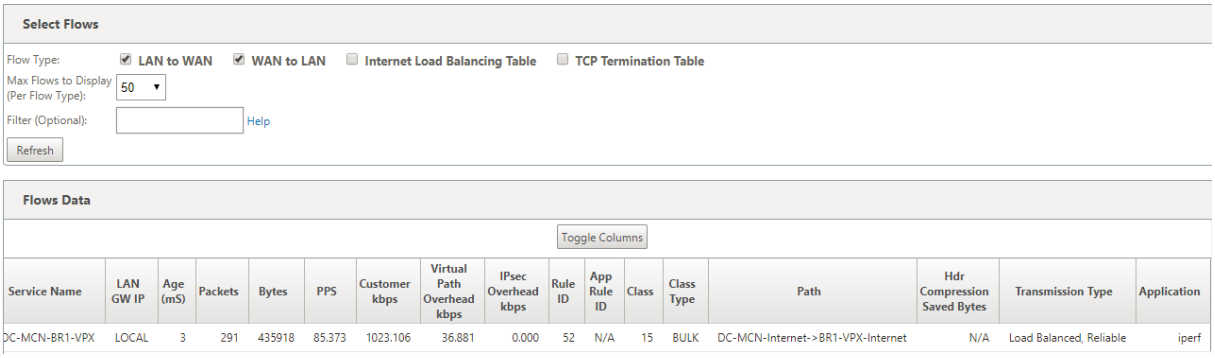
Surveillance des informations de chemin pour le flux de trafic dans l'interface graphique SD-WAN

Il est possible qu'en fonction du débit de trafic entrant exigeant une bande passante, un ou plusieurs chemins soient nécessaires pour traiter le trafic.

Pour déterminer comment le mappage de chemin est effectué, passez en revue les scénarios suivants :

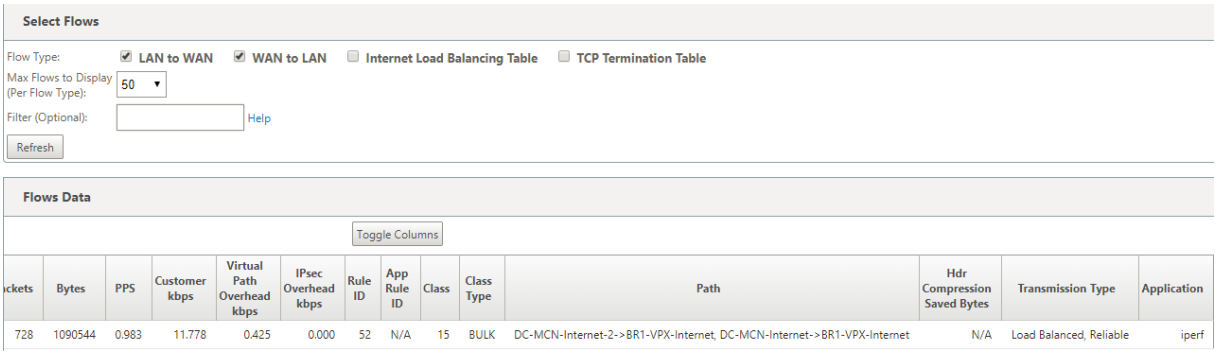
Mode de transmission à charge équilibrée :

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 comme **équilibré de charge.**



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 traitant 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**.

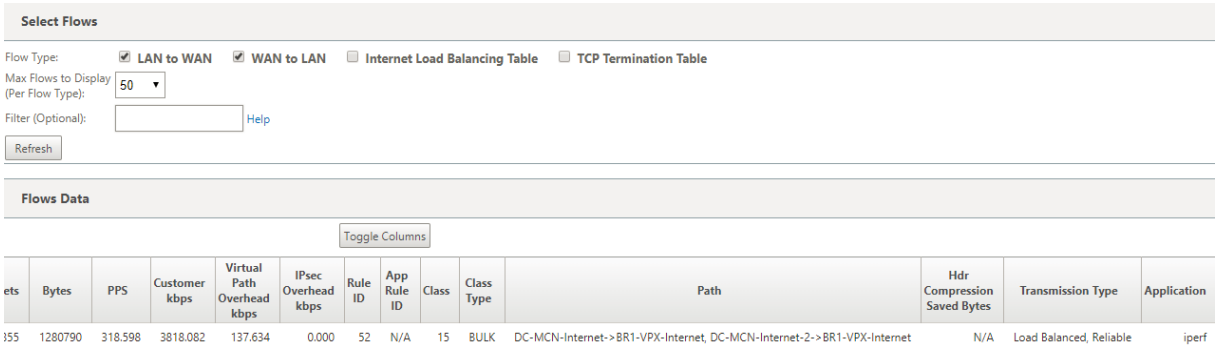
Le dernier meilleur chemin dans cet exemple est un indicateur du chemin qui a servi la connexion plus tôt.



La figure suivante illustre que lorsque le trafic est en cours et que plus d'un chemin est choisi 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 desservent actuellement le trafic sont affichés.

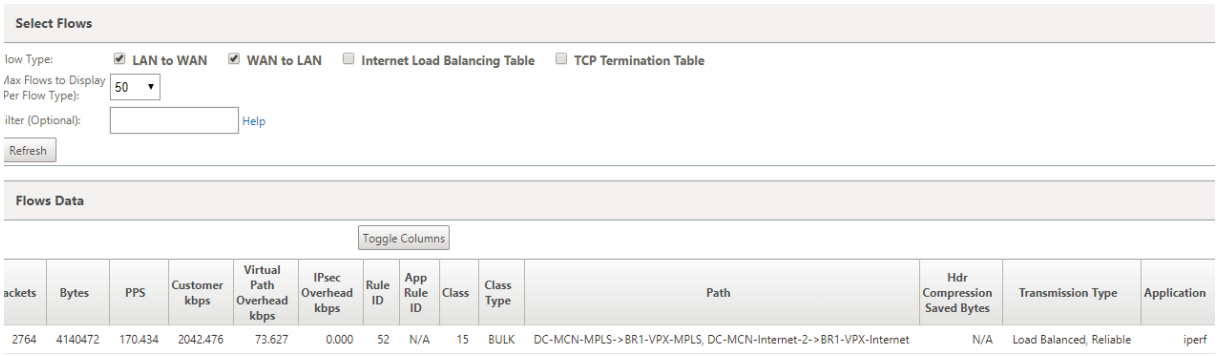
Notez que **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-Internet2->BR1-VPX-Internet** sont les deux chemins affichés dans le tableau **Flows Data** .

> **Remarque**
>
> Comme indiqué, seuls deux chemins maximum dans la table des flux sont affichés.



La figure suivante illustre que lorsque le trafic continue de 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 actuellement choisi apparaîtra en premier dans la section de chemin du tableau **Données de flux** suivi par le dernier meilleur chemin qui dessert le trafic.

Comme le **DC-MCN-Internet->BR1-VPX-Internet** n'était plus le meilleur, un nouveau meilleur chemin actuel a été choisi par le système sous le nom de **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 répondre à la demande de bande passante actuelle du trafic.



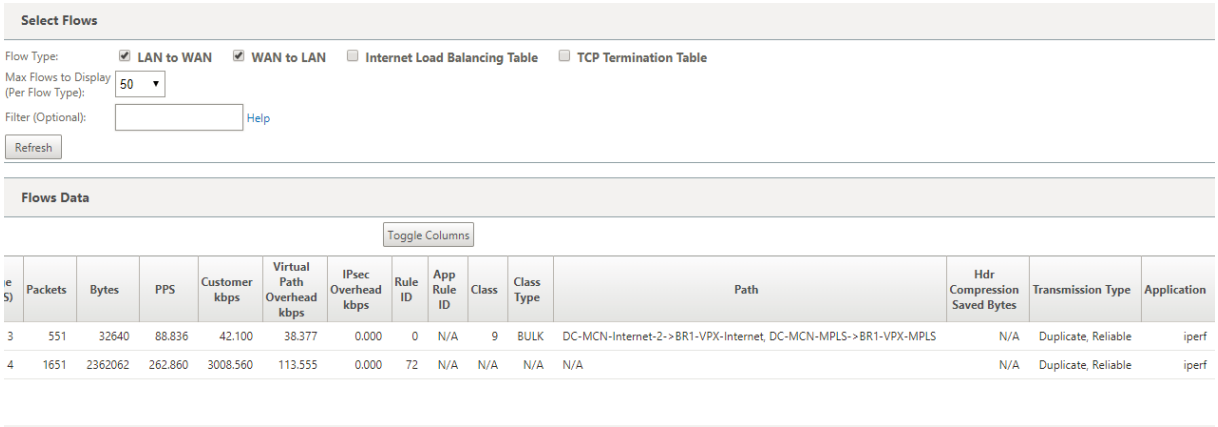
Mode de transmission en double

Le mode général de duplication des paquets garantit que deux chemins sont initialement pris pour le traitement des paquets de la même connexion afin d'assurer une livraison fiable en dupliquant les paquets sur deux chemins distincts.

