



Citrix SD-WAN 11.2

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

| | |
|---|------------|
| Versionshinweise | 10 |
| Fehlerbehebung bei Citrix SD-WAN 11.0 SE Netzwerkproblemen | 15 |
| Versionshinweise | 16 |
| Versionshinweise | 21 |
| Versionshinweise für Citrix SD-WAN 11.2.3b Version | 24 |
| Neue Benutzeroberfläche für SD-WAN-Appliances | 29 |
| Systemanforderungen | 60 |
| SD-WAN-Plattformmodelle und Softwarepakete | 62 |
| Upgradepfad | 66 |
| Virtuelles WAN-Softwareupgrade auf 9.3.5 mit funktionierender Virtual WAN-Bereitstellung | 67 |
| Upgrade auf 11.2 mit funktionierender Virtual WAN-Bereitstellung | 71 |
| Upgrade auf 11.2 ohne funktionierende virtuelle WAN-Bereitstellung | 78 |
| Reimage der Citrix SD-WAN Appliance-Software | 85 |
| Teilweise Softwareupgrade mit lokalem Änderungsmanagement | 87 |
| WANOP zu Premium Edition Konvertierung mit USB | 90 |
| Standard Edition in Premium Edition umwandeln | 94 |
| USB-Reimage-Dienstprogramm | 95 |
| Citrix SD-WAN -Lizenzoptionen | 98 |
| Lokale Lizenzierung | 100 |
| Remotelizenzierung | 100 |
| Zentrale Lizenzierung | 102 |
| Verwalten von Lizenzen | 106 |
| Lizenzablauf | 107 |

| | |
|---|------------|
| Konfiguration | 108 |
| Erstinstallation | 109 |
| Übersicht über das Layout des Web Interface (UI) | 110 |
| Einrichten der Appliance-Hardware | 117 |
| Konfigurieren der Verwaltungs-IP-Adresse | 118 |
| Datum und Uhrzeit festlegen | 123 |
| Sitzungstimeout | 125 |
| Alarmer konfigurieren | 128 |
| Rollback konfigurieren | 130 |
| Master-Kontrollknoten einrichten | 132 |
| MCN Übersicht | 134 |
| Zur MCN-Konsole wechseln | 134 |
| MCN konfigurieren | 138 |
| Aktivieren und Konfigurieren von Virtual WAN-Sicherheit und Verschlüsselung (optional) | 160 |
| Konfigurieren des sekundären MCN | 162 |
| MCN-Konfiguration verwalten | 164 |
| Einrichten von Zweigknoten | 176 |
| Zweigknoten konfigurieren | 177 |
| Klonen eines Zweigstandorts (optional) | 195 |
| Überwachung der Zweigkonfiguration | 197 |
| Konfigurieren des virtuellen Pfaddienstes zwischen MCN und Clientsites | 197 |
| MCN-Konfiguration bereitstellen | 207 |
| MCN Change Management durchführen | 208 |
| Konfiguration in Zweigen bereitstellen | 209 |

| | |
|--|------------|
| One-Touch-Start | 215 |
| Verbinden der Client-Appliances mit dem Netzwerk | 216 |
| Installieren der SD-WAN-Appliance-Pakete auf den Clients | 217 |
| Bereitstellen von Citrix SD-WAN Standard Edition in OpenStack mit CloudInit | 224 |
| Konfigurieren der LTE-Funktionalität auf 210 SE LTE-Appliance | 233 |
| Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Appliance | 246 |
| Konfigurieren eines externen USB-LTE-Modems | 260 |
| Bereitstellungen | 264 |
| Checkliste und Bereitstellung | 264 |
| Bewährte Methoden | 266 |
| Gateway-Modus | 272 |
| Inlinemodus | 287 |
| Virtueller Inline-Modus | 293 |
| Erstellen eines SD-WAN-Netzwerks | 309 |
| WAN-Optimierung nur mit Premium (Enterprise) Edition | 310 |
| Zwei-Box-Modus | 314 |
| Hohe Verfügbarkeit | 323 |
| Hochverfügbarkeit des Edge-Modus mit Glasfaser-Y-Kabel aktivieren | 332 |
| Keine Berührung | 335 |
| On-Prem Zero-Touch | 357 |
| AWS | 357 |
| Azure | 370 |
| Bereitstellung in einer Region | 390 |
| Bereitstellung in mehreren Regionen | 392 |

| | |
|--|------------|
| Konfigurationshandbuch für Citrix Virtual Apps and Desktops s-Workloads | 396 |
| Domänennamensystem | 410 |
| DHCP-Server und DHCP-Relay | 416 |
| Konfigurieren von DHCP-Server und DHCP-Relay | 417 |
| WAN-Link-IP-Adressen-Lernen über DHCP-Client | 422 |
| Dynamische PAC-Dateianpassung | 426 |
| GRE Tunnel | 430 |
| GRE-Tunnel für den MCN-Standort konfigurieren (optional) | 431 |
| GRE-Tunnel für einen Zweigstandort konfigurieren | 433 |
| In-Band- und Backup-Management | 435 |
| Internetzugriff | 442 |
| Direkter Internetbreakout in Branch mit integrierter Firewall | 444 |
| Direkter Internetzugang mit Secure Web Gateway | 447 |
| Backhaul Internet | 448 |
| Hairpin-Modus | 450 |
| Gehostete Firewalls | 452 |
| Palo Alto Networks Firewall-Integration auf SD-WAN 1100 Plattform | 453 |
| Check Point Firewall-Integration auf SD-WAN 1100 Plattform | 476 |
| Verknüpfungsaggregationsgruppen | 492 |
| Verknüpfen Zustandspropagierung | 495 |
| Mess- und Standby-WAN-Verbindungen | 496 |
| Office 365-Optimierung | 510 |
| Optimierung von Citrix Cloud und Gateway Service | 521 |
| Citrix SD-WAN Orchestrator für die lokale Konfiguration auf der Citrix SD-WAN-Appliance | 526 |

| | |
|--|------------|
| PPPoE-Sitzungen | 535 |
| Qualität der Dienstleistung | 546 |
| Klassen | 546 |
| Regeln nach IP-Adresse und Portnummer | 549 |
| Regeln nach Anwendungsname | 556 |
| Regelgruppen hinzufügen und MOS aktivieren | 563 |
| Anwendungsklassifizierung | 565 |
| QoS Fairness (ROT) | 579 |
| MPLS-Warteschlangen | 582 |
| Berichterstellung | 592 |
| Anwendung QoE | 592 |
| HDX QoE | 596 |
| Mehrere Net Flow Kollektoren | 598 |
| Routenstatistik | 601 |
| Routing | 604 |
| SD-WAN-Überlagerungsrouting | 605 |
| Routingdomäne | 632 |
| Routingdomäne konfigurieren | 633 |
| Routen konfigurieren | 635 |
| Verwenden von CLI für den Zugriff auf Routing | 636 |
| Dynamisches Routing | 637 |
| OSPF | 647 |
| BGP | 657 |
| iBGP | 665 |

| | |
|--|------------|
| eBGP | 665 |
| Anwendungsrouten | 666 |
| Routenfilterung | 671 |
| Routenzusammenfassung | 676 |
| Protokollpräferenz | 679 |
| Multicast-Routing | 680 |
| Routenkosten für virtuelle Pfade konfigurieren | 685 |
| Konfigurieren des Virtual Router-Redundanzprotokolls | 688 |
| Konfigurieren von Netzwerkobjekten | 694 |
| Routing-Unterstützung für die LAN-Segmentierung | 696 |
| Domänendienst für den übergreifenden Routing | 697 |
| Sicheres Peering | 703 |
| Auto Secure Peering an eine PE-Appliance von einer eigenständigen SD-WAN SE und WANOP Appliance am DC-Standort | 705 |
| Auto Secure Peering wurde von der PE-Appliance am DC-Standort und der PE-Appliance des Zweigstellenstandorts initiiert | 710 |
| Auto Secure Peering initiiert von PE-Appliance am DC-Standort und Zweigstelle mit eigenständiger SD-WAN SE und WANOP Appliance | 715 |
| Manuelles Secure Peering von der PE-Appliance am DC-Standort und Branch PE-Appliance initiiert | 720 |
| Manuelles Secure Peering von der PE-Appliance am DC-Standort in Zweigstelle Stand-alone SD-WAN SE und WANOP Appliance initiiert | 723 |
| Domänenbeitritt und Delegieren der Benutzererstellung | 727 |
| Sicherheit | 732 |
| IPsec-Tunnelterminierung | 733 |
| Citrix SD-WAN Integration mit AWS Transit Gateway | 733 |

| | |
|--|------------|
| Konfigurieren von IPsec-Tunneln für virtuelle und dynamische Pfade | 746 |
| Konfigurieren des IPsec-Tunnels zwischen SD-WAN und Drittanbieter-Geräten | 747 |
| Hinzufügen von IKE-Zertifikaten | 756 |
| So zeigen Sie die IPsec-Tunnelkonfiguration an | 756 |
| IPsec-Überwachung und -Protokollierung | 758 |
| Berechtigung für nicht-virtuelle IPsec-Pfadrouten | 761 |
| IPsec-Null-Verschlüsselung | 762 |
| FIPS-Konformität | 763 |
| Secure Web Gateway für Citrix SD-WAN | 767 |
| Zscaler Integration mit GRE-Tunneln und IPsec-Tunneln | 768 |
| Unterstützung der Firewall-Verkehrsumleitung mithilfe von Forcepoint in Citrix SD-WAN | 779 |
| Palo Alto Integration mit IPsec-Tunneln | 783 |
| Stateful Firewall und NAT-Unterstützung | 789 |
| Globale Firewall-Einstellungen | 792 |
| Erweiterte Firewall-Einstellungen | 793 |
| Zonen | 795 |
| Richtlinien | 798 |
| Netzwerkadressübersetzung (NAT) | 804 |
| Statische NAT | 804 |
| Dynamische NAT | 809 |
| Konfigurieren des virtuellen WAN-Dienstes | 816 |
| Konfigurieren der Firewall-Segmentierung | 819 |
| Zertifikatauthentifizierung | 824 |
| AppFlow und IPFIX | 828 |

| | |
|--|------------|
| SNMP | 838 |
| WAN-Optimierung | 842 |
| Citrix SD-WAN Premium Edition | 843 |
| Optimierung aktivieren und Standardeinstellungen konfigurieren | 845 |
| Konfigurieren der Standardoptimierungseinstellungen für die Optimierung | 849 |
| Konfigurieren von Standardanwendungsklassifizierern für die Optimierung | 851 |
| Konfigurieren von Standardserviceklassen für die Optimierung | 854 |
| Konfigurieren der Optimierung für einen Zweigstandort | 860 |
| SSL-Profil konfigurieren | 861 |
| Citrix WAN-Optimierungs-Client-Plug-In | 865 |
| Hardware- und Softwareanforderungen | 866 |
| Funktionsweise des WANOP-Plug-Ins | 867 |
| Bereitstellen von Appliances zur Verwendung mit Plug-Ins | 874 |
| Anpassen der Plug-In-MSI-Datei | 879 |
| Bereitstellen von Plug-Ins auf Windows-Systemen | 886 |
| WANOP-Plug-In-GUI-Befehle | 892 |
| Aktualisieren des WANOP-Plug-Ins | 896 |
| Problembehandlung beim WANOP-Plug-In | 896 |
| SMB 3.1.1 Anschluss | 898 |
| Anleitungen | 900 |
| Schnittstellengruppen | 900 |
| Konfigurieren der Identität virtueller IP-Adresse | 901 |
| Konfigurieren der Zugriffsoberfläche | 902 |
| Virtuelle IP-Adressen konfigurieren | 902 |

| | |
|---|------------|
| GRE Tunnel konfigurieren | 903 |
| Dynamische Pfade für Zweigkommunikation einrichten | 904 |
| Wan-zu-WAN-Weiterleitung | 908 |
| Überwachung und Fehlerbehebung | 908 |
| Virtuelles WAN überwachen | 909 |
| Statistische Informationen anzeigen | 910 |
| Anzeigen von Flussinformationen | 913 |
| Anzeigen von Berichten | 916 |
| Firewall-Statistiken anzeigen | 923 |
| Diagnose | 926 |
| Verbesserte Pfadzuordnung und Bandbreitennutzung | 943 |
| Fehlerbehebung bei Management-IP | 948 |
| Sitzungsbasierte HTTP-Benachrichtigungen | 950 |
| Aktive Bandbreitentests | 956 |
| Adaptive Bandbreitenerkennung | 958 |
| Bewährte Methoden | 960 |
| Sicherheit | 960 |
| Routing | 969 |
| QoS | 970 |
| WAN-Links | 970 |
| Häufig gestellte Fragen | 972 |
| Referenzmaterial | 981 |

Versionshinweise

August 29, 2022

In diesen Versionshinweisen werden neue, behobene Probleme und bekannte Probleme beschrieben, die für die Citrix SD-WAN -Software Release 11, Version 2 für die SD-WAN Standard Edition, WANOP, Premium Edition Appliances und das SD-WAN Center gelten.

Weitere Informationen zu den vorherigen Versionen finden Sie in der [Citrix SD-WAN](#)-Dokumentation.

Was ist neu?

Edge-Sicherheit - Die Citrix SD-WAN Edge Security-Funktion ermöglicht erweiterte Sicherheit auf Citrix SD-WAN SD-WAN-Zweiggeräten. Es vereinfacht das Informationssicherheitsmanagement, indem es einen einzigen Verwaltungs- und Berichtsbereich für **Network Edge Security** bereitstellt. Durch die Konsolidierung von Routing, SD-WAN und Sicherheitsfunktionen auf einer einzigen Appliance entfällt die Notwendigkeit für mehrere Zweigstellen. Dies reduziert die Netzwerkkomplexität, die Betriebskosten und bietet einen sichereren Netzwerkrand. Der Edge-Sicherheits-Stack umfasst die folgenden Sicherheitsfunktionen:

- Web-Filterung
- Anti-Malware
- Intrusion Prevention

Hinweis

Die Edge-Sicherheit wird nur für Citrix SD-WAN-Bereitstellungen unterstützt, die über den Citrix SD-WAN Orchestrator verwaltet werden.

LTE-Netzwerk- und Roaming-Unterstützung - Sie können jetzt das Mobilfunknetz auf Ihren Citrix SD-WAN SD-WAN-Appliances auswählen, die das interne LTE-Modem unterstützen. Die unterstützten Netzwerke sind 3G, 4G oder beides. Die Roaming-Option ist standardmäßig auf Ihren LTE-Appliances aktiviert. Sie können sie deaktivieren.

Weitere Informationen zur LTE-Netzwerk- und Roamingunterstützung finden Sie unter:

- [Konfigurieren der LTE-Funktionalität auf 210 SE LTE-Appliance](#)
- [Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Appliance](#)
- [Benutzeroberfläche für SD-WAN 110-SE Appliance](#)
- [Remote LTE-Standortverwaltung](#)

Neugestaltung der getakteten Verbindung - In Citrix SD-WAN UI wird eine neue Option - **Ungefähre Daten bereits verwendet** im Abschnitt **Metered/Standby Link** hinzugefügt. Um die korrekte getaktete Link-Nutzung zu verfolgen, muss der Benutzer die ungefähre Nutzung auf dem getakteten Link eingeben, wenn der Link bereits seit einigen Tagen im aktuellen Abrechnungszeitraum verwendet wurde. Diese ungefähre Verwendung wird nur für den ersten Zyklus verwendet.

DHCP-Unterstützung am Fail-to-Wire-Port - Die DHCP-Clientfunktion wird jetzt auf Fail-to-Wire-Port für den Zweigstandort mit serieller High Availability (HA) -Bereitstellungen erweitert. Diese Erweiterung:

- Ermöglicht die DHCP-Client-Konfiguration für die nicht vertrauenswürdige Schnittstellengruppe, die Fail-to-Wire-Bridge-Paar- und serielle HA-Bereitstellungen hat.
- Ermöglicht die Auswahl von DHCP-Schnittstellen als Teil von **privaten Intranet-WAN-Verbindungen** zusätzlich zu Internet-WAN-Verbindungen.

Kontrollpunkt-Firewall - Die **Checkpoint Firewall** ist in die SD-WAN 1100 Plattform integriert, um erweiterte Sicherheit für Zweigstellengeräte zu bieten. Die **Checkpoint Firewall** bietet die Firewall-Funktionen der nächsten Generation wie URL-Filter, Antivirus, SSL-Inspektion und Intrusion Prevention. Diese Integration bietet die Möglichkeit, das sichere SD-WAN an den Zweigstellen mithilfe des Citrix SD-WAN Center bereitzustellen, während die Sicherheitsrichtlinien mit der Check Point-Verwaltungsplattform verwaltet werden.

Aktivieren der Paketduplizierung für ICA-Echtzeit - Die Paketduplizierung ist jetzt standardmäßig für den HDX-Echtzeitverkehr aktiviert, wenn Multistream Independent Computing Architecture (ICA) verwendet wird.

Unterstützung von 256 virtuellen Pfaden mit SD-WAN SE in Azure - Früher wurden in Azure 128 virtuelle Pfade unterstützt. Ab Version 11.2 werden 256 virtuelle Pfade mit SD-WAN SE in Azure unterstützt.

Subnet-Unterstützung - Ab Release 11.2 lässt Citrix SD-WAN UI /31-Subnetze zur Konfiguration der Netzwerkadresse zu.

Unterstützung des TLSv1.3-Protokolls in HTTPS und Unterstützung für neue Algorithmen in SSH - Citrix SD-WAN unterstützt jetzt das TLSv1.3-Protokoll bei HTTPS-Zugriff und unterstützt auch neue Algorithmen beim SSH-Zugriff.

Cloud Direct-Unterstützung - Ab Release 11.2 wird der Cloud Direct-Dienst auf SD-WAN 2100, 4100 und 6100 Appliances unterstützt. Sowohl SD-WAN Center als auch Orchestrator ermöglichen die Bereitstellung der Cloud Direct-Dienstfunktion auf SD-WAN 2100, 4100 und 6.100 Appliances. Das SD-WAN Center unterstützt bis zu 250 Mbit/s Abonnementlizenzen für Cloud Direct.

WAN Link Bandbreitenfreigabe bei Inaktivität des Cloud Direct-Dienstes - Eine WAN-Link-Bandbreite muss nicht mehr ausschließlich für den Cloud Direct-Dienst reserviert werden. Wenn der Cloud Direct-Dienst nicht aktiv ist, können die anderen Dienste wie virtuelle Pfad-, Internet- oder Intranetdienste,

die auf dieser WAN-Verbindung konfiguriert sind, die Bandbreite gemäß den konfigurierten Freigaben verwenden.

Behobene Probleme

SDWANHELP-1098: Die Benutzeroberfläche von Citrix SD-WAN Optimization Rules stürzt ab, nachdem sie einen seiner Regelnamen mit doppelten Anführungszeichen hinzugefügt oder geändert hat. Dies gilt für **Anwendungsklassifizierer, Links, Serviceklassen und Traffic Shaping-Richtlinien**.

SDWANHELP-1159: Citrix SD-WAN wirbt nicht für die Routen zum OSPF-Nachbarn an. Dies geschieht, wenn die Routen in der SD-WAN-Appliance geändert werden oder virtuelle Pfade klappen passiert, wodurch virtuelle WAN-Routen über die Standorte neu synchronisiert werden. In diesem Fall kann die SD-WAN-Appliance in einen Zustand eintreten, wenn die Verbindung zum OSPF-Peer verlustbehaftet ist, in dem sie niemals die SD-WAN-Routen zum OSPF-Nachbarn ankündigt.

SDWANHELP-1169: Der SD-WAN-Dienst wird abgebrochen, wenn ein Paket für die Übertragung eines DVP geplant ist, für das noch nicht entfernt werden soll. Die Software versucht fälschlicherweise, es aus einer leeren Paketliste zu entfernen.

SDWANHELP-1189: Während des Software-Appliance-Upgrades kann der Installationsprozess auf den SD-WAN 210 Standard Edition-Appliances (SE) fehlschlagen. Um mit dem Upgrade fortzufahren, muss die Appliance neu gestartet werden.

SDWANHELP-1222: Wenn die Verbindungsverfolgung auf einer SD-WAN-Appliance aktiviert ist, kann eine bestimmte Kombination von IP-Adressen, Paketlänge und IP-Protokoll einen Fehler bei der Prüfsummenvalidierung verursachen. Daher werden die UDP- oder TCP-Pakete unangemessen gelöscht.

SDWANHELP-1241: In einigen Fällen werden Appliance-Informationen auf der Seite **Inventar** und **Status** des SD-WAN Centers aufgrund des Absturzes des SD-WAN Center-Dienstes nicht angezeigt.

SDWANHELP-1248: In wenigen Fällen kann der SD-WAN-Dienst während der Verarbeitung der IGMP-Pakete (Internet Group Management Protocol) in Konfigurationen mit mehreren Routingdomänen abgebrochen werden.

SDWANHELP-1253: Die Citrix SD-WAN Appliance kann den Internetverkehr in Konfigurationen mit mehreren Routingdomänen senken.

SDWANHELP-1256: Während eines Konfigurationsupdates in einer SD-WAN-Appliance, wenn ein Zweig alle Routingdomäne entfernt, schlägt die Network Address Translation (NAT) möglicherweise für den Internetverkehr fehl.

SDWANHELP-1276: Beim Klonen einer Site im Citrix SD-WAN Center werden die Zugriffsschnittstellen nicht richtig geklont. Die IP-Adressen bleiben identisch mit der ursprünglichen Site, auch wenn die Änderung während des Klonens durchgeführt wurde.

SDWANHELP-1284: Wenn Citrix SD-WAN BGP aktiviert hat, war es nicht erlaubt, BGP-Pakete, die von anderen Peers stammen und die für andere Peers bestimmt waren, den virtuellen Pfad zu anderen Sites zu übergehen.

SDWANHELP-1385: Die Seriennummer des SD-WAN-Geräts gehen möglicherweise aufgrund eines Problems in der BIOS-Firmware v1.0b auf der SD-WAN 210-Plattform auf der SD-WAN 210-Plattform auf der Standardzeichenfolge zurück.

NSSDW-21808: Die bereitgestellten Appliance-Informationen im SD-WAN Center werden gelöscht, bevor der eigentliche Aufheben der Bereitstellung auf der Appliance abgeschlossen wird. Wenn während der Aufhebung der Bereitstellung ein Fehler aufgetreten ist, können Sie keine Palo Alto spezifischen Vorgänge auf der Appliance vom SD-WAN Center aus ausführen.

NSSDW-25440: Bei Instanzen mit aktivierter Netzwerkbeschleunigung können in Azure erhebliche Paketverluste oder Netzwerkverzögerungen beobachtet werden.

NSSDW-27341: In Citrix SD-WAN Center können Sie die Konfiguration für die Benachrichtigungseinstellungen nicht durchführen, die E-Mail-Warnungen, SNMP-Traps, Syslog und HTTP sind.

NSSDW-27530: In Citrix SD-WAN kann das Ändern der IP-Adresse der Zugriffsschnittstelle für einen WAN-Link die Pfade verringern, die mit dem WAN Link verknüpft sind.

NSSDW-28146: Wenn die Citrix SD-WAN 11.2.0-Version einmal von der Version 10.2 aktualisiert oder auf Version 10.2 heruntergestuft wird, wird sie auf 11.0/11.1-Releases aktualisiert, schlägt ein erneuter Herunterstufen auf die Version 10.2 fehl.

Ebenso wurde nach dem Upgrade von Citrix SD-WAN Center von Version 10.2 auf Version 11.2.0 das Downgrade von SD-WAN Center von 11.2.0 auf Version 10.2 nicht unterstützt.

NSSDW-28971: Sobald Sie sich bei den SD-WAN-Appliances und virtuellen Maschinen angemeldet haben, erhalten Sie möglicherweise Root-Shell-Zugriff mit dem 11.x-basierten Image mit einem fest codierten Kennwort. Die betroffenen SD-WAN-Plattformen sind 110 und VPXs mit 11.x-Images bereitgestellt. Dies ist ein CLI-bezogenes Problem und gilt nicht für die GUI.

Bekannte Probleme

NSSDW-23558: Citrix SD-WAN Edge Security ist nicht mit den Funktionen Cloud Direct und Cloud Security interoperabel.

NSSDW-25452: Die Citrix SD-WAN Orchestrator-Benutzeroberfläche und der Citrix SD-WAN-Konfigurations-Compiler lassen den zulässigen Bereich des DHCP-Leasingintervalls nicht erkennen, wodurch der DHCP-Daemon ausfällt.

- **Problemumgehung** - Geben Sie an, dass die gültige Leasingzeit für DHCP 300—86400 Sek.

NSSDW-27105: Das Data Plane Development Kit (DPDK) ist jedes Mal abgestürzt, wenn einer der Ports während des Durchgangs des Datenverkehrs heruntergefahren wird. Zu diesem Zeitpunkt stürzt DPDK ab, der SD-WAN-Dienst wird neu gestartet und der virtuelle Pfad ist tot. Nach ein paar Minuten kommt der Virtual Path automatisch **auf**.

NSSDW - 27139: Citrix SD-WAN Edge Security ist nicht mit der WANOP-Funktion interoperabel.

NSSDW-27587: Eine Datenträger-Warnmeldung wird auf der SD-WAN VPX Appliance als MCN mit dem standardmäßigen 40 GB Speicherplatz angezeigt.

- **Problemumgehung** —Es wird empfohlen, 120/240 GB virtuelle Datenträger für den SD-WAN MCN VPX mit Unterstützung für bis zu 128/256 virtuelle Pfade zu verwenden.

NSSDW-27719: Der konvertierbare Managementport kann nicht für VPX verwendet werden, die auf Hypervisoren bereitgestellt werden, die den IXGBEVF-Treiber verwenden. Dies kann zu kritischen Softwarefehlern führen und der Dienst deaktiviert wird.

NSSDW-27727: Netzwerke mit VPX und VPXL-Instanz, die den IXGBEVF-Treiber verwenden, die für bestimmte Intel 10-GB-NICs verwendet werden, wenn SR-IOV aktiviert ist, dürfen nicht auf 11.2.0 aktualisiert werden. Dies kann zu einem Verlust der Konnektivität führen. Dieses Problem wirkt sich bekanntermaßen auf AWS-Instanzen mit aktiviertem SR-IOV aus.

NSSDW-27817: Die Webfilterfunktion von Citrix SD-WAN Edge Security schließt standardmäßig die TCP-Verbindung, wenn der Benutzer versucht, auf blockierte Websites zuzugreifen, wenn das HTTPS-Protokoll verwendet, anstatt den Benutzer auf eine informative Webseite mit Details zur blockierenden Anfrage umzuleiten.

NSSDW-27847: Überlappende IP-Adressen in verschiedenen Routingdomänen werden von Citrix SD-WAN Edge Security nicht unterstützt. Die Sitzungsprotokollmeldungen enthalten auch keine Routingdomäneninformationen.

NSSDW-27850: Citrix SD-WAN Anti-Malware-Engine leitet den Benutzer auf eine nicht routbare IP-Adresse um, wenn er einen Virus auf einer HTTP-Webseite erkennt. Infolgedessen reagiert der Endbenutzer-Browser nicht mehr, während er versucht, ihn abzurufen, bis es zu einem Timeout kommt.

NSSDW-27928: Sie können das Modem nicht aktivieren oder deaktivieren, wenn keine Konfiguration am LTE-Modem erfolgt.

- **Problemumgehung:** Führen Sie eine Konfigurationsänderung durch, z. B. - Update Access Point Name (APN).

NSSDW-27934: Wenn die Zwei-Box-Lösung aktiviert ist, können Sie nicht von der 11.2.0-Version auf obere Versionen aktualisieren, ohne die Two-Box-Lösung zu deaktivieren und nach Abschluss des Upgrades erneut zu aktivieren.

- **Problemumgehung:** Es wird empfohlen, dass Kunden, die Two-Box Solution verwenden, auf 11.2.1 (Future Release) anstelle von 11.2.0 durchführen müssen.

NSSDW-27935: HTTP-Serverwarnungen werden nicht von Citrix SD-WAN Appliances gesendet.

- **Problemumgehung:** Verwenden Sie Citrix SD-WAN Center, um HTTP-Serverwarnungen zu senden.

NSSDW-27938: Das über die CLI erstellte STS-Paket kann nicht über die SD-WAN GUI heruntergeladen werden.

- **Problemumgehung:** Verwenden Sie Citrix SD-WAN GUI, um das STS-Bundle zu erstellen.

SDWANHELP-1547: Nach einem Konfigurationsupdate sind WAN-Verbindungen möglicherweise nicht für Internet- oder Intranetdatenverkehr verfügbar.

- **Problemumgehung:** Starten Sie das Gateway-Gerät neu, setzen Sie den SD-WAN-Port zurück oder starten Sie den SD-WAN-Dienst neu.

Fehlerbehebung bei Citrix SD-WAN 110 SE Netzwerkproblemen

October 28, 2021

In diesem Abschnitt werden die Netzwerkkonnektivitätsprobleme der Citrix SD-WAN 110 SE Appliance zusammen mit Anweisungen zur Fehlerbehebung beschrieben.

Symptom

Die Citrix SD-WAN 110 SE-Appliance kann unter den folgenden Bedingungen keine Netzwerkkonnektivität herstellen.

- Die Appliance wird von SD-WAN Orchestrator verwaltet und/oder durch eine Zero-Touch-Bereitstellung (ZTD) hochgebracht.
- Die Appliance befindet sich im Werkszustand und ZTD/SD-WAN Orchestrator-Agenten sind nicht installiert.
- Die Appliance-Zeit (CMOS oder Hardware) liegt der tatsächlichen Zeit voraus.
- Die Appliance-Zeit wird vom NTP-Daemon vor dem Download/der Installation der ZTD/SD-WAN Orchestrator-Agenten rückwärts eingestellt.

Workaround

Nach der Erstinstallation (oder nach dem Zurücksetzen des Geräts auf die ursprüngliche Werkskonfiguration) muss der Endbenutzer, der SD-WAN 110 installiert, überprüfen, ob die Appliance erfolgreich mit dem Organisationsnetzwerk verbunden ist. Der Endbenutzer muss zusammen mit der Appliance organisationsspezifische Anweisungen erhalten (z. B. Wählen auf dem VoIP-Telefon), um die Netzwerkkonnektivität zu überprüfen. Wenn die Appliance keine Verbindung zum Netzwerk aufnimmt, kann der Endbenutzer die folgenden Anweisungen befolgen:

1. Lassen Sie das Gerät eingeschaltet und warten Sie 30 Minuten oder länger.
2. Drücken Sie kurz aber fest auf die Ein-/Aus-Taste (1—2 Sekunden), um sie herunterzufahren.
3. Nachdem die Lichter am Gerät dunkel sind, drücken Sie erneut die Ein-/Aus-Taste, um das Gerät wieder einzuschalten. Die SD-WAN 110-Appliance startet jetzt neu und stellt eine Verbindung zum Netzwerk her.

Versionshinweise

November 16, 2022

In diesem Versionshinweis werden neue, behobene Probleme und bekannte Probleme beschrieben, die für die Citrix SD-WAN -Software Version 11.2, Version 1 für die SD-WAN Standard Edition, WANOP, Premium Edition Appliances und das SD-WAN Center gelten.

Weitere Informationen zu den vorherigen Versionen finden Sie in der [Citrix SD-WAN-Dokumentation](#).

Neue Features

Neue Verbesserungen an der Benutzeroberfläche -

Die Unterstützung der neuen Benutzeroberfläche wird jetzt auf SD-WAN 210 Appliances erweitert. Alle lokalen Benutzer mit Administratorrolle und Remotebenutzer haben Zugriff auf die neue Benutzeroberfläche. Lokale Benutzer können ihr Kontokennwort ändern. Remote-Benutzerkonten werden über RADIUS- oder TACACS + -Authentifizierungsserver authentifiziert. Sie können entweder den RADIUS- oder TACACS+-Authentifizierungsserver konfigurieren. Die Möglichkeit, SIM-PIN-Operationen durchzuführen und die LTE-Firmware zu verwalten, werden ebenfalls eingeführt.

Optimierung des Gateway -

Sie können jetzt die erste Paketerkennung, -klassifizierung und das selektive Routing (direkter Internet-Breakout oder über den virtuellen Pfad) des für Citrix Cloud und Citrix Gateway Service bestimmten Datenverkehr (Kontrolle und Daten) aktivieren. Diese Funktion ist nur über Orchestrator ab SD-WAN Version 11.2.1 verfügbar.

Citrix SD-WAN 6100 Premium Edition-Appliance -

Die Citrix SD-WAN 6100 PE Appliance ist eine 2U-Appliance. Es verfügt über zwei 14-Core-Prozessoren für insgesamt 28 physische Kerne (mit aktiviertem Hyper-Threading) und 256 GB Speicher. Die Citrix SD-WAN 6100 PE-Einheit wird mit dem Citrix SD-WAN 10.2.7 Image ausgeliefert. Aktualisieren Sie die Software auf Citrix SD-WAN 11.2.1 und höher, um die PE-Funktionalität zu aktivieren.

Erweiterte Edge-Sicherheitsunterstützung für Citrix SD-WAN 210 SE-Appliances (Tech Preview) -

Citrix SD-WAN 210 SE und 210 SE LTE-Appliances unterstützen jetzt Advanced Edge Security-Funktionen mit Add-On-Lizenzen von Advanced Security. Um erweiterte Sicherheitsfunktionen auf einer Citrix SD-WAN 210 Appliance zu aktivieren, erstellen Sie ein Image der Appliance-Software auf Citrix SD-WAN 10.2.7.17 und installieren Sie die Advanced Security-Add-On-Lizenz. Weitere Informationen finden Sie unter [USB Reimage Dienstprogramm](#).

Hinweis

Die Aktivierung der Advanced Security Add-On-Lizenz auf der Citrix SD-WAN 210 Appliance kann zum ersten Mal bis zu 20 Minuten dauern.

LAG-Unterstützung für Citrix SD-WAN 2100 SE -

Citrix SD-WAN 2100 SE Appliance unterstützt einfaches LAG (ACTIVE-BACKUP). Die 802.3ad LACP-Protokoll-basierten Verhandlungen werden in der aktuellen Version nicht unterstützt. Zu jeder Zeit ist nur ein Port aktiv und die anderen Ports befinden sich im Backup-Modus.

Berichte in Echtzeit -

Citrix SD-WAN Orchestrator ermöglicht es Ihnen, die Echtzeitberichte für die folgenden Sicherheitsfunktionen anzuzeigen:

- **Web-Filterung:** Bietet den Echtzeitbericht der letzten 1000 Web-Ereignisse (HTTP, HTTPS) aus der Gesamtzahl der Web-Anfragen.
- **Anti-Malware:** Bietet den Echtzeitbericht der letzten 1000 Anti-Malware-Ereignisse aus der Gesamtzahl der gescannten Dateien.
- **Intrusion Prevention:** Bietet den Echtzeitbericht der letzten 1000 protokollierten und blockierten Intrusion Prevention-Systemereignisse aus der Gesamtzahl der Intrusionsereignisse.

Sie können auch auf die einzelnen Segmente des Kreisdiagramms oder auf die Legenden neben dem Kreisdiagramm klicken, um die 10 wichtigsten Ereignisdetails der Sicherheitsfunktionen Webfilterung, Anti-Malware und Intrusion Prevention anzuzeigen.

On-Prem Orchestrator -

Ab der Citrix SD-WAN 11.2.1-Version wird die sichere Appliance-Konnektivität auf dem On-prem SD-WAN Orchestrator zusammen mit den Optionen SD-WAN Appliance und On-Prem SD-WAN Orchestrator Certificates, Domain, Authentication Type und Advanced Configuration implementiert. Sie können entweder die On-Prem SD-WAN Orchestrator IP-Adresse oder Domäne oder beide (IP-Adresse und Domäne) verwenden, um die On-Prem SD-WAN Orchestrator-Konnektivität zu aktivieren.

RADIUS und TACACS+ Server - Der Timeout-Wert für den RADIUS- und TACACS+-Server wird von 10 Sekunden auf 60 Sekunden erhöht.

Behobene Probleme

SDWANHELP-1193: Für einen MCN im werkseitigen Standardzustand enthält das LCM-Paket, das unmittelbar nach dem Klicken auf das Staging heruntergeladen wurde, jedoch vor der Aktivierung der bereitgestellten Software, nicht den erforderlichen Inhalt.

SDWANHELP-1210: Wenn sowohl VRRP als auch HA konfiguriert sind, wird der GUI-Zugriff unterbrochen, es werden Verbindungsverluste und Ping-Fehler beobachtet. Initiieren Sie die VRRP-Instanz nicht auf der HA-Standby-Appliance.

SDWANHELP-1299: Ein Zweig mit dynamischem virtuellem Pfad, der mit einer anderen Zweigstelle eingerichtet wurde, und leitet die über den dynamischen virtuellen Pfad empfangenen Routen an andere Standorte weiter. Wenn der dynamische virtuelle Pfad heruntergeht, werden die gelernten Routen nicht von den anderen Sites entfernt.

SDWANHELP-1326: Nach dem Upgrade von SD-WAN auf 11.1.0/11.1.1 werden PPPoE-Links auf den folgenden Plattformen nicht verbunden:

- Citrix SD-WAN 410
- Citrix SD-WAN 210
- Citrix SD-WAN 1100
- Citrix SD-WAN 4100
- Citrix SD-WAN 5100
- Citrix SD-WAN 6100

SDWANHELP-1330: SD-WAN Center hat keine E-Mail-Benachrichtigungen zugestellt, da die E-Mail-Einstellungen in der SD-WAN Center-Datenbank auf Null gesetzt wurden.

SDWANHELP-1332: Wenn ein einzelner Datenfluss auf mehr als drei verschiedene WAN-Verbindungen gesendet wird, kann der SD-WAN-Dienst während der Erfassung von NetFlow-Statistiken abstürzen.

SDWANHELP-1337: Für die Elastic Compute Cloud (EC2) von AWS, die SD-WAN-Instanz mit mehr als 32 GB Speicher, fällt die virtuelle Instance auf den Standardwert von 16 statischen virtuellen Pfaden zurück. Es führt zu undefiniertem Verhalten und möglichen Absturzscenarien, wenn mehr als 16 statische virtuelle Pfade konfiguriert sind.

SDWANHELP-1365: In einem GEO-MCN-Setup mit hoher Verfügbarkeit und aktivierter WAN-to-WAN-Weiterleitung kann ein Down-Ereignis des Internetdienstes ein fehlerhaftes Szenario auslösen, bei dem Routen, die vom sekundären GEO-MCN gelernt wurden, eine höhere Priorität haben als der primäre GEO-MCN.

SDWANHELP-1370: Der SNMP-Dienst wurde aktiviert, nachdem das SD-WAN Center mit der standardmäßigen Community-Zeichenfolge als öffentlich Provisioning wurde, verursacht ein Schwachstellenproblem. Das SD-WAN Center unterstützt den SNMP-Dienst nicht. Daher ist der SNMP-Dienst dauerhaft deaktiviert, um das Sicherheitsanfälligkeitsproblem zu beheben.

SDWANHELP-1384: Routing-Domänendienst-Routen, wenn sie mit Netzwerkobjekten erstellt werden, werden nicht hinzugefügt. Die Exportroute Option für alle inter-Routing-Domänendienststrouten zum Exportieren der Route an andere verbundene Standorte funktioniert nicht.

SDWANHELP-1385: Die Informationen zur Seriennummer des SD-WAN-Geräts gehen möglicherweise aufgrund eines Problems in der BIOS-Firmware v1.0b auf der SD-WAN 210-Plattform auf die Standardzeichenfolge zurück.

SDWANHELP-1386: Der Benutzer kann keine Bandbreitentests für Pfade auf der SD-WAN-Appliance planen.

SDWANHELP-1432: Trace-Dateien werden nicht ordnungsgemäß analysiert, wenn der Dateiname ein **+-Symbol** enthält.

SDWANHELP-1464: Der SD-WAN-Dienst wird abgebrochen, während der über den Intranetdienst empfangene Pakete verarbeitet wird, der über den privaten MPLS-Link mit MPLS-Warteschlangen konfiguriert wurde.

NSSDW-27587: Eine Datenträger-Warnmeldung wird auf der SD-WAN VPX Appliance als MCN mit dem standardmäßigen 40 GB Speicherplatz angezeigt.

NSSDW-27727: Netzwerke mit VPX und VPXL-Instanz, die den IXGBEVF-Treiber verwenden und für bestimmte Intel 10-GB-NICs verwendet werden, wenn SR-IOV aktiviert ist, dürfen nicht auf 11.0.1 aktualisiert werden. Dies kann zu einem Verlust der Konnektivität führen. Das Problem hat bekanntermaßen Auswirkungen auf AWS-Instanzen mit aktiviertem SR-IOV.

NSSDW-27753: Wenn SD-WAN vor dem Upgrade auf SD-WAN 11.2.0 nicht bei MAS registriert war, kann es nach dem Upgrade auf SD-WAN 11.2.0 nicht bei MAS registriert werden.

NSSDW-27928: Sie können das Modem nicht aktivieren oder deaktivieren, wenn keine Konfiguration am LTE-Modem erfolgt.

NSSDW-27934: Wenn der Zwei-Box-Modus aktiviert ist, können Sie nicht von der Version 11.2.0 auf obere Versionen aktualisieren, ohne den Two-Box-Modus zu deaktivieren und ihn nach Abschluss des Upgrades erneut zu aktivieren.

NSSDW-27935: HTTP-Serverwarnungen werden nicht von Citrix SD-WAN Appliances gesendet.

NSSDW-27938: Das mit der CLI erstellte STS-Paket kann nicht über die SD-WAN-GUI heruntergeladen werden.

NSSDW-28146: Wenn die Citrix SD-WAN 11.2.0-Version einmal von der Version 10.2 aktualisiert oder auf Version 10.2 heruntergestuft wird, wird sie auf 11.0/11.1-Releases aktualisiert, schlägt ein erneuter

Herunterstufen auf die Version 10.2 fehl. Ebenso wurde nach dem Upgrade von Citrix SD-WAN Center von Version 10.2 auf Version 11.2.0 das Downgrade von SD-WAN Center von 11.2.0 auf Version 10.2 nicht unterstützt.

NSSDW-28799: Das Erstellen eines benutzerdefinierten Dashboards bietet Ihnen die Möglichkeit, es als primäres Dashboard festzulegen. Wenn Sie das Dashboard überprüfen und speichern, landen Sie standardmäßig bei jeder Anmeldung oder beim Navigieren zur Dashboard-Seite auf diesem gespeicherten Dashboard.

NSSDW-29581: Die Bandbreitenrate der Edge-Sicherheit ist nicht mit der Advanced Edition-Lizenz abgestimmt, die im SD-WAN Orchestrator geladen ist.

NSSDW-29699: Wenn Sie eine SD-WAN-Appliance mit Version 11.2.0 frisch bereitstellen, funktioniert Single Sign-On von SD-WAN Center bei MCN nicht wie erwartet. Funktionen wie Cloud Direct, Änderungsverwaltung, automatisierte Azure-Bereitstellung, virtuelles Azure-WAN, Zscaler funktionieren nicht vom SD-WAN Center aus.

Das Problem wurde in der Version SD-WAN 11.2.1 behoben. Wenn Sie ein Upgrade von einer neu bereitgestellten Version 11.2.0 auf Version 11.2.1 durchführen, erstellen Sie das Appliance-Zertifikat neu.

Bekannte Probleme

SDWANHELP-1292: Die Einstellung der Zeitzone, die mit dem SD-WAN Center durchgeführt wurde, wird auf die SD-WAN-Appliances nicht angewendet.

- **Umgehung:** Legen Sie die Zeitzone mithilfe der GUI der SD-WAN-Appliance oder der Appliance-REST-APIs oder der Appliance-CLI fest.

SDWANHELP-1323: MCN High Availability (HA) -Gerät zeigt nicht verbunden an, wenn das Kabel der ersten HA-Schnittstelle nicht angeschlossen ist (wenn mehrere HA-Schnittstellen definiert sind).

- **Problemumgehung:** Entfernen Sie die HA-Schnittstelle aus der Konfiguration, wenn sie nicht physisch verbunden ist.

NSSDW-27615: Wenn SD-WAN 210 Standard Edition (SE) in Advanced Edition (AE) konvertiert wird, werden die Speicherparameter (Huge Pages, Max Connections, Flow Limit und Anzahl der Paketpuffer) reduziert. Die Speicherparameter bleiben unverändert, auch wenn die SD-WAN 210 AE Appliance wieder in SE konvertiert wird.

NSSDW-29146: Sobald die Appliance-Rolle in der Legacy-Benutzeroberfläche von Client auf MCN umgestellt wurde, wird die neue Benutzeroberfläche, wenn sie in anderen Browsern geöffnet ist, nicht automatisch abgemeldet. Das Öffnen der neuen UI-Sitzung wirkt sich nicht auf die Legacy-Benutzeroberfläche aus. Optional können Sie die neue Benutzeroberflächensitzung schließen.

Sobald die Appliance-Rolle von MCN auf Client in der Legacy-Benutzeroberfläche umgestellt wurde, werden Sie nicht automatisch auf die neue Benutzeroberfläche umgeleitet. Sie können die Legacy-Benutzeroberfläche weiterhin verwenden. Wenn Sie die neue Benutzeroberfläche verwenden, durchsuchen Sie [https://< management-ip>](https://<management-ip>) eine neue Browserregisterkarte.

NSSDW-29513: VPX-Zweig wechselt in den Single-Site-Modus, wenn die neu bereitgestellte VM zuerst herabgestuft und dann wieder auf die Version aktualisiert wird, auf der die VM bereitgestellt wurde.

- **Problemumgehung:** Führen Sie das lokale Änderungsmanagement in der betroffenen Zweigstelle durch.

NSSDW-29526: Wenn der MCN mit HA ein teilweises Standort-Upgrade auf dem Geo-MCN durchführt, wird der Geo-MCN zum primären MCN. Nach dem teilweisen Upgrade kann das beendende Standby-MCN das neue primäre MCN nicht erkennen.

NSSDW-29819: Manchmal schlägt das Edge Security-Subsystem der Citrix SD-WAN 210 Appliance möglicherweise fehl und die Appliance wird möglicherweise nicht automatisch wiederhergestellt.

- **Problemumgehung:** Starten Sie die Citrix SD-WAN 210 Appliance neu.

NSSDW-29898: Die Sicherheitsberichte für die SD-WAN 210 AE-Appliance werden auf der Benutzeroberfläche von SD-WAN Orchestrator nicht angezeigt. Das Problem tritt aufgrund des Timing-Problems beim ersten Booten auf, bei dem der Datenbankbenutzer erstellt wird, aber keine Berechtigungen erteilt werden.

NSSDW-29900: Die SD-WAN AE-Aktivierung schlägt möglicherweise konsistent fehl, wenn die Edge-Sicherheitskomponente in einem nicht reagierenden Zustand feststeckt. Ein Neustart der fehlgeschlagenen Appliance sollte das Problem beheben und die Aktivierung fortsetzen.

Versionshinweise

May 10, 2021

In diesen Versionshinweisen werden neue, behobene Probleme und bekannte Probleme beschrieben, die für die Citrix SD-WAN -Software Version 11.2, Version 2 für die SD-WAN Standard Edition, WANOP, Premium Edition Appliances und das SD-WAN Center gelten.

Weitere Informationen zu den vorherigen Versionen finden Sie in der [Citrix SD-WAN-Dokumentation](#).

Neue Features

[Unterstützung für externes USB-Modem von MBIM und NCM -](#)

Externe USB-Modems, die den MBIM- und NCM-Modus verwenden, werden auf Citrix SD-WAN

110 und 210 Appliances unterstützt. Sie können die **APN-Einstellungen** und das Modem zum **Aktivieren/Deaktivieren** auch über die neue Citrix SD-WAN GUI und das Citrix SD-WAN Center konfigurieren. Mobile Breitbandvorgänge werden auf CDC Ethernet USB-Modems nicht unterstützt.

Edge Security Protokolle -

Citrix SD-WAN Edge-Sicherheitsprotokolle folgen jetzt dem CEF (Common Event Format). CEF ist ein Standard, der die Syntax von Protokollmeldungen definiert und daher die Interoperabilität mehrerer Geräte ermöglicht, die Protokollmeldungen in einer Lösung generieren.

Unterstützung von Citrix SD-WAN Advanced Edition -

Die Citrix SD-WAN Advanced Edition (AE) wird jetzt auf Citrix SD-WAN 210 SE und Citrix SD-WAN 210 SE LTE-Appliances unterstützt.

Office 365-Optimierung - Microsoft Office 365 Der standardmäßige Kategorieverkehr wird basierend auf allen Anwendungsendpunkten klassifiziert, die in der Kategorie Standard als erforderlich markiert sind. Weitere Informationen finden Sie unter [Office 365-URLs und IP-Adressbereiche](#).

Behobene Probleme

SDWANHELP-1161: Nach dem Upgrade auf 10.2.5.6 wurde der SD-WAN-UI-Zugriff sehr langsam.

SDWANHELP-1353: Der SD-WAN-Dienst wird möglicherweise abgebrochen, wenn im Rahmen des Konfigurationsupdates WAN-Verbindungen für den Internet-Lastenausgleich hinzugefügt werden.

SDWANHELP-1363: Der SD-WAN-Dienst wird möglicherweise abgebrochen, wenn der ARP-Eintrag vom Host auf den persistenten Typ aktualisiert wird.

SDWANHELP-1420: In der SD-WAN Premier Edition (PE) sind die WANOP GUI-Seiten über die virtuelle IP-Adresse des In-Band-Managements nicht zugänglich.

SDWANHELP-1423: Sie dürfen den Standortdiagnostetest nicht gleichzeitig für einen bestimmten Standort von der Peer-Appliance aus starten.

SDWANHELP-1463: Einige SD-WAN-Geräte traten für einige Minuten in die Kulanzzeit, da der Lizenzserver vorübergehend nicht erreichbar war.

SDWANHELP-1484: Ein Fehler bei der Verarbeitung von PKCS12-Bundles verhindert, dass Bündel, bei denen der Schlüssel vor der Verarbeitung des Zertifikats steht.

SDWANHELP-1503: Modems können im Laufe der Zeit nicht mehr reagieren, was zu einem qmi-proxy-Versagen bei der Annahme neuer Anfragen führt.

SDWANHELP-1504: Der SD-WAN-Dienst wird möglicherweise abgebrochen, wenn die ARP-Einträge manuell von der GUI gelöscht werden.

SDWANHELP-1535: Wenn Geo MCN als aktiver MCN verwendet wird, zeigt der Standby-RCN beim Geo-MCN den Status "Nicht verbunden" an. Dieses Problem kann auftreten, wenn ein Wechsel von Active MCN zu Geo MCN durchgeführt wurde.

SDWANHELP-1538: Die folgenden seltenen Probleme werden angesprochen:

- Der Datenpfad wechselt in einen Zustand, in dem Konfigurationsupdates der gelernten Quell-IP/Port, DHCP IP und PPPoE IP nicht angewendet/verpasst werden.
- Ein Konfigurationsupdate kann länger als erwartet dauern und einen Datenpfadabsturz verursachen.

SDWANHELP-1553: Back-End-Validierung, dass das Zertifikat mit der Unterzeichnerbehörde übereinstimmt, wurde beschädigt.

SDWANHELP-1554: Das Backend-Parsen von Zertifikatsinformationen wurde unterbrochen.

SDWANHELP-1555: Unterstriche waren bei der Eingabe des allgemeinen Namensfeldes nicht erlaubt.

Bekannte Probleme

NSSDW-20500: Wenn Sie auf der Citrix SD-WAN 5100 PE Appliance den Domänenbeitritt initiieren, kann eine Warnmeldung angezeigt werden, die besagt, dass WANOP initialisiert wird.

- **Problemumgehung:** Treten Sie der Domain nach 2 Minuten wieder bei.

NSSDW-28788: Die Client-Subnetze werden nicht exportiert, wenn sich die Bereitstellung im **Bridge-Modus** befindet.

NSSDW-30660: Beim Versuch, das Zertifikat an Sammler zu übertragen, wird ein Fehler ausgegeben, nachdem die Anmeldeinformationen des Collectors vom SD-WAN Center Headend während der ersten Entdeckung des RCN-basierten Netzwerks aus dem SD-WAN Center eingegeben wurden.

- **Problemumgehung:** Fügen Sie den NTP-Server hinzu und entdecken Sie das Netzwerk neu und geben Sie die IP und die Anmeldeinformationen des SD-WAN Center-Collectors ein, um das Zertifikat zu übertragen.

NSSDW-30662: Die Erkennung von RCN schlägt mit Appliance-Fehler fehl, wenn sich eine Appliance im Standby-Modus befindet, deren IP im SD-WAN-Center aufgeführt ist.

- **Umgehung:** Machen Sie die RCN-Appliance, deren Verwaltungs-IP in der Collector-Konfigurationstabelle aufgeführt ist, als aktiv, damit die Discovery fortgesetzt wird.

SDWANHELP-1400: Für eine Internetdienstroute in einer nicht standardmäßigen Routingdomäne und eine Pfadberechtigung, die konfiguriert wird, wenn der Pfad ausfällt und der Remote-Site, an dem die angegebene Routingdomäne nicht konfiguriert ist, ist die Internetroute nicht als nicht erreichbar markiert.

Versionshinweise für Citrix SD-WAN 11.2.3b Version

October 28, 2021

Dieser Versionshinweis beschreibt behobene Probleme und bekannte Probleme, die für Citrix SD-WAN-Softwareversion 11.2 Version 3 für die SD-WAN Standard Edition, WANOP, Premium Edition-Appliances und SD-WAN Center gelten.

Informationen zu den vorherigen Versionen finden Sie in der [Citrix SD-WAN-Dokumentation](#).

Hinweis

Die Version Citrix SD-WAN 11.2.3b behebt die in <https://support.citrix.com/article/CTX319135> beschriebenen Sicherheitslücken. Es ersetzt die Versionen 11.2.3 und 11.2.3 a.

Behobene Probleme

NSSDW-29862: Die virtuelle Maschine von Citrix SD-WAN Center, die auf einem VMware ESXi-Hypervisor ausgeführt wird, kann während eines Snapshots hängen bleiben.

NSSDW-31612: Damit der Citrix SD-WAN Orchestrator SD-WAN-Appliances, die mit 11.2.1- oder 11.2.2-Software geliefert werden, lokal verwalten kann, müssen Sie die SD-WAN-Appliance-Software auf die Version 11.3.0 aktualisieren.

NSSDW-32629: Automatisch generierte Sammelrouten, die für das Regional Control Node (RCN) -Netzwerk erstellt wurden, werden Kosten von 30.000 anstelle von 65534 zugewiesen.

SDWANHELP-1314: Schnittstellengruppen für Citrix SD-WAN 210 und 110 Appliances, die die REST-API über den MCN verwenden, können nicht konfiguriert werden. Der Fix bietet die Unterstützung zum Konfigurieren der Schnittstellengruppen für Citrix SD-WAN 210- oder 110-Sitemodell und BASE-Untermodule über REST-APIs.

SDWANHELP-1323: MCN Hochverfügbarkeitsgerät zeigt **nicht verbunden an**, wenn das Kabel der ersten Hochverfügbarkeitsschnittstelle nicht angeschlossen ist (wenn mehrere Hochverfügbarkeitsschnittstellen definiert sind).

SDWANHELP-1368: SNMP Walk zeigte nicht die korrekten MAC-Adressinformationen für Schnittstellen an.

SDWANHELP-1400: Für eine Internetdienstroute in einer nicht standardmäßigen Routingdomäne und einer konfigurierten Pfadberechtigung ist die Internetroute nicht als nicht erreichbar gekennzeichnet, wenn der Pfad ausfällt und der Remote-Site, auf dem die angegebene Routingdomäne nicht konfiguriert ist.

SDWANHELP-1437: Deaktivierung des unsicheren TLS1.0 und TLS1.1 zwischen Citrix SD-WAN und SD-WAN Center-Konnektivität.

SDWANHELP-1485: Pakete, die im Internet/Intranet-Dienst empfangen werden, können möglicherweise mit der falschen WAN-Verbindung verknüpft werden, wenn mehrere WAN-Link-Gateways auf dieselbe MAC-Adresse aufgelöst werden.

SDWANHELP-1507: Ein Problem im Konfigurationsmodul bestand darin, dass die Exportrouteneinstellung wahr war, während die WAN-zu-WAN-Weiterleitungseinstellung für die Site deaktiviert war. Nach dem Fix wird die Exportroute korrekt auf “false” gesetzt, wenn die WAN-zu-WAN-Weiterleitung deaktiviert ist und der Benutzer die Exportrouteneinstellung nicht explizit festgelegt hat.

SDWANHELP-1509: Die Standard-Community-Zeichenfolge (öffentlich) für die SNMP-Trap-Nachricht in Citrix SD-WAN kann nicht geändert werden.

SDWANHELP-1513: Die DNS-Einstellungen wurden nicht mit DHCP aktualisiert, wenn der Management-Port als DHCP-Client fungiert.

SDWANHELP-1520: Das Problem ist das IP-Lernen auf der Zweigstelle, bei dem die veralteten IP-Details für die getrennte WAN-Verbindung nicht gelöscht werden. Diese veralteten IP-Details verursachen einen virtuellen Pfad zwischen einem Zweig zu einem anderen Zweig in einem DEAD Zustand. Bereinigen Sie im Rahmen des Fix die alten IP-Details auf der Zweigstellen-Appliance während des IP-Lernens.

SDWANHELP-1531: Auf der Berichtsseite von Citrix SD-WAN Center stimmten die Daten im Bericht “**Top-Anwendungen**” einer Site nicht mit den Daten im Bericht “**Top-Sites**” überein. Dies geschah aufgrund einer unerwünschten Regex-Übereinstimmung des Site-Namens.

SDWANHELP-1537: Die Citrix SD-WAN Center-Authentifizierung für TACACS-basierte Benutzer scheiterte bei einigen Kombinationen von Passwörtern mit \$ - und #-Zeichen im Kennwort. Dieses Problem war in der Version 11.2.0 enthalten.

SDWANHELP-1547: Nach einem Konfigurationsupdate sind WAN-Verbindungen möglicherweise nicht für Internet- oder Intranetdatenverkehr verfügbar.

SDWANHELP-1558: Der Internetdienst verwendet die Backup-Links nicht, wenn der primäre Link ausfällt.

SDWANHELP-1580: Während das Erlernen öffentlicher IP-Adressen auf einer WAN-Verbindung in Zweigstellen aktiviert ist, lernt der RCN möglicherweise die neue öffentliche IP-Adresse nicht und führt zu einem toten Pfad, wenn:

- Es besteht eine Diskrepanz zwischen der Zweigstelle und dem RCN
- Die öffentliche IP-Adresse des Zweigs WAN-Link hat sich geändert

SDWANHELP-1616: Der lokale Internet-Breakout von Office365 funktioniert möglicherweise nicht, wenn mehrere Routingdomänen auf einer Site aktiviert sind.

SDWANHELP-1617: Wenn regionale Subnetze erstellt werden, werden die Sammelrouten automatisch mit 65534-Kosten erstellt. Wenn diese Route auf einer anderen Site beworben wird, werden die Kosten überrollt und werden zu einer nicht zusammenfassenden Route mit den niedrigsten Kosten.

SDWANHELP-1627: Verbindungen, die über die gehosteten Firewalls (Palo Alto) umgeleitet und über den Virtual Path-Dienst weitergeleitet werden, weisen Probleme mit hoher Latenz auf.

SDWANHELP-1641: Ein Absturz im Konfigurations-Compiler tritt auf, wenn die Gruppe der automatischen Pfade nicht in der WAN-Link-Verwendung für den dynamischen virtuellen Pfad festgelegt ist, wenn sie auf einer LTE-E1-Schnittstelle konfiguriert ist.

SDWANHELP-1646: Der Management-Port darf nicht in der Link Aggregation Group (LAG) hinzugefügt werden, daher wird die Verwaltungsschnittstelle bei der Bildung der LAG nicht aufgeführt.

SDWANHELP-1673: Citrix SD-WAN Anfrage zum Herunterladen der PAC-Datei vom Server wird von SD-WAN selbst abgefangen und bedient, wenn die Verwaltungs-IP mit der lokalen Route übereinstimmt.

SDWANHELP-1684: Als **Zertifikatssperrlisten** aktiviert wurden, trat ein Fehler auf, der wiederholte Download-Versuche der CRL verursachte.

SDWANHELP-1686: Die Verwendung der gleichen hochverfügbaren IPs an verschiedenen Standorten war bisher nicht erlaubt. Die hochverfügbaren IPs werden jetzt als privat behandelt, sodass sie an verschiedenen Standorten verwendet werden können.

SDWANHELP-1736: Die E-Mail-Benachrichtigung von Citrix SD-WAN Center fügt < CR > dem Befehl ein zusätzliches Zeichen hinzu, wodurch die SMTP-Sitzung beendet wird.

SDWANHELP-1783: Wenn die Protokollnachricht während der Erstellung eines dynamischen virtuellen Pfads mit einem unerwarteten IP-Wert (TOS) eingeht, kann dies zu einem Core-Dump führen.

SDWANHELP-1787: Der **Import** und **Export** großer Netzwerkkonfigurationen (wenn die Größe der Konfigurationsdatei 16 MB überschritt) in Citrix SD-WAN Center war fehlgeschlagen.

SDWANHELP-1804: Nach dem Upgrade des Citrix SD-WAN-Geräts auf die Version 11.2.2 fungiert mehr als ein VRRP-Gerät aufgrund der falschen VRRP-Ankündigungs-Paketgröße, die vom SD-WAN-Gerät gesendet wurde, als **Master**.

SDWANHELP-1866: Wenn der Management-Port auf Citrix SD-WAN 110- und 210-Plattformen als Data-Port konfiguriert ist, kann sich die **Host-ID** nach dem Upgrade auf eine neuere Version ändern. Die SD-WAN-Appliances verwenden die Grace-Lizenz, wenn dieses Problem auftritt.

Bekannte Probleme

NSSDW-25387: Wenn das lokale Änderungsmanagement auf eine SD-WAN-Appliance ohne Unterschied in der PPPoE-Konfiguration angewendet wird, werden die vorhandenen PPPoE-Sitzungen möglicherweise nicht neu gestartet.

- **Problemumgehung:** Stellen Sie die PPPoE-Verbindungen wieder her (unter **Überwachung > PPPoE**).

NSSDW-25452: Citrix SD-WAN Orchestrator-UI und Citrix SD-WAN Configuration Compiler lassen sich nicht aus dem zulässigen Bereich des DHCP-Leasingintervalls herausgreifen, wodurch der DHCP-Daemon ausfällt.

- **Problemumgehung:** Geben Sie an, dass die gültige Leasingzeit für DHCP 300—86400 beträgt.

NSSDW-28788: Die Client-Subnetze werden nicht exportiert, wenn sich die Bereitstellung im Bridge-Modus befindet.

NSSDW-29146: Sobald die Appliance-Rolle in der Legacy-Benutzeroberfläche von Client auf MCN umgestellt wurde, wird die neue Benutzeroberfläche, wenn sie in anderen Browsern geöffnet ist, nicht automatisch abgemeldet. Das Öffnen der neuen UI-Sitzung wirkt sich nicht auf die Legacy-Benutzeroberfläche aus. Optional können Sie die neue Benutzeroberflächensitzung schließen. Sobald die Appliance-Rolle von MCN auf Client in der Legacy-Benutzeroberfläche umgestellt wurde, werden Sie nicht automatisch auf die neue Benutzeroberfläche umgeleitet. Sie können die Legacy-Benutzeroberfläche weiterhin verwenden. Wenn Sie die neue Benutzeroberfläche verwenden, durchsuchen Sie **https:// < management-ip>** in einem neuen Browser-Tab.

NSSDW-29513: VPX-Zweig wechselt in den Single-Site-Modus, wenn die neu bereitgestellte virtuelle Maschine zuerst heruntergestuft und dann wieder auf die Version aktualisiert wird, auf der die virtuelle Maschine bereitgestellt wurde.

- **Problemumgehung:** Führen Sie Local Change Management (LCM) in der betroffenen Zweigstelle durch.

NSSDW-29526: Wenn der MCN mit hoher Verfügbarkeit ein teilweises Standort-Upgrade auf dem Geo-MCN durchführt, wird der Geo-MCN zum primären MCN. Nach dem teilweisen Upgrade kann das beendende Standby-MCN das neue primäre MCN nicht erkennen.

NSSDW-32879: Während des Stagings kann die Seite **Change Management** gelegentlich beim Schritt "Vorbereitungspakete" einfrieren.

- **Problemumgehung:** Wiederholen Sie das Staging, indem Sie auf die Registerkarte Änderungs-vorbereitung klicken.

SDWANHELP-1292: Die Änderung der **Zeitzoneneinstellungen** im Citrix SD-WAN Center wird auf einigen Seiten nicht wirksam. Die Zeit wird immer noch in UTC angezeigt.

SDWANHELP-1491: ICMP-Verbindungen werden WAN zu WAN zwischen Virtual Path und Intranetdienst über den IPsec-Tunnelpaketverlust weitergeleitet.

SDWANHELP-1454: Eine falsche WAN-Link-Nutzungseinstellung von Auto wurde für den Internetdienst zulässig, die einen Absturz verursachte. Der Konfigurationscode wurde korrigiert, um

Benutzer davon abzuhalten, die Option Auto für die Verwendung von WAN Link für den Internetdienst auszuwählen. Eine Prüfung wurde ebenfalls hinzugefügt, um diese Fehlkonfiguration zu erfassen.

SDWANHELP-1549: Ignoriert das WAN-Link-Statusverhalten wird auf SD-WAN 10.2 Versionsverhalten zurückgesetzt. Für Internet-/Intranetdatenverkehr wird nur die Verbindung verwendet, die Pfade im UP-Zustand hat. Wenn alle Pfade auf den Links, die für den Internet/Intranet-Dienst konfiguriert sind, tot sind und die Option **WAN-Link-Status ignorieren** aktiviert ist, wird die Verbindung mit der höchsten Bandbreite für Internet/Intranet-Datenverkehr verwendet.

SDWANHELP-1737: Wenn Sie einen neuen lokalen Benutzer in Citrix SD-WAN Center hinzufügen, wird ein gelbes Banner mit der Meldung angezeigt, dass der Firewallzugriff von **Aktiviert** in **Disabled** geändert wird.

SDWANHELP-1739: Wenn zwei virtuelle IP-Adressen (eine private und eine andere nicht privat) im selben Subnetz erstellt werden, tritt ein Problem auf, dass zwei Routen für dasselbe Subnetz erstellt werden und das Subnetz nicht an einen Remote-Site beworben wird.

SDWANHELP-1755: Snapshot-Erweiterungen von Azure funktionieren in der Build-Root-Umgebung nicht.

SDWANHELP-1764: Sie können eine neue Konfigurationsänderung nicht **Staging** und **Aktivieren**. Den Arbeitsspeicher- und CPU-Feldern werden einige Standardwerte zugewiesen, die nicht geändert werden können, da derzeit keine Option in der Benutzeroberfläche von SD-WAN Orchestrator verfügbar ist. Dieses Problem tritt auf, da die Standardwerte von Kunde zu Kunde unterschiedlich sind.

SDWANHELP-1780: Das Feld **Öffentliche IPv4-Adresse** wurde im Abschnitt **Basic** des Konfigurationseditors ausgegraut.

SDWANHELP-1799: Bei der DHCP-Serverkonfiguration beim Neustart oder Upgrade des Dienstes besteht eine Timing-Bedingung, aufgrund derer eine oder mehrere Schnittstellen nicht auf DHCP-Clientanforderungen reagieren können.

- **Problemumgehung:** Starten Sie den DHCP-Server von Citrix SD-WAN UI aus neu.

SDWANHELP-1806: Während des Herunterladens tritt ein SHA-256-Prüfsummenfehler auf, wenn ein Kunde eine Appliance mit einer neuen Konfiguration steckt.

SDWANHELP-1808: Eingehender VOIP-Anruf über T-Mobile Germany Carrier schlägt mit Citrix SD-WAN 210 Appliance fehl.

SDWANHELP-1835: Unter seltenen Bedingungen kann der Citrix SD-WAN-Dienst während der Verarbeitung der über den dynamischen virtuellen Pfad empfangenen Pakete zum Zeitpunkt der dynamischen Entfernung virtueller Pfade abstürzen.

Neue Benutzeroberfläche für SD-WAN-Appliances

October 28, 2021

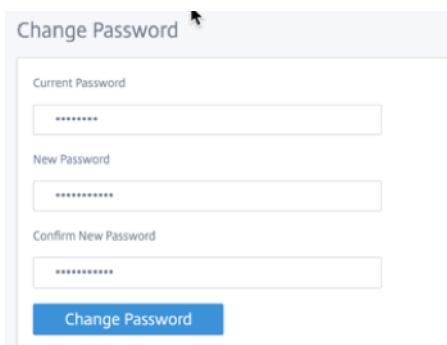
Eine neue Benutzeroberfläche (UI) wird für SD-WAN-Appliances eingeführt. Die neue Benutzeroberfläche wird mit den neuesten UI-Technologien erstellt. Das neue UI-Design verbessert die Sicherheit, hat ein verbessertes Aussehen und Gefühl, es ist leistungsfähiger, sicherer und reaktionsschneller. Die neue Benutzeroberfläche hat jedoch den Fluss und das Seitenlayout jedes Features aus der Legacy-Benutzeroberfläche beibehalten.

Die neue Benutzeroberfläche gilt nur für Kunden, die die folgenden Appliances verwenden:

| Gerät | Release |
|----------------------|-----------|
| Citrix SD-WAN 110 SE | 11.1.1 ab |
| Citrix SD-WAN 210 SE | 11.2.1 ab |

Hinweis

- Beim Provisioning von Citrix SD-WAN 210-SE als MCN, werden Sie zur Legacy-Benutzeroberfläche weitergeleitet.
- Alle lokalen Benutzer mit Administratorrolle und Remoteadministratorbenutzer können auf die neue Benutzeroberfläche zugreifen. Remote-Benutzerkonten werden über RADIUS- oder TACACS + -Authentifizierungsserver authentifiziert. Es ist zwingend erforderlich, das Standardkennwort für das Administratorkonto während der Provisioning der SD-WAN-Appliance zu ändern. Das Standardkennwort ist die Seriennummer der SD-WAN-Appliance und muss sich beim ersten Mal nach der Anmeldung am Gerät ändern.



Die ältere Benutzeroberfläche wird aus Gründen der Abwärtskompatibilität beibehalten und ist veraltet. Auf die Legacy-Benutzeroberfläche kann unter Verwendung der URL **<https://cgi-bin/login.cgi>**

zugegriffen werden. < ip-address > Der Benutzername und das Kennwort für den **Benutzeradministrator** bleiben in beiden (neuen/älteren) Benutzeroberflächen gleich, und die Erstanmeldung kann über eine der beiden Schnittstellen durchgeführt werden. Weitere Benutzer werden in zukünftigen Versionen der neuen Benutzeroberfläche unterstützt.

Citrix SD-WAN neue Benutzeroberfläche

Auf die neue Benutzeroberfläche kann mit den Browsern Google Chrome (Version 81), Mozilla Firefox, Microsoft Edge (Version 81+) und Legacy Microsoft Edge (Version 44+) zugegriffen werden.

HINWEIS

Microsoft Internet Explorer, Apple Safari und andere Browser werden nicht unterstützt.

Gehen Sie folgendermaßen vor, um auf die neue UI-Seite zuzugreifen:

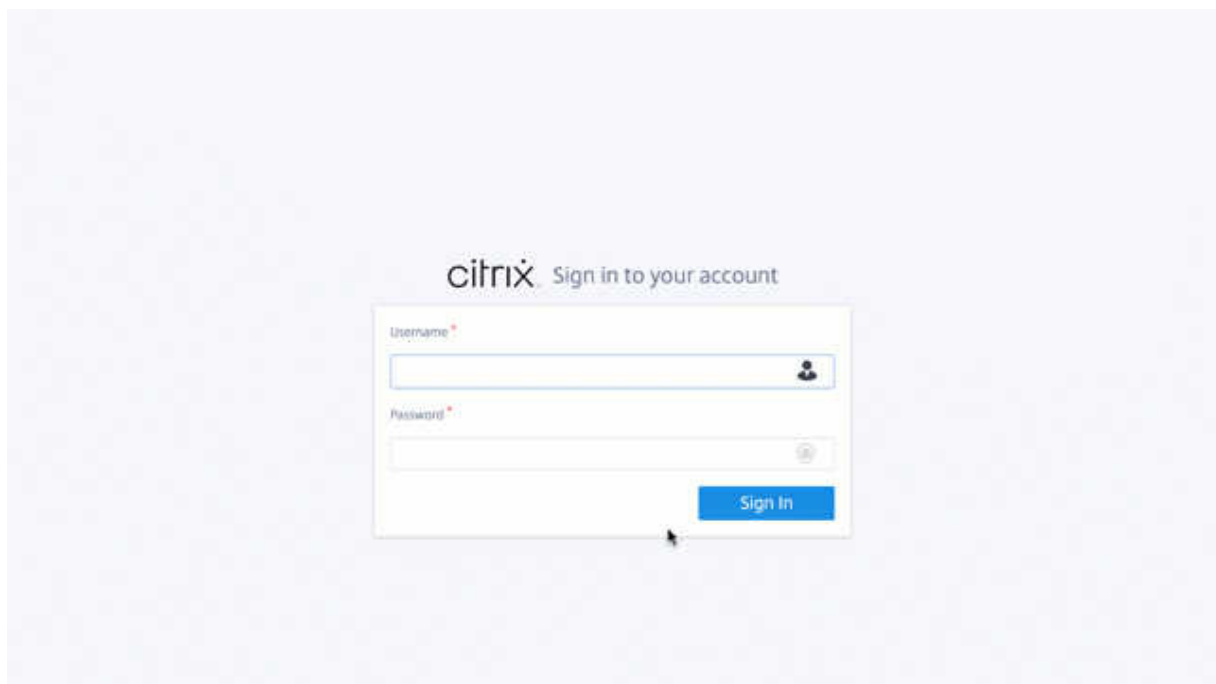
1. Öffnen Sie einen neuen Browser-Tab und navigieren Sie zu **https://** < management-ip >, um auf die neue Benutzeroberfläche der SD-WAN-Appliance zuzugreifen.

Hinweis

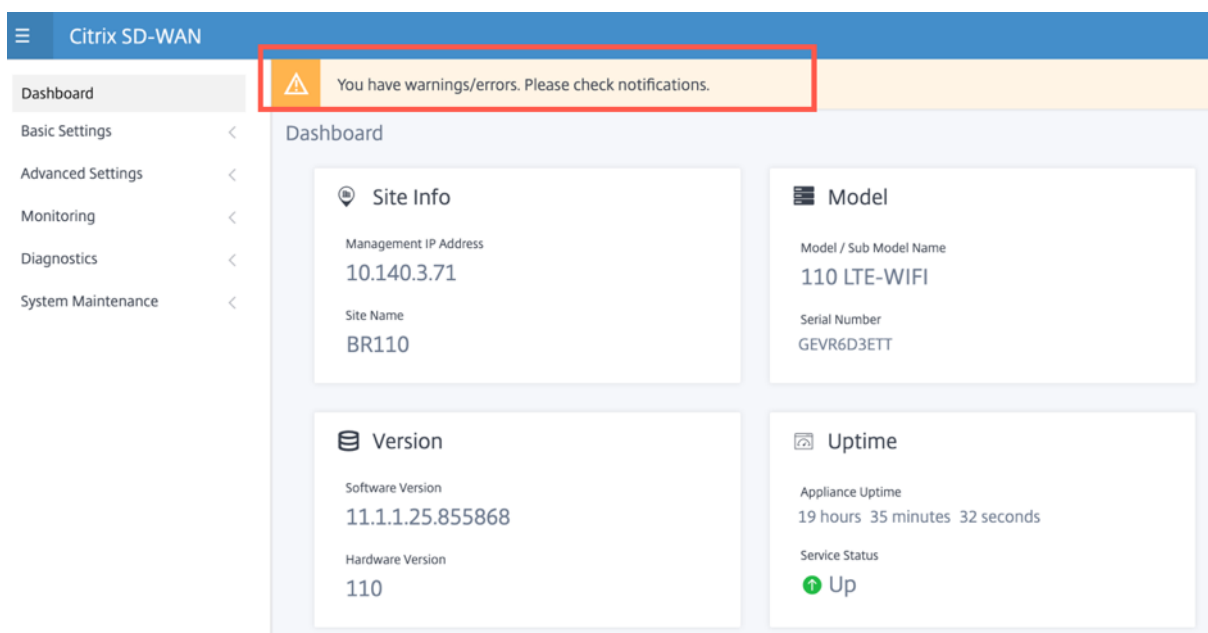
In dem Szenario, in dem das In-Band-Management aktiviert ist, kann die IP-Adresse der Schnittstelle bereitgestellt werden, < **management-ip** > um auf die neue Benutzeroberfläche zuzugreifen. Die In-Band-Verwaltung kann auf mehreren vertrauenswürdigen Schnittstellen aktiviert werden, die für IP-Dienste verwendet werden können. Sie können über die Management-IP und virtuelle In-Band-IPs auf die Benutzeroberfläche zugreifen.

1. Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf **Anmelden**.

Die Seite Citrix SD-WAN -Benutzeroberfläche wird angezeigt.



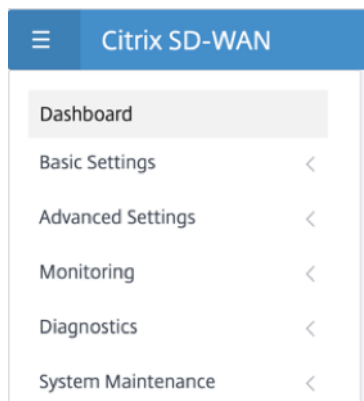
Sobald Sie sich erfolgreich angemeldet haben, sehen Sie, dass sich das Navigationsfeld auf der linken Seite befindet. Außerdem können Sie ein Benachrichtigungsbanner auf dem Dashboard sehen, wenn Warnungen oder Fehler vorliegen.



Navigation

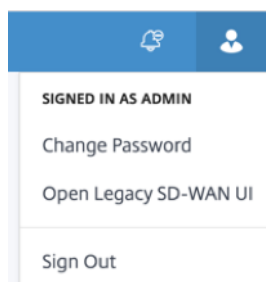
Die linke Navigations-Sidebar kann beim Klick auf das Hamburger-Symbol ausgeblendet oder sichtbar gemacht werden. Das Hamburger-Symbol in der oberen linken Ecke bietet Links zum Dashboard,

zu **grundlegenden/erweiterten** Einstellungen, zur Überwachung und zum Management.



Menüleiste

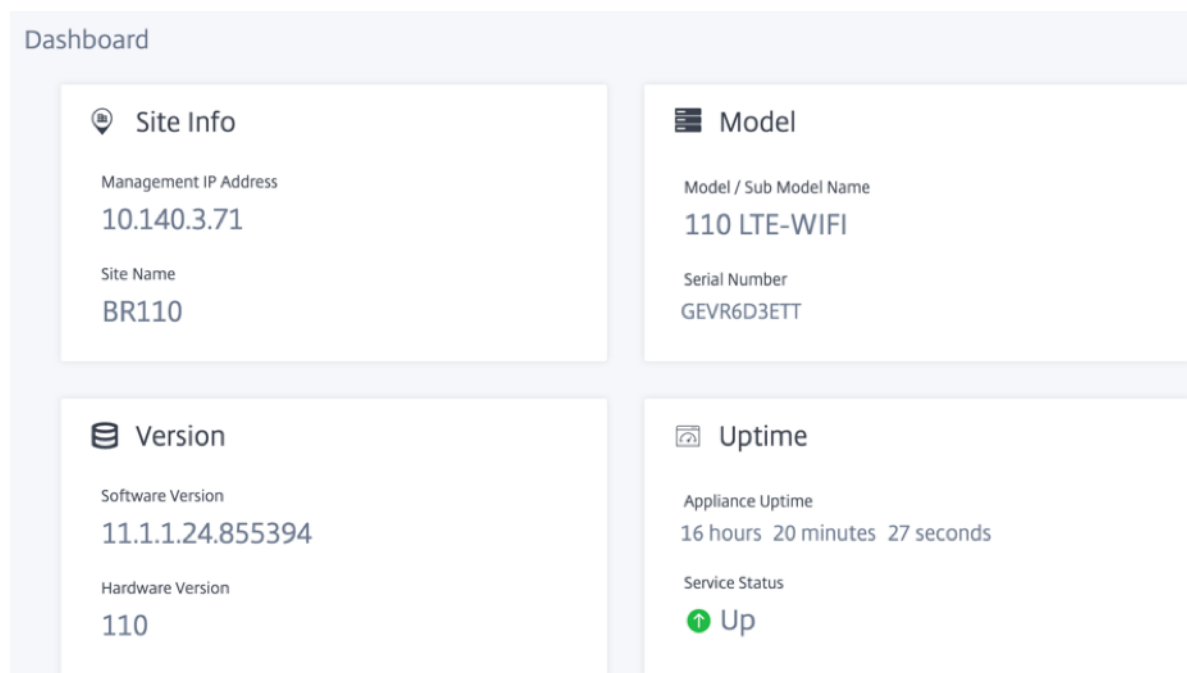
Das Benutzermenü in der oberen rechten Ecke zeigt die angemeldeten Benutzerdetails an. Sie können die Legacy-Benutzeroberfläche in einer neuen Browserregisterkarte **öffnen, indem Sie auf die Option Legacy SD-WAN UI** öffnen klicken. Klicken Sie auf das Glockensymbol für Benachrichtigungen.



Dashboard

Auf der Seite **Dashboard** werden die folgenden grundlegenden Informationen der SD-WAN-Appliance als Kachelansicht angezeigt:

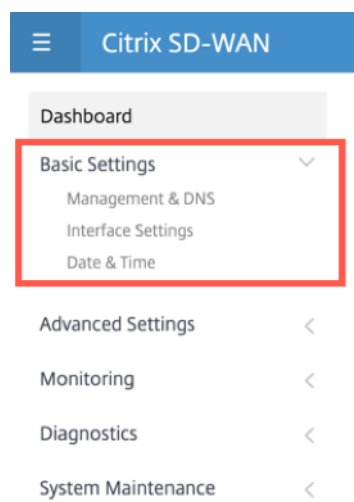
- **Site** — Zeigt die Site-Informationen mit der **Verwaltungs-IP-Adresse** und dem **Site-Namen an**
- **Modell** — Zeigt den **Modell-/Untersmodellnamen** und die **Seriennummer an**
- **Version** — Zeigt **Software-** und **Hardwareversion an**
- **Betriebszeit** - Zeigt **Appliance-Betriebszeit** und **Status des Citrix Virtual WAN-Dienstes an**



Grundeinstellungen

Die **Grundeinstellungen** der SD-WAN-Appliance umfassen die folgende Entitätenkonfiguration. Die neue Benutzeroberfläche bietet eine separate Seite für die Konfiguration jeder Entität einzeln.

- Verwaltung und DNS
- Interface-Einstellungen
- Datum/Uhrzeit
- RADIUS-Server
- TACACS+ Server



Verwaltung und DNS

Auf der Seite **Verwaltung und DNS** können Sie die IP-Adresse der Verwaltungsschnittstelle und die DNS-Einstellungen konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren der Management-IP-Adresse](#).

The screenshot displays the Citrix SD-WAN management interface. The left sidebar shows the navigation menu with 'Management & DNS' selected. The main panel, titled 'Network Adapters', contains the following configuration sections:

- Management Interface IP:** Includes a checked 'Enable DHCP' checkbox and input fields for 'IP Address', 'Subnet Mask', and 'Gateway IP Address'.
- DNS Settings:** Includes input fields for 'Primary DNS' and 'Secondary DNS', and a 'Clear' button.
- Current DNS:** Displays the current 'Primary DNS' and 'Secondary DNS' values.

A blue 'Save' button is located at the bottom of the configuration area.

Geben Sie die **IP-Adresse**, die **Subnetzmaske** und die **Gateway-IP-Adresse** für das Gerät ein, das Sie konfigurieren möchten. Geben Sie im Abschnitt **DNS-Einstellungen** die Details des primären und sekundären DNS-Servers an und klicken Sie auf **Speichern**.

Interface-Einstellungen

Auf der Seite **Interface-Einstellungen** werden die Konfigurationsdaten des Ethernet-Ports angezeigt. Die Ports, die heruntergefahren sind, werden als roter Punkt gegen die MAC-Adresse angezeigt.

☰

Citrix SD-WAN

Dashboard

Basic Settings

Management & DNS

Interface Settings

Date & Time

Advanced Settings

Monitoring

Diagnostics

System Maintenance

Ethernet Interface Settings

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

Save

Datum/Uhrzeit

Auf der Einstellungsseite für **Datum und Uhrzeit** müssen Sie Datum und Uhrzeit auf der Appliance festlegen. Weitere Informationen finden Sie unter [Datum und Uhrzeit festlegen](#).

☰

Citrix SD-WAN

Dashboard

Basic Settings

Management & DNS

Interface Settings

Date & Time

Advanced Settings

Monitoring

Diagnostics

System Maintenance

Date/Time Settings

If the Appliance date/time is turned back due to NTP or manual changes, reporting artifacts may occur.

NTP Settings

☒ Use NTP Server

Server Address

0.pool.ntp.org:1.pool.ntp.org:2.pool.ntp.org:3.pool.ntp.org

Save

Date/Time Settings

May 6, 2020 1:55 PM

Save

Timezone Settings

After changing the timezone setting, a reboot will be necessary for the timezone changes to take full effect.

Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.

Timezone

UTC

Save

RADIUS-Server

Sie können eine SD-WAN-Appliance konfigurieren, um den Benutzerzugriff mit einem oder mehreren RADIUS-Servern zu authentifizieren.

So konfigurieren Sie den RADIUS-Server:

1. Aktivieren Sie das Kontrollkästchen **Radius aktivieren**.
2. Geben Sie die **Server-IP-Adresse** und den **Authentifizierungsport** ein. Es können maximal drei Server-IP-Adressen konfiguriert werden.
3. Geben Sie den **Server-Schlüssel** ein und bestätigen Sie.
4. Geben Sie den **Timeout-Wert** in Sekunden ein.
5. Klicken Sie auf **Speichern**.

Sie können auch die RADIUS-Serververbindung testen. Geben Sie den **Benutzernamen** und **das Kennwort ein**. Klicken Sie auf **Verify**.

RADIUS Server

Server Settings

☒ Enable RADIUS

Server 1 IP Address *

Authentication Port

Server 2 IP Address

Authentication Port

Server 3 IP Address

Authentication Port

Server Key

Confirm Server Key

Timeout(seconds)

Test RADIUS Server Connection

User Name

Password

TACACS+ Server

Sie können einen TACACS+-Server für die Authentifizierung konfigurieren. Ähnlich wie bei der RADIUS-Authentifizierung verwendet TACACS+ einen geheimen Schlüssel, eine IP-Adresse und die Portnummer. Die Standardportnummer ist 49.

So konfigurieren Sie den TACACS+-Server:

1. **Aktivieren Sie das Kontrollkästchen Enable TACACS+.**
2. Geben Sie die **Server-IP-Adresse** und den **Authentifizierungsport** ein. Es können maximal drei Server-IP-Adressen konfiguriert werden.
3. Wählen Sie **PAP** oder **ASCII** als Authentifizierungstyp aus.
 - PAP: Verwendet PAP (Password Authentication Protocol), um die Benutzerauthentifizierung zu stärken, indem dem TACACS+-Server ein starkes gemeinsames Geheimnis zugewiesen wird.
 - ASCII: Verwendet ASCII-Zeichensatz, um die Benutzerauthentifizierung zu stärken, indem dem TACACS+-Server ein starkes gemeinsames Geheimnis zugewiesen wird.
4. Geben Sie den **Server-Schlüssel** ein und bestätigen Sie.
5. Geben Sie den **Timeout-Wert** in Sekunden ein.
6. Klicken Sie auf **Speichern**.