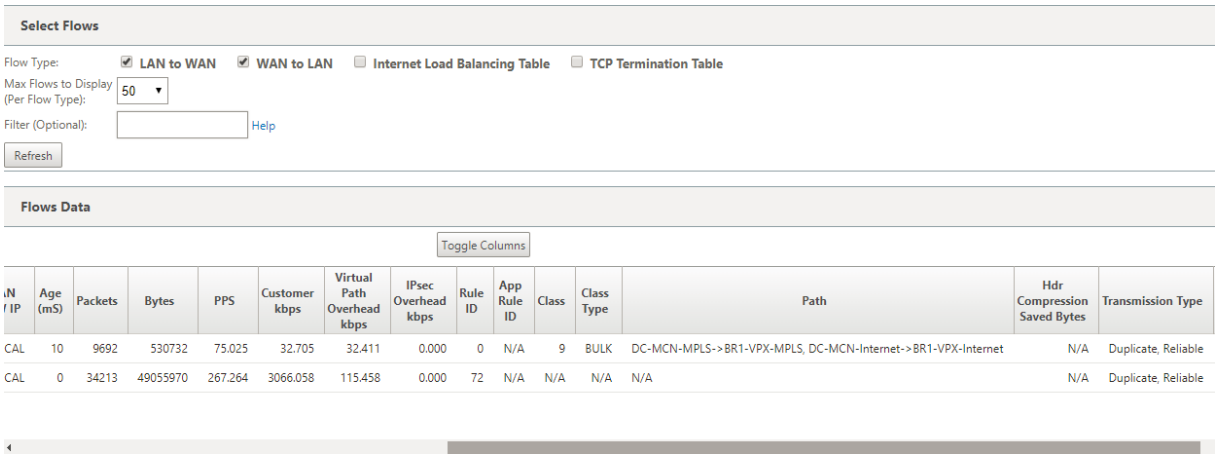
Pour le mappage de chemin, vous remarquez que deux chemins sont pris dans la section chemin de la table de flux tant qu'il existe deux chemins pour traiter les flux par duplication.

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 fourni par un seul chemin, ce mode dupliquera toujours le trafic sur deux chemins pour une livraison fiable des applications.

Vous remarquerez dans la figure ci-dessous, deux chemins dans la section Chemin d'accès de la table **Flows Data** : **DC-MCN-Internet2->BR-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS**.



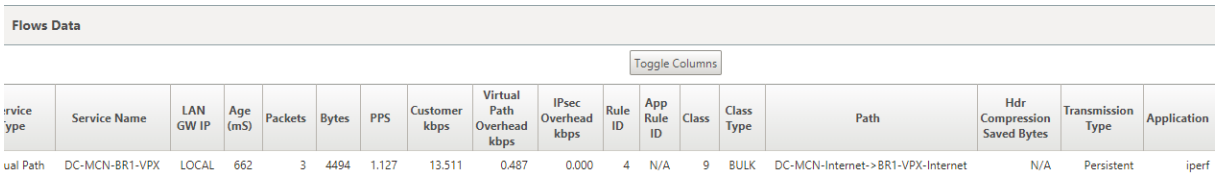
La figure suivante illustre que lorsque le trafic circule, si l'un des meilleurs chemins actuels devient inactif, un autre chemin est choisi et il reste deux chemins dans la section de chemin d'accès dans le tableau **Flows Data** .



Mode de transmission de chemin persistant

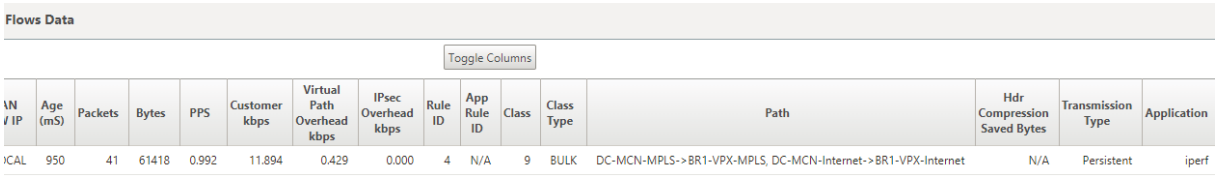
Le mode de transmission de chemin persistant permet de conserver les paquets d'un flux en fonction de l'impédance de latence de chemin.

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. Actuellement, il n'y a qu'un seul meilleur chemin qui est **DC-MCN-Internet->BR1-VPX-Internet.**



La figure suivante illustre que si le chemin **DC-MCN-Internet->BR1-VPX-Internet** devient sujet à latence ou est désactivé, vous remarquez que le nouveau chemin prend effet et que le chemin actuel **DC-MCN-Internet->BR1-VPX-Internet** devient le dernier meilleur chemin.

La nouvelle section de chemin affiche donc **DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet**.

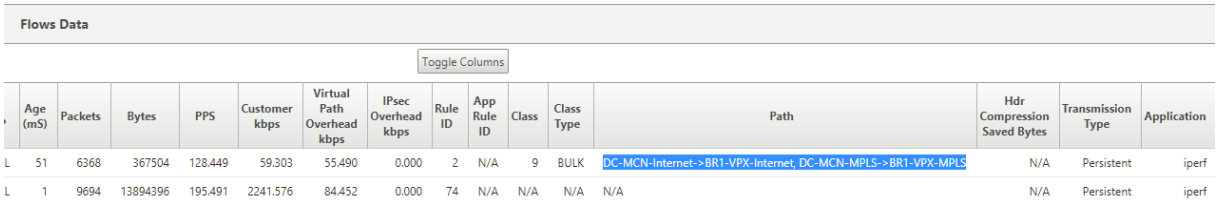

Flows Data

Toggle Columns

N / 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
CAL	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 meilleur et suivant meilleur dans la section chemin de la table de flux depuis le début du flux de trafic.

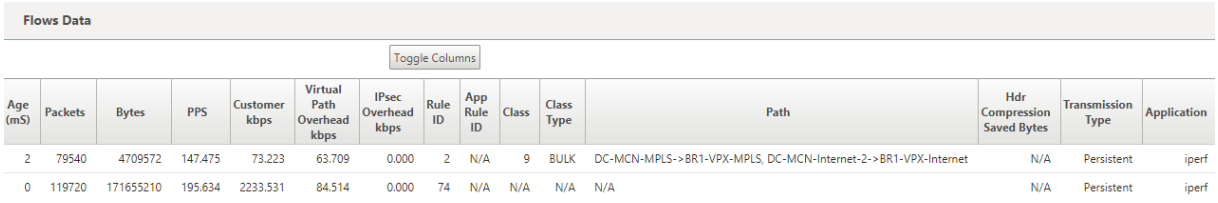
La figure suivante illustre que le flux n'a initialement besoin que de plus de deux chemins et qu'ils restent persistants tant qu'il n'y a pas de croisement d'impédance de latence de chemin (50 ms). Les deux chemins empruntés sont indiqués comme : **DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS.**


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
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
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** passe en latence élevée ou est désactivé. 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 cet instant du 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 IP de gestion

August 31, 2022

Voici les scénarios possibles que vous pouvez 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 plate-forme SD-WAN Standard Edition - appareils physiques et virtuels.

> **Remarque**
>
> Tous les modèles matériels d'appliances SD-WAN sont livrés avec une adresse IP de gestion par défaut d'usine. Assurez-vous de configurer l'adresse IP DHCP requise pour l'appliance au cours du processus d'installation.
>
> Tous les modèles virtuels d'appliances SD-WAN (modèles VPX) et d'appliances qui peuvent être déployés dans un environnement AWS n'ont pas d'adresse IP par défaut attribuée en usine.

Les appareils sont mis sous tension sans serveurs DHCP accessibles :

- Causes :
  - Câble de gestion Ethernet déconnecté
  - Le service DHCP est hors service 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 essaieront de renouveler le bail avant l'expiration de l'adresse
  - Les appliances commencent par 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 sous-réseau DHCP différent
- 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.

Recommandations :

- Affectez toujours un bail permanent pour les adresses DHCP affectées aux appliances Citrix SD-WAN (physique/virtuel). Cela permet aux appliances d'avoir une adresse IP de gestion prévisible.

Notifications HTTP basées sur une session

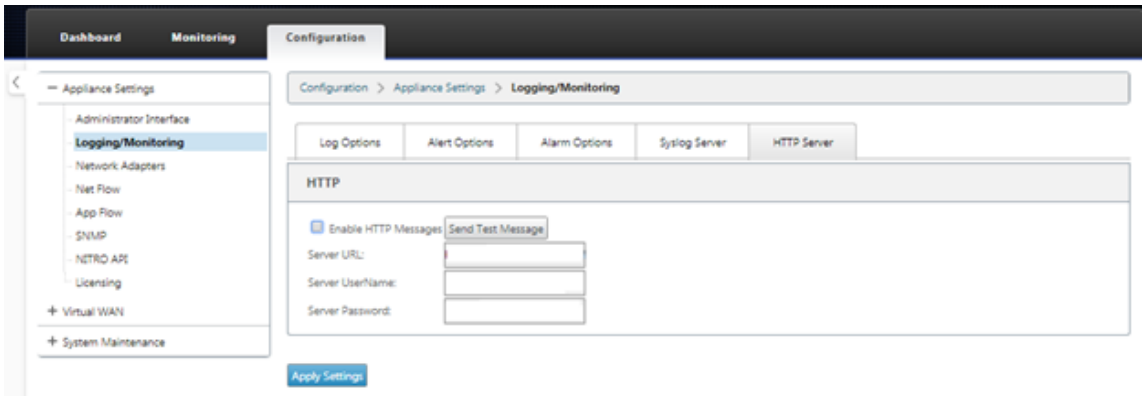
August 31, 2022

Vous pouvez désormais configurer les rapports d'événements et d'alarme pour les demandes de service API HTTP POST génériques dans l'interface graphique de l'appliance Citrix SD-WAN. La configuration de notification d'alarme HTTP et d'événement est similaire aux événements de messagerie et SNMP pour les événements et les alarmes pris en charge dans le SD-WAN.

La notification de publication HTTP basée sur une session est envoyée à un service externe, tel que Service Now. Les notifications d'événement pour le serveur HTTP peuvent être configurées dans l'interface graphique de l'appliance Citrix SD-WAN et Citrix SD-WAN Center.