Sie können auch die TACACS+-Serververbindung testen. Geben Sie den **Benutzernamen** und **das Kennwort ein**. Klicken Sie auf **Verify**.

TACACS+ Server

Settings

☒ Enable TACACS+

Server 1 IP Address *

Authentication Port

10.10.10.10

49

Server 2 IP Address

Authentication Port

Server 3 IP Address

Authentication Port

Authentication Type ☐ PAP ☒ ASCII

Server Key

Confirm Server Key

Timeout(seconds)

Save

Test TACACS+ Server Connection

User Name

test user

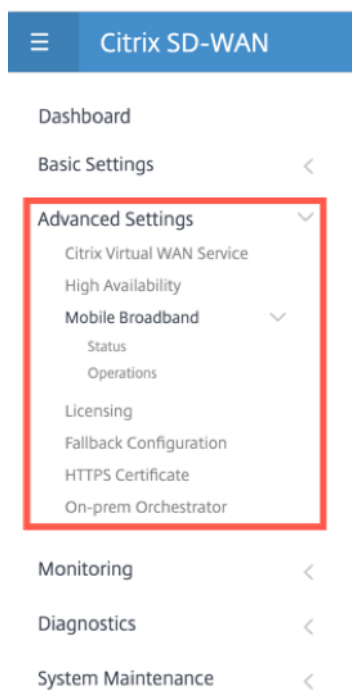
Password

Verify

Erweiterte Einstellungen

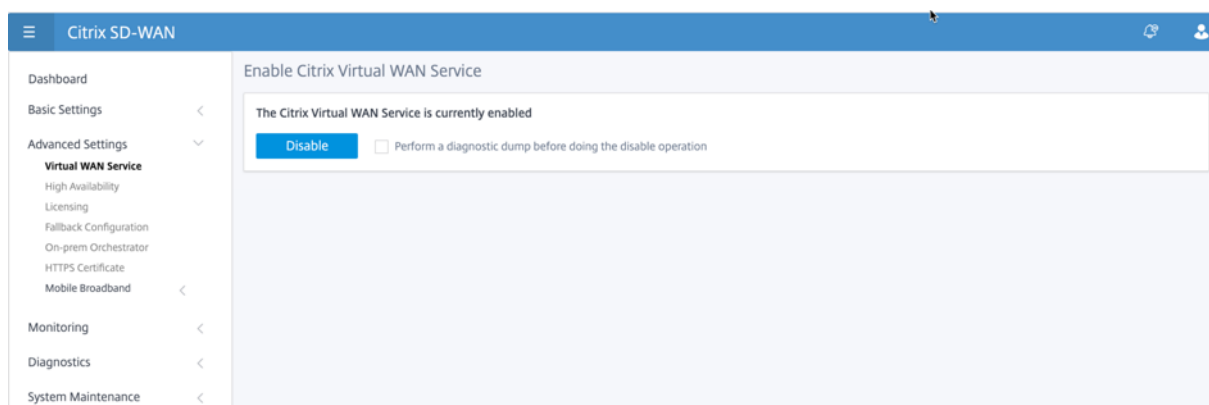
Die **erweiterten SD-WAN-Appliance-Einstellungen** enthalten die folgende Entitätenkonfiguration

- Citrix Virtual WAN-Dienst
- Hohe Verfügbarkeit
- Mobiles Breitband
- Lizenzierung
- Fallback-Konfiguration
- HTTPS-Zertifikat
- On-Prem Orchestrator



Citrix Virtual WAN-Dienst

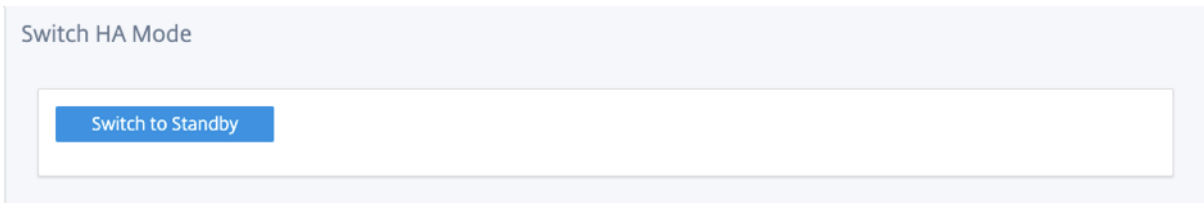
Auf der Seite **Citrix Virtual WAN Service** können Sie den Citrix Virtual WAN Service aktivieren/deaktivieren. Weitere Informationen finden Sie unter [Konfigurieren des virtuellen WAN-Dienstes](#).



Hohe Verfügbarkeit

Auf der Seite **“Hohe Verfügbarkeit”** können Sie zwischen aktivem und Standbystatus für ein SD-WAN High Availability (HA) -Setup umschalten. Der Hochverfügbarkeitsstatus ist im Dashboard verfügbar (wenn Hochverfügbarkeit konfiguriert ist). Weitere Informationen finden Sie unter [Hochverfügbarkeitsmodus](#).

Switch HA Mode

A screenshot of a web interface titled "Switch HA Mode". It features a single blue button with the text "Switch to Standby" centered within a light gray rectangular frame.

Mobiles Breitband

Die Citrix SD-WAN-Appliances wie die Citrix SD-WAN 210 SE LTE und 110 LTE Wi-Fi-Geräte verfügen über ein integriertes internes LTE-Modem. Sie können auch ein externes 3G/4G-USB-Modem auf den folgenden Citrix SD-WAN Geräten anschließen.

- 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 und NCM sind die drei unterstützten externen USB-Modems.

Weitere Informationen zum Konfigurieren von LTE mit der Legacy-GUI finden Sie im folgenden Thema:

- [Konfigurieren der LTE-Funktionalität auf 210 SE LTE-Appliance](#)
- [Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Appliance](#)
- [Konfigurieren eines externen USB-LTE-Modems](#)

Legen Sie bei einem internen LTE-Modem die SIM-Karte in den SIM-Kartensteckplatz der Citrix SD-WAN Appliance ein. Befestigen Sie die Antennen an der Citrix SD-WAN Appliance. Weitere Informationen finden Sie unter [Installieren der LTE-Antennen](#) und Einschalten des Geräts.

Hinweis:

Die Citrix SD-WAN 110-LTE-WiFi-Appliance verfügt über zwei Standard-SIM-Steckplätze (2FF). Verwenden Sie einen SIM-Adapter, um SIMs der Größe Micro (3FF) und Nano (4FF) zu verwenden. Schnappen Sie die kleinere SIM in den Adapter ein. Sie können den Adapter von Citrix als Field Replaceable Unit (FRU) oder vom SIM-Anbieter beziehen. Hot-Swapping von SIM für das interne LTE-Modem wird nur auf der Citrix SD-WAN 110-LTE-WiFi-Appliance unterstützt.

Perquisites für externes LTE-Modem:

- Verwenden Sie die unterstützten USB LTE Dongles. Die unterstützten Dongle-Hardwaremodelle sind Verizon USB730L und AT & T USB800.
- Stellen Sie sicher, dass eine SIM-Karte in den USB-LTE-Dongle eingelegt ist. Die CDC Ethernet LTE Dongles sind mit einer statischen IP-Adresse vorkonfiguriert, dies stört die Konfiguration

und verursacht Verbindungsfehler oder intermittierende Verbindung, wenn die SIM-Karte nicht eingelegt ist.

- Bevor Sie einen CDC Ethernet LTE-Dongle in die SD-WAN-Appliance einsetzen, schließen Sie den externen USB-Stick an einen Windows/Linux-Computer an und stellen Sie sicher, dass das Internet mit der richtigen APN- und Mobile Data Roaming-Konfiguration ordnungsgemäß funktioniert. Stellen Sie sicher, dass der **Verbindungsmodus** des USB-Dongle vom Standardwert **Manuell** auf **Auto** geändert wird.

Hinweis

- Die Citrix SD-WAN Appliances unterstützen jeweils nur einen USB-LTE-Dongle. Wenn mehr als ein USB-Dongle angeschlossen ist, ziehen Sie alle Dongles ab und stecken Sie nur einen Dongle an.
- Die Citrix SD-WAN Appliances unterstützen keinen Benutzernamen und kein Kennwort für USB-Modems. Stellen Sie sicher, dass die Benutzernamen- und Kennwortfunktion auf dem Modem während der Installation deaktiviert sind.
- Das Entfernen oder Neustarten eines externen MBIM-Dongles wirkt sich auf die interne LTE-Modem-Datensitzung aus. Dies ist ein erwartetes Verhalten.
- Wenn ein externes LTE-Modem angeschlossen ist, dauert die SD-WAN-Appliance etwa 3 Minuten, um es zu erkennen.

Um den Status des mobilen Breitbandnetzes anzuzeigen, wählen Sie den Modemtyp aus.

Dashboard
Basic Settings
Advanced Settings
Virtual WAN Service
High Availability
Mobile Broadband
Status
Operations
Licensing
Fallback Configuration
HTTPS Certificate
On-prem Orchestrator
Monitoring
Diagnostics
System Maintenance

Mobile Broadband Status

Modem Type
Status Of

Internal Modem
Device

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

Im Folgenden finden Sie einige nützliche Statusinformationen:

- **Modemtyp:** Wählen Sie den Modemtyp als Extern oder Intern aus. Internes Modem zeigt den Status auf der Seite **Mobiles Breitband > Status** an. Alle anderen Abschnitte wie SIM-Einstellung, APN-Einstellungen, Modem aktivieren/deaktivieren, Neustart-Modem und Refresh SIM sind auf der Seite **Mobiles Breitband > Vorgänge** verfügbar.
- **Aktive SIM:** Zu einem bestimmten Zeitpunkt kann nur eine SIM aktiv sein. Zeigt die aktuell aktive SIM an.
- **Betriebsart:** Zeigt den Modemstatus an.
- **SIM-Funktionen:** Zeigt an, ob die SIM unterstützt wird oder nicht.
- **Modell:** Zeigt den Namen des Moduls für mobiles Breitband an

Wenn Sie das **externe** Modem auswählen, wird der Status des externen Modems angezeigt. Wenn das externe Modem jedoch nicht konfiguriert ist, wird eine Warnmeldung angezeigt, da das **ausgewählte Modem auf diesem Gerät nicht konfiguriert ist**.

Geräteinformationen für externes CDC Ethernet-Modem.

| Mobile Broadband Status | |
|-------------------------|------------------|
| Modem Type | Status Of |
| External Modem | Device |
| Status | |
| Product ID | 9030 |
| Vendor ID | 1410 |
| Manufacturer | Novatel Wireless |
| Product | MIPI USB730L |

Geräteinformationen für externe MBIM- und NCM-Modems. Im Feld **Modemmodus** wird der Typ des externen Dongle angezeigt.

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

SIM-Details werden nur für externe MBIM- und NCM-Modems angezeigt.

Mobile Broadband Status

Modem Type

External Modem

Status Of

SIM One

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

mobiler Breitbandbetrieb Vorgänge, die auf internen und externen Modems unterstützt werden:

| Vorgänge | Internes Modem | Externes Modem - CDC Ethernet | Externes Modem - MBIM und NCM |
|---------------|--|-------------------------------|-------------------------------|
| SIM-Präferenz | Ja - Für Geräte, die Dual-SIM unterstützen | Nein | Nein |
| SIM-PIN | Ja | Nein | Nein |

| Vorgänge | Internes Modem | Externes Modem - CDC Ethernet | Externes Modem - MBIM und NCM |
|-------------------------------|----------------|-------------------------------|-------------------------------|
| APN-Einstellungen | Ja | Nein | Ja |
| Netzwerkeinstellungen | Ja | Nein | Nein |
| Roaming | Ja | Nein | Nein |
| Firmware verwalten | Ja | Nein | Nein |
| Modem aktivieren/deaktivieren | Ja | Nein | Ja |
| Modem neu starten | Ja | Nein | Nein |
| SIM aktualisieren | Ja | Nein | Nein |

SIM-Präferenz Sie können Dual-SIMs auf einer Citrix SD-WAN 110-LTE-WiFi-Appliance einfügen. Zu einem bestimmten Zeitpunkt ist nur eine SIM aktiv. Wählen Sie die **SIM-Einstellung** aus:

- **SIM One bevorzugt:** Wenn zwei SIMs eingelegt sind, verwendet das LTE-Modem beim Hochfahren SIM One, falls verfügbar. Wenn das LTE-Modem eingeschaltet ist und läuft, verwendet es die SIM (SIM One oder SIM Two), die in diesem Moment verwendet wird, und wird es weiterhin verwenden, bis die SIM aktiv ist.
- **SIM Two bevorzugt:** Wenn zwei SIMs eingelegt sind, verwendet das LTE-Modem beim Hochfahren SIM Two, falls verfügbar. Wenn das LTE-Modem eingeschaltet ist und läuft, verwendet es die SIM (SIM One oder SIM Two), die in diesem Moment verwendet wird, und wird es weiterhin verwenden, bis die SIM aktiv ist.
- **SIM Eins:** Es wird nur SIM One verwendet, unabhängig vom SIM-Zustand auf beiden SIM-Steckplätzen. SIM One ist immer aktiv.
- **SIM Two:** Es wird nur SIM Two verwendet, unabhängig vom SIM-Status auf beiden SIM-Steckplätzen. SIM Two ist immer aktiv.

Hinweis

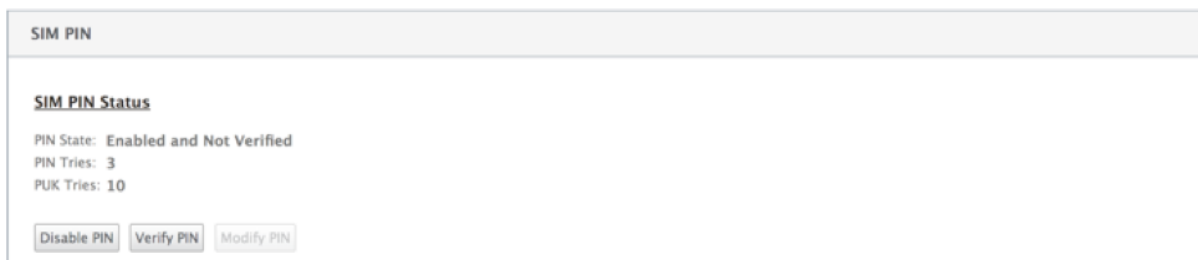
Die Option SIM-Einstellung ist für das Citrix SD-WAN 210-SE LTE Wi-Fi-Gerät nicht verfügbar, da es nur einen SIM-Kartensteckplatz hat.

The screenshot shows a web-based configuration interface for 'SIM Preference'. At the top, it says 'SIM Preference'. Below that, there's a label 'Preferred SIM' followed by a dropdown menu. The dropdown menu currently shows 'SIM Two' and has a small downward arrow on the right. Below the dropdown is a blue button with the text 'Apply' in white.

SIM-PIN

Wenn Sie eine SIM-Karte eingelegt haben, die mit einer PIN gesperrt ist, befindet sich der SIM-Status im Status **Aktiviert und Nicht überprüft**. Sie können die SIM-Karte erst verwenden, wenn sie mit der SIM-PIN verifiziert wurde. Sie können die SIM-PIN vom Anbieter erhalten.

Um SIM-PIN-Vorgänge auszuführen, navigieren Sie zu **Erweiterte Einstellungen > Mobiles Breitband > Vorgänge > SIM-PIN-Status**.



SIM PIN

SIM PIN Status

PIN State: Enabled and Not Verified

PIN Tries: 3

PUK Tries: 10

[Disable PIN](#) [Verify PIN](#) [Modify PIN](#)

Sie können die folgenden Vorgänge ausführen:

- **SIM-PIN überprüfen:** Klicken Sie auf **Überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Verifizieren**. Der Status ändert sich in **Aktiviert und Verifiziert**.
- **SIM-PIN aktivieren:** Sie können die SIM-PIN für eine SIM-PIN aktivieren, bei der die SIM-PIN Klicken Sie auf **Aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**. Wenn sich der SIM-PIN-Status in **Aktiviert und Nicht überprüft** ändert, bedeutet dies, dass die PIN nicht überprüft wird und Sie erst dann LTE-bezogene Vorgänge ausführen können, wenn die PIN überprüft wurde. Klicken Sie auf **Verify**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Verifizieren**.
- **SIM-PIN deaktivieren:** Sie können die SIM-PIN-Funktion für eine SIM-PIN deaktivieren, für die die SIM-PIN aktiviert und verifiziert ist. Klicken Sie auf **Deaktivieren**. Geben Sie die SIM-PIN ein und klicken Sie auf **De**
- **SIM-PIN ändern:** Sobald sich die PIN im Status Aktiviert und Verifiziert befindet, können Sie die PIN ändern. Klicken Sie auf **Ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **Ändern**.
- **SIM entsperren** - Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe des vom Mobilfunk-anbieters erhaltenen SIM-PUK zurücksetzen. Um die Blockierung einer SIM aufzuheben, klicken Sie auf **Sperre aufheben**. Geben Sie die vom Mobilfunk-anbieter erhaltene SIM-PIN und SIM PUK ein und klicken Sie auf **Entsperren**

Hinweis

Die SIM-Karte wird mit 10 erfolglosen PUK-Versuchen dauerhaft blockiert, während die SIM-Karte entsperrt wird. Wenden Sie sich an den Mobilfunk-anbieter, um eine neue SIM-

Karte zu erhalten.

APN-Einstellungen

1. Um die APN-Einstellungen zu konfigurieren, navigieren Sie zu **Erweiterte Einstellungen > Mobiles Breitband > Operationen** und gehen Sie zum Abschnitt **APN-Einstellungen**.

Hinweis

Rufen Sie die APN-Informationen vom Mobilfunkanbieter ab.

2. Wählen Sie die SIM-Karte aus und geben Sie den **APN, den Benutzernamen, das Kennwort** und die vom Mobilfunkanbieter bereitgestellte **Authentifizierung** ein. Sie können zwischen PAP, CHAP, PAPCHAP Authentifizierungsprotokollen wählen. Wenn der Anbieter keinen Authentifizierungstyp angegeben hat, setzen Sie ihn auf **Keine**.

Hinweis

Alle diese Felder sind optional.

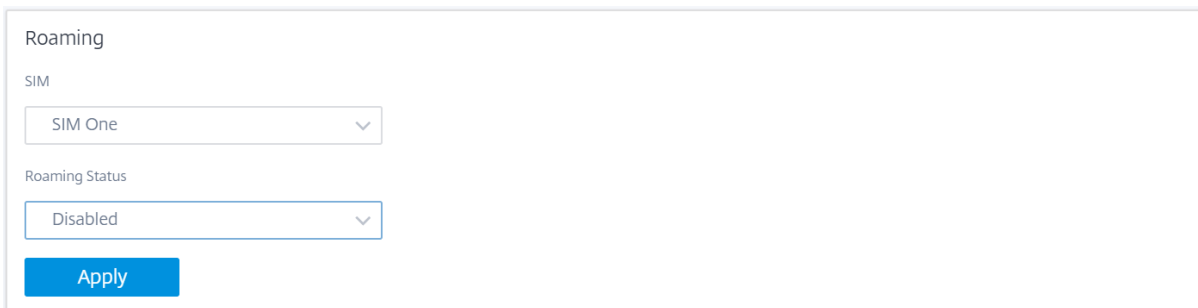
3. Klicken Sie auf **Apply**.

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

Netzwerkeinstellungen Sie können das Mobilfunknetz auf Citrix SD-WAN Appliances auswählen, die das interne LTE-Modem unterstützen. Die unterstützten Netzwerke sind 3G, 4G oder beides.

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

Roaming Die Roaming-Option ist standardmäßig auf Ihren LTE-Appliances aktiviert. Sie können sie deaktivieren.



Roaming

SIM

SIM One

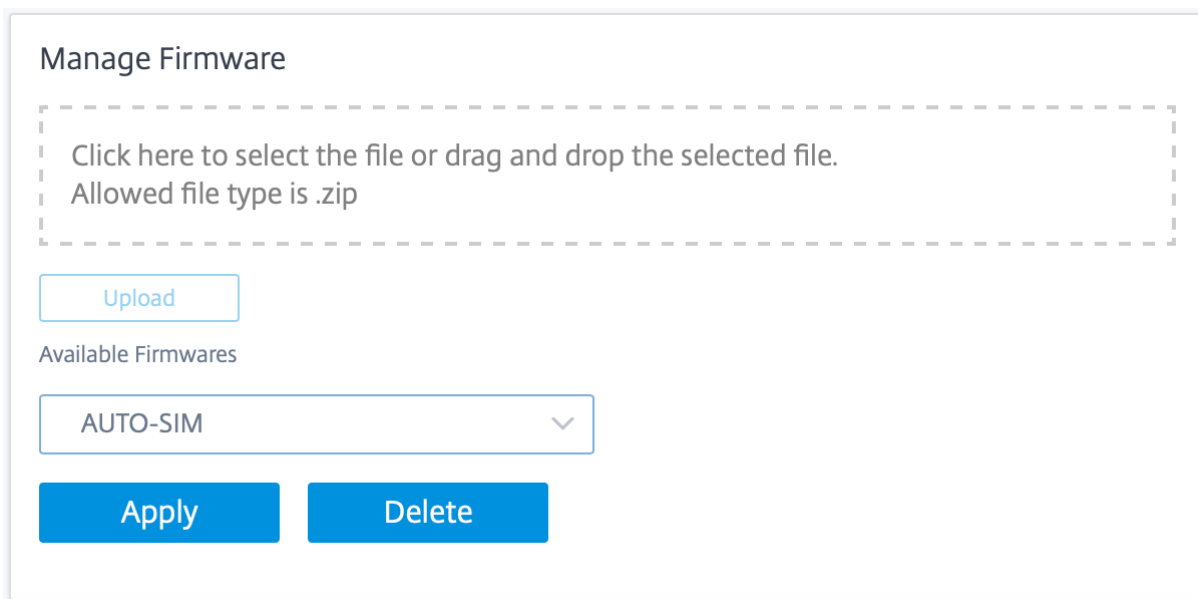
Roaming Status

Disabled

Apply

Firmware verwalten

Jede LTE-fähige Appliance verfügt über eine Reihe von Firmware. Sie können aus der vorhandenen Firmware-Liste auswählen oder eine Firmware hochladen und anwenden. Wenn Sie sich nicht sicher sind, welche Firmware Sie verwenden sollen, wählen Sie die Option **AUTO-SIM**. Mit der AUTO-SIM-Option kann das LTE-Modem basierend auf der eingesteckten SIM-Karte die am besten passende Firmware auswählen.



Manage Firmware

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


Upload

Available Firmwares

AUTO-SIM

Apply Delete

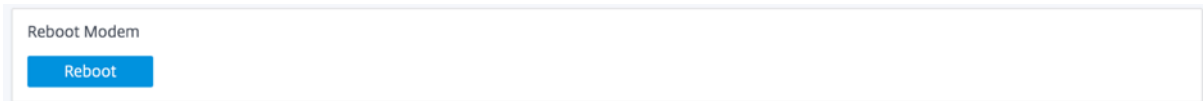
Modem aktivieren/deaktivieren Aktivieren/deaktivieren Sie das Modem abhängig von Ihrer Absicht, die LTE-Funktionalität zu verwenden. Standardmäßig ist das LTE-Modem aktiviert.



Enable/Disable Modem

Enable

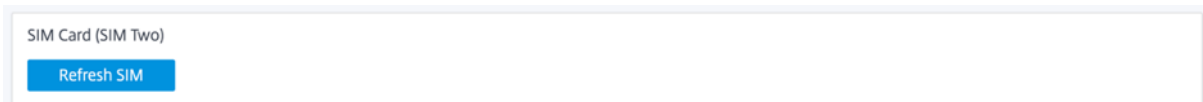
Modem neu starten Startet das Modem neu. Es kann bis zu 7 Minuten dauern, bis der Neustartvorgang abgeschlossen ist.



SIM aktualisieren Verwenden Sie die Option **SIM aktualisieren**, wenn die SIM-Karte vom LTE-WLAN-Modem nicht ordnungsgemäß erkannt wird.

Hinweis

Der Vorgang “SIM-Aktualisierung” gilt nur für die aktive SIM.



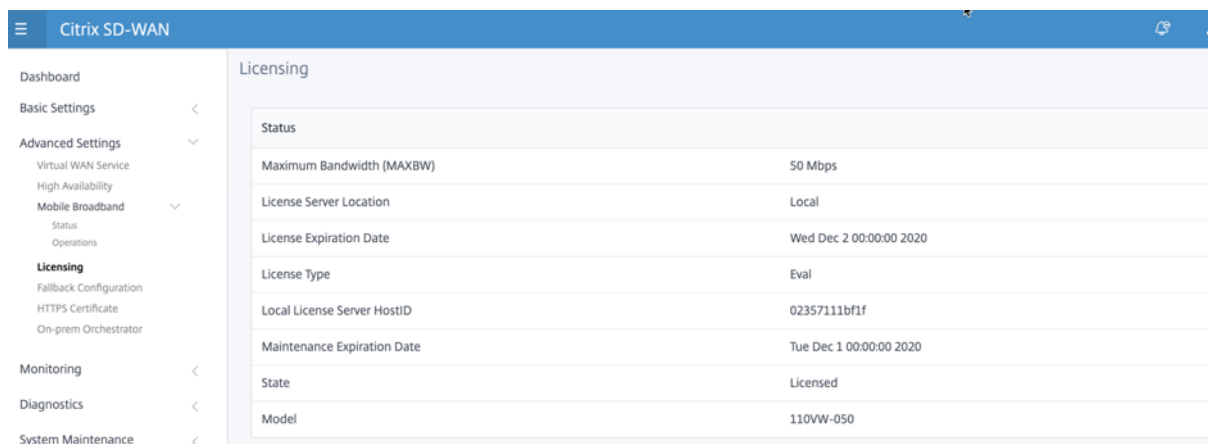
Mit dem Citrix SD-WAN Center können Sie alle LTE-Sites in Ihrem Netzwerk remote anzeigen und verwalten. Weitere Informationen finden Sie unter [Remote-LTE-Standortverwaltung](#).

Weitere Informationen zur LTE-Konfiguration finden Sie unter [Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Geräten](#) und [Konfigurieren der LTE-Funktionalität auf 210 SE LTE-Geräten](#).

Informationen zur Konfiguration eines externen LTE-Modems finden Sie unter [Konfigurieren eines externen USB-LTE-Modems](#).

Lizenzierung

Auf der Seite “**Lizenzierung**” werden die Lizenzdetails wie Serverstandort, Modell, Lizenztyp usw. angezeigt.



Hinweis Wenn Sie

eine Lizenz vom SD-WAN Center installieren und anwenden, stellen Sie sicher, dass Ihre spezifische Appliance die SD-WAN-Appliance-Edition unterstützt, die Sie aktivieren möchten, und dass Sie die richtige Softwareversion zur Verfügung haben.

Fallback-Konfiguration

Auf der Seite **Fallback-Konfiguration** werden die gespeicherten Fallback-Konfigurationsdaten angezeigt. Wenn die Fallback-Konfiguration deaktiviert ist, können Sie sie aktivieren, indem Sie den Schalter **Fallback-Konfiguration aktivieren aktivieren**.

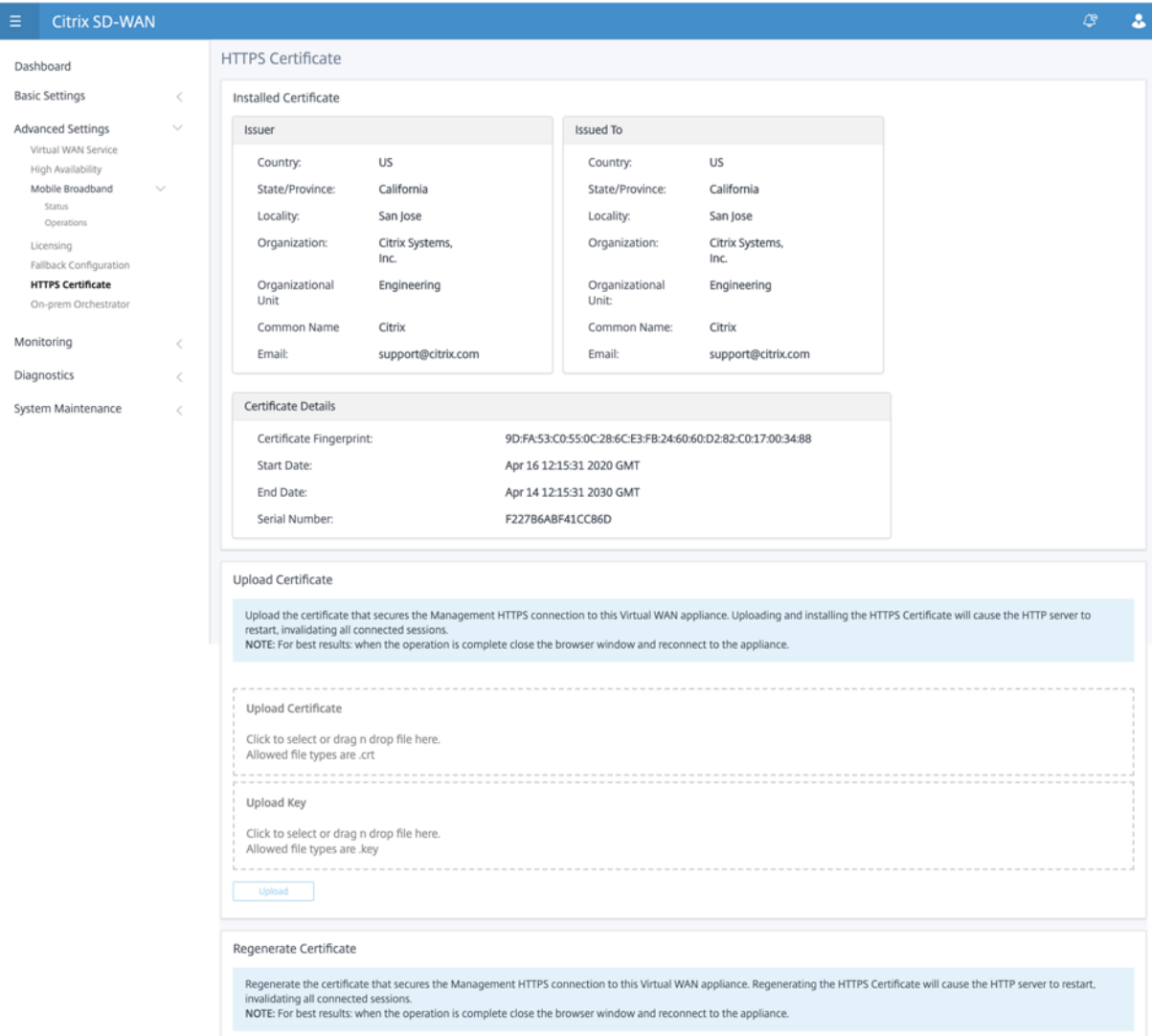
The screenshot displays the 'Fallback Configuration' page in the Citrix SD-WAN interface. The left sidebar contains navigation links: Dashboard, Basic Settings, Advanced Settings (with sub-links for Virtual WAN Service, High Availability, Mobile Broadband, Status, and Operations), Licensing, Fallback Configuration (selected), HTTPS Certificate, On-prem Orchestrator, Monitoring, Diagnostics, and System Maintenance. The main content area is titled 'Fallback Configuration' and includes a description: 'The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.' Below this is a toggle switch for 'Enable Fallback Configuration' (currently turned on) and a 'Reset' button. The 'WAN Settings' section states: 'WAN settings are currently not configurable. WAN ports are configured as independent WAN Links using DHCP client and monitor the Quad9 DNS service to determine WAN connectivity.' The 'LAN Settings' section includes fields for VLAN ID (0), IP Address (192.168.0.1/24), DHCP Start (192.168.0.50), DHCP End (192.168.0.250), DNS Server (9.9.9.9), and Alt DNS Server (149.112.112.112). There is also a checkbox for 'Internet Access'. The 'Port Settings' section includes a table for configuring ports (1/1, 1/2, 1/3, 1/4-MGMT, LTE-1, LTE-E1) with modes (WAN, LAN, Disabled) and IP addresses (9.9.9.9). The 'Unassigned Port Bypass Mode' is set to 'Fail to Block'.

Weitere Informationen finden Sie unter [Fallback-Konfiguration](#).

HTTPS-Zertifikat

HTTPS-Zertifikat ist erforderlich, um eine gesicherte Verbindung herzustellen. Auf der Seite “**HTTPS-Zertifikat**“ werden die Details des bereits installierten HTTPS-Zertifikats angezeigt. Weitere Informa-

tionen finden Sie unter [HTTPS-Zertifikate](#).



On-Prem Orchestrator (Ziel für die Zukunft)

Citrix On-Prem SD-WAN Orchestrator ist die lokale Softwareversion des Citrix SD-WAN Orchestrator Diensts. Citrix On-Prem SD-WAN Orchestrator bietet eine einzige Glasverwaltungsplattform für Citrix Partner zur zentralen Verwaltung mehrerer Kunden mit geeigneten rollenbasierten Zugriffskontrollen.

Sie können eine Verbindung zwischen der Citrix SD-WAN Appliance und dem Citrix On-Prem SD-WAN Orchestrator herstellen, indem Sie die Orchestrator-Konnektivität aktivieren und die On-Prem SD-WAN Orchestrator-Identität angeben.

Hinweis

- Die **On-Prem SD-WAN Orchestrator-Konfiguration auf der SD-WAN-Appliance-Funktion** ist ein Enabler für Citrix On-Prem SD-WAN Orchestrator. Die Citrix On-Prem SD-WAN Orchestrator Konfiguration auf dem SD-WAN-Gerät ist derzeit nicht verfügbar, sie ist für eine zukünftige Version vorgesehen.
- Die Zero-Touch-Bereitstellung funktioniert nicht, wenn die **On-prem SD-WAN Orchestrator-Konfiguration auf der SD-WAN-Appliance-Funktion** auf den SD-WAN-Appliances konfiguriert ist.

So aktivieren Sie die Orchestrator-Konnektivität:

1. Navigieren Sie in der Appliance-GUI zu **Erweiterte Einstellungen > On-prem Orchestrator > Identity**.
2. **Aktivieren Sie das Kontrollkästchen On-Prem SD-WAN Orchestrator-Konnektivität** aktivieren.

3. Geben Sie entweder die On-prem SD-WAN Orchestrator IP-Adresse oder Domäne oder beide (IP-Adresse und Domäne) für die Konfiguration ein.

Wenn der Kunde nur Domäne konfiguriert, muss er sicherstellen, dass DNS-Eintrag in seinem lokalen DNS-Server hinzugefügt wird, und die DNS-Server-IP-Adresse auf SD-WAN-Appliances konfigurieren. Um zu konfigurieren, navigieren Sie zu **Konfiguration > Netzwerkadapter > IP-Adresse**.

Wenn beispielsweise die On-Prem SD-WAN Orchestrator Domäne als citrix.com konfiguriert ist, müssen Sie im DNS-Server einen DNS-Eintrag für den folgenden FQDN und die On-Prem SD-WAN Orchestrator-IP-Adresse erstellen:

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

Im Falle einer erweiterten Konfiguration:

Beispiel: Wenn die On-prem Orchestrator-Domäne als **citrix.com** konfiguriert ist, wird die Download Management Service Domain als **download.citrix.com** konfiguriert, und die Statistics Management Service Domain ist als **statistics.citrix.com** konfiguriert. Dann müssen Sie einen DNS-Eintrag im DNS-Server für den folgenden FQDN und die entsprechende IP-Adresse erstellen:

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

On-Prem Orchestrator unterstützt möglicherweise die Ausführung von Diensten wie Download, Statistiken über unabhängige Serverinstanzen, um eine bessere Skalierbarkeit für große Netzwerke zu ermöglichen. Sie können die **erweiterte Konfiguration** auswählen und den **Download-Verwaltungsdienst und den Statistik-Verwaltungsdienst** konfigurieren.

Aktivieren Sie das Kontrollkästchen **Erweiterte Konfiguration** und geben Sie die folgenden Details an:

- **Download Management Service IP/Domain:** Geben Sie die IP-Adresse /domäne an, mit der Sie SD-WAN-Software und Konfigurationsdownloadaspekte auf eine unabhängige Serverinstanz auslagern können, um eine bessere Skalierbarkeit für große Netzwerke zu ermöglichen.
- **Statistic Management Service IP/Domain:** Stellen Sie die IP-Adresse/Domäne bereit, die die Erfassung und Verwaltung von SD-WAN-Statistiken von Geräten auf eine unabhängige Serverinstanz auslagert, um eine bessere Skalierbarkeit für große Netzwerke zu ermöglichen.

4. Klicken Sie auf **Apply**.

Um die SD-WAN-Appliance oder das On-Prem SD-WAN Orchestrator-Zertifikat zu regenerieren, herunterzuladen und hochzuladen, navigieren Sie zu **Erweiterte Einstellungen > On-prem Orchestrator > Zertifikat**.

Wenn der On-prem **Orchestrator-Authentifizierungstyp** deaktiviert ist, kann sich die Appliance entweder über **Keine Authentifizierung oder über die einseitige Authentifizierung** oder den **Zwei-Wege-Authentifizierungsmodus** mit dem On-Prem Orchestrator verbinden.

Wenn der On-prem **Orchestrator-Authentifizierungstyp** aktiviert ist, kann sich die Appliance nur über die **Zwei-Wege-Authentifizierung** mit dem On-prem Orchestrator verbinden.

Beim Deaktivieren des **Authentifizierungstyps** in On-prem Orchestrator vom Enable-Status wird vorhandene Geräte im Einweg-Authentifizierungsmodus in den Status "Getrennt" versetzt.

Kunden müssen den Authentifizierungstyp der Appliance in Zwei-Wege-Authentifizierung ändern und das SD-WAN-Appliance-Zertifikat in den On-Prem Orchestrator hochladen, um es zu verbinden.

Hinweis

- Generierte Zertifikate sind selbstsignierte X509-Zertifikate.
- Der Kunde muss die Zertifikate neu generieren, wenn das Zertifikat abgelaufen oder gefährdet ist.
- Die Gültigkeit des Zertifikats beträgt 10 Jahre.
- Sie können die Zertifikatdetails wie Fingerabdruck, Startdatum und Enddatum anzeigen
- Der Kunde muss sicherstellen, dass die Zertifikate neu generiert und zwischen On-Prem Orchestrator und SD-WAN-Appliance ausgetauscht werden, um den Verlust der Appliance-Konnektivität mit On-Prem Orchestrator zu vermeiden.

5. Wählen Sie den **Authentifizierungstyp** Im Folgenden werden die Authentifizierungstypen aufgeführt, die zwischen der SD-WAN-Appliance und der On-Prem SD-WAN Orchestrator Konnektivität unterstützt werden:

- **Keine Authentifizierung** —Keine Authentifizierung zwischen dem On-prem SD-WAN Orchestrator und der SD-WAN Appliance, und es ist nicht erforderlich, die SD-WAN Appliance oder das On-prem SD-WAN Orchestrator-Zertifikat zu verwenden. Sie können diese Option jedoch verwenden, wenn Sie über ein sicheres Netzwerk wie MPLS verfügen.

Secure Connectivity

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

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

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

Authentication Type

No Authentication

Apply

- **Einseitige Authentifizierung** —Bei Auswahl des Typs “Einseitige Authentifizierung” müssen Sie das On-prem Orchestrator-Zertifikat hochladen. Laden Sie den On-Prem Orchestrator aus dem On-Prem Orchestrator herunter und klicken Sie auf Hochladen. Die SD-WAN-Appliance vertraut dem On-Prem Orchestrator mithilfe der hochgeladenen Zertifikate.

Secure Connectivity

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

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

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

Authentication Type

One-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

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

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

Upload

- **Zwei-Wege-Authentifizierung** —On-prem Orchestrator- und Appliance-Zertifikate müssen untereinander ausgetauscht werden. Für die **Zwei-Wege-Authentifizierung** müssen Sie das SD-WAN-Appliance-Zertifikat auf den On-Prem Orchestrator regenerieren, herunterladen und hochladen. Die SD-WAN-Appliance und On-Prem Orchestrator vertrauen einander mithilfe der ausgetauschten Zertifikate.

Secure Connectivity

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

Authentication Type
 Two-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

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

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

Upload

SD-WAN Appliance Certificate

Certificate Details:

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

Regenerate Download

Hinweis

Es wird empfohlen, nur Unidirektionale Authentifizierung oder Zwei-Wege-Authentifizierung zu verwenden. Wenn keine Authentifizierung vorhanden ist, müssen Sie den sicheren DNS-Server auswählen.

Um die lokale SD-WAN Orchestrator-Konnektivität zu deaktivieren, deaktivieren Sie **On-prem SD-WAN Orchestrator-Konnektivität aktivieren** und klicken Sie auf **Übernehmen**. Um On-Prem Orchestrator-verwaltetes Netzwerk entweder in Cloud Orchestrator- oder MCN Managed Network zu konvertieren, müssen Sie On-Prem SD-WAN Orchestrator Konnektivität deaktivieren und die Konfiguration zurücksetzen. Um die Konfiguration zurückzusetzen, navigieren Sie zu **Konfiguration > Systemwartung > Configuration Reset**.

Upgrade und Downgrade

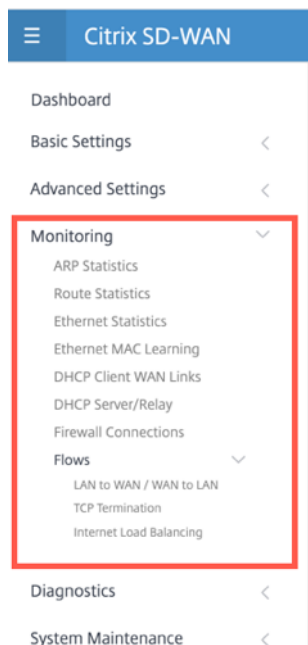
- Nach dem Upgrade der SD-WAN-Appliance von 11.1.1/11.2.0/10.2.7 auf Version 11.2.1 müssen Sie sowohl Appliance-Zertifikate als auch On-Prem Orchestrator-Zertifikate austauschen.
- Nach dem Downgrade der SD-WAN-Appliance von 11.2.1 auf 11.1.1/11.2.0/10.2.7 müssen Sie

die Identitätseinstellungen erneut auf der Benutzeroberfläche der Citrix SD-WAN Appliance anwenden. Wenn Probleme mit der On-Prem SD-WAN Orchestrator Konfiguration oder der Konnektivität der SD-WAN-Appliance auftreten, deaktivieren Sie die On-Prem SD-WAN Orchestrator Konnektivität, und aktivieren Sie dann die On-Prem SD-WAN Orchestrator-Konnektivität erneut.

Der On-prem SD-WAN Orchestrator-Authentifizierungstyp muss deaktiviert sein, um die SD-WAN-Appliances mit der 10.2.7/11.1.1/11.2.0-Softwareversion zu verwalten.

Überwachen

Im Abschnitt Überwachung können Sie die Statistiken zu **Address Resolution Protocol (ARP)**, **Route**, **Ethernet**, **Ethernet**, Ethernet sowie **WAN-Verbindungen für DHCP-Clients**, **DHCP Server/Relay**, **Firewall Connections** und **Flows** anzeigen.



- **ARP-, Routen-, Ethernet- und Ethernet-MAC-Statistiken:** Sie können die Statistikinformationen für ARP, Route, Ethernet und Ethernet MAC anzeigen. Mithilfe der Statistikinformationen können Sie alle Datenverkehrs- oder Schnittstellenfehler überprüfen. Weitere Informationen finden Sie unter [Anzeigen statistischer Informationen](#).
- **DHCP-Client-WAN-Links:** Die DHCP-Client-WAN-Links-Seite enthält den Status erlernter IPs. Sie können die Verlängerung der IP beantragen, wodurch die Leasingzeit aktualisiert wird. Sie können auch die **Erneuerung freigeben**, die eine neue IP-Adresse mit einer neuen Lease ausgibt. Weitere Einzelheiten finden Sie unter [Überwachen von WAN-Verbindungen von DHCP-Clients](#).

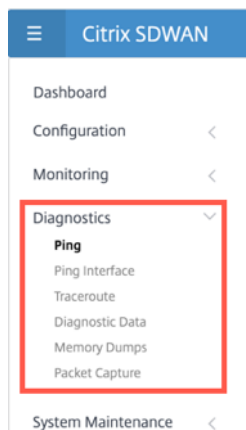
- **DHCP Server/Relay:** Sie können die SD-WAN-Appliance entweder als DHCP-Server oder als DHCP-Relay-Agenten verwenden.
 - Mit der DHCP-Serverfunktion können Geräte im gleichen Netzwerk wie die LAN/WAN-Schnittstelle der SD-WAN-Appliance ihre IP-Konfiguration von der SD-WAN-Appliance abrufen.
 - Mit der DHCP-Relayfunktion können Ihre SD-WAN-Appliances DHCP-Pakete zwischen DHCP-Client und Server weiterleiten.

Weitere Informationen finden Sie unter [DHCP-Server und DHCP-Relay](#).

- **Firewall-Verbindungen:** Die Seite **“Firewall-Verbindungen“** enthält die Firewall-Verbindungsstatistik. Sie können sehen, wie die Firewall-Richtlinien auf den Datenverkehr für jede Anwendung wirken. Weitere Informationen finden Sie unter [Anzeigen von Firewall-Statistiken](#).
- **Flows:** Der Abschnitt **“Flows“** enthält grundlegende Anweisungen zum Anzeigen von Virtual WAN-Flow-Informationen. Weitere Einzelheiten finden Sie unter [Anzeigen von Flow-Informationen](#).

Diagnose

Der Abschnitt **“Diagnose“** enthält die Optionen zum Testen und Untersuchen von Konnektivitätsproblemen. Weitere Informationen finden Sie unter [Diagnose](#).



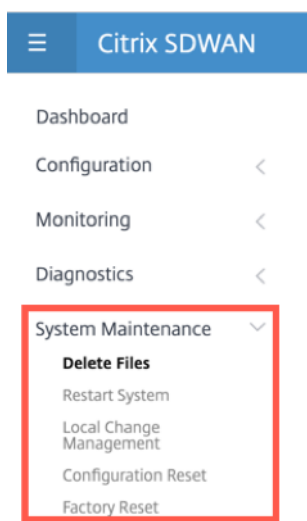
Hinweis

Für die Citrix SD-WAN 110 Appliance kann jeweils nur ein Diagnosepaket vorhanden sein. Für die Citrix SD-WAN 210 Appliance sind maximal fünf Diagnosepakete zulässig.

Systemwartung

Verwenden Sie den Abschnitt **Systemwartung**, um Wartungsaktivitäten durchzuführen. Die Seite **“Systemwartung“** enthält die folgenden Optionen:

- **Dateien löschen:** Sie können Protokolldateien, Backupdateien und archivierte Datenbanken löschen. Wählen Sie im Dropdownmenü die Datei aus, die Sie löschen möchten, und klicken Sie auf die Schaltfläche Löschen.
- **System neu starten:** Sie können den virtuellen WAN-Dienst neu starten oder das System neu starten.
- **Local Change Management:** Mit dem **lokalen Change Management-Prozess** können Sie ein neues Appliance-Paket auf diese einzelne Appliance hochladen.
- **Configuration Reset:** Sie können die Konfiguration zurücksetzen. Mit dieser Option werden Benutzerdaten, Protokolle, Verlauf und lokale Konfigurationsdaten auf dieser Appliance gelöscht.
- **Zurücksetzen auf Werkseinstellungen:** Verwenden Sie die Option **Factory** Reset, um die SD-WAN-Appliance auf die ausgelieferte



Hinweis

Alle diese Funktionen sind bereits in der vorhandenen [SD-WAN-Dokumentation](#) ausführlich erläutert.

Systemanforderungen

May 10, 2021

Hardwareanforderungen

Anweisungen für die Installation von SD-WAN-Appliances finden Sie unter [Einrichten der SD-WAN-Appliances](#).

Firmware-Anforderungen

Alle Citrix SD-WAN Appliance-Modelle in einer Virtual WAN-Umgebung müssen dieselbe Citrix SD-WAN Firmware-Version ausführen.

Hinweis

Appliances, auf denen frühere Softwareversionen ausgeführt werden, können keine Virtual Path-Verbindung mit der Appliance herstellen, auf der SD-WAN Version Für weitere Informationen wenden Sie sich bitte an das Citrix Support-Team.

Softwareanforderungen

Einzelheiten zu den Lizenzanforderungen finden Sie unter [Lizenzierung](#).

Browser-Anforderungen

Browser müssen Cookies aktiviert und JavaScript installiert und aktiviert haben.

Das SD-WAN Management Web Interface wird in den folgenden Browsern unterstützt:

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

Unterstützte Browser müssen Cookies aktiviert und JavaScript installiert und aktiviert sein.

Hypervisor

Citrix SD-WAN SE/PE VPX kann auf den folgenden Hypervisoren konfiguriert werden:

- VMware ESXi Server, Version 5.5.0 oder höher.
- Citrix Hypervisor 6.5 oder höher.
- Microsoft Hyper-V 2012 R2 oder höher.
- Linux KVM

Cloud-Plattform

Citrix SD-WAN SE/PE VPX kann auf den folgenden Cloud-Plattformen konfiguriert werden:

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

SD-WAN-Plattformmodelle und Softwarepakete

September 26, 2023

Dieser Abschnitt enthält Informationen zum Herunterladen der Citrix SD-WAN -Softwarepakete.

Hinweis

Bevor Sie die Software herunterladen, müssen Sie eine Citrix SD-WAN -Softwarelizenz erwerben und registrieren. Weitere Informationen finden Sie unter [Lizenzierung](#).

Ein SD-WAN-Appliance-Paket enthält das SD-WAN-Softwarepaket für ein bestimmtes Appliance-Modell, das mit einem bestimmten SD-WAN-Konfigurationspaket geliefert wird. Die beiden Pakete werden zusammen gebündelt und an die Clients verteilt, indem Sie den Assistenten für die **Änderungsverwaltung** im Management-Webinterface verwenden, das auf dem Master Control Node (MCN) ausgeführt wird.

Wenn es sich um eine Erstinstallation handelt, müssen Sie das entsprechende Appliance-Paket auf jeder der Client-Appliances, die sich im SD-WAN-Netzwerk befinden, manuell hochladen, bereitstellen und aktivieren. Wenn Sie die Konfiguration für eine vorhandene SD-WAN-Bereitstellung aktualisieren, verteilt und aktiviert der MCN automatisch das entsprechende Appliance-Paket auf jedem der vorhandenen Clients, wenn die virtuellen Pfade zu den Clients betriebsbereit sind.

Laden Sie die Softwarepakete herunter

Für jedes Appliance-Modell gibt es ein anderes Citrix SD-WAN -Softwarepaket. Sie müssen das entsprechende Softwarepaket für jedes Appliance-Modell herunterladen, das Sie in Ihr Netzwerk aufnehmen möchten.

Um die Citrix SD-WAN -Softwarepakete herunterzuladen, gehen Sie zur URL; [Produkt-Downloads](#). Anweisungen zum Herunterladen der Software finden Sie auf dieser Seite.

Citrix SD-WAN -Softwarepakete

Es gibt ein anderes Citrix SD-WAN -Softwarepaket für jedes unterstützte SD-WAN-Appliance-Modell. Sie müssen das entsprechende Paket für jedes Appliance-Modell erwerben, das Sie in Ihr Netzwerk integrieren möchten.

Unterstützte SD-WAN-Appliance-Modelle

Es gibt drei Hauptkategorien von Citrix SD-WAN Appliances:

- Hardware-Modelle der SD-WAN-Appliance
 - WANOP, Standard Edition und Premium Edition
- Virtuelle SD-WAN VPX Appliances (SD-WAN VPX)
 - Standard Edition und WANOP Edition

Hinweis

Alle SD-WAN-Appliance-Modelle in einer SD-WAN-Umgebung müssen dieselbe SD-WAN-Firmware-Version ausführen. Für weitere Informationen wenden Sie sich bitte an den Citrix SD-WAN Customer Support.

Eine vollständige Beschreibung der SD-WAN-Appliances finden Sie in der SD-WAN-Produktplattform-Edition [Datenblatt](#) auf der Produktdownloadsite.

SD-WAN Standard-Edition-Hardware-Appliances

Citrix SD-WAN Version 11.2 unterstützt die folgenden Hardware-Appliance-Modelle der SD-WAN Standard Edition:

| SD-WAN SE PLATFORM MODEL | ROLE |
|--------------------------|-----------------------------------|
| 110-SE/110-LTE-WiFi | Appliance für kleine Zweigstellen |
| 210-SE/210-SE LTE | Appliance für kleine Zweigstellen |
| 410-SE | Appliance für kleine Zweigstellen |
| 1000-SE | Appliance für kleine Zweigstellen |
| 1100-SE | Appliance für große Zweigstellen |
| 2100-SE | Appliance für große Zweigstellen |

| SD-WAN SE PLATFORM MODEL | ROLE |
|--------------------------|--|
| 4100-SE | Rechenzentrum —Master Control Node (MCN) -Appliance |
| 5100-SE | Rechenzentrum —Master Control Node (MCN) -Appliance |
| 6100-SE | Rechenzentrum —Master Control Node (MCN) -Appliance |

SD-WAN WAN Optimization Hardware-Appliances (SD-WAN WANOP)

Citrix SD-WAN 11.2 unterstützt die folgenden WANOP-Appliance-Modelle (SD-WAN Optimization):

| SD-WAN WANOP PLATFORM MODELS | ROLE |
|------------------------------|-----------------------------------|
| WANOP 800 | Appliance für kleine Zweigstellen |
| WANOP 1000 | Appliance für große Zweigstellen |
| WANOP 2000 | Appliance für große Zweigstellen |
| WANOP 3000 | Appliance für große Zweigstellen |
| WANOP 4100 | Rechenzentrum-Appliance |
| WanOp 5100 | Rechenzentrum-Appliance |

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

Citrix SD-WAN 11.2 unterstützt die folgenden SD-WAN VPX Virtual Appliance-Modelle (VPX-SE):

| SD-WAN VPX-SE PLATFORM MODELS | ROLE |
|-------------------------------|---|
| VPX 20-SE | MCN oder Client-Appliance, kleine Zweigstelle |
| VPX 50-SE | MCN oder Client-Appliance, kleine Zweigstelle |
| VPX 100-SE | MCN oder Client-Appliance, kleine Zweigstelle |
| VPX 200-SE | MCN oder Client-Appliance, kleine Zweigstelle |
| VPX 500-SE | MCN oder Client-Appliance, kleine Zweigstelle |
| VPX 1000-SE | MCN oder Client-Appliance, kleine Zweigstelle |

Weitere Informationen finden Sie in [Voraussetzungen](#) der Citrix SD-WAN Virtual VPX Standard Edition.

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

Citrix SD-WAN 11.2 unterstützt die folgenden SD-WAN WANOP Virtual Appliance-Modelle (VPX-WANOP):

| SD-WAN VPX WANOP PLATFORM MODELS | ROLE |
|----------------------------------|-----------------------------------|
| WANOP VPX-2 | Appliance für kleine Zweigstellen |
| WANOP VPX-6 | Appliance für kleine Zweigstellen |
| WANOP VPX-10 | Appliance für kleine Zweigstellen |
| WANOP VPX-20 | Appliance für kleine Zweigstellen |
| WANOP VPX-50 | Appliance für große Zweigstellen |
| WANOP VPX-100 | Appliance für große Zweigstellen |
| WANOP VPX-200 | Appliance für große Zweigstellen |

Wichtig

In Version 10.1 wird die Enterprise Platform Edition in “Premium Edition umbenannt. “

SD-WAN Premium Edition Hardware-Appliances (SD-WAN PE)

Citrix SD-WAN 11.2 unterstützt die folgenden SD-WAN Premium (Enterprise) Edition Appliance-Modelle (SD-WAN PE):

| SD-WAN EE PLATFORM MODELS | ROLE |
|---------------------------|--|
| 1000-PE | Große Zweigstelle, Rechenzentrum-Appliance |
| 1100-PE | Große Zweigstelle, Rechenzentrum-Appliance |
| 2100-PE | Große Zweigstelle, Rechenzentrum-Appliance |
| 5100-PE | Große Zweigstelle, Rechenzentrum-Appliance |
| 6100-PE | Große Zweigstelle, Rechenzentrum-Appliance |

Upgradepfad

October 28, 2021

Die folgende Tabelle enthält Details zu allen Citrix SD-WAN -Softwareversionen, auf die Sie aktualisieren können, aus den vorherigen Versionen.

| 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 | — | — | — | — | — | ✓ | ✓ | ✓ | ✓ |

Die Informationen zu den Upgradepfaden sind auch im [Citrix Upgrade Guide](#) verfügbar.

Hinweis

- Kunden, die ein Upgrade von Citrix SD-WAN Version 9.3.x durchführen, wird empfohlen, vor dem Upgrade auf eine Hauptversion auf 10.2.8 zu aktualisieren.
- Stellen Sie beim Durchführen eines Software-Upgrades sicher, dass das Staging für alle verbundenen Sites abgeschlossen ist, bevor Sie es aktivieren. Wenn die Aktivierung vor Abschluss des Stagingvorgangs durch Aktivieren von Unvollständig ignorieren erfolgt, wird der virtuelle Pfad möglicherweise nicht mit MCN für die Sites angezeigt, zu denen das Staging noch läuft. Um das Netzwerk wiederherzustellen, ist es erforderlich, das lokale Änderungsmanagement für diese Sites manuell durchzuführen.
- Ab Citrix SD-WAN Version 11.0.0 wird das zugrunde liegende Betriebssystem/Kernel für die SD-WAN-Software auf eine neuere Version aktualisiert. Es erfordert einen automatischen Neustart, der während des Upgradevorgangs durchgeführt wird. Infolgedessen wird die erwartete Zeit für das Upgrade jeder Appliance um ca. 100 Sekunden erhöht. Darüber hinaus wird durch die Einbeziehung des neuen Betriebssystems die Größe des Upgrade-Pakets,

das auf jede Zweigeinheit übertragen wird, um ca. 90 MB erhöht.

Virtuelles WAN-Softwareupgrade auf 9.3.5 mit funktionierender Virtual WAN-Bereitstellung

May 10, 2021

Hinweis:

Verwenden Sie eine funktionierende Virtual WAN-Konfiguration mit 9.3.4 oder niedriger Build mit virtuellen Pfaden, die von MCN zu den Zweigstandorten eingerichtet werden.

1. Navigieren Sie auf der MCN-Appliance zu **Konfiguration > Virtuelles WAN > Änderungsverwaltung**.
2. Rufen Sie die zutreffende *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* für alle Sites im Virtual WAN-Netzwerk unter [Citrix Downloadseite](#)
3. Laden Sie die Datei *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* für die in der Konfigurationsdatei definierten Zweige hoch, für die ein Upgrade durchgeführt werden muss. Führen Sie das Änderungsmanagement in der SD-WAN-Weboberfläche für die MCN-Appliance durch und schließen Sie den Änderungsmanagement-Prozess ab.

The screenshot displays the 'Configuration > Virtual WAN > Change Management' page. The 'Upload and Verify Files' section is active, showing instructions for uploading files and verifying configurations. Below this, a table lists the status of various appliances:

| Site Appliance | Model | State | Software | Config | Currently Active | Currently Staged | Traffic Interruption | Download Package |
|------------------------|--------|--------|-----------------|------------------|------------------|------------------|----------------------|------------------|
| MCN10Site-Appliance | CB1000 | active | 8.1.0.95.472519 | 15:54 on 6/29/17 | | | Loc Chg Mgt | active / none |
| Branch20Site-Appliance | CB2000 | active | 8.1.0.95.472519 | 15:54 on 6/29/17 | | | Loc Chg Mgt | active / none |
| Branch400-Appliance | CB400 | active | 8.1.0.95.472519 | 15:54 on 6/29/17 | | | Loc Chg Mgt | active / none |
| Branch100-Appliance | CB100 | active | 8.1.0.95.472519 | 15:54 on 6/29/17 | | | Loc Chg Mgt | active / none |
| VPX_100-Appliance | CB100 | active | 8.1.0.95.472519 | 15:54 on 6/29/17 | | | Loc Chg Mgt | active / none |

4. Klicken Sie auf **Weiter**, um fortzufahren.

The screenshots illustrate the 'Upload and Verify Files' process in the Citrix SD-WAN 11.2 interface. The first screenshot shows the 'Upload and Verify Files' dialog with a file selected. The second screenshot shows the 'Verification Results' dialog indicating successful validation. The third screenshot shows the 'License' dialog with the Citrix License Agreement.

Configuration Filenames: Active - Config_8_1_0_1k_MCN_2k_ven_esi_cb400_branch.cfg Staged -

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

Verification Results

Status: Validation Success

This Configuration is valid. (version 1498754288)

Files created:

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

License

CITRIX LICENSE AGREEMENT

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

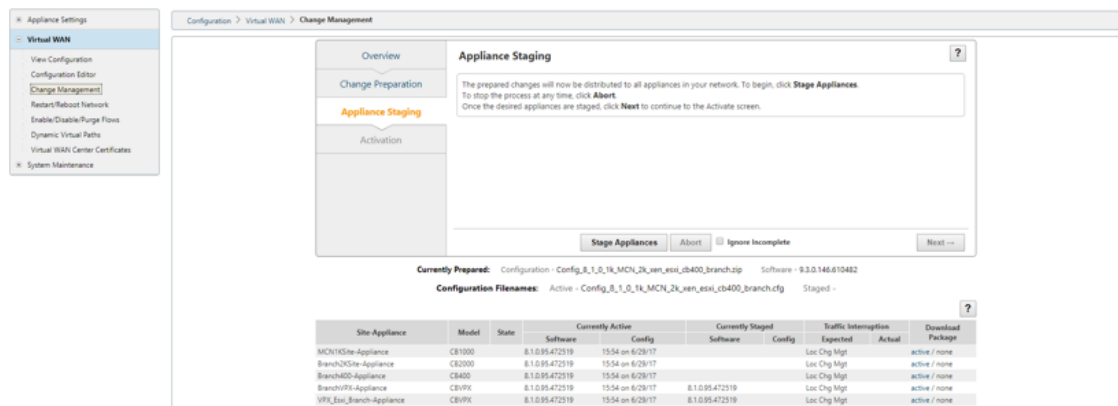
1. PRODUCT LICENSES.

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

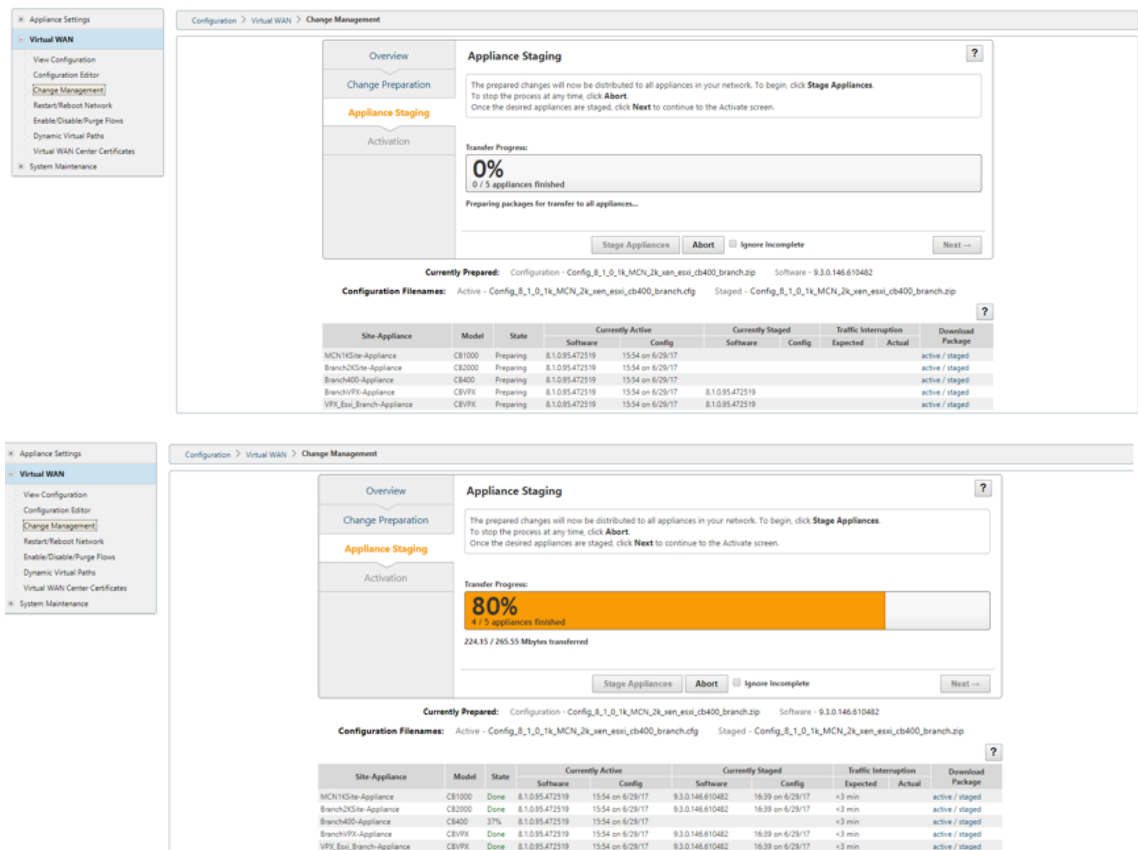
You must accept the license terms before installing the new package.

☒ I accept the End User License Agreement.

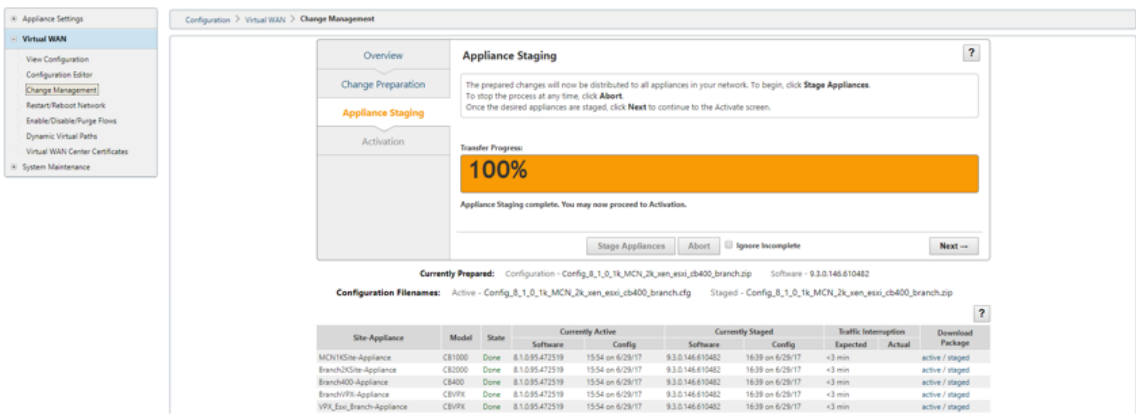
5. Nachdem Sie die Lizenzvereinbarung akzeptiert haben, navigieren Sie zu **Appliance-Staging**, wo Appliances bereitgestellt werden können, indem Sie auf **Stage Appliances** klicken.



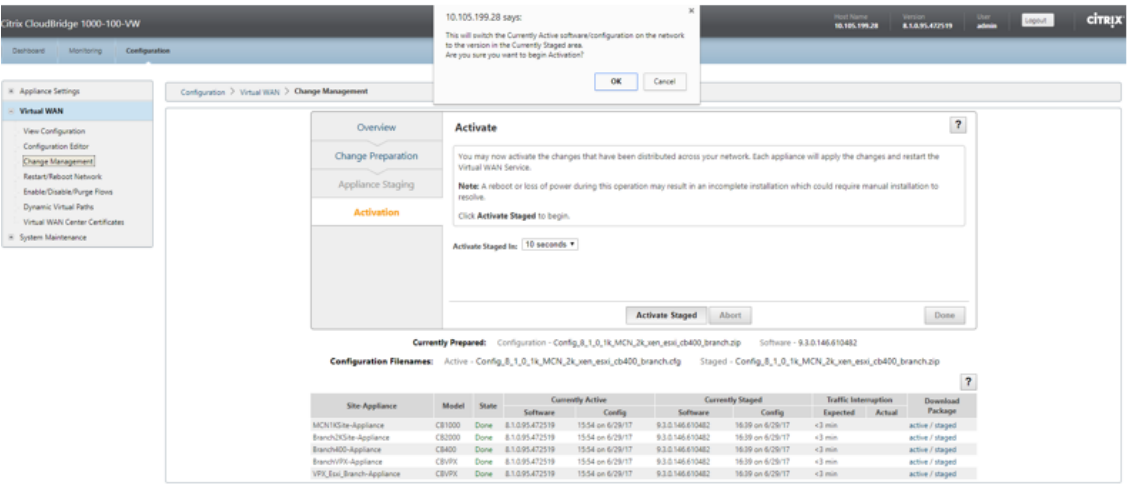
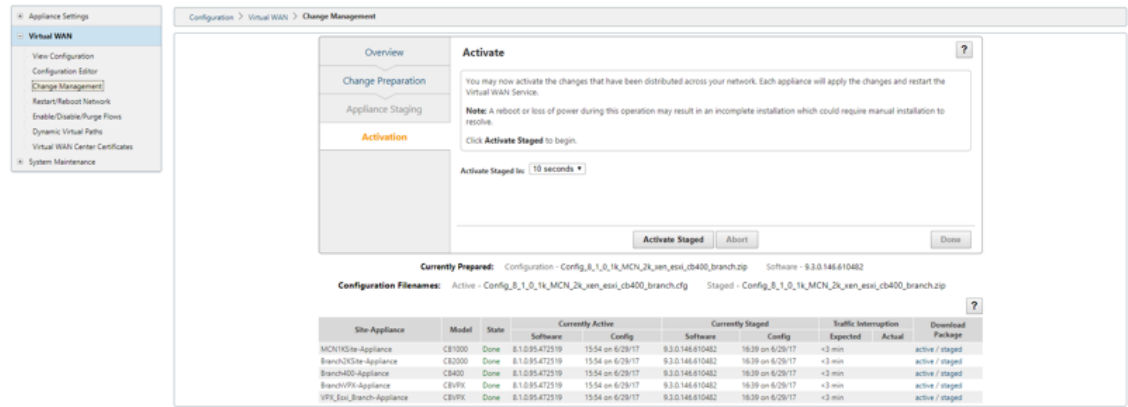
6. Der Status Übertragungsfortschritt wird beim Vorbereiten und Bereitstellen der Softwarepakete an die Appliances angezeigt.



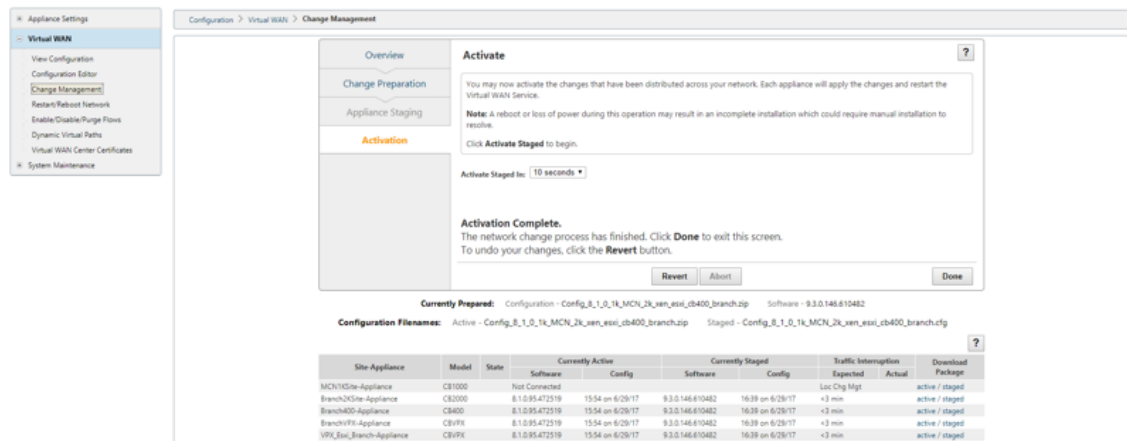
7. Klicken Sie auf **Weiter**, wenn Transferfortschritt 100% anzeigt und die Schaltfläche aktiviert ist, um fortzufahren.



8. Klicken Sie auf der Seite **Aktivierung** auf **Staged aktivieren**, um mit der Aktivierung zu beginnen.



9. Nach Abschluss der Aktivierung Countdown von 180 s klicken Sie auf **Fertig**.



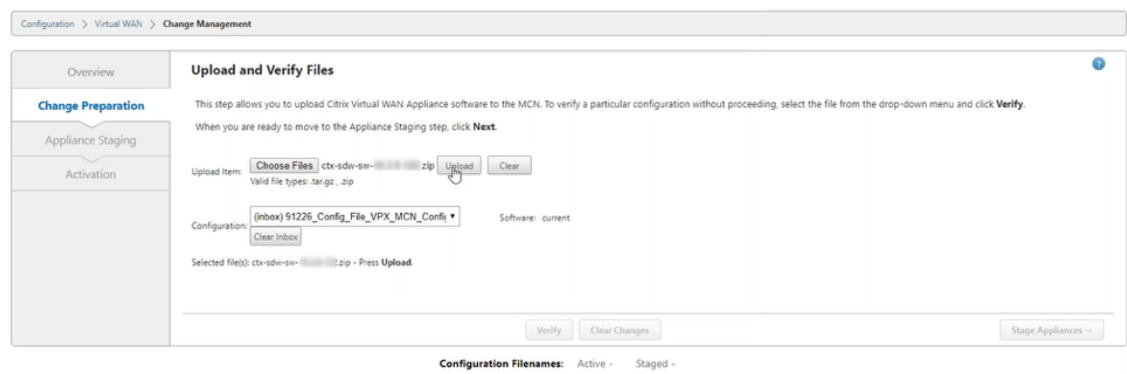
Upgrade auf 11.2 mit funktionierender Virtual WAN-Bereitstellung

May 10, 2021

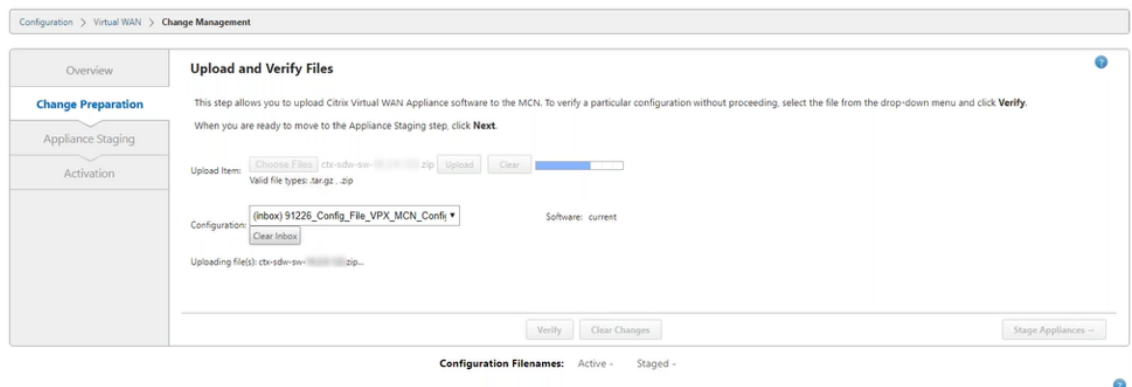
1. Klicken Sie auf der Seite **Change Management > Change Preparation** auf **Choose Files** und wählen Sie die Softwarepaketdatei *ctx-sdw-11.2.0.x.zip* aus. Klicken Sie auf **Upload**.

Hinweis:

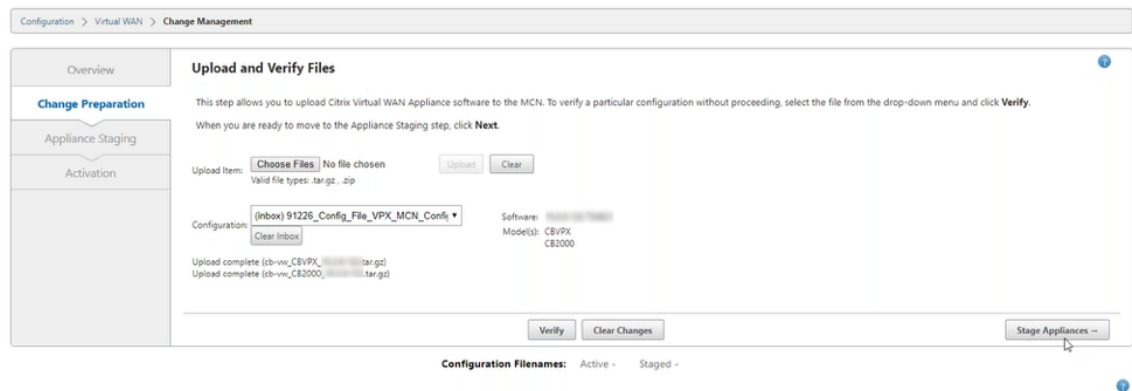
Sie können das Softwarepaket Citrix SD-WAN Release 11.2 von der [Downloads](#) Seite herunterladen.



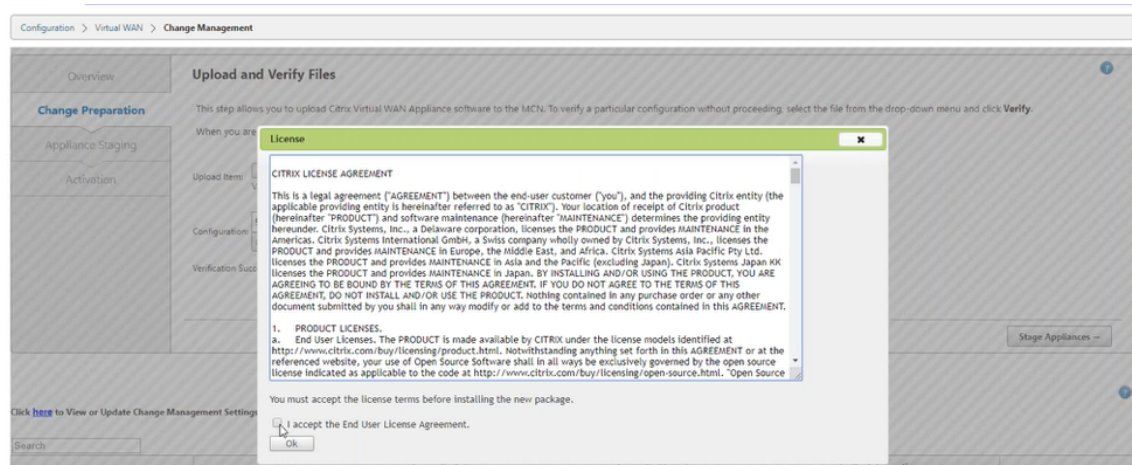
Ein Fortschrittsbalken wird angezeigt, in dem der aktuelle Upload-Fortschritt angezeigt wird.



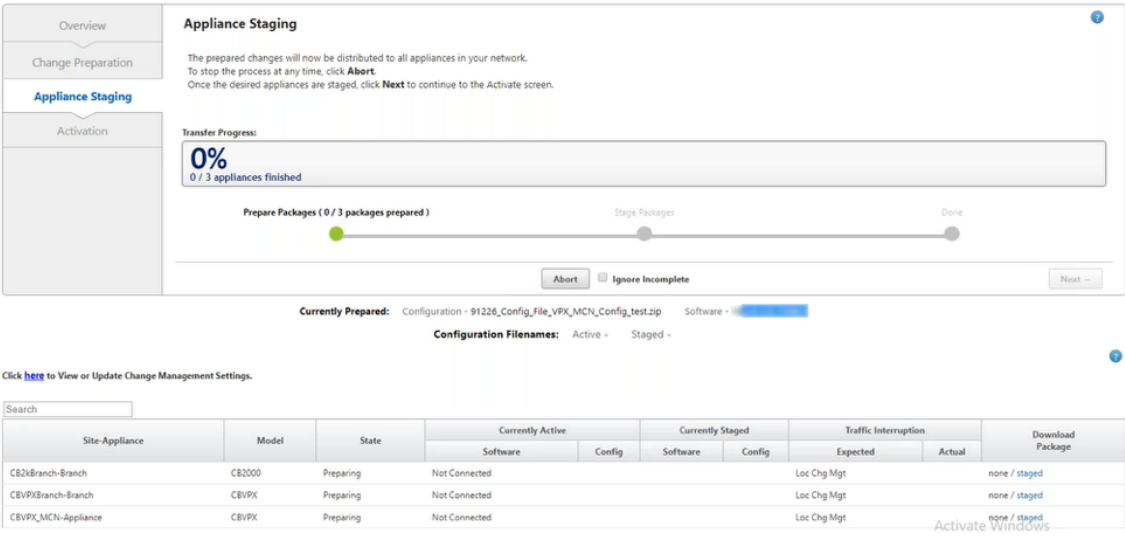
2. Nach erfolgreichem Upload-Vorgang werden relevante Appliance-Modelle angezeigt. Die Appliances würden basierend auf der Konfigurationsdatei aktualisiert.



3. Klicken Sie auf **Stage Appliance**, um mit der Validierung der Konfigurationsdatei fortzufahren. Die Seite Lizenzvereinbarung für die Benutzerakzeptanz wird angezeigt. Klicken Sie auf **Ich akzeptiere die Endbenutzer-Lizenzvereinbarung** und klicken Sie auf **OK**.



4. Der **Appliance-Staging-Prozess** wird gestartet. Die Änderungen werden an alle Appliances im Netzwerk verteilt. Der Transferfortschrittsbalken wird angezeigt, und die Site-Detailtabelle wird aktualisiert.



5. Sobald der Übertragungsfortschritt 100% abgeschlossen ist, klicken Sie auf **Weiter**, um mit der Aktivierung fortzufahren.

Appliance Staging

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

Transfer Progress:

100%

Appliance Staging complete. You may now proceed to Activation.

Prepare Packages Stage Packages Done

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

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

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

Global Multi-Region Summary

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

Region - Default_Region Details

Show 25 entries

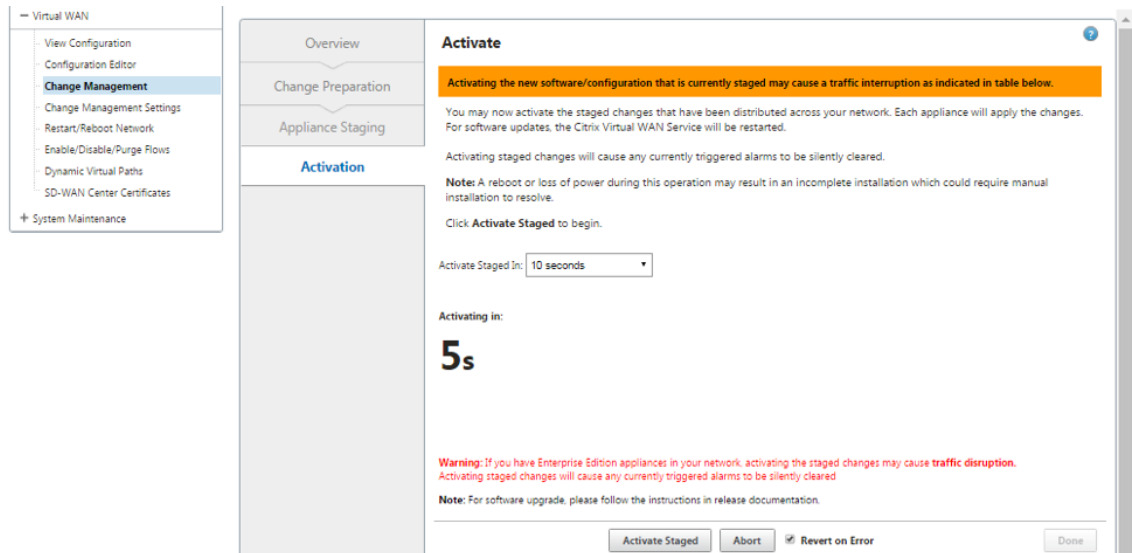
| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Traffic Interruption | | Download Package |
|--------------------------|--------|------------------|------------------|------------------|------------------|--------|----------------------|--------|------------------|
| | | | Software | Config | Software | Config | Expected | Actual | |
| MCN1-MCN1-CB4100 | CB4100 | 12:56 on 2/23/18 | 12:56 on 2/23/18 | 11:56 on 2/23/18 | <1 sec | 371 ms | active / staged | | |
| APAC_RCN-APAC_RCN-CB1000 | CB1000 | 12:56 on 2/23/18 | 12:56 on 2/23/18 | 11:56 on 2/23/18 | <1 sec | 269 ms | active / staged | | |
| BR1-BR1-CBVPXL | CBVPXL | 12:56 on 2/23/18 | 12:56 on 2/23/18 | 11:56 on 2/23/18 | <1 sec | 304 ms | active / staged | | |
| RCN01-2000-RCN01-2000 | CB2000 | 12:56 on 2/23/18 | 12:56 on 2/23/18 | 11:56 on 2/23/18 | <1 min | 183 ms | active / staged | | |

Die verschiedenen Zustände der Softwarepaketkonfiguration, die in der Übersichtstabelle angezeigt werden, zeigen Folgendes an:

- **Vorbereiten** - Lokale Verarbeitung zur Vorbereitung des Updatepakets für die Übertragung an die Appliance.
- **Regionspakete vorbereiten** - Lokale Verarbeitung zur Vorbereitung des Updatepakets für die Übertragung an RCN. (Gilt, wenn RCN Teil des Netzwerks ist).
- **Prozentsatz - Prozentsatz** des an die Appliance übertragenen Pakets.
- **Entpacken** - Remote-Appliance-Verarbeitung, um das Update-Paket anzuwenden.
- **Übertragende Region** - Paket wird an RCN übertragen. (Gilt, wenn RCN Teil des Netzwerks ist).
- **Fehlgeschlagen** - Remote hat unvollständige Übertragung erkannt.
- **Abgebrochen** - Vom Benutzer abgebrochen, wenn Unvollständige Ignorieren während der Stage Appliances überprüft wurde

- **Nicht erforderlich** —Das vorbereitete bereitgestellte Paket enthält diesen Site-Appliance-Namen nicht.
- **Nicht verbunden** - Lokal kann die aktiven Paketinformationen der Fernbedienung nicht sehen.

6. Klicken Sie auf **Staged** aktivieren, um die bereitgestellten Software zu aktivieren.



7. Nach dem Countdown zeigt eine Meldung an, dass die Aktivierung abgeschlossen ist. Klicken Sie auf **Fertig**.

View Configuration

Configuration Editor

Change Management

Change Management Settings

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

System Maintenance

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Activation Complete.

The network change process has finished. Click **Done** to exit this screen.

To undo your changes, click the **Revert** button.

Revert

Abort

Done

Currently Prepared:

Configuration - Multir_dvp9_ipsecFIPS.zip

Software - Current Running

Configuration Filenames:

Active - Multir_dvp9_ipsecFIPS.zip

Staged - Multir_dvp9_ipsecFIPS.zip

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

Global Multi-Region Summary

Search

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

Region - Default_Region Details

Show 25 entries

Search

Customize

Refresh

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

Previous 1 Next

8. Navigieren Sie zur Seite **Änderungsverwaltung**, um den Übertragungsstatus anzuzeigen.

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

76

Configuration > Virtual WAN > Change Management

Details

Active Configuration:
_MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Staged Configuration:
_MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Prepared Configuration:
_MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Overview

Change Preparation

Appliance Staging

Activation

Step 1
Upload Files to MCN

Step 2
Transfer Files to Clients

Step 3
Activate Change

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

Activate Staged

Begin →

Global Multi-Region Summary

Search

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

Region - region1 Details of Traffic Impacted Sites

Show 25 entries Search

Customize

Refresh

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

Previous

1

Next

Die Übersichtstabelle für mehrere Regionen enthält folgende Details:

- **Region** —Name der Region
- **Standort insgesamt** - Gesamtzahl der Standorte in der Region.
- **Nicht verbunden** - Gesamtzahl der Standorte, die in der Region nicht verbunden sind.
- **Verbunden** - Gesamtzahl der in der Region verbundenen Standorte.
- **Auswirkungen auf den Datenverkehr** - Gesamtzahl der Standorte, an denen der Datenverkehr in der Region betroffen ist.
- **Keine Auswirkungen auf den Datenverkehr** - Gesamtzahl der Websites, an denen der Datenverkehr in der Region nicht beeinträchtigt wird.
- **Staging In Progress** - Gesamtzahl der Standorte, für die lokale Verarbeitung versucht, das Updatepaket für die Übertragung in der Region vorzubereiten.
- **Kommissionierung abgeschlossen**- Gesamtzahl der Standorte, für die die Kommissionierung in der Region abgeschlossen wurde.
- **Staging fehlgeschlagen** - Gesamtanzahl der Websites, für die eine unvollständige Übertragung in der Region gelöscht wurde.

Global Multi-Region Summary

Search

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

Klicken Sie auf den Link **Globale Übersicht für mehrere Regionen**, um die regionspezifischen Konfigurationsberichte zu filtern.

Region - Default_Region Details of Connected Sites

Customize Refresh

Show 25 entries Search

| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Traffic Interruption | | Download Package |
|---------------------------------|-------|------------|-------------------|-------------------|-------------------|------------------|----------------------|--------|------------------|
| | | | Software | Config | Software | Config | Expected | Actual | |
| MCN-NY-MCN-NY-CB2000 | 2000 | | 10.2.0.116.750016 | 11:34 on 12/10/18 | 10.2.0.117.750016 | 6:30 on 12/10/18 | <3 min | 82 s | active / staged |
| Def-Site1-SC-Def-Site1-SC-CBVPX | VPX | | 10.2.0.116.750016 | 11:34 on 12/10/18 | 10.2.0.117.750016 | 6:30 on 12/10/18 | <3 min | 209 s | active / staged |
| R1-RCN-MUM-R1-RCN-MUM-CBVPX | VPX | Done(auto) | 10.2.0.116.750016 | 11:34 on 12/10/18 | 10.2.0.117.750016 | 6:30 on 12/10/18 | <3 min | 195 s | active / staged |
| R2-RCN-SA-R2-RCN-SA-CBVPX | VPX | Done(auto) | 10.2.0.116.750016 | 11:34 on 12/10/18 | 10.2.0.117.750016 | 6:30 on 12/10/18 | <3 min | 199 s | active / staged |

Previous 1 Next

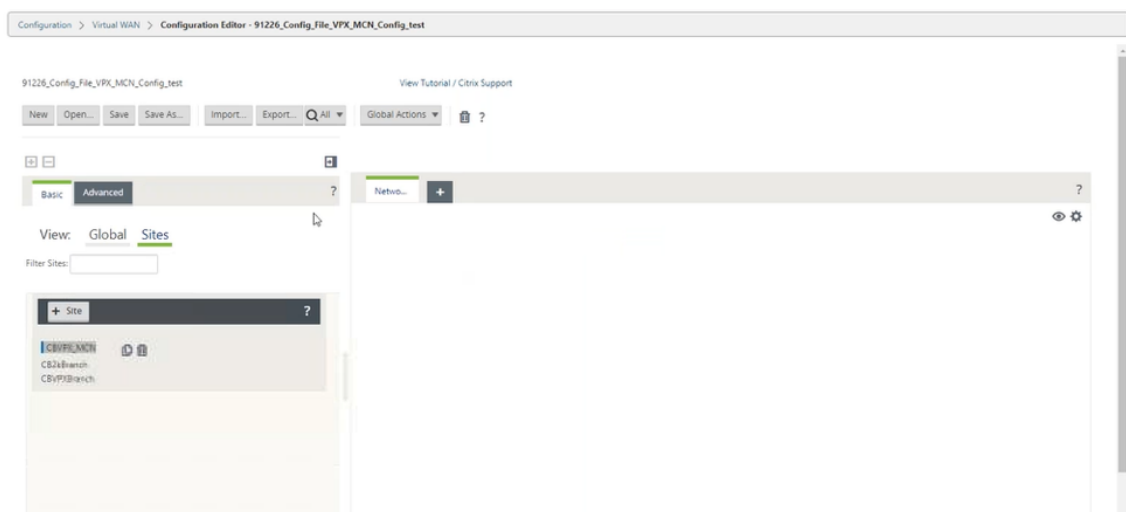
Navigieren Sie für die Bereitstellung von Muliregionen auf jedem RCN zur Seite **Änderungseinstellungen** und planen Sie die Installation abhängiger Komponenten. Standardmäßig weist der MCN/RCN die Installation von Zeitplänen zu, die jeden Tag um 21:20:00 Uhr basierend auf der Softwareverfügbarkeit in den Zweigen zu versuchen.Weitere Informationen finden Sie unter [Verwaltungseinstellungen ändern](#)

Upgrade auf 11.2 ohne funktionierende virtuelle WAN-Bereitstellung

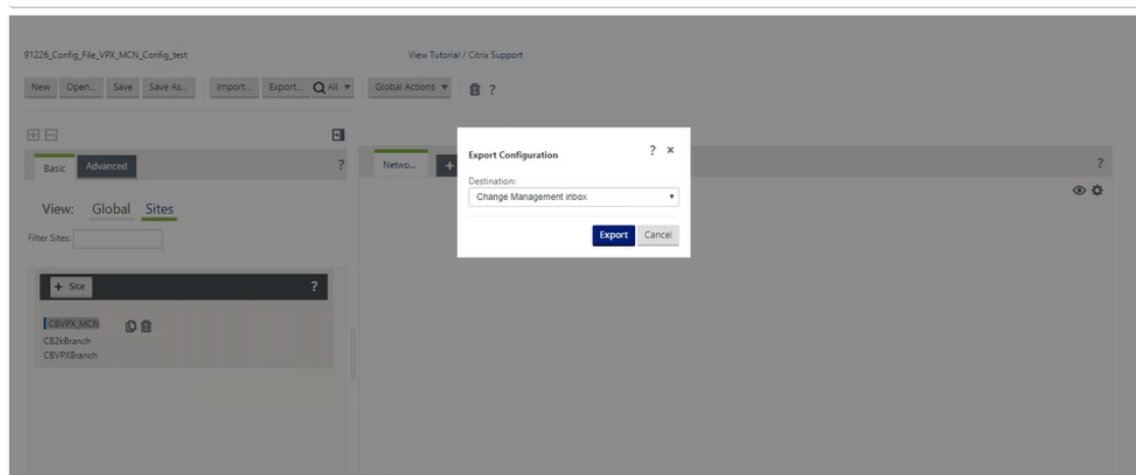
May 10, 2021

Hinweis: Um die neuesten 11.2-Funktionen zu konfigurieren, müssen Sie die MCN-Appliance auf 11.2-Software umlegen. Weitere Informationen finden Sie unter [Reimage der Citrix SD-WAN Appliance-Software](#)

1. Bereiten Sie die Konfiguration mit dem **Konfigurations-Editor** vor, und speichern Sie die Konfiguration unter einem gültigen Namen. Weitere Informationen finden Sie unter [Konfiguration](#).



2. Exportieren Sie die gespeicherte Konfiguration in Change Management. Klicken Sie auf **Exportieren**, und wählen Sie **Änderungsverwaltungseingang** als Ziel aus. Klicken Sie auf **Exportieren**.



3. Klicken Sie auf der Seite **Change Management > Change Preparation** auf Choose **Files and wählen** Sie die Softwarepaketdatei **ctx-sdw-11.2.0.x.zip** aus. Klicken Sie auf **Upload**.

Hinweis:

Sie können das Softwarepaket Citrix SD-WAN Release 11.2 von der [Downloads](#) Seite herunterladen.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

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

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

Upload Item:

Choose Files

 ctx-sdw-sw-...zip

Upload

Clear

Valid file types: .tar.gz, .zip

Configuration:

(inbox) 91226_Config_File_VPX_MCN_Config

Clear Inbox

 Software: current

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

Verify

Clear Changes

Stage Appliances --

Configuration Filenames: Active - Staged -

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

Search

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

Ein Fortschrittsbalken wird angezeigt, in dem der aktuelle Upload-Fortschritt angezeigt wird.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

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

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

Upload Item:

Choose Files

 ctx-sdw-sw-...zip

Upload

Clear

Valid file types: .tar.gz, .zip

Configuration:

(inbox) 91226_Config_File_VPX_MCN_Config

Clear Inbox

 Software: current

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

Verify

Clear Changes

Stage Appliances --

Configuration Filenames: Active - Staged -

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

Search

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

4. Nach erfolgreichem Upload-Prozess werden relevante Modelle angezeigt, die basierend auf der Konfigurationsdatei aktualisiert werden, die Informationen zu den einzelnen Zweigplattformmodellen enthält.

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

80

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

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

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

Valid file types: tar.gz, .zip

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

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

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

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

Configuration Filenames: Active - Staged -

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

Search

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

5. Klicken Sie auf **Stage Appliance**, um mit der Validierung der Konfigurationsdatei fortzufahren. Die Seite Lizenzvereinbarung für die Benutzerakzeptanz wird angezeigt. Klicken Sie auf **Ich akzeptiere die Endbenutzer-Lizenzvereinbarung** und klicken Sie auf **OK**.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

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

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

Valid file types: tar.gz, .zip

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

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

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

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

Configuration Filenames: Active - Staged -

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

Search

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

LICENSE

CITRIX LICENSE AGREEMENT

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

1. PRODUCT LICENSES.

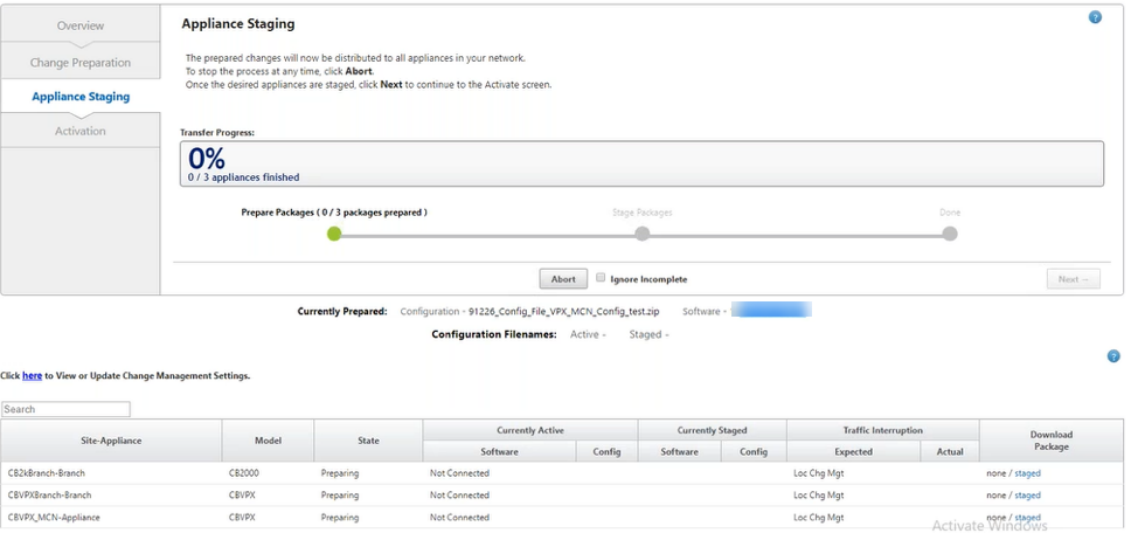
a. End User Licenses. The PRODUCT is made available by CITRIX under the license models identified at <http://www.citrix.com/buy/licensing/product.html>. Notwithstanding anything set forth in this AGREEMENT or at the referenced website, your use of Open Source Software shall in all ways be exclusively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

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

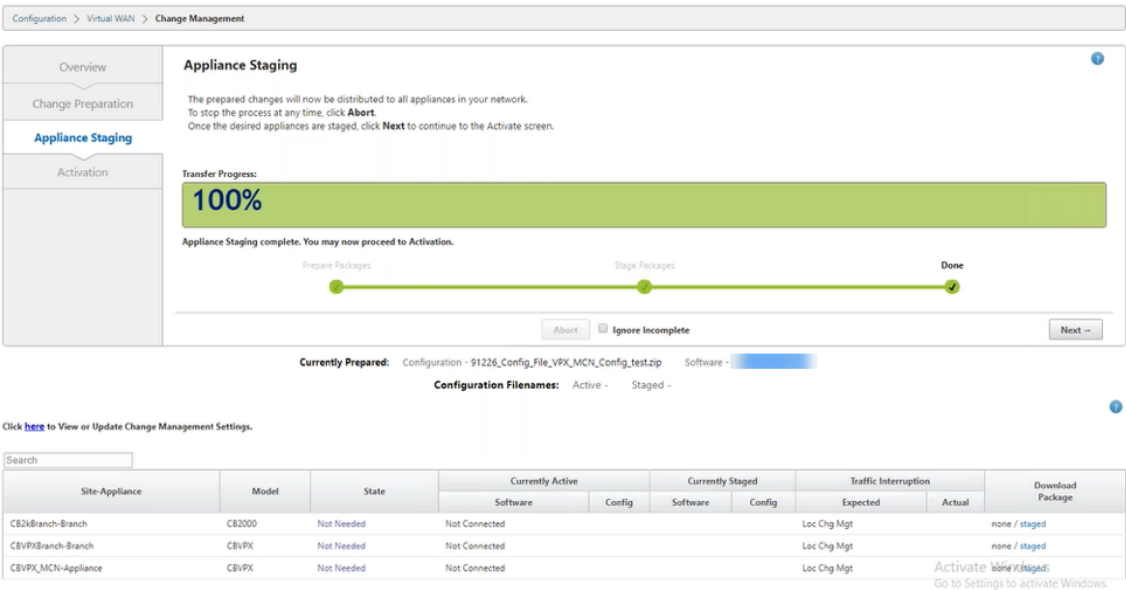
☒ I accept the End User License Agreement.

OK

6. Der **Appliance-Staging-Prozess** wird initiiert, die Änderungen werden an alle Appliances im Netzwerk verteilt. Der Transferfortschrittsbalken wird angezeigt, und die Site-Detailtabelle wird aktualisiert.

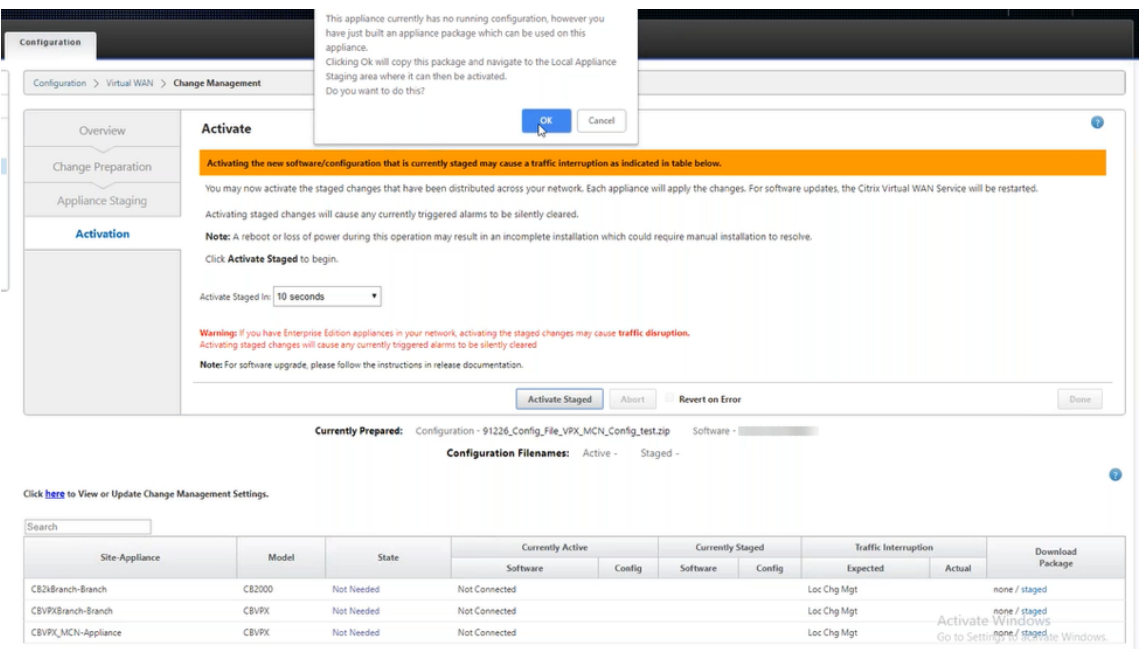


7. Sobald der Übertragungsfortschritt 100% abgeschlossen ist, klicken Sie auf **Weiter**, um mit der Aktivierung fortzufahren.

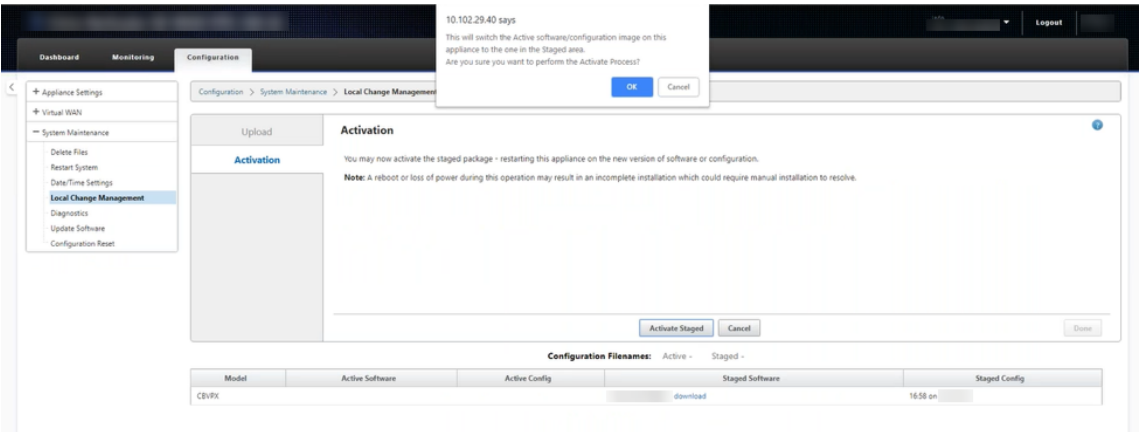


8. Klicken Sie auf **Activate Staged**. Eine Popupmeldung für die Benutzerakzeptanz wird angezeigt, da dies das erste Mal ist, dass die Appliance bereitgestellt wird.

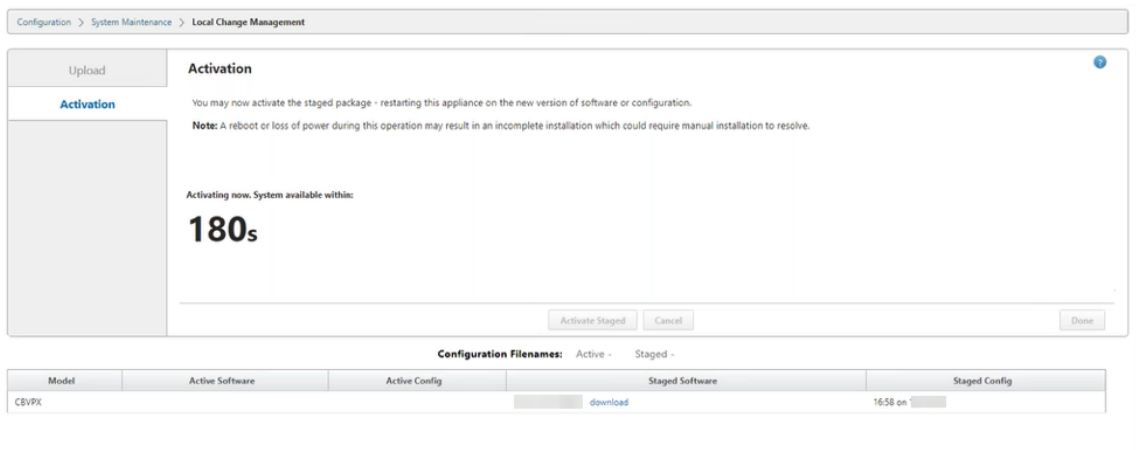
Sie werden zur Seite **Lokale Änderungsverwaltung** weitergeleitet, um die lokale Appliance zu aktivieren. Klicken Sie auf **OK**, um fortzufahren.



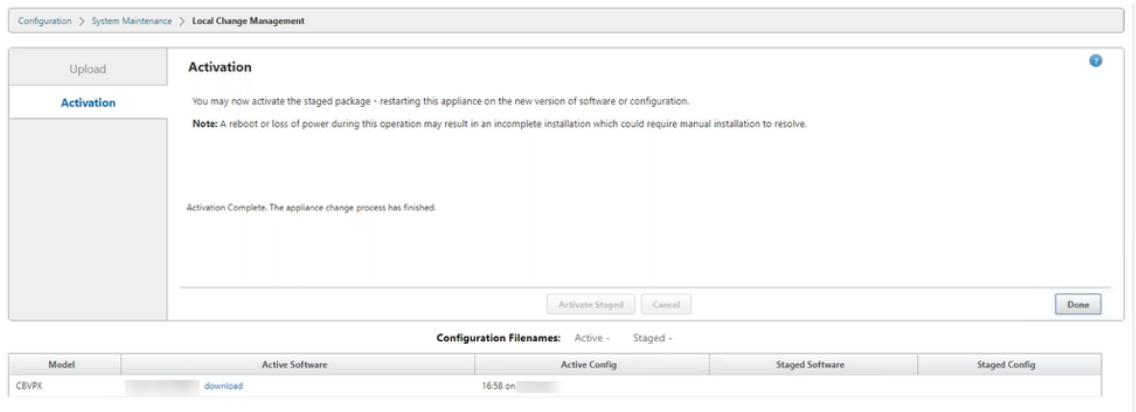
9. Klicken Sie in Local Change Management auf **Staged aktivieren**. Es wird eine Aktivierungsbestätigungsmeldung angezeigt. Klicken Sie auf **OK**.



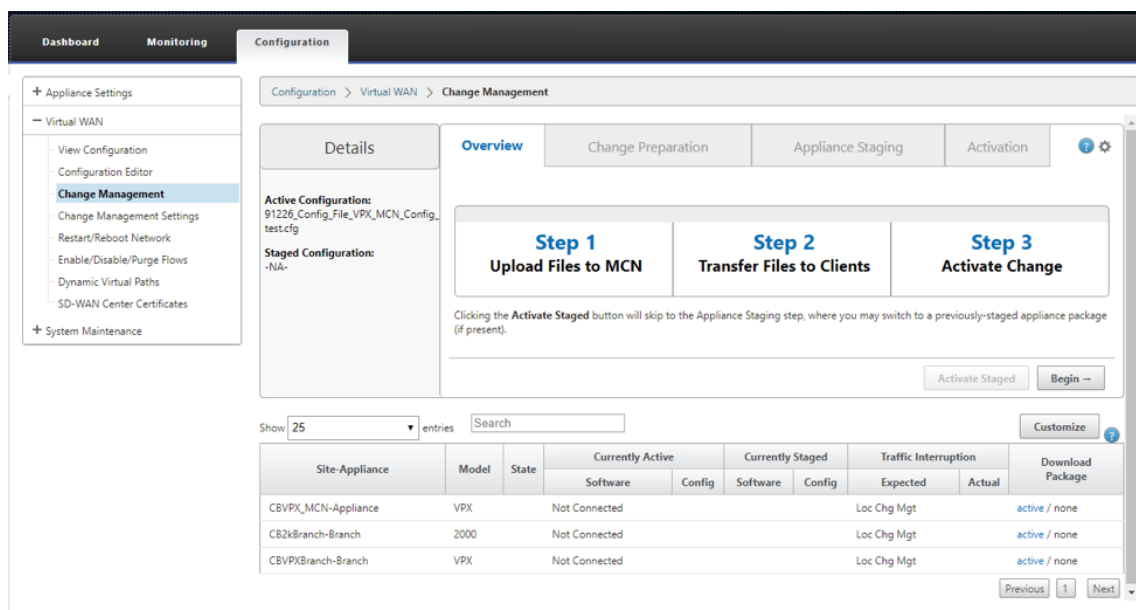
Die Aktivierung beginnt mit einem Countdown-Timer von 180 Sekunden.



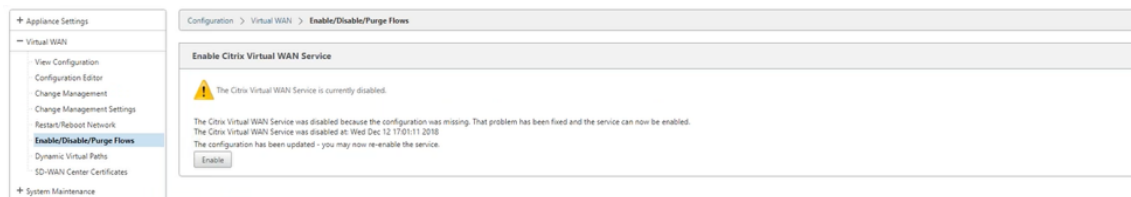
10. Nach dem Countdown zeigt eine Meldung an, dass die Aktivierung abgeschlossen ist. Klicken Sie auf **Fertig**, die Appliance wird neu gestartet.



11. Navigieren Sie nach dem Neustart der Appliance zur Seite **Änderungsverwaltung**, um die lokalen Änderungsverwaltungspakete für die jeweiligen Zweige herunterzuladen, die Sie nur mit dem Virtual WAN-Software-Upgrade in das Netzwerk booten müssen.



12. Aktivieren Sie den SD-WAN-Dienst auf der Appliance. Navigieren Sie zu **Virtuelles WAN > Flows aktivieren/deaktivieren/löschen**, und klicken Sie auf **Aktivieren**.



Um weitere Sites zu konfigurieren und dem Netzwerk hinzuzufügen, folgen Sie der Vorgehensweise unter [Zweigknoten konfigurieren](#).

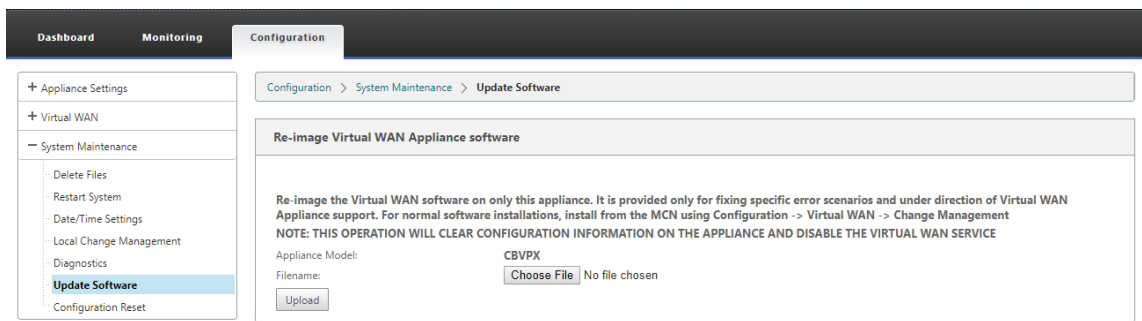
Reimage der Citrix SD-WAN Appliance-Software

May 10, 2021

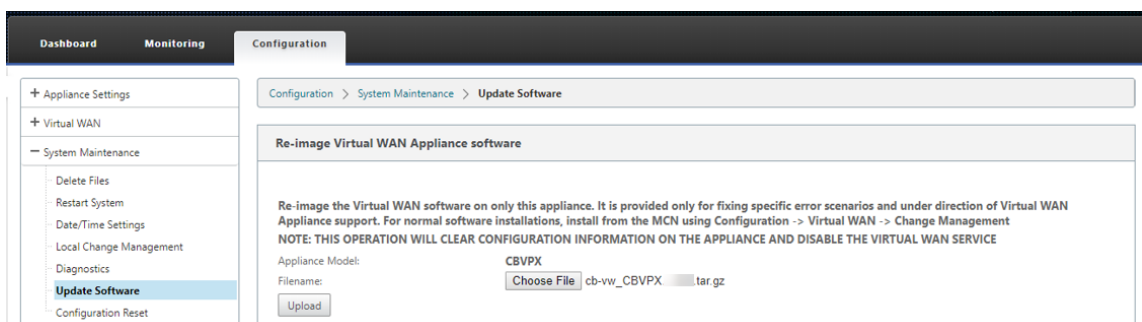
Laden Sie die Datei `.tar.gz` der erforderlichen Citrix SD-WAN -Softwareversion und -plattform vom Portal [Citrix Downloads](#) herunter.

So erstellen Sie ein neues Image der Citrix SD-WAN Appliance-Software:

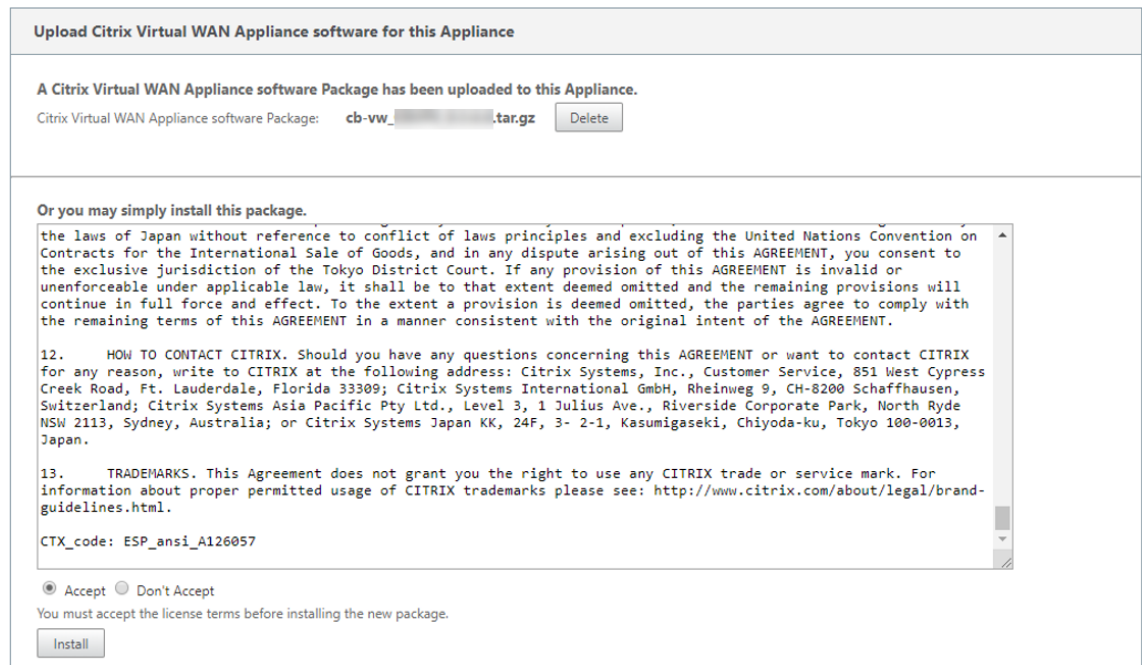
1. Navigieren Sie in der Benutzeroberfläche der SD-WAN-Appliance zu **Konfiguration > Systemwartung > Software aktualisieren**.



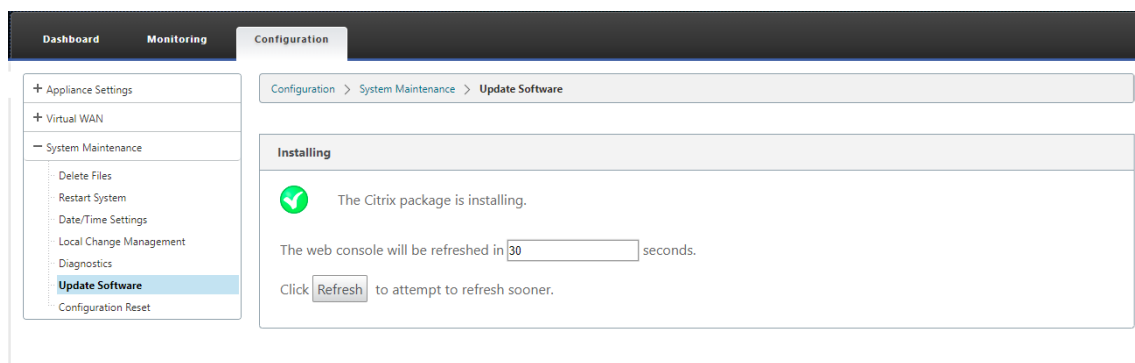
2. Klicken Sie auf **Datei auswählen**, und wählen Sie die heruntergeladene Citrix SD-WAN Appliance-Software aus. Klicken Sie auf **Upload**.



3. Lesen und akzeptieren Sie die Lizenzbedingungen. Klicken Sie auf **Akzeptieren**, und klicken Sie dann auf **Installieren**.



Das Softwareupdate dauert etwa 35 Sekunden, danach wird die Appliance neu gestartet.



Teilweise Softwareupgrade mit lokalem Änderungsmanagement

May 10, 2021

Wichtig

Standardmäßig ist die Option **partielles Software-Upgrade** deaktiviert.

Sie können eine neuere Version der SD-WAN-Softwareversion auf einer Teilmenge von Client-Sites installieren, indem Sie die Option **Lokales Änderungsmanagement** verwenden. Dies wird durch die partielle Software-Upgrade-Funktion erreicht, die es dem Netzwerkadministrator ermöglicht, die Software an Standorten im Netzwerk selektiv zu aktualisieren, ohne dass alle Standorte gleichzeitig aktualisiert werden müssen. Ein spezieller Anwendungsfall für diese Funktion ist ein Administrator, der die neue Software auf wenigen Zweigstandorten testet, bevor sie auf allen Standorten im Netzwerk installiert wird.

Voraussetzungen und Anforderungen

Bevor Sie mit der Durchführung eines teilweisen Software-Upgrades fortfahren, überprüfen Sie die folgenden Anforderungen:

1. Haben Sie eine aktive SD-WAN Version 10.0 oder neuere Software. **Aktivieren Sie das Kontrollkästchen Teilweise Software-Upgrade** aktivieren. Wenn Sie das Kontrollkästchen deaktivieren, wird die Software, die derzeit auf der MCN-Appliance ausgeführt wird, auf die Zweige angewendet, in denen aktive virtuelle Pfade ausgeführt werden.

Configuration > Virtual WAN > Change Management Settings

Enable/Disable Partial Software Upgrade

☐ Enable Partial Software Upgrade Apply

Scheduling Information

Show 10 entries Search

Edit Selected Refresh

| | Site Name | Scheduling Information | Status | Edit |
|--------------------------|------------------------|--|--------|------|
| <input type="checkbox"/> | RCN3BR2 | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ... | |
| <input type="checkbox"/> | RCNDefaultBR2VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ! | |
| <input type="checkbox"/> | RCNDefaultBR1VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ... | |
| <input type="checkbox"/> | RCN3BR2(HA-Secondary) | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ✖ | |
| <input type="checkbox"/> | MCNVPXHA | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ✓ | |
| <input type="checkbox"/> | MCNVPXHA(HA-Secondary) | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ✓ | |
| <input type="checkbox"/> | GeoMCNVPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ● | |
| <input type="checkbox"/> | RCN1BR11000 | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ● | |
| <input type="checkbox"/> | RCN1BR2VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ● | |
| <input type="checkbox"/> | RCN1RCN | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | ● | |

Showing 1 to 10 of 17 entries

Previous 1 2 Next

Configuration > Virtual WAN > Change Management Settings

Enable/Disable Partial Software Upgrade

☒ Enable Partial Software Upgrade Apply

Scheduling Information

Show 10

Help

Enable/Disable Partial Software Upgrade

- Use this section to control the Partial Software Upgrade feature of change management.
- Enable Partial Software Upgrade to allow sites in the network to be selectively upgraded
- Disable Partial Software Upgrade to turn off the feature and synchronize all sites in the network with the MCN. This may cause network disruption while synchronization is in progress.

Close

2. Stationieren Sie die neue Version der Software mithilfe des MCN **Change Management-Prozesses** mit derselben Hauptversionsnummer wie die aktive Software und derselben Konfiguration wie die aktive Konfiguration.
3. Die neue Software sollte dieselbe Hauptversion der Software sein wie die aktive Software. Bei der Nebenversion kann es sich um eine andere Softwareversion handeln.
4. Die neue Software muss zuerst auf allen Standorten aus dem MCN bereitgestellt werden. Been-

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

88

den Sie den Schritt **Staged aktivieren** des Änderungsmanagements.

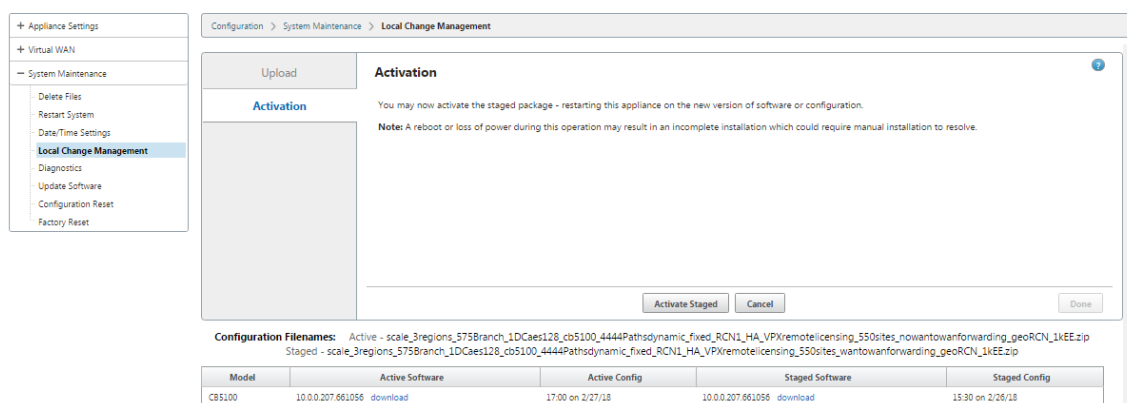
Für die Konfiguration des Standorts Aktiv und Teilweise muss die Software auf den MCN- und Zweigstandorten identisch sein. Es ist nicht möglich, einen anderen Featuresatz auf teilweise aktualisierten Websites aktiviert zu haben. Fahren Sie mit den einzelnen Standorten fort, um die **lokale Änderungsverwaltung** durchzuführen. Lesen Sie die folgenden Anweisungen zur Bereitstellung von Hochverfügbarkeit.

So führen Sie ein partielles SD-WAN-Software-Upgrade durch:

Es gibt zwei Szenarien, in denen Sie ein partielles SD-WAN-Software-Upgrade auf einem Zweigknoten durchführen können: Hochverfügbarkeitsmodus und Nicht-Hochverfügbarkeitsmodus.

Upgrade-Zweigknoten ohne Hochverfügbarkeitsmodus

1. Navigieren Sie in der Citrix SD-WAN -Webverwaltungsschnittstelle zu dem Zweigstandort, der im Rahmen des Teilstandsupdateprozesses aktualisiert werden muss.
2. Öffnen Sie die **lokale Änderungsverwaltung**. Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Activate Staged**. Jeder Zweigstandort wird nun mit einer neuen Softwareversion installiert.



Aktualisieren des Zweigknotens im Hochverfügbarkeitsmodus

1. Navigieren Sie in der SD-WAN-Webverwaltungsschnittstelle zu dem Zweigstandort, der über das Teilstandsupdate aktualisiert werden muss.
2. Deaktivieren Sie den Dienst auf der Standby-Appliance.
3. Öffnen Sie auf der primären Appliance die **lokale Änderungsverwaltung**.
4. Klicken Sie auf **Activate Staged**. Diese Appliance wird nun mit einer neuen Softwareversion installiert.

5. Öffnen Sie auf der Standby-Appliance **Local Change Management**.
6. Klicken Sie auf **Activate Staged**. Die Standby-Appliance wird nun mit einer neuen Softwareversion installiert.
7. Nachdem die primären und Standby-Appliances den Aktivierungsvorgang abgeschlossen haben, aktivieren Sie den Dienst auf der Standby-Appliance.

Upgrade-Netzwerk

Wenn Sie bereit sind, das Netzwerk synchron zu machen, navigieren Sie zum Bildschirm MCN-Netzwerkänderungsverwaltung, und klicken Sie auf **Staged aktivieren**.

WANOP zu Premium Edition Konvertierung mit USB

May 10, 2021

Hinweis

Nur die SD-WAN 1000 und 2000 WANOP Appliances können in SD-WAN Premium Edition Appliances umgewandelt werden.

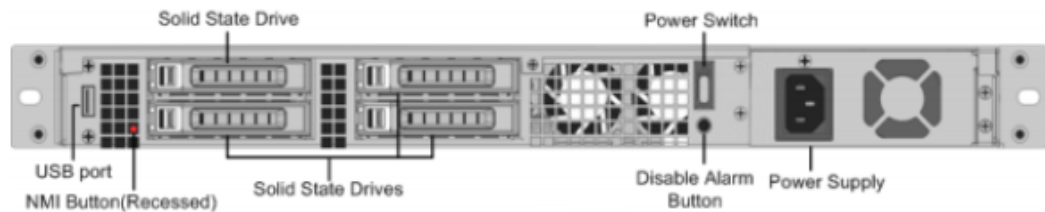
Bevor Sie beginnen

- Stellen Sie sicher, dass Sie nur die 1000 Appliance und nicht die 1000 WS konvertieren. Die 1000 WS-Appliance unterstützt keine Konvertierung in die SD-WAN Premium (Enterprise) Edition-Appliance.
- Stellen Sie sicher, dass Sie über die Standardanmeldeinformationen verfügen, um sich bei der vorhandenen *Dom-0 - root/nsroot* anzumelden.

Upgradeverfahren

Das Konvertierungsverfahren ist ein zweistufiger Prozess, der die folgenden Schritte umfasst:

- Setzen Sie den beiliegenden USB-Stick in die Citrix SD-WAN Appliance ein.
- Stellen Sie sicher, dass die serielle Konsole angeschlossen ist, und fahren Sie mit dem Konvertierungsvorgang fort.



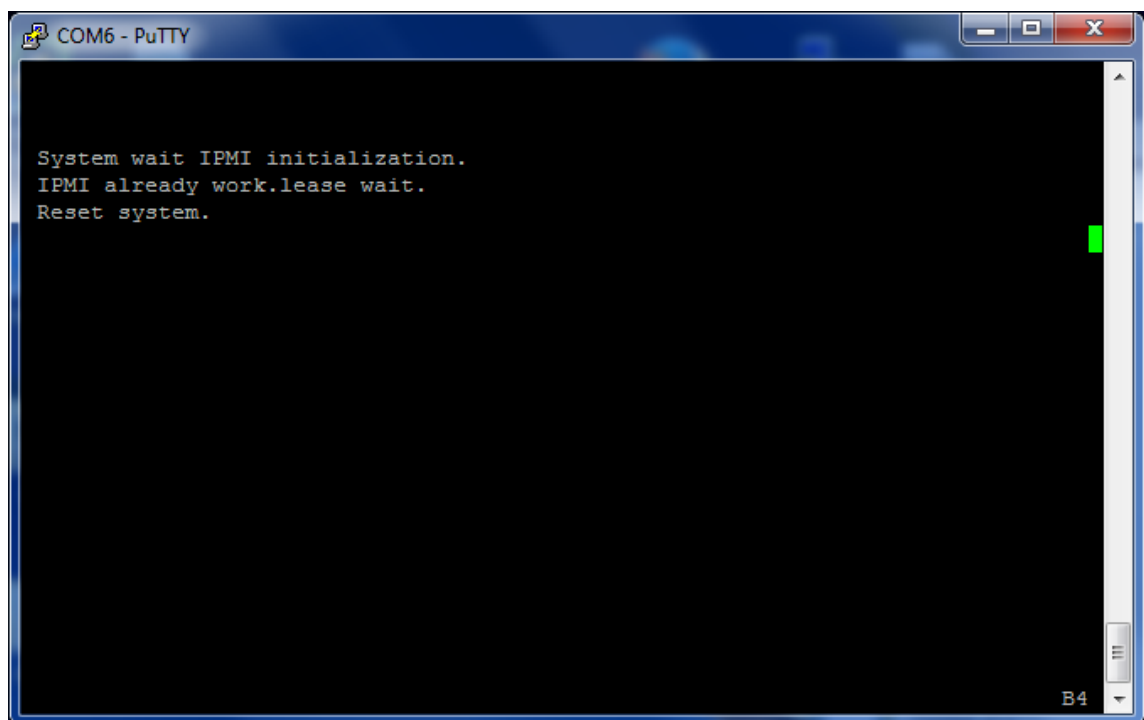
Wie man mit USB-Stick konvertieren

So aktualisieren Sie die Appliance mit einem USB-Stick:

1. Legen Sie den beiliegenden USB-Stick in die Citrix SD-WAN Appliance ein.
2. Verbinden Sie sich mit der seriellen Konsole der Appliance.
3. Starten Sie die Appliance neu.
4. Wenn der Cursor während des Startvorgangs über den Bildschirm bewegt wird, gehen Sie wie folgt vor:
 - a) Halten Sie die **ESC-Taste** gedrückt.
 - b) Halten Sie die **UMSCHALTTASTE** gedrückt.
 - c) Drücken Sie die Taste **1** (SHIFT +1 =!) und lassen Sie alle Tasten los.
 - d) Wiederholen Sie die Schritte a, b und c, bis der Cursor nicht mehr bewegt.

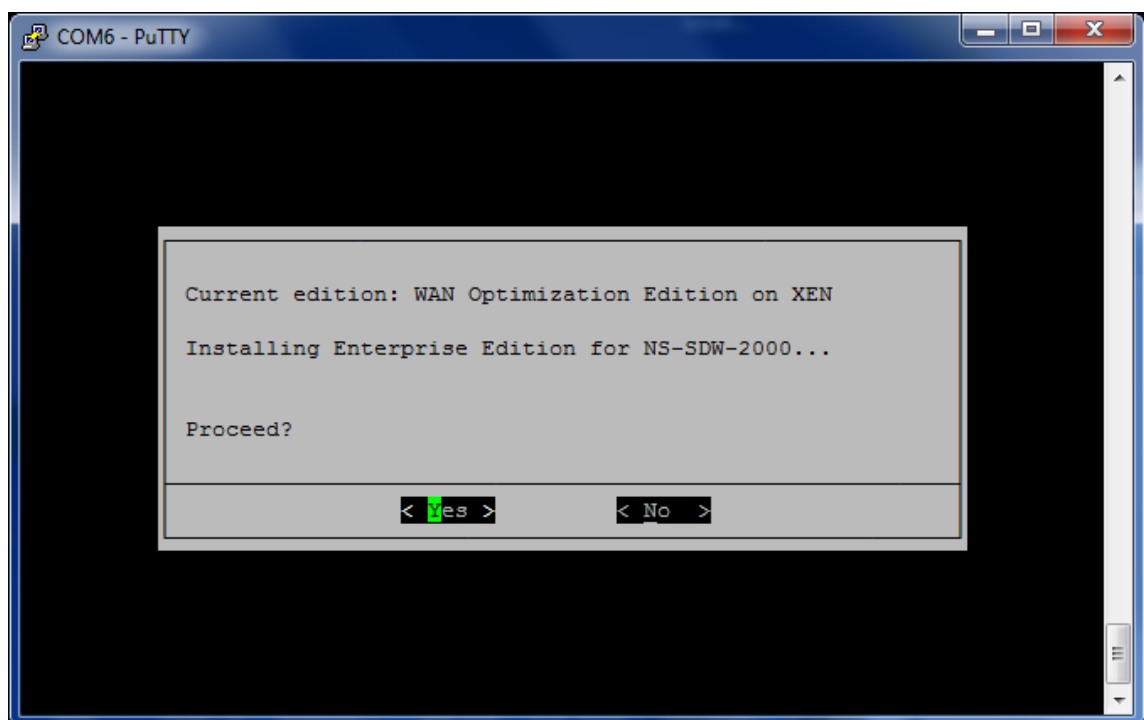
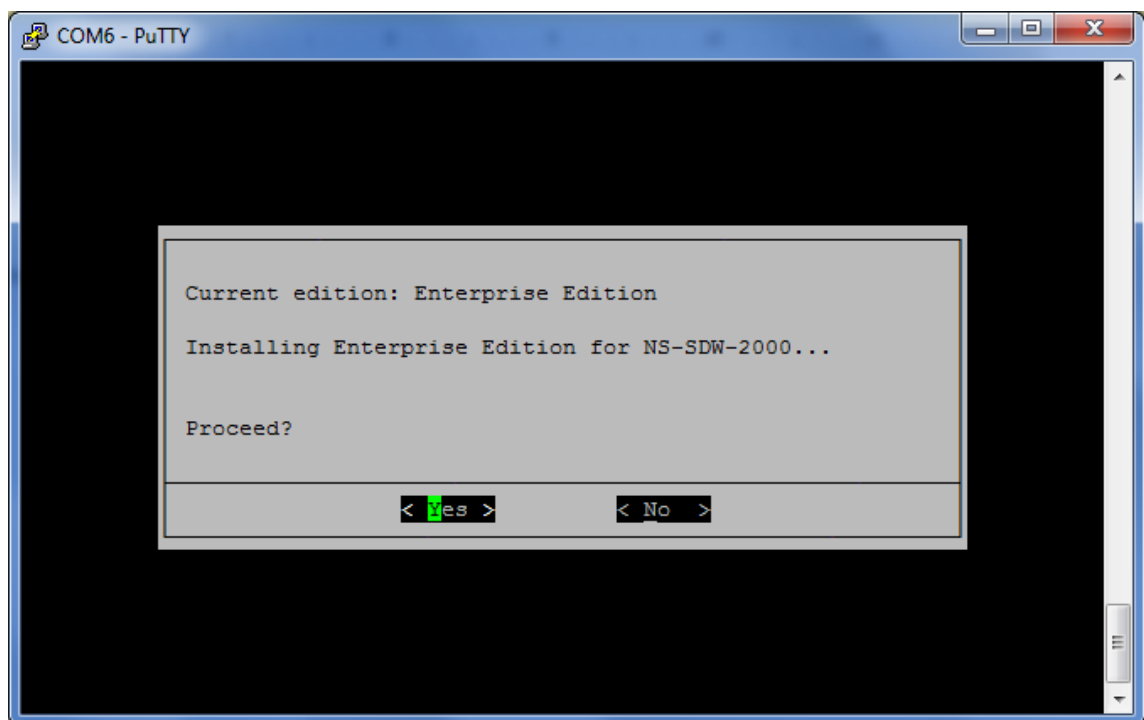
Hinweis

Die oben genannten Schritte sollten während des Neustarts der Appliance ausgeführt werden. Die Tastenstriche sollten während der BIOS-Postphase erfolgen, wie in Schritt 4 beschrieben.



5. Wenn das BIOS geladen wird, wählen Sie beispielsweise das externe USB-Laufwerk; PNY USB 2.0 FD 1100, um die Appliance zu booten. Das externe USB-Laufwerk wird von Citrix ausgeliefert, wenn Sie dafür bestellt haben.

Sie müssen die Plattform-Edition auswählen, die Sie verwenden möchten, wenn die Plattform mehr als eine Edition unterstützt, z. B. 1000 und 2000. Wählen Sie daher zuerst Premium (Enterprise) Edition, bevor Sie die Bestätigung bestätigen.



6. Wählen Sie die **Enterprise Edition-Softwareupdate-Option**, wenn Sie dazu aufgefordert werden.
7. Der Upgrade-Prozess ist in 20-30 Minuten abgeschlossen. Das System startet nach 1-2 Minuten neu und die Anmeldeaufforderung wird angezeigt. Für die 1000-Plattform-Edition dauert der Upgrade-Prozess etwa eine Stunde, da die Aktualisierung des internen USB-Laufwerks selbst

etwa eine halbe Stunde dauert.

8. Ziehen Sie den USB-Stick nach Abschluss des Vorgangs ab.



Referenzen

- Lizenzierung für Citrix SD-WAN Produkte finden Sie im Support-Link unter: <http://support.citrix.com/article/ctx131110>
- Informationen zu Dokumentation und Versionshinweisen zu Citrix SD-WAN finden Sie unter; <http://support.citrix.com/article/ctx131110>

Standard Edition in Premium Edition umwandeln

May 10, 2021

Wichtig

In Release Version 10.1 wird die Plattform-Edition “Enterprise” auf den Begriff “Premium” umbenannt.

So führen Sie eine Plattformkonvertierung von Standard Edition in Premium (Enterprise) Edition durch:

1. Exportieren Sie die Konfiguration lokal.
2. Laden Sie das **Active Package** von der Seite **Änderungsverwaltung** herunter.

3. Aktualisieren Sie die Appliance mithilfe des heruntergeladenen Pakets von **Systemwartung > Update-Software > Reimage Virtual WAN Appliance software**.
4. Klicken Sie auf **Datei auswählen**, um die Datei *cb-vw_CB1000_x.x.x.x.tar.gz* anzugeben. Dabei ist x.x.x.x die Version der SD-WAN-Software.
5. Klicken Sie auf **Upload**. Wählen Sie **Akzeptieren** aus und klicken Sie auf **Installieren**, um for
6. Installieren Sie die Premium (Enterprise) Edition-Lizenz.
7. Führen Sie die **lokale Änderungsverwaltung** auf der Appliance mithilfe des heruntergeladenen aktiven Pakets in Schritt 2 aus.

Im Folgenden sind die Bedingungen für die WAN-Optimierungsbereitstellung Provisioning:

1. Wenn die Site-Rolle MCN ist, erfolgt die WAN-Optimierungsbereitstellung nur:
 - Das Software-Upgrade erfolgt mit dem ZIP-Paket (SSUP)
 - Lizenz ist PE
 - Der virtuelle WAN-Dienst ist aktiviert
2. Wenn die Site-Rolle Client ist, geschieht die WAN-Optimierungsbereitstellung nur:
 - Das Software-Upgrade erfolgt mit dem ZIP-Paket (SSUP)
 - Der virtuelle WAN-Dienst ist aktiviert
 - Lizenz ist PE
 - Virtual Path wird mit MCN gebildet
3. Um die WAN-Optimierung sofort bereitzustellen, legen Sie den Wert für das Wartungsfenster auf der Seite Änderungsverwaltungseinstellungen für die entsprechende Site auf 0 fest.

USB-Reimage-Dienstprogramm

May 10, 2021

Das SD-WAN USB reimage Utility ermöglicht die Neuverwendung von Hardware, indem ein sauberes Factory-Image von einem bootfähigen USB-Stick installiert wird. Citrix stellt ein USB-Stick Field Replaceable Unit (FRU) mit einem vorinstallierten SD-WAN-Softwareimage zur Verfügung. Verwenden Sie die USB-FRU, um ein Image der Appliance auf die erforderlichen unterstützten Editionen (SE/PE/AE) zu erstellen. Die verwendete Appliance-Lizenz/-Konfiguration bestimmt die Appliance-Edition.

Die folgende Tabelle enthält Details zu den verfügbaren USB-FRU-Images und den von SD-WAN-Appliances unterstützten Editionen.

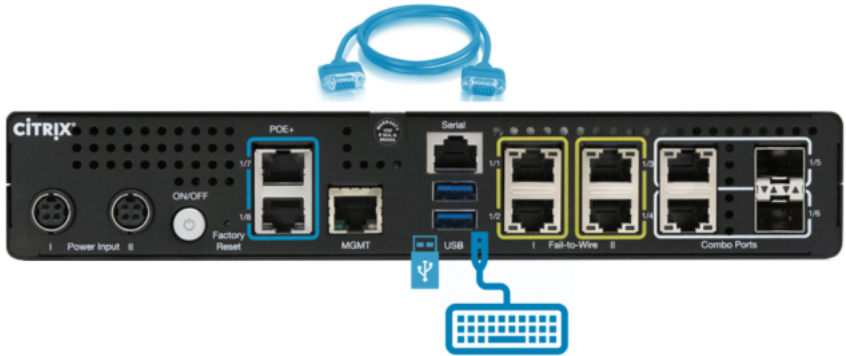
| Gerät | USB-FRU-Image | Unterstützte Editionen |
|--------------------|---------------|------------------------|
| Citrix SD-WAN 110 | 11.1.1.39 | SE |
| Citrix SD-WAN 210 | 10.2.7.17 | SE, AE |
| Citrix SD-WAN 410 | 10.2.3.32 | SE |
| Citrix SD-WAN 1100 | 10.2.7.17 | SE, PE, AE |
| Citrix SD-WAN 2100 | 10.2.7.17 | SE, PE |
| Citrix SD-WAN 4100 | 10.2.7.17 | SE |
| Citrix SD-WAN 5100 | 10.2.7.17 | SE, PE |
| Citrix SD-WAN 6100 | 10.2.7.17 | SE, PE |

So führen Sie ein USB-Reimaging durch:

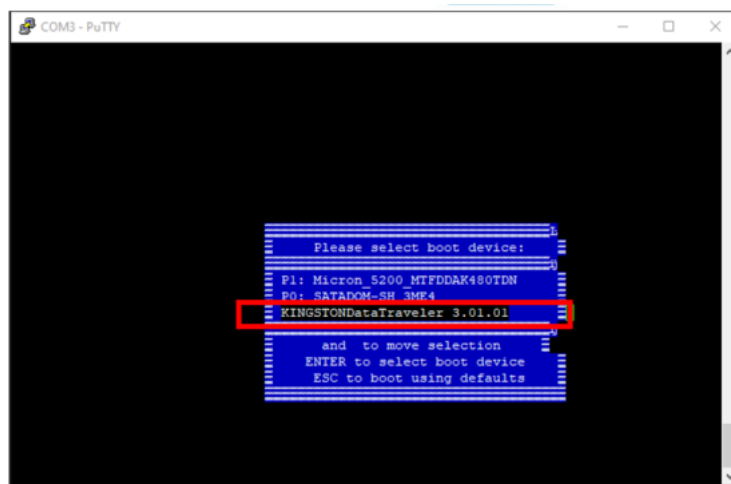
1. Stecken Sie den von Citrix bereitgestellten USB-Stick in einen der USB-Ports der Appliance ein.
2. Schließen Sie eine USB-Tastatur an einen anderen USB-Port an.

Tipp

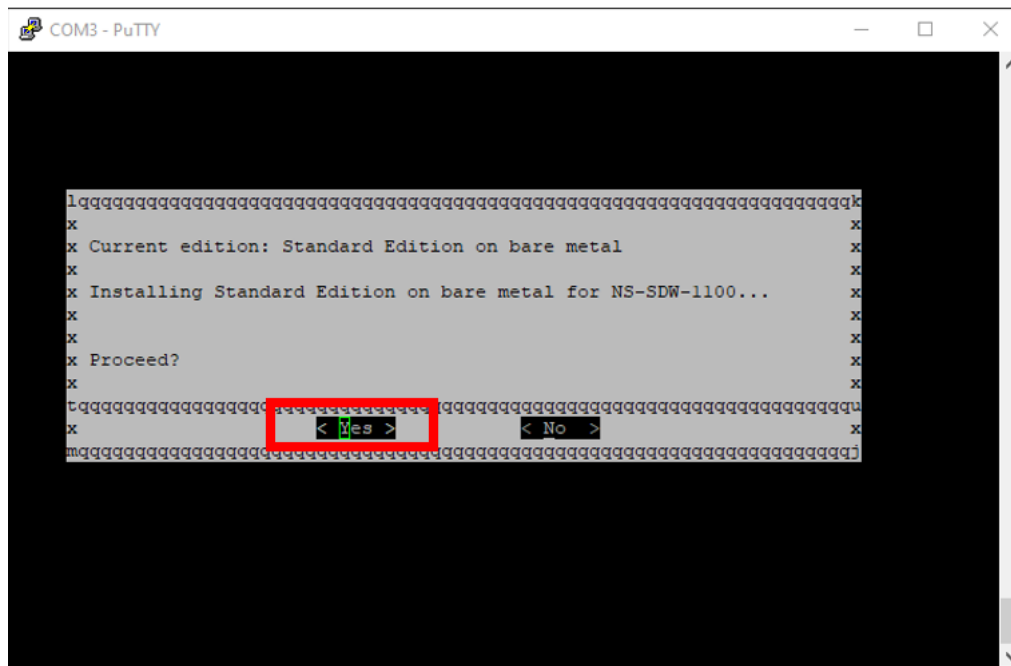
Wenn sich an der Appliance ein einzelner USB-Anschluss befindet, verwenden Sie einen USB-Splitter, um sowohl den USB-Stick als auch die USB-Tastatur anzuschließen.



3. Melden Sie sich als Administrator bei der seriellen Konsole an und geben Sie den Befehl zum Neustart der Appliance über die CLI aus.
4. Drücken Sie beim Hochfahren kontinuierlich die Taste **F11** auf der über USB angeschlossenen Tastatur oder **SHIFT+ESC+1** über eine serielle Konsolenverbindung.
5. Wählen Sie das USB-Laufwerk aus dem Startgerätemenü und drücken Sie die Eingabetaste.



6. Abhängig von der Edition, die für die Plattform unterstützt wird, erscheint ein Bildschirm, in dem Sie die Erlaubnis erhalten, mit der Installation fortzufahren. Wählen Sie **Ja** aus.



Hinweis

Für PE- und AE-Reimage wird die Appliance möglicherweise in der GUI als Standard Edition angezeigt, bis die entsprechende Betriebssystem- und PE/AE-Lizenzinstallation abgeschlossen ist.

Die Installation dauert 30 Minuten. Schalten Sie das Gerät während des Reimaging-Vorgangs nicht aus. Es kann mehrmals neu gestartet werden.

7. Für das Factory-Image ist DHCP standardmäßig aktiviert. Die standardmäßige Verwaltungs-IP-Adresse auf allen Plattformen ist 192.168.100.1. Verwenden Sie es, um auf die SD-WAN GUI zuzu-

greifen.

Sie können die Management-IP auch manuell über die serielle Konsole konfigurieren, indem Sie die folgenden Befehle ausführen:

Ausgabebebefehl ‘*management_ip*’

Ausgabebebefehl ‘*Schnittstelle setzen 192.168.100.1 255.255.255.0 192.168.100.254*’

Ausgabe-Befehl ‘*apply*’

8. Die Software ist standardmäßig ein Upgrade auf SE. Installieren Sie die PE- oder AE-Lizenz je nach Bedarf, je nach den von der Appliance unterstützten Editionen.

Hinweis

Sie können AE-Funktionen nur über den SD-WAN Orchestrator konfigurieren und verwalten. Weitere Informationen, siehe [Edge-Sicherheit](#).

Citrix SD-WAN -Lizenzoptionen

May 10, 2021

Es gibt vier Citrix SD-WAN -Editionen mit jeweils einem anderen Satz oder einer Teilmenge von SD-WAN-Features. Der Lizenztyp, den Sie installieren, bestimmt die Plattformversion - Standard Edition, WANOP Edition, Premium Edition und Advanced Edition-Appliances.

Hinweis

Stellen Sie beim Installieren und Anwenden einer Lizenz sicher, dass Ihre spezifische Appliance die SD-WAN-Appliance-Edition unterstützt, die Sie aktivieren möchten, und dass Sie die richtige Softwareversion zur Verfügung haben.

Citrix SD-WAN Plattformsoftwareunterstützung

Die folgende Tabelle zeigt, welche Citrix SD-WAN Plattformen für jede der verfügbaren SD-WAN-Softwareversionen unterstützt werden.

Hinweis

In Release-Version 10.2 wird die Enterprise-Plattform-Edition in die **Premium** Edition umbenannt.

| Version | WAN-Optimierungs-Edition | Standard Edition | Premium Edition | Advanced Edition |
|----------------------------|--------------------------|------------------|-----------------|------------------|
| Version 7.x | Ja | Nein | Nein | Nein |
| Release 8.x | Nein | Ja | Nein | Nein |
| Release 9.0, 9.1, 9.2, 9.3 | Ja | Ja | Ja | Nein |
| Release 10.0, 10.1, 10.2 | Ja | Ja | Ja | Nein |
| Release 11.0, 11.1 | Ja | Ja | Ja | Nein |
| Release 11.2 | Ja | Ja | Ja | Ja |

Informationen zum Anzeigen aller in Citrix SD-WAN Release 11.2 unterstützten Appliance-Modelle finden Sie unter [Citrix SD-WAN —Datenblatt](#).

Bevor Sie die Software herunterladen können, müssen Sie eine Citrix SD-WAN -Softwarelizenz erwerben und registrieren. Anweisungen zum Erhalt einer SD-WAN-Softwarelizenz erhalten Sie von Citrix Customer Support. Anweisungen zum Hochladen und Installieren der Lizenzdatei auf Ihren Appliances finden Sie im Abschnitt [Hochladen und Installieren der SD-WAN-Softwarelizenzdatei](#). Bevor Sie die Lizenz installieren, müssen Sie zuerst die Appliance-Hardware einrichten und Datum und Uhrzeit für die Appliance festlegen.

Das Lizenzverfahren für die Provisioning Lizenzen für SD-WAN-Plattform-Editionen behandelt die folgenden Themen:

- Unterstütztes SD-WAN-Lizenzmodell: Lokal, Remote und Zentralisiert.
- Remote-Lizenzserver-Unterstützung für SD-WAN-Appliances.
- Voraussetzungen für die Verwendung von Remotelizenzserver.

Hinweis

Ab dem 4. November 2020 gibt es eine Änderung am Prozess "Citrix Lizenzen Return and Modify". Mit diesem neuen Prozess können Sie Ihre Lizenzen nicht über das Portal "Lizenzen verwalten" auf Citrix.com und die My Licensing Tools on Partner Central zurückgeben oder ändern.

Weitere Informationen und eine Liste der Anwendungsfälle finden Sie unter [KB Artikel CTX285157](#).

Lokale Lizenzierung

May 10, 2021

Bei lokaler Lizenz müssen Sie sich bei jeder Appliance im Netzwerk anmelden und die Lizenzdatei hochladen. Selbst mit dem ZTD-Dienst wird die Appliance nur mit einer Gnadenlizenz verfügbar. Sie müssen eine Lizenzdatei für die aktive Netzwerkverbindung hochladen. Die Lizenzdateien werden basierend auf den Host-IDs der einzelnen Appliances generiert.

Sie können die Lizenz für SD-WAN-Appliances über die SD-WAN-Webverwaltungsschnittstelle installieren und konfigurieren.

Importieren von Lizenzen für SD-WAN-Appliances, die auf XenServer/ESXi/Hyper-V-Plattformen bereitgestellt werden:

1. Navigieren Sie in der SD-WAN-Webverwaltungsschnittstelle zu **Konfiguration > Einheiteneinstellungen > Lizenzierung**.
2. Wählen Sie **Lokal** und laden Sie die Lizenz hoch. Klicken Sie auf **Hochladen und Installieren**.
3. Speichern Sie Ihre Änderungen, indem Sie auf **Einstellungen anwenden** klicken.

The screenshot shows the 'License Configuration' web interface. At the top, there's a header 'License Configuration'. Below it, there are two radio buttons: 'Local' (selected) and 'Remote'. Underneath, there's a section titled 'Upload License for this Appliance'. This section contains a 'Filename:' label, a 'Choose File' button, the text 'No file chosen', and an 'Upload and Install' button. Below this section, there's a 'Licenses Uploaded' section. It shows a 'Filename: CCB_4100VW-2000_SSERVER_Retail.lic' with a small square icon to its right. At the bottom of this section, there are two buttons: 'Delete Selected Licenses' and 'Apply Settings'.

Remotelizenzierung

May 10, 2021

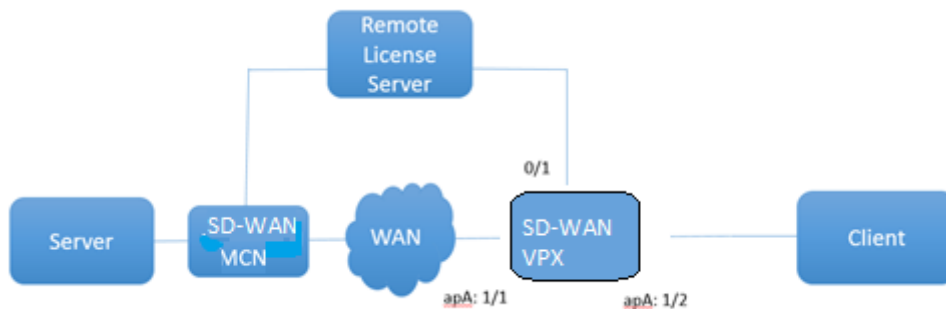
Voraussetzungen für die Verwendung von Remote-Lizenzserver für SD-WAN-Appliances.

- NTP sollte sowohl für Lizenzserver als auch für SD-WAN konfiguriert werden (Datum und Uhrzeit sollten synchronisiert sein)

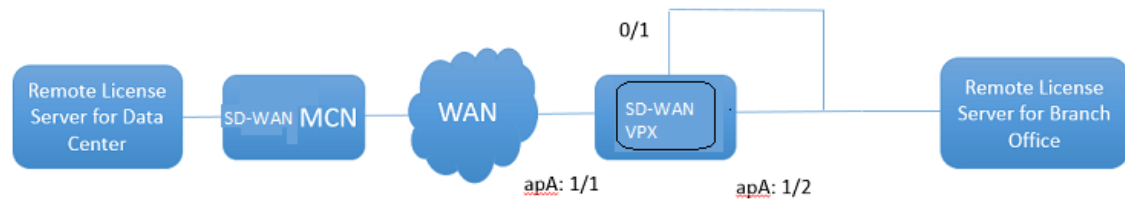
- Es wird empfohlen, die neueste Lizenzserverversion zu verwenden:
 - Release 9.1, 9.2: 11.13.1 L.S
 - Release 10.0, 10.1, 10.2, 11.0, 11.0.1, 11.0.2: 11.14.1 L.S
 - Release 11.0.3, 11.1, 11.2: 11.16.3 L.S

Anwendungsfälle:

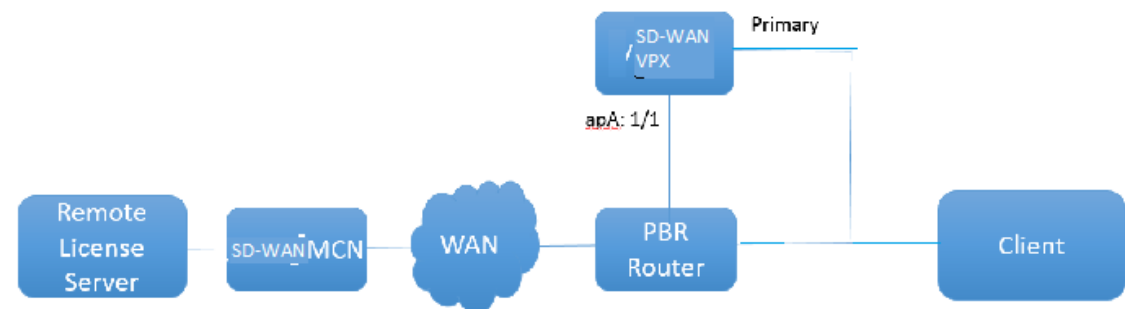
1. Remote-Lizenzserver, der über das Verwaltungsnetzwerk erreichbar ist, ohne Daten/apA-Ports zu verwenden.



2. Remote-Lizenzserver im Zweignetzwerk.

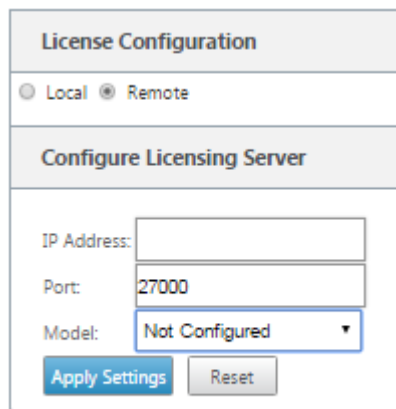


3. SD-WAN VPX-SE - PBR-Bereitstellung in der Zweigstelle.

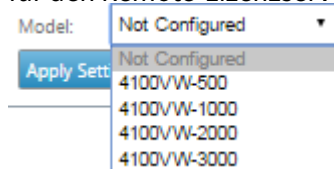


Remote-Lizenz:

1. Navigieren Sie in der SD-WAN-Webverwaltungsschnittstelle zu **Konfiguration > Einheiteneinstellungen > Lizenzierung**.
2. Wählen Sie **Remote** aus, und geben Sie die Details der Remote-Server-IP-Adresse ein.



3. Wählen Sie das gewünschte **Einheitenmodell** aus dem Dropdownmenü aus. Der Standardport für den Remote-Lizenzserver ist 27000.



Wichtig

Wenn Sie Remote-Lizenzen für die SD-WAN-Appliance mithilfe des SD-WAN Centers installieren möchten, stellen Sie sicher, dass Sie die Zentrale Lizenzierung auf der SD-WAN MCN-Appliance in den globalen Einstellungen des Konfigurations-Editors für die SD-WAN-Webverwaltungsschnittstelle aktivieren.

Zentrale Lizenzierung

May 10, 2021

Wenn die Netzwerkbereitstellungen mit einer großen Anzahl von Netzwerkknoten wachsen, wird die Verwaltung und Lizenzierung von Appliances umständlich. Um diesen Prozess für ein effizientes Onboarding der SD-WAN-Appliances und einfache Netzwerkoperationen zu vereinfachen, wurde ein zentralisiertes Lizenzierungsmodell für das SD-WAN-Netzwerk eingeführt.

Im neuen zentralisierten Lizenzmodell bietet die Web-Management-Schnittstelle des SD-WAN Centers (SD-WAN Appliance Management and Reporting Portal) Lizenzierungsdienste für einzelne SD-WAN-Appliances im Netzwerk, ohne dass Sie sich bei der Appliance anmelden müssen.

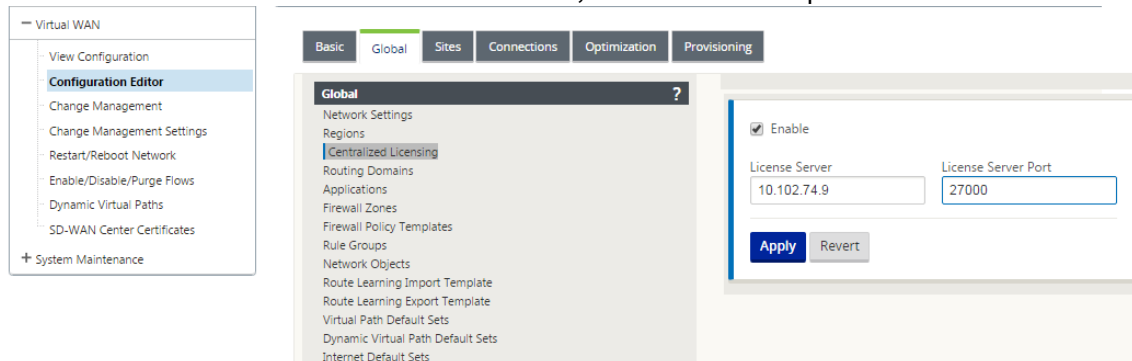
Die IP-Adresse des SD-WAN-Centers wird in der Benutzeroberfläche der SD-WAN-Appliance unter

Global > Zentralisierte Lizenzierung bereitgestellt. Diese IP-Adresse wird über die Konfigurationspakete oder -aktualisierungen an einzelne Appliances weitergegeben. Wenn die IP-Adresse geändert wird, müssen Sie den Change Management-Prozess durchlaufen, um es Appliances zu übertragen. Die globale Einstellung kann durch die lokalen Standorteinstellungen außer Kraft gesetzt werden.

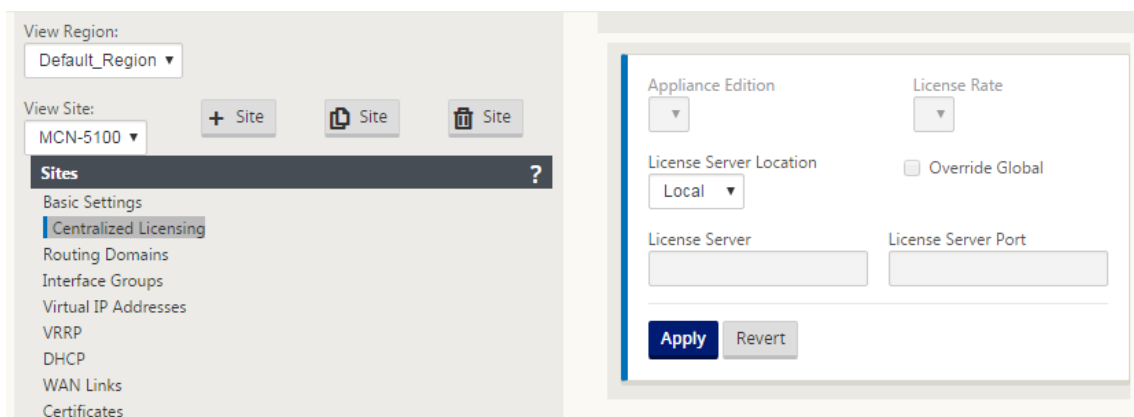
Die Lizenzbandbreite kann mit dem Appliance-Modell für Site-Einstellungen ausgewählt werden. Die Bandbreite der WAN-Verbindungen wird anhand der ausgewählten Lizenz geprüft.

So aktivieren Sie die zentralisierte Lizenzierung in der Benutzeroberfläche der SD-WAN-Appliance:

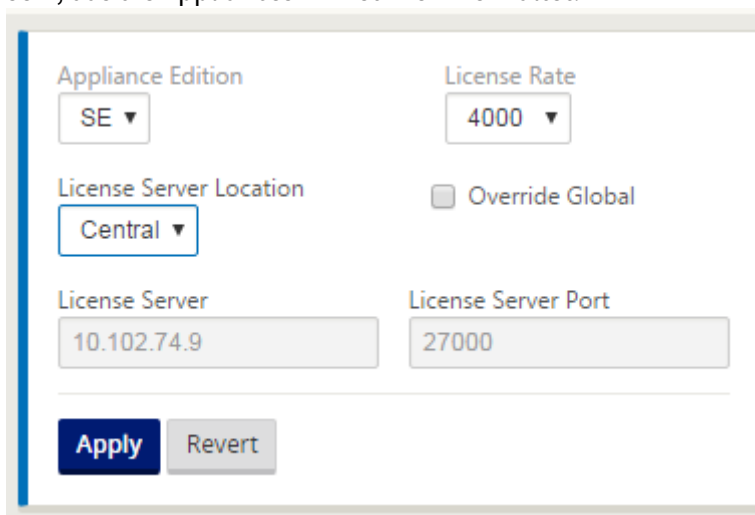
1. Navigieren Sie zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor** . Öffnen Sie ein vorhandenes virtuelles WAN-Konfigurationspaket oder erstellen Sie ein Konfigurationspaket. Das Konfigurationspaket wird geöffnet.
2. Navigieren Sie zur Registerkarte **Global** . Wählen Sie **Zentrale Lizenzierung** aus. Klicken Sie auf **Aktivieren**.
3. Geben Sie die IP-Adresse des Lizenzservers ein, von dem Sie SD-WAN-Lizenzen herunterladen und verwalten können. Geben Sie die SD-WAN Center-Verwaltungs-IP-Adresse an, damit das Konfigurationspaket für den SD-WAN MCN oder Zweige-Appliances die Lizenz vom SD-WAN Center herunterladen kann.
4. Geben Sie **27000** für den **Lizenzserver-Port** ein, der eine Standardportnummer ist.



5. Klicken Sie auf **Übernehmen**.
6. Navigieren Sie zur Registerkarte **Sites** . Wählen Sie unter **Standort anzeigen** die Option MCN oder Zweigstandort aus, je nach Region und Standort, für die Sie die zentrale Lizenzierung verwalten möchten.
7. Wählen Sie **Zentrale Lizenzierung** aus. Die Ansicht der zentralen Lizenzierungsoptionen wird angezeigt. Standardmäßig ist die Option **Lokal** für den **Lizenzserverspeicherort** ausgewählt.



8. Klicken Sie auf das Dropdownmenü, und wählen Sie **Central**, um den Standardspeicherort des Lizenzservers zu ändern. Dadurch werden die IP-Adresse und Port-Informationen angezeigt, die Sie für den Lizenzserver angegeben haben, wenn Sie die zentrale Lizenzierung in den globalen Einstellungen aktivieren. Beispiel: Der Lizenzserver könnte die IP-Adresse des SD-WAN-Centers sein, das die Appliances im Netzwerk verwaltet.



9. Wählen Sie die **Appliance Edition** und den **Lizenzpreis** abhängig von den zu installierenden Appliances. Klicken Sie auf **Übernehmen**.

Hinweis: Sie können die Lizenzserverinformationen überschreiben, die in den globalen Einstellungen der Konfiguration bereitgestellt werden.

10. Wählen Sie **Global überschreiben**, um globale Einstellungen zu überschreiben. Konfigurieren Sie die neue IP-Adresse des Lizenzservers. Behalten Sie die standardmäßige Portnummer des Lizenzservers bei; 27000. Klicken Sie auf **Übernehmen**

Sie können jetzt Lizenzen für alle Knoten in Zweig- und MCN-Standorten verwalten, die für ein bestimmtes SD-WAN-Einheiten-Konfigurationspaket konfiguriert sind.

Der Lizenzserver kann ein SD-WAN Center-Verwaltungsportal sein, das Lizenzen erwirbt, die aus der Netzwerkkonfiguration an die Standorte über den Änderungsmanagement-Prozess erworben werden.

Lizenz basierend auf der Bandbreitenzuweisung:

Jede Appliance kann eine Lizenz auswählen, deren Bandbreite größer oder gleich der konfigurierten Bandbreite ist. Wenn die konfigurierte Bandbreitenlizenz nicht verfügbar ist, wird die Möglichkeit

einer Appliance hinzugefügt, die nächste höhere Bandbreitenlizenz auszuwählen. Diese Funktion gilt sowohl für die zentrale als auch für die Remote-Lizenzserverfunktionalität. Zum Beispiel:

- Wenn Sie drei 410—200 Mbit/s Lizenzen haben. Sie würden dieselben Lizenzen für alle Bandbreitenzuweisungen verwenden, die mit der 410-Appliance verknüpft sind. Standort A (20 Mbit/s), Standort B (50 Mbit/s) und Standort C (200 Mbit/s) sollten 410-200 Mbit/s Lizenzen verwenden können.
- Wenn Sie jeweils eine 410-20 Mbit/s Lizenz und eine 410-200 Mbit/s Lizenz besitzen. Standort A ist für den Verbrauch von 50 Mbit/s konfiguriert, dann kann Standort A 410—200 Mbit/s Lizenz verwenden.

Lizenz-Nachfrist:

Die zulässige Kulanzfrist beträgt 30 Tage, wenn die Lizenzdatei oder die Lizenzkonfiguration von der Appliance entfernt wird. Grace-Warnungen werden für Syslog und E-Mails unterstützt.

Hinweis

Wenn die ausgewählte Lizenzrate nicht mit der konfigurierten WAN-Verbindungsrate übereinstimmt, wird die folgende Meldung auf der Benutzeroberfläche der Appliance für Lizenzierungsereignisse angezeigt.

Meldung: Die gesamte konfigurierte zulässige Rate (LAN zu WAN) NNNN (Kbps) darf die doppelte Lizenzrate, die NNNN (Kbps) ist, nicht überschreiten.

Schweregrad: WARNUNG

Ereignisse: Syslog, E-Mail

Verwalten von Lizenzen

May 10, 2021

Citrix SD-WAN Appliances Lizenzen werden über die Kommunikation mit dem Remotelizenzdienst verwaltet, um nach Lizenzen zu suchen. Wenn die Appliance lizenziert ist, werden die Netzwerkvorgänge ohne Unterbrechung fortgesetzt. Wenn die Appliance nicht lizenziert ist, wird der Gnadenlizenzmodus initiiert.

Lizenzverwaltungsprozess für die SD-WAN-Appliance:

1. Jeder Standort kommuniziert über die Webverwaltungsschnittstelle mit dem Remoteserver oder dem SD-WAN Center. Diese Kommunikation erfolgt über einen Heartbeat-Mechanismus zur Überwachung der Konnektivität und einen Checkout-Mechanismus, der den Lizenzstatus überprüft.

2. Heartbeats werden alle 10 bis 20 Minuten über eine TCP-Verbindung an den Lizenzserver gesendet, um die Konnektivität zu überprüfen.
3. Nach einem Verlust von zwei aufeinanderfolgenden Heartbeats wechselt die Appliance in einen Gnadenmodus. Die Checkout-Methode bestimmt den Lizenzstatus. Dieser Status kann “Real”, “Grace” oder “Verweigert” sein, der vom SD-WAN-Center an die Appliance gesendet wird. Jedes Mal, wenn eine Appliance das SD-WAN Center für den Lizenzstatus erreicht, wird die neue Lizenz eingeecheckt und ausgecheckt. Wenn das SD-WAN-Center keine zwei Herzschläge erhält, gibt das SD-WAN-Center die dem Standort zugewiesene Lizenz in den Pool frei. Die Nachfrist beträgt 30 Tage, so dass nach Verlust von 2 Herzschlägen das Gerät in die Nachfrist geht. Während dieser 30 Tage muss die Kommunikation wiederhergestellt werden. Nach der Wiederherstellung kehrt die Appliance in den normalen Betriebsmodus zurück. Wenn die Kommunikation NICHT wiederhergestellt wird, wird die Appliance in den Status Nicht lizenziert versetzt und folgt dem Verfahren zum Ablauf der Lizenz.

Out-of-Box-Lizenzierung (OOB) für MCN-Appliance:

- Die MCN-Appliance hat keine anfängliche Kulanzfrist. Es muss lizenziert werden, um zu kommen.

Out-of-Box-Lizenzierung (OOB) für Client-Appliance:

- Der Client-Knoten verfügt über eine 30-tägige Gnadenfrist mit oder ohne ZTD-Funktionalität.
- Die Appliance ist mit einer OOB-Lizenzdatei aktiviert, die 30 Tage lang gültig ist.
- Sie haben 30 Tage Zeit, um eine Lizenzdatei hochzuladen oder über den Centralized Licensing Server lizenziert zu werden.
- Wenn die Appliance lizenziert ist, funktioniert sie normal und ist Teil des Netzwerks.
- Wenn die Appliance nicht innerhalb von 30 Tagen lizenziert ist, wird das Lizenzablaufverfahren durchgeführt.

Die einzige Möglichkeit, die Appliance zurückzusetzen, um wieder mit OOB-Lizenz zu kommen, besteht darin, einen “Factory Reset” durchzuführen.

Lizenzablauf

May 10, 2021

Die SD-WAN-Appliance verläuft in eine 30-tägige Kulanzfrist und Sie müssen die Lizenz nach Ablauf der Lizenz hochladen.

Während der Kulanzzeit funktionieren alle Operationen normal. Wenn die Lizenz nicht rechtzeitig hochgeladen wird (30 Tage nach Ablauf), ist Virtual WAN Service deaktiviert.

Zentralisierte Lizenzierung verfügt über eine Protokolldatei, um die Funktionsweise von Kulanzzeitraum, nicht lizenzierte, lizenzierte, Kommunikationsstatus und Fehler zu verfolgen.

In der grafischen Benutzeroberfläche der SD-WAN-Appliance steht unter Diagnose die MCN-Konnektivitätstestfunktionalität im SD-WAN Center für andere Standorte zur Verfügung. Dies kann verwendet werden, um zu testen, ob jede Appliance den Lizenzserver erreichen kann. Sites, Lizenzstatus und Statustabelle stehen für die Verwaltung und Nachverfolgung von Lizenzen zur Verfügung.

Kulanzzeitraum:

1. Für Out-of-Box-Client-Knoten wird eine 30-tägige Nachfrist bereitgestellt. Benachrichtigung zeigt an, dass sich die Appliance im Out-of-Box-Modus befindet und eine gültige Lizenz benötigt. Diese Option verwendet eine Gnadenlizenzdatei.
2. Lizenzablauf: Nach Ablauf der Lizenz wird eine Frist von 30 Tagen bereitgestellt. Benachrichtigung gibt an, dass der Grund für die Kulanzfrist der Lizenzablauf ist und eine Verlängerung erforderlich ist.
3. Verlust der Kommunikation mit SD-WAN Center: Nach 2 Herzschrägen Verlust geht das Gerät für 30 Tage in den Gnadenmodus. Benachrichtigung gibt an, dass der Grund für die Kulanzfrist ein Kommunikationsfehler ist.