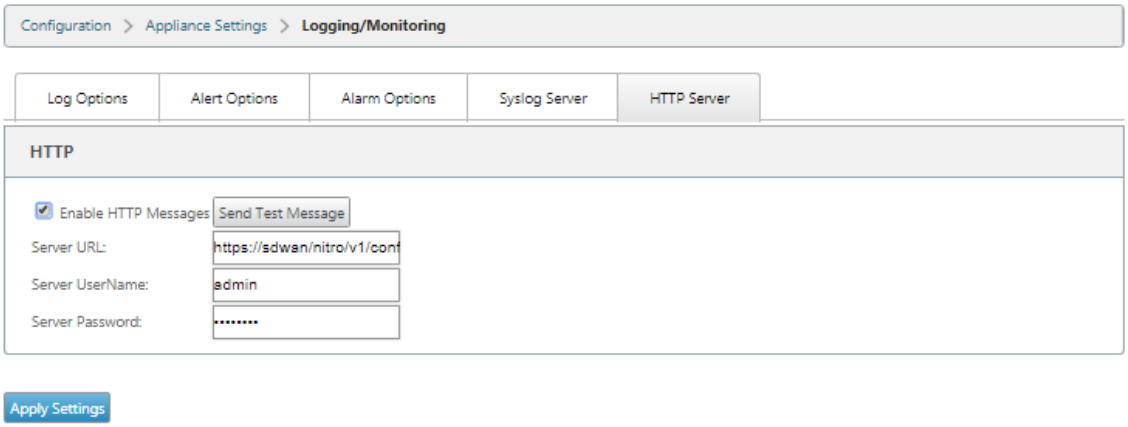
Pour configurer les notifications HTTP POST dans l'interface graphique de l'appliance Citrix SD-WAN :

1. Accédez à **Configuration** > **Journalisation/surveillance** > **Serveur HTTP**.



2. Cliquez sur **Activer les messages HTTP**.

3. Entrez **l'URL** du serveur HTTP dont vous souhaitez recevoir des notifications. Entrez le **nom d'utilisateur** et le **mot de passe du serveur**.

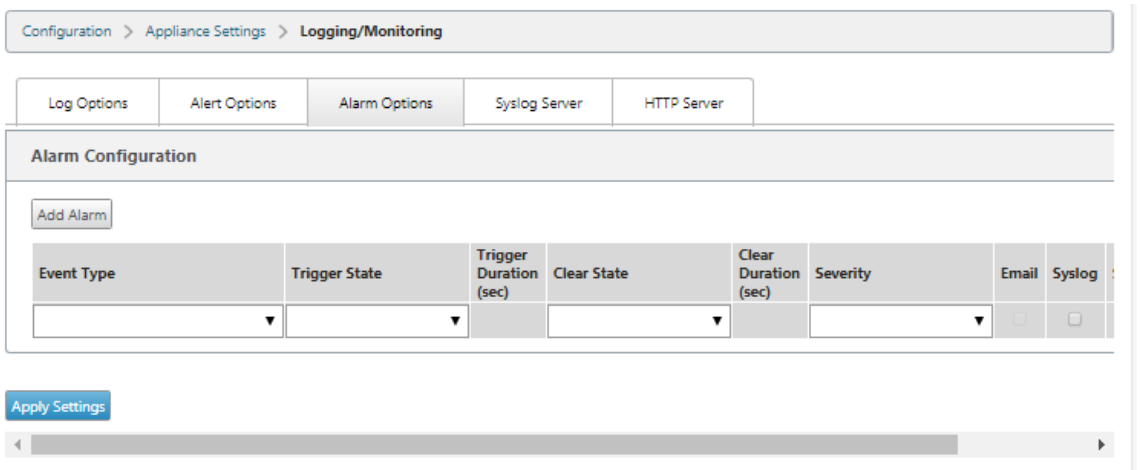


4. Cliquez sur **Appliquer les paramètres**. La page est actualisée après l'application des paramètres de notifications du serveur HTTP.

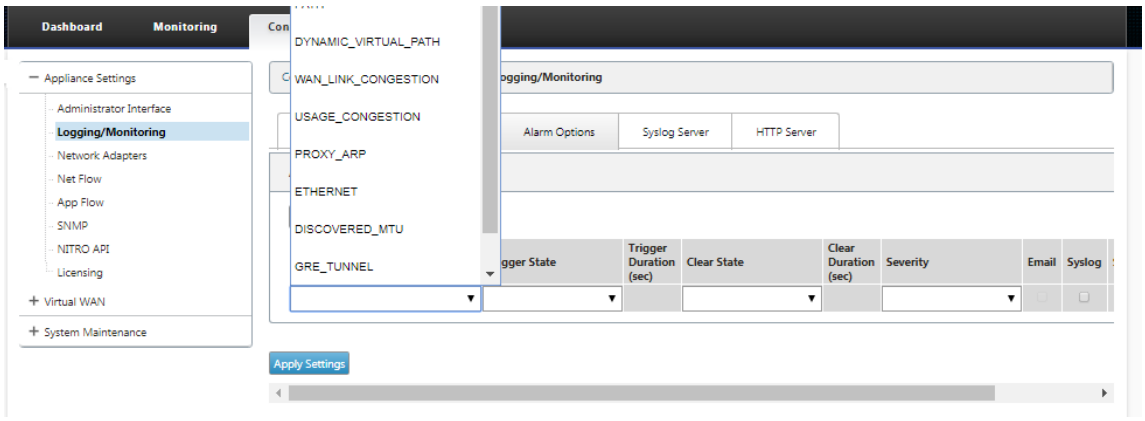
> **Remarque**
>
> Utilisez l'option **Envoyer un message de test** pour vérifier que la connexion au serveur HTTP a réussi.

Pour ajouter une notification d'alarme pour la session du serveur HTTP :

1. Dans la page **Logging/Monitoring**, accédez à l'onglet **Alarm Options (Options d'alarme)**.
2. Cliquez sur **Ajouter une alarme**.

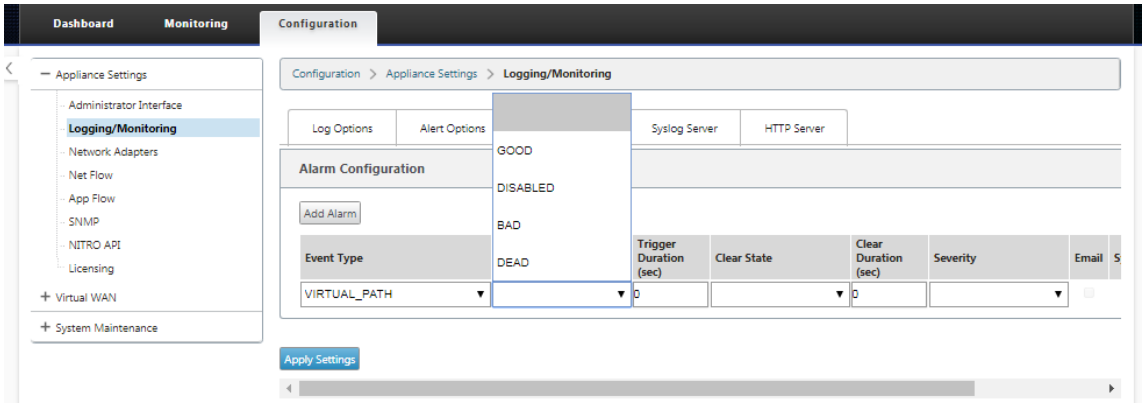


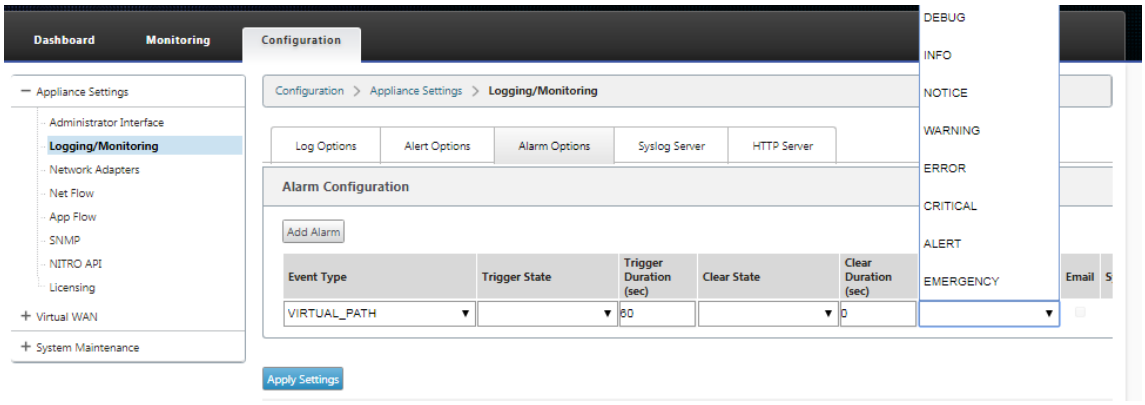
3. Sélectionnez un **type d'événement** dans la liste déroulante.



4. Sélectionnez les états de notification d'alarme suivants pour le **type d'événement**choisi. L'état du déclencheur et l'état d'effacer changent en fonction du type d'événement sélectionné.