Konfiguration

May 10, 2021

Nachdem Sie die SD-WAN-Software und Lizenzen installiert haben, können Sie SD-WAN-Appliance-Einstellungen konfigurieren, um mit der Verwaltung Ihres Netzwerks und der Bereitstellung zu beginnen.

Die Konfiguration der SD-WAN Appliance umfasst Folgendes:

MCN konfigurieren: Der MCN dient als Verteilungspunkt für die anfängliche Systemkonfiguration und alle nachfolgenden Konfigurationsänderungen. Sie führen die meisten Upgradeprozeduren über das Management-Webinterface auf dem MCN aus. In einem virtuellen WAN kann nur ein aktives MCN vorhanden sein.

Standardmäßig haben Appliances die vorab zugewiesene Rolle des Clients. Um eine Appliance als MCN einzurichten, müssen Sie zuerst den MCN-Standort hinzufügen und konfigurieren und dann die Konfiguration und das entsprechende Softwarepaket auf der angegebenen MCN-Appliance bereitstellen und aktivieren.

Zweig konfigurieren: Das Verfahren zum Hinzufügen eines Zweigstandorts ähnelt dem Erstellen und Konfigurieren der MCN-Site sehr. Einige Konfigurationsschritte und -einstellungen unterscheiden sich

jedoch geringfügig für einen Zweigstandort. Wenn Sie einen anfänglichen Zweigstandort hinzugefügt haben, können Sie außerdem für Sites mit demselben Appliance-Modell die Funktion **Klonen** (Duplizieren) verwenden, um das Hinzufügen und Konfigurieren dieser Sites zu optimieren. Wie beim Erstellen des MCN-Standorts müssen Sie zum Einrichten eines Zweigstandorts den **Konfigurations-Editor** im Management-Webinterface auf der MCN-Appliance verwenden. Der **Konfigurations-Editor** ist nur verfügbar, wenn die Schnittstelle auf den **MCN-Konsolenmodus** eingestellt ist.

Konfigurieren des virtuellen Pfads zwischen MCN und Zweigstandorten: Konfigurieren Sie den Virtual Path Service zwischen dem MCN und jedem Client-Sites (Zweig). Dazu verwenden Sie die Konfigurationsformulare und -einstellungen, die im Konfigurationsbaum des **Konfigurationseditors** im Abschnitt **Verbindungen** verfügbar sind.

Aktivieren und Konfigurieren der WAN-Optimierung: Der Abschnitt enthält schrittweise Anweisungen zum Aktivieren und Konfigurieren von SD-WAN Premium (Enterprise) Edition WAN-Optimierungsfunktionen für Ihr Virtual WAN. Dazu verwenden Sie die Formulare für den Abschnitt **Optimierung** im **Konfigurationseditor** der Webverwaltungsschnittstelle auf dem MCN.

Erstinstallation

September 26, 2023

Diese Verfahren müssen für jede Appliance abgeschlossen sein, die Sie Ihrem SD-WAN hinzufügen möchten. Daher erfordert dieser Prozess eine gewisse Abstimmung mit Ihren Standortadministratoren im gesamten Netzwerk, um sicherzustellen, dass die Appliances zur richtigen Zeit vorbereitet und bereit sind. Sobald der Master Control Node (MCN) konfiguriert und bereitgestellt wurde, können Sie Ihrem SD-WAN jedoch jederzeit Client-Appliances (Clientknoten) hinzufügen.

Für jede Appliance, die Sie Ihrem Virtual WAN hinzufügen möchten, müssen Sie Folgendes tun:

1. Richten Sie die SD-WAN Appliance-Hardware und alle SD-WAN VPX Virtual Appliances (SD-WAN VPX-VW) ein, die Sie bereitstellen.
2. Legen Sie die Verwaltungs-IP-Adresse für die Appliance fest, und überprüfen Sie die Verbindung.
3. Legen Sie Datum und Uhrzeit auf der Appliance fest.
4. Legen Sie den Schwellenwert für die **Konsolensitzung** auf einen hohen oder maximalen Wert fest.

Warnung

Wenn Ihre Konsolensitzung ein Timeout vornimmt oder Sie sich vor dem Speichern der Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten Konfigurationsänderungen verloren. Sie müssen sich dann wieder beim System an-

melden und den Konfigurationsvorgang von Anfang an wiederholen. Aus diesem Grund wird dringend empfohlen, dass Sie das **Zeitüberschreitungsintervall** der Konsolensitzung beim Erstellen oder Ändern eines Konfigurationspakets oder beim Ausführen anderer komplexer Aufgaben auf einen hohen Wert festlegen.

5. Laden Sie die Softwarelizenzdatei hoch und installieren Sie sie auf der Appliance.

Anweisungen zum Installieren einer virtuellen SD-WAN Appliance (SD-WAN VPX) finden Sie in den folgenden Abschnitten:

- [Über SD-WAN VPX](#).
- [Installieren und Bereitstellen eines SD-WAN VPX-SE auf ESXi](#).

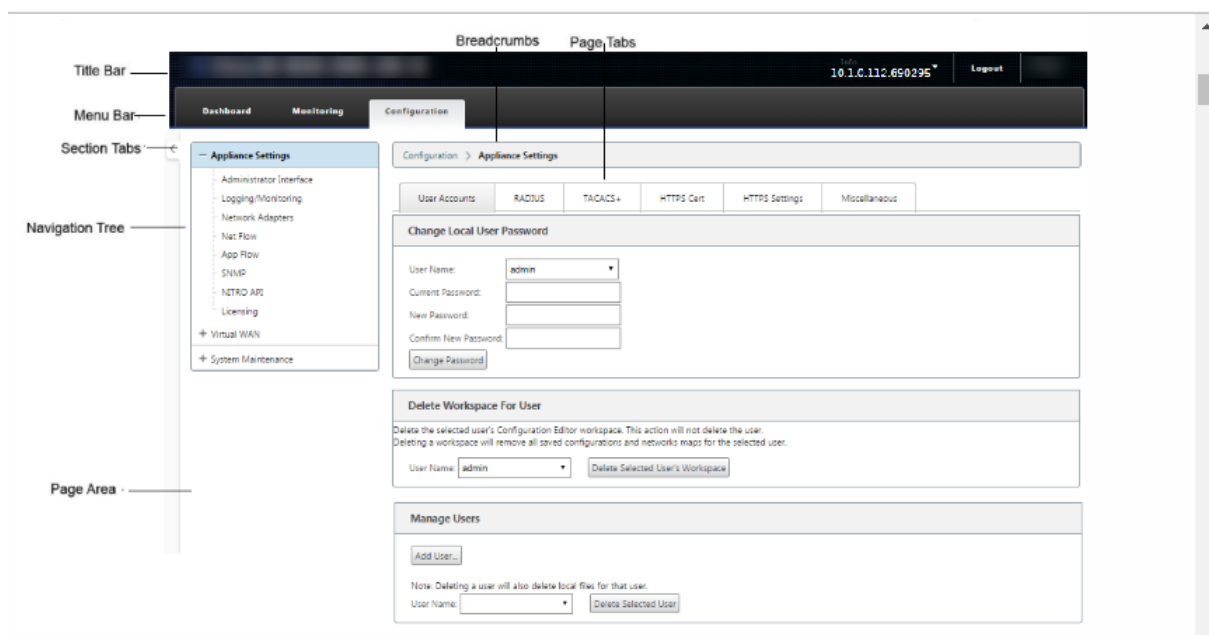
Übersicht über das Layout des Web Interface (UI)

May 10, 2021

Dieser Abschnitt enthält grundlegende Navigationsanweisungen und eine Navigations-Roadmap der Seitenhierarchie der SD-WAN-Webverwaltungsschnittstelle. Ebenfalls enthalten sind spezifische Navigationsanweisungen für den **Konfigurations-Editor** und den **Assistenten für die Änderungsverwaltung**.

Grundlegende Navigation

In der folgenden Abbildung werden die grundlegenden Navigationselemente der Webverwaltungsschnittstelle und die zur Identifizierung verwendete Terminologie beschrieben.



Die grundlegenden Navigationselemente lauten wie folgt:

- **Titelleiste** —Zeigt die Appliance-Modellnummer, Host-IP-Adresse für die Appliance, die Version des derzeit auf der Appliance ausgeführten Softwarepakets und den Benutzernamen für die aktuelle Anmeldesitzung an. Die Titelleiste enthält auch die Schaltfläche **Abmelden** zum Beenden der Sitzung.
- **Hauptmenüleiste** —Dies ist die Leiste, die unter der Titelleiste auf jedem Management-Webinterface-Bildschirm angezeigt wird. Diese enthält die Abschnittsregisterkarten zur Anzeige des Navigationsbaums und der Seiten für einen ausgewählten Abschnitt.
- **Abschnittsregisterkarten** —Die Abschnittsregisterkarten befinden sich in der Hauptmenüleiste oben auf der Seite. Dies sind die Kategorien der obersten Ebene für die Seiten und Formulare der Webverwaltungsschnittstelle. Jeder Abschnitt verfügt über einen eigenen Navigationsbaum zum Navigieren in der Seitenhierarchie in diesem Abschnitt. Klicken Sie auf eine **Abschnittsregisterkarte**, um die Navigationsstruktur für diesen Abschnitt anzuzeigen.
- **Navigationsbaum** —Der Navigationsbaum befindet sich im linken Bereich unterhalb der Hauptmenüleiste. Daraufhin wird der Navigationsbaum für einen Abschnitt angezeigt. Klicken Sie auf eine Abschnittsregisterkarte, um die Navigationsstruktur für diesen Abschnitt anzuzeigen. Der Navigationsbaum bietet folgende Anzeige- und Navigationsoptionen:
 - Klicken Sie auf eine Abschnittsregisterkarte, um die Navigationsstruktur und die Seitenhierarchie für diesen Abschnitt anzuzeigen.
 - Klicken Sie auf + (Pluszeichen) neben einem Zweig in der Struktur, um die verfügbaren Seiten für dieses Zweigthema anzuzeigen.
 - Klicken Sie auf einen Seitennamen, um diese Seite im Seitenbereich anzuzeigen.

- Klicken Sie auf —(Minuszeichen) neben einem Zweigelement, um den Zweig zu schließen.
- **Breadcrumbs** —Zeigt den Navigationspfad zur aktuellen Seite an. Die Breadcrumbs befinden sich oben im Seitenbereich, direkt unter der Hauptmenüleiste. Aktive Navigationslinks werden in blauer Schrift angezeigt. Der Name der aktuellen Seite wird in schwarzer Fettschrift angezeigt.
- **Seitenbereich** —Dies ist die Seitenanzeige und der Arbeitsbereich für die ausgewählte Seite. Wählen Sie ein Element im Navigationsbaum aus, um die Standardseite für dieses Element anzuzeigen.
- **Seitenregisterkarten** —Einige Seiten enthalten Registerkarten, mit denen weitere untergeordnete Seiten für dieses Thema oder dieses Konfigurationsformulars angezeigt werden können. Diese befinden sich oben im Seitenbereich, direkt unterhalb der Paniermehl. Manchmal (wie beim Assistenten für die **Änderungsverwaltung**) befinden sich Registerkarten im linken Bereich des Seitenbereichs zwischen der Navigationsstruktur und dem Arbeitsbereich der Seite.
- **Seitenbereichskalierung** — Bei einigen Seiten können Sie die Breite des Seitenbereichs (oder Abschnitte davon) vergrößern oder verkleinern, um weitere Felder in einer Tabelle oder einem Formular anzuzeigen. In diesem Fall befindet sich am rechten Rand eines Seitenbereiches, eines Formulars oder einer Tabelle eine graue vertikale Größenänderungsleiste. Bewegen Sie den Cursor über die Größenänderungsleiste, bis sich der Cursor in einen bidirektionalen Pfeil ändert. Klicken Sie dann auf und ziehen Sie die Leiste nach rechts oder links, um die Flächenbreite zu vergrößern oder zu verkleinern.

Wenn die Größenänderungsleiste für eine Seite nicht verfügbar ist, können Sie auf den rechten Rand des Browsers klicken und ziehen, um die ganze Seite anzuzeigen.

Dashboard für die Webmanagement-Benutzeroberfläche

Klicken Sie auf die Registerkarte **Dashboard**, um grundlegende Informationen für die lokale Appliance anzuzeigen.

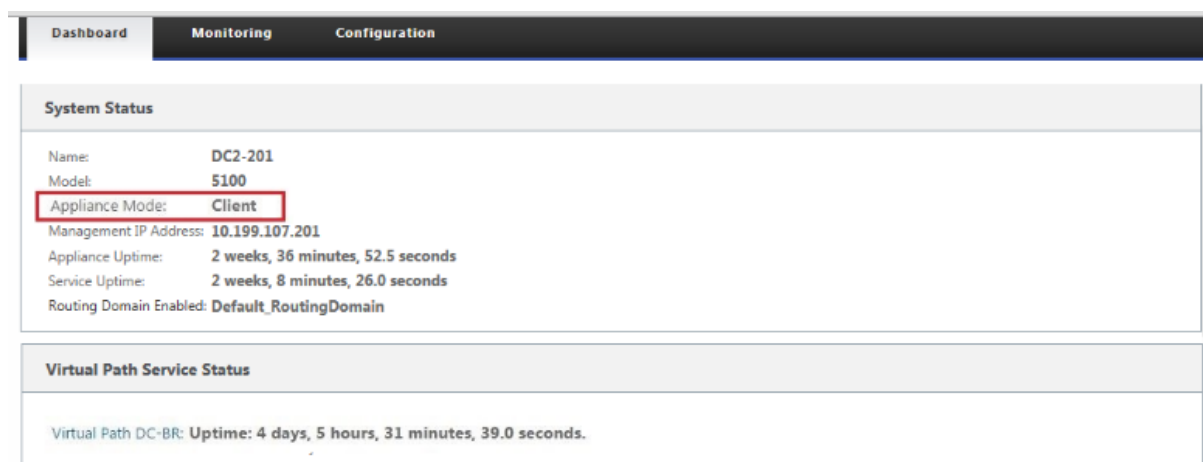
Auf der Seite **Dashboard** werden die folgenden grundlegenden Informationen für die Appliance angezeigt:

- Systemstatus
- Status des virtuellen Pfaddiensts
- Versionsinformationen des Softwarepakets der lokalen Appliance

Die folgende Abbildung zeigt eine Beispielanzeige des Master-Control Node (MCN) **-Appliance-Dashboards**.



Die folgende Abbildung zeigt eine Beispiel-Dashboard-Anzeige der Client-Appliance.



Konfigurationseditor

Mit dem Konfigurations-Editor können Sie Virtual WAN-Appliance-Standorte, Verbindungen, Optimierung und Provisioning hinzufügen und konfigurieren sowie die Virtual WAN-Konfiguration erstellen und definieren.

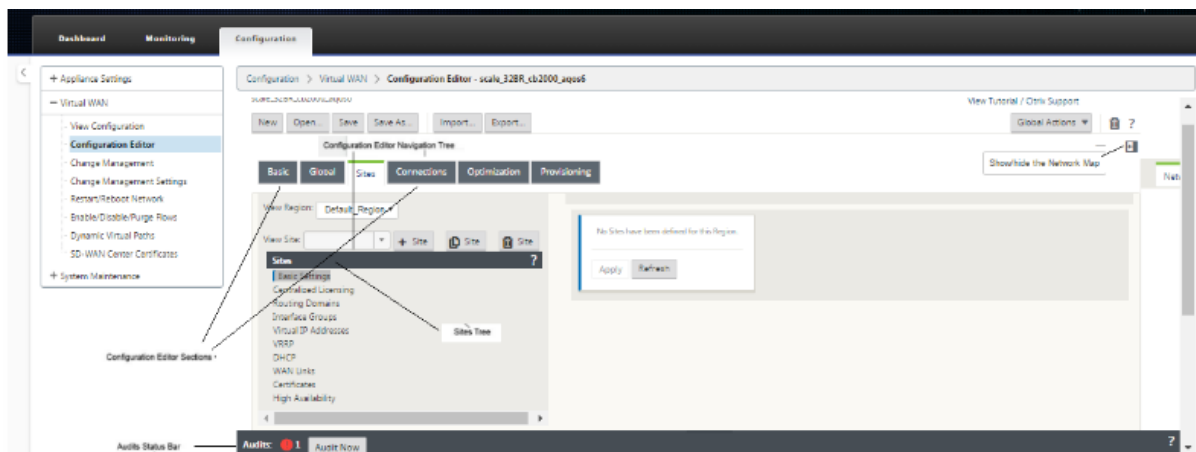
Der Konfigurations-Editor ist nur verfügbar, wenn sich die Webverwaltungsschnittstelle im MCN-Konsolenmodus befindet. Standardmäßig ist das Webinterface einer neuen Appliance auf den Clientmodus eingestellt. Sie müssen die Moduseinstellung auf MCN-Konsole ändern, bevor Sie auf den Konfigurationseditor zugreifen können. Anweisungen finden Sie im Abschnitt [Umschalten der Managementoberfläche in den MCN-Konsolenmodus](#).

Gehen Sie folgendermaßen vor, um zum **Konfigurations-Editor** zu navigieren:

1. Melden Sie sich bei der Webverwaltungsschnittstelle der MCN-Appliance.1 an. Wählen Sie die Registerkarte **Konfiguration.1**. Klicken Sie im Navigationsbaum neben dem **Virtual WAN-Zweig** in der Struktur auf **+**. Dadurch werden die verfügbaren Seiten für die **Virtual**

WAN-Kategorie.1 angezeigt. Wählen Sie im Zweig Virtual WAN der Struktur die Option **Konfigurations-Editor** aus.

In der folgenden Abbildung werden die grundlegenden Navigations- und Seitenelemente des **Konfigurations-Editors** sowie die zur Identifizierung verwendeten Terminologie beschrieben.



Im Folgenden werden die primären Navigations Elemente des **Konfigurations-Editors** beschrieben, auf die in diesem Handbuch verwiesen wird:

- **Menüleiste des Konfigurations-Editors** —Dies befindet sich oben im Seitenbereich, direkt unter den Breadcrumbs Links. Die Menüleiste enthält die primären Aktivitätsschaltflächen für **Konfigurations-Editor-Vorgänge**. Darüber hinaus befindet sich am rechten Rand der Menüleiste die Linkschaltfläche **Tutorial anzeigen**, um das Tutorial zum **Konfigurations-Editor** zu initiieren. Das Lernprogramm führt Sie durch eine Reihe von Blasenbeschreibungen für jedes Element der Anzeige des **Konfigurations-Editors**.
- **Abschnittsstruktur des Konfigurationseditors** —Dies ist der Stapel von dunkelgrauen Balken, der sich im linken Bereich des Seitenbereichs des **Konfigurations-Editors** befindet. Jeder graue Balken stellt einen Abschnitt der obersten Ebene dar. Klicken Sie auf einen Abschnittsnamen, um die Unterzweige für diesen Abschnitt anzuzeigen.
- **Sektionsbaumverzweigungen** —Klicken Sie auf einen Abschnittsnamen im Sektionsbaum, um einen Abschnittszweig zu öffnen. Jeder Abschnittszweig enthält einen oder mehrere Unterzweige von Konfigurationskategorien und Formularen, die wiederum mehrere untergeordnete Zweige und Formulare enthalten können.
- **Sites tree** —Diese Liste listet die Standortknoten auf, die der Configuration hinzugefügt wurden, die derzeit im **Konfigurations-Editor** geöffnet ist. In der Abschnittsstruktur. Klicken Sie auf einen Standortnamen, um den Zweig für diesen Standort zu öffnen. Klicken Sie auf die Site, um einen Zweig zu schließen. Ausführliche Anweisungen zum Navigieren und Verwenden der **Sites-Struktur** und der Konfigurationsformulare finden Sie in den folgenden Abschnitten:
 - [Einrichten des Master Control Node \(MCN\) -Sites](#)

- [Hinzufügen und Konfigurieren der Zweigstandorte](#)

- **Audit-Statusleiste** —Dies ist die dunkelgraue Leiste am unteren Rand der Seite **Konfigurations-Editor** und erstreckt sich über die gesamte Breite des Management-Webinterface-Bildschirms. Die Statusleiste **Audits** ist nur verfügbar, wenn der **Konfigurations-Editor** geöffnet ist. Ein Audit-Warnsymbol (roter Punkt oder Goldrute Delta) ganz links in der Statusleiste zeigt einen oder mehrere Fehler an, die in der aktuell geöffneten Konfiguration vorhanden sind. Klicken Sie auf die Statusleiste, um eine vollständige Liste aller nicht aufgelösten Überwachungswarnungen für diese Konfiguration anzuzeigen.

Assistenten zur Änderungsverwaltung

Die Assistenten für die **Änderungsverwaltung** führen Sie durch den Prozess des Hochladens, des Herunterladens, der Bereitstellung und der Aktivierung der Virtual WAN-Software und der Konfiguration auf der MCN-Appliance (Master Control Node) und den Client-Appliances. Es gibt zwei Versionen des Assistenten für die **Änderungsverwaltung**, eine für das systemweite (“globale”) Virtual WAN und eine für die lokale Änderungsverwaltung, wie folgt:

- **MCN (Global) Change Management Wizard** —Der **MCN Global Change Management Wizard** ist die primäre (Haupt-) Version und ist nur in der Webverwaltungsschnittstelle der MCN-Appliance verfügbar. Verwenden Sie diese Option, um die Virtual WAN-Appliance-Pakete zu generieren, die für jeden Virtual WAN-Appliance-Typ in Ihrem Netzwerk bereitgestellt werden. Sie können den Assistenten auch verwenden, um Konfigurationsänderungen automatisch an Appliances zu übertragen, die bereits in Ihrem virtuellen WAN bereitgestellt wurden. Grundlegende Navigationsanweisungen finden Sie im Abschnitt “Verwenden des MCN Global Change Management Wizard” unten. Anweisungen zur Verwendung des Assistenten für die globale **MCN-Änderungsverwaltung** zum Erstellen der Appliance-Pakete finden Sie im Abschnitt [Vorbereiten der Virtual WAN Appliance-Pakete auf dem MCN](#).
- **Assistent für die lokale Änderungsverwaltung** —Der **Assistent für die lokale Änderungsverwaltung** ist in der Webverwaltungsschnittstelle verfügbar, die sowohl auf dem MCN als auch auf allen Clientknoten Anwendungen ausgeführt wird. Hiermit können Sie das entsprechende Virtual WAN Appliance-Paket auf einer lokalen Appliance hochladen, bereitstellen und aktivieren, die Ihrem Virtual WAN hinzugefügt werden soll. Sie können diesen Assistenten auch verwenden, um ein aktuelles Appliance-Paket speziell auf den lokalen MCN oder auf eine einzelne, lokale virtuelle WAN-Appliance hochzuladen, die bereits in Ihrem Netzwerk bereitgestellt wurde.

Verwenden des MCN-Assistenten für das globale Änderungsmanagement

Gehen Sie folgendermaßen vor, um den MCN Global **Change Management** Wizard zu öffnen:

1. Melden Sie sich bei der Webverwaltungsschnittstelle der MCN-Appliance an.
2. Wählen Sie die Registerkarte **Konfiguration** aus. Klicken Sie im Navigationsbaum neben dem **Virtual WAN-Zweig** in der Struktur auf **+**.
3. Im **Virtual WAN-Zweig**. Wählen Sie **Änderungsverwaltung** aus.

Dies zeigt die erste Seite des Assistenten für die **Änderungsverwaltung**, die Seite **Übersicht über den Änderungsprozess**, an, wie in der folgenden Abbildung dargestellt.

Configuration Filenames: Active - MCN_VPX_23_Site_VPX_JLB_20180517_1430.zip Staged - MCN_VPX_23_Site_VPX_JLB_20180517_1430.zip

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

Global Multi-Region Summary

| Region | Total Sites | Not Connected | Preparing/Staging | Staged | Failed |
|----------------|--------------------|---------------|-------------------|--------|--------|
| Default_Region | 10 | 2 | 0 | 8 | 0 |
| r3 | 7 | 1 | 0 | 6 | 0 |
| r4 | 552 | 1 | 0 | 0 | 0 |
| r4 | Data not available | | | | |

Region - Default Region Details

Show 25 entries

| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Traffic Interruption | | Download Package |
|------------------|-------|-------|-------------------|------------------|------------------|-----------------|----------------------|--------|------------------|
| | | | Software | Config | Software | Config | Expected | Actual | |
| MCN_23-Appliance | CBVPX | | 10.1.0.111.690027 | 11:56 on 6/26/18 | 10.0.2.32.685295 | 17:59 on 6/6/18 | <3 min | 137 s | active / staged |
| Site1-Appliance | CBVPX | | 10.1.0.111.690027 | 11:56 on 6/26/18 | 10.0.2.32.685295 | 17:59 on 6/6/18 | <3 min | 162 s | active / staged |

Active / Staged Download Links

4. Klicken Sie auf Starten, um den Assistenten **zu starten**.

Ausführliche Anweisungen zur Verwendung des Assistenten zum Hochladen, Stationieren und Aktivieren der SD-WAN-Software und -Konfiguration auf den Appliances finden Sie in den folgenden Abschnitten:

- [Vorbereiten der Virtual WAN Appliance-Pakete auf dem MCN](#)
- [Installieren der Virtual WAN Appliance-Pakete auf den Clients](#)

Der Assistent zur **Änderungsverwaltung** enthält die folgenden Navigations Elemente:

- **Seitenbereich** —Zeigt die Formulare, Tabellen und Aktivitätsschaltflächen für jede Seite des **Änderungsmanagement-Assistenten** an.
- **Registerkarten des Assistenten für die Änderungsverwaltung** —Die Seitenregisterkarten befinden sich im linken Bereich des Seitenbereichs auf jeder Seite des Assistenten. Registerkarten werden in der Reihenfolge aufgeführt, in der die entsprechenden Schritte im Prozess des Assistenten ausgeführt werden. Wenn eine Registerkarte aktiv ist, können Sie darauf klicken, um zu einer vorherigen Seite im Assistenten zurückzukehren. Wenn eine Registerkarte

aktiv ist, wird der Name in blauer Schrift angezeigt. Graue Schrift zeigt eine inaktive Registerkarte an. Registerkarten sind inaktiv, bis alle Abhängigkeiten (vorherige Schritte) fehlerfrei erfüllt wurden.

- **Tabelle Appliance-Site** —Dies befindet sich am unteren Rand des Assistentenseitenbereichs auf den meisten Assistentenseiten. Die Tabelle enthält Informationen zu den einzelnen konfigurierten Appliance-Standorten sowie Links zum Herunterladen der aktiven oder bereitgestellten Appliance-Pakete für das jeweilige Appliance-Modell und den Standort. Ein Paket in diesem Kontext ist ein Zip-Dateipaket, das das entsprechende SD-WAN-Softwarepaket für dieses Appliance-Modell und das angegebene Konfigurationspaket enthält. Der Abschnitt **Konfigurationsdateinamen** oberhalb der Tabelle zeigt den Paketnamen für die aktuellen aktiven und bereitgestellten Pakete auf der lokalen Appliance.
- **Aktiv/Staged Download-Links** —Diese befinden sich im Feld **Download-Paket** (ganz rechts Spalte) jedes Eintrags in der Tabelle **Appliance-Site**. Klicken Sie auf einen Link in einem Eintrag, um das aktive oder bereitgestufte Paket für diese Appliance-Website herunterzuladen.
- **Beginnen** —Klicken Sie auf **Beginnen**, um den Prozess des **Änderungsmanagement-Assistenten** zu starten und zur Registerkarte **Änderungsvorbereitung** zu wechseln.
- **Staged aktivieren** — Wenn es sich nicht um eine Erstbereitstellung handelt und Sie die derzeit bereitgestellten Konfiguration aktivieren möchten, haben Sie die Möglichkeit, direkt mit dem **Aktivierungsschritt** fortzufahren. Klicken Sie auf **Staged aktivieren**, um direkt zur Seite Aktivierung zu gelangen und die Aktivierung der aktuell bereitgestellten Konfiguration zu initiieren.

Einrichten der Appliance-Hardware

May 10, 2021

Gehen Sie folgendermaßen vor, um die Hardware der Citrix SD-WAN Appliance (physische Appliance) einzurichten:

1. Richten Sie das Chassis ein.

Citrix SD-WAN Appliances können in einem Standard-Rack installiert werden. Platzieren Sie das Gehäuse für die Desktop-Installation auf einer ebenen Fläche. Stellen Sie sicher, dass ein Mindestabstand von 2 Zoll an den Seiten und an der Rückseite des Geräts vorhanden ist, um eine ordnungsgemäße Belüftung zu gewährleisten.

2. Schließen Sie die Stromversorgung an.

- a) Stellen Sie sicher, dass der Netzschalter auf Aus eingestellt ist.

- b) Schließen Sie das Netzkabel an das Gerät und eine Netzsteckdose an.
 - c) Drücken Sie den Netzschalter auf der Vorderseite des Geräts.
- 3. Schließen Sie die Stromversorgung an.
 - a) Stellen Sie sicher, dass der Netzschalter auf Aus eingestellt ist.
 - b) Schließen Sie das Netzkabel an das Gerät und eine Netzsteckdose an.
 - c) Drücken Sie den Netzschalter auf der Vorderseite des Geräts.
- 4. Verbinden Sie den Verwaltungs-Port der Appliance mit einem PC.

Sie müssen die Appliance mit einem PC verbinden, um das nächste Verfahren abzuschließen und die Verwaltungs-IP-Adresse für die Appliance festzulegen.

Hinweis

Stellen Sie vor dem Anschließen der Appliance sicher, dass der Ethernet-Port am PC aktiviert ist. Verwenden Sie ein Ethernet-Kabel, um den Verwaltungs-Port der SD-WAN Appliance mit dem Standard-Ethernet-Port eines PCs zu verbinden.

SD-WAN VPX-SE-Verwaltungsport

Die virtuelle SD-WAN VPX-SE Appliance ist eine virtuelle Maschine, daher gibt es keinen physischen Verwaltungs-Port. Wenn Sie jedoch die Verwaltungs-IP-Adresse für den SD-WAN VPX-SE beim Erstellen der virtuellen VPX-Maschine nicht konfiguriert haben, müssen Sie dies jetzt tun, wie im Abschnitt [Konfigurieren der Verwaltungs-IP-Adresse für den SD-WAN VPX-SE](#) beschrieben.

Die virtuelle SD-WAN VPX-SE Appliance ist eine virtuelle Maschine, daher gibt es keinen physischen Verwaltungs-Port. Wenn Sie jedoch die Verwaltungs-IP-Adresse für den SD-WAN VPX-SE beim Erstellen der virtuellen VPX-Maschine nicht konfiguriert haben, müssen Sie dies jetzt tun, wie im Abschnitt [Konfigurieren der Verwaltungs-IP-Adresse für den SD-WAN VPX-SE](#) beschrieben.

Konfigurieren der Verwaltungs-IP-Adresse

September 26, 2023

Um den Remotezugriff auf eine SD-WAN-Appliance zu aktivieren, müssen Sie eine eindeutige Verwaltungs-IP-Adresse für die Appliance angeben. Um dies zu tun, müssen Sie zuerst die Appliance an einen PC anschließen. Sie können dann einen Browser auf dem PC öffnen und eine direkte Verbindung mit der Managementoberfläche der Appliance herstellen, wo Sie die Verwaltungs-IP-Adresse für diese Appliance festlegen können. Die Verwaltungs-IP-Adresse muss für jede Appliance eindeutig sein.

Die Verfahren zum Festlegen der Management-IP-Adresse für eine Hardware-SD-WAN-Appliance und eine virtuelle VPX-Appliance (Citrix SD-WAN VPX-SE) sind unterschiedlich. Anweisungen zum Konfigurieren der Adresse für jeden Appliance-Gerätetyp finden Sie unter:

- **Virtuelle SD-WAN VPX Appliance** — Siehe die Abschnitte, [Konfigurieren der Verwaltungs-IP-Adresse für die SD-WAN VPX-SE](#) und [\[Unterschiede zwischen einer SD-WAN VPX-SE und SD-WAN WANOP VPX Installation\]](#).

Gehen Sie folgendermaßen vor, um die Verwaltungs-IP-Adresse für eine Hardware-SD-WAN-Appliance zu konfigurieren:

Hinweis

Sie müssen den folgenden Vorgang für jede Hardware-Appliance wiederholen, die Sie Ihrem Netzwerk hinzufügen möchten.

1. Wenn Sie eine Hardware-SD-WAN-Appliance konfigurieren, schließen Sie die Appliance physisch an einen PC an.
 - Wenn Sie dies noch nicht getan haben, schließen Sie ein Ende eines Ethernetkabels an den Verwaltungs-Port der Appliance und das andere Ende an den Standard-Ethernet-Port am PC an.

Hinweis

Stellen Sie sicher, dass der Ethernet-Port auf dem PC aktiviert ist, den Sie für die Verbindung mit der Appliance verwenden.

2. Notieren Sie die aktuellen Ethernet-Port-Einstellungen für den PC, den Sie zum Festlegen der Appliance-Verwaltungs-IP-Adresse verwenden.

Sie müssen die **Ethernet-Porteinstellungen** auf dem PC ändern, bevor Sie die IP-Adresse der Appliance festlegen können. Achten Sie darauf, die ursprünglichen Einstellungen aufzuzeichnen, damit Sie sie nach der Konfiguration der Verwaltungs-IP-Adresse wiederherstellen können.

3. Ändern Sie die IP-Adresse für den PC.

Öffnen Sie auf dem PC die Netzwerkschnittstelleneinstellungen, und ändern Sie die IP-Adresse für Ihren PC folgendermaßen:

- 192.168.100.50

4. Ändern Sie die Einstellung **Subnetzmaske** auf Ihrem PC wie folgt:

- 255.255.0.0

5. Öffnen Sie auf dem PC einen Browser und geben Sie die Standard-IP-Adresse für die Appliance ein. Geben Sie die folgende IP-Adresse in die Adresszeile des Browsers ein:

- 192.168.100.1

Hinweis

Es wird empfohlen, dass Sie den Google Chrome-Browser verwenden, wenn Sie eine Verbindung mit einer SD-WAN-Appliance herstellen.

Ignorieren Sie alle Browserzertifikatwarnungen für das Management-Webinterface.

Dadurch wird der Anmeldebildschirm der SD-WAN-Verwaltungswebschnittstelle auf der angeschlossenen Appliance geöffnet.

6. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie auf **Anmelden**.

- Standardbenutzername des Administrators: *admin*
- Standard-Administratorkennwort: *Kennwort*

Hinweis

Es wird empfohlen, das Standardkennwort zu ändern. Vergewissern Sie sich, dass Sie das Kennwort an einem sicheren Ort aufzeichnen, da die Kennwortwiederherstellung möglicherweise ein Zurücksetzen der Konfiguration erforderlich ist.

Nachdem Sie sich bei der Management-Weboberfläche angemeldet haben, wird die **Dashboard-Seite** angezeigt, wie unten dargestellt.



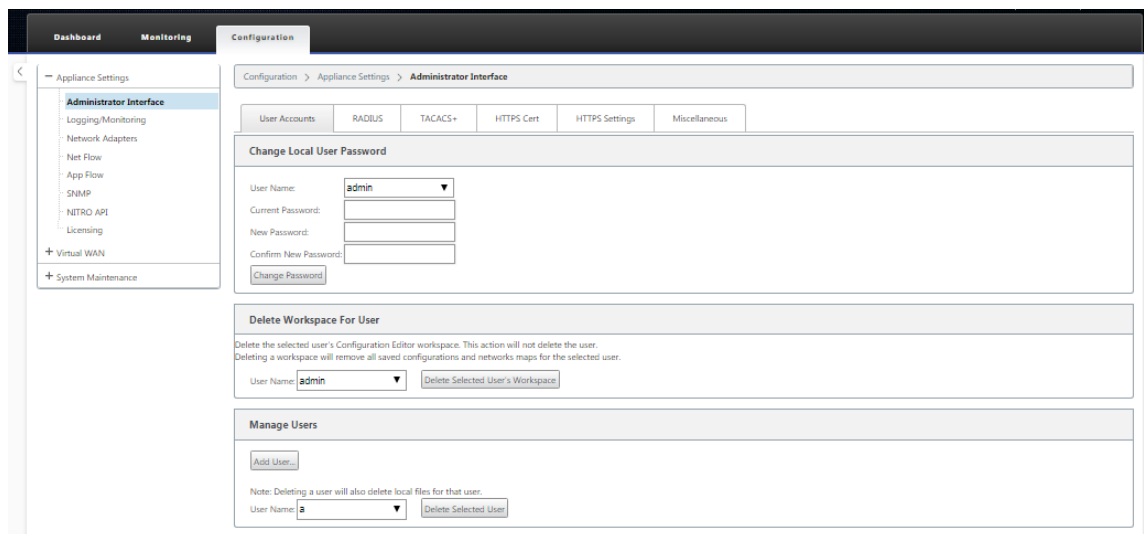
Wenn Sie sich zum ersten Mal bei der Management-Weboberfläche einer Appliance anmelden, zeigt das **Dashboard** ein Warnsymbol (Goldenrod Delta) und eine Warnmeldung an, die angibt, dass der SD-WAN-Dienst deaktiviert ist und die Lizenz nicht installiert wurde. Vorerst können Sie diese Warnung ignorieren. Die Warnung wird behoben, nachdem Sie die Lizenz installiert haben und den Konfigurations- und Bereitstellungsprozess für die Appliance abgeschlossen haben.

7. Wählen Sie in der Hauptmenüleiste die Registerkarte **Konfiguration**.

Daraufhin wird die **Konfigurations-Navigationsstruktur** im linken Bereich des Bildschirms angezeigt. Die **Konfigurations-Navigationsstruktur** enthält die folgenden drei primären Zweige:

- Appliance-Einstellungen
- Virtuelles WAN
- Systemwartung

Wenn Sie die Registerkarte **Konfiguration** auswählen, wird automatisch der Zweig **Appliance-Einstellungen** geöffnet, wobei standardmäßig die Seite **Administratorschnittstelle** vorausgewählt ist, wie in der folgenden Abbildung dargestellt.



8. Wählen Sie im Zweig **Appliance-Einstellungen** der Navigationsstruktur die Option **Netzwerkadapter** aus. Dadurch wird die Einstellungsseite für **Netzwerkadapter** mit der standardmäßig vorausgewählten Registerkarte **IP-Adresse** angezeigt, wie in der folgenden Abbildung gezeigt.

The screenshot shows the Citrix SD-WAN 11.2 Configuration page for Network Adapters. The left sidebar contains a navigation menu with options like Appliance Settings, Administrator Interface, Logging/Monitoring, Network Adapters (selected), Net Flow, App Flow, SNMP, NITRO API, Licensing, Virtual WAN, and System Maintenance. The main content area is titled 'Configuration > Appliance Settings > Network Adapters'. It has tabs for IP Address, Ethernet, and Mobile Broadband. The 'Management Interface IP' section includes a 'DHCP' section with an 'Enable DHCP' checkbox and a 'Manual' section with input fields for IP Address (10.102.78.154), Subnet Mask (255.255.255.0), and Gateway IP Address (10.102.78.1). Below these are 'Change Settings' and 'Clear Settings' buttons. The 'DNS Settings' section has input fields for Primary DNS and Secondary DNS, also with 'Change Settings' and 'Clear Settings' buttons. The 'Management Interface Whitelist' section includes a table for Allowed Network with a Remove button and an Add Network(s) input field. The 'Management Interface DHCP Server' section contains a status indicator (stopped), an 'Enable DHCP Server' checkbox, and input fields for Lease Time (minutes), Domain Name, Start IP Address, and End IP Address. The 'Management Interface DHCP Relay' section has an 'Enable DHCP Relay' checkbox and a 'DHCP Server IP Address' input field. Each section has a 'Change Settings' button.

9. Geben Sie auf der Registerkarte **IP-Adresse** die folgenden Informationen für die SD-WAN-Appliance ein, die Sie konfigurieren möchten.

- IP-Adresse
- Subnetzmaske
- Gateway-IP-Adresse

Hinweis

Die Verwaltungs-IP-Adresse muss für jede Appliance eindeutig sein.

10. Klicken Sie auf **Change Settings**. Es wird ein Bestätigungsdialogfeld angezeigt, in dem Sie aufgefordert werden, zu überprüfen, ob Sie diese Einstellungen ändern möchten.

11. Klicken Sie auf **OK**.

12. Ändern Sie die Netzwerkschnittstelleneinstellungen auf Ihrem PC wieder auf die ursprünglichen Einstellungen.

Hinweis

Wenn Sie die IP-Adresse für Ihren PC ändern, wird die Verbindung zur Appliance automatisch geschlossen und Ihre Anmeldesitzung auf der Management-Weboberfläche beendet.

13. Trennen Sie die Appliance vom PC, und verbinden Sie die Appliance mit Ihrem Netzwerkrouter oder Switch. Trennen Sie das Ethernet-Kabel vom PC, trennen Sie es jedoch nicht von Ihrer Appliance. Schließen Sie das freie Ende des Kabels an Ihren Netzwerkrouter oder Switch an.

Die SD-WAN-Appliance ist jetzt mit Ihrem Netzwerk verbunden und in diesem verfügbar.

14. Testen Sie die Verbindung. Öffnen Sie auf einem PC, der mit Ihrem Netzwerk verbunden ist, einen Browser und geben Sie die Verwaltungs-IP-Adresse ein, die Sie für die Appliance konfiguriert haben.

Wenn die Verbindung erfolgreich ist, wird der **Anmeldebildschirm** für die SD-WAN-Management-Weboberfläche auf der von Ihnen konfigurierten Appliance angezeigt.

Tipp

Melden Sie sich nach dem Überprüfen der Verbindung nicht von der Management-Weboberfläche ab. Sie verwenden es, um die verbleibenden Aufgaben, die in den nachfolgenden Abschnitten beschrieben sind, abzuschließen.

Sie haben nun die Verwaltungs-IP-Adresse Ihrer SD-WAN-Appliance festgelegt und können von jedem Standort im Netzwerk aus eine Verbindung mit der Appliance herstellen.

Datum und Uhrzeit festlegen

May 10, 2021

Bevor Sie die SD-WAN-Softwarelizenz auf einer Appliance installieren, müssen Sie Datum und Uhrzeit auf der Appliance festlegen.

Hinweis

Sie müssen diesen Vorgang für jede Appliance wiederholen, die Sie Ihrem Netzwerk hinzufügen möchten.

Gehen Sie folgendermaßen vor, um Datum und Uhrzeit festzulegen:

1. Melden Sie sich bei der Verwaltungswebschnittstelle der zu konfigurierenden Appliance an.

2. Wählen Sie in der Hauptmenüleiste die Registerkarte **Konfiguration** aus.

Daraufhin wird die **Konfigurations-Navigationsstruktur** im linken Bereich des Bildschirms angezeigt.

3. Öffnen Sie den **Zweig Systemwartung** in der Navigationsstruktur.
4. Wählen Sie im **Zweig Systemwartung** die Option **Datums-/Uhrzeiteinstellungen** aus. Daraufhin wird die Seite **Datums-/Uhrzeiteinstellungen** wie folgt angezeigt.

Configuration > System Maintenance > Date/Time Settings

Note: If the Appliance date/time is turned back due to NTP or manual changes, Reporting artifacts may occur. These can be cleared by creating a new archive of the current database on the Reports screens.

NTP Settings

Use NTP Server ☒

Server Address:

[Change Settings](#)

Date/Time Settings

Date:

Time:

[Change Date](#)

Timezone Settings

Note: After changing the timezone setting, a reboot will also be necessary for any timezone changes to take full effect. Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.

Time Zone:

[Change Timezone](#)

5. Wählen Sie im Dropdownmenü **Zeitzone** am unteren Rand der Seite die Zeitzone aus.

Hinweis

Wenn Sie die Zeitzoneneinstellung ändern müssen, müssen Sie dies vor dem Festlegen von Datum und Uhrzeit tun, sonst bleiben Ihre Einstellungen nicht wie eingegeben erhalten.

6. Klicken Sie auf **Zeitzone ändern**. Dadurch wird die Zeitzone aktualisiert und die aktuelle Datums- und Uhrzeiteinstellung entsprechend neu berechnet. Wenn Sie vor diesem Schritt das richtige Datum und die richtige Uhrzeit festlegen, sind Ihre Einstellungen nicht mehr korrekt. Wenn die Zeitzoneaktualisierung abgeschlossen ist, werden im oberen Bereich der Seite ein Erfolgswarnungssymbol (grünes Häkchen) und eine Statusmeldung angezeigt.
7. (Optional) Aktivieren Sie den NTP-Serverdienst.

- a) Wählen Sie **NTP-Server verwenden** aus.
 - b) Geben Sie die Serveradresse in das Feld **Serveradresse** ein.
 - c) Klicken Sie auf **Change Settings**.
Ein Erfolgswarnungssymbol (grünes Häkchen) und eine Statusmeldung werden angezeigt, wenn die Aktualisierung abgeschlossen ist.
8. Wählen Sie in den Dropdownmenüs **Datum** den Monat, den Tag und das Jahr aus.
 9. Wählen Sie die Stunde, Minuten und Sekunden aus den Dropdownmenüs im Feld **Zeit** aus.
 10. Klicken Sie auf **Datum ändern**.

Hinweis:

Dadurch werden die Datums- und Uhrzeiteinstellung aktualisiert, aber kein Erfolgswarnungssymbol oder keine Statusmeldung angezeigt.

Der nächste Schritt besteht darin, den Schwellenwert für die **Konsolensitzung** auf den Maximalwert festzulegen. Dieser Schritt ist optional, wird jedoch empfohlen. Dadurch wird verhindert, dass die Sitzung vorzeitig beendet wird, während Sie an der Konfiguration arbeiten, was zu einem Arbeitsverlust führen kann. Anweisungen zum Festlegen des **Zeitüberschreitungswertes** für die Konsolensitzung finden Sie im folgenden Abschnitt. Wenn Sie den Timeout-Schwellenwert nicht zurücksetzen möchten, können Sie direkt mit dem Abschnitt fortfahren [Hochladen und Installieren der SD-WAN-Softwarelizenzdatei](#).

Warnung

Wenn Ihre Konsolensitzung ein Timeout vornimmt oder Sie sich vor dem Speichern der Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten Konfigurationsänderungen verloren. Melden Sie sich wieder am System an, und wiederholen Sie den Konfigurationsvorgang von Anfang an.

Sitzungstimeout

May 10, 2021

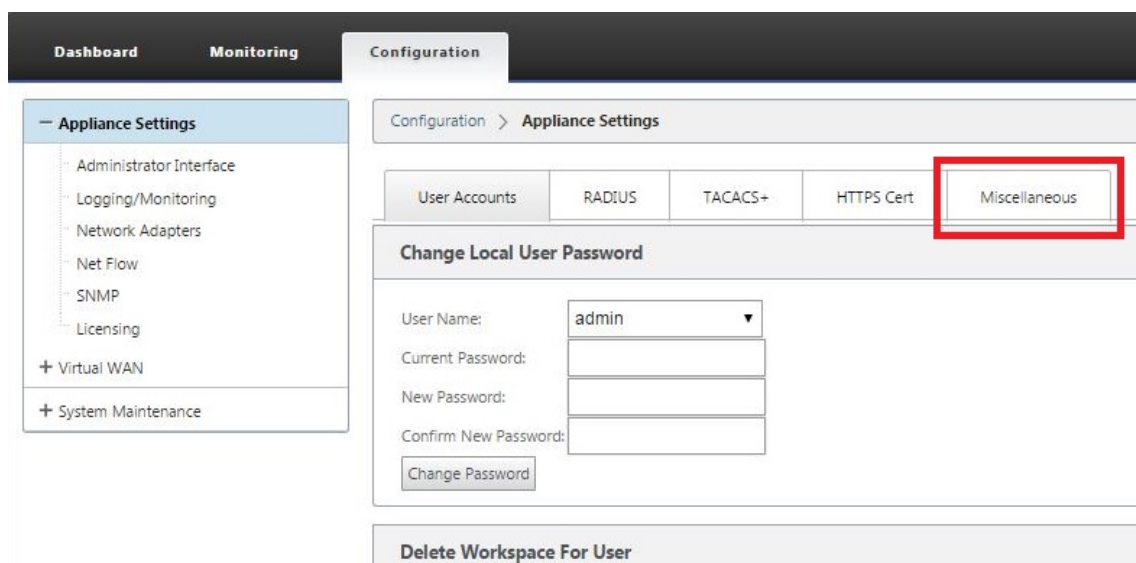
Wenn Ihre Konsolensitzung ein Timeout vornimmt oder Sie sich vor dem Speichern der Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten Konfigurationsänderungen verloren. Sie müssen sich dann wieder beim System anmelden und den Konfigurationsvorgang von Anfang an wiederholen. Aus diesem Grund wird empfohlen, dass Sie das **Timeout-Intervall** für Konsolensitzungen beim Erstellen oder Ändern eines Konfigurationspakets oder beim Ausführen anderer komplexer Aufgaben auf einen hohen Wert festlegen. Der Standardwert beträgt 60 Minuten. Das

Maximum beträgt 9.999 Minuten. Aus Sicherheitsgründen sollten Sie ihn dann auf einen niedrigeren Schwellenwert zurücksetzen, nachdem Sie diese Aufgaben abgeschlossen haben.

Gehen Sie wie folgt vor, um das **Zeitüberschreitungsintervall** der Konsolensitzung zurückzusetzen:

1. Wählen Sie die Registerkarte **Konfiguration** aus, und wählen Sie dann den Zweig **Einheiteneinstellungen** in der Navigationsstruktur aus.


Daraufhin wird die Seite **Einheiteneinstellungen** angezeigt, wobei standardmäßig die Registerkarte **Benutzerkonten** ausgewählt ist.



The screenshot shows the Citrix SD-WAN configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' tab is active, and the 'Appliance Settings' sub-tab is selected. In the left-hand navigation pane, 'Appliance Settings' is expanded, showing options like 'Administrator Interface', 'Logging/Monitoring', 'Network Adapters', 'Net Flow', 'SNMP', 'Licensing', '+ Virtual WAN', and '+ System Maintenance'. The main content area shows the 'Configuration > Appliance Settings' breadcrumb. Below this, there are tabs for 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', and 'Miscellaneous'. The 'Miscellaneous' tab is highlighted with a red box. Under the 'Miscellaneous' tab, the 'Change Local User Password' section is visible. It includes a 'User Name' dropdown menu set to 'admin', and three input fields for 'Current Password', 'New Password', and 'Confirm New Password'. A 'Change Password' button is located below these fields. At the bottom of the section, there is a 'Delete Workspace For User' button.

2. Wählen Sie die Registerkarte **Sonstiges** (ganz rechts).

Daraufhin wird das Register **Sonstiges** angezeigt.



The screenshot shows the Citrix SD-WAN configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' tab is active, and the 'Appliance Settings' sub-tab is selected. In the left-hand navigation pane, 'Appliance Settings' is expanded, showing options like 'Administrator Interface', 'Logging/Monitoring', 'Network Adapters', 'Net Flow', 'SNMP', 'Licensing', '+ Virtual WAN', and '+ System Maintenance'. The main content area shows the 'Configuration > Appliance Settings' breadcrumb. Below this, there are tabs for 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', and 'Miscellaneous'. The 'Miscellaneous' tab is selected. Under the 'Miscellaneous' tab, the 'Change Web Console Timeout' section is visible. It includes a 'Timeout' input field set to '60' and a 'Change Timeout' button. To the right of the input field, there is a text label: 'Enter the new timeout value in minutes (1-9999)'. Below this section, there is a 'Switch to Client Console' section with a 'Switch Console' button.

3. Geben Sie den Wert für die **Zeitüberschreitung der Konsole** ein.

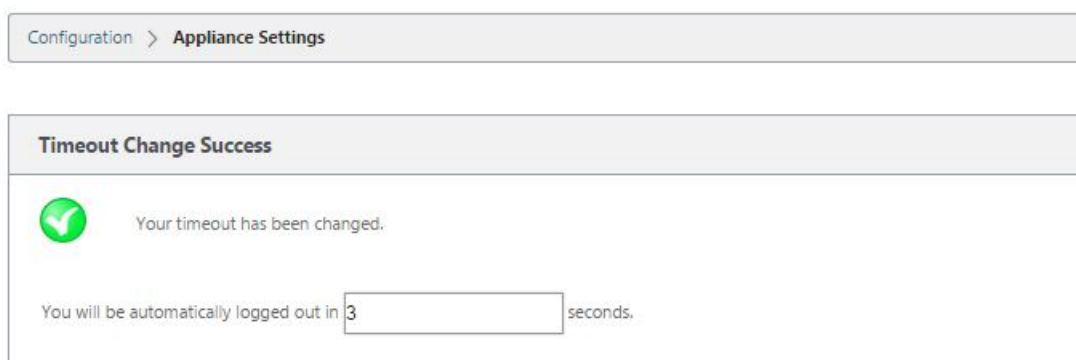
Geben Sie im Abschnitt **Zeitüberschreitung ändern** im Feld **Zeitüberschreitung der Webkonsole** einen höheren Wert (in Minuten) bis zum Maximalwert 9999 ein. Der Standardwert ist 60, was für eine erste Konfigurationssitzung viel zu kurz ist.

Hinweis

Stellen Sie aus Sicherheitsgründen sicher, dass Sie diesen Wert nach Abschluss der Konfiguration und Bereitstellung auf ein niedrigeres Intervall zurücksetzen.

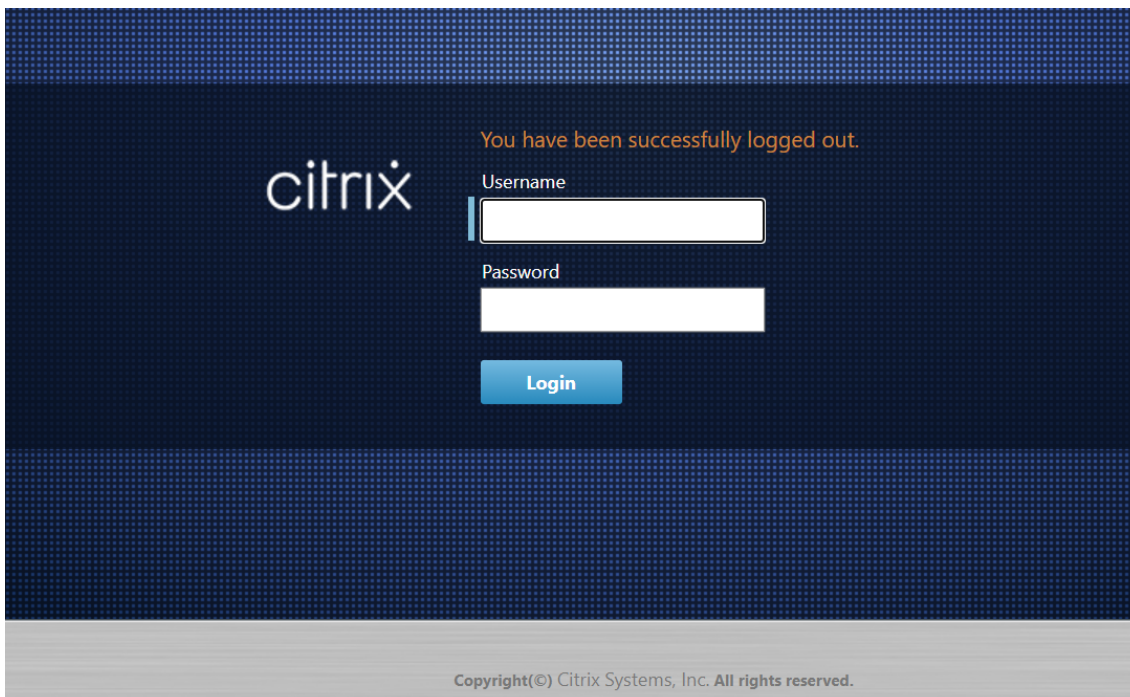
4. Klicken Sie auf **Zeitüberschreitung ändern**.

Dadurch wird das **Zeitüberschreitungsintervall** der Sitzung zurückgesetzt und eine Erfolgsmeldung angezeigt, wenn der Vorgang abgeschlossen ist.



The screenshot shows the 'Appliance Settings' page in the Citrix SD-WAN Management Web Interface. A message box titled 'Timeout Change Success' displays a green checkmark icon and the text 'Your timeout has been changed.' Below this, it states 'You will be automatically logged out in 3 seconds.' The number '3' is in a small input field.

Nach einem kurzen Intervall (einige Sekunden) wird die Sitzung beendet und Sie werden automatisch vom Management Web Interface abgemeldet. Die Anmeldeseite wird angezeigt.



The screenshot shows the Citrix SD-WAN Management Web Interface login page. The background is dark blue with a grid pattern. The Citrix logo is on the left. On the right, there is a message 'You have been successfully logged out.' in orange. Below this, there are input fields for 'Username' and 'Password', and a blue 'Login' button. At the bottom, there is a copyright notice: 'Copyright(©) Citrix Systems, Inc. All rights reserved.'

5. Geben Sie den Administratorbenutzernamen (*admin*) und das Kennwort (*Kennwort*) ein, und klicken Sie auf **Anmelden**.

Der nächste Schritt besteht darin, die SD-WAN-Softwarelizenzdatei auf der Appliance hochzuladen und zu installieren.

Alarmer konfigurieren

May 10, 2021

Sie können jetzt Ihre SD-WAN-Appliance so konfigurieren, dass Alarmbedingungen basierend auf Ihrem Netzwerk und Ihren Prioritäten identifiziert werden, Warnungen generieren und Benachrichtigungen per E-Mail, Syslog oder SNMP-Trap empfangen.

Ein Alarm ist eine konfigurierte Warnung, die aus einem Ereignistyp, einem Triggerzustand, einem klaren Zustand und einem Schweregrad besteht.

So konfigurieren Sie Alarmeinstellungen:

1. Navigieren Sie in der SD-WAN-Webverwaltungsschnittstelle zu **Konfiguration > Appliance-Einstellungen > Logging/Überwachung**, und klicken Sie auf **Alarmoptionen**.
2. Klicken Sie auf **Alarm hinzufügen**, um einen neuen Alarm hinzuzufügen.

| Event Type | Trigger State | Trigger Duration (sec) | Clear State | Clear Duration (sec) | Severity | Email | Syslog | SNMP | |
|--------------|---------------|------------------------|-------------|----------------------|-----------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|
| PATH | DEAD | 0 | GOOD | 0 | EMERGENCY | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| VIRTUAL PATH | DEAD | 0 | GOOD | 0 | CRITICAL | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| WAN LINK | DEAD | 0 | GOOD | 0 | ERROR | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

3. Wählen Sie Werte für die folgenden Felder aus, oder geben Sie sie ein:

- **Ereignistyp:** Die SD-WAN-Appliance kann Alarmer für bestimmte Subsysteme oder Objekte im Netzwerk auslösen, die als Ereignistypen bezeichnet werden. Die verfügbaren Ereignistypen sind SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL, and IPSEC_TUNNEL.
- **Triggerstatus:** Der Ereignisstatus, der einen Alarm für einen Ereignistyp auslöst. Die verfügbaren Optionen für den Triggerstatus hängen vom gewählten Ereignistyp ab.

- **Triggerdauer:** Die Dauer in Sekunden bestimmt, wie schnell die Appliance einen Alarm auslöst. Geben Sie 0 ein, um sofortige Warnungen zu erhalten, oder geben Sie einen Wert zwischen 15-7200 Sekunden ein. Alarmer werden nicht ausgelöst, wenn innerhalb des Zeitraums der Triggerdauer mehrere Ereignisse auf demselben Objekt auftreten. Mehr Alarmer werden nur ausgelöst, wenn ein Ereignis länger als der Zeitraum der Triggerdauer bleibt.
 - **Clear State:** Der Ereignisstatus, der einen Alarm für einen Ereignistyp löscht, nachdem der Alarm ausgelöst wurde. Die verfügbaren Optionen für den Clear State sind vom gewählten Triggerstatus abhängig.
 - **Dauer löschen:** Die Dauer in Sekunden, die bestimmt, wie lange gewartet werden soll, bevor ein Alarm gelöscht wird. Geben Sie '0' ein, um den Alarm sofort zu löschen, oder geben Sie einen Wert zwischen 15-7200 Sekunden ein. Der Alarm wird nicht gelöscht, wenn innerhalb der angegebenen Zeit ein weiteres Clear-State-Ereignis am selben Objekt auftritt.
 - **Schweregrad:** Ein benutzerdefiniertes Feld, das bestimmt, wie dringend ein Alarm ist. Der Schweregrad wird in den Alerts, die bei Auslösung oder Löschvorgang des Alarms gesendet werden, und in der Zusammenfassung der ausgelösten Alarmer angezeigt.
 - **E-Mail:** Alarmauslöser und Löschwarnungen für den Ereignistyp werden per E-Mail gesendet.
 - **Syslog:** Alarmauslöser und Clear Alerts für den Ereignistyp werden über Syslog gesendet.
 - **SNMP:** Alarmauslöser und klare Alarmer für den Ereignistyp werden über SNMP-Trap gesendet.
4. Fügen Sie nach Bedarf weitere Alarmer hinzu.
5. Klicken Sie auf **Einstellungen anwenden**.

Anzeigen von ausgelösten Alarmen

So zeigen Sie eine Zusammenfassung aller ausgelösten Alarmer an:

Navigieren Sie in der SD-WAN-Webverwaltungsschnittstelle zu **Konfiguration > Systemwartung > Diagnose > Alarmer**.

Eine Liste aller ausgelösten Alarmer wird angezeigt.

System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Alarms

Enable Auto Refresh☐ Time Interval 5 seconds Refresh

Clear Checked Alarms

Clear All Alarms

Triggered Alarms Summary

Filters: Any column Apply

Show 100 entries Showing 1 to 11 of 11 entries

| Severity | Event Type | Object Name | Trigger State | Trigger Duration (sec) | Clear State | Clear Duration (sec) | Clear Action |
|-----------|--------------|-----------------------------------|---------------|------------------------|-------------|----------------------|--------------------------|
| EMERGENCY | PATH | Client-1-WL-1-3G->MCN-WL-1-MPLS | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| EMERGENCY | PATH | Client-1-WL-1-MPLS->MCN-WL-1-MPLS | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| CRITICAL | VIRTUAL_PATH | MCN-DC:Client-1 | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| EMERGENCY | PATH | MCN-WL-1-MPLS->Client-1-WL-1-3G | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| EMERGENCY | PATH | MCN-WL-1-MPLS->Client-1-WL-1-MPLS | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| EMERGENCY | PATH | Client-2-WL-1-MPLS->MCN-WL-1-MPLS | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| EMERGENCY | PATH | Client-2-WL-1-3G->MCN-WL-1-MPLS | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| CRITICAL | VIRTUAL_PATH | MCN-DC:Client-2 | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| EMERGENCY | PATH | MCN-WL-1-MPLS->Client-2-WL-1-3G | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| EMERGENCY | PATH | MCN-WL-1-MPLS->Client-2-WL-1-MPLS | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |
| ERROR | WAN_LINK | MCN-WL-1-MPLS | DEAD | 0 | GOOD | 0 | <input type="checkbox"/> |

Showing 1 to 11 of 11 entries

Ausgelöste Alarme löschen

So löschen Sie ausgelöste Alarme manuell:

- 1. Navigieren Sie in der SD-WAN-Webverwaltungsschnittstelle zu **Konfiguration > Systemwartung > Diagnose > Alarme**.
- 2. Wählen Sie in der Spalte **Aktion löschen** die Alarme aus, die Sie löschen möchten.
- 3. Klicken Sie auf **Ausgeprüfte Alarme löschen**. Klicken Sie alternativ auf **Alle Alarme löschen**, um alle Alarme zu löschen.

Rollback konfigurieren

May 10, 2021

Die Funktion Configuration Rollback ermöglicht es dem Change Management-System, die folgenden Software-/Konfigurationsfehler zu erkennen und wiederherzustellen, indem es auf die zuvor aktive Software/Konfiguration zurückgesetzt wird:

- Nach einem Software-Upgrade ist der virtuelle Pfad tot und der Dienst wird deaktiviert, wenn der Software-Absturz auftritt.
- Nach den Konfigurationsänderungen ist der virtuelle Pfad ohne Software-Absturz tot.
- Wenn die Konfiguration für die MCN-Appliance selbst ein Netzwerkproblem auf der MCN-Website verursacht, wird der Ausfall nicht erkannt und sich nicht selbst zurückgesetzt. Alle anderen Clients im Netzwerk setzen sich jedoch selbst zurück, da sie keine Verbindung zum MCN herstellen konnten.

Die Konfigurations-Rollback-Funktion ist standardmäßig aktiviert, um diese Funktion zu deaktivieren, deaktivieren Sie die Option Bei **Fehler zurücksetzen auf** der Registerkarte **Aktivierung** des Assistenten für die Änderungsverwaltung.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Warning: If you have Enterprise Edition appliances in your network, activating the staged changes may cause **traffic disruption**.
Activating staged changes will cause any currently triggered alarms to be silently cleared

Note: For software upgrade, please follow the instructions in release documentation.

Activate Staged Abort ☒ **Revert on Error** Done

Currently Prepared: Configuration - Config-30May.cfg Software - Current Running

Wenn ein Systemkonfigurationsfehler auf einem Client auftritt, während das bereitgestellte Paket von einem MCN aus aktiviert wird, kehrt er zur vorherigen Softwarekonfiguration zurück und eine Fehlermeldung wird wie im folgenden Screenshot gezeigt angezeigt.

Der Client generiert ein kritisches Schweregrad für das SOFTWARE_UPDATE-Objekt, wenn ein Appliance-Absturz erkannt wird, oder generiert ein kritisches Schweregrad für das CONFIG_UPDATE-Objekt, wenn ein Netzwerkausfall erkannt wird.

Dashboard Monitoring Configuration

Click here to collapse the navigation tree

- Logging/Monitoring
- Network Adapters
- Net Flow
- SNMP
- Licensing
- + Virtual WAN
- + System Maintenance

Configuration > Appliance Settings > Administrator Interface

Error:

- This appliance experienced a network outage after an update. Local Change Management has rolled back to the staged software and configuration to resolve the problem.

User Accounts RADIUS TACACS+ HTTPS Cert HTTPS Settings Miscellaneous

Change Local User Password

User Name: admin

Current Password:

New Password:

Confirm New Password:

Change Password

Delete Workspace For User

Delete the selected user's Configuration Editor workspace. This action will not delete the user. Deleting a workspace will remove all saved configurations and networks maps for the selected user.

User Name: admin Delete Selected User's Workspace

Manage Users

Add User...

Note: Deleting a user will also delete local files for that user.

User Name: Delete Selected User

Wenn **Fehler wiederherstellen** aktiviert ist, überwachen die Client-Appliances etwa 30 Minuten lang selbst. Wenn die Software innerhalb von 30 Minuten abstürzt oder das Netzwerk 30 Minuten lang heruntergefahren ist (kein virtueller Pfad zum MCN eingerichtet werden kann), wird ein Rollback ausgelöst.

Auf dem MCN wird eine Fehlermeldung angezeigt, wie im folgenden Screenshot gezeigt. Wenn die Clients wieder dem Netzwerk beitreten, meldet der Typ des aufgetretenen Fehlers. In der Fehlermeldung wird eine zusammengefasste Anzahl der Fehler angezeigt.

Appliance Settings

Virtual WAN

View Configuration

Configuration Editor

Change Management

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

System Maintenance

Configuration > Virtual WAN > Change Management

Error:

This MCN has rolled back the network software and/or configuration to the previous version due to errors detected on the network. A summary of problems follows.

Software Errors : 1

Configuration Errors : 1

Please view [Change Management](#) for a complete list of branch nodes. The nodes with errors will be marked.

Overview

Change Process Overview

The Change Management process allows a user to upload changes to the network, whether it be a configuration, software, or both. This three-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied in a reliable, fail-safe way.

Step 1

Change Preparation

Upload Files to MCN

MCN

Step 2

Appliance Staging

Transfer Files to Clients

MCN

Clients

Step 3

Activation

Activate Change

MCN

Clients

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

Activate Staged

Begin --

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

Search

| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Traffic Interruption | | Download Package |
|--------------------------------|--------|---------------------|--------------------|-----------------|--------------------|------------------|----------------------|--------|------------------|
| | | | Software | Config | Software | Config | Expected | Actual | |
| Dallas_MCN-Appliance | CBVPX | Software Error | 9.3.0.952.99998118 | 4:37 on 6/12/17 | 9.3.0.952.99998118 | 10:56 on 6/12/17 | 0 sec | 0 ms | active / staged |
| Dallas_MCN-Dallas_HA_secondary | CBVPX | | 9.3.0.952.99998118 | 4:37 on 6/12/17 | 9.3.0.952.99998118 | 10:56 on 6/12/17 | 0 sec | 0 ms | active / staged |
| Bangalore-Bangalore-CBVPX | CBVPX | | 9.3.0.952.99998118 | 4:37 on 6/12/17 | 9.3.0.952.99998118 | 10:56 on 6/12/17 | 0 sec | 0 ms | active / staged |
| Bangalore-BLR_HA_secondary | CBVPX | | 9.3.0.952.99998118 | 4:37 on 6/12/17 | 9.3.0.952.99998118 | 10:56 on 6/12/17 | 0 sec | 0 ms | active / staged |
| Beijing-Appliance | CBVPX | | 9.3.0.952.99998118 | 4:37 on 6/12/17 | 9.3.0.952.99998118 | 10:56 on 6/12/17 | 0 sec | 0 ms | active / staged |
| Sanjose-Appliance | CB2000 | Configuration Error | 9.3.0.952.99998118 | 4:37 on 6/12/17 | 9.3.0.952.99998118 | 10:56 on 6/12/17 | 0 sec | 63 ms | active / staged |

Im Fenster **Änderungsverwaltung** des MCN wird der Status der Standort-Appliances angezeigt, der angibt, ob auf diesem Standort ein Softwarefehler oder ein Konfigurationsfehler aufgetreten ist.

Master-Kontrollknoten einrichten

May 10, 2021

Der **SD-WAN Master Control Node (MCN)** ist die Headend-Appliance im Virtual WAN. In der Regel handelt es sich um eine virtuelle WAN-Appliance mit 4000 oder 5100, die im Rechenzentrum des Unternehmens bereitgestellt wird. Der MCN dient als Verteilungspunkt für die anfängliche Systemkonfiguration und alle nachfolgenden Konfigurationsänderungen. Darüber hinaus führen Sie die meisten Upgradeprozeduren über das Management-Webinterface auf dem MCN durch. In einem virtuellen

WAN kann nur ein aktives MCN vorhanden sein.

Standardmäßig haben Appliances die vorab zugewiesene Rolle des Clients. Um eine Appliance als MCN einzurichten, müssen Sie zuerst den MCN-Standort hinzufügen und konfigurieren und dann die Konfiguration und das entsprechende Softwarepaket auf der angegebenen MCN-Appliance bereitstellen und aktivieren.

Zusätzliche Informationen zur Bereitstellung von MCN-Standorten

Die folgenden Knowledge Base-Supportartikel werden empfohlen:

- Schritte zur Bereitstellung virtueller WAN-PBR-Modus ([CTX201577](http://support.citrix.com/article/CTX201577))
<http://support.citrix.com/article/CTX201577>
- Schritte zur Bereitstellung des virtuellen WAN-Gateway-Modus ([CTX201576](http://support.citrix.com/article/CTX201576))
<http://support.citrix.com/article/CTX201576>

Übersicht über die MCN-Standortkonfigurationsprozeduren

Die Schritte zum Hinzufügen und Konfigurieren der MCN-Site lauten wie folgt:

1. Wechseln Sie die Managementoberfläche in den **MCN-Konsolenmodus**.
2. Fügen Sie die MCN-Website hinzu.
3. Konfigurieren Sie die virtuellen Schnittstellengruppen für die MCN-Site.
4. Konfigurieren Sie die virtuellen IP-Adressen für die MCN-Site.
5. (Optional) Konfigurieren Sie die LAN GRE Tunnel für den Standort.
6. Konfigurieren Sie die WAN-Links für die MCN-Site.
7. Konfigurieren Sie die Access Interfaces für die MCN-Site.
8. Konfigurieren Sie die Routen für die MCN-Site.
9. (Optional) Konfigurieren Sie Hochverfügbarkeit für die MCN-Site.
10. (Optional) Konfigurieren Sie Virtual WAN-Sicherheit und Verschlüsselung.
11. Benennen und speichern Sie die MCN-Standortkonfiguration.

Anweisungen für jede dieser Aufgaben finden Sie in den folgenden Abschnitten.

MCN Übersicht

May 10, 2021

Der **Master Control Node (MCN)** ist die zentrale Virtual WAN Appliance, die als Master-Controller des virtuellen WAN fungiert, und der zentrale Verwaltungspunkt für die Clientknoten. Alle Konfigurationsaktivitäten sowie die Vorbereitung der Appliance-Pakete und deren Verteilung an die Clients werden auf dem MCN durchgeführt. Darüber hinaus sind bestimmte Virtual WAN-Überwachungsinformationen nur auf dem MCN verfügbar. Der MCN kann das gesamte virtuelle WAN überwachen, während Clientknoten nur ihre lokalen Intranets überwachen können, zusammen mit einigen Informationen für die Clients, mit denen sie verbunden sind.

Der Hauptzweck des MCN besteht darin, virtuelle Pfade mit einem oder mehreren Clientknoten im virtuellen WAN einzurichten und zu verwenden, die für die Kommunikation zwischen Unternehmensstandort und Standort vorhanden sind. Ein MCN kann virtuelle Pfade zu mehreren Client-Knoten verwalten und haben. Es kann mehr als ein MCN geben, aber nur eine kann zu einem bestimmten Zeitpunkt aktiv sein.

Die folgende Abbildung zeigt die grundlegenden Rollen und den Kontext der MCN-Appliances (Rechenzentrum) und Client-Appliances (Zweigknoten) für eine Virtual WAN Edition-Bereitstellung.



Zur MCN-Konsole wechseln

May 10, 2021

Um die MCN-Website hinzuzufügen und zu konfigurieren, müssen Sie sich zuerst bei der Verwaltungswebschnittstelle auf der Appliance anmelden, die Sie zur MCN-Rolle heraufstufen, und die Verwaltungswebschnittstelle in den **MCN-Konsolenmodus** wechseln. Der **MCN-Konsolenmodus** ermöglicht den Zugriff auf den Konfigurations-Editor im Management-Webinterface, mit dem Sie gerade verbunden sind. Anschließend können Sie den **Konfigurations-Editor** verwenden, um die MCN-Website hinzuzufügen und zu konfigurieren.

Hinweis

Wenn Sie in den **MCN-Konsolenmodus** wechseln, wird nur der Betriebsmodus des Management-Webinterface-Modus und nicht die aktive Rolle der Appliance selbst geändert. Um eine Appliance zur Rolle von MCN heraufstufen zu können, müssen Sie zuerst den MCN-Standort hinzufügen und konfigurieren und das Konfigurations- und Softwarepaket auf der angegebenen MCN-Appliance aktivieren.

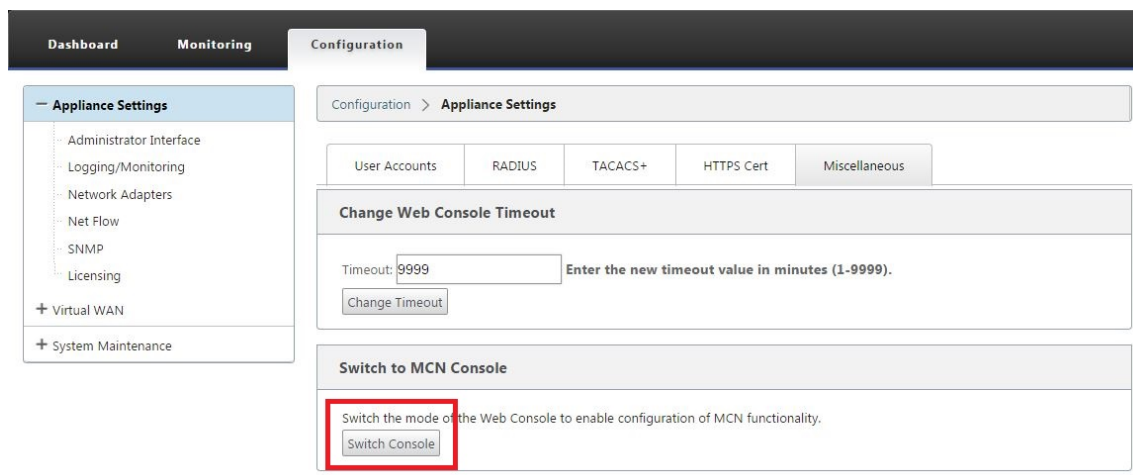
Gehen Sie folgendermaßen vor, um das Management-Webinterface in den **MCN-Konsolenmodus** zu wechseln:

1. Melden Sie sich bei der Managementoberfläche der Appliance an, die Sie als MCN konfigurieren möchten.
2. Klicken Sie in der Hauptmenüleiste des Hauptbildschirms Management Web Interface auf **Konfiguration** (blaue Leiste oben auf der Seite).
3. Öffnen Sie in der Navigationsstruktur (linker Bereich) den Zweig **Einheiteneinstellungen**, und klicken Sie auf **Administratorschnittstelle**.

Dadurch wird die Seite Administratorschnittstelle im mittleren Bereich angezeigt.

4. Wählen Sie die Registerkarte **Sonstiges**.

Daraufhin wird die Seite **Sonstige administrative** Einstellungen angezeigt.



Unten auf der Registerkarte **Sonstiges** ist der Abschnitt Zu [Client > MCN-Konsole wechseln]. **Dieser Abschnitt enthält die** Schaltfläche “Switch Console” zum Umschalten zwischen den Konsolenmodi der Appliance.

Die Abschnittsüberschrift zeigt den aktuellen Konsolenmodus wie folgt an:

- Im **Client-Konsolenmodus** (Standard) lautet die Abschnittsüberschrift **Switch to MCN Console**.

- Im **MCN-Konsolenmodus** lautet die Abschnittsüberschrift **Zur Client-Konsole wechseln**.

Standardmäßig ist eine neue Appliance auf den **Client-Konsolenmodus** eingestellt.

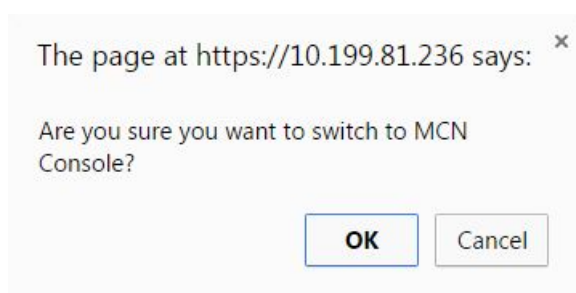
Der **MCN-Konsolenmodus** aktiviert den **Configuration Editor-Zweig** in der Navigationsstruktur. Der **Konfigurations-Editor** ist nur auf der MCN-Appliance verfügbar.

Hinweis

Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie sicher, dass die Appliance weiterhin auf den Standardwert (**Client-Konsolenmodus**) eingestellt ist. Die Abschnittsüberschrift sollte sein: **Wechseln Sie zur MCN-Konsole**.

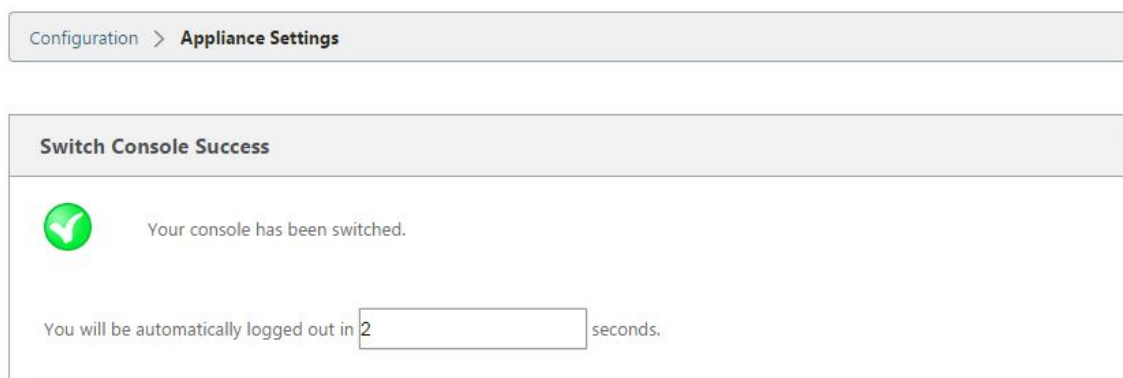
5. Klicken Sie auf **Modus wechseln**, um den Einheitenmodus auf **MCN-Konsolenmodus** festzulegen.

Daraufhin wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, zu bestätigen, dass Sie in den MCN-Modus wechseln möchten.



6. Klicken Sie auf **OK**.

Dadurch wird der Konsolenmodus in den **MCN-Konsolenmodus** umgeschaltet und die aktuelle Sitzung beendet. Eine Erfolgsmeldung wird zusammen mit einem Countdown-Status angezeigt, der angibt, wie viele Sekunden vor dem Beenden der Sitzung verbleiben.



Nach Abschluss des Countdowns wird die Sitzung beendet und die Anmeldeseite wird angezeigt.



7. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie auf **Anmelden**.

- Standardbenutzername des Administrators: *admin*
- Standard-Administratorkennwort: *Kennwort*

Nach der Anmeldung wird das **Dashboard** angezeigt und zeigt nun an, dass sich die Appliance im MCN-Modus befindet.

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN 11.2 interface. It contains three sections:

- System Status:**
 - Name: MCN_23
 - Model: VPX
 - Sub-Model: BASE
 - Appliance Mode: MCN
 - Serial Number: 67e0772c-5190-a2ee-d183-9244189b30a0
 - Management IP Address: 10.102.78.154
 - Appliance Uptime: 1 days, 10 hours, 49 minutes, 48.5 seconds
 - Service Uptime: 1 days, 10 hours, 42 minutes, 20.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions:**
 - Software Version: 10.1.0.111.690027
 - Built On: Jun 21 2018 at 23:42:30
 - Hardware Version: VPX
 - OS Partition Version: 4.6
- Virtual Path Service Status:**
 - Virtual Path MCN_23-Site1: Uptime: 1 days, 10 hours, 39 minutes, 19.0 seconds.

Der nächste Schritt besteht darin, eine neue Konfiguration zu öffnen, die MCN-Site zur Tabelle Sites hinzuzufügen und mit der Konfiguration der neuen MCN-Site zu beginnen.

MCN konfigurieren

May 10, 2021

Der erste Schritt besteht darin, ein neues Konfigurationspaket zu öffnen und die MCN-Site der neuen Konfiguration hinzuzufügen.

Hinweis

Der **Konfigurations-Editor** ist nur im **MCN-Konsolenmodus** verfügbar. Wenn die Option des **Konfigurationseditors** im Zweig Virtual WAN des Navigationsbaums nicht verfügbar ist [Umschalten der Management-Weboberfläche in den MCN-Konsolenmodus](#), finden Sie im Abschnitt Anweisungen zum Ändern des Konsolenmodus.

Es wird empfohlen, das Konfigurationspaket häufig oder an Schlüsselpunkten in der Konfigura-

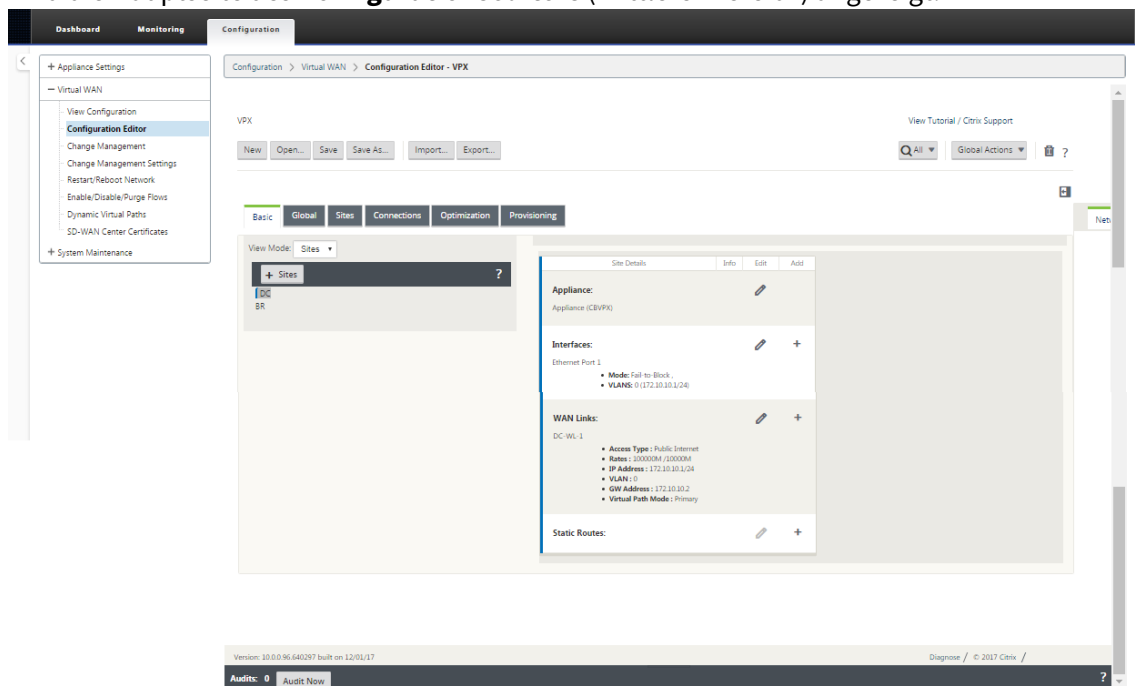
tion zu speichern. Anweisungen finden Sie im Abschnitt [Benennen, Speichern und Sichern der MCN-Standortkonfiguration](#).

Warnung

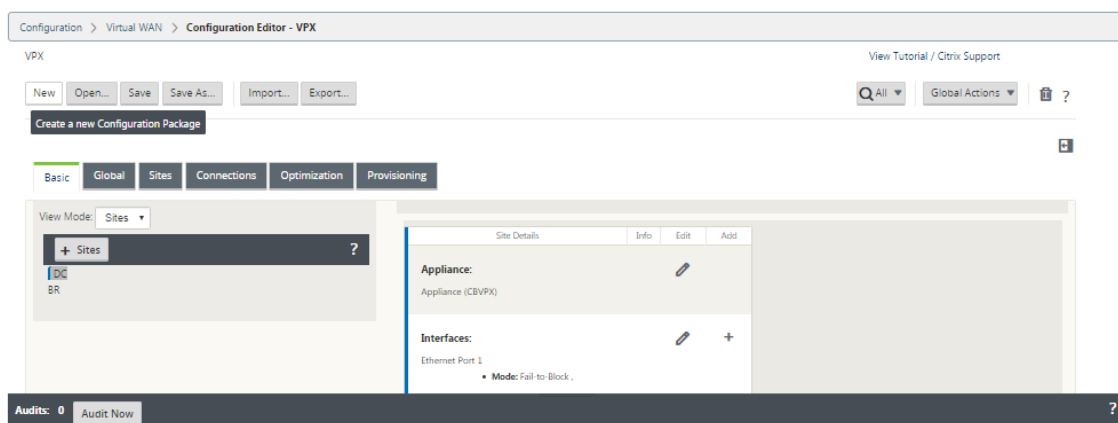
Wenn die Konsolensitzung ein Timeout oder Sie sich vor dem Speichern der Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten Konfigurationsänderungen verloren. Sie müssen sich dann wieder beim System anmelden und den Konfigurationsvorgang von Anfang an wiederholen. Aus diesem Grund wird empfohlen, das Zeitüberschreitungsintervall der Konsolensitzung beim Erstellen oder Ändern eines Konfigurationspakets oder beim Ausführen anderer komplexer Aufgaben auf einen hohen Wert festzulegen. Der Standardwert beträgt 60 Minuten. Das Maximum beträgt 9.999 Minuten. Aus Sicherheitsgründen müssen Sie ihn dann nach Abschluss dieser Aufgaben auf einen niedrigeren Schwellenwert zurücksetzen. Anweisungen finden Sie im Abschnitt [Einstellen des Zeitüberschreitungsintervalls für Konsolensitzungen \(optional\)](#)

Gehen Sie folgendermaßen vor, um die MCN-Appliance-Site hinzuzufügen und mit der Konfiguration zu beginnen:

1. Navigieren Sie in der Navigationsstruktur zu **Virtual WAN > Konfigurations-Editor**. Dadurch wird die Hauptseite des **Konfigurationseditors** (mittlerer Bereich) angezeigt.



2. Klicken Sie auf **Neu**, um mit der Definition einer neuen Konfiguration zu beginnen. Daraufhin wird die Seite **Neue Konfigurationseinstellungen** angezeigt.



3. Klicken Sie in der **Siteleiste auf +Sites**, um mit dem Hinzufügen und Konfigurieren der MCN-Site zu beginnen. Daraufhin wird das Dialogfeld **Site hinzufügen** angezeigt.

4. Geben Sie die Siteinformationen ein.

Gehen Sie wie folgt vor:

1. Geben Sie den **Site-Namen und den Secure Key** ein.
2. Wählen Sie das **Einheitenmodell** aus.
3. Wählen Sie den **Modus** aus.
4. Wählen Sie den **primären MCN** als Modus aus.

Hinweis

Im Menü **Modelloptionen** werden die generischen Modellnamen für die unterstützten Appliance-Modelle aufgeführt. Die generischen Namen enthalten nicht das Standardausgabe-Modellsuffix, entsprechen aber den entsprechenden SD-WAN-Appliance-Modellen. Wählen Sie die entsprechende Modellnummer für dieses SD-WAN-Appliance-Modell aus. (Wählen Sie z. B.

4000 aus, wenn es sich um eine SD-WAN 4000-SE-Einheit handelt.)

Einträge dürfen keine Leerzeichen enthalten und müssen im Linux-Format vorliegen.

So fügen Sie eine Website hinzu:

1. Klicken Sie auf **Hinzufügen**, um die Website hinzuzufügen. Dadurch wird die neue Site zur **Sitestructur** hinzugefügt und das Konfigurationsformular **Grundeinstellungen** für die neue Site angezeigt.

The screenshot displays the Citrix SD-WAN configuration interface. At the top, there are tabs for 'Basic', 'Global', 'Sites', 'Connections', 'Optimization', and 'Provisioning'. The 'Sites' tab is selected. Below the tabs, there is a 'View Region' dropdown set to 'Default_Region'. A 'View Site' dropdown is set to 'NA-DC', with buttons for '+ Site', 'Site', and 'Site'. A 'Sites' sidebar on the left lists various settings: 'Basic Settings' (selected), 'Centralized Licensing', 'Routing Domains', 'Interface Groups', 'Virtual IP Addresses', 'VRRP', 'DHCP', 'WAN Links', 'Certificates', and 'High Availability'. The main configuration area on the right is titled 'Basic Settings' and contains the following fields:

- Site Name:** NA-DC
- Appliance Name:** NA-DC-CBVPX
- Secure Key:** 8a463b0fed92c1a (with a 'Regenerate' button)
- Model:** CBVPX
- Mode:** primary MCN
- Site Location:** (empty field)
- Default Direct Route Cost:** 5
- Gateway ARP Timer (ms):** 1000
- Host ARP Timer (ms):** 1000
- ☐ **Enable Source MAC Learning**

At the bottom of the configuration area are 'Apply' and 'Refresh' buttons.

Nachdem Sie auf **Anwenden** geklickt haben, werden Überwachungswarnungen angezeigt, die darauf hinweisen, dass weitere Maßnahmen erforderlich sind. Ein Rotpunkt- oder Goldrute-Delta-Symbol weist auf einen Fehler in dem Abschnitt hin, in dem es angezeigt wird. Sie können diese Warnungen verwenden, um Fehler oder fehlende Konfigurationsinformationen zu identifizieren. Bewegen Sie den Mauszeiger über ein Überwachungswarnsymbol, um eine kurze Beschreibung der Fehler in diesem Abschnitt anzuzeigen. Sie können auch auf die dunkelgraue **Statusleiste** (unten auf der Seite) klicken, um eine vollständige Liste aller nicht aufgelösten Überwachungswarnungen anzuzeigen. Konfigurierbarer Host-ARP-Timer (ms) wird während der Konfiguration auf Standortebene hinzugefügt. Der aktuelle Standardwert beträgt 1.000 ms. Der konfigurierbare Bereich liegt zwischen 1.000 ms und 180.000 ms. Die Host-ARP-Zeitgeberkonfiguration gilt nicht für den Verwaltungsport.

2. Geben Sie die Grundeinstellungen für die neue Website ein, oder übernehmen Sie die Standardeinstellungen. In Citrix SD-WAN Bereitstellungen wie Gateway und One-Arm werden beim häufigen Empfang der ARP-Anforderungen die Zugriffspunkte überlastet, was sich auf den Datenfluss auswirkt. Sie können jetzt ARP-Timer so konfigurieren, dass ARP-Anforderungen mit bestimmten Intervallzeiten gesendet werden. Das Zeitintervall wird in Sekunden konfiguriert. Sie können ARP-Zeitintervalle konfigurieren, wenn Sie den Rechenzentrumsstandort auf der Registerkarte **Grundeinstellungen** in der Benutzeroberfläche der Citrix SD-WAN Appliance konfigurieren.
3. (Optional, empfohlen) Speichern Sie die Konfiguration in Bearbeitung.

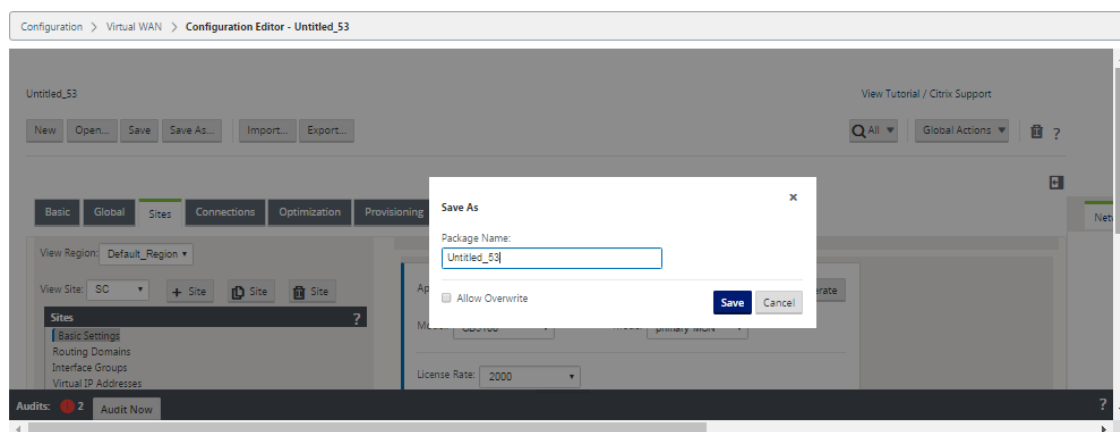
Wenn Sie die Konfiguration nicht in einer Sitzung abschließen können, können Sie sie jederzeit speichern, sodass Sie sie später abschließen können. Die Konfiguration wird in Ihrem Workspace auf der lokalen Appliance gespeichert. Um die Arbeit in einer gespeicherten Konfiguration fortzusetzen, klicken Sie in der Menüleiste des **Konfigurations-Editors** (oben im Seitenbereich) auf **Öffnen**. Daraufhin wird ein Dialogfeld angezeigt, in dem Sie die Konfiguration auswählen können, die Sie ändern möchten.

Hinweis

Als zusätzliche Vorsichtsmaßnahme wird empfohlen, dass Sie Speichern unter anstelle von Speichern verwenden, um ein Überschreiben des falschen Konfigurationspakets zu vermeiden.

Gehen Sie folgendermaßen vor, um das aktuelle Konfigurationspaket zu speichern:

1. Klicken Sie auf **Speichern unter** (oben im mittleren Bereich des **Konfigurations-Editors**). Dadurch wird das Dialogfeld **Speichern unter** geöffnet.



2. Geben Sie den Namen des Konfigurationspakets ein. Wenn Sie die Konfiguration in einem vorhandenen Paket speichern, müssen Sie vor dem Speichern die Option **Überschreiben zulassen** auswählen.
3. Klicken Sie auf **Speichern**.

Konfigurieren von Schnittstellengruppen für den MCN

Nach dem Hinzufügen der neuen MCN-Site besteht der nächste Schritt darin, die virtuellen Schnittstellengruppen für die Site zu erstellen und zu konfigurieren.

Im Folgenden finden Sie einige Richtlinien für die Konfiguration virtueller Schnittstellengruppen:

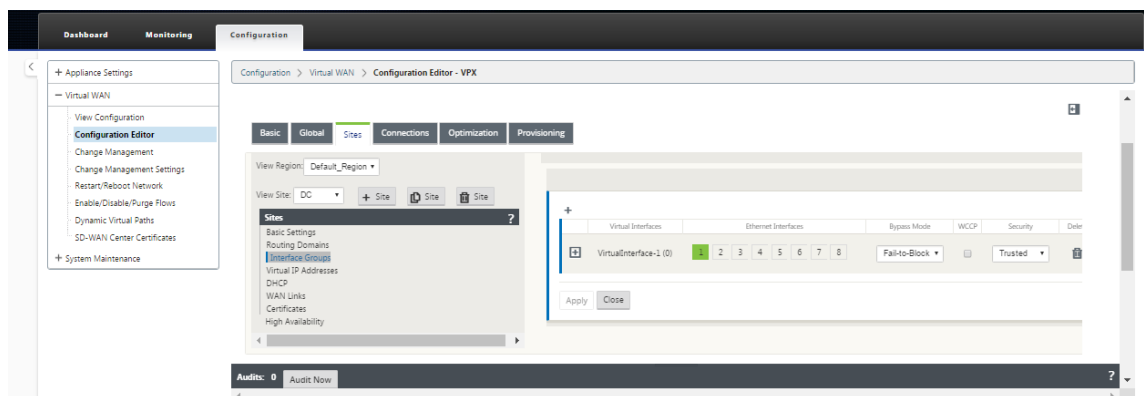
- Verwenden Sie logische Namen, die die Gruppe am besten beschreiben.
- Vertrauenswürdige Netzwerke sind Netzwerke, die hinter einer Firewall geschützt sind.
- Virtuelle Schnittstellen verknüpfen Schnittstellen mit Fail-to-Wire-Paaren (FTW).
- Einzelne WAN-Schnittstellen können sich nicht in einem FTW-Paar befinden.
- Die IPv6-Adresse wird in Version 11.1.0 eingeführt und wird nur für nicht vertrauenswürdige Schnittstellen unterstützt. Nicht vertrauenswürdige Schnittstellen sind nicht routingfähig und werden für den virtuellen Pfadverkehr verwendet.

Hinweis

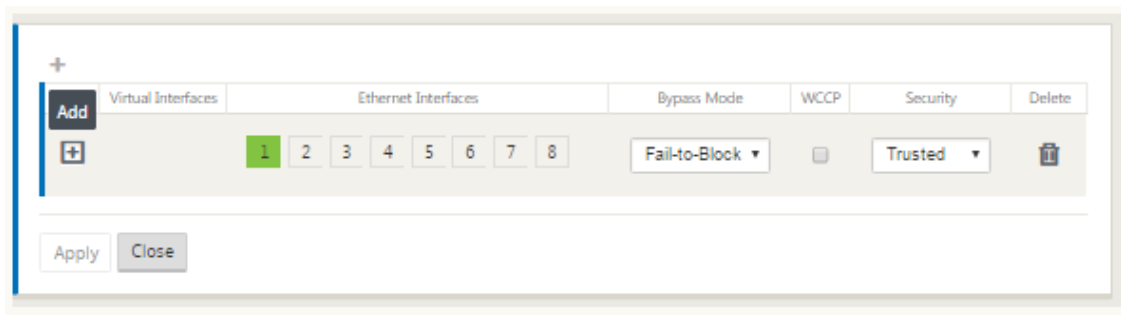
Weitere Richtlinien und Informationen zum Konfigurieren virtueller Schnittstellengruppen finden Sie im Abschnitt Virtuelles Routing und Weiterleitung.

Gehen Sie folgendermaßen vor, um der neuen MCN-Website eine virtuelle Schnittstellengruppe hinzuzufügen:

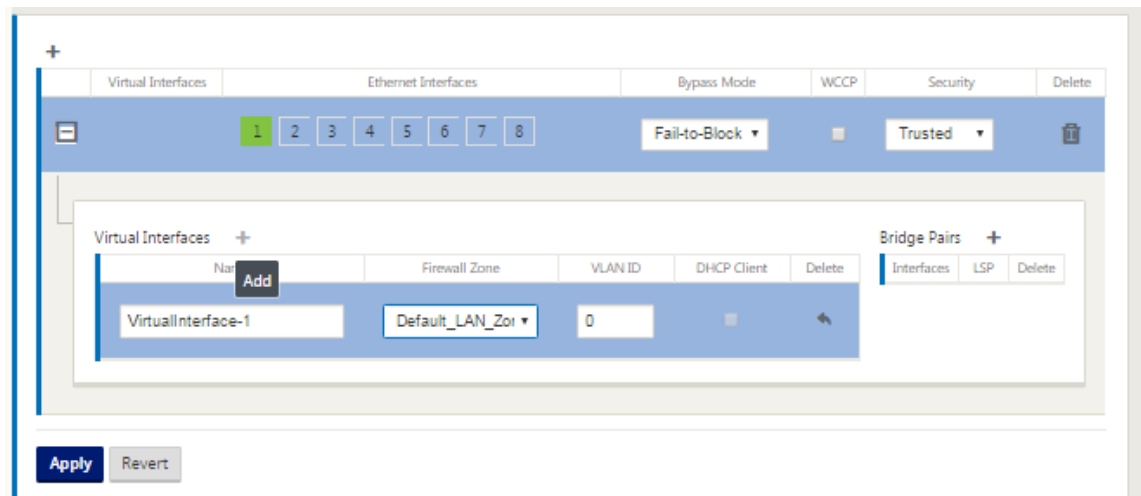
1. Wählen Sie in der **Sitesansicht** des **Konfigurationseditors** den Standort aus dem Dropdownmenü **Site anzeigen** aus. Dadurch wird die Konfigurationsansicht für den ausgewählten Standort geöffnet.



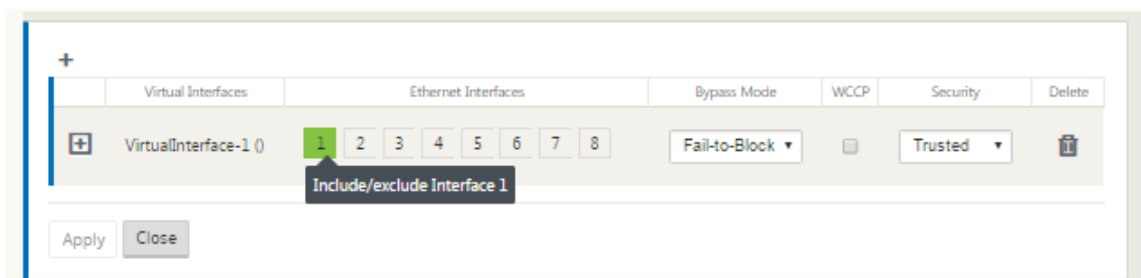
2. Klicken Sie auf **+**, um die **Gruppe der virtuellen Schnittstelle** hinzuzufügen. Dadurch wird der Tabelle ein neuer leerer Eintrag für die virtuelle Schnittstelle hinzugefügt und zur Bearbeitung geöffnet.



3. Klicken Sie rechts neben **Virtuelle Schnittstellen** auf **+**. Dadurch wird der Tabelle ein neuer leerer Gruppeneintrag hinzugefügt und zur Bearbeitung geöffnet.



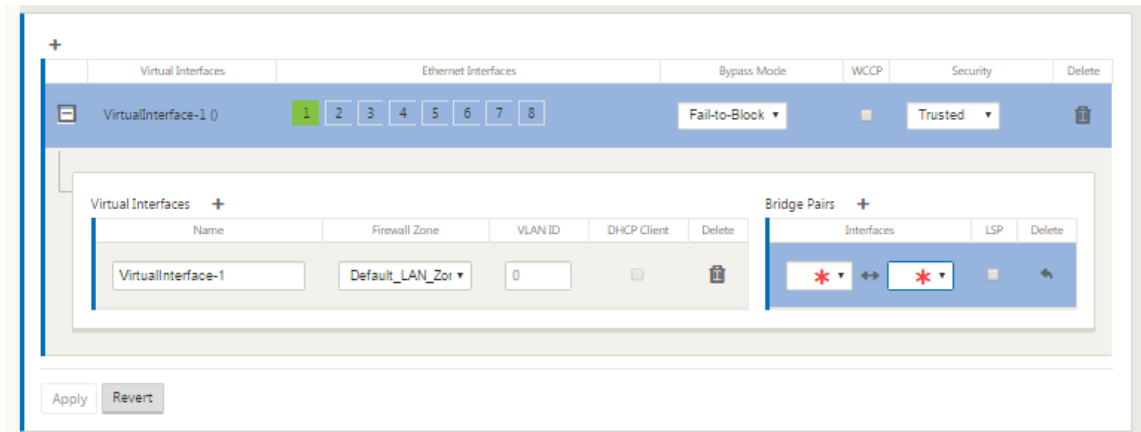
4. Wählen Sie die **Ethernet-Schnittstellen** aus, die in die Gruppe aufgenommen werden sollen. Klicken Sie unter **Ethernet-Schnittstellen** auf eine Schnittstelle, um diese Schnittstelle ein- bzw. auszuschließen. Sie können beliebig viele Schnittstellen auswählen, die in die Gruppe aufgenommen werden sollen.



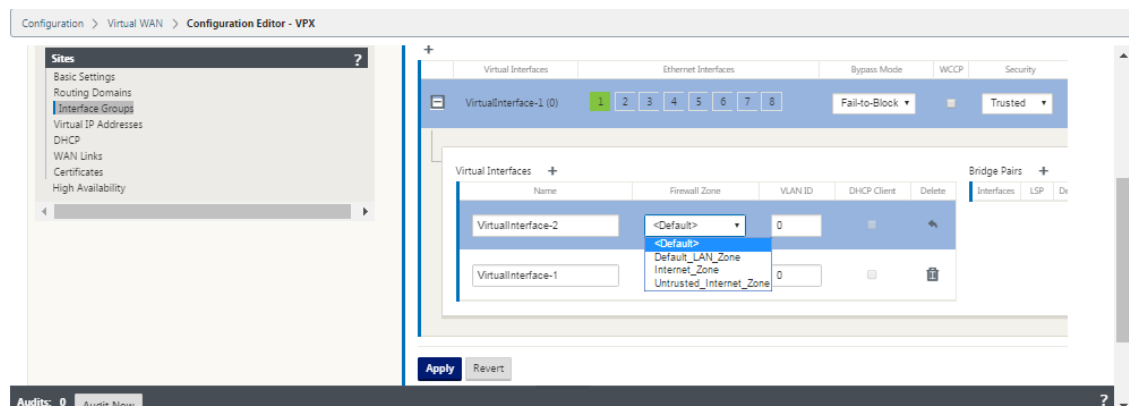
5. Wählen Sie im Dropdownmenü den **Umgehungsmodus** (keine Standardeinstellung). Der **Umgehungsmodus** gibt das Verhalten von Bridgepaarten Schnittstellen in der virtuellen Schnittstellengruppe an, wenn eine Appliance oder ein Dienstausschlag oder ein Neustart auftritt. Die Optionen sind: **Fail-to-Wire** oder **Fail-to-Block**.
6. Wählen Sie die **Sicherheitsstufe** aus dem Dropdownmenü. Dies gibt die Sicherheitsstufe für das Netzwerksegment der virtuellen Schnittstellengruppe an. Die Optionen sind: **Ver-**

vertrauenswürdig oder **Nicht vertrauenswürdig**. Vertrauenswürdige Segmente werden durch eine Firewall geschützt (Standard ist Vertrauenswürdig).

7. Klicken Sie am linken Rand der hinzugefügten virtuellen Schnittstelle auf **+**. Daraufhin wird die Tabelle **Virtuelle Schnittstellen** angezeigt.



8. Klicken Sie rechts neben **Virtuelle Schnittstellen** auf **+**. Dies zeigt den **Namen, die Firewall-Zone, die VLAN-ID, die gerichtete Broadcast, den Client-Modus** und die **automatische Konfiguration von Stateless Address (SLAAC)** an.



9. Geben Sie den **Namen** und die **VLAN-ID** für diese virtuelle Schnittstellengruppe ein.
 - **Name** —Dies ist der Name, mit dem diese virtuelle Schnittstelle referenziert wird.
 - **Firewall-Zone** - Wählen Sie eine Firewall-Zone aus dem Dropdownmenü aus.
 - **VLAN-ID** —Dies ist die ID zum Identifizieren und Markieren von Datenverkehr zu und von der virtuellen Schnittstelle. Verwenden Sie die ID 0 (Null) für native/nicht markierte Datenverkehr.
 - **Client-Modus** —Wählen Sie den Client-Modus aus dem Dropdown-Menü aus.
 - **Directed Broadcast** - Auf der virtuellen Schnittstelle können Directed Broadcasts-Pakete durch Aktivieren des Kontrollkästchens für Virtual IP-Subnetze weitergeleitet werden.

- **SLAAC** —Aktivieren des Kontrollkästchens **Stateless Address Auto-Configuration (SLAAC)** auf einer virtuellen Schnittstelle ermöglicht es ihr, automatisch eine globale IPv6-Adresse vom verbundenen Router zu erhalten. Virtuelle Schnittstellen mit aktiviertem **SLAAC** benötigen keine konfigurierte virtuelle IP-Adresse.

HINWEIS

SLAAC kann nur auf einer Zweigstelle auf einer nicht vertrauenswürdigen Schnittstelle aktiviert werden.

Sie haben die Möglichkeit, die IP-Adressen für SLAAC freizugeben oder zu erneuern.

10. Klicken Sie rechts neben **Brückenpaaren** auf **+**. Dies fügt einen neuen **Bridge Pairs** Eintrag hinzu und öffnet ihn zur Bearbeitung.
11. Wählen Sie die Ethernet-Schnittstellen, die gekoppelt werden sollen, aus den Dropdownmenüs aus. Um weitere Paare hinzuzufügen, klicken Sie erneut auf **+** neben **Bridge-Paare**.
12. Klicken Sie auf **Übernehmen**. Dies wendet Ihre Einstellungen an und fügt die neue virtuelle Schnittstellengruppe zur Tabelle hinzu. Zu diesem Zeitpunkt sehen Sie rechts neben dem neuen Eintrag für die Gruppe der virtuellen Schnittstelle ein gelbes Deltaüberwachungswarnsymbol. Dies liegt daran, dass Sie noch keine virtuellen IP-Adressen (VIPs) für die Site konfiguriert haben. Vorerst können Sie diese Warnung ignorieren, da sie automatisch aufgelöst wird, wenn Sie die virtuellen IPs für die Site richtig konfiguriert haben.
13. Um weitere virtuelle Schnittstellengruppen hinzuzufügen, klicken Sie rechts neben dem Zweig **Schnittstellengruppen** auf **+**, und fahren Sie wie oben dargestellt fort.

Konfigurieren der virtuellen IP-Adresse für den MCN

Der nächste Schritt besteht darin, die virtuellen IP-Adressen für den Standort zu konfigurieren und sie der entsprechenden Gruppe zuzuweisen.

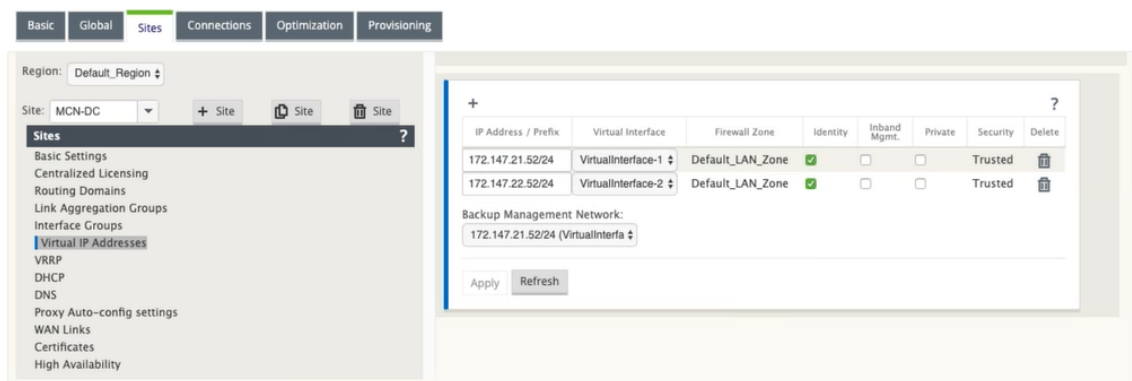
1. Klicken Sie in der Ansicht **Sites** für die neue MCN-Site auf **+** links neben den **virtuellen IP-Adressen**. Dadurch wird die Tabelle **Virtuelle IP-Adressen** für den neuen Standort angezeigt.
2. Klicken Sie rechts neben **Virtuelle IP-Adressen** auf **+**, um eine Adresse hinzuzufügen. Dadurch wird das Formular zum Hinzufügen und Konfigurieren einer neuen virtuellen IP-Adresse geöffnet.
3. Geben Sie die **IP-Adresse/Präfix-Informationen** ein, und wählen Sie die **virtuelle Schnittstelle** aus, mit der die Adresse verknüpft ist. Die virtuelle IP-Adresse muss die vollständige Hostadresse und die Netzmaske enthalten.
4. Wählen Sie die gewünschten Einstellungen für die virtuelle IP-Adresse aus, z. B. Firewall-Zone, Identität, Privat und Sicherheit.

5. Wählen Sie **Inband Mgmt**, damit die virtuelle IP-Adresse eine Verbindung zu Verwaltungsdiensten wie Web-UI und SSH herstellen kann.

Hinweis:

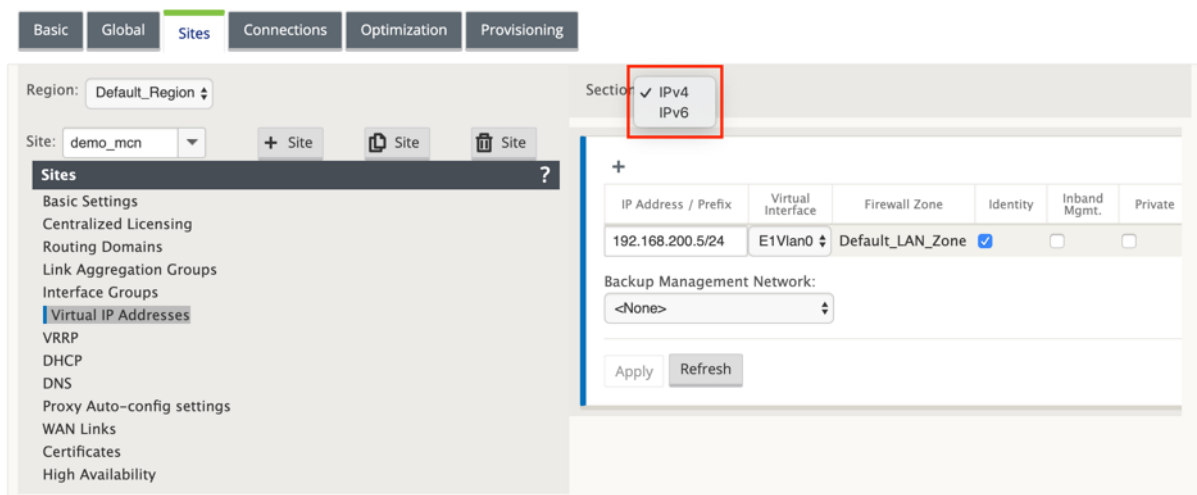
Die Schnittstelle sollte den Sicherheitstyp **Vertrauenswürdig** und **Identität** aktiviert haben.

6. Wählen Sie eine virtuelle IP als **Backup-Management-Netzwerk** aus. Auf diese Weise können Sie die virtuelle IP-Adresse für die Verwaltung verwenden, wenn der Verwaltungsport nicht mit einem Standard-Gateway konfiguriert ist.



7. Klicken Sie auf **Übernehmen**. Dadurch werden die Adressinformationen zur Site hinzugefügt und in die Tabelle **Virtuelle IP-Adressen** des Standortes aufgenommen.
8. Um weitere virtuelle IP-Adressen hinzuzufügen, klicken Sie rechts neben den **Virtuellen IP-Adressen** auf **+**, und fahren Sie wie oben beschrieben fort.

Ab Version 11.1.0 stehen unter der **virtuellen IP-Adresse** zwei Unterabschnitte zur Verfügung: **IPv4-Adressen** und **IPv6-Adressen**.



Einschränkungen

- Es wird nur ein Pfadpaar erstellt, wenn sowohl IPv4- als auch IPv6-Access Interfaces für dieselbe WAN-Verbindung konfiguriert sind.
- Wenn der IPv6-Pfad ausfällt, findet kein Fallback auf IPv4 für dieselbe WAN-Verbindung statt.
- Tracking von IPv6-Adressen wird für Version 11.1.0 nicht unterstützt.
- IPv6 wird nur für die Kommunikation zwischen SD-WAN-Geräten über Virtual Path unterstützt. Internet- und Intranetdienste werden nicht unterstützt. Keine Unterstützung für Verwaltungsebene in Version 11.1.0.
- IPv6 wird für LTE-Links auf 210 Geräten für 11.1.0 Version nicht unterstützt.
- DHCPv6-Client und -Server werden für IPv6 nicht unterstützt. Sie können SLAAC für die automatische Adressierung konfigurieren.

Sie müssen eine virtuelle IP-Adresse für die neu erstellte nicht vertrauenswürdige Schnittstelle hinzufügen, oder Sie können SLAAC aktivieren, wenn es sich um einen Zweigstandort handelt. So fügen Sie virtuelle IP-Adresse hinzu:

1. Wählen Sie im Dropdownmenü Abschnitt die Option IPv6 aus.
2. Definieren Sie die folgenden Felder:
3. IP-Adresse/Präfix —Geben Sie die vollständige Host-Adresse und Netzmaske an.
4. Virtuelle Schnittstelle —Wählen Sie eine der zugeordneten virtuellen Schnittstellen aus dem Dropdownmenü aus.
5. Firewallzone —Die Firewallzone für die virtuelle Schnittstelle.
6. Lokal verknüpfen (Optional): Wenn das Kontrollkästchen Lokal verknüpfen aktiviert ist, kann diese virtuelle IPv6-IP-Adresse als lokale Linkadresse für die virtuelle Schnittstelle verwendet werden.

HINWEIS

Wenn das Kontrollkästchen Lokal verknüpfen nicht aktiviert ist, generiert die Appliance automatisch eine lokale Linkadresse und weist sie zu.

Section: IPv6

| IP Address / Prefix | Virtual Interface | Firewall Zone | Link Local | Private | Security | Delete |
|---------------------|-------------------|-------------------------|--------------------------|-------------------------------------|-----------|--------|
| 2607:f0d0:2001:0... | E2Vlan0 | Untrusted_Internet_Zone | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Untrusted | |

Apply Refresh

HINWEIS:

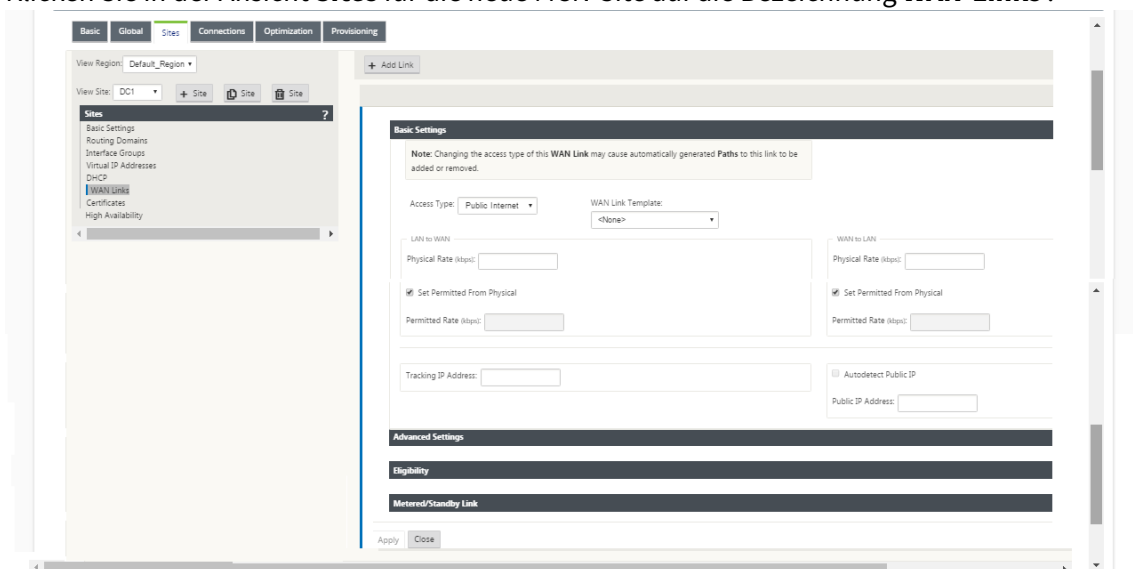
Neighbor Discovery Protocol (NDP) wird von IPv6 unterstützt.

Wenn sowohl IPv4- als auch IPv6-Access Interfaces für die lokale und die Remotesite definiert sind, wird der Pfad nur mit IPv6-Adresse geformt.

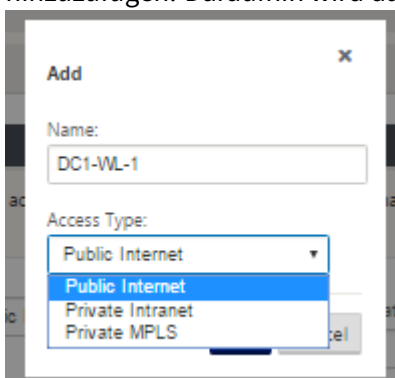
So konfigurieren Sie WAN-Links für den MCN

Der nächste Schritt besteht darin, die WAN-Links für die Site zu konfigurieren.

1. Klicken Sie in der Ansicht **Sites** für die neue MCN-Site auf die Bezeichnung **WAN-Links**.

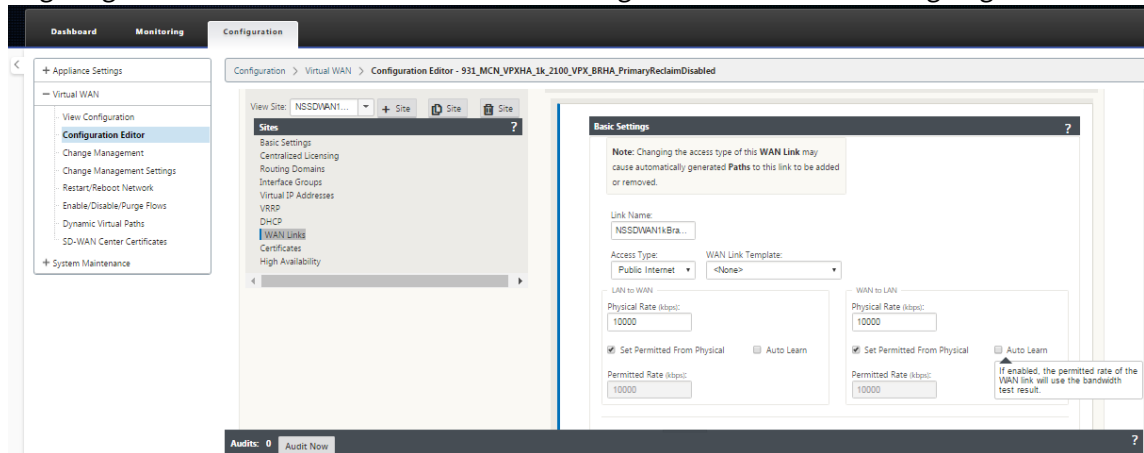


2. Klicken Sie rechts neben den **WAN-Links** auf **Link hinzufügen**, um eine neue WAN-Verbindung hinzuzufügen. Daraufhin wird das Dialogfeld **Hinzufügen** geöffnet.



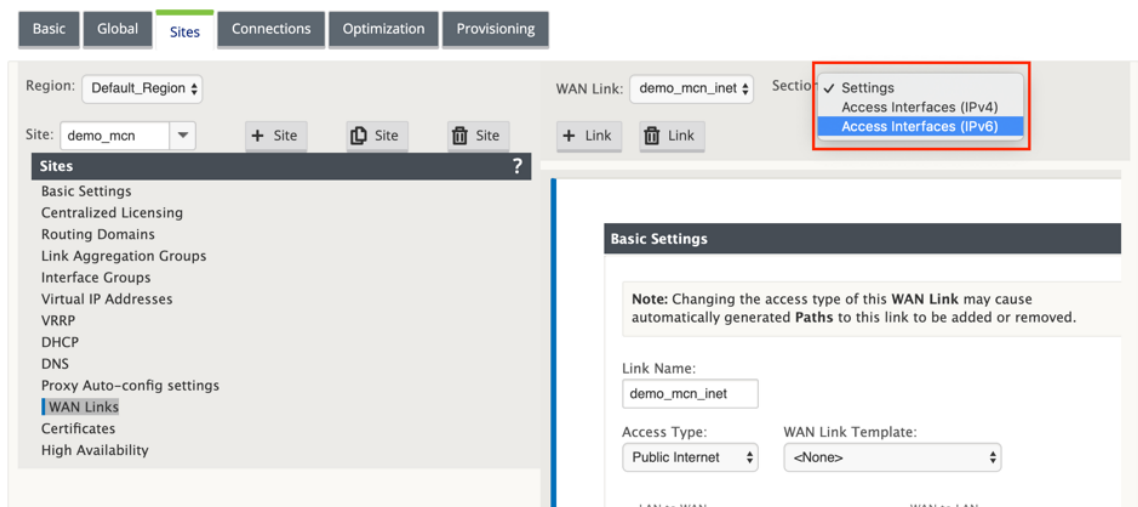
3. (Optional) Geben Sie einen Namen für die WAN-Verbindung ein, wenn Sie die Standardeinstellung nicht verwenden möchten. Der Standardwert ist der Site-Name, der mit dem folgenden Suffix angehängt <number> <number> wird: WL-, wobei die Anzahl der WAN-Links für diese Site ist, erhöht um eins.

- Wählen Sie im Dropdownmenü den **Zugriffstyp** aus. Die Optionen sind **öffentliches Internet**, **privates Intranet** oder **Privates MPLS**.
- Klicken Sie auf **Hinzufügen**. Dadurch wird die Konfigurationsseite **WAN-Links** Basic Settings angezeigt und der Seite wird der neuen nicht konfigurierten WAN-Link hinzugefügt.



Nur-IPv6-Pfad zwischen zwei Sites wird erstellt, wenn sowohl IPv4- als auch IPv6-Access Interfaces für dieselbe WAN-Verbindung konfiguriert sind.

- Wählen Sie im Dropdown-Menü **Einstellung** die Option **Access Interfaces (IPv6)** aus.



- Definieren Sie die folgenden Felder:

- Name** —Geben Sie den Namen des Access Interface an.
- Virtuelle Schnittstelle** —Sobald eine Routingdomäne ausgewählt wurde, wählen Sie eine der zugehörigen virtuellen Schnittstellen aus dem Dropdown-Menü aus.
- IP-Adresse** —Geben Sie eine statische IP-Adresse für den Endpunkt der Zugriffsschnittstelle auf dem SD-WAN an.
- Gateway-IP-Adresse** —Geben Sie die IP-Adresse des Gateway-Routers an.

HINWEIS:

Sie können die IP-Adresse und die Gateway-IP-Adresse nicht konfigurieren, wenn das virtuelle Gerät für die Verwendung des SLAAC-Modus konfiguriert ist.

- **Virtueller Pfadmodus** - Wählen Sie den virtuellen Pfadmodus aus dem Dropdown-Menü aus, um die Priorität für den virtuellen Pfadverkehr auf diesem WAN-Link zu bestimmen.
- **Gateway-MAC-Adressbindung** — Wenn das Kontrollkästchen **Gateway-MAC-Adressbindung** aktiviert ist, muss die Quell-MAC-Adresse der im Internet oder Intranetdienste empfangenen Pakete mit der GATEWAY-MAC-Adresse übereinstimmen.

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Gateway MAC Address Binding | Delete |
|------------------|-------------------|-------------------------------|-------------------------------|-------------------|-------------------------------------|--------|
| demo_mcn_inet... | E2Vlan0 | 2607:fd0:2001:000a:0000:00... | 2607:fd0:2001:000a:0000:00... | Primary | <input checked="" type="checkbox"/> | |

Sobald die IPv6-Schnittstelle für die WAN-Verbindung erstellt wurde, können Sie diese Schnittstelle verwenden, um mit dem Internet Service Provider (ISP) zu kommunizieren.

HINWEIS:

Da das anfängliche IPv6-Angebot nur Virtual Path-Konnektivität ist, können wir keine LAN-seitigen IPv6-Pakete senden.

Automatisches Lernen von Bandbreitenverbrauch

Auto Learn wird beim Systemstart ausgeführt und wiederholt sich alle fünf Minuten, bis ein erfolgreiches Ergebnis beobachtet wird. Auto learn wird auch ausgeführt, nachdem Änderungen der WAN-Verbindungskonfiguration im Konfigurations-Editor vorgenommen wurden.

Sie können Tests manuell ausführen oder Tests in der SD-WAN-GUI planen. Die Ergebnisse dieser Tests sollten auch für die zulässige Rate gelten, wenn der Test erfolgreich ist und das automatische Lernen aktiviert ist.

Wenn Sie Auto Learn in großen Netzwerken verwenden, werden bei Neustart der Konfigurationsänderung alle Standorte gleichzeitig Tests auf dem MCN ausgeführt, was zu einer hohen Bandbreitenauslastung führt, die zu ungenauen Ergebnissen führt. Es wird empfohlen, Bandbreitentests ein- oder zweimal täglich zu planen, normalerweise wenn das Verkehrsaufkommen niedrig ist.

Hinweis

Automatische Erkennung der WAN Link-Bandbreite, gilt nur für Zweige und nicht für MCN/RCN.

The screenshot shows the 'Diagnostics' section of the Citrix SD-WAN interface. It includes tabs for Ping, Traceroute, Packet Capture, Path Bandwidth, System Info, Diagnostic Data, Events, Alarms, and Diagnostics Tool. The 'Path Bandwidth' tab is active, displaying 'Instant Path Bandwidth Testing' and 'Schedule Path Bandwidth Testing' sections. The 'Instant Path Bandwidth Testing' section has a 'Path' dropdown set to 'DC_VPX-Inet->BR_21' and a 'Test' button. The 'Schedule Path Bandwidth Testing' section has an 'Add' button and a table with columns for Path Name, Frequency, Day of Week, Hour, and Minute. Below these is the 'History Path Bandwidth Testing Result' section, which shows a table with columns for Num, From Link, To Link, Test Time, Min Bandwidth (kbps), Max Bandwidth (kbps), and Avg Bandwidth (kbps). The table currently shows 'No data available in table'.

1. Geben Sie die Linkdetails für den neuen WAN-Link ein. Konfigurieren Sie die LAN-zu-WAN-, **WAN-zu-LAN-Einstellungen**. Einige Richtlinien lauten wie folgt:
 - Einige Internetlinks könnten asymmetrisch sein.
 - Eine falsche Konfiguration der zulässigen Geschwindigkeit kann sich negativ auf die Leistung für diesen Link auswirken
 - Vermeiden Sie die Verwendung von Burstgeschwindigkeiten, die die festgeschriebene Rate übertreffen.
 - Achten Sie bei Internet-WAN-Verbindungen darauf, die öffentliche IP-Adresse hinzuzufügen.
2. Klicken Sie auf die graue Bereichsleiste **Erweiterte Einstellungen**. Dadurch wird das Formular **Erweiterte Einstellungen** für den Link geöffnet.

The screenshot shows the 'WAN Link' configuration page. It includes a 'View Region' dropdown set to 'Default_Region' and a 'View Site' dropdown set to 'MCN-DC'. There are buttons for '+ Site', 'Site', and 'Delete Site'. The 'WAN Link' dropdown is set to 'MCN-DC-WL-1' and the 'Section' dropdown is set to 'Settings'. There are buttons for '+ Add Link' and 'Delete Link'. The 'Basic Settings' tab is active, showing fields for 'Provider ID', 'Frame Cost (bytes)', 'Congestion Threshold (μs)', and 'MTU Size (bytes)'. The 'Advanced Settings' tab is also visible, showing fields for 'Eligibility' and 'Metered/Standby Link'. There are 'Apply' and 'Revert' buttons at the bottom.

3. Geben Sie die **erweiterten Einstellungen** für den Link ein:
 - **Provider-ID** —(Optional) Geben Sie eine eindeutige ID-Nummer 1—100 ein, um WAN-Links festzulegen, die mit demselben Dienstanbieter verbunden sind. Virtual WAN

verwendet die Provider-ID, um Pfade beim Senden doppelter Pakete zu unterscheiden.

- **Frame Cost (Bytes)** —Geben Sie die Größe (in Bytes) des Headers/Trailers ein, der zu jedem Paket hinzugefügt wurde. Zum Beispiel die Größe der hinzugefügten Ethernet-IPG- oder AAL5-Anhänger in Bytes.
- **Stauschwellenwert** —Geben Sie den Stauschwellenwert (in Mikrosekunden) ein, nach dem die WAN-Verbindung die Paketübertragung drosselt, um weitere Staus zu vermeiden.
- **MTU-Größe (Byte)** —Geben Sie die größte Rohpaketgröße (in Byte) ein, ohne die Frame-Kosten.

4. Klicken Sie auf die graue **Auswahlleiste**. Dadurch wird das Formular **Berechtigungseinstellungen** für den Link geöffnet.
5. Wählen Sie die **Berechtigungseinstellungen** für den Link aus.

View Region: Default_Region

View Site: MCN-DC

Sites

- Basic Settings
- Routing Domains
- Interface Groups
- Virtual IP Addresses
- VRRP
- DHCP
- WAN Links**
- Certificates
- High Availability

WAN Link: MCN-DC-WL-1

Section: Settings

+ Add Link Delete Link

Basic Settings

Advanced Settings

Eligibility

| | LAN to WAN | WAN to LAN |
|-------------|-------------------------------------|-------------------------------------|
| Realtime | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Interactive | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Bulk | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Metered/Standby Link

Apply Revert

6. Klicken Sie auf die graue Abschnittleiste mit **Metered Link**. Dadurch wird das Formular **Metered Link-Einstellungen** für den Link geöffnet.
7. (Optional) Wählen Sie **Metering** aktivieren, um die Messung für diesen Link zu aktivieren. Daraufhin werden die Felder **Metering-Einstellungen aktivieren** angezeigt.

View Site: MCN-DC

Sites

- Basic Settings
- Routing Domains
- Interface Groups
- Virtual IP Addresses
- VRRP
- DHCP
- WAN Links**
- Certificates
- High Availability

Basic Settings

Advanced Settings

Eligibility

Metered/Standby Link

Metering

☐ Enable Metering

Standby

Standby Mode:

Disabled

Disabled

Last-Resort

On-Demand

Apply Revert

The screenshot displays three configuration sections in a light gray box:

- Metering:** Contains two checked checkboxes: "Enable Metering" and "Disable if Data Cap reached". Below these are three fields: "Data Cap (MB):" with a value of "0", "Billing Cycle:" with a dropdown menu set to "Monthly", and "Starting From:" with a text box containing "MM/DD/YYYY".
- Standby:** Contains a "Standby Mode:" dropdown menu set to "Disabled".
- Heartbeat Interval:** Features a yellow warning box stating "Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure." Below this is an "Active Heartbeat Interval:" dropdown menu set to "DEFAULT".

8. Konfigurieren Sie die Messeinstellungen für den Link. Geben Sie Folgendes ein:

- **Data Cap (MB)** —Geben Sie die Daten-Cap-Zuweisung für den Link in Megabyte ein.
- **Abrechnungszeitraum** —Wählen Sie entweder **Monatlich** oder **Wöchentlich** aus dem Dropdownmenü.
- Beginnend **von** —Geben Sie das Startdatum des Abrechnungszyklus ein.
- **Letztes Resort** festlegen —Wählen Sie diese Option, um diesen Link als Link der letzten Instanz zu aktivieren, wenn alle anderen verfügbaren Links ausfallen. Unter normalen WAN-Bedingungen sendet Virtual WAN nur minimalen Datenverkehr über getaktete Links, um den Linkstatus zu überprüfen. Im Falle eines Ausfalls kann SD-WAN jedoch aktive gemessene Links als letzter Ausweg für die Weiterleitung des Produktionsverkehrs verwenden.

Klicken Sie auf **Übernehmen**. Dadurch werden die angegebenen Einstellungen auf die neue WAN-Verbindung angewendet.

Der nächste Schritt besteht darin, die Access Interfaces für die neue WAN-Verbindung zu konfigurieren. Eine Zugriffsoberfläche besteht aus einer virtuellen Schnittstelle, einer WAN-Endpunkt-IP-Adresse, einer Gateway-IP-Adresse und einem virtuellen Pfadmodus, die gemeinsam als Schnittstelle für eine bestimmte WAN-Verbindung definiert sind. Jede WAN-Verbindung muss über mindestens eine Zugriffsoberfläche verfügen.

So konfigurieren Sie die Zugriffsoberfläche:

1. Wählen Sie auf der Seite WAN-Link-Konfiguration für den Link **Zugriffsschnittstellen** aus. Dadurch wird die Ansicht **Access Interfaces** für die Site geöffnet.

The screenshot shows the top of the WAN Link configuration page. It includes a "WAN Link:" dropdown set to "DC1-WL-1", a "Section:" dropdown menu with "Access Interfaces" selected (highlighted in blue), and two buttons: "+ Add Link" and "Delete Link".

2. Klicken Sie auf **+**, um eine Schnittstelle hinzuzufügen. Dadurch wird der Tabelle ein leerer Eintrag hinzugefügt und zur Bearbeitung geöffnet. Geben Sie die Einstellungen für **Access Interfaces** für den Link ein. Jede WAN-Verbindung muss mindestens ein Access Interface haben.

3. Geben Sie Folgendes ein:

- **Name** —Dies ist der Name, mit dem diese Access Interface referenziert wird. Geben Sie einen Namen für die neue Access-Schnittstelle ein, oder übernehmen Sie die Standardeinstellung. Der Standardwert verwendet die folgende Benennungskonvention:
wan_link_name-ai-number: Wobei *wan_link_name* der Name der WAN-Verbindung ist, die Sie dieser Schnittstelle zuordnen, und *number* ist die Anzahl der derzeit für diesen Link konfigurierten Access Interfaces, erhöht um 1.

Hinweis

Wenn der Name abgeschnitten angezeigt wird, können Sie den Cursor in das Feld setzen, dann klicken und halten und rollen Sie die Maus nach rechts oder links, um den abgeschnittenen Teil zu sehen.

- **Virtuelle Schnittstelle** —Dies ist die virtuelle Schnittstelle, die diese Access Interface verwendet. Wählen Sie einen Eintrag aus dem Dropdownmenü der Virtuellen Schnittstellen aus, die für diesen Zweigstandort konfiguriert sind.
- **Routingdomäne** - Die Routingdomäne, die Sie für die Zugriffsoberfläche auswählen möchten.
- **IP-Adresse** —Dies ist die IP-Adresse für den Access Interface Endpunkt von der Appliance zum WAN.
- **Gateway IP-Adresse** — Dies ist die IP-Adresse für den Gateway-Router.

- **Virtueller Pfadmodus** —Gibt die Priorität für den virtuellen Pfadverkehr auf dieser WAN-Verbindung an. Die Optionen sind: **Primär**, **Sekundär** oder **Ausschließen**. Wenn diese Zugriffsoberfläche auf **Ausschließen** festgelegt ist, wird diese Zugriffsoberfläche nur für den Internet- und Intranetverkehr verwendet.
- **Proxy ARP** —Aktivieren Sie das zu aktivierte Kontrollkästchen. Wenn diese Option aktiviert ist, antwortet die Virtual WAN Appliance auf ARP-Anforderungen für die Gateway-IP-Adresse, wenn das Gateway nicht erreichbar ist.

1. Klicken Sie auf **Übernehmen**.

Sie haben nun die Konfiguration der neuen WAN-Verbindung abgeschlossen. Wiederholen Sie diese Schritte, um weitere WAN-Links für die Site hinzuzufügen und zu konfigurieren.

Der nächste Schritt besteht darin, die Routen für die Site hinzuzufügen und zu konfigurieren.

So konfigurieren Sie Routen für den MCN

Gehen Sie folgendermaßen vor, um die Routen für die Site hinzuzufügen und zu konfigurieren:

1. Klicken Sie auf die Ansicht **Verbindungen** für die neue MCN-Website und wählen Sie **Routen** aus. Dadurch wird die **Routenansicht** für die Site angezeigt.
2. Klicken Sie rechts neben **Routen** auf **+**, um eine Route hinzuzufügen. Daraufhin wird das Dialogfeld **Routen** zur Bearbeitung geöffnet.

The screenshot shows a dialog box titled "Add" with the following fields and options:

- Network IP Address**: A text input field with a red asterisk indicating it is required.
- Cost**: A text input field containing the value "5".
- Service Type**: A dropdown menu currently set to "Local".
- Gateway IP Address**: A text input field with a red asterisk indicating it is required.
- Export Route**: A checked checkbox.
- Summary Route**: An unchecked checkbox.
- Eligibility Based On Path**: An unchecked checkbox.
- Path:**: A dropdown menu currently set to "<None>".
- Eligibility Based On Gateway**: An unchecked checkbox.
- Buttons**: "Add" and "Cancel" buttons at the bottom right.

3. Geben Sie die Routenkonfigurationsinformationen für die neue Route ein. Geben Sie Folgendes ein:

- **Netzwerk-IP-Adresse** —Geben Sie die **Netzwerk-IP-Adresse** ein.

- **Kosten** —Geben Sie eine Gewichtung zwischen 1 und 15 ein, um die Routenpriorität für diese Route zu bestimmen. Lower-Cost-Routen haben Vorrang vor höheren Kosten Routen. Der Standardwert ist 5.
- **Servicetyp** —Wählen Sie den Servicetyp für die Route aus dem Dropdownmenü für dieses Feld aus.
 - **Virtueller Pfad** —Dieser Dienst verwaltet den Datenverkehr über die virtuellen Pfade. Ein virtueller Pfad ist eine logische Verbindung zwischen zwei WAN-Verbindungen. Es umfasst eine Sammlung von WAN-Pfaden, die kombiniert werden, um eine hohe Service-Level-Kommunikation zwischen zwei SD-WAN-Knoten zu ermöglichen. Dies wird durch ständige Messung und Anpassung an veränderte Anwendungsanforderungen und WAN-Bedingungen erreicht. SD-WAN-Appliances messen das Netzwerk pro Pfad. Ein virtueller Pfad kann statisch (immer vorhanden) oder dynamisch sein (nur vorhanden, wenn der Datenverkehr zwischen zwei SD-WAN-Appliances einen konfigurierten Schwellenwert erreicht).
 - **Internet** —Dieser Dienst verwaltet den Datenverkehr zwischen einem Enterprise-Standort und Websites im öffentlichen Internet. Datenverkehr dieses Typs ist nicht gekapselt. In Zeiten der Überlastung verwaltet das SD-WAN aktiv die Bandbreite, indem es den Internetverkehr relativ zum virtuellen Pfad einschränkt, und den Intranetverkehr entsprechend der vom Administrator festgelegten SD-WAN-Konfiguration begrenzt.
 - **Intranet** —Dieser Dienst verwaltet Enterprise-Intranet-Datenverkehr, der nicht für die Übertragung über einen virtuellen Pfad definiert wurde. Wie beim Internetverkehr bleibt er ungekapselt, und das SD-WAN verwaltet die Bandbreite, indem dieser Datenverkehr im Verhältnis zu anderen Diensttypen während der Staus begrenzt wird. Unter bestimmten Bedingungen und wenn für Intranet-Fallback auf dem virtuellen Pfad konfiguriert ist, kann Datenverkehr, der normalerweise über einen virtuellen Pfad verläuft, stattdessen als Intranetdatenverkehr behandelt werden, um die Netzwerkzuverlässigkeit aufrechtzuerhalten.
 - **Passthrough** —Dieser Dienst verwaltet den Datenverkehr, der über das virtuelle WAN übergeben werden soll. Der an den Passthrough-Dienst gerichtete Datenverkehr umfasst Broadcasts, ARPs und anderen Nicht-IPv4-Datenverkehr sowie Datenverkehr im lokalen Subnetz der Virtual WAN Appliance, konfigurierten Subnetzen oder vom Netzwerkadministrator angewendete Regeln. Dieser Datenverkehr wird vom SD-WAN nicht verzögert, geformt oder geändert. Daher müssen Sie sicherstellen, dass Passthrough-Datenverkehr keine erheblichen Ressourcen auf den WAN-Verbindungen verbraucht, die die SD-WAN-Appliance für andere Dienste konfiguriert ist.
 - **Lokal** —Dieser Dienst verwaltet den lokalen IP-Datenverkehr auf der Website, der keinem anderen Dienst entspricht. SD-WAN ignoriert Datenverkehr, der für eine lokale Route bestimmt ist.
 - **GRE-Tunnel** —Dieser Dienst verwaltet den IP-Datenverkehr, der für einen GRE-Tunnel bes-

timmt ist, und stimmt mit dem am Standort konfigurierten LAN-GRE-Tunnel überein. Mit der Funktion GRE Tunnel können Sie SD-WAN Appliances so konfigurieren, dass GRE Tunnel im LAN beendet werden. Bei einer Route mit Servicetyp GRE Tunnel muss sich das Gateway in einem der Tunnelsubnetze des lokalen GRE Tunnels befinden.

- **LAN IPsec-Tunnel** —Dieser Dienst verwaltet den IP-Datenverkehr, der für den IPsec-Tunnel bestimmt ist.
- **Inter-Routing** - Dieser Service ermöglicht das Leck von Routen zwischen Routingdomänen innerhalb einer Site oder zwischen verschiedenen Standorten. Dadurch entfällt die Notwendigkeit, dass ein Edgerouter Routeleaking verarbeitet.
- **Gateway-IP-Adresse** —Geben Sie die **Gateway-IP-Adresse** für diese Route ein.
- **Berechtigung** - Basierend auf Pfad (Kontrollkästchen) —(Optional) —(Optional) Wenn diese Option aktiviert ist, erhält die Route keinen Traffic, wenn der ausgewählte Pfad ausgefallen ist.
- **Pfad** —Dies gibt den Pfad an, der zum Bestimmen der Routenberechtigung verwendet werden soll.

Je nach Servicetyp werden folgende Einstellungen angezeigt:

| Servicetyp | Einstellungen für Diensttyp |
|-----------------|---|
| Virtueller Pfad | Next Hop Site —Dies gibt die Remote-Site an, an die Virtual Path Pakete weitergeleitet werden. |
| Internet | Route exportieren: Aktivieren/Deaktivieren, um Routen zu anderen verbundenen Standorten zu exportieren, Berechtigung basierend auf Pfad |
| Intranet | Exportroute, Intranet-Service, Berechtigung basierend auf Pfad, Berechtigung basierend auf Tunnel |
| Passthrough | Berechtigung basierend auf dem Pfad |
| Lokal | Route exportieren, Übersichtsrouten, Berechtigung basierend auf Pfad |
| GRE Tunnel | Route exportieren, Berechtigung basierend auf Pfad, Berechtigung basierend auf Gateway |
| IPsec-Tunnel | Route exportieren, Berechtigung basierend auf Pfad, IPsec-Tunnel, Berechtigung basierend auf Tunnel |
| Verwerfen | Route exportieren, Übersichtsrouten |
| Inter-Routing | Inter-Routingdomänendienst |

1. Klicken Sie auf **Übernehmen**.

Hinweis

Nachdem Sie auf **Übernehmen** geklickt haben, werden möglicherweise Überwachungswarnungen angezeigt, die darauf hinweisen, dass weitere Maßnahmen erforderlich sind. Ein Rotpunkt- oder Goldrute-Delta-Symbol weist auf einen Fehler in dem Abschnitt hin, in dem es angezeigt wird. Sie können diese Warnungen verwenden, um Fehler oder fehlende Konfigurationsinformationen zu identifizieren. Bewegen Sie den Mauszeiger über ein Überwachungswarnsymbol, um eine kurze Beschreibung der Fehler in diesem Abschnitt anzuzeigen. Sie können auch auf die dunkelgraue Statusleiste für **Audits** (unten auf der Seite) klicken, um eine vollständige Liste aller Überwachungswarnungen anzuzeigen.

+

Search:

| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|-------|--------------|--------------|--------------------|------|------|--------|
| 1 | 0.0.0.0/0 | 5 | Virtual Path | Branch1 | | | | |
| 2 | 172.147.21.52/24 | 5 | Local | | | | | |
| 3 | 172.147.22.52/24 | 5 | Local | | | | | |
| 4 | 0.0.0.0/0 | 65535 | Passthrough | | | | | |

⏪

⏩

1

⏪

⏩

Apply

Close

Sie können konfigurierte Routen auch wie folgt bearbeiten.

Edit

?

×

Network IP Address

Cost

Service Type

Gateway IP Address

0.0.0.0/0

5

Virtual Path

Next Hop Site:

Branch1

☒ Eligibility Based On Path

Path:

Branch1-WL-1->MCN-DC-WL-1

Apply

Cancel

Um weitere Routen für die Site hinzuzufügen, klicken Sie rechts neben dem Zweig **Routen** auf **+**, und

fahren Sie wie oben beschrieben fort.

Sie haben nun die Eingabe der primären Konfigurationsinformationen für den neuen MCN-Standort abgeschlossen. Die folgenden zwei Abschnitte enthalten Anweisungen für weitere optionale Schritte:

- [Konfigurieren von Hochverfügbarkeit \(HA\) für den MCN-Standort \(optional\).](#)
- [Aktivieren und Konfigurieren von Virtual WAN-Sicherheit und Verschlüsselung \(optional\).](#)

Wenn Sie diese Funktionen jetzt nicht konfigurieren möchten, können Sie direkt zum Abschnitt [Benennen, Speichern und Sichern der MCN-Standortkonfiguration.](#)

Aktivieren und Konfigurieren von Virtual WAN-Sicherheit und Verschlüsselung (optional)

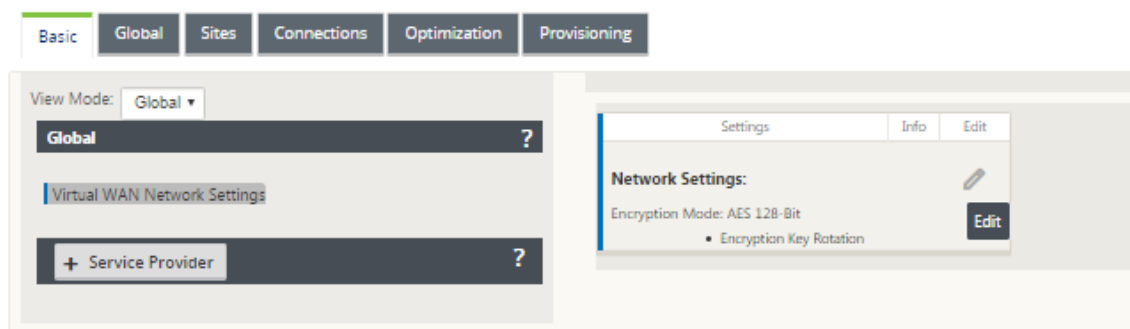
May 10, 2021

Gehen Sie folgendermaßen vor, um Virtual WAN-Sicherheit und Verschlüsselung zu aktivieren und zu konfigurieren:

Hinweis

Die Aktivierung der Virtual WAN-Sicherheit und Verschlüsselung ist optional.

1. Navigieren Sie im **Konfigurations-Editor** zur Registerkarte **Basic**, wählen Sie **Global** aus **Ansichtsmodus** aus. Das Konfigurationsformular für virtuelle Netzwerkeinstellungen wird angezeigt.



2. Klicken Sie auf **Bearbeiten** (Bleistiftsymbol), um die Bearbeitung für das Formular zu aktivieren.

Edit ✕

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode:
 AES 128-Bit ▼

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type:
 32-Bit Checksum ▼

Apply Cancel

3. Geben Sie Ihre globalen Sicherheitseinstellungen ein. Die folgenden Optionen stehen zur Auswahl:

- **Netzwerkverschlüsselungsmodus** —Dies ist der Verschlüsselungsalgorithmus, der für verschlüsselte Pfade verwendet wird. Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü: **AES 128 Bits** oder **AES 256 Bits**.
- **Encryption Key Rotation aktivieren:** Wenn diese Option aktiviert ist, werden die Verschlüsselungsschlüssel in Intervallen von 10 bis 15 Minuten gedreht.
- **Extended Packet Encryption Header aktivieren:** Wenn diese Option aktiviert ist, wird ein verschlüsselter Leistungsindikator mit 16 Bytes dem verschlüsselten Datenverkehr vorangestellt, der als Initialisierungsvektor dient und die Paketverschlüsselung randomisiert.
- **Extended Packet Authentication Trailer aktivieren:** Wenn diese Option aktiviert ist, wird ein Authentifizierungscode an den Inhalt des verschlüsselten Datenverkehrs angehängt, um zu überprüfen, ob die Nachricht unverändert übermittelt wird.
- **Trailertyp für erweiterte Paketauthentifizierung:** Dies ist der Typ des Trailers, der zum Validieren von Paketinhalten verwendet wird. Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü: **32-Bit-Prüfsumme** oder **SHA-256**.

4. Klicken Sie auf **Übernehmen**, um die Einstellungen auf die Konfiguration anzuwenden.

Damit ist die Konfiguration der MCN-Site abgeschlossen. Der nächste Schritt besteht darin, die neue MCN-Standortkonfiguration zu benennen und zu speichern (optional, aber empfohlen), wie im folgenden Abschnitt beschrieben.

Warnung

Wenn Ihre Konsolensitzung ein Timeout vornimmt oder Sie sich vor dem Speichern der Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten Konfigurationsänderungen verloren. Sie müssen sich dann wieder beim System anmelden und den Konfigurationsvorgang von Anfang an wiederholen. Aus diesem Grund wird empfohlen, das Konfigurationspaket häufig oder an Schlüsselpunkten in der Konfiguration zu speichern.

Konfigurieren des sekundären MCN

October 28, 2021

Sie können einen Standort als sekundären MCN konfigurieren, um MCN-Redundanz zu unterstützen. Der sekundäre MCN überwacht kontinuierlich den Zustand des primären MCN. Wenn der primäre MCN ausfällt, übernimmt der sekundäre MCN die Rolle des MCN. Um einen sekundären MCN zu erstellen, während Sie einen neuen Standort in der Option **Modus** hinzufügen, wählen Sie sekundäres MCN aus. Sie können die virtuelle Schnittstelle, die virtuelle IP, die WAN-Verbindung und andere Einstellungen manuell konfigurieren. In ähnlicher Weise können Sie auch einen sekundären RCN konfigurieren.

Hinweis

Verwechseln Sie die sekundäre MCN-Konfiguration nicht mit der Hochverfügbarkeitskonfiguration. In der sekundären MCN-Konfiguration wird ein Zweig-/Clientstandort an einem anderen geografischen Standort als sekundärer MCN konfiguriert, um eine Notfallwiederherstellung zu ermöglichen. In der HA-Konfiguration werden zwei Appliances mit demselben Subnetz oder geografischen Standort konfiguriert, um Fehlertoleranz zu gewährleisten. Informationen zur Konfiguration der Hochverfügbarkeitskonfiguration finden Sie unter [Hochverfügbarkeitsbereitstellung](#).

Sie können ein Appliance-Modell für den sekundären MCN basierend auf der Nutzung, der Bandbreitenanforderung und der Anzahl der zu unterstützenden Standorte auswählen.

Die primäre Umschaltung von MCN zu sekundärem MCN erfolgt nach 15 Sekunden, wenn der primäre MCN inaktiv ist. Sie können den primären Rückgewinn für sekundären MCN nicht konfigurieren, die primäre Rückgewinnung erfolgt automatisch, nachdem das primäre Gerät wieder eingeschaltet ist und der Haltezeitgeber abläuft.

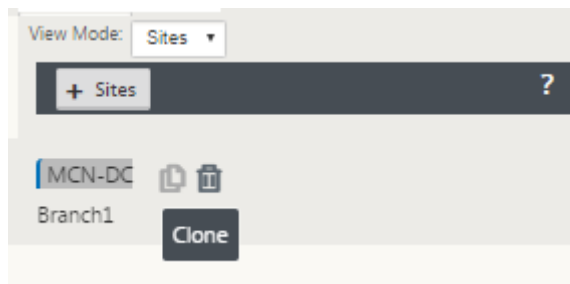
Der beste Weg, einen sekundären MCN zu konfigurieren, besteht darin, den vorhandenen MCN zu klonen, da er den größten Teil der MCN-Konfiguration beibehält. Wenn eine Site geklont wird, werden die gesamten Konfigurationseinstellungen für die Site kopiert und in einem einzigen Formularbildschirm angezeigt. Sie können die Einstellungen dann schnell und einfach an die Anforderungen anpassen.

Hinweis

Sie können einen MCN klonen, um einen sekundären MCN oder Zweigstandorte zu erstellen. Sie können nur einen sekundären MCN konfigurieren.

So klonen Sie eine MCN-Site und erstellen einen sekundären MCN:

1. Navigieren Sie im Konfigurationseditor zu **Basic > Sites** und klicken Sie auf das Klonsymbol für die MCN-Site.



2. Geben Sie die Konfigurationsparametereinstellungen für den neuen Standort ein.

Clone

Please review the following fields and make the appropriate changes for the new Site.

Site Name:
MCN-DC

Appliance Name:
Appliance

Mode:
secondary MCN

Secure Key:
250bcca02112f3b6

Routing Domains

| Name | Enable | Default |
|-----------------------|-------------------------------------|-------------------------------------|
| Default_RoutingDomain | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Virtual Interfaces

| Name | VLAN ID | DHCP |
|--------------------|---------|--------------------------|
| VirtualInterface-1 | 0 | <input type="checkbox"/> |
| VirtualInterface-2 | 0 | <input type="checkbox"/> |

Virtual IP Addresses

| Include | Virtual Interface | Virtual IP Address/Prefix |
|-------------------------------------|--------------------|---------------------------|
| <input checked="" type="checkbox"/> | VirtualInterface-1 | 172.147.21.52/24 |
| <input checked="" type="checkbox"/> | VirtualInterface-2 | 172.147.22.52/24 |

Local Routes

| Include | Network Address | Routing Domain | Gateway |
|---------|-----------------|----------------|---------|
|---------|-----------------|----------------|---------|

WAN Links

| Include Link | WAN Link | Access Type | | | | | | | | | | |
|--|------------------|--------------------|--------------------|------------------|-------------------|--------------------|---------|-------------------------------------|-----------------|--------------------|---------------|--------------|
| <input checked="" type="checkbox"/> | MCN-DC-WL-1 | | | | | | | | | | | |
| <div><div>Access Interfaces</div><table><thead><tr><th>Include Interface</th><th>Access Interface</th><th>Virtual Interface</th><th>Virtual IP Address</th><th>Gateway</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>MCN-DC-WL-1-...</td><td>VirtualInterface-1</td><td>172.147.21.52</td><td>172.147.21.1</td></tr></tbody></table></div> | | | Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway | <input checked="" type="checkbox"/> | MCN-DC-WL-1-... | VirtualInterface-1 | 172.147.21.52 | 172.147.21.1 |
| Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway | | | | | | | | |
| <input checked="" type="checkbox"/> | MCN-DC-WL-1-... | VirtualInterface-1 | 172.147.21.52 | 172.147.21.1 | | | | | | | | |
| <input checked="" type="checkbox"/> | MCN-DC-WL-2 | | | | | | | | | | | |

GRE Tunnels

| Include | Name | Source IP | Destination IP | Tunnel IP / Prefix |
|---------|------|-----------|----------------|--------------------|
|---------|------|-----------|----------------|--------------------|

Clone

Cancel

Hinweis:

Ein hervorgehobenes Feld mit einem Audit-Alert-Symbol (roter Punkt) zeigt eine erforderliche Parametereinstellung an, die einen anderen Wert als die aktuelle Einstellung haben muss.

- 3. Wählen Sie im Feld **Modus** den **sekundären MCN** aus. Lösen Sie alle Audit-Warnungen.
- 4. Klicken Sie auf **Klonen**, um die sekundäre MCN-Site zu erstellen

MCN-Konfiguration verwalten

May 10, 2021

Der nächste Schritt besteht darin, die neue Konfiguration zu benennen und zu speichern, die auch als Konfigurationspaket angesehen wird. Dieser Schritt ist an dieser Stelle in der Konfiguration optional, wird jedoch empfohlen. Das Konfigurationspaket wird in Ihrem Workspace auf der lokalen Appliance gespeichert. Sie melden sich dann von der Managementoberfläche ab und setzen den Konfigurationsprozess später fort. Wenn Sie sich jedoch abmelden, sollten Sie die gespeicherte Konfiguration erneut öffnen, wenn Sie fortfahren. Anweisungen zum Öffnen einer gespeicherten Konfiguration finden Sie unten.

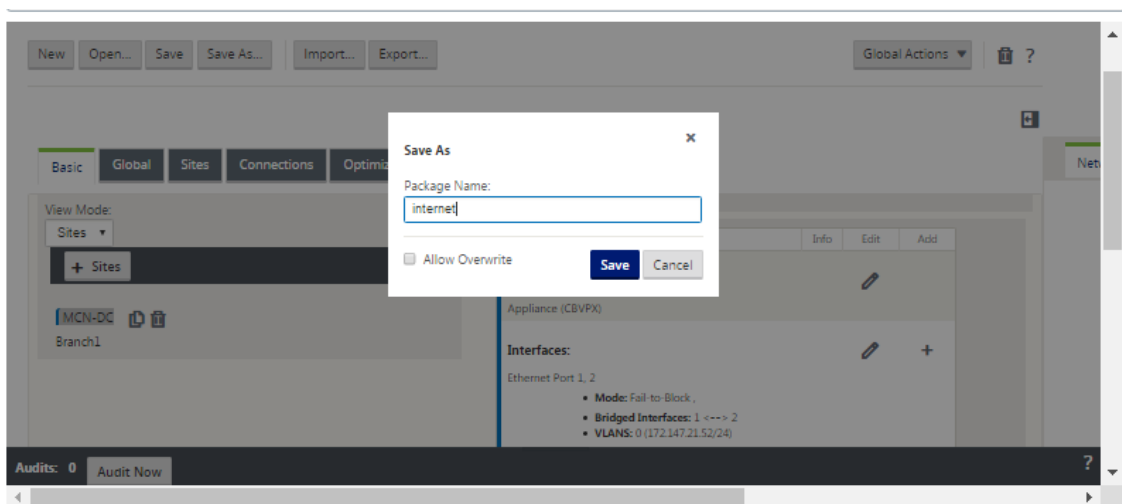
Warnung

Wenn die Konsolensitzung ein Timeout oder Sie sich vor dem Speichern der Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten Konfigurationsänderungen verloren. Sie sollten sich wieder beim System anmelden und den Konfigurationsvorgang von Anfang an wiederholen. Aus diesem Grund wird empfohlen, das Konfigurationspaket häufig oder an Schlüsselpunkten in der Konfiguration zu speichern.

Tipp:

Als zusätzliche Vorsichtsmaßnahme empfiehlt es sich, Speichern unter anstelle von Speichern zu verwenden, um ein Überschreiben des falschen Konfigurationspakets zu vermeiden.

1. Klicken Sie auf **Speichern unter** (oben im mittleren Bereich des **Konfigurations-Editors**). Das Dialogfeld **Speichern unter** wird geöffnet.



2. Geben Sie den Namen des Konfigurationspakets ein.

Hinweis

Wenn Sie die Konfiguration in einem vorhandenen Konfigurationspaket speichern, müssen Sie vor dem Speichern die Option **Überschreiben zulassen** auswählen.

3. Klicken Sie auf **Speichern**.

Hinweis

Nach dem Speichern der Konfigurationsdatei können Sie sich vom Management-Webinterface abmelden und den Konfigurationsvorgang später fortsetzen. Wenn Sie sich jedoch abmelden, sollten Sie die gespeicherte Konfiguration erneut öffnen, wenn Sie fortfahren. Anweisungen finden Sie im Abschnitt [Laden eines gespeicherten Konfigurationspakets in den Konfigurations-Editor](#).

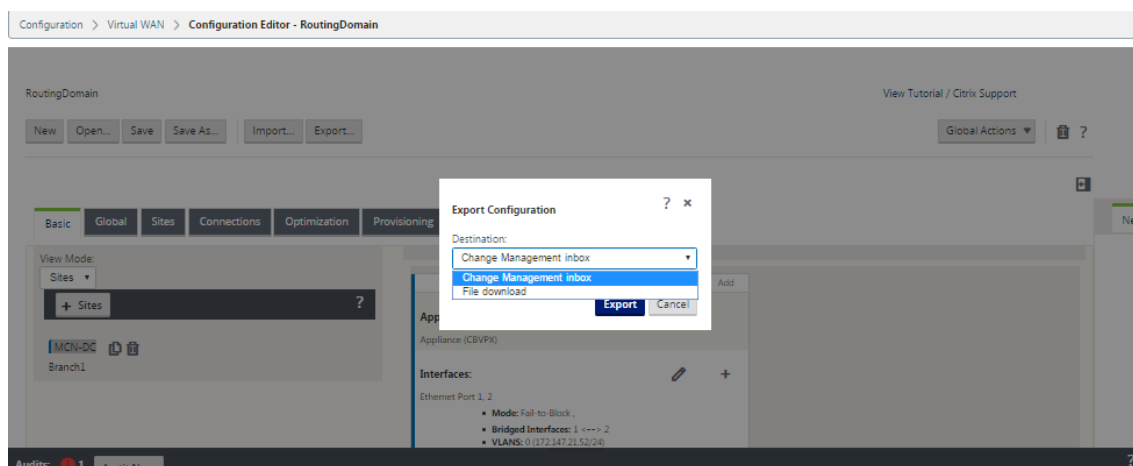
Sie haben nun die MCN-Standortkonfiguration abgeschlossen und ein neues SD-WAN-Konfigurationspaket erstellt. Sie können nun die Zweig-Sites hinzufügen und konfigurieren. Anweisungen finden Sie in [Setup Branch Sites](#) (/en-us/citrix-sd-wan/11-2/configuration/setup-branch-nodes.html).

Exportieren der Sicherungskopie des Konfigurationspakets

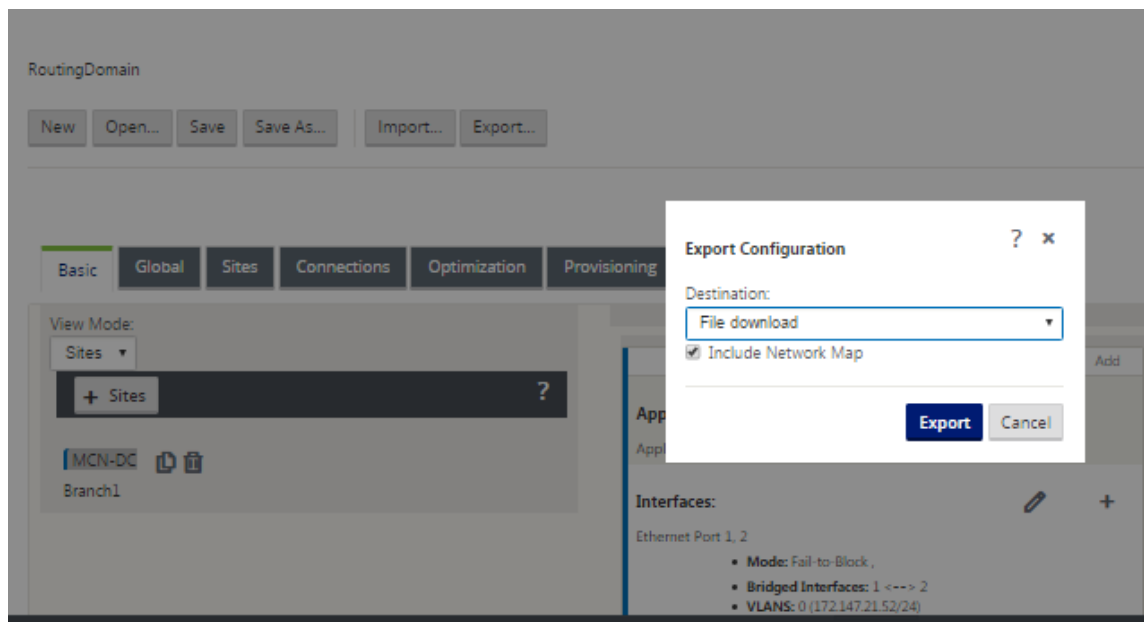
Es wird empfohlen, dass Sie nicht nur die laufende Konfiguration in Ihrem Appliance-Workspace speichern, sondern auch die Konfiguration regelmäßig auf Ihrem lokalen PC sichern.

Gehen Sie folgendermaßen vor, um das aktuelle Konfigurationspaket auf Ihren PC zu exportieren:

1. Klicken Sie auf **Exportieren**. Daraufhin wird das Dialogfeld **Konfiguration exportieren** angezeigt.



2. Wählen Sie im Dropdownmenü **Ziel** die Option **Dateidownload** aus. Dadurch wird die Option **Netzwerkzuordnung einschließen angezeigt**, die standardmäßig ausgewählt ist.



3. Übernehmen Sie die Standardeinstellung, und klicken Sie auf **Exportieren**. Dies schließt die **Netzwerkzuordnungsinformationen** im Konfigurationspaket ein und öffnet einen Dateibrowser zur Angabe des Namens und des Speicherorts für die Konfiguration.
4. Navigieren Sie zum Speicherort auf Ihrem PC und klicken Sie auf **Speichern**. Dadurch wird das Konfigurationspaket auf Ihrem PC gespeichert.

Hinweis

Zum Wiederherstellen eines gesicherten Konfigurationspakets können Sie das Paket mit **Import** von Ihrem PC importieren und in den **Konfigurations-Editor** laden. Anschließend können Sie das importierte Paket zur späteren Verwendung in Ihrem Management-Webinterface-Workspace speichern.

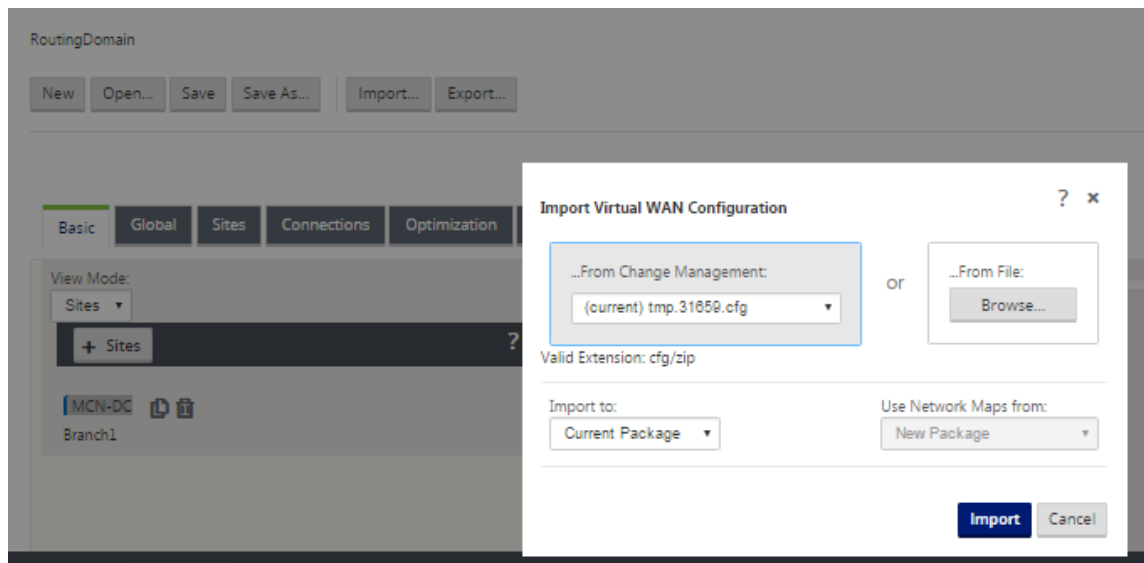
Importieren eines gesicherten Konfigurationspakets

Manchmal möchten Sie möglicherweise auf eine frühere Version eines Konfigurationspakets zurückkehren. Wenn Sie eine Kopie der früheren Version auf Ihrem lokalen PC gespeichert haben, können Sie sie wieder in den Konfigurations-Editor importieren und dann zur Bearbeitung öffnen. Wenn es sich nicht um eine Erstbereitstellung handelt, können Sie auch ein vorhandenes Konfigurationspaket aus dem globalen Change Management-Posteingang auf dem aktuellen MCN importieren. Anweisungen für diese beiden Verfahren finden Sie im Folgenden.

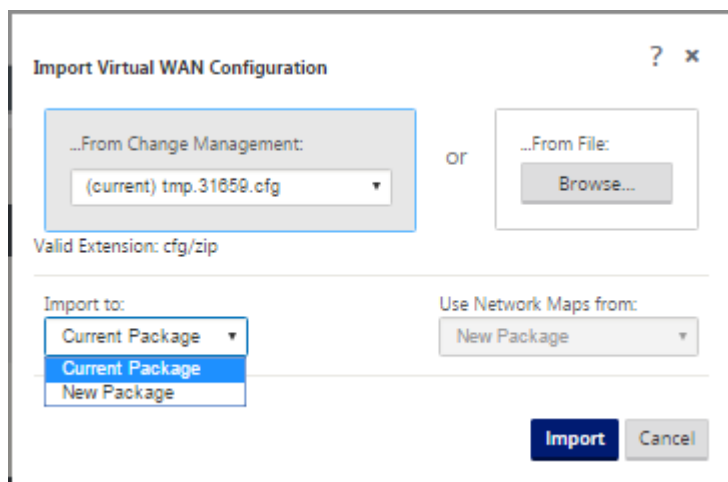
Gehen Sie folgendermaßen vor, um ein Konfigurationspaket zu importieren:

1. Öffnen Sie den **Konfigurations-Editor**.
2. Klicken Sie in der Menüleiste des **Konfigurations-Editors** auf **Importieren**.

Das Dialogfeld **Virtuelle WAN-Konfiguration importieren** wird angezeigt.



3. Wählen Sie den Speicherort aus, von dem das Paket importiert werden soll.
 - So importieren Sie ein Konfigurationspaket aus der Änderungsverwaltung: Wählen Sie das Paket aus dem Dropdownmenü **Von Änderungsverwaltung** (obere linke Ecke) aus.
 - So importieren Sie ein Konfigurationspaket von Ihrem lokalen PC: Klicken Sie auf **Durchsuchen**, um einen Dateibrowser auf Ihrem lokalen PC zu öffnen. Wählen Sie die Datei aus, und klicken Sie auf **OK**.
4. Wählen Sie das Importziel (falls zutreffend) aus. Wenn bereits ein Konfigurationspaket im **Konfigurations-Editor** geöffnet ist, ist das Dropdownmenü **Importieren nach:** verfügbar.