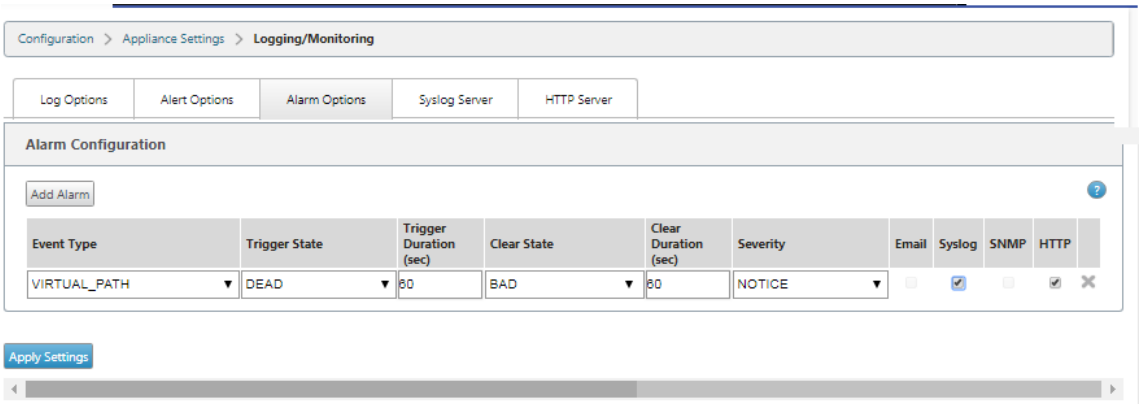
   - État de déclenchement : GOOD, DISABLED, BAD, DEAD
   - Durée de déclenchement : durée en secondes
   - État clair - GOOD, DISABLED, BAD, DEAD
   - Effacer la durée —temps en secondes
   - Gravité : DÉBOGAGE, INFO, AVIS, AVERTISSEMENT, ERREUR, CRITIQUE, ÉVÉNEMENT, URGENCE





5. Cochez les cases **Syslog** et **HTTP** pour recevoir des notifications spécifiques aux événements

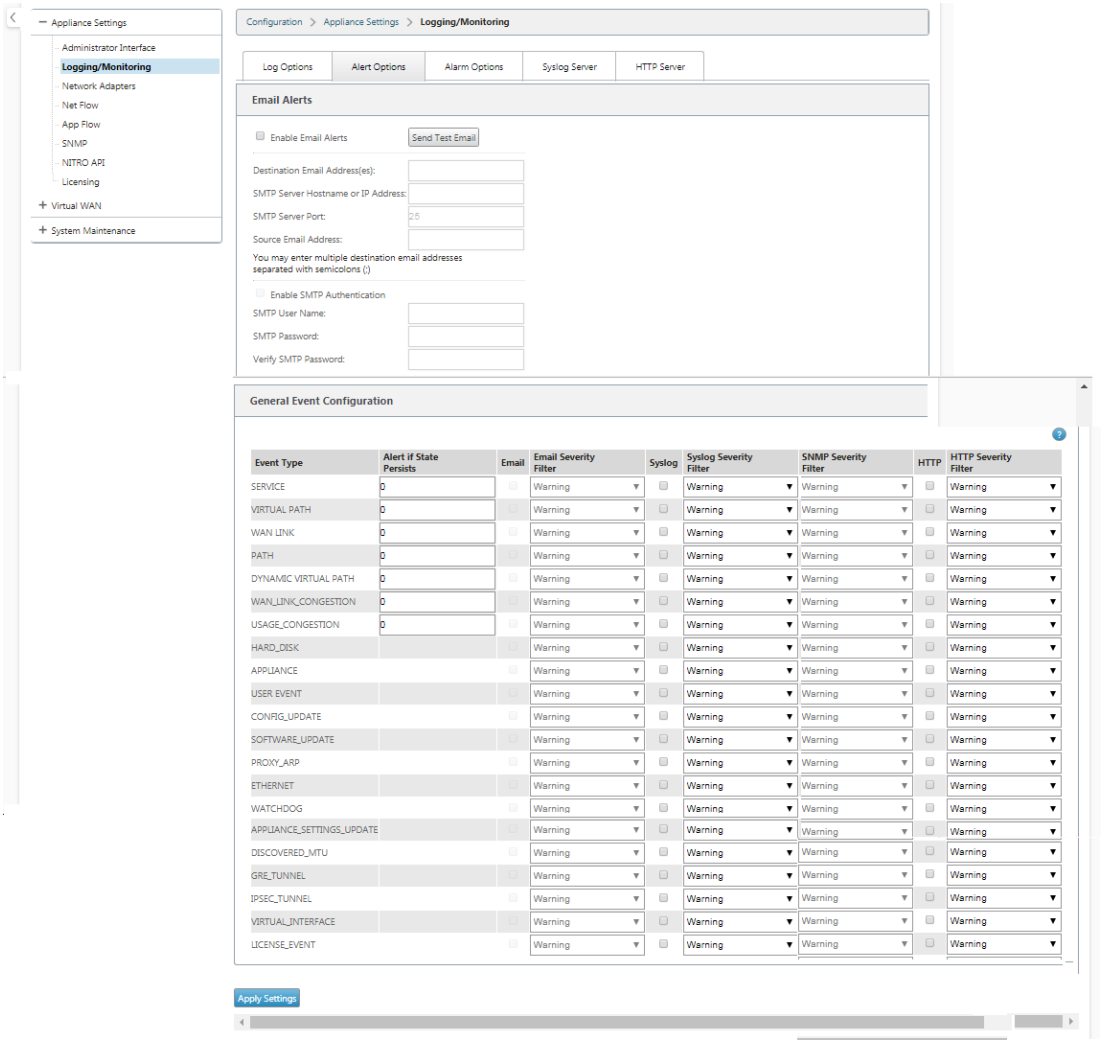
Syslog et HTTP. Cliquez sur **Appliquer les paramètres**.



Pour configurer les options d'événement :

Accédez à 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**.

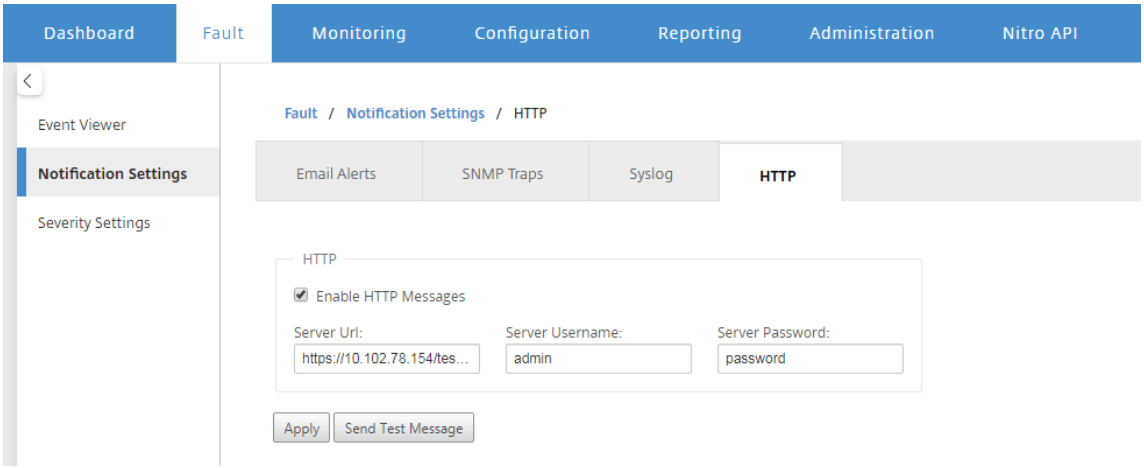
- HTTP
- Filtre de gravité HTTP



Configurer les notifications HTTP dans Citrix SD-WAN Center

Pour configurer les notifications HTTP :

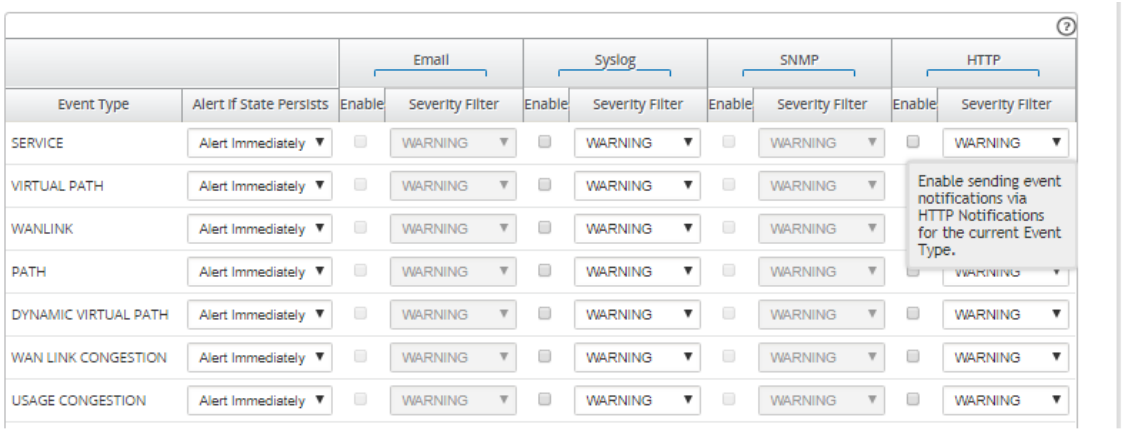
1. Accédez à **Défaut** > **Paramètres de notification** > **HTTP**.



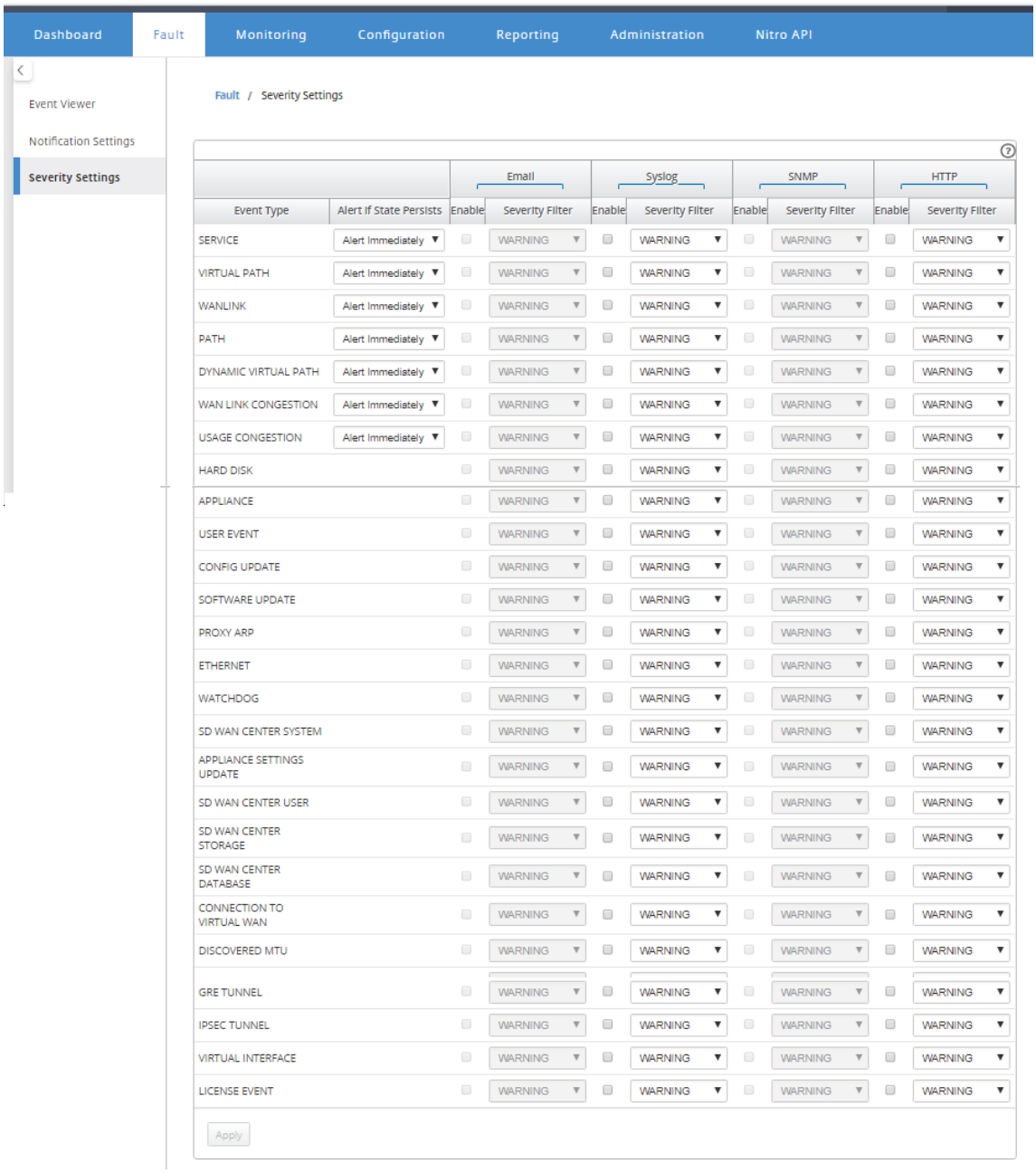
2. Entrez l'**URL du serveur, le nom d'utilisateur duserveur et le mot de passe** du serveur pour le serveur HTTP.
3. Cliquez sur **Appliquer**

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.



2. Vous pouvez choisir de surveiller les notifications d'événements Email, Syslog, SNMP et HTTP pour les types d'événements suivants. Cliquez sur **Appliquer**.



Test de la bande passante active

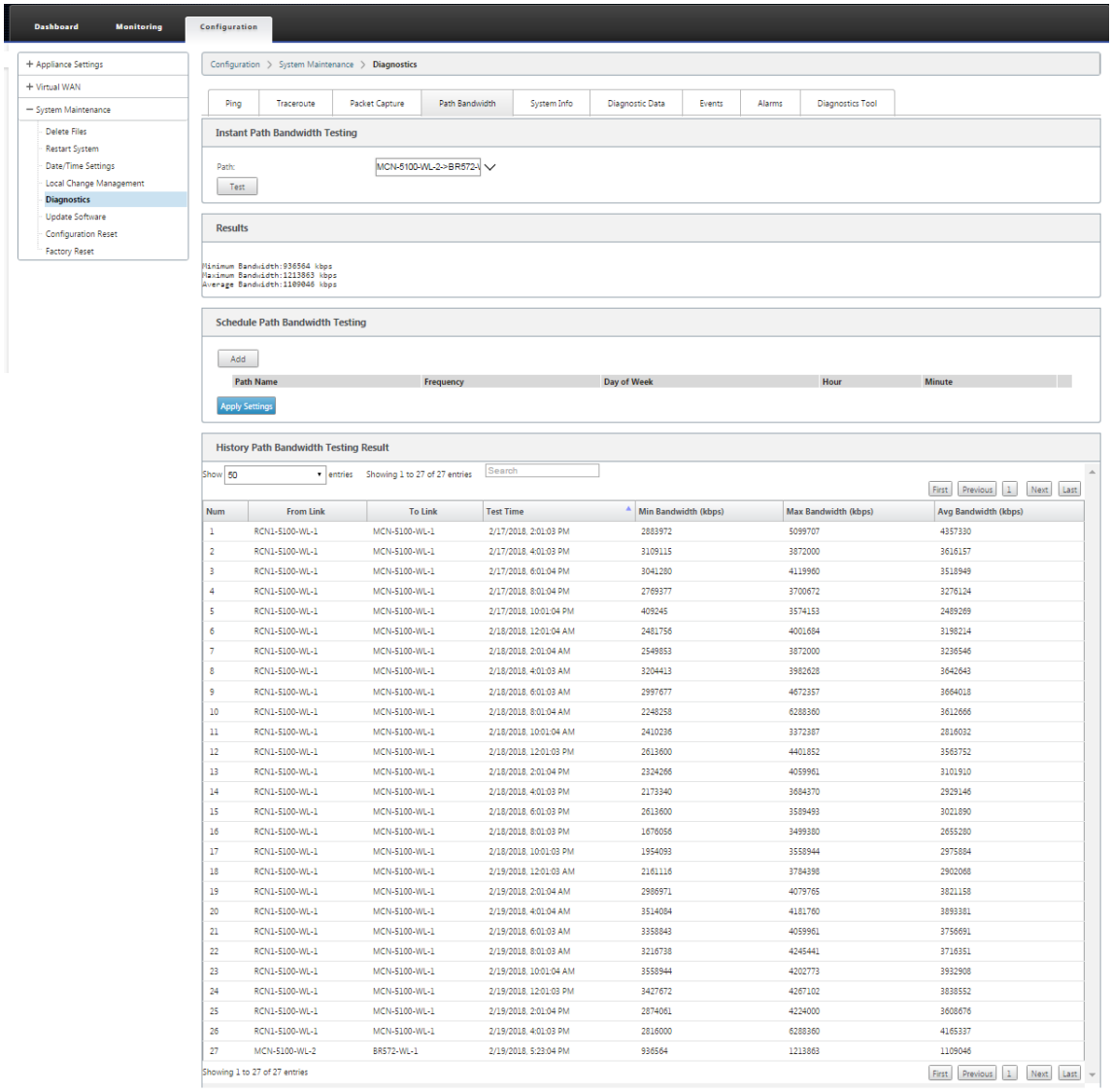
August 31, 2022

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 au cours d'installations nouvelles et existantes, ainsi que pour tester les chemins afin de déterminer le résultat des modifications de configuration 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 :

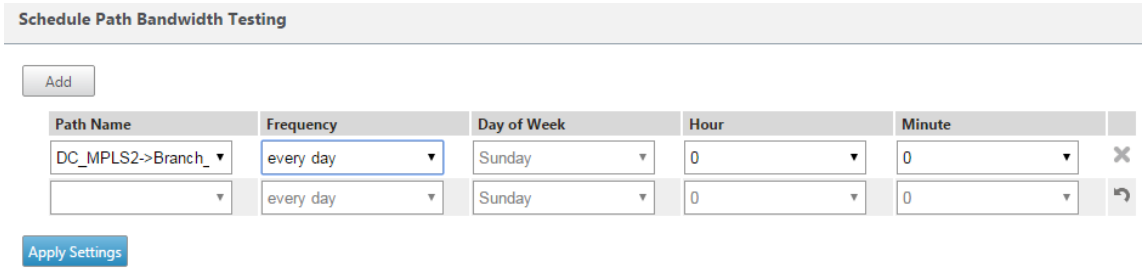
1. Accédez à **Maintenance du système** > **Diagnostics** > **Bande passante du chemin**.
2. Sélectionnez le **chemin** souhaité, puis cliquez sur **Tester**.



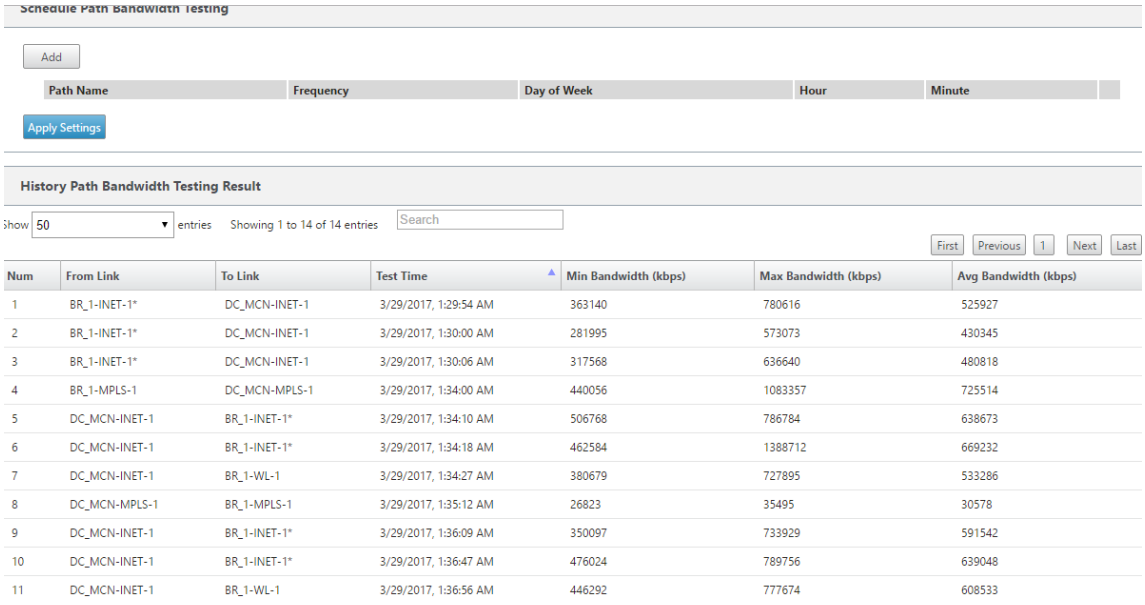
La sortie affiche la bande passante moyenne utilisée comme valeur à définir comme taux autorisé pour les résultats de bande passante minimale et maximale de liaison WAN du test. En plus de la possibilité de tester la bande passante, vous pouvez maintenant modifier le fichier de configuration pour utiliser la bande passante apprise. Pour ce faire, l'option Apprentissage automatique se trouve sous **Site** > [Nom du site] > **Liens WAN**> [Nom du lien WAN] > **Paramètres**

et si elle est activée, le système utilise la bande passante apprise.