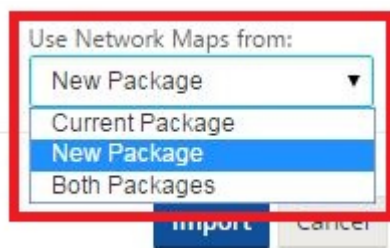


Wählen Sie eine der folgenden Optionen:

Aktuelles Paket —Wählen Sie diese Option aus, um den Inhalt des aktuell geöffneten Konfigurationspakets durch den Inhalt des importierten Pakets zu ersetzen und den Namen des

geöffneten Pakets beizubehalten. Der Inhalt der gespeicherten Version des aktuellen Pakets wird jedoch erst überschrieben, wenn Sie das geänderte Paket explizit speichern. Wenn Sie **Speichern unter** verwenden, um das Paket zu speichern, wählen Sie **Überschreiben zulassen** aus, um das Überschreiben der vorherigen Version zu aktivieren.

- **Neues Paket** —Wählen Sie diese Option aus, um ein neues, leeres Konfigurationspaket zu öffnen und es mit dem Inhalt des importierten Pakets zu füllen. Das neue Paket hat automatisch denselben Namen wie das importierte Paket.
5. Geben Sie an, welche Netzwerkzuordnungen eingeschlossen werden sollen (falls zutreffend). Wenn bereits ein Konfigurationspaket im **Konfigurations-Editor** geöffnet ist, ist das Dropdownmenü **Netzwerkarten verwenden von** verfügbar.

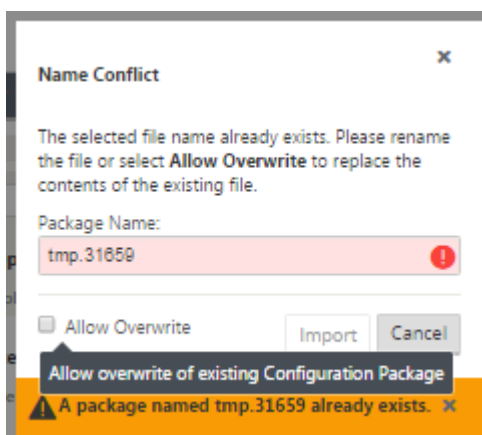


Wählen Sie eine der folgenden Optionen:

- **Aktuelles Paket** —Hierbei werden die Netzwerkzuordnungen beibehalten, die derzeit im Paket konfiguriert sind, das jetzt im Konfigurations-Editor verfügbar ist, und alle Netzwerkzuordnungen aus dem importierten Paket werden verworfen.
 - **Neues Paket** —Dies ersetzt die Netzwerkzuordnungen, die derzeit im aktuell geöffneten Paket konfiguriert sind, durch die Netzwerkzuordnungen (falls vorhanden) aus dem importierten Paket.
 - **Beide Pakete** —Dies umfasst alle Netzwerkkarten aus dem aktuellen und dem importierten Paket.
6. Klicken Sie auf **Importieren**. Die importierte Datei wird entsprechend Ihren Vorgaben in den **Konfigurations-Editor** geladen.

Hinweis

Wenn ein Paket mit demselben Namen in Ihrem Workspace vorhanden ist, wird das Dialogfeld **Namenskonflikt** angezeigt.



Führen Sie einen der folgenden Schritte aus, um den Namen anzugeben, der für das importierte Paket verwendet werden soll:

- Geben Sie einen anderen Namen in das Feld **Paketname** ein, um das neue Paket umzubenennen, und aktivieren Sie die Schaltfläche **Importieren**. Das importierte Paket wird mit dem angegebenen Namen in den **Konfigurations-Editor** geladen. Der Paketname wird jetzt in Ihrem Workspace gespeichert, der Paketinhalt wird jedoch in Ihrem Workspace gespeichert, bis Sie das Paket explizit speichern.
- Wählen Sie **Überschreiben zulassen** aus, um zu bestätigen, dass Sie den vorhandenen Namen beibehalten und das Überschreiben des Inhalts des gespeicherten Pakets aktivieren möchten. Der Inhalt der gespeicherten Version des aktuellen Pakets wird jedoch erst überschrieben, wenn Sie das geänderte Paket explizit speichern.

Dadurch wird auch die Schaltfläche **Importieren** im Dialogfeld **Namenskonflikt** aktiviert. Klicken Sie auf **Importieren**, um den Importvorgang abzuschließen.

Gespeichertes Konfigurationspaket laden

Um die Arbeit an einem gespeicherten Konfigurationspaket fortzusetzen, müssen Sie zuerst das Paket öffnen und es in den **Konfigurations-Editor** laden.

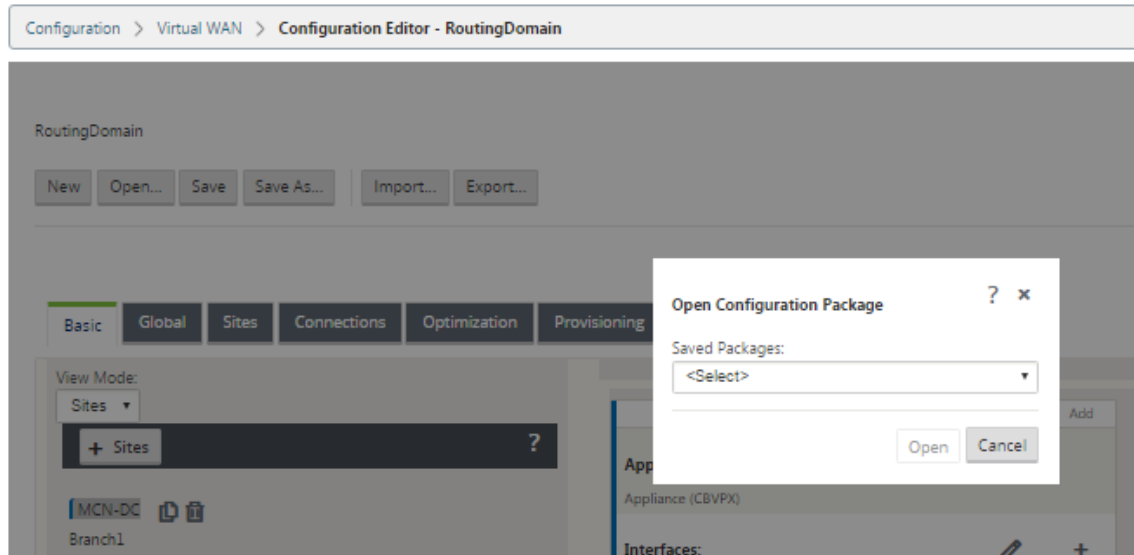
Gehen Sie folgendermaßen vor, um ein gespeichertes Konfigurationspaket zu laden:

1. Melden Sie sich wieder an der Management-Weboberfläche an, und navigieren Sie zum **Konfigurations-Editor**. Dadurch wird die Hauptseite des **Konfigurations-Editors** für eine neue Sitzung geöffnet.

Wenn Sie sich wieder bei der Managementoberfläche angemeldet haben, wird der **Konfigurations-Editor** zunächst für eine neue Sitzung geöffnet, ohne das Konfigurationspaket geladen zu haben. Sie können eine neue Konfiguration starten (**Neu**), eine vorhandene gespeicherte

Konfiguration **öffnen** oder **importieren** und dann eine zuvor auf Ihrem lokalen PC gesicherte Konfiguration **öffnen**.

2. Klicken Sie auf **Öffnen**. Das Dialogfeld **Konfigurationspaket öffnen** wird angezeigt.



3. Wählen Sie das zu öffnende Paket aus dem Dropdownmenü **Gespeicherte Pakete** aus.

Hinweis

Wenn Sie den **Konfigurations-Editor** geöffnet haben, kann es einige Sekunden oder zwei Minuten dauern, bis das Menü **Gespeicherte Pakete** aufgefüllt wird, abhängig von der Anzahl der Konfigurationen, die Sie in Ihrem Workspace gespeichert haben. Ist dies der Fall, wird in der Zwischenzeit im Menüfeld **Gespeicherte Pakete** möglicherweise die Meldung **Keine gespeicherten Pakete** angezeigt. Klicken Sie in diesem Fall auf **Abbrechen**, um das Dialogfeld zu schließen, warten Sie einige Augenblicke, und klicken Sie erneut auf **Öffnen**, um das Dialogfeld erneut zu öffnen.

4. Klicken Sie auf **Öffnen**.

Hinweis

Dadurch wird das angegebene Konfigurationspaket geöffnet und nur zur Bearbeitung in den **Konfigurations-Editor** geladen. Dadurch wird die ausgewählte Konfiguration nicht für die lokale Appliance bereitgestellt oder aktiviert.

Umbenennen von Websites

Wenn Sie den Namen des MCN-Standorts im Konfigurationseditor ändern, müssen Sie die Konfiguration mit dem umbenannten Standort auf das MCN- und SD-WAN-Netzwerk anwenden. Je nach MCN-

Rolle und ob Hochverfügbarkeit aktiviert oder deaktiviert ist, gelten die folgenden Szenarien für die SD-WAN-Netzwerkconfiguration beim Umbenennen von Standorten.

- MCN
- MCN mit hoher Verfügbarkeit
- GEO
- GEO mit hoher Verfügbarkeit
- RCN
- RCN mit hoher Verfügbarkeit

MCN-Site umbenennen

Nachdem Sie den MCN umbenannt haben, müssen Sie die neue Konfiguration mit der umbenannten Site laden.

So laden Sie eine neue Konfiguration für umbenannte Site hoch:

1. Aus dem MCN, Staging des Netzwerks mit der neuen Konfiguration.
2. Laden Sie das Staging-Konfigurationspaket für den umbenannten MCN herunter.
3. Navigieren Sie zur Seite **Lokale Änderungsverwaltung** des MCN.
 - a) Laden Sie das zuvor heruntergeladene Paket hoch.
 - b) Klicken Sie auf **Weiter**, nachdem die Verarbeitung abgeschlossen ist.
 - c) Klicken Sie auf **Aktivieren**.

Hinweis

Nachdem Schritt 3 (c) abgeschlossen ist, aktiviert der Änderungsverwaltungsprozess automatisch die bereitgestellten Software für Appliances (Knoten) im Netzwerk.

MCN-Site mit hoher Verfügbarkeit umbenennen

Nachdem Sie den MCN umbenannt haben, für den Hochverfügbarkeit aktiviert ist, müssen Sie die neue Konfiguration laden.

1. Aus dem MCN, Staging des Netzwerk mit neuer Konfiguration.
2. Laden Sie das Staging-Konfigurationspaket für die aktiven und hochverfügbaren MCN-Appliances mit neuem Namen herunter.
3. Deaktivieren Sie den Dienst auf der Standby-MCN-Appliance.
4. Navigieren Sie zur Seite **Lokale Änderungsverwaltung** des aktiven MCN.
 - a) Laden Sie das zuvor heruntergeladene Paket hoch.

- b) Klicken Sie auf **Weiter**, wenn die Verarbeitung abgeschlossen ist.
- c) Klicken Sie auf **Aktivieren**.
- d) Wiederholen Sie die Schritte i, ii, iii, iv für die deaktivierte Standby-MCN-Appliance mit hoher Verfügbarkeit.
- e) Aktivieren Sie den Dienst auf der Standby-MCN-Appliance.

Hinweis

Nachdem Schritt 4 (c) abgeschlossen ist, aktiviert der Änderungsverwaltungsprozess automatisch die bereitgestellten Software für Appliances im Netzwerk.

GEO-Site umbenennen

So laden Sie eine neue Konfiguration für eine umbenannte GEO-Site hoch:

1. Stage aus dem MCN Netzwerk mit neuer Konfiguration, die den umbenannten GEO-Site enthält.
2. Laden Sie vom MCN das Staging-Konfigurationspaket für die umbenannte GEO-Site herunter.
3. Wählen Sie im **MCN** die Option **Staged for network aktivieren** aus. Dadurch wird die umbenannte Site deaktiviert und die Site wird nicht mehr verfügbar.
4. Navigieren Sie auf der GEO-Site zur Seite **Lokales Änderungsmanagement**.
 - a) Laden Sie das zuvor heruntergeladene Paket hoch.
 - b) Klicken Sie auf **Weiter**, wenn die Verarbeitung des Pakets abgeschlossen ist.
 - c) Klicken Sie auf **Aktivieren**.

Umbenennen von GEO-Site mit hoher Verfügbarkeit

So laden Sie eine neue Konfiguration mit einer umbenannten GEO-Site hoch, die mit hoher Verfügbarkeit aktiviert ist:

1. Stage aus dem MCN Netzwerk mit neuer Konfiguration, die den umbenannten GEO-Site enthält.
2. Laden Sie das Staging-Konfigurationspaket für die aktiven und hochverfügbaren Appliances mit der umbenannten GEO-Site aus dem MCN herunter.
3. Wählen Sie im **MCN** die Option **Staged für das Netzwerk aktivieren** aus. Dadurch wird die umbenannte Site deaktiviert, und die Site wird nicht mehr verfügbar.
4. Navigieren Sie zur aktiven GEO-Appliance.
 - a) Wechseln Sie zur Seite Lokale Änderungsverwaltung.
 - b) Laden Sie das zuvor heruntergeladene Paket hoch.

- c) Klicken Sie auf **Weiter**, wenn die Verarbeitung des Pakets abgeschlossen ist.
- d) Klicken Sie auf **Aktivieren**.
- e) Wiederholen Sie die Schritte a, b, c und d für die Standby-Appliance.

RCN-Site umbenennen

So laden Sie eine neue Konfiguration mit umbenannten RCN-Site hoch:

1. Aus dem MCN das Netzwerk mit einer neuen Konfiguration, die den umbenannten RCN-Site enthält.
2. Laden Sie das Stagingpaket für die umbenannte RCN-Site aus dem MCN herunter.
3. Wählen Sie im **MCN** die Option **Staged for network aktivieren** aus. Dadurch wird der umbenannte RCN-Site deaktiviert, und der Region-Site wird im MCN nicht verfügbar. Der RCN-Standort und die Zweige in der Region kommunizieren miteinander. Bis Schritt 4 abgeschlossen ist, kann die Region jedoch nicht mit dem MCN kommunizieren (es sei denn, es gibt einen GEO-RCN, der nicht umbenannt wird).
4. Navigieren Sie zur Seite Lokales Änderungsmanagement des RCN:
 - a) Laden Sie das zuvor heruntergeladene Paket hoch.
 - b) Klicken Sie auf **Weiter**, wenn die Paketverarbeitung abgeschlossen ist.
 - c) Klicken Sie auf **Aktivieren**.

Hinweis

Die Zweige in der Region benötigen einige Zeit, um verfügbar zu werden, da die Region-Staging erst nach Abschluss von Schritt 4 (c) erfolgt. Der Change Management-Prozess des RCN verwaltet die Region Staging.

Umbenennen von RCN-Site mit hoher Verfügbarkeit

Um eine neue Konfiguration hochzuladen, bei der umbenannte RCN-Site mit hoher Verfügbarkeit aktiviert ist.

1. Aus dem MCN das Netzwerk mit einer neuen Konfiguration, die den umbenannten RCN-Site enthält.
2. Laden Sie das Stagingpaket aus dem MCN für die aktive und hochverfügbare Appliances mit umbenannter RCN-Site herunter. Dadurch wird der umbenannte RCN-Site deaktiviert, und der Region-Site wird im MCN nicht verfügbar. Der RCN-Standort und die Zweige in der Region kommunizieren miteinander. Bis Schritt 4 abgeschlossen ist, kann die Region jedoch nicht mit dem MCN kommunizieren (es sei denn, es gibt einen GEO-RCN, der nicht umbenannt wird).

3. Wählen Sie im **MCN** die Option **Staged für Netzwerk aktivieren** aus.
4. Deaktivieren Sie den Dienst auf der Standby-RCN-Appliance.
5. Navigieren Sie zur Seite **Lokales Änderungsmanagement** des aktiven RCN:
 - a) Laden Sie das zuvor heruntergeladene Paket hoch.
 - b) Klicken Sie auf **Weiter**, wenn die Verarbeitung des Pakets abgeschlossen ist.
 - c) Klicken Sie auf **Aktivieren**.
 - d) Wiederholen Sie die Schritte a, b und c für die deaktivierte Standby-RCN-Einheit.
6. Aktivieren Sie den Dienst auf der Standby-RCN-Appliance.

Umbenennen der GEO RCN-Website

So laden Sie eine neue Konfiguration mit umbenannten GEO RCN-Site hoch:

1. Aus dem MCN, Staging des Netzwerks mit neuer Konfiguration mit umbenannten GEO RCN Standort.
2. Laden Sie vom MCN das Stagingpaket für die umbenannte GEO RCN-Site herunter.
3. Wählen Sie im **MCN** die Option **Staged for network aktivieren** aus. Dadurch wird die umbenannte Site deaktiviert, und die Site wird nicht mehr verfügbar. Wenn der primäre RCN online ist, bleibt die Region beim Umbenennen des GEO RCN-Standorts mit dem Netzwerk verbunden.
4. Navigieren Sie zur Seite **Lokales Änderungsmanagement** des GEO RCN:
 - a) Laden Sie das zuvor heruntergeladene Paket hoch.
 - b) Klicken Sie auf **Weiter**, wenn die Verarbeitung des Pakets abgeschlossen ist.
 - c) Klicken Sie auf **Aktivieren**.

Umbenennen von GEO RCN-Site mit hoher Verfügbarkeit

1. Aus dem MCN, Staging des Netzwerks mit neuer Konfiguration mit umbenannten GEO RCN Standort.
2. Laden Sie das Stagingpaket sowohl für die aktive als auch für die Hochverfügbarkeits-Appliance für die umbenannte GEO RCN-Site herunter.
3. Wählen Sie im **MCN** die Option **Staged for network aktivieren** aus. Dadurch wird die umbenannte Site deaktiviert, und die Site wird nicht mehr verfügbar. Wenn der primäre RCN online ist, bleibt die Region beim Umbenennen des GEO RCN-Standorts mit dem Netzwerk verbunden.
4. Navigieren Sie zur Seite **Local Change Management** des aktiven GEO RCN:
 - a) Laden Sie das zuvor heruntergeladene Paket hoch.

- b) Klicken Sie auf **Weiter**, wenn die Verarbeitung des Pakets abgeschlossen ist.
- c) Klicken Sie auf **Aktivieren**.
- d) Wiederholen Sie die Schritte a, Band c für die Standby-Appliance.

Einrichten von Zweigknoten

May 10, 2021

Dieses Kapitel enthält Anweisungen zum Hinzufügen und Konfigurieren der Zweigstandorte. Das Verfahren zum Hinzufügen eines Zweigstandorts ähnelt dem Erstellen und Konfigurieren der MCN-Site sehr. Einige Konfigurationsschritte und -einstellungen unterscheiden sich jedoch geringfügig für einen Zweigstandort. Wenn Sie einen anfänglichen Zweigstandort hinzugefügt haben, können Sie außerdem für Sites mit demselben Appliance-Modell die Funktion **Klonen** (Duplizieren) verwenden, um das Hinzufügen und Konfigurieren dieser Sites zu optimieren.

Wie beim Erstellen des MCN-Standorts zum Einrichten eines Zweigstandorts müssen Sie den **Konfigurations-Editor** im Management-Webinterface auf der MCN-Appliance verwenden. Der **Konfigurations-Editor** ist nur verfügbar, wenn die Schnittstelle auf den **MCN-Konsolenmodus** eingestellt ist.

Zusätzliche Informationen zur Bereitstellung von Zweigstandort

Zusätzlich zu diesem Handbuch werden auch die folgenden Knowledge Base-Supportartikel empfohlen:

- Schritte zur Bereitstellung virtueller WAN-PBR-Modus ([CTX201577](http://support.citrix.com/article/CTX201577))
<http://support.citrix.com/article/CTX201577>
- Schritte zur Bereitstellung des virtuellen WAN-Gateway-Modus ([CTX201576](http://support.citrix.com/article/CTX201576))
<http://support.citrix.com/article/CTX201576>

Übersicht über die Konfigurationsprozeduren für Zweigstandort

Die Schritte, um diesen Prozess abzuschließen, sind wie folgt:

1. Fügen Sie den Zweigstandort hinzu.
2. Konfigurieren Sie die virtuellen Schnittstellengruppen für den Zweigstandort.
3. Konfigurieren Sie die virtuellen IP-Adressen für den Zweigstandort.

4. (Optional) Konfigurieren Sie die LAN GRE Tunnel für den Zweigstandort.
5. Konfigurieren Sie die WAN-Links für den Zweigstandort.
6. Konfigurieren Sie die Routen für den Zweigstandort.
7. (Optional) Konfigurieren Sie Hochverfügbarkeit für den Zweigstandort.
8. (Optional) Klonen Sie den neuen Zweigstandort, um zusätzliche Sites zu erstellen und zu konfigurieren.

Hinweis

Das Klonen der Site ist optional. Die Virtual WAN-Appliance-Modelle müssen sowohl für die ursprüngliche als auch für die geklonten Sites identisch sein. Sie können das angegebene Einheitenmodell für einen Klon nicht ändern. Wenn sich das Appliance-Modell für einen Standort unterscheidet, müssen Sie die Site manuell hinzufügen.

9. Lösen Sie alle Konfigurationsüberwachungswarnungen.
10. Speichern Sie die abgeschlossene Konfiguration.

Zweigknoten konfigurieren

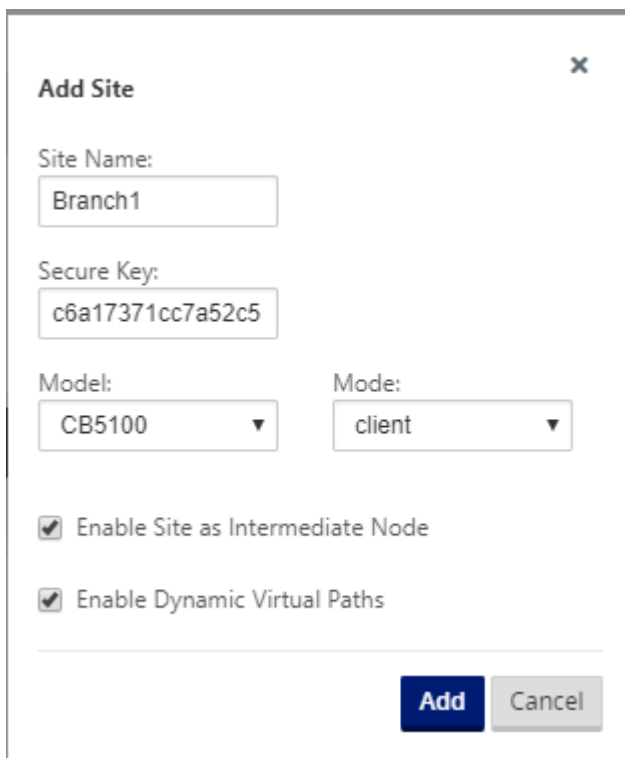
May 10, 2021

Gehen Sie folgendermaßen vor, um der Tabelle **Sites** einen neuen Zweigstandort hinzuzufügen und mit der Konfiguration der Site zu beginnen:

Hinweis

Wenn Sie sich nach dem Erstellen und Speichern des neuen Konfigurationspakets vom MCN abgemeldet haben, müssen Sie sich erneut anmelden und die Konfiguration erneut öffnen, bevor Sie fortfahren können. Klicken Sie dazu in der Menüleiste des **Konfigurations-Editors** (oben im Seitenbereich) auf **Öffnen** . Hier wird ein Dialogfeld angezeigt, in dem Sie die Konfiguration auswählen können, die Sie ändern möchten.

1. Klicken Sie im **Konfigurations-Editor** auf **Hinzufügen** in der **Siteleiste**, um mit dem Hinzufügen und Konfigurieren des neuen Zweigstandorts zu beginnen. Das Dialogfeld **Site hinzufügen** wird angezeigt.



2. Geben Sie die folgenden Standortinformationen ein.

Hinweis

Einträge dürfen keine Leerzeichen enthalten und müssen im Linux-Format vorliegen.

- **Standortname** —Geben Sie einen Namen für die Site ein.
 - **Appliance-Name** —Geben Sie den Namen ein, den Sie der Appliance zuweisen möchten.
 - **Sicherer Schlüssel** —Dies ist ein Hexadezimalschlüssel mit 8 bis 32 Ziffern, der für die Verschlüsselung und die Mitgliedschaftsüberprüfung in der SD-WAN-Appliance verwendet wird. Standardmäßig ist dieses Feld mit einem automatisch generierten Sicherheitsschlüssel vorausgefüllt. Übernehmen Sie die Standardeinstellung, oder geben Sie ein benutzerdefiniertes Hexadezimalformat ein.
 - **Modell** —Wählen Sie das Appliance-Modell aus dem Dropdownmenü aus.
 - **Modus** —Wählen Sie den Client als Modus aus.
3. Klicken Sie auf **Hinzufügen**, um die Website hinzuzufügen. Die neue Site wird der **Sitestruktur** hinzugefügt und öffnet das Konfigurationsformular **Grundeinstellungen** für die Site.

The screenshot shows the 'Basic Settings' configuration page for a new site. On the left, a sidebar lists various configuration categories: Sites, Basic Settings (selected), Routing Domains, Interface Groups, Virtual IP Addresses, VRRP, DHCP, WAN Links, Certificates, and High Availability. The main area contains the following fields:

- Site Name:** Branch
- Appliance Name:** Branch-CB1000
- Secure Key:** 805a85b2611f305c (with a 'Regenerate' button)
- Model:** CB1000 (dropdown)
- Mode:** client (dropdown)
- Site Location:** SC
- Default Direct Route Cost:** 5
- Gateway ARP Timer (ms):** 1000
- ☐ **Enable Source MAC Learning**

At the bottom are 'Apply' and 'Close' buttons.

4. Geben Sie die Grundeinstellungen für die Website ein, und klicken Sie auf **Übernehmen**.

Der nächste Schritt besteht darin, die Schnittstellengruppen für den neuen Zweigstandort hinzuzufügen und zu konfigurieren.

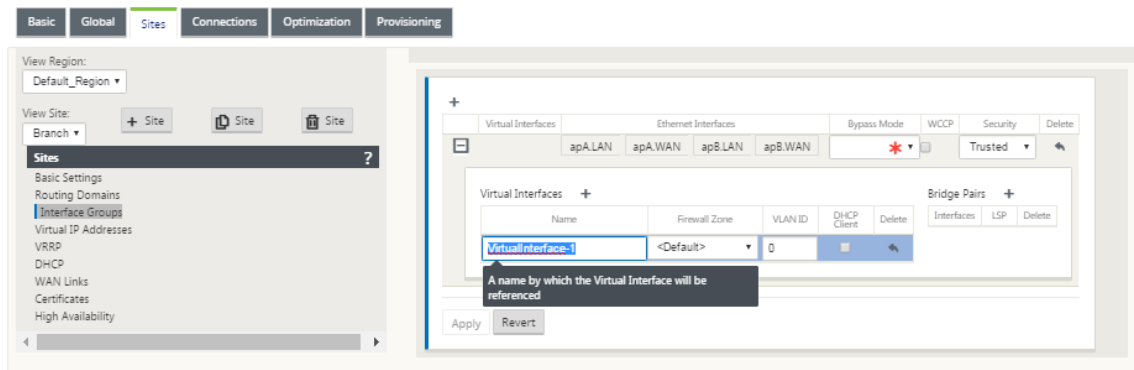
Konfigurieren von Schnittstellengruppen für den Zweig

Gehen Sie folgendermaßen vor, um der neuen Zweigstellensite eine Schnittstellengruppe hinzuzufügen:

1. Wählen Sie in der **Sitesansicht** des **Konfigurationseditors** den Zweigstandort aus dem Dropdownmenü **Site anzeigen** aus. Dadurch wird die Konfigurationsansicht für den ausgewählten Standort geöffnet.

The screenshot shows the 'Interface Groups' configuration page. At the top, there are tabs for 'Basic', 'Global', 'Sites' (selected), 'Connections', 'Optimization', and 'Provisioning'. Below the tabs, the 'View Region:' dropdown is set to 'Default_Region'. The 'View Site:' dropdown is set to 'Branch'. The sidebar on the left shows the 'Interface Groups' category selected. The main area contains a table with columns: 'Virtual Interfaces', 'Ethernet Interfaces', 'Bypass Mode', 'WCCP', 'Security', and 'Delete'. An 'Add' button is visible in the top left of the table area. At the bottom are 'Apply' and 'Close' buttons.

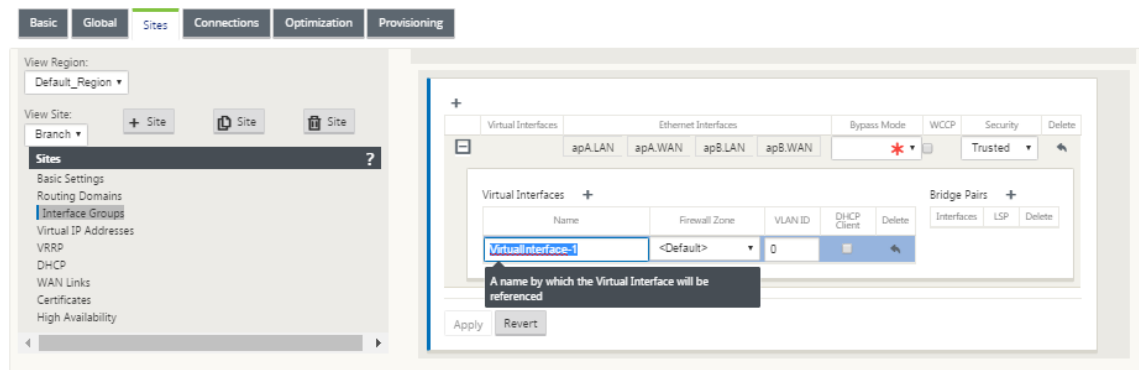
2. Klicken Sie auf **+**, um die **Gruppe der virtuellen Schnittstelle** hinzuzufügen. Der Tabelle wird ein neuer leerer Eintrag für virtuelle Schnittstellengruppen hinzugefügt und zur Bearbeitung geöffnet.
3. Klicken Sie rechts neben **Virtuelle Schnittstellen** auf **+**. Ein neuer leerer Gruppeneintrag wird zur Tabelle hinzugefügt und zur Bearbeitung geöffnet.



4. Wählen Sie die **Ethernet-Schnittstellen** aus, die in die Gruppe aufgenommen werden sollen.
Klicken Sie unter **Ethernet-Schnittstellen** auf eine Schnittstelle, um diese Schnittstelle ein- bzw. auszuschließen. Sie können beliebig viele Schnittstellen auswählen, die in die Gruppe aufgenommen werden sollen.



5. Wählen Sie im Dropdownmenü den **Umgehungsmodus** (keine Standardeinstellung).
Der **Umgehungsmodus** gibt das Verhalten von Bridgepaarten Schnittstellen in der virtuellen Schnittstellengruppe an, wenn eine Appliance oder ein Dienstausschlag oder ein Neustart auftritt. Die Optionen sind: **Fail-to-Wire** oder **Fail-to-Block**.
6. Wählen Sie die **Sicherheitsstufe** aus dem Dropdownmenü.
Dies gibt die Sicherheitsstufe für das Netzwerksegment der virtuellen Schnittstellengruppe an. Die Optionen sind: **Vertrauenswürdig** oder **Nicht vertrauenswürdig**. Vertrauenswürdige Segmente werden durch eine Firewall geschützt (Standard ist Vertrauenswürdig).
7. Klicken Sie am linken Rand der hinzugefügten virtuellen Schnittstelle auf **+**. Daraufhin wird die Tabelle **Virtuelle Schnittstellen** angezeigt.



8. Klicken Sie rechts neben **Virtuelle Schnittstellen** auf **+**. Die IDs **Name**, **Firewall Zone** und **VLAN-ID** werden angezeigt.
9. Geben Sie den **Namen** und die **VLAN-ID** für diese virtuelle Schnittstellengruppe ein.
 - **Name** —Der Name, mit dem auf diese virtuellen Schnittstellen verwiesen wird.
 - **Firewall-Zone** - Wählen Sie eine Firewall-Zone aus dem Dropdownmenü aus.
 - **VLAN-ID** —Die ID zum Identifizieren und Markieren von Datenverkehr zu und von der virtuellen Schnittstelle. Verwenden Sie die ID 0 (Null) für native/nicht markierte Datenverkehr.
10. Klicken Sie rechts neben **Brückenpaaren** auf **+**. Ein neuer **Bridge Pairs** Eintrag wird hinzugefügt und wird zur Bearbeitung geöffnet.
11. Wählen Sie die Ethernet-Schnittstellen, die gekoppelt werden sollen, aus den Dropdownmenüs aus. Um weitere Paare hinzuzufügen, klicken Sie erneut auf **+** neben **Bridge-Paare**.
12. Klicken Sie auf **Übernehmen**. Ihre Einstellungen werden angewendet und der neuen virtuellen Schnittstellengruppe der Tabelle hinzugefügt.

Hinweis

Zu diesem Zeitpunkt sehen Sie rechts neben dem neuen Eintrag für die Gruppe der virtuellen Schnittstelle ein gelbes Deltaüberwachungswarnsymbol. Dies liegt daran, dass Sie noch keine virtuellen IP-Adressen (VIPs) für die Site konfiguriert haben. Vorerst können Sie diese Warnung ignorieren, da sie automatisch aufgelöst wird, wenn Sie die virtuellen IPs für die Site richtig konfiguriert haben.

13. Um weitere virtuelle Schnittstellengruppen hinzuzufügen, klicken Sie rechts neben dem Zweig **Schnittstellengruppen** auf **+** und fahren Sie wie oben fort.

Konfigurieren der virtuellen IP-Adresse für den Zweigstandort

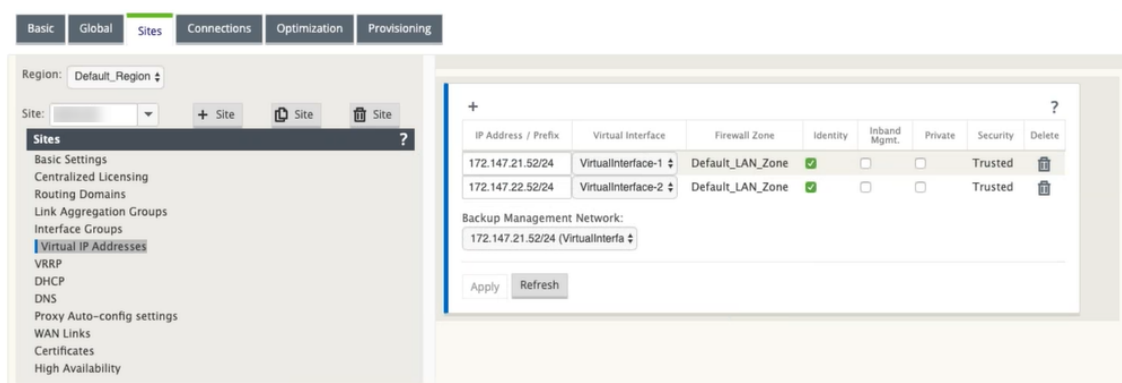
Der nächste Schritt besteht darin, die virtuellen IP-Adressen für den Standort zu konfigurieren und sie der entsprechenden Gruppe zuzuweisen.

1. Klicken Sie in der Ansicht **Sites** für den neuen Zweigstandort auf **+** links neben den **Virtuellen IP-Adressen**. Dadurch wird die Tabelle **Virtuelle IP-Adressen** für den neuen Standort angezeigt.
2. Klicken Sie rechts neben **Virtuelle IP-Adressen** auf **+**, um eine Adresse hinzuzufügen. Das Formular zum Hinzufügen und Konfigurieren einer neuen virtuellen IP-Adresse wird angezeigt.
3. Geben Sie die **IP-Adresse/Präfix-Informationen** ein, und wählen Sie die **virtuelle Schnittstelle** aus, mit der die Adresse verknüpft ist. Die virtuelle IP-Adresse muss die vollständige Hostadresse und die Netzmaske enthalten.
4. Wählen Sie die gewünschten Einstellungen für die virtuelle IP-Adresse aus, z. B. Firewall-Zone, Identität, Privat und Sicherheit.
5. Wählen Sie **Inband Mgmt**, damit die virtuelle IP-Adresse eine Verbindung zu Verwaltungsdiensten wie Web-UI und SSH herstellen kann.

Hinweis:

Die Schnittstelle sollte den Sicherheitstyp **Vertrauenswürdig** und **Identität** aktiviert haben.

6. Wählen Sie eine virtuelle IP als **Backup-Management-Netzwerk** aus. Auf diese Weise können Sie die virtuelle IP-Adresse für die Verwaltung verwenden, wenn der Verwaltungsport nicht mit einem Standard-Gateway konfiguriert ist.

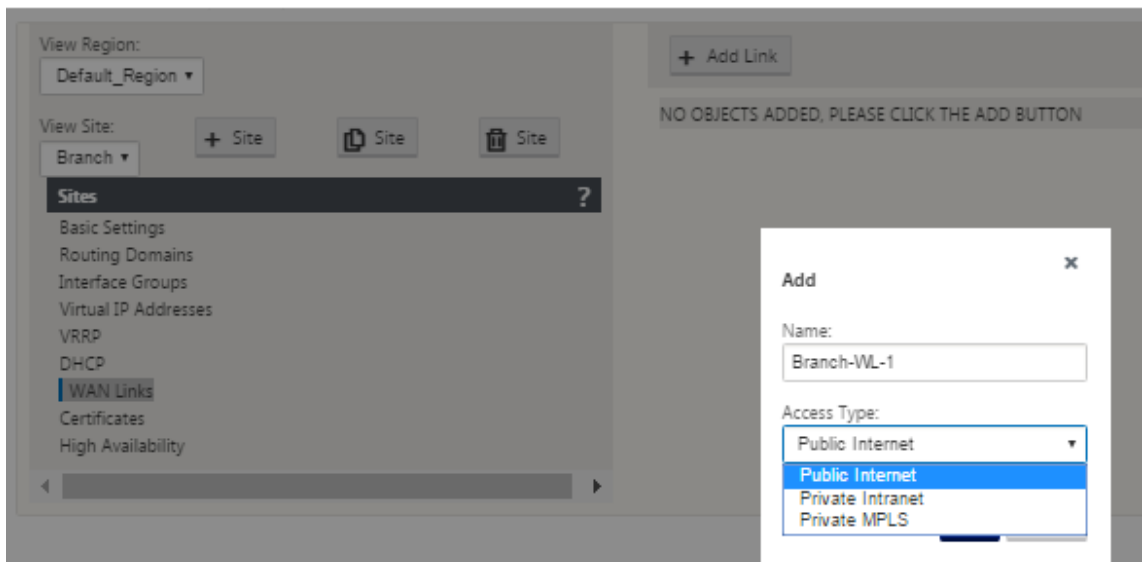


7. Klicken Sie auf **Übernehmen**. Die Adressinformationen zum Standort werden hinzugefügt und enthalten sie in die Tabelle **Virtuelle IP-Adressen** des Standortes.
8. Um weitere virtuelle IP-Adressen hinzuzufügen, klicken Sie rechts neben den **Virtuellen IP-Adressen** auf **+**, und fahren Sie wie oben beschrieben fort.

So konfigurieren Sie WAN-Links für den Zweig

Der nächste Schritt besteht darin, die WAN-Links für die Site zu konfigurieren.

1. Klicken Sie in der Ansicht **Sites** für den neuen Zweigstandort auf die Bezeichnung **WAN-Links**.
2. Klicken Sie rechts neben den **WAN-Links** auf **Link hinzufügen**, um eine neue WAN-Verbindung hinzuzufügen. Das Dialogfeld **Hinzufügen** wird angezeigt.



3. (Optional) Geben Sie einen Namen für die WAN-Verbindung ein, wenn Sie die Standardeinstellung nicht verwenden möchten.

Der Standardwert ist der Site-Name, der mit dem folgenden Suffix angehängt wird:

<number>-WL-

Wo <number> ist die Anzahl der WAN-Links für diese Website, erhöht um eins.

4. Wählen Sie im Dropdownmenü den **Zugriffstyp** aus.

Die Optionen sind **Public Internet**, **Private Intranet** oder **Private Multiprotocol Label Switching**.

5. Klicken Sie auf **Hinzufügen**. Die Konfigurationsseite **WAN-Links** Basic Settings wird angezeigt und fügt der Seite den neuen nicht konfigurierten WAN-Link hinzu.

6. Geben Sie die Verknüpfungsdetails für die neue WAN-Verbindung ein. Konfigurieren Sie die LAN-zu-WAN-, **WAN-zu-LAN-Einstellungen**.

Einige Richtlinien lauten wie folgt:

- Einige Internetlinks könnten asymmetrisch sein. Eine falsche Konfiguration der zulässigen Geschwindigkeit kann sich negativ auf die Leistung dieser Verbindung auswirken.
- Vermeiden Sie die Verwendung von Burstgeschwindigkeiten, die die festgeschriebene Rate übertreffen.
- Achten Sie bei Internet-WAN-Verbindungen darauf, die öffentliche IP-Adresse hinzuzufügen.

7. Klicken Sie auf die graue Bereichsleiste **Erweiterte Einstellungen**. Dadurch wird das Formular **Erweiterte Einstellungen** für den Link geöffnet.

View Region: Default_Region

View Site: Branch

WAN Link: Branch-WL-1

Section: Settings

Basic Settings

Advanced Settings

Provider ID:

Frame Cost (bytes):

Congestion Threshold (µs):

MTU Size (bytes):

Eligibility

Metered/Standby Link

Apply Revert

8. Geben Sie die **erweiterten Einstellungen** für den Link ein.

- **Provider-ID** —(Optional) Geben Sie eine eindeutige ID-Nummer 1—100 ein, um WAN-Links festzulegen, die mit demselben Dienstanbieter verbunden sind. Virtual WAN verwendet die Provider-ID, um Pfade beim Senden doppelter Pakete zu unterscheiden.
- **Frame Cost (Bytes)** —Geben Sie die Größe (in Bytes) des Headers/Trailers ein, der zu jedem Paket hinzugefügt wurde. Zum Beispiel die Größe der hinzugefügten Ethernet-IPG- oder AAL5-Anhänger in Bytes.
- **Stauschwellenwert** —Geben Sie den Stauschwellenwert (in Mikrosekunden) ein, nach dem die WAN-Verbindung die Paketübertragung drosselt, um weitere Staus zu vermeiden.
- **MTU-Größe (Byte)** —Geben Sie die größte Rohpaketgröße (in Byte) ein, ohne die Frame-Kosten.

9. Klicken Sie auf die graue **Auswahlleiste**. Dadurch wird das Formular **Berechtigungseinstellungen** für den Link geöffnet.

10. Wählen Sie die **Berechtigungseinstellungen** für den Link aus.

View Region: Default_Region

View Site: Branch

WAN Link: Branch-WL-1

Section: Settings

Basic Settings

Advanced Settings

Eligibility

| | LAN to WAN | WAN to LAN |
|-------------|-------------------------------------|-------------------------------------|
| Realtime | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Interactive | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Bulk | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Metered/Standby Link

Apply Revert

11. Klicken Sie auf die graue Abschnittleiste mit **Metered Link**. Dadurch wird das Formular **Metered Link-Einstellungen** für den Link geöffnet.
12. (Optional) Wählen Sie **Metering** aktivieren, um die Messung für diesen Link zu aktivieren. Daraufhin werden die Felder **Metering-Einstellungen aktivieren** angezeigt.

The screenshot shows the Citrix SD-WAN configuration interface. On the left, a sidebar lists various configuration options: View Site, Branch, Site, Sites, Basic Settings, Routing Domains, Interface Groups, Virtual IP Addresses, VRRP, DHCP, **WAN Links** (highlighted), Certificates, and High Availability. The main panel displays the 'Metered/Standby Link' configuration. It includes sections for 'Basic Settings', 'Advanced Settings', 'Eligibility', and 'Metered/Standby Link'. The 'Metering' section has a checkbox for 'Enable Metering' which is checked, and a checkbox for 'Disable if Data Cap reached' which is also checked. Below these are fields for 'Data Cap (MB)' (set to 0), 'Billing Cycle' (set to Monthly), and 'Starting From' (set to MM/DD/YYYY). The 'Standby' section has a dropdown for 'Standby Mode' set to 'Disabled'. The 'Heartbeat Interval' section has a warning message: 'Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.' and a dropdown for 'Active Heartbeat Interval' set to 'DEFAULT'.

13. Konfigurieren Sie die Messeinstellungen für den Link. Geben Sie Folgendes ein:
 - **Data Cap (MB)** —Geben Sie die Daten-Cap-Zuweisung für die Verknüpfung in MB ein.
 - **Abrechnungszyklus** —Wählen Sie entweder **monatlich** oder **wöchentlich** aus dem Dropdown-Menü aus.
 - **Beginnend von** —Geben Sie das Startdatum des Abrechnungszyklus ein.
 - **Letztes Resort festlegen** —Wählen Sie diese Option aus, um diesen Link als letzten Ausweg im Falle eines Ausfalls aller anderen verfügbaren Links zu aktivieren. Unter normalen WAN-Bedingungen sendet Virtual WAN nur minimalen Datenverkehr über getaktete Links, um den Linkstatus zu überprüfen. Im Falle eines Ausfalls kann SD-WAN jedoch

aktive gemessene Links als letzter Ausweg für die Weiterleitung des Produktionsverkehrs verwenden.

14. Klicken Sie auf **Übernehmen**. Dadurch werden die angegebenen Einstellungen auf die neue WAN-Verbindung angewendet.

Der nächste Schritt besteht darin, die Access Interfaces für die neue WAN-Verbindung zu konfigurieren. Eine Zugriffsoberfläche besteht aus einer virtuellen Schnittstelle, einer WAN-Endpunkt-IP-Adresse, einer Gateway-IP-Adresse und einem virtuellen Pfadmodus, die gemeinsam als Schnittstelle für eine bestimmte WAN-Verbindung definiert sind. Jede WAN-Verbindung muss über mindestens eine Zugriffsoberfläche verfügen.

Hinweis

Eine Option zur automatischen Bereitstellung von Freigaben unter Berücksichtigung der Remotebandbreite wird hinzugefügt, um WAN-Verbindungen zu konfigurieren. Mit der Option Provisioning mit Remotebandbreite festlegen können Benutzer mit großen Netzwerken und unterschiedlichen Bandbreitenkonfigurationen die Bandbreitenbereitstellung für Rechenzentrumsstandorte dynamisch verwalten.

15. Wählen Sie auf der Seite WAN-Link-Konfiguration für den Link **Zugriffsschnittstellen** aus. Dadurch wird die Ansicht **Access Interfaces** für die Site geöffnet.

The screenshot shows two states of the WAN Link configuration page. In the top state, the 'Section:' dropdown is set to 'Settings'. In the bottom state, it is set to 'Access Interfaces', and a modal window for adding a new access interface is open. The modal window contains a table with the following columns: Add, Routing Domain, Virtual Interface, IP Address, Gateway IP Address, Virtual Path Mode, Proxy ARP, Internet Access for All Routing Domains, and Delete. The 'Add' button is highlighted in the modal.

16. Klicken Sie auf **+**, um eine Schnittstelle hinzuzufügen. Ein leerer Eintrag zur Tabelle wird hinzugefügt und zur Bearbeitung geöffnet. Geben Sie die Einstellungen für die **Access Interfaces** für die Verknüpfung ein.

Hinweis

Jede WAN-Verbindung muss über mindestens eine Zugriffsoberfläche verfügen.

17. Geben Sie Folgendes ein:

- **Name:** Dies ist der Name, mit dem diese Access Interface referenziert wird. Geben Sie einen Namen für die neue Access-Schnittstelle ein, oder übernehmen Sie die Standardeinstellung. Der Standardwert verwendet die folgende Namenskonvention:

WAN_link_name-AI-number

Wobei *wan_link_name* der Name der WAN-Verbindung ist, die Sie dieser Schnittstelle zuordnen, und *number* ist die Anzahl der derzeit für diesen Link konfigurierten Access Interfaces, erhöht um 1.

Hinweis

Wenn der Name abgeschnitten angezeigt wird, können Sie den Cursor in das Feld setzen, dann klicken und halten und rollen Sie die Maus nach rechts oder links, um den abgeschnittenen Teil zu sehen.

- **Virtuelle Schnittstelle** —Die virtuelle Schnittstelle, die von dieser Access Interface verwendet wird. Wählen Sie einen Eintrag aus dem Dropdownmenü der Virtuellen Schnittstellen aus, die für diesen Zweigstandort konfiguriert sind.
- **IP-Adresse** —Die IP-Adresse für den Access Interface Endpunkt von der Appliance zum WAN.
- **Gateway IP-Adresse** - Dies ist die IP-Adresse für den Gateway-Router.
- **Virtueller Pfadmodus** —Die Priorität für den virtuellen Pfadverkehr auf dieser WAN-Verbindung. Die Optionen sind: **Primär**, **Sekundär** oder **Ausschließen**. Wenn diese Zugriffsoberfläche auf **Ausschließen** festgelegt ist, wird diese Zugriffsoberfläche nur für den Internet- und Intranetverkehr verwendet.
- **Proxy ARP** —Aktivieren Sie das Kontrollkästchen, das aktiviert werden soll. Wenn diese Option aktiviert ist, antwortet die Virtual WAN Appliance auf ARP-Anforderungen für die Gateway-IP-Adresse, wenn das Gateway nicht erreichbar ist.

18. Klicken Sie auf **Übernehmen**.

Sie haben nun die Konfiguration der neuen WAN-Verbindung abgeschlossen. Wiederholen Sie diese Schritte, um zusätzliche WAN-Links für die Site hinzuzufügen und zu konfigurieren.

Der nächste Schritt besteht darin, die Routen für die Site hinzuzufügen und zu konfigurieren.

So konfigurieren Sie Routen für den Zweig

Gehen Sie folgendermaßen vor, um die Routen für die Site hinzuzufügen und zu konfigurieren:

1. Klicken Sie auf die Ansicht **Verbindungen** für den neuen Zweigstandort, und wählen Sie **Routen** aus. Dadurch wird die **Routenansicht** für die Site angezeigt.
2. Klicken Sie rechts neben **Routen** auf **+**, um eine Route hinzuzufügen. Daraufhin wird das Dialogfeld **Routen** zur Bearbeitung geöffnet.

The screenshot shows a dialog box titled "Add" with the following fields and options:

- Network IP Address:** A text input field with a red asterisk indicating it is required.
- Cost:** A text input field containing the value "5".
- Service Type:** A dropdown menu currently showing "Local".
- Gateway IP Address:** A text input field with a red asterisk indicating it is required.
- Export Route:** A checked checkbox.
- Summary Route:** An unchecked checkbox.
- Eligibility Based On Path:** An unchecked checkbox.
- Path:** A dropdown menu currently showing "<None>".
- Eligibility Based On Gateway:** An unchecked checkbox.
- Buttons:** "Add" and "Cancel" buttons at the bottom right.

3. Geben Sie die Routenkonfigurationsinformationen für die neue Route ein.

- **Netzwerk-IP-Adresse** —Geben Sie die Netzwerk-IP-Adresse ein.
- **Kosten** —Geben Sie ein Gewicht zwischen 1 und 15 ein, um die Routenpriorität für diese Route zu bestimmen. Lower-Cost-Routen haben Vorrang vor höheren Kosten Routen. Der Standardwert ist 5.
- **Servicetyp** —Wählen Sie den Servicetyp für die Route aus dem Dropdownmenü für dieses Feld aus. Die folgenden Optionen stehen zur Auswahl:
 - **Virtueller Pfad** —Dieser Dienst verwaltet den Datenverkehr über die virtuellen Pfade. Ein virtueller Pfad ist eine logische Verbindung zwischen zwei WAN-Verbindungen. Es umfasst eine Sammlung von WAN-Pfaden, die kombiniert werden, um eine hohe Service-Level-Kommunikation zwischen zwei SD-WAN-Knoten zu ermöglichen. Dies geschieht durch ständige Messung und Anpassung an veränderte Anwendungsanforderungen und WAN-Bedingungen. SD-WAN-Appliances messen das Netzwerk

pro Pfad. Ein virtueller Pfad kann statisch (immer vorhanden) oder dynamisch sein (nur vorhanden, wenn der Datenverkehr zwischen zwei SD-WAN-Appliances einen konfigurierten Schwellenwert erreicht).

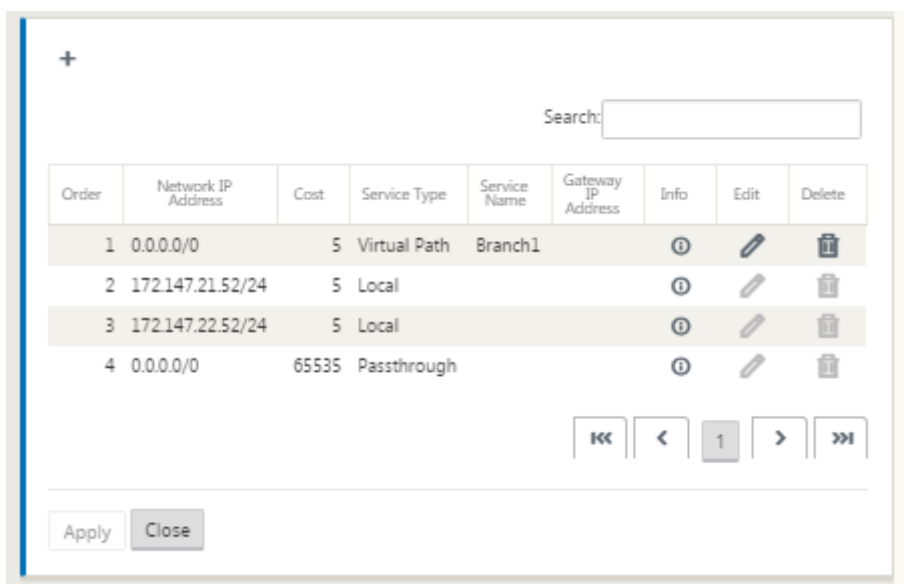
- **Internet** —Dieser Dienst verwaltet den Datenverkehr zwischen einem Enterprise-Standort und Websites im öffentlichen Internet. Datenverkehr dieses Typs ist nicht gekapselt. In Zeiten der Überlastung verwaltet das SD-WAN aktiv die Bandbreite, indem es den Internetverkehr relativ zum virtuellen Pfad einschränkt, und den Intranetverkehr entsprechend der vom Administrator festgelegten SD-WAN-Konfiguration begrenzt.
- **Intranet** —Dieser Dienst verwaltet Enterprise-Intranet-Datenverkehr, der nicht für die Übertragung über einen virtuellen Pfad definiert wurde. Wie beim Internetverkehr bleibt er ungekapselt, und das SD-WAN verwaltet die Bandbreite, indem dieser Datenverkehr im Verhältnis zu anderen Diensttypen während der Staus begrenzt wird. Unter bestimmten Bedingungen und wenn für Intranet-Fallback auf dem virtuellen Pfad konfiguriert ist, kann Datenverkehr, der normalerweise mit einem virtuellen Pfad reist, stattdessen als Intranetdatenverkehr behandelt werden, um die Netzwerkzuverlässigkeit aufrechtzuerhalten.
- **Passthrough** —Dieser Dienst verwaltet den Datenverkehr, der über das virtuelle WAN übergeben werden soll. Der an den Passthrough-Dienst gerichtete Datenverkehr umfasst Broadcasts, ARPs und anderen Nicht-IPv4-Datenverkehr sowie Datenverkehr im lokalen Subnetz der Virtual WAN Appliance, konfigurierten Subnetzen oder vom Netzwerkadministrator angewendete Regeln. Dieser Datenverkehr wird vom SD-WAN nicht verzögert, geformt oder geändert. Daher müssen Sie sicherstellen, dass Passthrough-Datenverkehr keine erheblichen Ressourcen auf den WAN-Verbindungen verbraucht, die die SD-WAN-Appliance für andere Dienste konfiguriert ist.
- **Lokal** —Dieser Dienst verwaltet den lokalen IP-Datenverkehr auf der Website, der keinem anderen Dienst entspricht. SD-WAN ignoriert Datenverkehr, der für eine lokale Route bestimmt ist.
- **GRE-Tunnel** —Dieser Dienst verwaltet den IP-Datenverkehr, der für einen GRE-Tunnel bestimmt ist, und stimmt mit dem am Standort konfigurierten LAN-GRE-Tunnel überein. Mit der Funktion GRE Tunnel können Sie SD-WAN Appliances so konfigurieren, dass GRE Tunnel im LAN beendet werden. Bei einer Route mit Servicetyp GRE Tunnel muss sich das Gateway in einem der Tunnelsubnetze des lokalen GRE Tunnels befinden.
- **LAN IPsec-Tunnel** —Dieser Dienst verwaltet den IP-Datenverkehr, der für den IPsec-Tunnel bestimmt ist.

- **Inter-Routing** - Dieser Service ermöglicht das Leck von Routen zwischen Routing-domänen innerhalb einer Site oder zwischen verschiedenen Standorten. Dadurch entfällt die Notwendigkeit, dass ein Edgerouter Routeleaking verarbeitet.
- **Gateway IP Address** —Geben Sie die Gateway-IP-Adresse für diese Route ein.
- **Berechtigung basierend auf Pfad** (Kontrollkästchen) —(Optional) Wenn diese Option aktiviert ist, erhält die Route keinen Datenverkehr, wenn der ausgewählte Pfad ausgefallen ist.
- **Pfad** —Dies gibt den Pfad an, der zum Bestimmen der Routenberechtigung verwendet werden soll.

4. Klicken Sie auf **Übernehmen**.

Hinweis

Nachdem Sie auf **Übernehmen** geklickt haben, werden möglicherweise Überwachungswarnungen angezeigt, die darauf hinweisen, dass weitere Maßnahmen erforderlich sind. Ein Rotpunkt- oder Goldrute-Delta-Symbol weist auf einen Fehler in dem Abschnitt hin, in dem es angezeigt wird. Sie können diese Warnungen verwenden, um Fehler oder fehlende Konfigurationsinformationen zu identifizieren. Bewegen Sie den Mauszeiger über ein Überwachungswarnsymbol, um eine kurze Beschreibung der Fehler in diesem Abschnitt anzuzeigen. Sie können auch auf die dunkelgraue Statusleiste für **Audits** (unten auf der Seite) klicken, um eine vollständige Liste aller Überwachungswarnungen anzuzeigen.



Sie können auch konfigurierte Routen bearbeiten, wie unten gezeigt.

Edit ? x

Network IP Address: 172.147.61.0/24 Cost: 5 Service Type: Intranet Gateway IP Address:

☐ Export Route

Intranet Service: Intranet

☒ Eligibility Based On Path

Path: Branch1-WL-2->MCN-DC-WL-1

☐ Eligibility Based On Tunnel

Apply Cancel

Sie haben nun die erforderlichen Schritte zum Konfigurieren eines Clientstandorts abgeschlossen. Es gibt auch einige zusätzliche, optionale Schritte, die Sie ausführen können, bevor Sie mit der nächsten Phase der Bereitstellung fortfahren. Eine Liste dieser Schritte und Links zu Anweisungen finden Sie unten. Wenn Sie diese Funktionen jetzt nicht konfigurieren möchten, können Sie [direkt mit \(/en-us/citrix-sd-wan/11-2/configuration/installing-virtual-wan-appliance-packages-clients.html\)](/en-us/citrix-sd-wan/11-2/configuration/installing-virtual-wan-appliance-packages-clients.html)

Die optionalen Schritte sind wie folgt:

- **High Availability konfigurieren** —High Availability ist eine Konfiguration, bei der zwei Virtual WAN Appliances an einem Standort in einer Active/Standby-Partnerschaftskapazität für Redundanzzwecke bereitgestellt werden. Wenn Sie Hochverfügbarkeit für diese Website nicht implementieren, können Sie diesen Schritt überspringen. Anweisungen finden Sie unter [Konfigurieren von Hochverfügbarkeit \(hohe Verfügbarkeit\) für den Zweigstandort \(optional\)](#).
- **Klonen des neuen Zweigstandorts** —Sie haben die Möglichkeit, den von Ihnen konfigurierten Zweigstandort zu klonen und diese als Vorlage zum Hinzufügen einer anderen Site zu verwenden. Die Appliance-Modelle für die Original-Site und den Klon müssen identisch sein. Anweisungen finden Sie unter [Klonen des Zweigstandorts \(optional\)](#).
- **Konfigurieren der WAN-Optimierung** —Wenn Ihre Citrix SD-WAN Virtual WAN-Lizenz WAN-Optimierungsfunktionen enthält, können Sie diese Funktionen aktivieren und Ihrer Konfiguration hinzufügen. Dazu müssen Sie den Abschnitt **Optimierung** im **Konfigurations-Editor** ausfüllen und die geänderte Konfiguration speichern.

Konfiguration speichern

Der nächste Schritt besteht darin, die abgeschlossene Sites Konfiguration zu speichern. Die Konfiguration wird in Ihrem Workspace auf der lokalen Appliance gespeichert.

Warnung

Wenn die Konsolensitzung ein Timeout oder Sie sich vor dem Speichern der Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten Konfigurationsänderungen verloren. Sie müssen sich dann wieder beim System anmelden und den Konfigurationsvorgang von Anfang an wiederholen. Aus diesem Grund wird empfohlen, das Konfigurationspaket häufig oder an Schlüsselpunkten in der Konfiguration zu speichern.

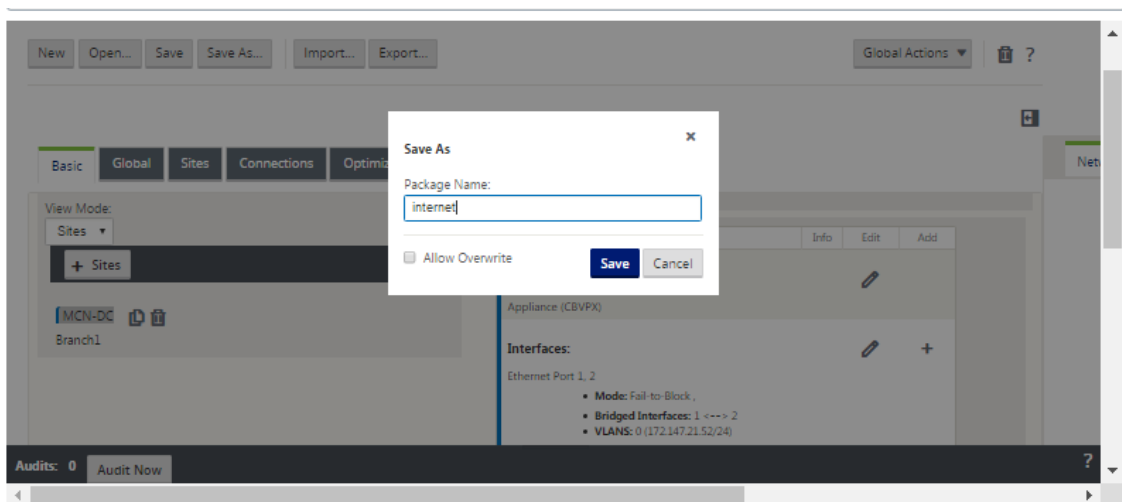
Hinweis

Als zusätzliche Vorsichtsmaßnahme wird empfohlen, dass Sie Speichern unter anstelle von Speichern verwenden, um ein Überschreiben des falschen Konfigurationspakets zu vermeiden.

Nach dem Speichern der Konfigurationsdatei haben Sie die Möglichkeit, sich vom Management Web Interface abzumelden und den Konfigurationsvorgang später fortzusetzen. Wenn Sie sich jedoch abmelden, müssen Sie die gespeicherte Konfiguration erneut öffnen, wenn Sie fortfahren. Anweisungen finden Sie im Abschnitt unter **MCN konfigurieren**; [Laden eines gespeicherten Konfigurationspakets in den Konfigurations-Editor](#).

Gehen Sie folgendermaßen vor, um das aktuelle Konfigurationspaket zu speichern:

1. Klicken Sie auf **Speichern unter** (oben im mittleren Bereich des **Konfigurations-Editors**). Dadurch wird das Dialogfeld **Speichern unter** geöffnet.



2. Geben Sie den Namen des Konfigurationspakets ein. Klicken Sie auf **Speichern**.

Hinweis

Wenn Sie die Konfiguration in einem vorhandenen Konfigurationspaket speichern, müssen Sie vor dem Speichern die Option **Überschreiben zulassen** auswählen.

Der nächste Schritt besteht darin, die virtuellen Pfade und den Virtual Path Service zwischen dem MCN und den Client-Sites zu konfigurieren. Anweisungen finden Sie in der [Konfigurieren des Virtual Path Service zwischen MCN und Client-Sites](#).

Zweigstandort umbenennen

Nachdem Sie den Zweigstandort umbenannt haben, müssen Sie ein neues Konfigurationspaket in das Netzwerk hochladen.

1. Stationieren Sie im MCN das Netzwerk mit einer neuen Konfiguration, die den umbenannten Zweigstandort enthält.
2. Laden Sie das Stagingpaket für den umbenannten Zweigstandort herunter.
3. Wählen Sie im **MCN** die Option **Staged network aktivieren** aus. Dadurch wird die umbenannte Site deaktiviert, und die Site wird nicht mehr verfügbar.
4. Navigieren Sie zur Seite **Lokale Änderungsverwaltung**.
5. Laden Sie das zuvor heruntergeladene Paket hoch. Klicken Sie auf **Weiter** und dann auf **Aktivieren**.

Umbenennen von Zweigstandort mit hoher Verfügbarkeit

So laden Sie eine neue Konfiguration hoch, nachdem Sie einen Zweigstandort umbenannt haben, der mit hoher Verfügbarkeit aktiviert ist:

1. Stationieren Sie im MCN das Netzwerk mit einer neuen Konfiguration, die den umbenannten Zweigstandort enthält.
2. Laden Sie das Stagingpaket für die aktive und hochverfügbare Appliance mit umbenannten Zweigstandort herunter.
3. Wählen Sie im **MCN** die Option **Staged for network aktivieren** aus. Dadurch wird die umbenannte Site deaktiviert, und die Site wird nicht mehr verfügbar.
4. Navigieren Sie zur aktiven Appliance in der Zweigstelle. Rufen Sie die Seite **Local Change Management** auf.
5. Laden Sie das zuvor heruntergeladene Paket hoch. Klicken Sie auf **Weiter** und dann auf **Aktivieren**.

6. Wiederholen Sie die Schritte 4 (a) und 4 (b) für die Standby-Appliance.

Klonen eines Zweigstandorts (optional)

May 10, 2021

Dieser Abschnitt enthält Anweisungen zum Klonen des neuen Zweigstandorts zur Verwendung als Teilverlage zum Hinzufügen weiterer Zweigstandorte.

Hinweis

Das Klonen der Site ist optional. Die Virtual WAN-Appliance-Modelle müssen sowohl für die ursprüngliche als auch für die geklonten Sites identisch sein. Sie können das angegebene Einheitenmodell für einen Klon nicht ändern. Wenn sich das Appliance-Modell für einen Standort unterscheidet, müssen Sie die Site manuell hinzufügen, wie in den vorherigen Abschnitten beschrieben.

Das Klonen einer Site vereinfacht das Hinzufügen und Konfigurieren weiterer Zweigknoten. Wenn eine Site geklont wird, werden die gesamten Konfigurationseinstellungen für die Site kopiert und auf einer einzigen Formularseite angezeigt. Anschließend können Sie die Einstellungen entsprechend den Anforderungen der neuen Website ändern. Einige der ursprünglichen Einstellungen können ggf. beibehalten werden. Die meisten Einstellungen müssen jedoch für jede Site eindeutig sein.

Gehen Sie folgendermaßen vor, um eine Site zu klonen:

1. Klicken Sie in der **Sitestruktur** (mittlerer Bereich) des **Konfigurations-Editors** auf den Zweigstandort, den Sie duplizieren möchten.

Dadurch wird der Standortzweig in der **Sitestruktur** geöffnet und die Schaltfläche **Klonen** (Doppelseitiges Symbol) und Löschen (Papierkorb) angezeigt.

2. Klicken Sie auf das Symbol **Klonen** rechts neben dem Namen der Zweigstelle in der Struktur.

Dadurch wird die Seite Konfiguration **der Website klonen** geöffnet.

Clone

Please review the following fields and make the appropriate changes for the new Site.

Site Name: BR1 ! Appliance Name: Appliance Mode: client Secure Key: ada97484370f0d1 Region: r1

Routing Domains

| Name | Enable | Default |
|-----------------------|-------------------------------------|-------------------------------------|
| Default_RoutingDomain | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Virtual Interfaces

| Name | VLAN ID | DHCP |
|--------------------|---------|--------------------------|
| VirtualInterface-1 | 0 | <input type="checkbox"/> |
| VirtualInterface-2 | 0 | <input type="checkbox"/> |

Virtual IP Addresses

| Include | Virtual Interface | Virtual IP Address/Prefix |
|-------------------------------------|--------------------|---|
| <input checked="" type="checkbox"/> | VirtualInterface-1 | 172.110.0.5/24 ! |
| <input checked="" type="checkbox"/> | VirtualInterface-2 | 192.110.0.5/24 ! |

Local Routes

Include Network Address Routing Domain Gateway

WAN Links

| Include Link | WAN Link | Access Type |
|-------------------------------------|---|-------------|
| <input checked="" type="checkbox"/> | BR1-WL-1 ! | |

Access Interfaces

| Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway |
|-------------------------------------|------------------|--------------------|--|--|
| <input checked="" type="checkbox"/> | BR1-WL-1-AI-1 | VirtualInterface-1 | 172.110.0.5 ! | 172.110.0.1 ! |

BR1-WL-2 !

Access Interfaces

| Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway |
|-------------------------------------|------------------|--------------------|--|--|
| <input checked="" type="checkbox"/> | BR1-WL-2-AI-1 | VirtualInterface-2 | 192.110.0.5 ! | 192.110.0.1 ! |

GRE Tunnels

Include Name Source IP Destination IP Tunnel IP / Prefix

- Geben Sie die Konfigurationsparametereinstellungen für den neuen Standort ein.

Ein rosafarbenes Feld mit einem Symbol für die Überwachungswarnung (roter Punkt) weist auf eine erforderliche Parametereinstellung hin, die einen anderen Wert als die Einstellung für die ursprüngliche geklonte Site aufweisen muss. Normalerweise muss dieser Wert eindeutig sein.

Tipp

Um den Klonvorgang weiter zu optimieren, verwenden Sie beim Benennen der Klonen eine konsistente, vordefinierte Benennungskonvention.

- Lösen Sie alle Überwachungswarnungen.

Um einen Fehler zu diagnostizieren, drehen Sie den Cursor über das Symbol **Audit Alert** (roter Punkt oder Goldrod Delta), um die Hilfe der Blase für diese bestimmte Warnung anzuzeigen.

- Klicken Sie auf **Klonen** (ganz rechts), um die Site zu erstellen und der Tabelle **Sites** hinzuzufügen.

Hinweis

Die Schaltfläche **Klonen** bleibt nicht verfügbar, bis Sie alle erforderlichen Werte eingegeben haben und die neue Standortkonfiguration fehlerfrei ist.

6. (Optional.) Speichern Sie Ihre Änderungen an der Konfiguration.

Hinweis

Als zusätzliche Vorsichtsmaßnahme wird empfohlen, dass Sie **Speichern unter** anstelle von **Speichern** verwenden, um ein **Überschreiben des falschen Konfigurationspakets zu vermeiden**. Stellen Sie sicher, dass Sie **Überschreiben zulassen auswählen, bevor Sie** in einer vorhandenen Konfiguration speichern, oder Ihre Änderungen werden nicht gespeichert.

Wiederholen Sie die Schritte bis zu diesem Punkt für jeden Zweigstandort, den Sie hinzufügen möchten.

Nachdem Sie alle Sites hinzugefügt haben, überprüfen Sie im nächsten Schritt die Konfiguration für Überwachungswarnungen und nehmen ggf. Korrekturen oder Ergänzungen vor.

Überwachung der Zweigkonfiguration

May 10, 2021

Ein Audit-Alert-Symbol (ein roter Punkt oder ein Goldrute-Delta) neben einem Element weist auf einen Konfigurationsfehler oder fehlende Parameterinformationen für dieses Element hin. Eine Zahl neben dem Symbol gibt die Anzahl der zugeordneten Fehler für diese Warnung an. Wenn Sie die Hilfe für eine bestimmte Warnung anzeigen möchten, drehen Sie den Cursor über das Warnsymbol. Dies zeigt eine kurze Beschreibung der spezifischen Fehler an, die von dieser Warnung gekennzeichnet sind. Sie müssen alle Überwachungswarnungen in der Konfiguration auflösen, sonst können Sie das Konfigurationspaket später im Bereitstellungsprozess nicht überprüfen, bereitstellen und aktivieren.

Wenn Sie alle Überwachungswarnungen (falls vorhanden) lösen, wird die **Sites** Phase der Konfiguration abgeschlossen. Der nächste Schritt besteht darin, die abgeschlossene **Sites** Konfiguration zu speichern.

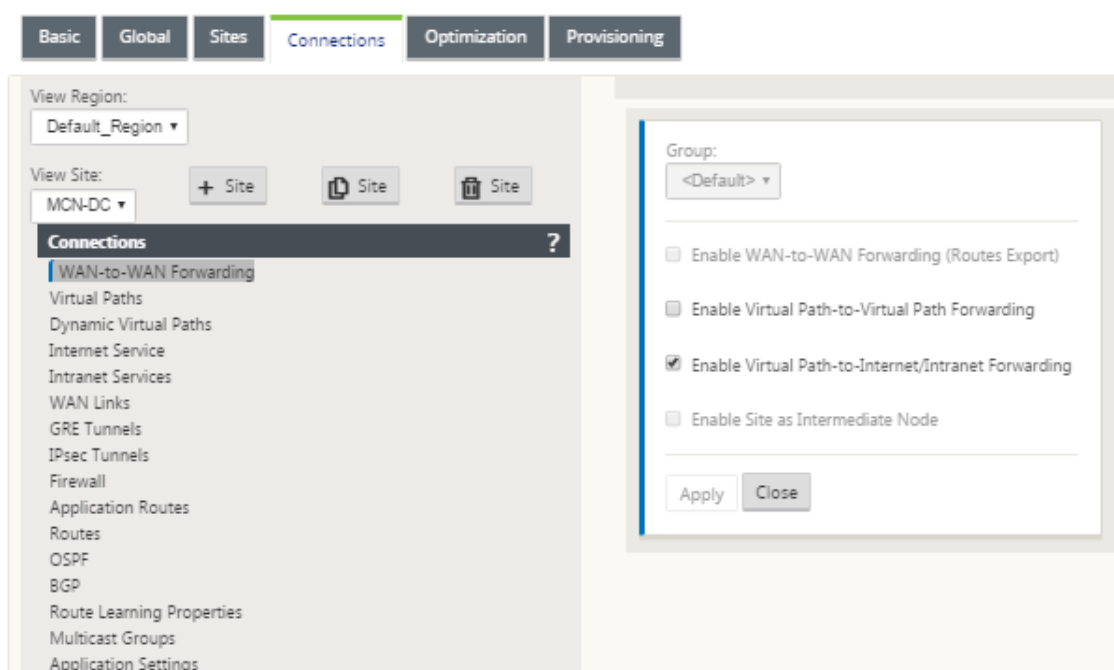
Konfigurieren des virtuellen Pfaddienstes zwischen MCN und Clientsites

May 10, 2021

Der nächste Schritt besteht darin, den Virtual Path Service zwischen dem MCN und jedem der Client-Sites (Zweigstellen) zu konfigurieren. Dazu verwenden Sie die Konfigurationsformulare und -einstellungen, die im Konfigurationsbaum des **Konfigurationseditors** im Abschnitt **Verbindungen** verfügbar sind.

Gehen Sie folgendermaßen vor, um den Virtual Path Service zwischen dem MCN und einem Clientstandort zu konfigurieren:

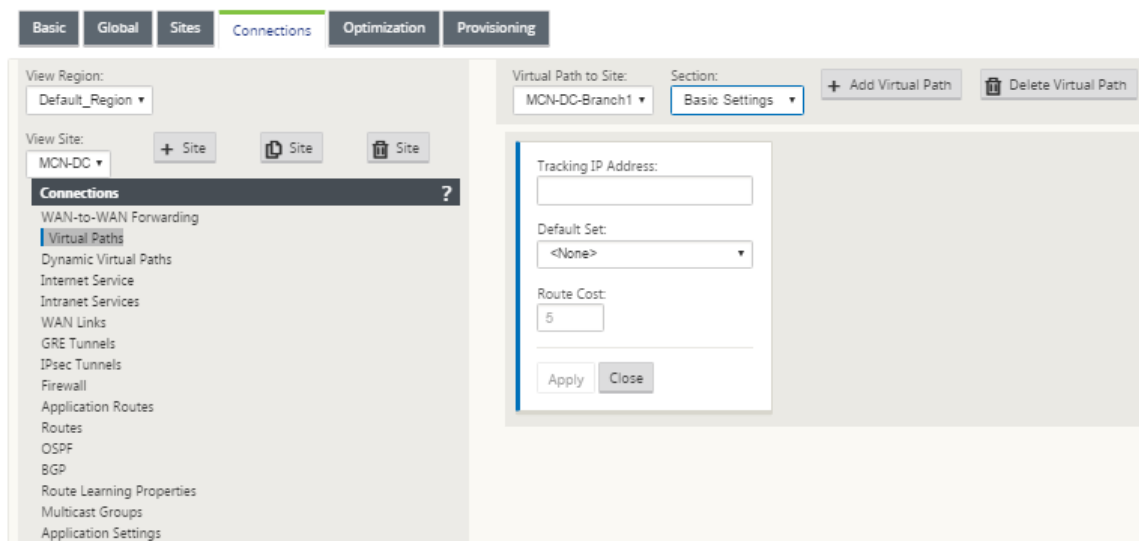
1. Klicken Sie im **Konfigurations-Editor** auf die Registerkarte **Verbindungen**. Daraufhin wird die Konfigurationsstruktur des Abschnitts **Verbindungen** angezeigt.
2. Wählen Sie auf der Abschnittseite **Verbindungen** das Dropdownmenü **MCN** aus **Ansicht Site** aus. Dadurch wird der MCN-Standort in der **Verbindungskonfiguration** geöffnet.



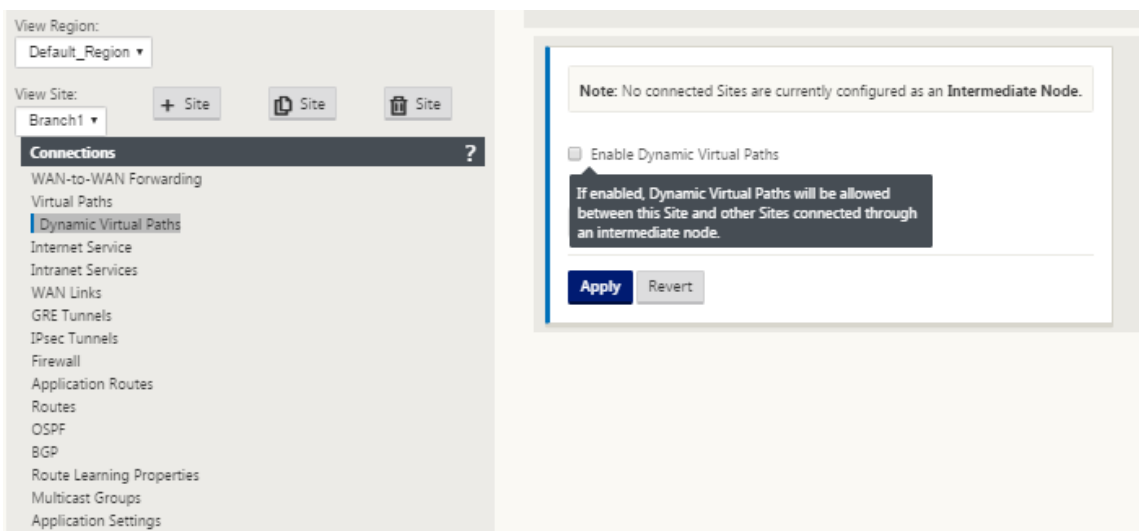
Hinweis

WAN-zu-WAN-Weiterleitungsgruppen werden nur innerhalb einer Region und nicht über Regionen hinweg unterstützt. Sie können Regionen verwenden, um Netzwerke zu trennen, anstatt sich auf WAN zu WAN-Weiterleitungsgruppen zu verlassen.

3. Klicken Sie auf **Virtuelle Pfade**. Dadurch wird der **Konfigurationsabschnitt für virtuelle Pfade** (untergeordneter Zweig) für den MCN-Site geöffnet. Dieser Abschnitt enthält Einstellungen und Formulare zum Konfigurieren des Virtual Path Service zwischen dem MCN und jedem Virtual WAN-Clientstandort. Die folgende Abbildung zeigt einen Beispielabschnitt für virtuelle Pfade für eine MCN-Site.



Die folgende Abbildung zeigt einen Beispielabschnitt für **dynamische virtuelle Pfade** für einen Zweigstandort.



Im Abschnitt **Dynamische virtuelle Pfade** können Sie Folgendes konfigurieren:

- **Dynamische virtuelle Pfade** —(Optional) Mit den Einstellungen in diesem Abschnitt können Sie dynamische virtuelle Pfade aktivieren und deaktivieren und die maximal zulässigen dynamischen virtuellen Pfade für die Site festlegen. Dynamische virtuelle Pfade sind virtuelle Pfade, die direkt zwischen Standorten basierend auf einem konfigurierten Schwellenwert eingerichtet werden. Der Schwellenwert basiert in der Regel auf dem Umfang des Datenverkehrs zwischen diesen Websites. Dynamische virtuelle Pfade sind erst nach Erreichen des angegebenen Schwellenwerts betriebsbereit. Dynamische virtuelle Pfade sind für den normalen Betrieb nicht erforderlich, daher ist die Konfiguration dieses Abschnitts optional.
- **<MCN_Site_Name>_<Branch_Site_Name>** –Das System fügt zunächst automatisch

einen statischen virtuellen Pfad zwischen dem MCN und einer Client-Site hinzu, da dieser virtuelle Pfad erforderlich ist. Der Name für den Pfad verwendet das folgende Formular:

<MCN_Site_Name>_<Branch_Site_Name>

Dabei gilt Folgendes:

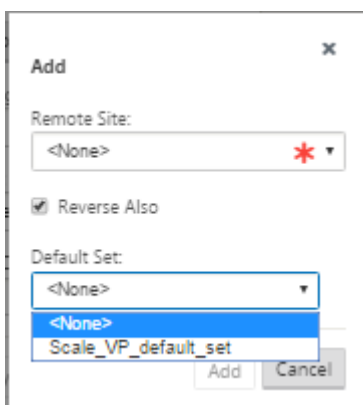
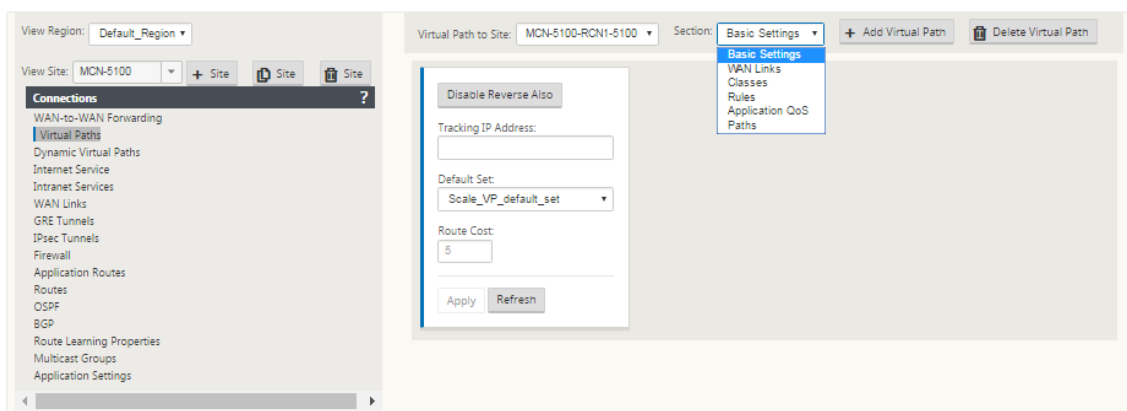
MCN_Site_Name ist der Name des MCN für dieses virtuelle WAN.

Branch_Site_Name ist der Name eines Clientstandorts, der im aktuellen Konfigurationspaket identifiziert wird.

Benutzerkonfigurierbare Standardeinstellungen werden zunächst auf den statischen virtuellen Pfad angewendet, wie im Abschnitt **Virtueller Pfad > Standardsätze** der Konfigurationsstruktur **Verbindungen** definiert. Sie können jedoch die definierten **Standardsätze** anpassen oder hinzufügen und die Konfiguration für einen bestimmten Standort und einen virtuellen Pfad anpassen.

Hinweis

Um weitere statische virtuelle Pfade für eine Site hinzuzufügen, müssen Sie dies manuell tun. Anweisungen zum manuellen Hinzufügen eines statischen virtuellen Pfads finden Sie in den Schritten wie folgt.

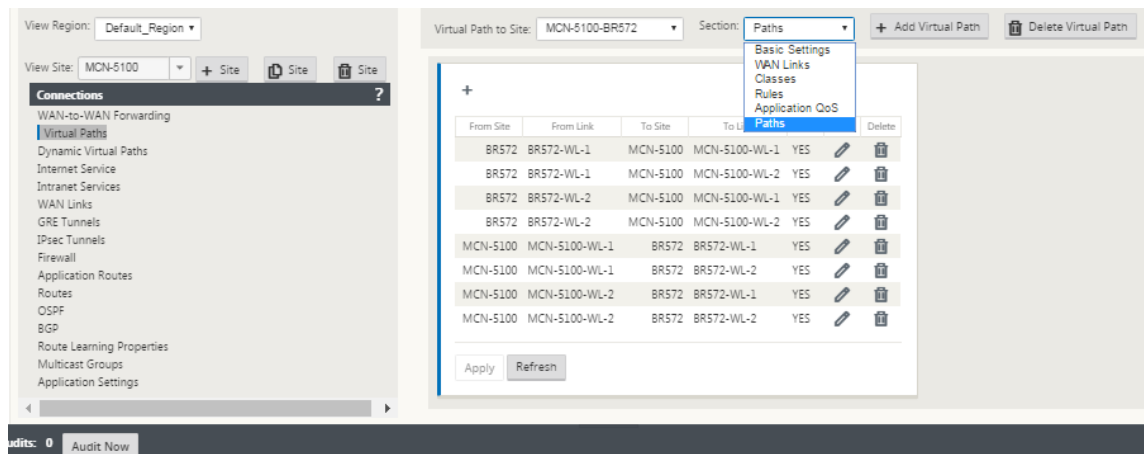


4. Klicken Sie im Abschnitt **Virtuelle Pfade** neben dem Namen des statischen virtuellen Pfads auf **+ Virtuellen Pfad hinzufügen**. Dies zeigt mehr Konfiguration für den statischen virtuellen Pfad:

- a) **Remote-Site** —In diesem Abschnitt können Sie die Einstellungen für den **virtuellen Pfad** aus der Perspektive einer Remote-Site anzeigen und konfigurieren. Sie können **Klassen** oder **Regeln** nach Bedarf für diesen bestimmten virtuellen Pfad anzeigen, anpassen und hinzufügen. Sie können bei Bedarf auch virtuelle Pfade zur Remote-Site hinzufügen.
- b) **Reverse Also**- Wenn aktiviert, werden Klassen und Regeln auf beiden Sites der virtuelle Pfad gespiegelt.
- c) **Standardsatz** - Name des Standardsatzes für den virtuellen Pfad, der zum Auffüllen von Regeln und Klassen für den virtuellen Pfad auf der Site verwendet wird.

Die folgende Abbildung zeigt ein Beispiel für statische MCN-Zweige mit Virtual Path und untergeordnete Zweige.

5. Wählen Sie **Pfade** aus dem Dropdownmenü **Abschnitt**.



6. Klicken Sie oberhalb der Tabelle **Pfade** auf **+** (Hinzufügen).

Daraufhin wird das Dialogfeld **Pfad hinzufügen** (Konfigurationsformular) angezeigt.

Add Path [X]

From Site: MCN_DC-01_K ▼

From WAN Link: MCN_DC-01_K ▼

To Site: BR-01_K

To WAN Link: BR-01_K-WL-1 ▼

☒ Reverse Also

Add Cancel

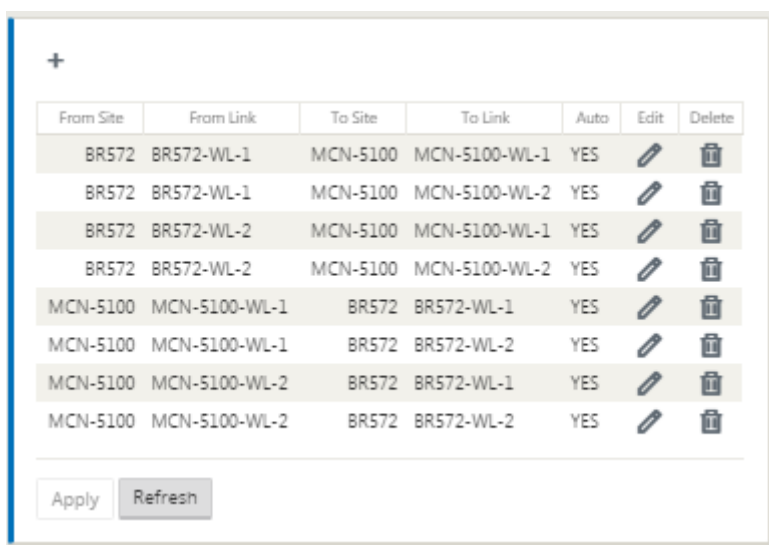
7. Geben Sie die Quell- und Zielstandortinformationen für den neuen virtuellen Pfad an.
8. Geben Sie in den verfügbaren Dropdownmenüs Folgendes an:

Hinweis

Je nachdem, wie die WAN-Links für die Sites konfiguriert sind, sind einige Felder schreibgeschützt. Felder, die konfigurierbar sind, stellen ein Dropdownmenü der verfügbaren Auswahlen bereit.

- **Von Site** —Dies ist die Quellsite für den virtuellen Pfad. Für den erforderlichen statischen virtuellen Pfad wird dieser standardmäßig als MCN-Site konfiguriert.
 - **Von WAN-Link** —Dies ist der ursprüngliche WAN-Link für den virtuellen Pfad.
 - **An Site** —Dies ist die Zielsite für den virtuellen Pfad.
 - **Zu WAN-Link** —Dies ist der Ziel-WAN-Link für den virtuellen Pfad.
9. Klicken Sie auf **Hinzufügen**.

Dadurch wird der konfigurierte virtuelle Pfad sowohl dem MCN als auch dem zugehörigen Clientstandort in der Struktur **Verbindungen > Virtuelle Pfade** hinzugefügt. Dadurch wird auch automatisch das Konfigurationsformular **Pfadeinstellungen** für die **Von Site** für den virtuellen Pfad geöffnet (in diesem Fall der MCN).



| From Site | From Link | To Site | To Link | Auto | Edit | Delete |
|-----------|---------------|----------|---------------|------|------|--------|
| BR572 | BR572-WL-1 | MCN-5100 | MCN-5100-WL-1 | YES | | |
| BR572 | BR572-WL-1 | MCN-5100 | MCN-5100-WL-2 | YES | | |
| BR572 | BR572-WL-2 | MCN-5100 | MCN-5100-WL-1 | YES | | |
| BR572 | BR572-WL-2 | MCN-5100 | MCN-5100-WL-2 | YES | | |
| MCN-5100 | MCN-5100-WL-1 | BR572 | BR572-WL-1 | YES | | |
| MCN-5100 | MCN-5100-WL-1 | BR572 | BR572-WL-2 | YES | | |
| MCN-5100 | MCN-5100-WL-2 | BR572 | BR572-WL-1 | YES | | |
| MCN-5100 | MCN-5100-WL-2 | BR572 | BR572-WL-2 | YES | | |

Apply Refresh

10. Klicken Sie auf Bearbeiten (Bleistiftsymbol) rechts neben der Bezeichnung MCN-to-Client Virtual Path. Dadurch wird das Konfigurationsformular für den Virtual Path Service zur Bearbeitung geöffnet.
11. Konfigurieren Sie die Einstellungen für den virtuellen Pfad, oder übernehmen Sie die Standardeinstellungen.

Das Konfigurationsformular **Pfade** enthält die folgenden Einstellungen:

- Abschnitt **Von Site** :
 - **Site** —Dies ist die Quellsite für den virtuellen Pfad. Für den erforderlichen statischen virtuellen Pfad wird dieser standardmäßig als MCN-Site konfiguriert.
 - **WAN-Link** —Dies ist der ursprüngliche WAN-Link für den virtuellen Pfad.
- Abschnitt **Zu Site** :
 - **Site** —Dies ist die Ziel-Site für den virtuellen Pfad.
 - **WAN-Link** —Dies ist der Ziel-WAN-Link für den virtuellen Pfad.
- **Reverse Auch** - Aktivieren Sie dieses Kontrollkästchen, um Reverse Auch für diesen virtuellen Pfad zu aktivieren. Wenn diese Option aktiviert ist, erstellt das System automatisch einen virtuellen Pfad in der entgegengesetzten Richtung des konfigurierten Pfades, wobei dieselben WAN-Verbindungen verwendet werden, die für den ursprünglichen Pfad konfiguriert sind.
- **IP DSCP Tagging** —Wählen Sie ein Tag aus dem Dropdownmenü aus. Dies gibt das DSCP-Tag an, das im IP-Header für Datenverkehr über diesen virtuellen Pfad festgelegt wird.
- **Verschlüsselung aktivieren** —Aktivieren Sie dieses Kontrollkästchen, um die Verschlüsselung von Paketen zu aktivieren, die entlang dieses virtuellen Pfades gesendet werden.

- **Fehlerhafte Verluste** —Wählen Sie eine Einstellung aus dem Dropdownmenü aus. Es gibt folgende Optionen:

- **Aktivieren**—(Standard) Wenn diese Option aktiviert ist, werden **Pfade aufgrund eines Verlustes als BAD** gekennzeichnet, und es wird eine Pfadbewertungsstrafe verursacht.
- **Deaktivieren** —Die Deaktivierung von **Schadverlusten** kann nützlich sein, wenn der Bandbreitenverlust unerträglich ist.
- **Benutzerdefiniert** —Wählen Sie Benutzerdefiniert aus, um den Prozentsatz des Verlustes im Laufe der Zeit anzugeben, der erforderlich ist, um einen Pfad als BAD zu markieren. Wenn Sie diese Option auswählen, werden die folgenden weiteren Einstellungen angezeigt:
 - ★ **Prozentsatz Verlust (%)** —Dieser Wert gibt den Prozentsatz der Verlustschwelle an, bevor ein Pfad als BAD markiert wird, wie er über die angegebene Zeit gemessen wird. Standardmäßig basiert der Prozentsatz auf den letzten 200 empfangenen Paketen.
 - ★ **Über Zeit (ms)** —Geben Sie den Zeitraum (in Millisekunden) an, über den der Paketverlust gemessen werden soll. Wählen Sie im Dropdownmenü für dieses Feld eine Option zwischen 100 und 2000 aus.
- **Silence Period (ms)** —Gibt die Dauer (in Millisekunden) an, bevor der Pfadzustand von **GOOD** nach **BAD** übergeht.

Der Standardwert ist 150 Millisekunden. Wählen Sie im Dropdownmenü für dieses Feld eine Option zwischen 150 und 1000 aus.

- **Path Probation Period (ms)** —Dies gibt die Wartezeit (in Millisekunden) an, bevor ein Pfad von BAD zu GOOD übergeht. Wählen Sie im Dropdownmenü für dieses Feld eine Option zwischen 500 und 60000 aus. Der Standardwert ist 10.000 Millisekunden.
- **Instabilitätssensitiv** —Aktivieren Sie dieses Kontrollkästchen, um es zu aktivieren. Wenn diese Option aktiviert ist, werden Latenzstrafen aufgrund eines Pfadzustands **BAD** und anderer Latenzspitzen im Pfadauswertungsalgorithmus berücksichtigt.
- **IP-Adresse verfolgen** —Geben Sie im virtuellen Pfad eine virtuelle IP-Adresse ein, die angepingt werden kann, um den Status des Pfads zu bestimmen.
- **Reverse Tracking IP-Adresse** —Wenn **Reverse Auch** für den virtuellen Pfad aktiviert ist, geben Sie eine virtuelle IP-Adresse für den Pfad ein, der angepingt werden kann, um den Status des umgekehrten Pfads zu bestimmen.

12. Klicken Sie auf **Übernehmen**. Dies zeigt, dass die beiden neuen virtuellen Pfade **Von Standort** und **Zu Standort** zwischen MCN und Client-Site der Tabelle Pfade hinzugefügt wurden.

Edit [X]

Convert to Static Path

Convert Path, AND all other Paths associated by WAN Link, Generated by an Autopath Group, to a Static Path. This action cannot be undone

| | |
|----------------------|-------------------------|
| MCN-5100 | BR572 |
| WAN Link: BR572-WL-1 | WAN Link: MCN-5100-WL-1 |

☒ Reverse Also ☒ Enable Encryption

IP DSCP Tagging:
Any ▼

Bad Loss Sensitive:
Enable (Default) ▼

Silence Period (ms):
DEFAULT ▼

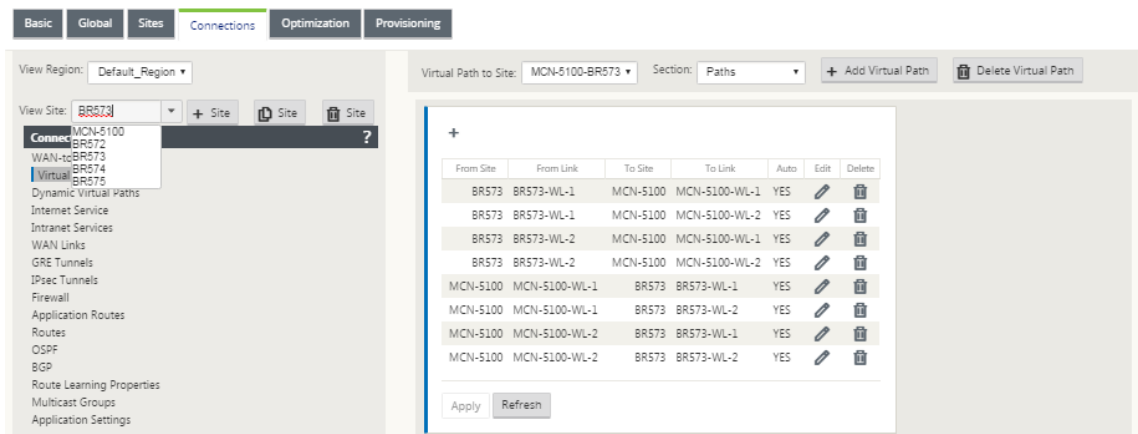
Path Probation Period (ms):
10000 (Default) ▼

☒ Instability Sensitive

Tracking IP Address: Reverse Tracking IP Address:

Apply Cancel

13. Wiederholen Sie die obigen Schritte für jeden Zweig, den Sie mit dem MCN verbinden möchten.
- Als Nächstes haben Sie die Möglichkeit, die Konfigurationen für virtuelle Pfade für die Client-Sites anzupassen und weitere Pfade zwischen Clients hinzuzufügen und zu konfigurieren. Anweisungen finden Sie in den verbleibenden Schritten unten.
14. Wählen Sie im Dropdownmenü **Site anzeigen** einen Client-Site-Zweig aus. Die Konfiguration für den Clientstandortzweig in der **Verbindungsstruktur** wird geöffnet.

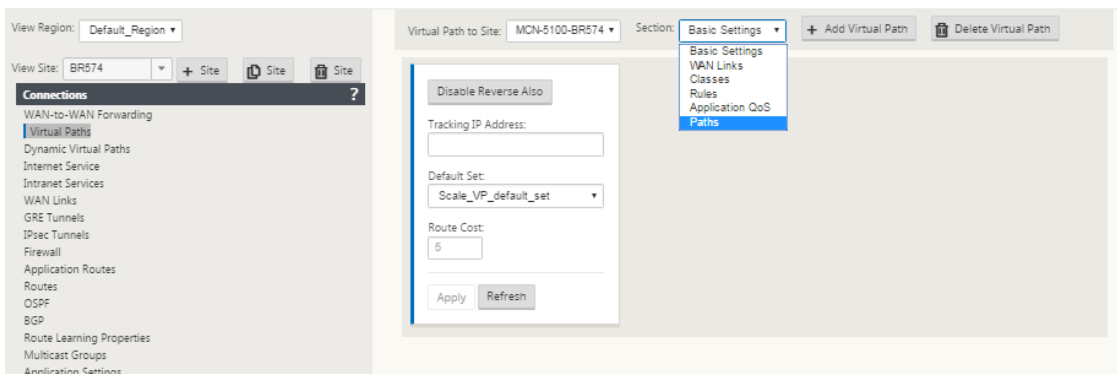


15. Navigieren Sie zum Konfigurationsformular **Pfadeinstellungen** für jeden virtuellen Pfad des Clientstandorts, den Sie konfigurieren möchten.

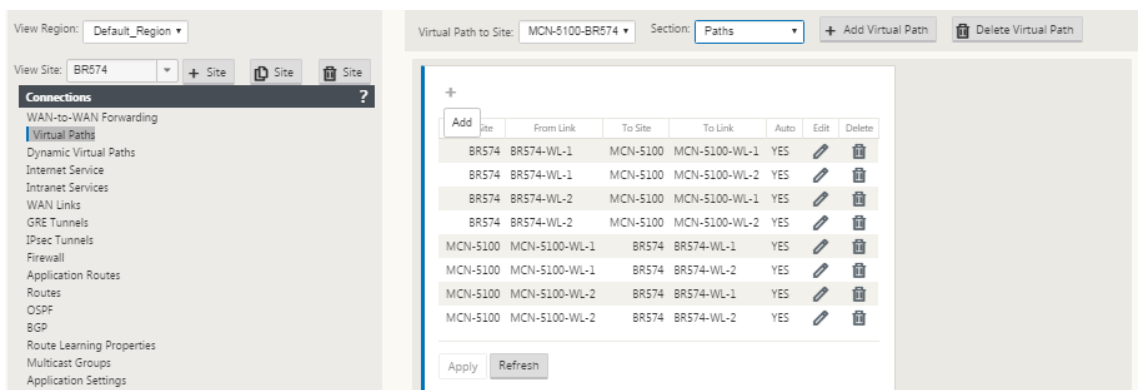
Gehen Sie folgendermaßen vor, um zum Formular **Pfadeinstellungen** für den Clientstandort zu navigieren:

16. Wählen Sie **Pfade** aus der Registerkarte **Abschnitt** der Zweigseite für den Client-Site aus.

Die folgende Abbildung zeigt ein Beispiel für **Pfadeinstellungen** für den neuen **From Site-Pfad**, der in den vorherigen Schritten hinzugefügt wurde.



17. Konfigurieren Sie die Einstellungen für jeden Pfad, den Sie anpassen möchten. Führen Sie die gleichen Schritte aus, wie Sie die virtuellen Pfade für die MCN-Site konfigurieren.



Damit ist die grundlegende Konfiguration der virtuellen Pfade zwischen den Clientstandorten und dem MCN abgeschlossen.

Hinweis

Weitere Informationen zum Konfigurieren weiterer Einstellungen in den Abschnitten **Verbindungen** oder **Provisioning** des **Konfigurations-Editors** finden Sie in der Online-Hilfe für das Management Web Interface für diese Abschnitte. Wenn Sie diese Einstellungen derzeit nicht konfigurieren möchten, können Sie mit dem unten angegebenen Schritt fortfahren.

Der nächste Schritt hängt von der SD-WAN Edition-Lizenz ab, die Sie für Ihre Bereitstellung aktiviert haben:

- **SD-WAN Premium (Enterprise) Edition** — Die Premium (Enterprise) Edition enthält den vollständigen Satz von WAN-Optimierungsfunktionen. Wenn Sie die WAN-Optimierung für Ihre Sites konfigurieren möchten, fahren Sie mit dem [Aktivieren und Konfigurieren der WAN-Optimierung](#) Thema fort. Andernfalls können Sie direkt mit [Installieren der SD-WAN-Appliance-Pakete auf den Clients](#).
- **SD-WAN Edition** — Diese Edition enthält keine WAN-Optimierungsfunktionen. Sie können nun direkt zu [Installieren der SD-WAN-Appliance-Pakete auf den Clients](#).

MCN-Konfiguration bereitstellen

May 10, 2021

Der nächste Schritt besteht darin, die SD-WAN-Appliance-Pakete für die Verteilung an die Clientknoten vorzubereiten. Hierbei handelt es sich um die folgenden zwei Verfahren:

1. Exportieren Sie das Konfigurationspaket in Change Management.

Bevor Sie die Appliance-Pakete generieren können, müssen Sie zuerst das fertige Konfigurationspaket aus dem **Konfigurations-Editor** in den globalen **Change Management**-Staging-Posteingang auf dem MCN exportieren. Anweisungen finden Sie im Abschnitt [Change Management durchführen](#).

2. Generieren und bereitstellen Sie die Appliance-Pakete.

Nachdem Sie das neue Konfigurationspaket dem **Change Management-Posteingang** hinzugefügt haben, können Sie die Appliance-Pakete generieren und bereitstellen. Dazu verwenden Sie den Assistenten für die **Änderungsverwaltung** im Management-Webinterface auf dem MCN. Anweisungen finden Sie im Abschnitt [Stellen Sie die Konfiguration in Zweigen bereit](#).

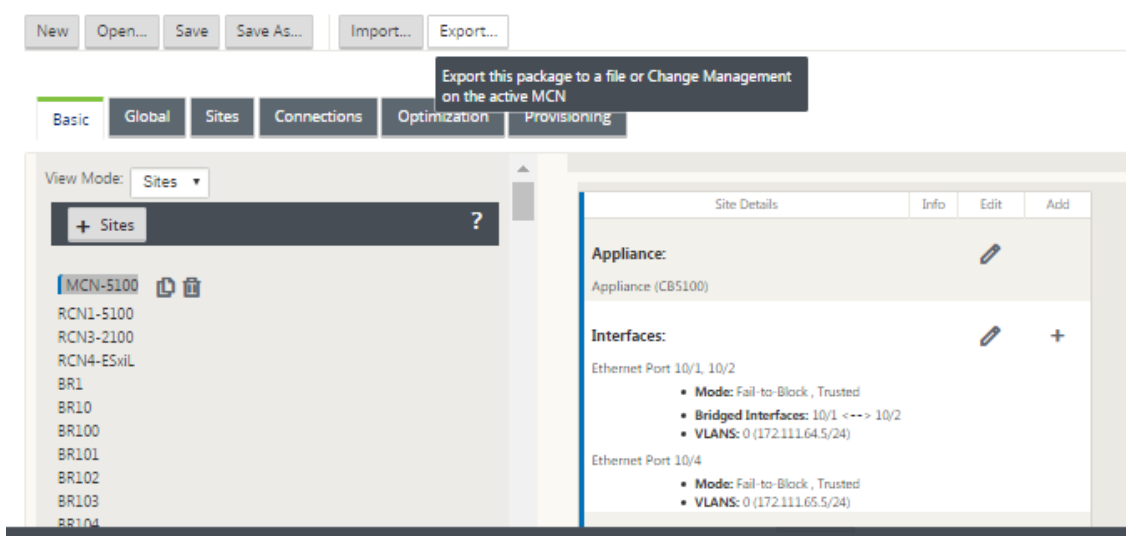
MCN Change Management durchführen

May 10, 2021

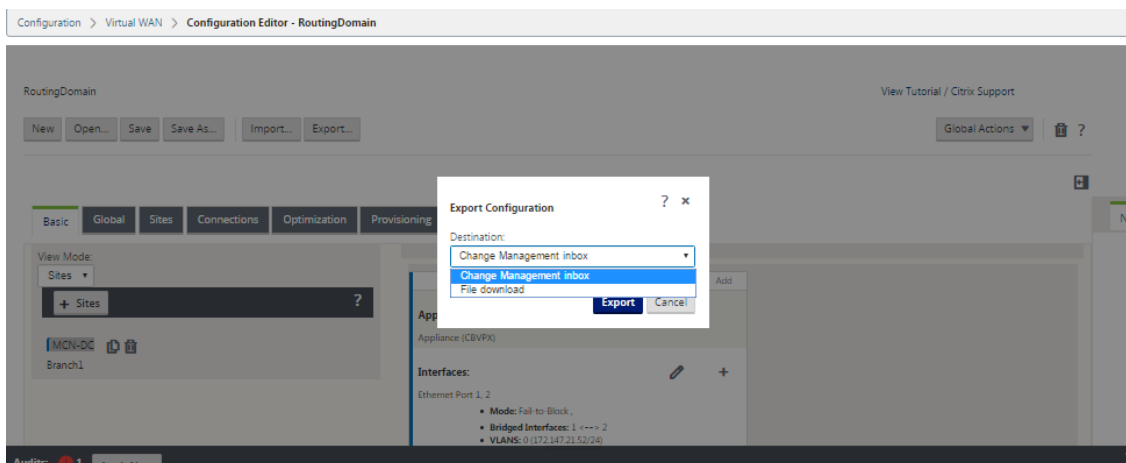
Bevor Sie die Appliance-Pakete generieren können, müssen Sie zuerst das fertige Konfigurationspaket in das Management Web Interface **Change Management** System exportieren.

Gehen Sie folgendermaßen vor, um das Konfigurationspaket in **Change Management** zu exportieren:

1. Klicken Sie auf der Seite **Konfigurations-Editor** auf **Exportieren** (oben auf der Seite).



Daraufhin wird das Dialogfeld **Konfiguration exportieren** geöffnet.



2. Wählen Sie **Änderungsverwaltungseingang** als Exportziel aus. Verwenden Sie das Dropdownmenü im Feld **Ziel**, um Ihre Auswahl zu treffen.
3. Klicken Sie **Exportieren**.

Wenn der Exportvorgang abgeschlossen ist, wird oben auf der Seite eine grüne Erfolgsstatusmeldung angezeigt.

Tipp

Sie können in der Erfolgsmeldung auf den blauen Link **Änderungsverwaltung** klicken, um direkt zur Seite **Änderungsvorbereitung — Dateien hochladen und überprüfen** (zweite Seite) des Assistenten zur **Änderungsverwaltung** zu wechseln. Sie müssen zu dieser Seite navigieren, um den nächsten Schritt im Konfigurationsprozess auszuführen. Die Erfolgsmeldung wird jedoch nur für einige Sekunden angezeigt. Danach müssen Sie den Assistenten mithilfe der Navigationsstruktur öffnen und dann zu dieser Seite wechseln. Anweisungen finden Sie im nächsten Abschnitt.

Sie können nun die SD-WAN-Softwarepakete auf die MCN-Appliance hochladen und die Appliance-Pakete für die Verteilung an die Clientknoten vorbereiten.

Konfiguration in Zweigen bereitstellen

May 10, 2021

Nachdem Sie die Konfiguration mit dem Konfigurationseditor vorbereitet und das Konfigurationspaket in den Posteingang zur Änderungsverwaltung exportiert haben, besteht der nächste Schritt darin, die SD-WAN-Appliance-Pakete für die Verteilung an die Clientknoten vorzubereiten. Verwenden Sie den Assistenten **für die Änderungsverwaltung** im Management-Webinterface auf dem MCN.

Für jedes SD-WAN-Appliance-Modell gibt es ein anderes SD-WAN-Softwarepaket. Ein Appliance-Paket besteht aus dem Softwarepaket für ein bestimmtes Modell, das zusammen mit dem Konfigurationspaket, das Sie bereitstellen möchten. Daher muss für jedes Appliance-Modell in Ihrem Netzwerk ein anderes Appliance-Paket vorbereitet und generiert werden.

Hinweis

Wenn Sie die erforderlichen SD-WAN-Softwarepakete noch nicht auf einen PC heruntergeladen haben, der mit Ihrem Netzwerk verbunden ist, können Sie dies jetzt tun. Informationen zum Erwerb und Herunterladen der Software finden Sie im Abschnitt [Erwerb der SD-WAN-Softwarepakete](#)

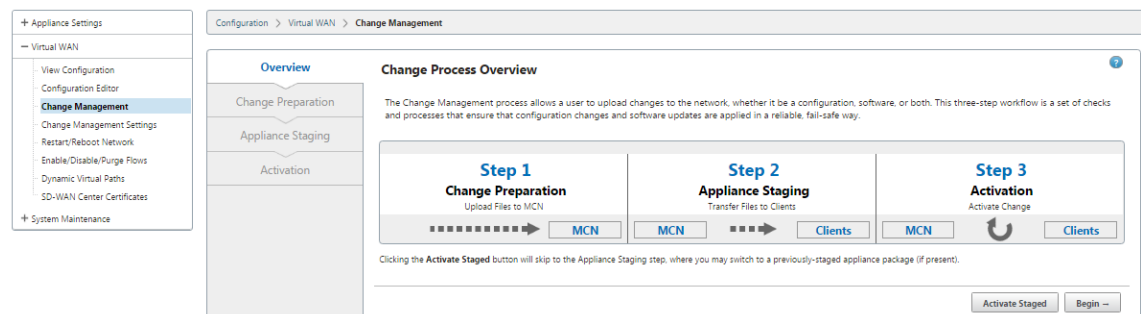
Gehen Sie folgendermaßen vor, um das Paket und die Konfiguration in den MCN hochzuladen und zu installieren:

1. Melden Sie sich bei der Managementoberfläche der MCN-Appliance an.

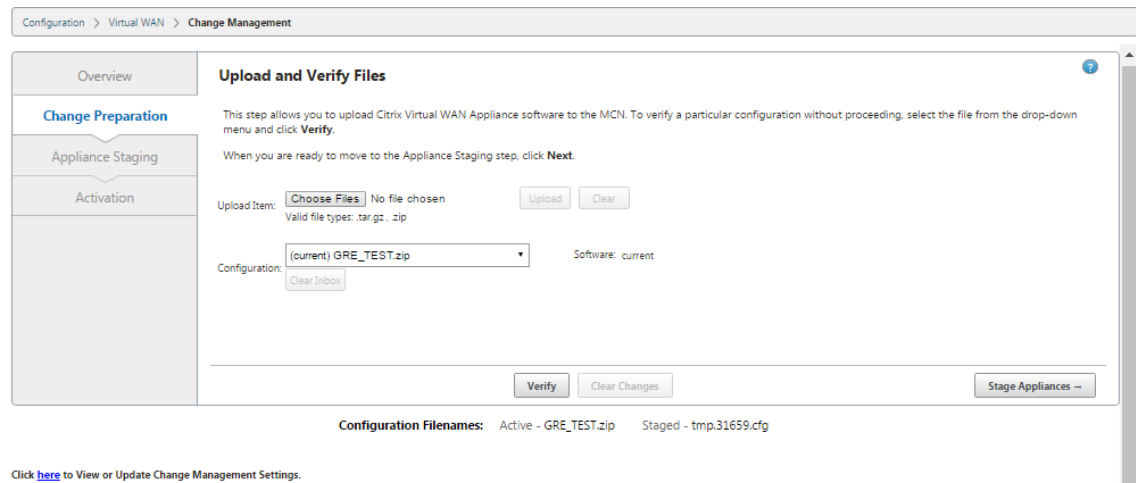
Hinweis

Sie laden die zuvor heruntergeladenen Softwarepakete auf den angeschlossenen PC hoch. Der Einfachheit halber möchten Sie möglicherweise denselben PC verwenden, um erneut eine Verbindung zum MCN herzustellen.

2. Wählen Sie die Registerkarte **Konfiguration** aus.
3. Öffnen Sie im linken Bereich den Abschnitt **Virtuelles WAN**, und wählen Sie **Änderungsverwaltung** aus. Die erste Seite des **Change Management**-Assistenten, die Seite **Change Process Overview**, wird angezeigt.

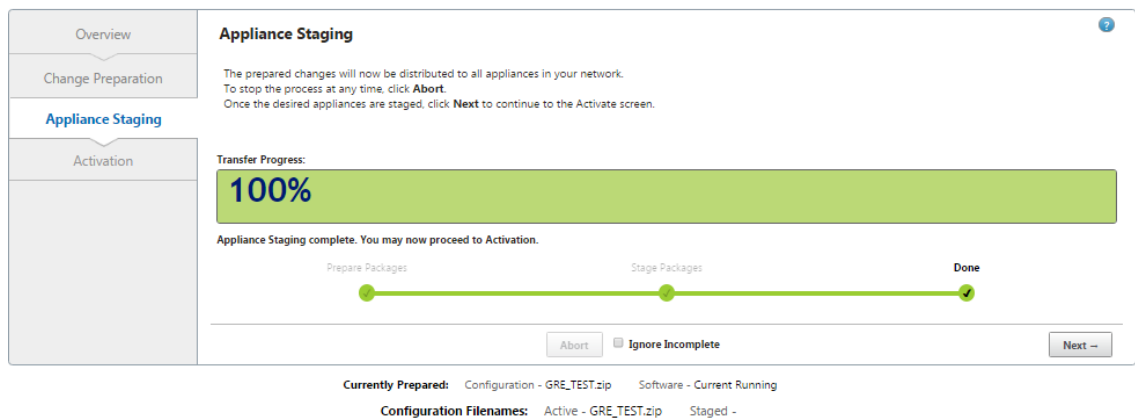


4. Klicken Sie auf **Beginnen**. Die Seite **Änderungsvorbereitung** zum Hochladen und Überprüfen, ob die angegebenen Konfigurations- und Softwarepakete angezeigt werden.



5. Laden Sie alle SD-WAN-Softwarepakete hoch, die für Ihr Netzwerk erforderlich sind. Gehen Sie für jedes SD-WAN-Softwarepaket, das Sie bereitstellen möchten, folgendermaßen vor:
 - a) Klicken Sie neben dem Feld **Element hochladen** auf **Datei auswählen**. Dadurch wird ein Dateibrowser geöffnet, mit dem Sie ein SD-WAN-Softwarepaket auswählen können, das hochgeladen werden soll.
 - b) Wählen Sie ein SD-WAN-Softwarepaket aus, und klicken Sie auf **OK**.

- c) Navigieren Sie zu den SD-WAN-Softwarepaketen, die Sie zuvor auf den lokalen PC heruntergeladen haben, und wählen Sie das Paket aus, das hochgeladen werden soll.
 - d) Klicken Sie auf **Hochladen**
 - e) Wiederholen Sie die Schritte (i) bis (iii) für jedes SD-WAN-Softwarepaket, das für Ihr Netzwerk erforderlich ist.
6. Wählen Sie im Dropdownmenü **Konfiguration** das neue Konfigurationspaket aus, das Sie gerade in **Change Management** exportiert haben.
 7. Klicken Sie auf **Stage Appliance**. Die Appliance-Staging initiiert die folgenden Aktionen:
 - Überträgt das ausgewählte Softwarepaket und die Konfiguration an den MCN.
 - Generiert ein Appliance-Paket für jedes Appliance-Modell, das in der ausgewählten Konfiguration identifiziert wurde.
 - Fügt die neuen Appliance-Pakete zur Liste der verfügbaren Pakete in der Site-Appliance-Tabelle hinzu.
 - Stationiert die neue Konfiguration und das entsprechende Softwarepaket auf dem MCN.
 8. Klicken Sie auf **Weiter**. Daraufhin wird die Seite **Appliance-Staging** fortgesetzt.



Wenn der Staging-Vorgang abgeschlossen ist, wird die **Tabelle Site-Appliance mit den neu bereitgestellten Appliance-Paketinformationen gefüllt.

Hinweis

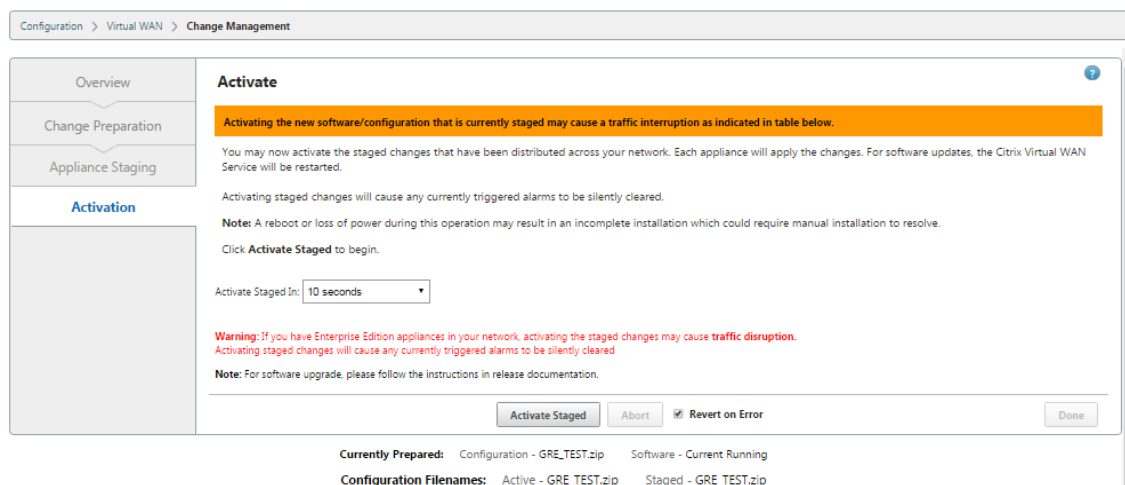
Wenn es sich um eine Erstbereitstellung handelt, wird nur der MCN jetzt aktualisiert und bereitgestellt. Wenn Sie eine vorhandene Bereitstellung aktualisieren und die virtuellen Pfade bereits zwischen den bereitgestellten Standorten funktionieren, werden auch die entsprechenden Appliance-Pakete an die bereitgestellten Clientknoten verteilt und das Staging auf diesen Knoten initiiert. Wenn Sie jedoch neue Clientknoten zu einer vorhandenen Virtual WAN-Bereitstellung hinzufügen, müssen Sie das entsprechende Appliance-

Paket auf jedem neuen Client manuell hochladen, bereitstellen und aktivieren, wie in den übrigen Schritten in diesem Verfahren beschrieben.

Ab Citrix SD-WAN 11.2.2 Release wird die Site auf der Änderungsverwaltungsseite als **nicht verbunden** angezeigt, während des Staging-Vorgangs als fehlgeschlagen markiert und der Fortschrittsbalken wird auf 100% abgeschlossen. Sobald die **nicht verbundene** Website wieder online und verbunden ist, korrigiert MCN sie automatisch.

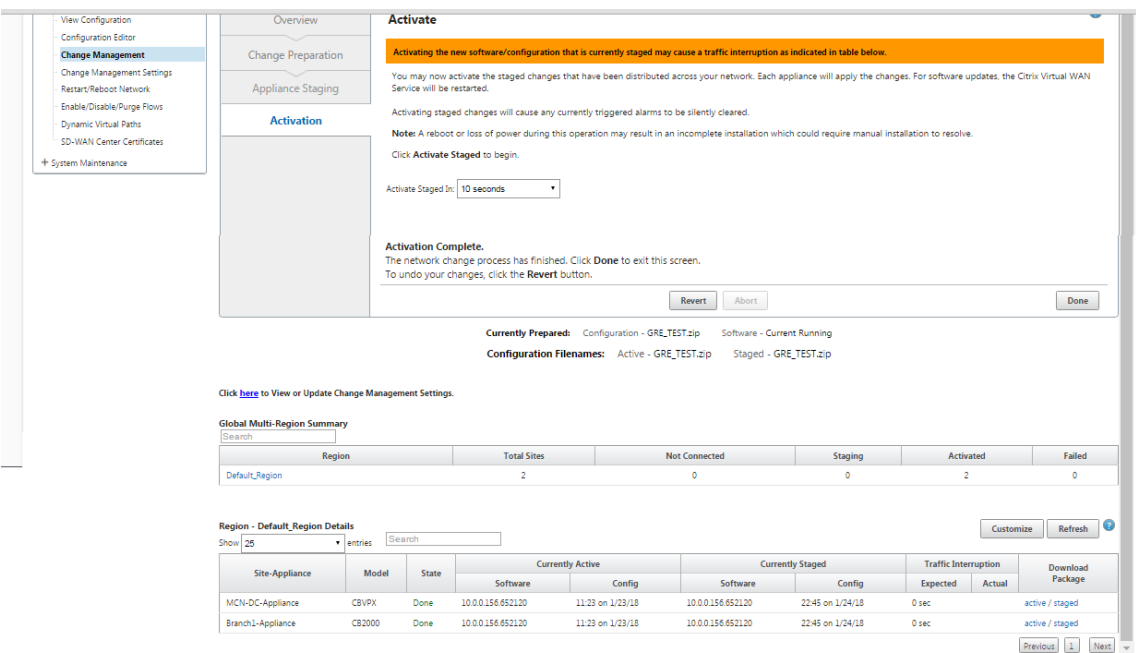
Wählen Sie für Versionen vor Citrix SD-WAN 11.2.2 die Option **Unvollständig ignorieren** aus, wenn Sie weitere Standorte zum Netzwerk hinzufügen oder wenn sich die Site im Status **“Nicht verbunden“** befindet. Dies zeigt an, dass nur die verbundenen Standorte und der MCN aktualisiert und bereitgestellt werden. Sobald die Site, die sich im Status **“Nicht verbunden“** befand, wieder in den verbundenen Zustand versetzt, wird sie automatisch von MCN als Teil der Autokorrektur bereitgestellt und aktualisiert.

9. Wählen Sie **Bei Fehler wiederherstellen** aus, um bei Auftreten eines Fehlers zum vorherigen Anwendungspaket zurückzukehren. Weitere Informationen finden Sie unter Konfigurationsroll-back.
10. Klicken Sie auf **Activate Staged**.



Die Ergebnisse und die nächsten Schritte werden zu diesem Zeitpunkt unterschiedlich sein, je nachdem, ob es sich um eine Erstkonfiguration handelt oder Sie eine vorhandene Konfiguration aktualisieren oder ersetzen, wie folgt:

- Wenn Sie die Konfiguration einer vorhandenen Bereitstellung aktualisieren oder ändern.
 - Wenn es sich nicht um eine Erstkonfiguration handelt, werden die neue Konfiguration und das entsprechende Appliance-Paket auf der MCN-Appliance aktiviert. Das entsprechende Appliance-Paket wird dann an jeden Client in Ihrem SD-WAN verteilt und automatisch aktiviert. Dies kann einige Sekunden dauern.

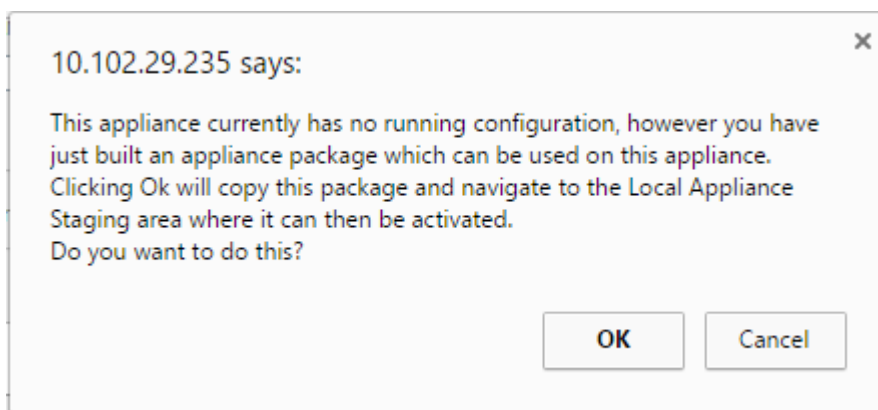


Wenn die Aktivierung abgeschlossen ist, wird eine Statusmeldung **Aktivierung abgeschlossen** angezeigt, und die Schaltfläche **Fertig** ist aktiviert. Darüber hinaus zeigt die Statuszeile für **Konfigurationsdateinamen** (über der Tabelle) jetzt den Namen des neu aktivierten Pakets im Feld **Aktiv** an.

11. Klicken Sie auf ****Fertig**, und fahren Sie mit einem der folgenden Schritte fort:
- Wenn Sie Ihrem SD-WAN keine neuen Knoten hinzufügen, ist damit die Vorbereitung, Verteilung und Aktivierung der neuen Appliance-Pakete in Ihrem SD-WAN abgeschlossen. Sie können direkt mit fortfahren **Aktivieren des virtuellen WAN-Diensts**.
 - Wenn Sie neue Clientknoten zu Ihrem SD-WAN hinzufügen möchten, fahren Sie mit **Verbinden der Client-Appliances mit Ihrem Netzwerk**.
 - Wenn Sie eine Erstkonfiguration aktivieren, wird das neue Konfigurationspaket zu diesem Zeitpunkt nicht aktiviert, und es gibt weitere Schritte, die Sie ausführen müssen. Der nächste Schritt besteht darin, das Konfigurationspaket in den Bereich Lokale Appliance-Staging zu kopieren, um das Staging und Aktivieren des Konfigurationspakets auf dem MCN vorzubereiten.

Gehen Sie wie folgt vor:

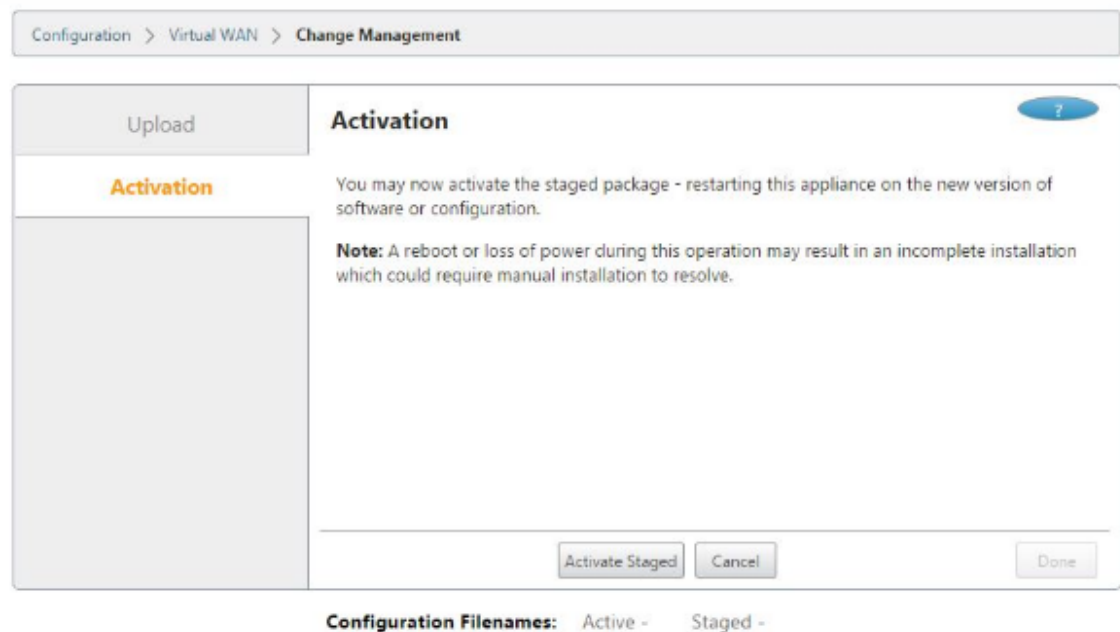
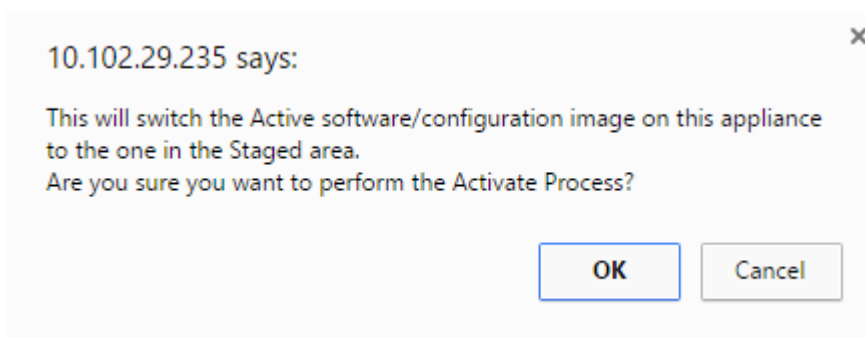
12. Sobald Sie auf **Staged aktivieren** geklickt haben, wird die folgende Meldung angezeigt.



13. Klicken Sie auf **OK**.

14. Klicken Sie auf **Staging aktivieren**.

Daraufhin wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, den Aktivierungsvorgang zu bestätigen.



15. Klicken Sie auf **OK**.

Dadurch wird die Aktivierung des bereitgestellten Konfigurationspakets gestartet. Dieser Vorgang dauert mehrere Sekunden, während der eine Statusmeldung angezeigt wird.

Wenn die Aktivierung abgeschlossen ist, wird eine Statusmeldung angezeigt, in der die Aktivierung abgeschlossen angezeigt wird, und die Schaltfläche **Fertig** ist aktiviert.

16. Klicken Sie auf **Fertig**. Sie gelangen zur Seite **Management-Webinterface-Dashboard**, auf der Sie die Aktivierungsergebnisse anzeigen können.

Sie haben nun die Vorbereitung der SD-WAN Appliance-Pakete auf dem MCN abgeschlossen. Fahren Sie mit (</en-us/citrix-sd-wan/11-2/configuration/connecting-client-appliances-to-network.html>) fort, um die Client-Appliances mit Ihrem Netzwerk zu verbinden.

Tipp

Mit dem Assistenten zur **Änderungsverwaltung** können Sie die Site-Appliance-Tabelle durchsuchen. Auf diese Weise können Sie Sites in einem großen Netzwerk mit mehreren Sites suchen und die erforderliche Stufen-Konfiguration herunterladen. Sie können auch nach Fehlerzuständen suchen, zum Beispiel: 'Fail' oder 'Not Connected'. Dadurch erhalten Sie eine Liste aller Sites in diesem Zustand.

One-Touch-Start

May 10, 2021

Once touch start ermöglicht es Ihnen, Ihre SD-WAN-Appliance beim ersten Start einfach und schnell als Client zu konfigurieren.

Die Ein-Touch-Startoption wird angezeigt, wenn die Appliance zum ersten Mal hochfährt.

The screenshot shows the 'Configuration' tab of the Citrix SD-WAN Management-Webinterface-Dashboard. The 'One Touch Start' section is active, displaying two configuration options: 'Appliance Mode' with radio buttons for 'MCN' (selected) and 'Client', and 'Installation Mode' with radio buttons for 'Existing Package' and 'Create New Package' (selected). A 'Next →' button is located at the bottom left of the configuration area.

Hinweis

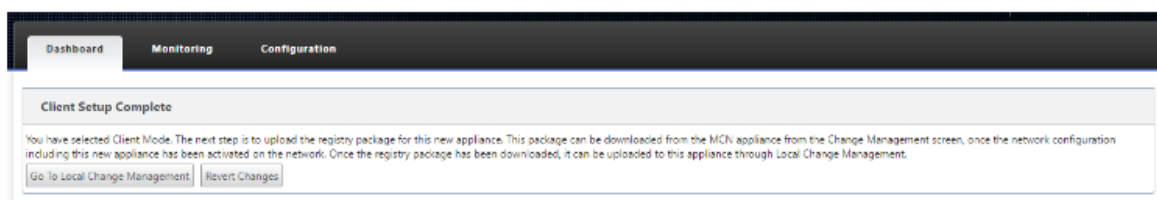
Um die SD-WAN-Appliance als MCN zu konfigurieren, erstellen Sie eine Konfiguration oder importieren Sie eine vorhandene Konfiguration mit dem **Konfigurations-Editor**. Weitere Informationen finden Sie unter [Vorbereiten der SD-WAN-Appliance-Pakete auf dem MCN](#)

So konfigurieren Sie Ihre SD-WAN-Appliance als Client mithilfe einer vorhandenen Konfigurationsdatei:

1. Wählen Sie **Client** als Appliance-Modus aus.
2. Wählen Sie **Vorhandenes Paket** Installationsmodus aus. Der Administrator muss die Konfiguration des MCN regelmäßig speichern, um ein bestehendes Paket des MCN zu verwenden.
3. Klicken Sie auf **Datei** auswählen, um das Konfigurationspaket auf Ihrem lokalen Computer auszuwählen.
4. Klicken Sie auf **Hochladen und Installieren**.

So konfigurieren Sie Ihre SD-WAN-Appliance mithilfe der lokalen Änderungsverwaltung als Client:

1. Wählen Sie **Client** als Appliance-Modus aus.
2. Wählen Sie **Neues Paket erstellen** aus, um das Konfigurationspaket für diese Appliance mithilfe der lokalen Änderungsverwaltung hochzuladen. Das Paket kann von der MCN-Appliance aus dem Fenster Änderungsverwaltung heruntergeladen werden.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Gehe zu lokaler Änderungsverwaltung**.



Befolgen Sie die Schritte im Thema [Installieren der SD-WAN-Appliance-Pakete auf den Clients](#).

Verbinden der Client-Appliances mit dem Netzwerk

May 10, 2021

Bei einer ersten Bereitstellung oder wenn Sie Clientknoten zu einem vorhandenen SD-WAN hinzufügen, besteht der nächste Schritt darin, dass die Zweigstandadministratoren die Client-Appliances an ihren jeweiligen Zweigstandorten mit dem Netzwerk verbinden. Dies ist in Vorbereitung auf

das Hochladen und Aktivieren der entsprechenden SD-WAN-Appliance-Pakete auf die Clients. Verbinden Sie die einzelnen Zweigstandadministratoren, um diese Verfahren zu initiieren und zu koordinieren.

Um die Standort-Appliances mit dem SD-WAN zu verbinden, sollten Site-Administratoren die folgenden Schritte ausführen:

1. Wenn Sie dies noch nicht getan haben, richten Sie die Client-Appliances ein.

Gehen Sie für jede Appliance, die Sie Ihrem SD-WAN hinzufügen möchten, folgendermaßen vor:

- a) Richten Sie die SD-WAN-Appliance-Hardware und alle virtuellen SD-WAN VPX-Appliances (SD-WAN VPX-SE) ein, die Sie bereitstellen.
 - b) Legen Sie die Verwaltungs-IP-Adresse für die Appliance fest, und überprüfen Sie die Verbindung.
 - c) Legen Sie Datum und Uhrzeit auf der Appliance fest. Legen Sie den Schwellenwert für die Konsolensitzung auf einen hohen oder maximalen Wert fest.
 - d) Laden Sie die Softwarelizenzdatei hoch und installieren Sie sie auf der Appliance.
2. Verbinden Sie die Appliance mit dem Zweigstands-LAN. Schließen Sie ein Ende eines Ethernetkabels an einen Port an, der für LAN an der SD-WAN-Einheit konfiguriert ist. Verbinden Sie dann das andere Ende des Kabels mit dem LAN-Switch.
 3. Verbinden Sie die Appliance mit dem WAN. Schließen Sie ein Ende eines Ethernetkabels an einen Port an, der für WAN an der SD-WAN-Appliance konfiguriert ist. Verbinden Sie dann das andere Ende des Kabels mit dem WAN-Router.

Der nächste Schritt besteht darin, dass die Zweigstandadministratoren das entsprechende SD-WAN-Appliance-Paket auf ihren jeweiligen Clients installieren und aktivieren.

Installieren der SD-WAN-Appliance-Pakete auf den Clients

May 10, 2021

Nachdem Sie die Appliance-Pakete vorbereitet und den MCN angeschlossen haben und die Administratoren der Zweigstelle ihre jeweiligen Client-Appliances mit dem LAN und dem WAN verbunden haben, müssen Sie im nächsten Schritt das entsprechende SD-WAN-Appliance-Paket auf jedem Client hochladen und aktivieren. Der Assistent zur Änderungsverwaltung führt Sie durch diesen Prozess.

Gehen Sie folgendermaßen vor, um die Software und Konfiguration auf einer Client-Appliance zu installieren und zu aktivieren:

1. Öffnen Sie auf einem angeschlossenen PC einen Browser, und melden Sie sich am Management Web Interface der MCN-Appliance an.

Geben Sie die Verwaltungs-IP-Adresse für den MCN in das Adressfeld des Browsers ein. Dadurch wird die Seite **Management-Webinterface-Dashboard** für die MCN-Appliance angezeigt.

2. Wählen Sie die Registerkarte **Konfiguration** aus. Wählen Sie im Navigationsbereich auf der linken Seite **Virtual WAN** und dann **Change Management** aus.

Daraufhin wird die Seite **Änderungsprozessübersicht** angezeigt (die erste Seite des Assistenten für die **Änderungsverwaltung**).

DashboardMonitoringConfiguration

ConfigurationVirtual WANChange Management

Appliance SettingsVirtual WANView ConfigurationConfiguration EditorChange ManagementChange Management SettingsRestart/Reboot NetworkEnable/Disable/Purge FlowsDynamic Virtual PathsSD-WAN Center CertificatesSystem Maintenance

OverviewChange PreparationAppliance StagingActivation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Warning: If you have Enterprise Edition appliances in your network, activating the staged changes may cause traffic disruption. Activating staged changes will cause any currently triggered alarms to be silently cleared.

Note: For software upgrade, please follow the instructions in release documentation.

Activate StagedAbortRevert on ErrorDone

Currently Prepared: Configuration - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN1_LkEE.zipSoftware - Current Running

Configuration Filenames: Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN1_LkEE.zipStaged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensino_550sites_wantowanforwardino_oeoRCN1_LkEE.zip

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

Global Multi-Region Summary

| Region | Total Sites | Not Connected | Preparing/Staging | Staged | Failed |
|----------------|--------------------|---------------|-------------------|--------|--------|
| Default_Region | 10 | 2 | 0 | 8 | 0 |
| r1 | 552 | 4 | 4 | 547 | 0 |
| r3 | 8 | 2 | 1 | 5 | 0 |
| r4 | Data not available | | | | |

Region - Default_Region Details

Show 25 entries

| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Traffic Interruption | | Download Package |
|-----------------------------|--------|---------------------|-------------------|------------------|-------------------|------------------|----------------------|--------|------------------|
| | | | Software | Config | Software | Config | Expected | Actual | |
| MCN-5100-Appliance | CB5100 | Done | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| BR572-Appliance | CBVPX | Done | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| BR573-Appliance | CBVPX | Done | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| BR574-Appliance | CBVPX | Done | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| BR575-Appliance | CBVPX | Done | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| RCN1-5100-Appliance | CB5100 | Transferring Region | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| RCN1-5100-RCN1_HA-Appliance | CB5100 | Done | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| RCN3-2100-Appliance | CB2100 | Done | 10.0.0.184.657939 | 13:18 on 2/14/18 | 10.0.0.184.657939 | 14:58 on 2/14/18 | 0 sec | | active / staged |
| RCN3Geo-2100-Appliance | CB2100 | Cancelled | Not Connected | | | | Loc Chg Mgt | | active / staged |
| RCN4-ESiL-Appliance | CBVPXL | Cancelled | Not Connected | | | | Loc Chg Mgt | | active / staged |

Unten auf dieser Seite finden Sie eine Tabelle mit den einzelnen Sites und Appliances. Ganz rechts neben der Tabelle in der Spalte **Paket herunterladen** sind Links für die Pakete **Aktiv** (falls verfügbar) und **Staged appliance**.

| Traffic Interruption | | Download Package |
|----------------------|--------|------------------|
| Expected | Actual | |
| 0 sec | | active / staged |
| Loc Chg Mgt | | active / staged |

Hinweis

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

218

Wenn es sich um eine Erstinstallation handelt, sind die **aktiven** Links noch nicht verfügbar und werden durch einen Nur-Text-Marker **none** ersetzt.

3. Klicken Sie auf den Link **Staged** für das Paket, das Sie herunterladen möchten.

Suchen Sie in der Tabelle **Site-Appliance** den Eintrag für Ihre Standort-Appliance, und klicken Sie in der Spalte **Paket herunterladen** dieses Eintrags auf den Link **Staged**. Ein Dateibrowser zur Auswahl des Downloadorts (auf dem lokalen PC) wird angezeigt.

4. Wählen Sie den Download-Speicherort aus und klicken Sie auf **OK**.
5. (Optional.) Melden Sie sich nach Abschluss des Downloads vom MCN Management Web Interface ab.
6. Öffnen Sie einen Browser, und geben Sie die IP-Adresse des Clients ein, auf den Sie die ZIP-Datei des Appliance-Pakets hochladen möchten.

Hinweis

Bitte ignorieren Sie alle Browserzertifikatwarnungen für das Management-Webinterface.

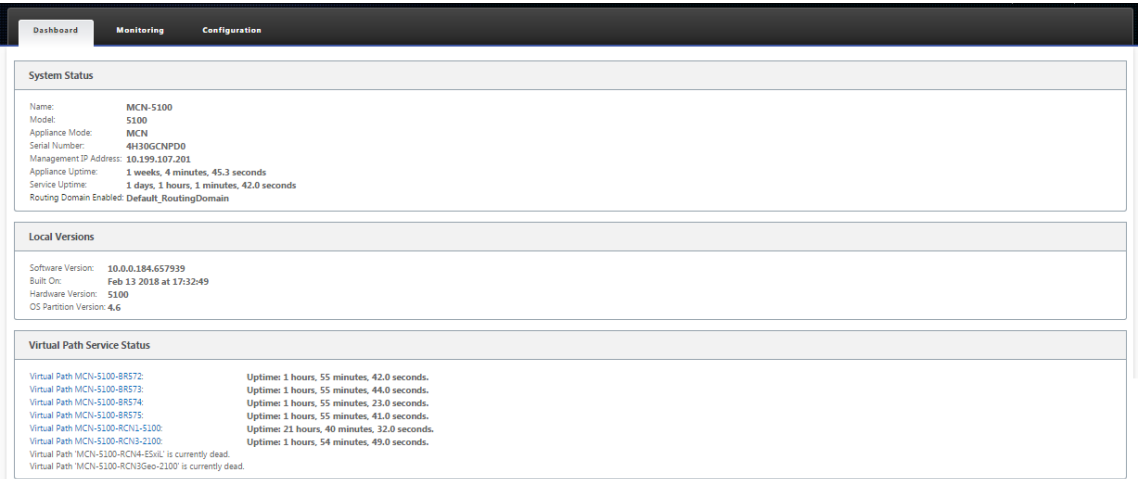
Dadurch wird der Anmeldebildschirm für Citrix SD-WAN Management Web Interface auf der Client-Appliance geöffnet.



7. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie auf

Anmelden. Der standardmäßige Administratorbenutzername ist *admin*. Das Standardkennwort ist *password*.

Dadurch wird die Seite **Management-Webinterface-Dashboard** für die Client-Appliance angezeigt.

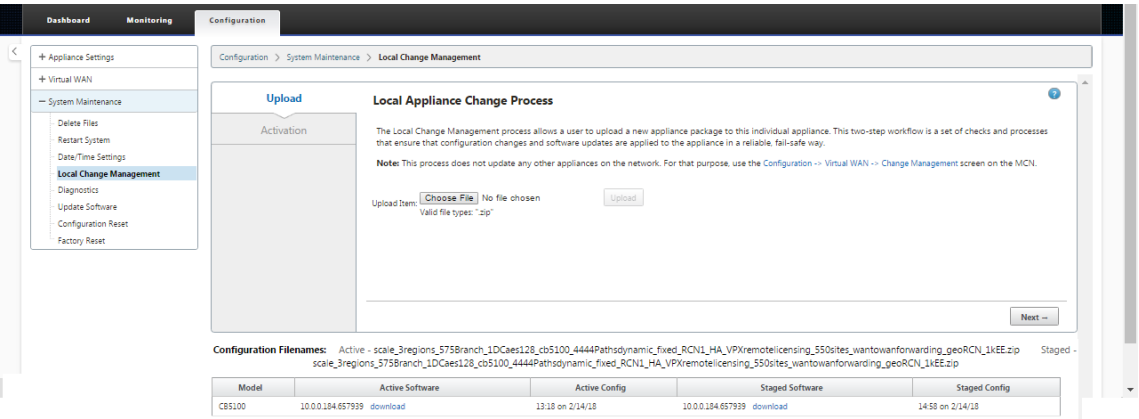


Hinweis

Wenn es sich um eine Erstinstallation handelt oder wenn Sie den Virtual WAN-Dienst auf dieser Appliance vorübergehend deaktiviert haben, wird ein Symbol für die Goldrüd-Überwachungswarnung mit einer Statusmeldung angezeigt, die angibt, dass der virtuelle WAN-Dienst inaktiv oder deaktiviert ist. Sie können diese Warnung vorerst ignorieren. Die Warnung bleibt auf der **Dashboard-Seite**, bis Sie den Dienst nach Abschluss der Installation manuell starten.

- 8. Wählen Sie die Registerkarte **Konfiguration** aus.
- 9. Öffnen Sie den Zweig Systemwartung in der Navigationsstruktur (linker Bereich), und wählen Sie **Lokale Änderungsverwaltung** aus.

Dadurch wird die Seite **Local Appliance Change Process Upload** zum Hochladen eines Appliance-Pakets angezeigt.



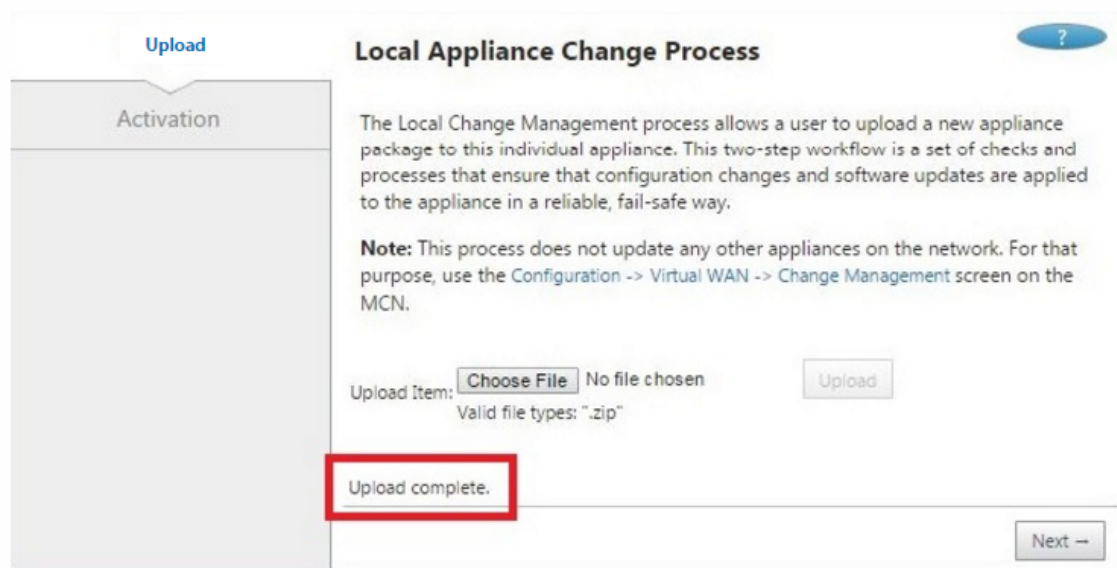
10. Klicken Sie neben dem Label **Element hochladen** auf **Datei auswählen**.

Dadurch wird ein Dateibrowser geöffnet, in dem Sie das Appliance-Paket auswählen können, das Sie auf den Client hochladen möchten.

11. Navigieren Sie zu der ZIP-Datei des SD-WAN-Appliance-Pakets, die Sie gerade aus dem MCN heruntergeladen haben, wählen Sie sie aus, und klicken Sie auf **OK**.

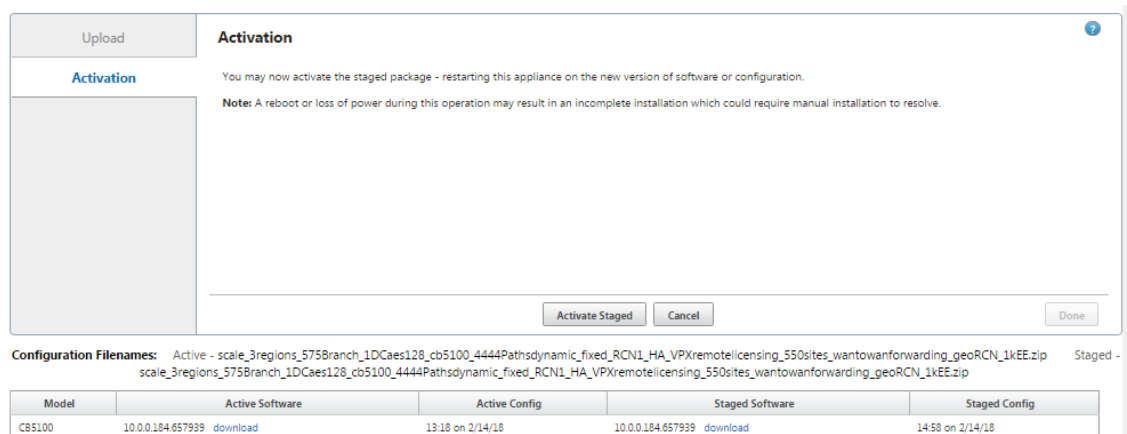
12. Klicken Sie auf **Upload**.

Der Upload-Vorgang dauert einige Sekunden. Nach Abschluss wird eine Statusmeldung (linke Mitte der Seite) mit der Angabe **Upload abgeschlossen angezeigt**.



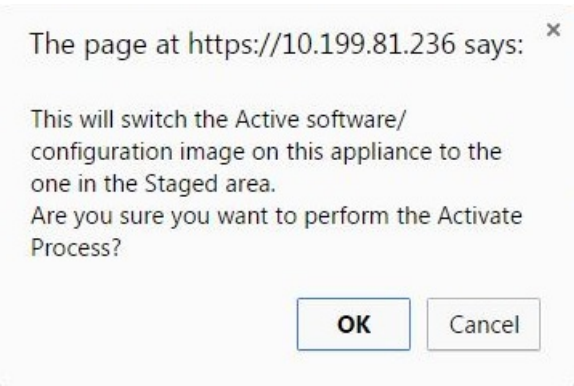
13. Klicken Sie auf **Weiter**.

Dadurch wird das angegebene Softwarepaket hochgeladen und die Seite **Aktivierung** der lokalen Änderungsverwaltung angezeigt.



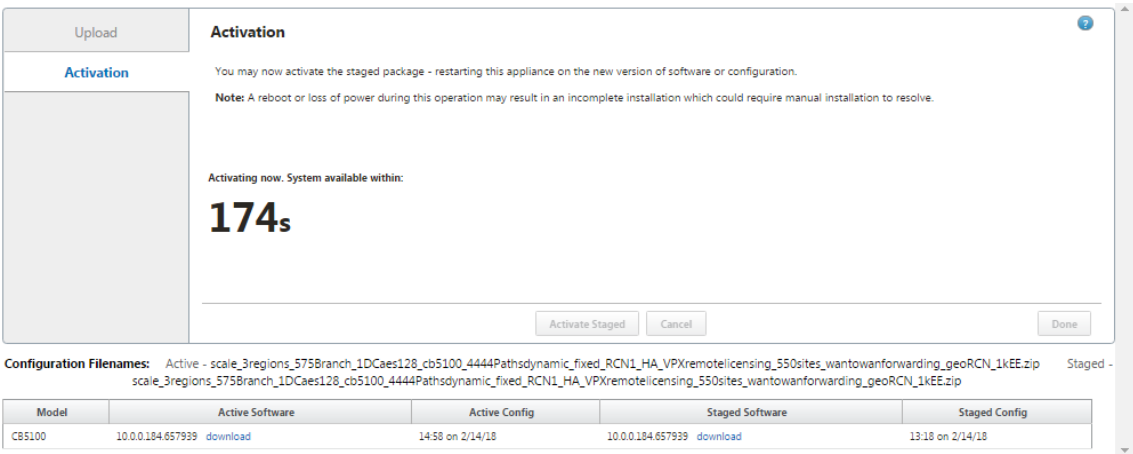
14. Klicken Sie auf **Activate Staged**.

Daraufhin wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, den Aktivierungsvorgang zu bestätigen.

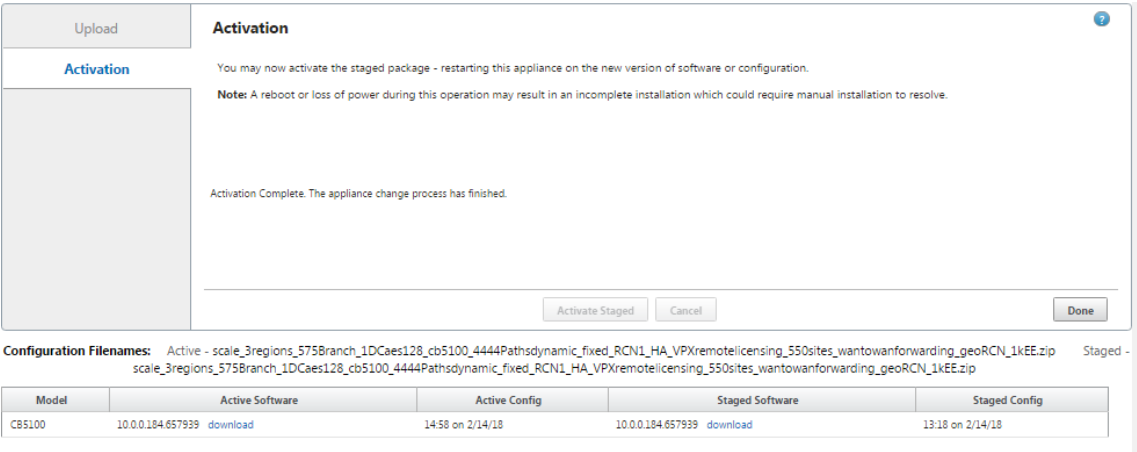


15. Klicken Sie auf **OK**.

Dadurch wird das neu installierte Paket aktiviert und, wenn es sich nicht um eine Erstbereitstellung handelt, wird der Virtual WAN-Dienst auf der Client-Appliance gestartet. Dieser Vorgang dauert mehrere Sekunden, während der eine Statusmeldung angezeigt wird.



Wenn die Aktivierung abgeschlossen ist, wird eine Statusmeldung mit der Angabe **Aktivierung abgeschlossen** angezeigt, und die Schaltfläche **Fertig** wird verfügbar.

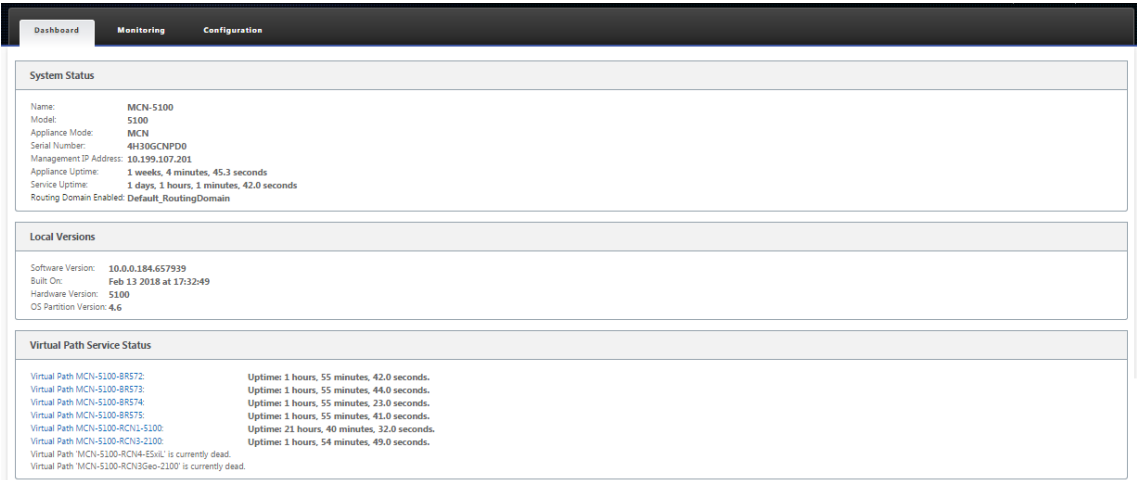


16. Klicken Sie auf **Fertig**, um den Assistenten zu beenden und die Aktivierungsergebnisse anzuzeigen.

Nachdem die Aktivierung abgeschlossen ist, klicken Sie auf der Seite **Aktivierung** auf **Fertig**, um zur Seite **Management-Webinterface-Dashboard** zurückzukehren.

Wenn es sich nicht um eine Erstbereitstellung handelt, sollten auf dieser Seite nun aktualisierte Informationen für die aktuell aktive Version des Softwarepakets, die Betriebssystempartition und den Status des virtuellen Pfads angezeigt werden. Wenn es sich um eine Erstinstallation handelt, wird ein Goldrute-Audit-Alert-Symbol sowie eine Statusmeldung angezeigt, die angibt, dass der virtuelle WAN-Dienst inaktiv oder deaktiviert ist. In diesem Fall müssen Sie den Dienst manuell aktivieren, wie unter beschrieben [Aktivieren des virtuellen WAN-Diensts](#).

Die folgende Abbildung zeigt eine **Beispiel-Client-Dashboard-Seite**, auf der das Warnsymbol und die Statusmeldung angezeigt werden.



Der letzte Schritt zum Abschließen einer anfänglichen SD-WAN-Bereitstellung besteht darin, den Virtual WAN-Dienst zu aktivieren. Anweisungen finden Sie im Abschnitt [Aktivieren des virtuellen WAN-Diensts](#).

Bereitstellen von Citrix SD-WAN Standard Edition in OpenStack mit CloudInit

May 10, 2021

Sie können jetzt Citrix SD-WAN Standard Edition (SE) in einer OpenStack-Umgebung bereitstellen. Hierzu muss das Citrix SD-WAN -Image die Konfigurationslaufwerksfunktionalität unterstützen.

HINWEIS:

Erstellen Sie ein Citrix Image, um die Konfigurationslaufwerksfunktionen zu unterstützen.

Die Config-Drive-Funktionalität unterstützt die folgende Parameterkonfiguration, um die Kommunikation mit Citrix Orchestrator über das Verwaltungsnetzwerk herzustellen:

- Mgmt. ipv4 Adresse
- Mgmt. Gateway
- Name-server1
- Name-server2
- Seriennummer - Wird für die Authentifizierung verwendet und muss für die neue Instanz wiederverwendet werden. Seriennummer, die in Clouding übergeben wird, muss die automatisch generierte Testnummer in der VPX-Instanz überschreiben.

Hinweis

- Um die Seriennummer wiederverwenden zu können, ist ein Init-Skript in SD-WAN integriert, das auf einem OpenStack ausgeführt wird und die Seriennummer in `/etc/default/family` ändert.
- Orchestrator muss über eine eindeutige Seriennummer mit SD-WAN-Appliances verfügen, um funktionieren zu können.

Cloudinit-Skript unterstützt die Kontextualisierung für die SD-WAN-Bereitstellung in OpenStack mit config-drive.

Während der Kontextualisierung stellt die Infrastruktur den Kontext für die virtuelle Maschine zur Verfügung und die virtuelle Maschine interpretiert den Kontext. Bei der Kontextualisierung kann die virtuelle Maschine bestimmte Dienste starten, Benutzer erstellen oder Netzwerk- und Konfigurationsparameter festlegen.

Für eine SD-WAN-Instanz in OpenStack sind die Eingaben für Management IP, DNS und Seriennummer der Benutzer erforderlich. Das Cloudinit-Skript analysiert diese Eingaben und stellt der Instanz die angegebenen Informationen zur Verfügung.

Beim Starten von Instanzen in einer OpenStack-Cloud-Umgebung muss die Citrix SD-WAN Appliance zwei Technologien unterstützen: User Data und CloudInit, um die automatisierte Konfiguration von Instanzen beim Booten zu unterstützen.

Führen Sie die folgenden Schritte aus, um SD-WAN SE in einer OpenStack-Umgebung Provisioning:

Voraussetzungen

Gehen Sie zu **Images** und klicken Sie auf **Create Image**.

Create Image

Image Details
Specify an image to upload to the Image Service.

Image Name
i

Image Description

Image Source
File
Browse...

Format

Image Requirements
Kernel: Choose an image
Ramdisk: Choose an image
Architecture
Minimum Disk (GB): 0
Minimum RAM (MB): 0

Image Sharing
Visibility: Public Private
Protected: Yes No

Cancel < Back Next > Create Image

- **Imagename** - Geben Sie den Imagenamen an.
- **Imagebeschreibung** —Fügen Sie eine Bildbeschreibung hinzu.
- **Datei** - Suchen Sie von Ihrem lokalen Laufwerk nach der kvm.qcow2-Imagedatei und wählen Sie sie aus.
- **Format** —Wählen Sie das Datenträgerformat QCOW2 —QEMU Emulator aus der Dropdownliste aus.

Klicken Sie auf **Image erstellen**.

Sowohl Netzwerk- als auch Netzwerk-Port müssen zunächst erstellt und vordefiniert werden. So erstellen Sie einen Netzwerk-Port:

1. Wählen Sie unter **Netzwerk** die Option **Netzwerke** aus und gehen Sie zur Registerkarte **Port**.
2. Klicken Sie auf **Port erstellen**, geben Sie die erforderlichen Details an und klicken Sie auf Erstellen.

Create Port ✕

Info

Security Groups

Name

Mgt-port

☒ Enable Admin State

Device ID ?

Device Owner ?

Specify IP address or subnet ?

Fixed IP Address ▼

Fixed IP Address* ?

10.106.36.xx|

MAC Address ?

☒ Port Security ?

VNIC Type ?

Normal ▼

Description:

You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.

Cancel

Create

Wenn Sie **Feste IP-Adresse** auswählen, müssen Sie die Subnetz-IP-Adresse für den neuen Port angeben.

Project / Network / Networks / public

public

Overview Subnets Ports

Ports

Filter

+ Create Port

Delete Ports

Displaying 12 items

| Name | Fixed IPs | MAC Address | Attached Device | Status | Admin State | Actions |
|-----------------|--------------|-------------------|------------------|--------|-------------|-----------|
| Mgt-Port | 10.106.36.41 | fa:16:3e:24:8a:8c | Detached | Down | UP | Edit Port |
| (0b1273e8-1205) | 10.106.36.31 | fa:16:3e:c4:bc:eb | compute:compute1 | Active | UP | Edit Port |
| test1 | 10.106.36.36 | fa:16:3e:52:2d:8b | compute:compute2 | Active | UP | Edit Port |
| tiny_mgmt | 10.106.36.44 | fa:16:3e:8d:83:04 | Detached | Down | UP | Edit Port |

Der Port wird erstellt und da er nicht an ein Gerät angeschlossen ist, wird der aktuelle Status als Detached angezeigt.

Erstellen Sie OpenStack-Instanz, um config-drive zu aktivieren und die user_data zu übergeben.

3. Melden Sie sich bei OpenStack an und konfigurieren Sie Instanzen.

Project / Compute / Instances

Instances

Instance ID

Filter

Launch Instance

Delete Instances

More Actions

Displaying 9 items

| Instance Name | Image Name | IP Address | Flavor | Key Pair | Status | Availability Zone | Task | Power State | Age | Actions |
|---------------------|------------------|---|-----------|----------|--------|-------------------|------|-------------|----------------|-----------------|
| router_image | test_linux | 10.106.36.43 | m1.medium | - | Active | compute1 | None | Running | 1 day, 5 hours | Create Snapshot |
| sdwan-11configd ata | sdwan-finalti ny | 10.106.36.36 | m1.large | - | Active | compute2 | None | Running | 1 week, 1 day | Create Snapshot |
| sdwan-release11 | sdwan-finalti ny | 10.106.36.31 | m1.large | - | Active | compute1 | None | Running | 1 week, 1 day | Create Snapshot |
| sdwan-sample | sdwan_priv | test_3 172.16.12.44 public 10.106.36.42 test_1 172.16.10.67 | m1.large | - | Active | compute2 | None | Running | 1 week, 1 day | Create Snapshot |

4. Laden Sie die **kvm.qcow2.gz-Datei** herunter und entpacken Sie sie.

5. Gehen Sie zu **Instances** und klicken Sie auf **Launch Instance**

HINWEIS

Sie können zu **Instances** zurückkehren und auf **Launch Instance** klicken oder im Bildschirm Images auf **Launch** klicken, sobald das Image erstellt wurde.

| | | | | | | | | |
|-------|-----------------|-------|--------|--------|----|-------|---------|--------|
| admin | sdwan-finaltiny | Image | Active | Public | No | QCOW2 | 1.33 GB | Launch |
| admin | sdwan_mtu_check | Image | Active | Public | No | QCOW2 | 1.32 GB | Launch |
| admin | sdwan_priv | Image | Active | Public | No | QCOW2 | 1.29 GB | Launch |

6. Geben Sie auf der Registerkarte **Details** die folgenden Informationen an:

- Instanzname** —Geben Sie den Hostnamen für die Instance an.
- Beschreibung** —Fügt eine Beschreibung für die Instanz hinzu.

- **Availability Zone** —Wählen Sie die Availability Zone aus der Dropdown-Liste aus, in der Sie die Instanz bereitstellen möchten.
- **Count** —Geben Sie die Instanzanzahl ein Sie können die Anzahl erhöhen, um mehrere Instanzen mit denselben Einstellungen zu erstellen. Klicken Sie auf **Weiter**.

Launch Instance

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *
sdwan-openstack

Description

Availability Zone
Any Availability Zone

Count *
1

Total Instances (30 Max)
40%
11 Current Usage
1 Added
18 Remaining

Details
Source *
Flavour *
Networks *
Network Ports
Security Groups
Key Pair
Configuration
Server Groups
Scheduler Hints
Metadata

Buttons: **Cancel**, **< Back**, **Next >** (highlighted), **Launch Instance**

7. Wählen Sie auf der Registerkarte **Quelle** unter **Neues Volume erstellen** die Option **Nein** aus und klicken Sie auf **Weiter**. Instanzquelle ist die Vorlage, die zum Erstellen einer Instanz verwendet wird.

Launch Instance

Details

Source *

Flavour *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source

Image

Create New Volume

Yes

No

Allocated

| Name | Updated | Size | Type | Visibility |
|---|---------|------|------|------------|
| Select an item from Available items below | | | | |

Available 10

Select one

Q

Click here for filters or full text search.

X

| Name | Updated | Size | Type | Visibility | |
|---------------------|------------------|----------|-------|------------|---|
| > cirros | 8/7/19 9:25 PM | 12.65 MB | qcow2 | Public | ↑ |
| > sdwan-finaltiny | 11/7/19 10:42 AM | 1.33 GB | qcow2 | Public | ↑ |
| > sdwan_mtu_check | 8/19/19 1:34 PM | 1.32 GB | qcow2 | Public | ↑ |
| > sdwan_priv | 11/5/19 10:34 AM | 1.29 GB | qcow2 | Public | ↑ |
| > SDWAN_VPX_IMG_NEW | 8/8/19 8:31 PM | 1.31 GB | qcow2 | Public | ↑ |
| > test_branch_1 | 10/4/19 10:07 AM | 1.72 GB | qcow2 | Public | ↑ |
| > test_brnach_2 | 10/4/19 10:08 AM | 1.72 GB | qcow2 | Public | ↑ |
| > test_dynamips | 10/4/19 10:06 AM | 1.72 GB | qcow2 | Public | ↑ |
| > test_linux | 10/4/19 10:07 AM | 1.72 GB | qcow2 | Public | ↑ |
| > test_mcn | 10/4/19 10:08 AM | 1.72 GB | qcow2 | Public | ↑ |

Cancel

< Back

Next >

Launch Instance

8. Wählen Sie **Flavour** für die Instanz aus und klicken Sie auf Weiter. Das für eine Instanz ausgewählte Flavour verwaltet die Menge an Rechen-, Speicher- und Speicherkapazität der Instanz.

HINWEIS:

Dem ausgewählten Flavour müssen genügend Ressourcen zugewiesen sein, um den Instanztyp zu unterstützen, den Sie erstellen möchten. Flavours, die nicht genügend Ressourcen für Ihre Instanz bereitstellen, werden in der verfügbaren Tabelle mit einem gelben Warnsymbol gekennzeichnet.

Administratoren sind für die Erstellung und Verwaltung von Geschmacksrichtungen verantwortlich. Klicken Sie auf den Pfeil (rechts), den Sie zuweisen möchten.

Launch Instance

Details

Source *

Flavour

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Flavours manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

| Name | VCPUS | RAM | Total Disk | Root Disk | Ephemeral Disk | Public |
|------------|-------|------|------------|-----------|----------------|--------|
| > m1.large | 4 | 8 GB | 80 GB | 80 GB | 0 GB | Yes |

Available 4

Select one

Click here for filters or full text search.

| Name | VCPUS | RAM | Total Disk | Root Disk | Ephemeral Disk | Public |
|-------------|-------|--------|------------|-----------|----------------|--------|
| > m1.tiny | 1 | 512 MB | 1 GB | 1 GB | 0 GB | Yes |
| > m1.small | 1 | 2 GB | 20 GB | 20 GB | 0 GB | Yes |
| > m1.medium | 2 | 4 GB | 40 GB | 40 GB | 0 GB | Yes |
| > m1.xlarge | 8 | 16 GB | 160 GB | 160 GB | 0 GB | Yes |

Cancel

Back

Next >

Launch Instance

9. Wählen Sie das Netzwerk aus und klicken Sie auf **Weiter**. Netzwerke stellen die Kommunikationskanäle für Instanzen bereit.

HINWEIS:

Ein Administrator wird die Provider-Netzwerke erstellt, und diese Netzwerke sind einem vorhandenen physischen Netzwerk im Rechenzentrum zugeordnet. Ähnlich werden Projekt-Netzwerke von Benutzern erstellt, und diese Netzwerke sind vollständig isoliert und projektspezifisch.

Launch Instance

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud.

▼ Allocated 1

Select networks from those listed below.

| Network | Subnets Associated | Shared | Admin State | Status |
|------------|--------------------|--------|-------------|--------|
| 1 > public | public_subnet | Yes | Up | Active |

▼ Available 30

Select at least one network

Q

Click here for filters or full text search.

×

| Network | Subnets Associated | Shared | Admin State | Status |
|--|--------------------------------------|--------|-------------|--------|
| > 08c39ca9-c86e-4e80-8dd2-5b775497069c | 09408ac1-6dfb-4381-bd2b-34c128f5280c | No | Up | Active |
| > 0ce9e8b1-ad5d-4210-87dc-62917c827c17 | 76268f54-7faf-45ff-ae2a-b97fb72e3d6b | No | Up | Active |
| > 26a6e41d-6f64-4f6b-b510-810938d9a669 | c81c3a0e-e84e-46b1-9e29-3300b8e7323c | No | Up | Active |
| > 272165f0-443b-4f81-9358-38a9e2ea0fa3 | 373b775b-9576-484d-abd8-9011362284da | No | Up | Active |
| > test_4 | subnet_4 | No | Up | Active |
| > 8b69e4a3-c47a-4821-bb17-09aca96a4fe9 | ab3c53f6-ca4b-4958-aedf-7c444b21c257 | No | Up | Active |
| > test_1 | subnet_1 | No | Up | Active |
| > Hw_provider3_vlan20 | provider3_subnet | No | Up | Active |
| > f1d4edbe-8272-400c-bba1-c350864eecd | 366f5024-cf0a-4648-8053-c3fe946df958 | No | Up | Active |
| > f3158a09-c8dc-421a-9e8f-04814860b955 | 736e9da4-7526-4072-aa93-666071df24f8 | No | Up | Active |
| > test_3 | subnet_3 | No | Up | Active |
| > network_ipv6 | subnetwork_ipv6 ipv4_subnet | No | Up | Active |

✕ Cancel

< Back

Next >

Launch Instance

10. Wählen Sie einen Netzwerkport für die Instanz und klicken Sie auf **Weiter**. Netzwerkports stellen zusätzliche Kommunikationskanäle für die Instanzen bereit.

HINWEIS:

Sie können Ports anstelle von Netzwerken oder eine Mischung aus beiden auswählen.

Launch Instance

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both.