Vous pouvez également planifier des tests récurrents de la bande passante de chemin à intervalles hebdomadaires, quotidiens ou horaires.



> **Remarque**
>
> Un historique des résultats des tests de bande passante de chemin est affiché en bas de cette page et les résultats sont archivés tous les sept jours.



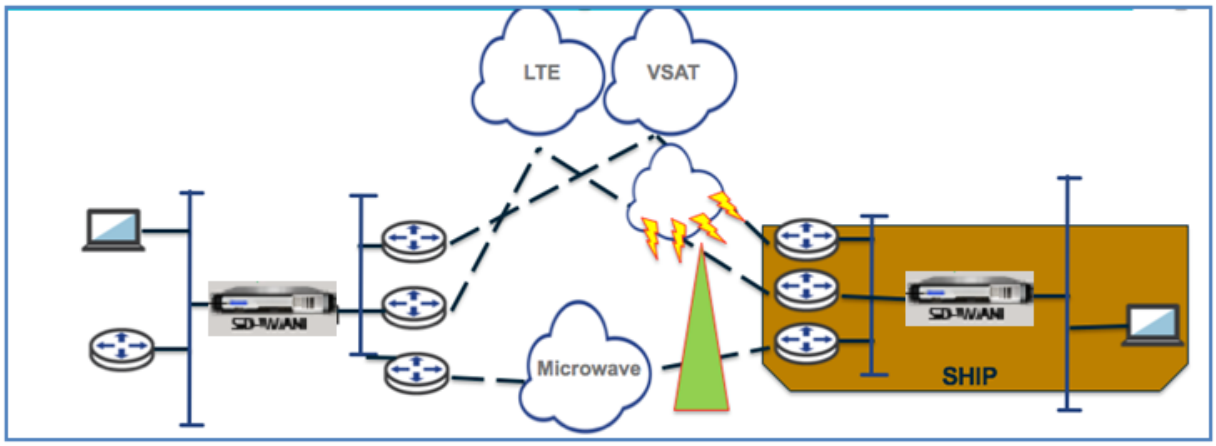
Détection adaptative de la bande passante

November 16, 2022

Cette fonctionnalité est applicable 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'obstruction 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.

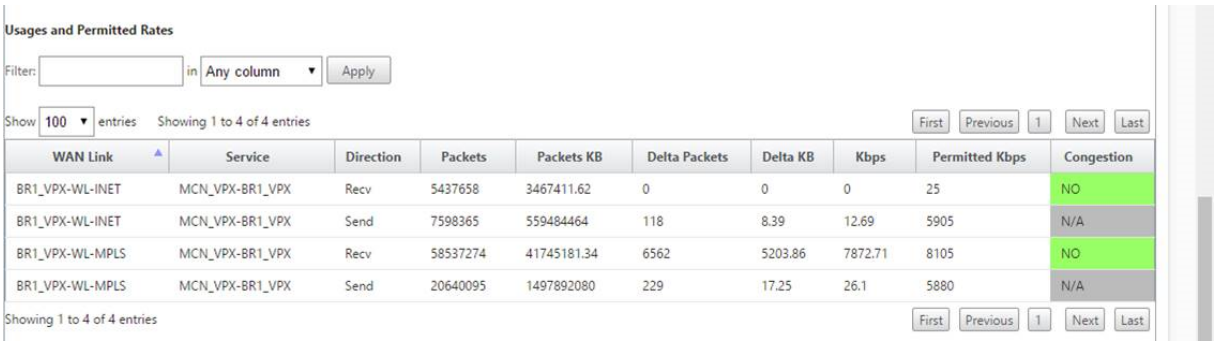
- Plus grande fiabilité de la bande passante (sur VSAT, micro-ondes, 3G/4G et LTE)
- Prévisibilité accrue de la bande passante adaptative par rapport aux paramètres configurés par l'utilisateur



Pour activer la détection de bande passante adaptative :

Cette fonctionnalité nécessite l'option de sensibilité à la perte incorrecte pour être activée (par défaut/personnalisé) comme condition préalable. À partir de la version 11.5 de SD-WAN, vous pouvez l'activer sur le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez Détection adaptative de la bande passante

Consultez le tableau **Utilisation et taux autorisés** en accédant à **Monitor** > **Statistics** > **WAN Link Usage > Usageand PermittedRates**.



Recommandations

August 31, 2022

Les rubriques suivantes présentent les meilleures pratiques à suivre lors de la conception, de la planification et de l'exécution de la solution Citrix SD-WAN sur votre réseau.

Sécurité

August 31, 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 :

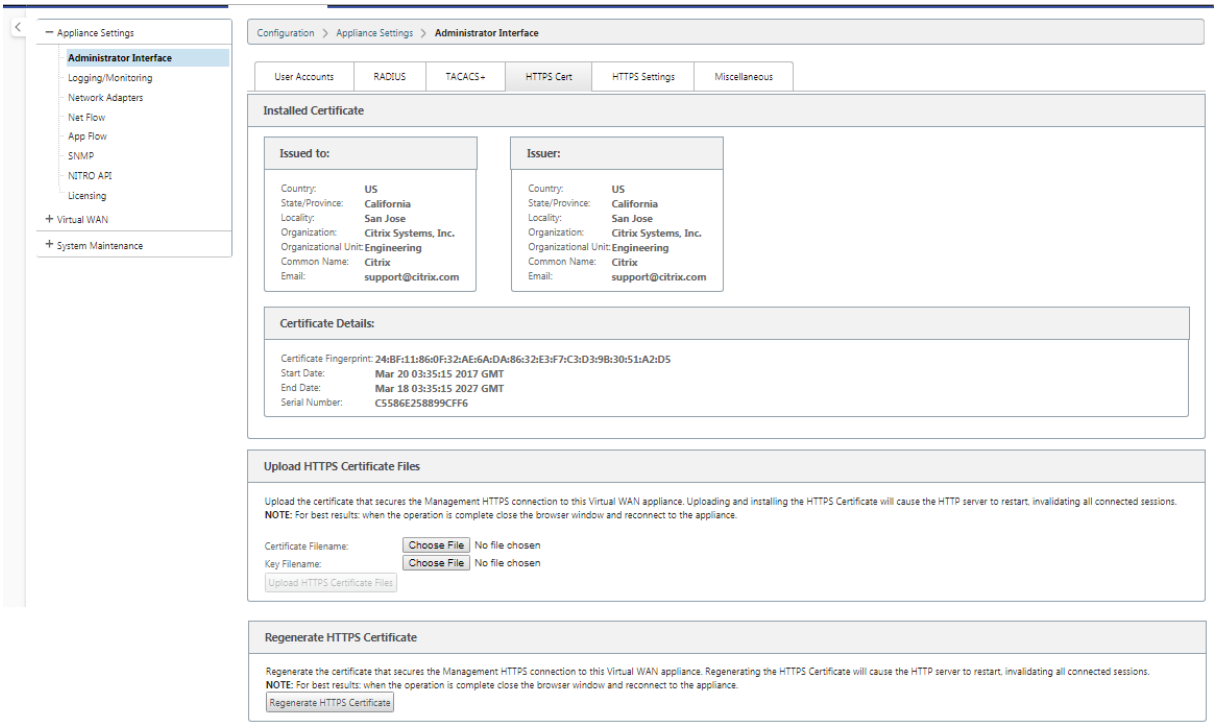
- Modifier le mot de passe utilisateur local
- Gérer les utilisateurs

Certs HTTPS :

- Certificat
- Key

Divers :

- Expiration de la console Web



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 Introduction à 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.

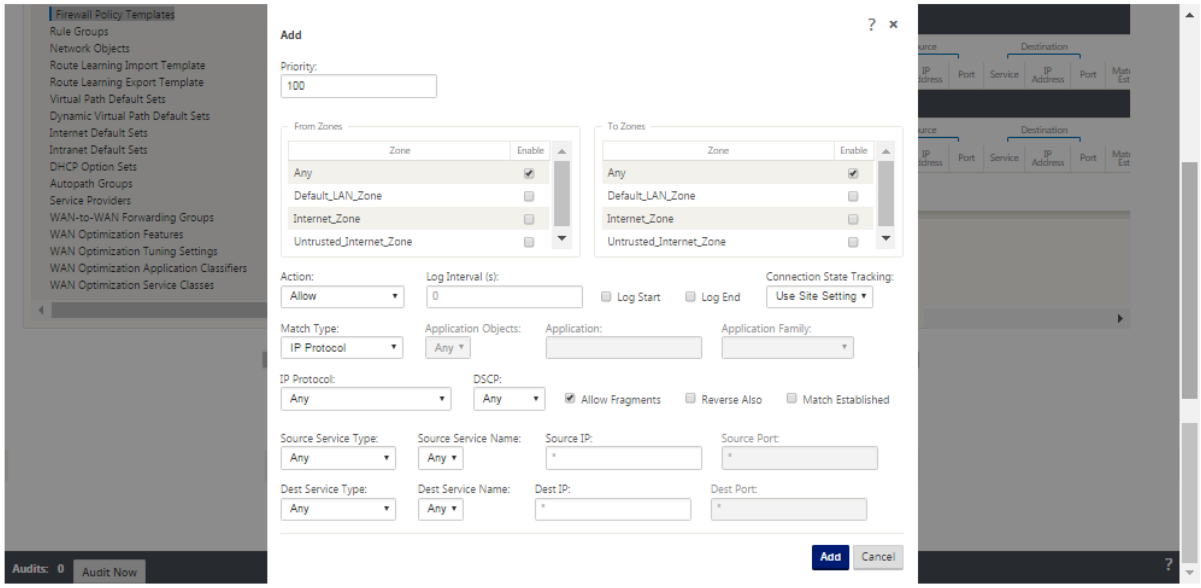
Modèles de pare-feu globaux : les modèles de pare-feu permettent de configurer des paramètres globaux qui ont un impact sur le fonctionnement du pare-feu sur des appliances individuelles fonctionnant dans l'environnement de superposition SD-WAN.

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.

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

August 31, 2022

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, une route **locale** ou une route **relais** est configurée pour atteindre le routeur de passerelle. 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 en tant que route **locale** sur le MCN, elle est apprise par tous les sites SD-WAN de branche et configurée en tant qu'**itinéraire 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

L'ordre de priorité de routage :

- Correspondance des préfixes : la plus longue correspondance des préfixes.
- Service : Local, Service de chemin virtuel, Internet, Intranet, Passthrough
- Coût d'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

August 31, 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

August 31, 2022

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 liens WAN :

- Configurez le débit **autorisé et le débit physique** en tant que bande passante réelle de la liaison WAN. Dans les cas où la totalité de la capacité de liaison WAN n'est pas censée être utilisée par l'appliance SD-WAN, modifiez le débit **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 fonction 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 liens 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 de diagnostic** pour vérifier l'état et la capacité du lien.
- Si le SD-WAN est déployé en mode à **bras unique**, veillez à ne pas dépasser la capacité physique du lien sous-jacent.

Vérification de l'intégrité du lien FAI

Pour les nouveaux déploiements, antérieurs au déploiement SD-WAN et lors de l'ajout d'un lien ISP 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 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 ne dispose pas d'une visibilité complète sur l'utilisation des liens, il est possible que SD-WAN suralloue le lien, 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 branches et les services WAN (chemin virtuel/Internet/Intranet) reçoivent une part égale de la bande passante.
- Les sites de provisionnement doivent être modifiés lorsqu'il y a une grande disparité en termes d'exigence de bande passante ou de disponibilité entre les sites de connexion.
- Lorsque des chemins virtuels dynamiques sont activés entre des sites disponibles maximum, la capacité de liaison WAN est partagée entre le chemin virtuel statique vers le contrôleur de domaine et les chemins virtuels dynamiques.

FAQ

August 31, 2022

Haute disponibilité

Quelle est la différence entre l'appliance 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 High Availability sont configurées au sein du même site ou du même emplacement géographique. Une appliance de succursale située dans un emplacement géographique différent est configurée en tant qu'appliance secondaire (Geo) MCN/RCN.
- Les appareils primaires et secondaires à 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 High Availability and Secondary (Geo), en cas de défaillance de l'appliance, la solution haute disponibilité secondaire 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.
- Dans la haute disponibilité, le basculement principal/secondaire se produit instantanément ou dans les 10 à 12 secondes selon le déploiement de haute disponibilité. Le basculement MCN/RCN principal vers secondaire (Geo) MCN/RCN se produit après 15 secondes après que le primaire soit inactif.

- La configuration de haute disponibilité vous permet de configurer la remise en état 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 le délai de mise en attente expire.

Mise à niveau en une étape

> **Remarque**
>
> Les composants WANOP, SVM et XenServer Supplemental/HFS sont considérés comme des composants du système d'exploitation.

Dois-je utiliser *.tar.gz* ou le package *.zip* de mise à niveau en une seule étape pour mettre à niveau vers la version 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/préparer les packages logiciels des composants du système d'exploitation. Après l'activation, le MCN transférer/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 simple étape (fichier .zip) faire, je dois effectuer.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 elle est installée conformément aux 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 passer d'une version antérieure à la version 9.3 à la version 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 Gestion des modifications, le système renvoie une erreur indiquant que le package n'est pas reconnu. Par conséquent, commencez par mettre à niveau le logiciel SD-WAN vers la version 9.3 ou supérieure, puis effectuez la gestion des modifications à l'aide de la. paquet*zip* .

Comment les composants du système d'exploitation seront-ils installés via la mise à niveau en une seule étape, si.La mise à niveau de*upg* n'est pas effectuée ?

Le MCN transférera ou transfère les packages logiciels des composants du système d'exploitation en fonction du modèle d'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/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'appliance a reçu tous les packages nécessaires au site, même lorsque la valeur de la **fenêtre de maintenance** est définie sur « **0** ».

Quelle est l'utilisation de la planification de l'installation ? 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 du logiciel 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 moment différent de la mise à niveau de la version du logiciel VW.

Pourquoi les informations de planification de la page Paramètres de gestion des modifications apparaissent après la date de planification par défaut et qu'est-ce que cela signifie ?

La page **Paramètres de gestion des modifications** affiche les informations de planification par défaut, à savoir *"'start": "2016-05-21 21:20:00,'"'window": 1, "repeat": 1, "unit": "days'"*. Si la date est une date passée, cela signifie que, l'installation planifiée est basée sur l'heure et d'autres paramètres tels que la fenêtre de maintenance, la fenêtre de répétition et l'unité, et non sur la date.

Quelle est la date/heure d'installation par défaut définie sur, est-ce que cela dépend de l'appliance générique ou locale ?

Par défaut, les détails de la planification sont définis sur *'2016-05-21 at 21:20:00 (Maintenance window of 1 hour and repeated every 1 day)'*. Ce détail dépend du site local de l'appliance.

Comment puis-je installer immédiatement les composants du système d'exploitation sans attendre la maintenance ou la fenêtre planifiée ?

Définissez la valeur de la **fenêtre de maintenance** sur « **0** » dans la page **Paramètres de gestion des modifications**, cela 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 effectuer la mise à niveau vers toute version supérieure lorsque la version logicielle actuelle 9.3.x ou supérieure.

Quand les fichiers des composants du système d'exploitation sont-ils transférés/préparés vers les branches ?

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 appliances reçoivent les fichiers des composants du système d'exploitation, dépendent-elles de la plate-forme ou toutes les branches les reçoivent ?

Les appliances basées sur un hyperviseur, telles que **SD-WAN —400, 800, 1000, 2000 SE** et Bare metal **SD-WAN —2100** exécutées sous licence EE recevront les composants du système d'exploitation à mettre à niveau.

Comment fonctionne la planification ?

Par défaut, les détails de planification sont définis comme *2016-05-21 à 21:20:00 (fenêtre de maintenance d'une heure et répétée tous les 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 sera maintenue. fenêtre de **1 heure** et l'installation sera déclenchée/tentée (si un nouveau logiciel est disponible) à **21 h 20** (heure locale de l'appliance) à compter du **2016-05-21**

Comment savoir si les composants du système d'exploitation ont été mis à niveau ?

Dans la colonne **Statut**, vous pouvez voir une coche verte. Lorsque vous passez la survolée, vous pouvez voir le message La **mise à niveau est réussie** .

Comment planifier l'installation des composants du système d'exploitation pour RCN et ses succursales ?

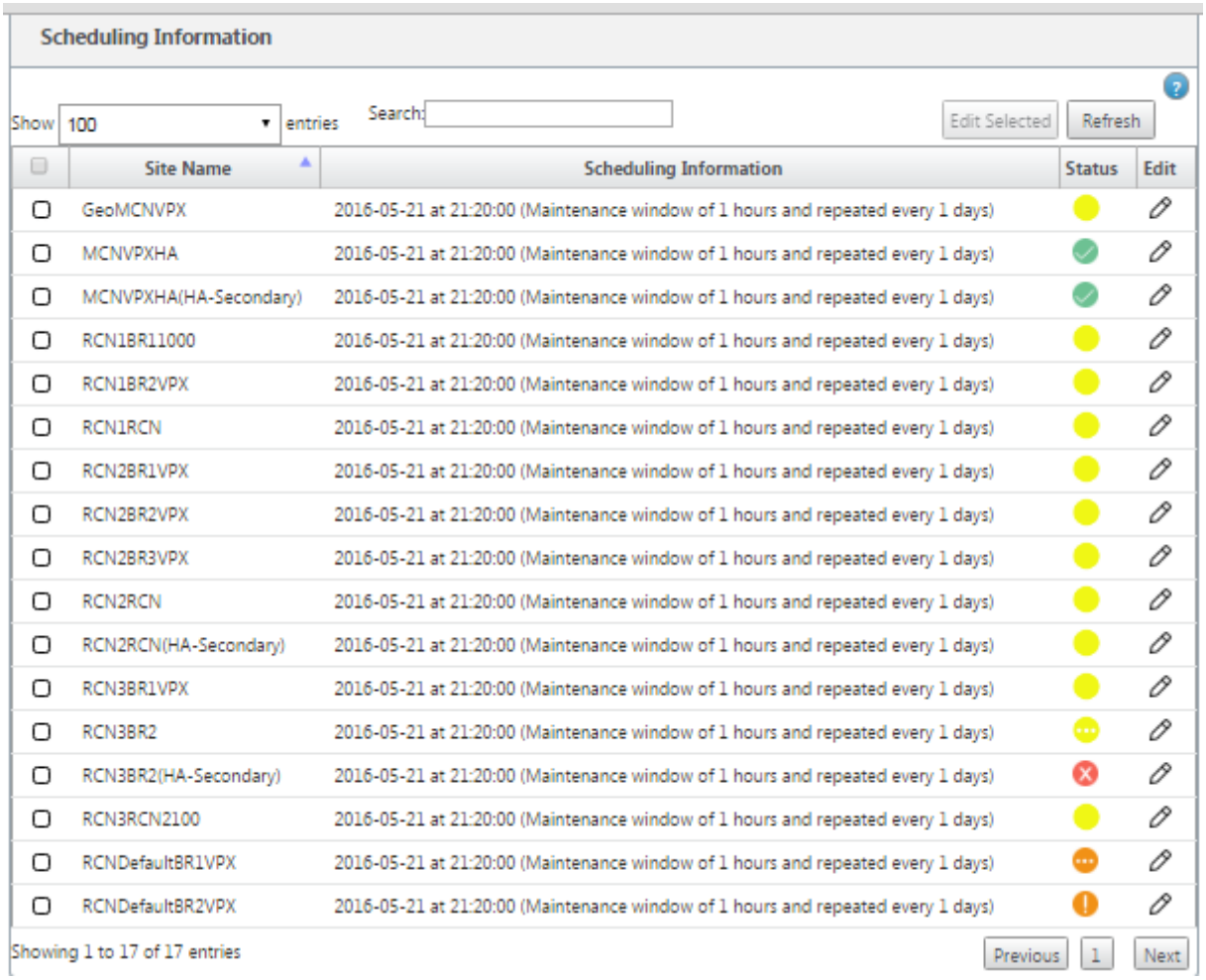
La planification pour RCN est effectuée à partir de la page **Paramètres de gestion des modifications** MCN. Pour les succursales RCN, vous devez vous connecter au RCN respectif et définir les détails de la planification.

D'où puis-je obtenir l'état de l'installation planifiée ?

L'état de l'installation planifiée de RCN peut être obtenu à partir de la page **Paramètres de gestion des modifications** MCN. Pour les succursales RNC, vous devez vous connecter au RNC respectif pour obtenir le statut.

Comment puis-je 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

Show 100 entries Search: Edit Selected Refresh

Site Name	Scheduling Information	Status	Edit
GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
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 une mise à niveau logicielle à l'aide du fichier.*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 actuelles des composants du système d'exploitation ?

Vous ne pouvez désormais 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 obtenir STS pour afficher ces informations.

Quelle différence cela ferait si j'avais des appareils métalliques nus dans mon réseau ? La planification a-t-elle un impact sur les appareils virtuels ou les appareils virtuels ?

Les appliances Bare Metal telles que le **SD-WAN —410,2100,4100,5100 SD-WAN** exécutent unique-

ment le logiciel SD-WAN. Les appareils métalliques nus n'ont pas besoin d'ensembles 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 prendra pas effet pour ces appliances, car aucun composant du système d'exploitation n'a besoin d'être mis à niveau.

Comment le SSU fonctionne-t-il dans un environnement à haute disponibilité ou un déploiement ?

Dans le déploiement à haute disponibilité chez MCN, nous avons une limitation, où le commutateur MCN actif active/bascule le rôle de MCN principal pendant la gestion des changements et le MCN de standby/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 des packages ou vous pouvez revenir au MCN principal en basculant le rôle du MCN actif afin que le MCN principal d'origine puisse prendre le rôle des packages de composants du système d'exploitation à remonter vers d'autres modules. branches.

Comment fonctionne la mise à niveau en une seule étape dans un environnement ou un déploiement haute disponibilité ?

Lors de la mise à niveau en une seule étape dans le déploiement de haute disponibilité, le rôle du MCN principal et du MCN de secours est basculé. C'est une limitation. Dans ce cas, exécutez à nouveau la gestion des modifications avec le package *.zip* sur le MCN actif. Vous pouvez également revenir au MCN principal en basculant le rôle du MCN actif afin que le MCN principal d'origine puisse préparer les packages de composants du système d'exploitation vers les branches.

La mise à niveau en une seule étape prend-elle en charge le déploiement sans intervention pour redémarrer les appliances ?

Oui, il peut être utilisé.

Puis-je utiliser la 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. Seul le dispositif SD-WAN faisant partie du mode deux boîtes sera mis à niveau et non l'appliance autonome WANOP.

Quel paquet dois-je utiliser pour effectuer la mise à niveau vers un réseau multi-niveaux ?

Utilisez le fichier de mise à niveau en une étape *ns-sdw-sw- .zip* <release-version>lorsque la version logicielle actuelle est 9.3.x ou supérieure. MCN s'occupe du paquet de mise en scène pour le progiciel RCN et RCNS à ses succursales respectives.

Après avoir téléchargé le <release-version>fichier *ns-sdw-sw- .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 ne pouvez voir que le modèle de plate-forme MCN sous le logiciel actuel. Les autres packages d'appliance sont listés/affichés/traités lorsque vous cliquez sur le bouton **Vérifier** ou **Stage Appliance** .

Pour les appareils VPX/VPXL/bare metal, quels packages sont préparés pour RCN ?

Le paquet est mis en scène sur les RCN car les branches 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 le stage et passer à l'étape suivante de la gestion des modifications ? Quel impact a-t-il sur les sites qui n'ont pas terminé la mise en scène lorsque ce bouton est sélectionné ?

Oui, vous pouvez cliquer sur **Ignorer les incomplets.** 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 la fin de la préparation pour ce site, afin que les utilisateurs puissent passer à l'étape suivante en ignorant l'état de la phase et en procédant à l'activation. Une fois le site affiché, MCN met en place le package après l'activation terminée.

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 une version plus récente de la version 10.x à partir du MCN et activer la version logicielle préparée à partir de la page **Gestion des modifications locales** sur les sites/branches sélectionnés. Avant d'activer le logiciel de mise en scène sur le site/branche, assurez-vous que la case à cocher est activée à partir du MCN.

- Cette fonction est désactivée par défaut. Le mécanisme de correction existant maintient le réseau en synchronisation. L'utilisateur doit choisir d'autoriser les mises à niveau partielles du site en cochant une case sur 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.

Vous trouverez ci-dessous le cas d'utilisation/scénario dans lequel une mise à niveau partielle du logiciel de site peut être utilisée :

Valider si un correctif logiciel avec les modifications pertinentes est compatible et fonctionne pour un site spécifique (où une 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 le 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 logicielle partielle du 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. Seulement 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 partielle du logiciel en les activant à partir de la configuration ?

Non, la mise à niveau partielle du logiciel nécessite que les configurations actives et mises en scène 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 partielle du logiciel peut être activée ou désactivée à partir du MCN uniquement. Au RCN, la fonction est en mode lecture seule.

Puis-je utiliser la mise à niveau partielle du logiciel lorsque j'ai actif en tant que 9.3.x et 10.0.x comme mis en scène ?

Non, l'appliance doit être exécutée sur la version 10.0 en tant que logiciel actif.

Que se passe-t-il lorsque l'option de mise à niveau logicielle partielle est désactivée depuis MCN, alors que certaines branches sont déjà mises à niveau via cette fonctionnalité ?

MCN envoie une notification à toutes les appliances du réseau que la fonctionnalité de mise à niveau logicielle partielle est désactivée, puis toutes les appliances du réseau sont automatiquement corrigées par MCN pour correspondre à sa version active et intermédiaire. Toutefois, notez que MCN s'attend à ce que l'option Activate Staged soit cliquée sur la page Activation de **Change Management**.

Vous pouvez choisir d'activer le réseau en cliquant sur le bouton **Activer la** préparation ou en cliquant sur **Modifier la préparation** pour annuler l'état en acceptant la confirmation.

Retour arrière 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 fonctionnalité 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 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 Staged est activée. Le logiciel actif est restauré à Staged.

Quels sont les critères pour le redémarrage de la configuration ?

La restauration 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 config/logiciel, si le service Virtual Path est hors service 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 défectueuse est présentée en tant que logiciel Staged.

Comment les utilisateurs sont-ils informés que la reculer s'est produite ?

Une bannière jaune en haut de l'interface graphique indiquant que Config est annulée en raison d' erreurs respectives est affichée. En outre, vous pouvez voir qu'il s'agit d'une table d'état de gestion des modifications. Il affiche **une erreur de configuration ou uneerreur logicielle** correspondant au site pour lequel la fonction de retour en arrière a eu lieu.

Est-ce que la configuration et le logiciel sont 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 retour en arrière dans la section Gestion des modifications. Vous pouvez résoudre le problème sur MCN manuellement.

Pouvons-nous désactiver cette fonctionnalité ?

Oui, nous pouvons désactiver cette fonctionnalité juste avant l'activation. Toutefois, cette fonctionnalité est activée par défaut.

Comment le retour arrière interagit-il avec la mise à niveau partielle du logiciel lorsque j'ai un réseau à plusieurs niveaux ?

- Si la mise à niveau logicielle partielle est désactivée et si un site dans une région (ou le RCN) est annulé, la région avec le problème est annulée et, une fois terminée, la restauration se propage jusqu'au MCN. En conséquence, le MCN et le reste du réseau à rétablir. La RCN de la région qui a été annulée et le MCN affichent la bannière d'annulation que le MCN ne peut pas rejeter automatiquement la bannière d'annulation au niveau de la RCN.
- Si la mise à niveau partielle du logiciel est activée et si un site d'une région (ou le 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 reculera pas lui-même ou le réseau.

Dans ces deux scénarios, le RCN affiche la bannière d'annulation jusqu'à ce qu'elle soit rejetée. Parce qu'elle ne peut pas être rejetée automatiquement par MCN.

Matériel de référence

August 31, 2022

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.