▼ Allocated 1

Select ports from those listed below.

| Name | IP | Admin State | Status |
|---------------|--------------------------------------|-------------|--------|
| 1 > tiny_mgmt | 10.106.36.44 on subnet public_subnet | Up | Down |

▼ Available 31

Select one

Filter

| Name | IP | Admin State | Status |
|--|--------------------------------------|-------------|--------|
| > 3865f021-d8df-40a9-964a-7bb7f3728353 | 192.168.234.239 on subnet | Up | Down |
| > 3f7888d2-dd2b-487d-ad88-6cf3261ebf8b | 192.168.234.113 on subnet | Up | Down |
| > 7847377d-6f82-4a7f-9e8d-26703bfc7b0b | 192.168.234.240 on subnet | Up | Down |
| > 2bd26300-4af2-4503-8ec8-728ad5967c5f | 192.168.237.88 on subnet | Up | Down |
| > 6ca1aeab-4b38-41f3-86cc-8973a3bfc3bd | 192.168.240.223 on subnet | Up | Down |
| > 9dc0d02b-7933-4689-92a3-18c3177c7c0d | 192.168.240.251 on subnet | Up | Down |
| > c378ba39-0c61-4e35-8a2c-0419fa8c2989 | 192.168.240.4 on subnet | Up | Down |
| > 958ad235-94b0-4ccd-8f07-88539bc5b584 | 172.16.22.1 on subnet | Up | Down |
| > Mgt-Port | 10.106.36.41 on subnet public_subnet | Up | Down |

✕ Cancel

< Back

Next >

Launch Instance

11. Gehen Sie zu **Configuration** und klicken Sie auf **Choose file** Wählen Sie die **user_daten** Datei aus. Sie können die **Management-IP**-, **DNS**- und **Seriennummerninformationen** in der Datei **user_data** anzeigen.
12. Aktivieren Sie das Kontrollkästchen **Konfigurationslaufwerk**. Wenn Sie das Konfigurationslaufwerk aktivieren, können Sie die Benutzermetadaten in das Image einfügen.

Launch Instance

You can customise your instance after it has launched using the options available here. "Customisation Script" is analogous to "User Data" in other systems.

Load Customisation Script from a file

Choose file No file chosen

Customisation Script (Modified) Content size: 213 bytes of 16.00 KB

```
#config
management_ip
address 10.106.36.43
netmask 255.255.255.0
gateway 10.106.36.1
dns
```

Disk Partition

Automatic

☒ Configuration Drive

✕ Cancel < Back Next > Launch Instance

13. Klicken Sie auf **Launch Instance**.

Konfigurieren der LTE-Funktionalität auf 210 SE LTE-Appliance

September 26, 2023

Sie können eine Citrix SD-WAN 210-SE LTE-Appliance über eine LTE-Verbindung mit Ihrem Netzwerk verbinden. In diesem Thema finden Sie Details zum Konfigurieren mobiler Breitbandeinstellungen, zum Konfigurieren des Rechenzentrums und der Zweigstellen für LTE usw. Weitere Informationen zur Citrix SD-WAN 210-SE LTE-Hardwareplattform finden Sie unter [Citrix SD-WAN 210 Standard Edition Appliances](#).

Hinweis

Die LTE-Konnektivität hängt vom SIM-Netzbetreiber oder Dienstanbieter-Netzwerk ab.

Erste Schritte mit Citrix SD-WAN 210-SE LTE

1. Legen Sie die SIM-Karte in den SIM-Kartensteckplatz des Citrix SD-WAN 210-SE LTE ein.

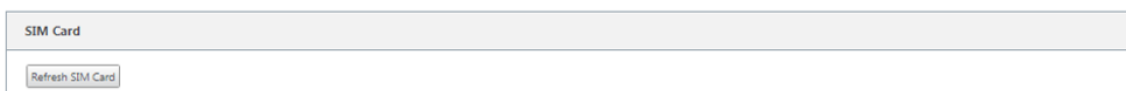
Hinweis:

Es wird nur eine Standard- oder 2FF-SIM-Karte (15x25 mm) unterstützt.

2. Befestigen Sie die Antennen an der Citrix SD-WAN 210-SE LTE-Einheit. Weitere Informationen finden Sie unter [Installieren der LTE-Antennen](#).
3. Schalten Sie die Appliance ein.

Hinweis

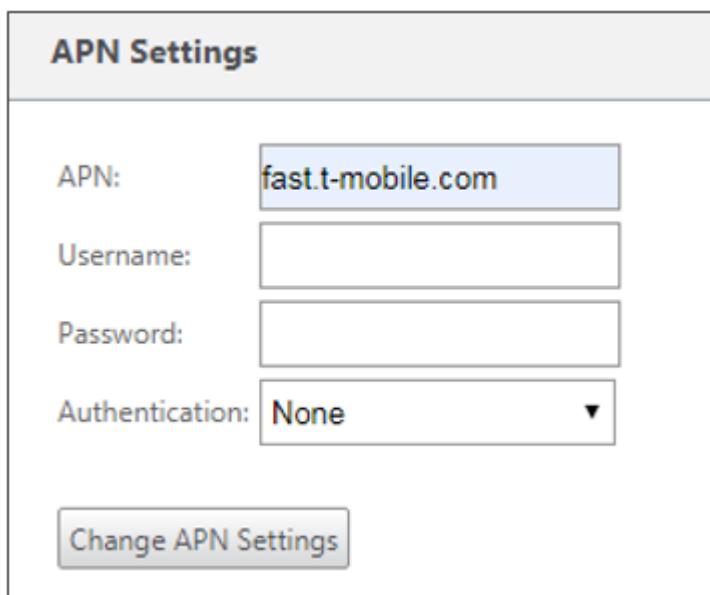
Wenn Sie die SIM-Karte in eine Appliance eingelegt haben, die bereits eingeschaltet und hochgefahren ist, navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband > SIM-Karte** und klicken Sie auf **SIM-Karte aktualisieren**.



4. Konfigurieren Sie die APN-Einstellungen. Navigieren Sie in der SD-WAN GUI zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband > APN-Einstellungen**.

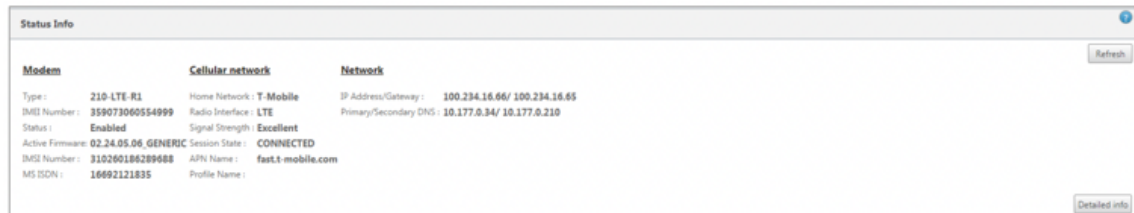
Hinweis:

Rufen Sie die APN-Informationen vom Anbieter ab.



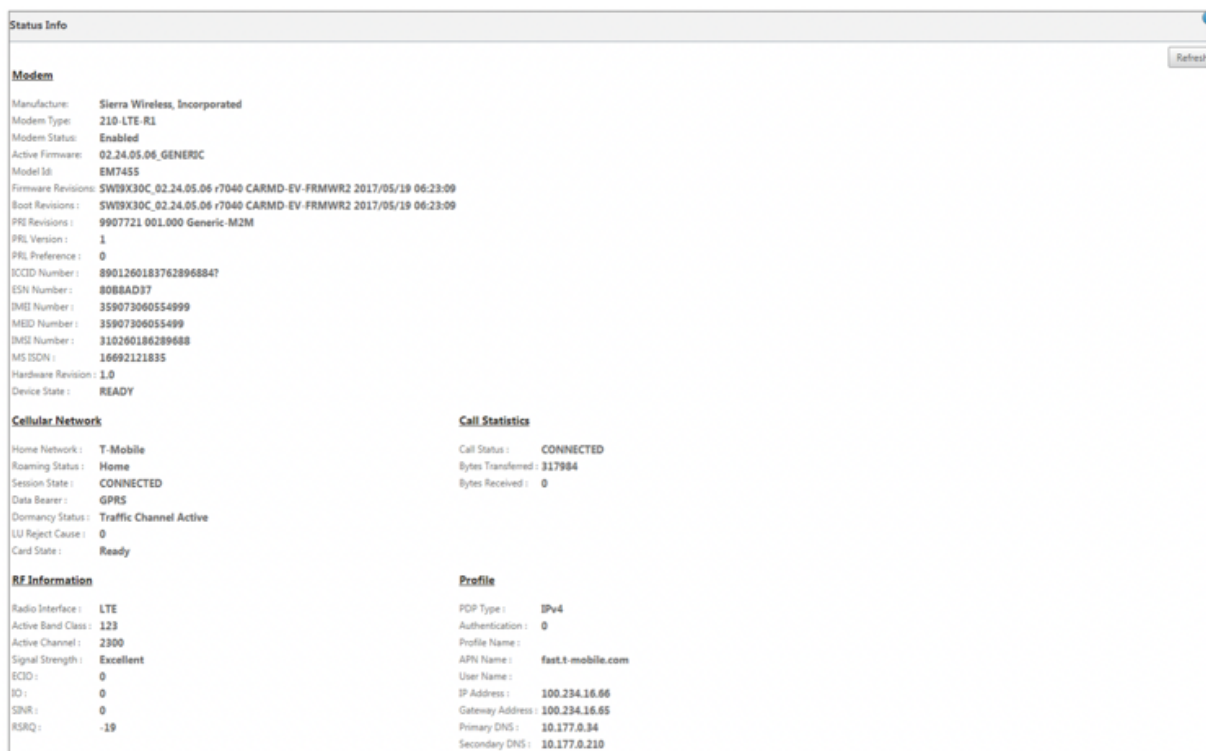
5. Geben Sie den **APN**, den **Benutzernamen**, das **Kennwort** und die **Authentifizierung** ein, die vom Anbieter bereitgestellt werden. Sie können zwischen PAP, CHAP, PAPCHAP Authentifizierungsprotokollen wählen. Wenn der Anbieter keinen Authentifizierungstyp angegeben hat, setzen Sie ihn auf **Keine**.
6. Klicken Sie auf **APN-Einstellungen ändern**.
7. Navigieren Sie in der GUI der SD-WAN-Appliance zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband**.

Sie können die Statusinformationen für mobile Breitbandeinstellungen anzeigen.



Im Folgenden finden Sie einige nützliche Statusinformationen:

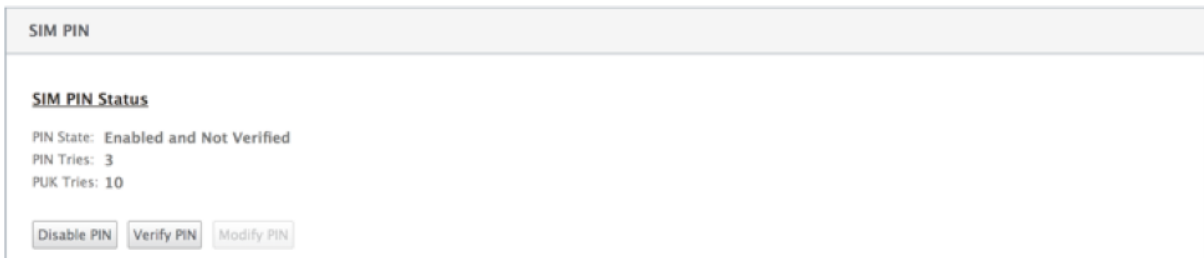
- **Betriebsart:** Zeigt den Modemstatus an.
- **Aktive SIM:** Zu einem bestimmten Zeitpunkt kann nur eine SIM aktiv sein. Die aktuell aktive SIM wird angezeigt.
- **Kartenstatus:** Vorhanden zeigt an, dass die SIM ordnungsgemäß eingelegt ist.
- **Signalstärke:** Qualität der Signalstärke - ausgezeichnet, gut, fair, schlecht oder kein Signal.
- **Heimnetzwerk:** Träger der eingelegten SIM-Karte.
- **APN-Name:** Der vom LTE-Modem verwendete Zugriffspunktname.
- **Sitzungsstatus:** Verbunden zeigt an, dass das Gerät dem Netzwerk beigetreten ist. Wenn der Sitzungsstatus getrennt ist, prüfen Sie beim Anbieter, ob das Konto aktiviert wurde, ob der Datentarif aktiviert ist.



SIM-PIN

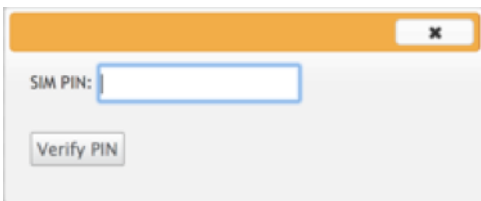
Wenn Sie eine SIM-Karte eingelegt haben, die mit einer PIN gesperrt ist, lautet der SIM-Status Aktiviert und Nicht** verifiziert. Sie können die SIM-Karte erst verwenden, wenn sie mit der SIM-PIN verifiziert wurde. Sie können die SIM-PIN vom Anbieter erhalten.

Um SIM-PIN-Vorgänge durchzuführen, navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Mobiles Breitband > SIM-PIN**.



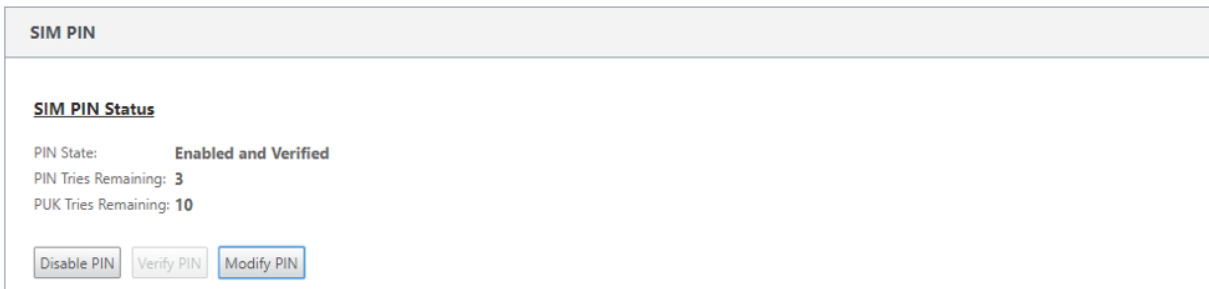
The screenshot shows the 'SIM PIN' configuration page. Under the 'SIM PIN Status' section, the 'PIN State' is 'Enabled and Not Verified', 'PIN Tries' are 3, and 'PUK Tries' are 10. At the bottom, there are three buttons: 'Disable PIN', 'Verify PIN', and 'Modify PIN'.

Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.



The screenshot shows a dialog box for PIN verification. It has a title bar with a close button. Inside, there is a label 'SIM PIN:' followed by a text input field. Below the input field is a 'Verify PIN' button.

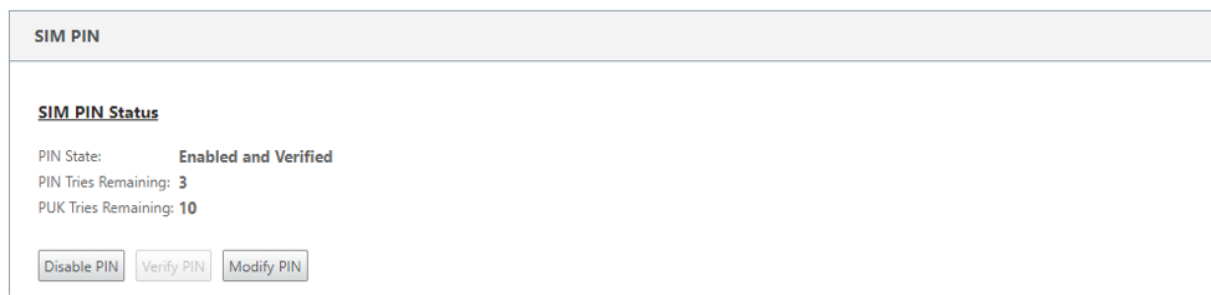
Der Status ändert sich in **Aktiviert und Verifiziert**.



The screenshot shows the 'SIM PIN' configuration page after verification. The 'PIN State' is now 'Enabled and Verified', 'PIN Tries Remaining' are 3, and 'PUK Tries Remaining' are 10. The 'Verify PIN' button is now highlighted with a blue border.

SIM-PIN deaktivieren

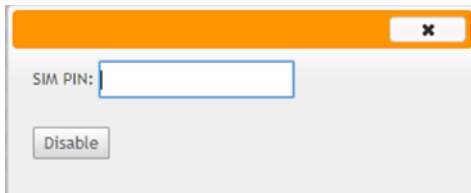
Sie können die SIM-PIN-Funktionalität für eine SIM-Karte deaktivieren, für die SIM-PIN aktiviert und verifiziert ist.



SIM PIN

SIM PIN Status

PIN State: **Enabled and Verified**
PIN Tries Remaining: **3**
PUK Tries Remaining: **10**

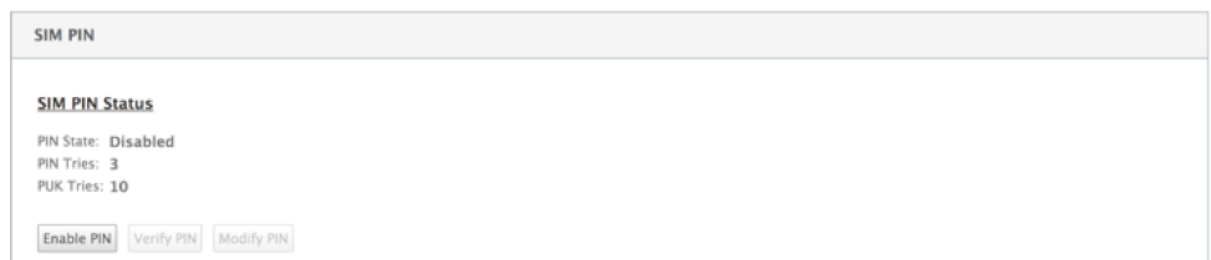


SIM PIN:

Klicken Sie auf **PIN deaktivieren**. Geben Sie die **SIM-PIN** ein und klicken Sie auf **Deaktivieren**.

SIM-PIN aktivieren

Die SIM-PIN kann für die SIM aktiviert werden, für die sie deaktiviert ist.

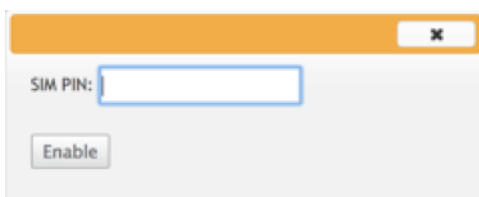


SIM PIN

SIM PIN Status

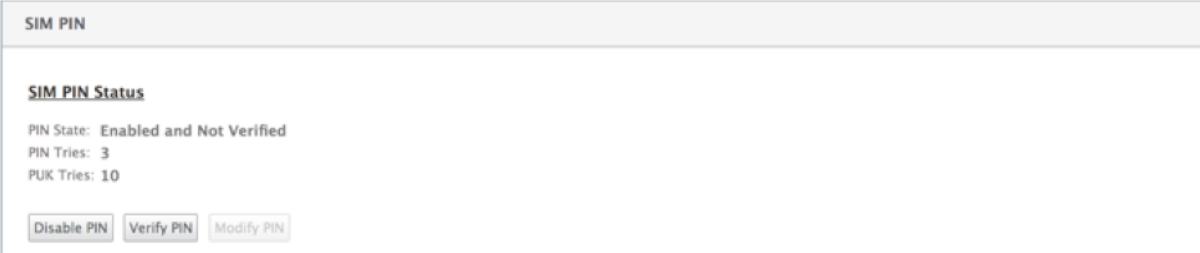
PIN State: **Disabled**
PIN Tries: **3**
PUK Tries: **10**

Klicken Sie auf **PIN aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**.



SIM PIN:

Wenn sich der SIM-PIN-Status in **Aktiviert und Nicht überprüft** ändert, bedeutet dies, dass die PIN nicht überprüft wird und Sie erst dann LTE-bezogene Vorgänge ausführen können, wenn die PIN überprüft wurde.



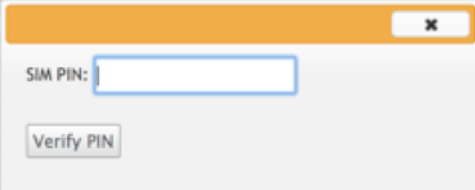
SIM PIN

SIM PIN Status

PIN State: Enabled and Not Verified
PIN Tries: 3
PUK Tries: 10

Disable PIN Verify PIN Modify PIN

Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.

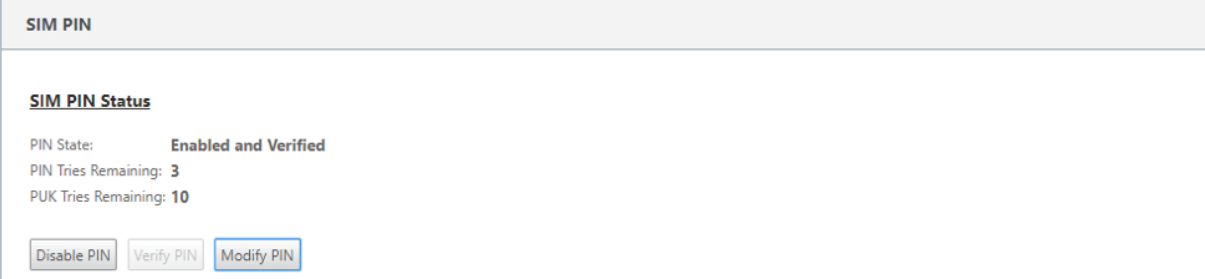


SIM PIN:

Verify PIN

SIM-PIN ändern

Sobald die PIN im Status **Aktiviert und Verifiziert** ist, können Sie die PIN ändern.



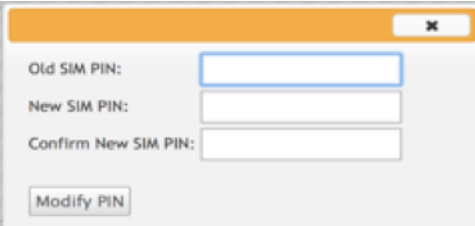
SIM PIN

SIM PIN Status

PIN State: Enabled and Verified
PIN Tries Remaining: 3
PUK Tries Remaining: 10

Disable PIN Verify PIN Modify PIN

Klicken Sie auf **PIN ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **PIN ändern**.



Old SIM PIN:

New SIM PIN:

Confirm New SIM PIN:

Modify PIN

SIM aufheben

Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe der vom Träger erhaltenen SIM-PUK zurücksetzen.

| IP Address | Ethernet | Mobile Broadband |
|--|----------|------------------|
| Status Info | | |
| This SIM Card is Blocked . Please contact the carrier service for a PUK code to unblock the SIM card. | | |
| PIN State: Blocked | | |
| PIN Tries: 3 | | |
| PUK Tries: 10 | | |
| <input type="button" value="Unblock"/> | | |

Um die Blockierung einer SIM aufzuheben, klicken Sie auf **Sperre aufheben**. Geben Sie die vom Netzbetreiber erhaltene **SIM-PIN** und **SIM-PUK** ein und klicken Sie auf **Entsperren**.

SIM PIN:

SIM PUK:

Hinweis:

Die SIM-Karte wird mit 10 erfolglosen PUK-Versuchen dauerhaft blockiert, während die SIM-Karte entsperrt wird. Sie müssen sich an den Anbieter für eine neue SIM-Karte wenden.

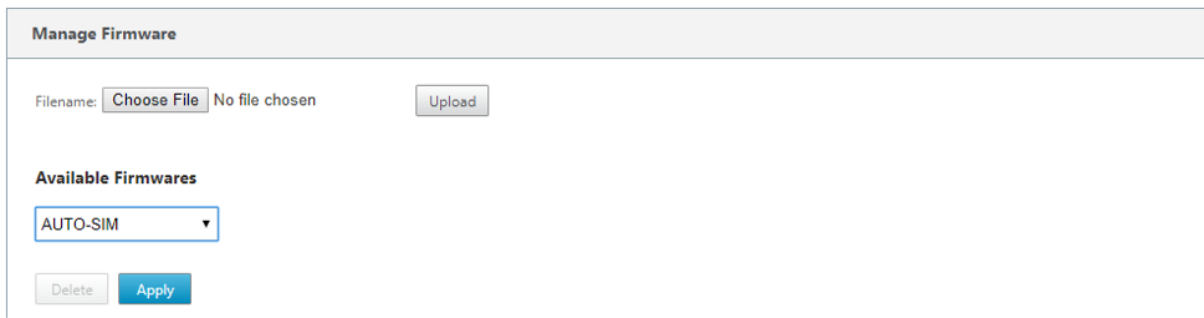
Configuration > Appliance Settings > Network Adapters

| IP Address | Ethernet | Mobile Broadband |
|--|----------|------------------|
| Status Info | | |
| This SIM Card is Permanently Blocked . Please contact the carrier service for a new SIM card. | | |

Firmware verwalten

Jedes Gerät, das LTE aktiviert hat, verfügt über eine Reihe verfügbarer Firmware. Sie können aus der vorhandenen Firmware-Liste auswählen oder eine Firmware hochladen und anwenden.


Wenn Sie sich nicht sicher sind, welche Firmware Sie verwenden sollen, wählen Sie die Option AUTO-SIM, damit das LTE-Modem die am besten passende Firmware basierend auf der eingelegten SIM-Karte auswählen kann.



The **Manage Firmware** interface includes a file upload section with a 'Filename:' label, a 'Choose File' button, the text 'No file chosen', and an 'Upload' button. Below this is the **Available Firmwares** section, which features a dropdown menu currently set to 'AUTO-SIM'. At the bottom of this section are 'Delete' and 'Apply' buttons.

Netzwerkeinstellungen


Sie können das Mobilfunknetz auf Citrix SD-WAN Appliances auswählen, die internes LTE-Modem unterstützen. Die unterstützten Netzwerke sind 3G, 4G oder beides.



The **Network Settings** interface shows a 'Network Type' dropdown menu with a list of options: '3G', '4G' (which is selected and marked with a checkmark), and 'Both'. An 'Apply' button is located at the bottom left of the settings panel.

Roaming

Die Roaming-Option ist standardmäßig auf Ihren LTE-Appliances aktiviert. Sie können sie deaktivieren.



The **Roaming** interface features a 'Roaming:' dropdown menu currently set to 'Disabled'. An 'Apply' button is positioned at the bottom left of the panel.

Modem aktivieren/deaktivieren

Aktivieren/deaktivieren Sie das Modem abhängig von Ihrer Absicht, die LTE-Funktionalität zu verwenden. Standardmäßig ist das LTE-Modem aktiviert.

Modem neu starten

Startet das Modem neu. Es kann bis zu 3-5 Minuten dauern, bis der Neustartvorgang abgeschlossen ist.

SIM aktualisieren

Verwenden Sie diese Option, wenn Sie die SIM-Karte per Hot-Swap austauschen, um die neue SIM-Karte durch das 210-SE LTE-Modem zu erkennen.

The screenshot shows the Citrix SD-WAN Center web interface. The 'Manage Firmware' section includes a 'Filename' field with a 'Choose File' button and an 'Upload' button. Below it, the 'Available Firmwares' section shows a dropdown menu set to 'AUTO-SIM' and 'Delete' and 'Apply' buttons. The 'Enable/Disable Modem' section has a 'Disable Mobile Broadband' button. The 'Reboot Modem' section has a 'Reboot Modem' button. The 'SIM Card' section has a 'Refresh SIM Card' button.

Mit Citrix SD-WAN Center können Sie alle LTE-Standorte in Ihrem Netzwerk remote anzeigen und verwalten. Weitere Informationen finden Sie unter [Remote-LTE-Standortverwaltung](#).

Konfigurieren der LTE-Funktionalität mit CLI

Konfigurieren des 210-SE LTE-Modems mithilfe der CLI.

1. Melden Sie sich bei der Citrix SD-WAN Appliance-Konsole an.
2. Geben Sie an der Eingabeaufforderung den Benutzernamen und das Kennwort ein, um Zugriff auf die CLI-Schnittstelle zu erhalten.
3. Geben Sie an der Eingabeaufforderung den Befehl ein **lte**. Tippen Sie **>help**. Hier wird die Liste der für die Konfiguration verfügbaren LTE-Befehle angezeigt.

```
site210>lte
lte>help
status                # Show status
show                  # Show settings
disable               # Disable LTE modem
enable                # Enable LTE modem
apn <apn> [<user name> [<password> [<PAP|CHAP|PAPCHAP>]]] # Set APN
sim-power <off|on|reset> # Off, on, reset SIM card power
sim-pin <show>        # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin> # Modify SIM card PIN
sim-pin <unlock> <sim puk> <sim pin> # Unblock SIM card PIN
reboot                # Reboot modem
ping                  # Check if modem manager ready
list-fw               # List available firmware
apply-fw <fw>        # Apply the specified firmware
```


In der folgenden Tabelle sind die Beschreibungen des **LTE**-Befehls aufgeführt.

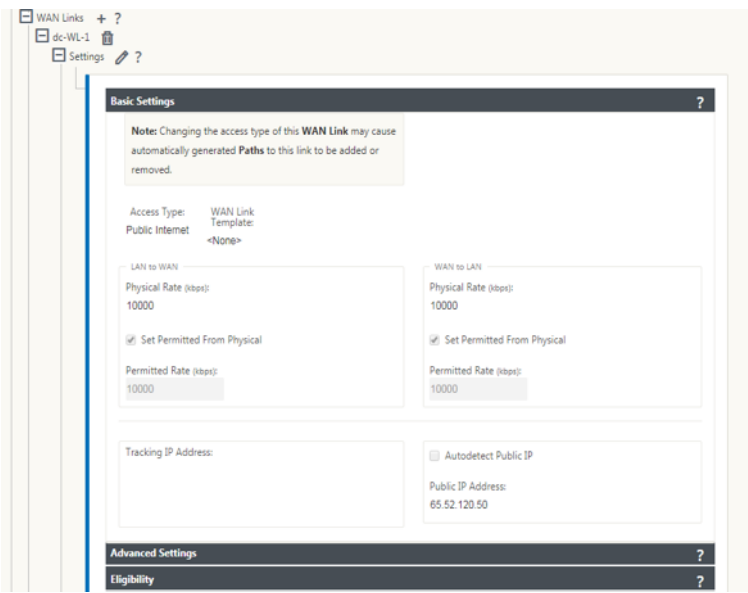
| Command | Beschreibung |
|--|--|
| Help {lte>help} | Listet die verfügbaren LTE-Befehle und -Parameter auf |
| Status {lte>status} | Zeigt den LTE-Konnektivitätsstatus an |
| Show {lte>show} | Zeigt LTE-Einstellungen an |
| Disable {lte>disable} | Deaktiviert das LTE-Modem |
| Aktiviere {lte>enable} | Aktiviert LTE-Modem |
| Apn {lte>apn} | Konfiguriert Informationen zu APN-Einstellungen |
| SIM-Energie aus, ein, zurücksetzen> {lte>sim-power off, on, reset} | Schaltet die SIM-Karte aus, Einschalten der SIM-Karte, Aktualisieren der SIM-Karte |
| SIM PIN {lte>sim-pin} | Schaltet die SIM-Karte aus, Einschalten der SIM-Karte, Aktualisieren der SIM-Karte |
| Reboot {lte>reboot} | Neustart des LTE-Modems |
| Ping {lte>ping} | Pings LTE-Modem |
| List-fw {lte>list-fw} | Listet die auf den R1- oder R2 LTE-Modems verfügbare Firmware auf |
| Apply-fw {lte>apply-fw} | Wendet Firmware spezifisch auf einen Spediteur an |

MCN für LTE konfigurieren

Sie können eine 210-LTE-Appliance nicht als MCN konfigurieren. Damit ein MCN jedoch mit einer LTE-Zweigeinheit arbeitet, führen Sie die folgenden Konfigurationen auf der MCN-Appliance durch.

So konfigurieren Sie einen MCN:

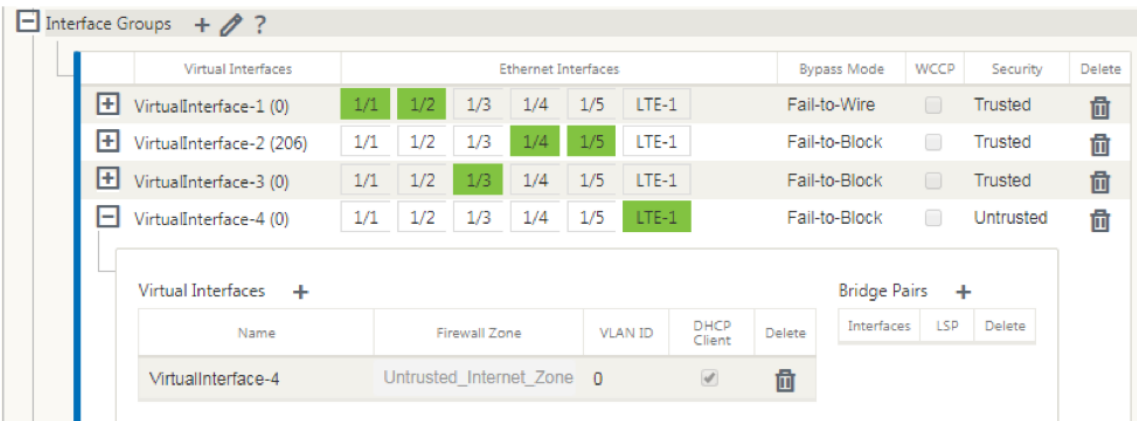
1. Melden Sie sich bei der GUI der SD-WAN-Appliance an. Wechseln Sie zum Konfigurationseditor. Vollständige Konfiguration für den MCN-Site, siehe [Konfigurieren von MCN](#).
2. Stellen Sie sicher, dass Sie routingfähige öffentliche IP-Adresse als Teil der WAN-Link-Konfiguration angeben. Sie müssen keine öffentliche IP-Adresse für Client-Appliances konfigurieren.



Zweig für LTE konfigurieren

So konfigurieren Sie die 210-SE LTE-Appliance als Zweigstelle:

1. Wechseln Sie in der Benutzeroberfläche der SD-WAN-Appliance zum Konfigurationseditor. Siehe [Zweig konfigurieren](#).
 - Erstellen Sie Schnittstellengruppen.
 - Erstellen Sie bis zu eine virtuelle Schnittstelle und eine Schnittstellengruppe für den LTE-Adapter, um die WAN-Verbindung zu konfigurieren, indem Sie Folgendes auswählen:
 - Ethernet-Schnittstelle —LTE 1
 - Sicherheit —nicht vertrauenswürdig (Standard)
 - DHCP-Client —Aktiviert (Standard)



2. Aktivieren Sie die **AutoDetect Public IP** für WAN-Verbindungskonfiguration, wenn Sie die WAN-Verbindung mithilfe der für die LTE-Schnittstelle erstellten virtuellen Schnittstelle

konfigurieren.

br210-WL-4

Settings

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Access Type: WAN Link

Public Internet Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

☒ Autodetect Public IP

Public IP Address:

Advanced Settings

3. Wenn Sie versuchen, WAN-Verbindung mithilfe der LTE-Schnittstelle zu konfigurieren, wird die WAN-Verbindung standardmäßig als Metered Link und Last Resort Standby-Modus markiert. Sie können diese Standardeinstellungen bei Bedarf ändern.

Advanced Settings

Eligibility

Metered/Standby Link

Metering

☒ Enable Metering

Data Cap (MB): 0

Billing Cycle: Monthly

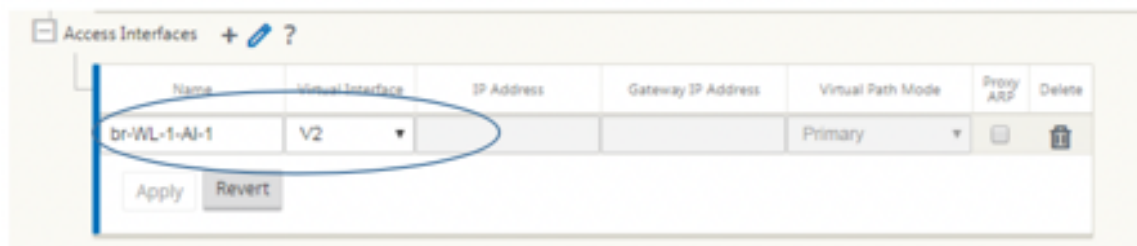
Starting From: MM/DD/YYYY

Standby

Standby Mode: Last-Resort

Priority: 1

Die IP-Adresse und die Gateway Adresse für die Access Interface der WAN-Verbindung müssen nicht konfiguriert werden, da sie diese Informationen vom Träger über DHCP empfängt.



4. Vollständiger Rest der erforderlichen Zweigkonfiguration für die 210-SE LTE-Appliance. Siehe [Zweig konfigurieren](#).
5. Führen Sie das Änderungsmanagement durch Hochladen der SD-WAN-Software durch. Siehe das [Change-Management-Verfahren](#).
6. Aktivieren Sie die Konfiguration über den lokalen Change Management-Prozess. Wenn Sie Change Management ausführen, wird die Konfiguration aktiviert und die erforderliche Konfiguration wird angewendet.

Zero-Touch-Bereitstellung über LTE

Voraussetzungen für die Aktivierung des Zero-Touch-Bereitstellungsdienstes über LTE

1. Installieren Sie die Antenne und die SIM-Karte für das 210-SE LTE-Gerät.
2. Stellen Sie sicher, dass die SIM-Karte über einen aktivierten Datenplan verfügt.
3. Stellen Sie sicher, dass der Management-Port nicht angeschlossen ist.
 - Wenn der Management-Port angeschlossen ist, trennen Sie den Management-Port und starten Sie die Appliance neu.
 - Wenn eine statische IP-Adresse auf der Verwaltungsschnittstelle konfiguriert ist, müssen Sie die Verwaltungsschnittstelle mit DHCP konfigurieren, die Konfiguration anwenden und dann den Management-Port trennen und die Appliance neu starten.
4. Stellen Sie sicher, dass für die 210-SE-Appliance-Konfiguration ein Internetdienst für die LTE-Schnittstelle definiert ist

Wenn die Appliance eingeschaltet ist, verwendet der Zero-Touch-Bereitstellungsdienst den LTE-Port, um die neueste SD-WAN-Software und SD-WAN-Konfiguration nur dann abzurufen, wenn der Management-Port nicht angeschlossen wurde.

Sie können die grafische Benutzeroberfläche des SD-WAN Centers verwenden, um die 210-SE LTE-Appliance für den Zero-Touch-Bereitstellungsdienst bereitzustellen und zu konfigurieren.

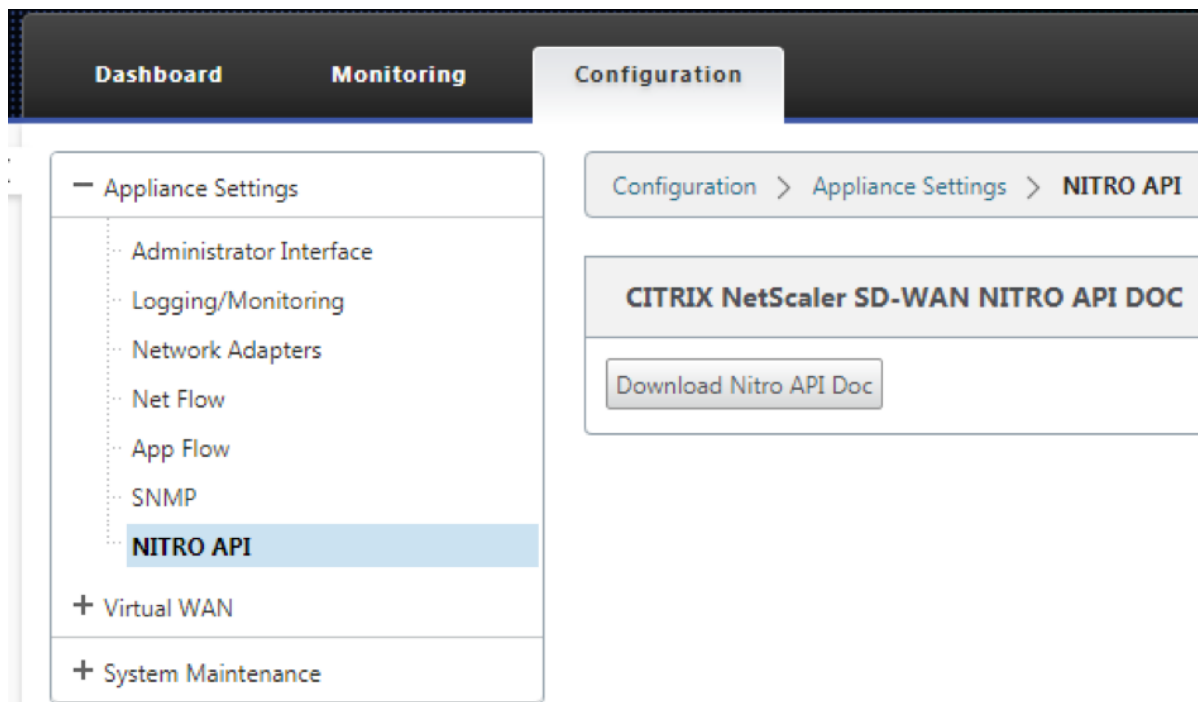
Weitere Informationen zur Bereitstellung und Konfiguration der 210-SE LTE-Appliance mit SD-WAN Center finden Sie im [Zero-Touch-Bereitstellungsverfahren](#).

Zero-Touch-Bereitstellungsdienst über Verwaltungsschnittstelle für 210-SE LTE-Appliance

Verbinden Sie den Management-Port und verwenden Sie das standardmäßige [Zero-Touch-Bereitstellungsverfahren](#), das auf allen anderen Nicht-LTE-Plattformen unterstützt wird.

LTE REST API

Informationen zur LTE REST-API erhalten Sie, wenn Sie zur SD-WAN GUI navigieren und zu **Konfiguration > Appliance-Einstellungen > NITRO-API** gehen. Klicken Sie auf **Nitro API Doc herunterladen**. Die REST-API für SIM-PIN-Funktionalität wird in Citrix SD-WAN 11.0 eingeführt.



Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Appliance

October 28, 2021

Sie können eine Citrix SD-WAN 110-LTE-WiFi-Appliance über eine LTE-Verbindung mit Ihrem Netzwerk verbinden. In diesem Thema finden Sie Details zum Konfigurieren mobiler Breitbandeinstellungen, zum Konfigurieren des Rechenzentrums und der Zweigstellen für LTE usw. Weitere Informationen zur Citrix 110-LTE-WiFi-Hardwareplattform finden Sie unter [Citrix SD-WAN 110 Standard Edition Appliances](#).

Hinweis

Die LTE-Konnektivität hängt vom SIM-Netzbetreiber oder Dienstanbieter-Netzwerk ab.

Erste Schritte mit Citrix SD-WAN 110-LTE-WiFi

1. Schalten Sie die Appliance ein, und legen Sie die SIM-Karte in den SIM-Karten-Steckplatz der Citrix SD-WAN 110-LTE-WiFi-Einheit ein.

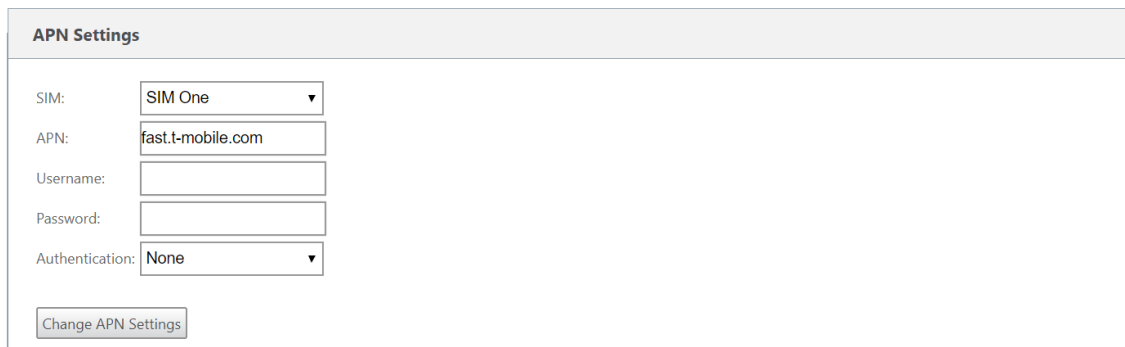
Hinweis

Die Citrix SD-WAN 110-LTE-WiFi-Appliance verfügt über zwei Standard-SIM-Steckplätze (2FF). Verwenden Sie einen SIM-Adapter, um SIMs der Größe Micro (3FF) und Nano (4FF) zu verwenden. Schnappen Sie die kleinere SIM in den Adapter ein. Sie können den Adapter von Citrix als Field Replaceable Unit (FRU) oder vom SIM-Anbieter beziehen.

2. Befestigen Sie die Antennen an der Citrix SD-WAN 110-LTE-WiFi-Einheit. Weitere Informationen finden Sie unter [Installieren der LTE-Antennen](#).
3. Schalten Sie die Appliance ein.
4. Konfigurieren Sie die APN-Einstellungen. Navigieren Sie in der SD-WAN GUI zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband > APN-Einstellungen**.

Hinweis

Rufen Sie die APN-Informationen vom Mobilfunkanbieter ab.



5. Wählen Sie die SIM-Karte aus, geben Sie den **APN**, den **Benutzernamen**, das **Kennwort** und die **Authentifizierung** ein, die vom Netzbetreiber bereitgestellt wurden. Sie können zwischen PAP, CHAP, PAPCHAP Authentifizierungsprotokollen wählen. Wenn der Anbieter keinen Authentifizierungstyp angegeben hat, setzen Sie ihn auf **Keine**.

Hinweis

Alle diese Felder sind optional.

6. Klicken Sie auf **APN-Einstellungen ändern**.
7. Navigieren Sie in der Benutzeroberfläche der **SD-WAN-Appliance** zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband**.

Sie können die Statusinformationen für mobile Breitbandeinstellungen anzeigen.

| Status Info | | | Refresh |
|---|-------------------------------------|--|---------------|
| Modem | Cellular network | Network | |
| Operating Mode: online | Home Network: airtel | IP Address/Gateway: 100.105.88.189/100.105.88.190 | Detailed info |
| IMEI Number: 867698040397609 | Radio Interface: lte | Primary/Secondary DNS: 125.22.47.102/59.144.144.106 | |
| Active SIM: SIM One | Signal Strength: Excellent | | |
| IMSI Number: 404450986042323 | Session State: connected | | |
| ICCID Number: 8991000902637718627f | APN Name: | | |
| Card State (SIM One): present | Card State (SIM Two): absent | | |

Im Folgenden finden Sie einige nützliche Statusinformationen:

- **Betriebsart:** Zeigt den Modemstatus an.
- **Aktive SIM:** Zu einem bestimmten Zeitpunkt kann nur eine SIM aktiv sein. Die aktuell aktive SIM wird angezeigt.
- **Kartenstatus:** Vorhanden zeigt an, dass die SIM ordnungsgemäß eingelegt ist.
- **Signalstärke:** Qualität der Signalstärke - ausgezeichnet, gut, fair, schlecht oder kein Signal.
- **Heimnetzwerk:** Träger der eingelegten SIM-Karte.
- **APN-Name:** Der vom LTE-Modem verwendete Zugriffspunktname.
- **Sitzungsstatus:** Verbunden zeigt an, dass das Gerät dem Netzwerk beigetreten ist. Wenn der Sitzungsstatus getrennt ist, erkundigen Sie sich beim Mobilfunkanbieter, ob das Konto aktiviert ist und der Datenplan aktiviert ist.

SIM-Präferenz

Sie können zwei SIMs auf einer Citrix SD-WAN 110-LTE-WiFi-Appliance einfügen. Zu einem bestimmten Zeitpunkt ist nur eine SIM aktiv. Wählen Sie die **SIM-Einstellung** aus:

- **SIM One bevorzugt:** Wenn zwei SIMs eingelegt sind, verwendet das LTE-Modem beim Hochfahren SIM One, falls verfügbar. Wenn das LTE-Modem eingeschaltet ist und läuft, verwendet es die SIM (SIM One oder SIM Two), die in diesem Moment verwendet werden kann. Es wird weiterhin verwendet, bis die SIM aktiv ist.

- **SIM Two bevorzugt:** Wenn zwei SIMs eingelegt sind, verwendet das LTE-Modem beim Hochfahren SIM Two, falls verfügbar. Wenn das LTE-Modem eingeschaltet ist und läuft, verwendet es die SIM (SIM One oder SIM Two), die in diesem Moment verwendet werden kann. Es wird weiterhin verwendet, bis die SIM aktiv ist.
- **SIM Eins:** Es wird nur SIM One verwendet, unabhängig vom SIM-Zustand auf beiden SIM-Steckplätzen. SIM One ist immer aktiv.
- **SIM Two:** Es wird nur SIM Two verwendet, unabhängig vom SIM-Status auf beiden SIM-Steckplätzen. SIM Two ist immer aktiv.

The screenshot shows a window titled "SIM Preference". Inside, there is a label "Preferred SIM:" followed by a dropdown menu currently set to "SIM One preferred". Below this is a blue button labeled "Apply".

SIM-PIN

Wenn Sie eine SIM-Karte eingelegt haben, die mit einer PIN gesperrt ist, ist der SIM-Status **aktiviert und nicht überprüft**. Sie können die SIM-Karte erst verwenden, wenn sie mit der SIM-PIN verifiziert wurde. Sie können die SIM-PIN vom Anbieter erhalten.

Hinweis

Die SIM-PIN-Vorgänge gelten nur für die aktive SIM.

Um SIM-PIN-Vorgänge durchzuführen, navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Mobiles Breitband > SIM-PIN**.

The screenshot shows a window titled "SIM PIN". Under the heading "SIM PIN Status", it displays the following information: "PIN State: enabled-not-verified", "PIN Retries Remaining: 3", and "PUK Retries Remaining: 10". At the bottom, there are four buttons: "Disable PIN", "Verify PIN", "Modify PIN", and "Unblock".

Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.

The screenshot shows a small dialog box with a title bar. Inside, there is a label "SIM PIN:" followed by a text input field. Below the input field is a button labeled "Verify PIN".

Der Status ändert sich in “**Aktiviert-verifiziert**”.

The screenshot shows a web interface for SIM PIN management. At the top, there's a header 'SIM PIN'. Below it, the section 'SIM PIN Status' displays the current status as 'enabled-verified'. It also shows 'PIN Retries Remaining: 3' and 'PUK Retries Remaining: 10'. At the bottom, there are four buttons: 'Disable PIN', 'Verify PIN', 'Modify PIN', and 'Unblock'.

SIM-PIN deaktivieren

Sie können die SIM-PIN-Funktionalität für eine SIM-Karte deaktivieren, für die SIM-PIN aktiviert und verifiziert ist.

This screenshot is identical to the one above, showing the 'SIM PIN Status' as 'enabled-verified' with buttons for 'Disable PIN', 'Verify PIN', 'Modify PIN', and 'Unblock'.

Klicken Sie auf **PIN deaktivieren**. Geb die **SIM-PIN** ein und klicke auf **Deaktivieren**

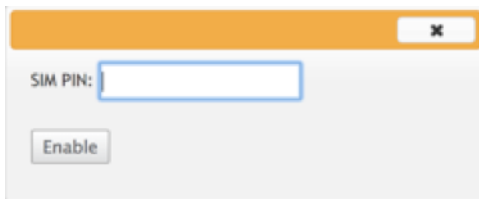
The screenshot shows a modal dialog box for deactivating the SIM PIN. It has an orange header bar with a close button (X). Inside, there's a label 'SIM PIN:' followed by a text input field. Below the input field is a button labeled 'Disable'.

SIM-PIN aktivieren

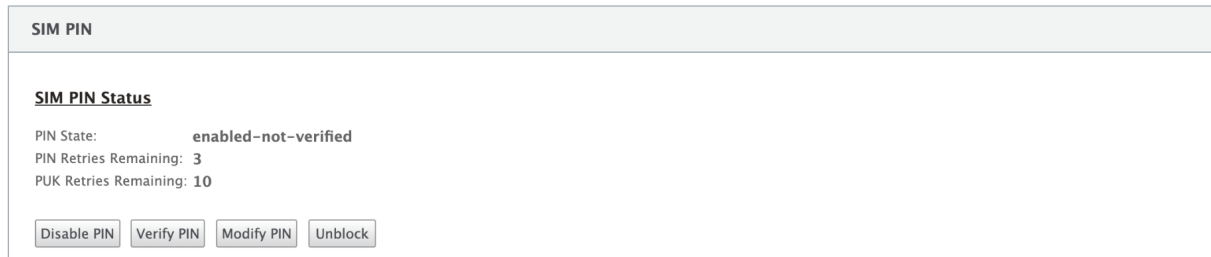
Die SIM-PIN kann für die SIM aktiviert werden, für die sie deaktiviert ist.

The screenshot shows the 'SIM PIN Status' page where the status is now 'disabled'. The 'PIN Retries Remaining' is still 3, and 'PUK Retries Remaining' is still 10. The buttons at the bottom are 'Enable PIN', 'Verify PIN', 'Modify PIN', and 'Unblock'.

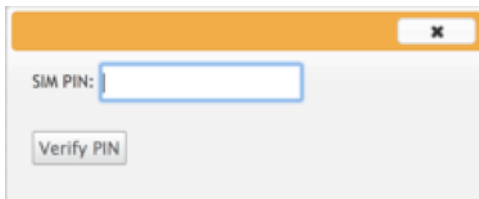
Klicken Sie auf **PIN aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**.



Wenn sich der SIM-PIN-Status in “**Nicht verifiziert**” ändert, bedeutet dies, dass die PIN nicht überprüft wird und Sie keine LTE-bezogenen Vorgänge ausführen können, bis die PIN überprüft wurde.

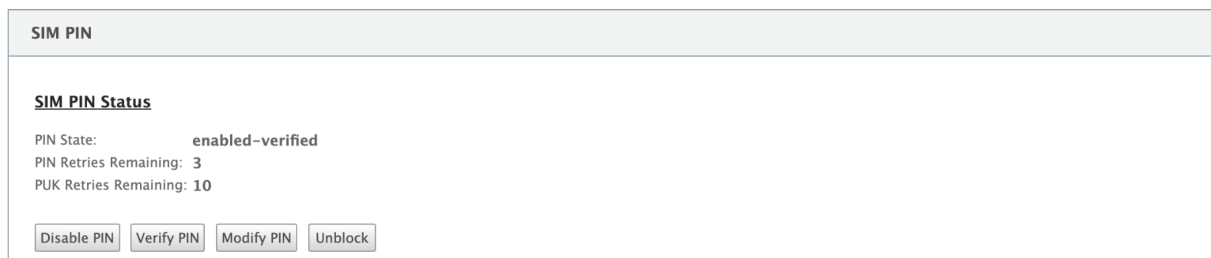


Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.

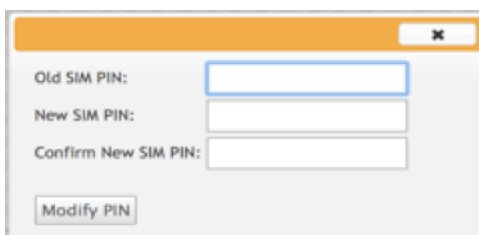


SIM-PIN ändern

Sobald sich die PIN im Status “**Aktiviert**” befindet, können Sie die PIN ändern.



Klicken Sie auf **PIN ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **PIN ändern**.



SIM aufheben

Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe der vom Träger erhaltenen SIM-PUK zurücksetzen.

The screenshot shows the 'Mobile Broadband' tab selected. Under 'Status Info', a message states: 'This SIM Card is **Blocked**. Please contact the carrier service for a PUK code to unblock the SIM card.' Below this, the status is detailed: 'PIN State: Blocked', 'PIN Tries: 3', and 'PUK Tries: 10'. An 'Unblock' button is visible at the bottom left of the status box.

Um die Blockierung einer SIM aufzuheben, klicken Sie auf **Sperre aufheben**. Geben Sie die **SIM-PIN** Ihrer Wahl ein. Geben Sie das vom Mobilfunkanbieter erhaltene **SIM-PUK** ein und klicken Sie auf **Entsperren**.

The dialog box has an orange header bar with a close button. It contains two input fields: 'SIM PIN:' and 'SIM PUK:'. Below the fields is an 'Unblock' button.

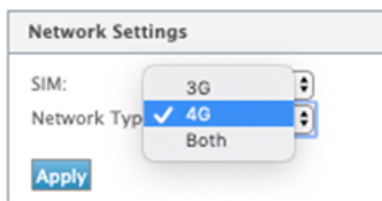
Hinweis:

Die SIM-Karte wird mit 10 erfolglosen PUK-Versuchen dauerhaft blockiert, während die SIM-Karte entsperrt wird. Sie müssen sich an den Anbieter für eine neue SIM-Karte wenden.

The screenshot shows the 'Configuration > Appliance Settings > Network Adapters' path. The 'Mobile Broadband' tab is selected. Under 'Status Info', a message states: 'This SIM Card is **Permanently Blocked**. Please contact the carrier service for a new SIM card.'

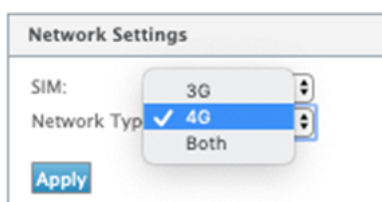
Netzwerkeinstellungen

Sie können das Mobilfunknetz auf den Citrix SD-WAN Appliances auswählen, die internes LTE-Modem unterstützen. Die unterstützten Netzwerke sind 3G, 4G oder beides.



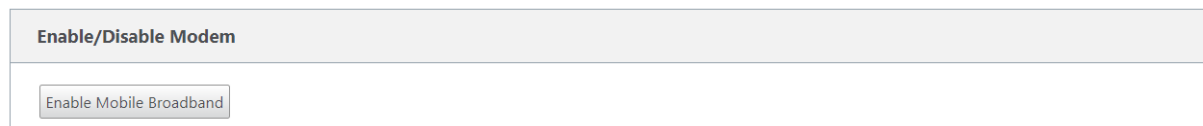
Roaming

Die Roaming-Option ist standardmäßig auf Ihren LTE-Appliances aktiviert. Sie können sie deaktivieren.



Modem aktivieren/deaktivieren

Aktivieren/deaktivieren Sie das Modem abhängig von Ihrer Absicht, die LTE-Funktionalität zu verwenden. Standardmäßig ist das LTE-Modem aktiviert.



Modem neu starten

Startet das Modem neu. Es kann bis zu 7 Minuten dauern, bis der Neustartvorgang abgeschlossen ist.

SIM aktualisieren

Verwenden Sie diese Option, wenn die SIM-Karte durch das 110-LTE-WiFi-Modem nicht richtig erkannt wird.

Hinweis

Der Vorgang SIM aktualisieren gilt nur für die aktive SIM.

SIM Card (SIM One)

Refresh SIM Card

Mit Citrix SD-WAN Center können Sie alle LTE-Standorte in Ihrem Netzwerk remote anzeigen und verwalten. Weitere Informationen finden Sie unter [Remote-LTE-Standortverwaltung](#).

Konfigurieren der LTE-Funktionalität mit CLI

So konfigurieren Sie das 110-LTE-WiFi-Modem mit CLI.

- 1. Melden Sie sich bei der Citrix SD-WAN Appliance-Konsole an.
- 2. Geben Sie an der Eingabeaufforderung den Benutzernamen und das Kennwort ein, um Zugriff auf die CLI-Schnittstelle zu erhalten.
- 3. Geben Sie an der Eingabeaufforderung den Befehl ein **lte**. Tippen Sie **>help**. Hier wird die Liste der für die Konfiguration verfügbaren LTE-Befehle angezeigt.

```
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
```

In der folgenden Tabelle sind die Beschreibungen des **LTE**-Befehls aufgeführt.

| Command | Beschreibung |
|---------------------|---|
| Help {lte>help} | Listet die verfügbaren LTE-Befehle und -Parameter auf |
| Status {lte>status} | Zeigt den LTE-Konnektivitätsstatus an |
| Show {lte>show} | Zeigt LTE-Einstellungen an |

| Command | Beschreibung |
|--|--|
| Disable {lte>disable} | Deaktiviert das LTE-Modem |
| Aktiviere {lte>enable} | Aktiviert LTE-Modem |
| Apn {lte>apn} | Konfiguriert Informationen zu APN-Einstellungen |
| SIM-Energie aus, ein, zurücksetzen> {lte>sim-power off, on, reset} | Schaltet die SIM-Karte aus, Einschalten der SIM-Karte, Aktualisieren der SIM-Karte |
| Wählen Sie [1l2] [1l2] {lte>select [1l2] [1l2]} | Wählen Sie die SIM für LTE-Modem aus. |
| SIM-Bevorzugen {lte>sim-prefer} | Wählen Sie die bevorzugte oder zu verwendende SIM aus. |
| SIM PIN {lte>sim-pin} | SIM-PIN-bezogene Vorgänge |
| Reboot {lte>reboot} | Neustart des LTE-Modems |

Hinweis

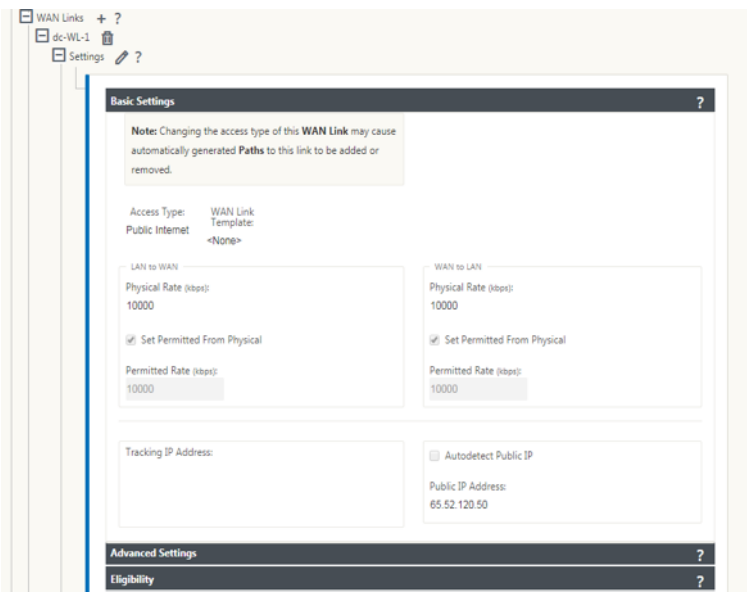
Die Firmware-Vorgänge werden von der 110-LTE-WiFi-Appliance nicht unterstützt.

MCN für LTE konfigurieren

Sie können eine 110-LTE-WiFi-Appliance nicht als MCN konfigurieren. Damit ein MCN jedoch mit einer LTE-Zweigeinheit arbeitet, führen Sie die folgenden Konfigurationen auf der MCN-Appliance durch.

So konfigurieren Sie einen MCN:

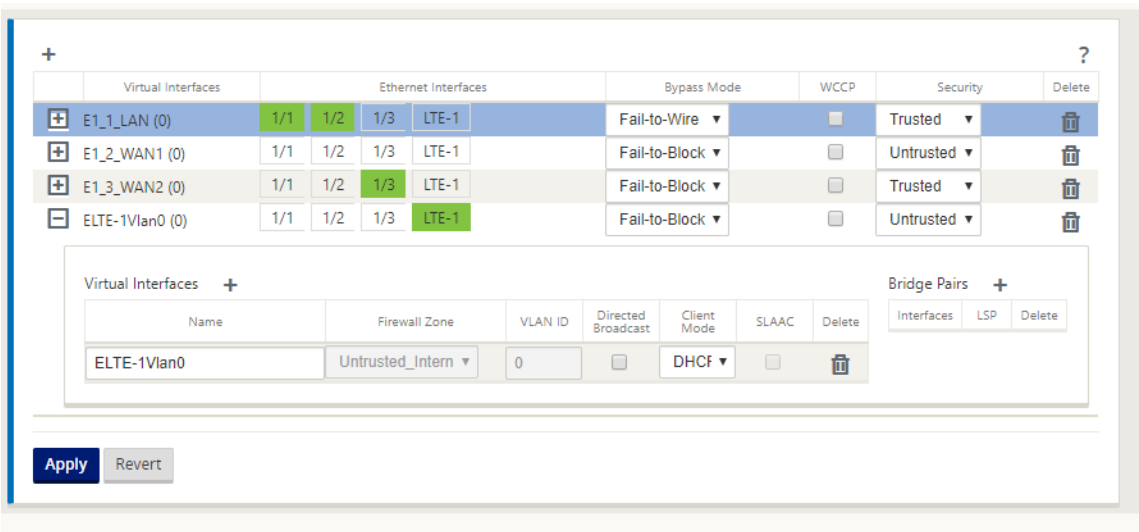
1. Melden Sie sich bei der GUI der SD-WAN-Appliance an. Wechseln Sie zum Konfigurationseditor. Schließen Sie die Konfiguration für den MCN-Site ab, siehe [MCN konfigurieren](#).
2. Stellen Sie sicher, dass Sie routingfähige öffentliche IP-Adresse als Teil der WAN-Link-Konfiguration angeben. Sie müssen keine öffentliche IP-Adresse für Client-Appliances konfigurieren.



Zweig für LTE konfigurieren

So konfigurieren Sie die 110-LTE-WiFi-Einheit als Zweigstandort:

1. Wechseln Sie in der Benutzeroberfläche der SD-WAN-Appliance zum Konfigurationseditor. Siehe [Zweig konfigurieren](#).
 - Erstellen Sie Schnittstellengruppen.
 - Erstellen Sie bis zu eine virtuelle Schnittstelle und eine Schnittstellengruppe für den LTE-Adapter, um die WAN-Verbindung zu konfigurieren, indem Sie Folgendes auswählen:
 - Ethernet-Schnittstelle —LTE 1
 - Sicherheit —nicht vertrauenswürdig (Standard)
 - DHCP-Client —Aktiviert (Standard)



2. Aktivieren Sie die **AutoDetect Public IP** für WAN-Verbindungskonfiguration, wenn Sie die WAN-Verbindung mithilfe der für die LTE-Schnittstelle erstellten virtuellen Schnittstelle konfigurieren.

The screenshot displays the configuration window for a WAN link named 'br210-WL-4'. The 'Basic Settings' tab is active, showing the 'Access Type' as 'WAN Link' and 'Public Internet'. A note indicates that changing the access type may affect automatically generated paths. Below this, there are two columns for 'LAN to WAN' and 'WAN to LAN' traffic. Each column has a 'Physical Rate (kbps)' and a 'Permitted Rate (kbps)' both set to 10000. There are checkboxes for 'Set Permitted From Physical' (checked) and 'Auto Learn' (unchecked). At the bottom, there is a 'Tracking IP Address' field and a checkbox for 'Autodetect Public IP' (checked), with a 'Public IP Address' field below it. The 'Advanced Settings' tab is visible at the bottom.

br210-WL-4 Settings ?

Basic Settings ?

Note: Changing the access type of this **WAN Link** may cause automatically generated **Paths** to this link to be added or removed.

Access Type: WAN Link
Public Internet Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

WAN to LAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 10000

☒ Autodetect Public IP

Public IP Address:

Advanced Settings ?

3. Wenn Sie versuchen, WAN-Verbindung mithilfe der LTE-Schnittstelle zu konfigurieren, wird die WAN-Verbindung standardmäßig als Metered Link und Last Resort Standby-Modus markiert. Sie können diese Standardeinstellungen bei Bedarf ändern.

| Advanced Settings | ? |
|---|---|
| Eligibility | ? |
| Metered/Standby Link | ? |
| Metering <input checked="" type="checkbox"/> Enable Metering <div> Data Cap (MB): <input type="text" value="0"/> Billing Cycle: <input type="text" value="Monthly"/> Starting From: <input type="text" value="MM/DD/YYYY"/> </div> | |
| Standby <div> Standby Mode: <input type="text" value="Last-Resort"/> Priority: <input type="text" value="1"/> </div> | |

Die IP-Adresse und die Gateway Adresse für die Access Interface der WAN-Verbindung müssen nicht konfiguriert werden, da sie diese Informationen vom Träger über DHCP empfängt.

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Delete |
|--------------|-------------------|------------|--------------------|-------------------|--------------------------|--------|
| br-WL-1-AI-1 | V2 | | | Primary | <input type="checkbox"/> | |

Apply Revert

- Vervollständigen Sie den Rest der erforderlichen Branch-Konfiguration für die 110-LTE-WiFi-Appliance. Siehe [Zweig konfigurieren](#).
- Führen Sie das Änderungsmanagement durch Hochladen der SD-WAN-Software durch. Siehe das [Change-Management-Verfahren](#).
- Aktivieren Sie die Konfiguration über den lokalen Change Management-Prozess. Wenn Sie Change Management ausführen, wird die Konfiguration aktiviert und die erforderliche Konfiguration wird angewendet.

Zero-Touch-Bereitstellung über LTE

Die SD-WAN 110 SE-Appliance unterstützt sowohl die Day-0-Provisioning als auch die Day-n-Verwaltung von SD-WAN-Appliances über die Management- und Datenports

Voraussetzungen für die Aktivierung des Zero-Touch-Bereitstellungsdienstes über LTE:

- Installieren Sie die Antenne, schalten Sie das Gerät ein und legen Sie die SIM-Karte ein.
- Stellen Sie sicher, dass die SIM-Karte über einen aktivierten Datenplan verfügt.

3. Stellen Sie sicher, dass der Verwaltung-/Datenport nicht verbunden ist.
 - Wenn der Verwaltung-/Datenport angeschlossen ist, trennen Sie den Verwaltung-/Datenport.
 - Wenn eine statische IP-Adresse auf der Verwaltungs-/Datenschnittstelle konfiguriert ist, müssen Sie die Verwaltung/Datenschnittstelle mit DHCP konfigurieren, die Konfiguration anwenden und dann den Verwaltung-/Datenport trennen.
4. Stellen Sie sicher, dass die Konfiguration der 110-LTE-WiFi-Appliance für die LTE-Schnittstelle definiert ist.

Wenn die Appliance eingeschaltet ist, verwendet der Zero-Touch-Bereitstellungsdienst den LTE-Port, um die neueste SD-WAN-Software und SD-WAN-Konfiguration zu erhalten.

Sie können die Benutzeroberfläche des SD-WAN Centers verwenden, um die 110-LTE-WiFi-Appliance für den Zero-Touch-Bereitstellungsdienst bereitzustellen und zu konfigurieren.

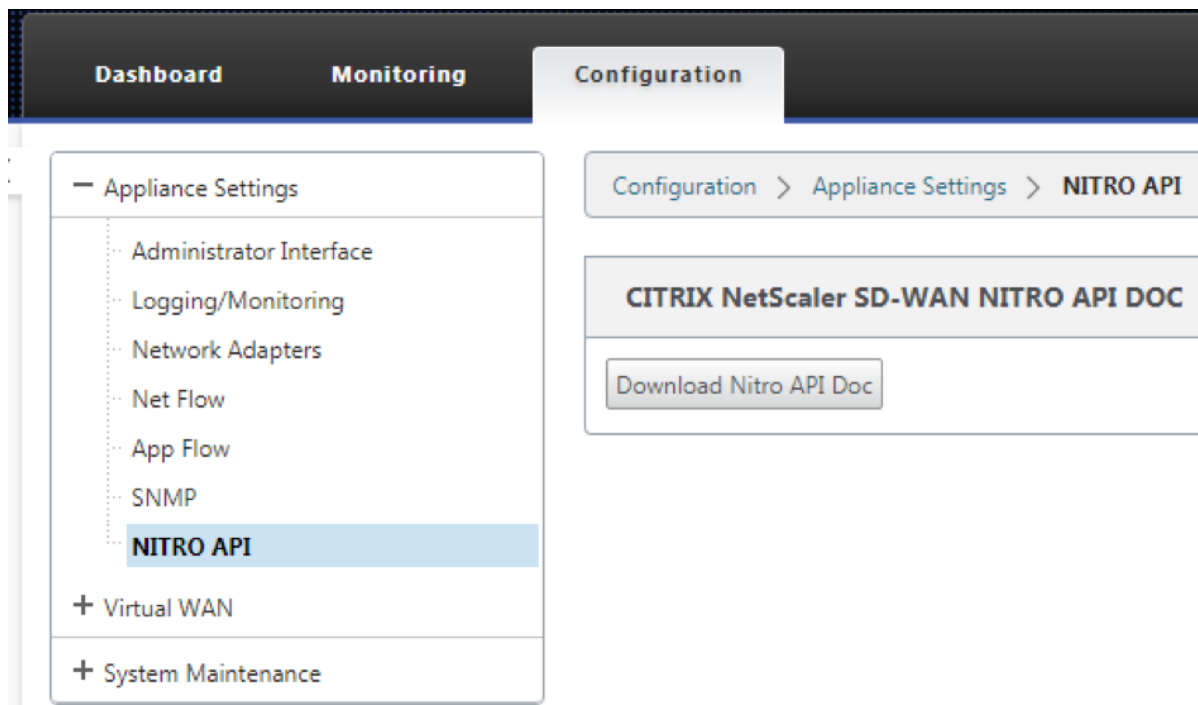
Weitere Informationen zum Bereitstellen und Konfigurieren von 110-LTE-WiFi-Appliance mit SD-WAN Center finden Sie im [Zero-Touch-Bereitstellungsverfahren](#).

Zero-Touch-Bereitstellung Service über Management-/Datenschnittstelle für 110-SE LTE Appliance

Verbinden Sie den Management-/Datenport mit dem Internet und verwenden Sie das standardmäßige [Zero-Touch-Bereitstellungsverfahren](#), das auf allen anderen Nicht-LTE-Plattformen unterstützt wird.

LTE REST API

Informationen zur LTE REST-API erhalten Sie, wenn Sie zur SD-WAN GUI navigieren und zu **Konfiguration > Appliance-Einstellungen > NITRO-API** gehen. Klicken Sie auf **Nitro API Doc herunterladen**. Die REST-API für SIM-PIN-Funktionalität wird in Citrix SD-WAN 11.0 eingeführt.



Konfigurieren eines externen USB-LTE-Modems

October 28, 2021

Sie können ein externes 3G/4G-USB-Modem auf bestimmten Citrix SD-WAN Appliances anschließen. Die Appliances verwenden das 3G/4G-Netzwerk zusammen mit anderen Verbindungen, um ein virtuelles Netzwerk zu bilden, das Bandbreite aggregiert und Ausfallsicherheit bietet. Wenn auf den anderen Schnittstellen ein Verbindungsfehler auftritt, wird der Datenverkehr automatisch über das USB-LTE-Modem umgeleitet. Die folgenden Appliances unterstützen ein externes USB-Modem:

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

Die [Citrix SD-WAN 210 SE LTE](#) und [Citrix SD-WAN 110 LTE Wi-Fi SE](#) Appliances verfügen über ein eingebautes LTE-Modem. Aktives Dual LTE wird auf diesen Geräten unterstützt.

CDC Ethernet, MBIM und NCM sind die drei unterstützten externen USB-Modems. Sie können die **APN-Einstellungen** konfigurieren und das Modem aktivieren/deaktivieren über die [neue Citrix SD-WAN GUI](#) und das [Citrix SD-WAN Center](#). Mobile Breitbandvorgänge werden auf CDC Ethernet USB-Modems nicht unterstützt.

Anschließen des USB-Modems

Aktivieren und testen Sie das USB-Modem gemäß den Richtlinien Ihres Mobilfunkanbieters.

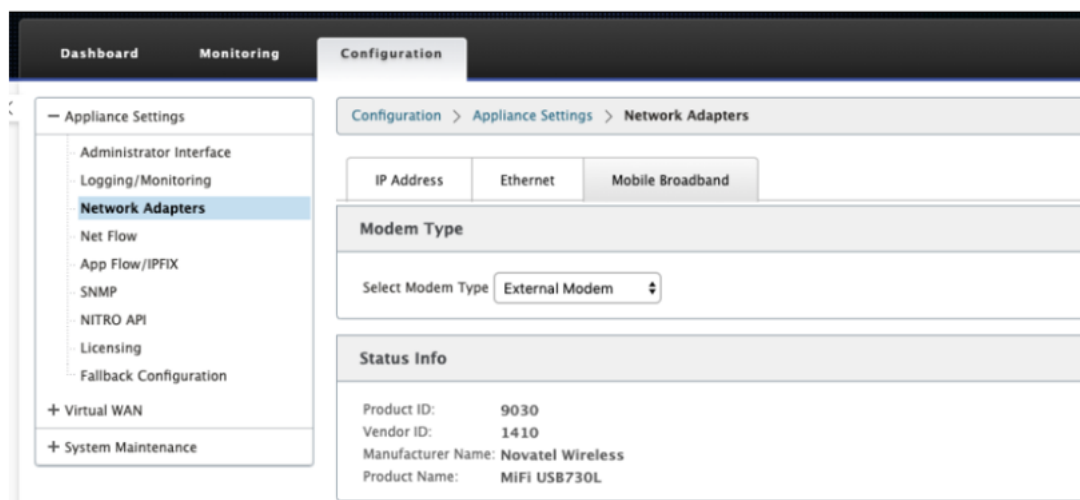
Perquisites für externes LTE-Modem:

- Verwenden Sie die unterstützten USB LTE Dongles. Die unterstützten Dongle-Hardwaremodelle sind Verizon USB730L und AT & T USB800.
- Stellen Sie sicher, dass eine SIM-Karte in den USB-LTE-Dongle eingelegt ist. Die CDC Ethernet LTE Dongles sind mit einer statischen IP-Adresse vorkonfiguriert, dies stört die Konfiguration und verursacht Verbindungsfehler oder intermittierende Verbindung, wenn die SIM-Karte nicht eingelegt ist.
- Bevor Sie einen CDC Ethernet LTE-Dongle in die SD-WAN-Appliance einsetzen, schließen Sie den externen USB-Stick an einen Windows/Linux-Computer an und stellen Sie sicher, dass das Internet mit der richtigen APN- und Mobile Data Roaming-Konfiguration ordnungsgemäß funktioniert. Stellen Sie sicher, dass der **Verbindungsmodus** des USB-Dongle vom Standardwert **Manuell** auf **Auto** geändert wird.

Hinweis

- Die Citrix SD-WAN Appliances unterstützen jeweils nur einen USB-LTE-Dongle. Wenn mehr als ein USB-Dongle angeschlossen ist, ziehen Sie alle Dongles ab und stecken Sie nur einen Dongle an.
- Die Citrix SD-WAN Appliances unterstützen keinen Benutzernamen und kein Kennwort für USB-Modems. Stellen Sie sicher, dass die Benutzernamen- und Kennwortfunktion auf dem Modem während der Installation deaktiviert sind.
- Das Entfernen oder Neustarten eines externen MBIM-Dongles wirkt sich auf die interne LTE-Modem-Datensitzung aus. Dies ist ein erwartetes Verhalten.
- Wenn ein externes LTE-Modem angeschlossen ist, dauert die SD-WAN-Appliance etwa 3 Minuten, um es zu erkennen.

Um die Details zum externen Modem anzuzeigen, navigieren Sie in der Benutzeroberfläche der **Appliance zu Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband**. Wählen Sie **Externes Modem** als Modemtyp aus.



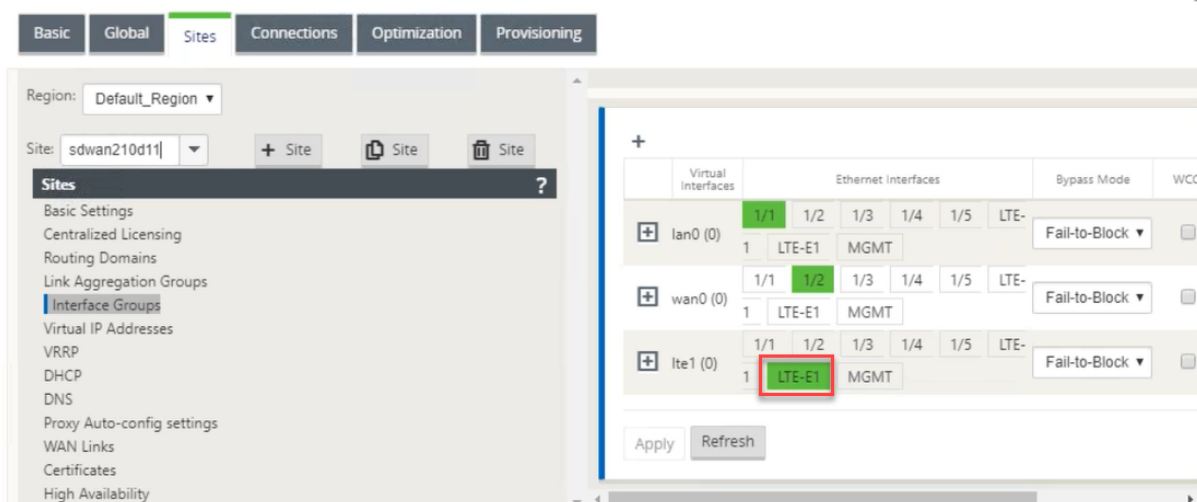
Hinweis

- Die SIM-PIN und andere LTE-Modemkonfigurationen werden derzeit nicht unterstützt.
- Die Modellnummer des LTE-USB-Dongle wird im Abschnitt **“Statusinformationen”** nicht angezeigt.

Mit dem Citrix SD-WAN Center können Sie alle LTE-Sites in Ihrem Netzwerk remote anzeigen und verwalten. Weitere Informationen finden Sie unter [Remote-LTE-Standortverwaltung](#).

Konfigurieren des externen USB-Modems

Um ein externes USB-Modem zu konfigurieren, navigieren Sie im Konfigurationseditor zu **Sites**, wählen Sie eine Site aus und klicken Sie auf **Interface-Gruppen**. Die externe USB-Modemschnittstelle LTE-E1 steht zur Konfiguration zur Verfügung. Weitere Informationen zum Konfigurieren einer Zweigstelle für LTE finden Sie unter [Konfigurieren des Zweigs für LTE](#).



Zero-Touch-Bereitstellung über LTE

Voraussetzungen für die Aktivierung des Zero-Touch-Bereitstellungsdienstes über USB-LTE-Modem:

- Legen Sie das USB-Modem in die Citrix SD-WAN Appliance ein. Weitere Informationen finden Sie unter Anschließen des USB-Modems.
- Stellen Sie sicher, dass die SIM-Karte auf dem USB-Modem über einen aktivierten Datentarif verfügt.
- Stellen Sie sicher, dass der Verwaltung/Datenport nicht verbunden ist. Wenn der Verwaltung/Datenport verbunden ist, trennen Sie ihn.
- Stellen Sie sicher, dass in der Appliance-Konfiguration der Internetdienst für die LTE-Schnittstelle definiert ist.

Wenn die Appliance eingeschaltet ist, verwendet der Zero-Touch-Bereitstellungsdienst den LTE-E1-Port, um die neueste SD-WAN-Software und SD-WAN-Konfiguration zu erhalten.

Verwenden Sie die Benutzeroberfläche des SD-WAN Centers, um die Appliance für den Zero-Touch-Bereitstellungsdienst bereitzustellen und zu konfigurieren. Weitere Informationen finden Sie unter [Zero Touch-Bereitstellung](#).

Informationen zur Zero-Touch-Bereitstellung über den SD-WAN Orchestrator finden Sie unter [Zero Touch Deployment](#).

Unterstützte USB-Modems

Die folgenden Modems sind mit Citrix SD-WAN Appliances kompatibel.

Hinweis:

Citrix kontrolliert nicht die Firmware-Aktualisierungen des Mobilfunkanbieters. Daher ist die Kompatibilität der neuen Modem-Firmware mit der Citrix SD-WAN -Software nicht gewährleistet. Das Modem-Firmware-Update wird vom Kunden gesteuert. Citrix empfiehlt, ein Firmware-Update an einem einzelnen Standort zu testen, bevor es über das gesamte Netzwerk übertragen wird.

| Region | Wireless Carrier/ Manufacturer | USB-Modem | Unterstützter Modemtyp | Schnittstellen |
|--------|-----------------------------------|-------------------------------|---------------------------|----------------|
| USA | Verizon | Globales Modem USB730L | cdc_ether | Nur 4G |
| USA | AT&T | AT&T Globales Modem USB800 | cdc_ether | Nur 4G |

Bereitstellungen

May 10, 2021

Im Folgenden finden Sie einige der Anwendungsszenarien, die mithilfe von Citrix SD-WAN Appliances implementiert wurden:

- [Bereitstellen von SD-WAN im Gateway-Modus](#)
- [Inlinemodus](#)
- [Bereitstellen von SD-WAN im PBR-Modus \(Virtueller Inlinemodus\)](#)
- [Dynamische Pfade für Zweigkommunikation](#)
- [WAN-zu-WAN-Weiterleitung](#)
- [Aufbau eines SD-WAN-Netzwerks](#)
- [Routing für die LAN-Segmentierung](#)
- [Nutzung der Premium Edition-Appliance zur Bereitstellung von WAN-Optimierungsdiensten](#)
- [Zwei-Box-Modus](#)
- [Zero Touch-Bereitstellung](#)
- [Bereitstellung in einer Region](#)
- [Bereitstellung mehrerer Regionen](#)
- [Hohe Verfügbarkeit](#)

Checkliste und Bereitstellung

May 10, 2021

Es wird dringend empfohlen, vor Beginn der Installation zuerst das Citrix Virtual WAN Deployment Planning Guide zu lesen. In diesem Artikel werden die wesentlichen Virtual WAN-Konzepte und -Features erläutert und Richtlinien für die Planung der Bereitstellung bereitgestellt.

Vorbereitung auf die Bereitstellung

In der folgenden Liste werden die Schritte und Verfahren beschrieben, die bei der Bereitstellung der SD-WAN Standard und Premium (Enterprise) Edition erforderlich sind.

Weitere Informationen zum Anzeigen einiger Bereitstellungs-Anwendungsfälle finden Sie unter [Bereitstellungen](#).

1. Sammeln Sie Informationen zur Citrix SD-WAN Bereitstellung.
2. Richten Sie die Citrix SD-WAN Appliances ein.
 - Für jede Hardware-Appliance, die Sie Ihrer SD-WAN-Bereitstellung hinzufügen möchten, müssen Sie die folgenden Aufgaben ausführen:
 - Richten Sie die Appliance-Hardware ein.
 - Legen Sie die Verwaltungs-IP-Adresse für die Appliance fest, und überprüfen Sie die Verbindung.
 - Legen Sie Datum und Uhrzeit auf der Appliance fest.
 - (Optional) Legen Sie das **Zeitüberschreitungsintervall** der Konsolensitzung auf einen hohen oder maximalen Wert fest.
3. Laden Sie die Softwarelizenzdatei hoch und installieren Sie sie auf der Appliance.

Installations- und Konfigurationsprüfliste

Sammeln Sie die folgenden Informationen für jede SD-WAN-Site, die Sie bereitstellen möchten:

- Die Lizenzinformationen für Ihr Produkt
- Erforderliche Netzwerk-IP-Adressen für jede zu bereitzustellende Appliance:
 - Verwaltungs-IP-Adresse
 - Virtuelle IP-Adressen
 - Sitenamen
 - Appliance-Name (einer pro Standort)
 - SD-WAN-Appliance-Modell (für jede zu bereitzustellende Appliance)
 - Bereitstellungsmodus (MCN oder Client)
 - Topologie
 - Gateway-MPLS
 - GRE Tunnel Informationen
 - Routen
 - VLANs
 - Bandbreite an jedem Standort für jede Schaltung

Bewährte Methoden

May 10, 2021

In diesem Artikel werden bewährte Methoden für die Bereitstellung der Citrix SD-WAN Lösung beschrieben. Es bietet allgemeine Anleitungen, Vorteile und Anwendungsfälle für den folgenden Citrix SD-WAN Bereitstellungsmodus.

Kante/Gateway-Modus

Empfehlungen

Im Folgenden finden Sie die Empfehlungen für die Bereitstellung im **Gateway-Modus**:

1. Der Gateway-Modus wird am besten für SD-WAN-Zweige verwendet, in denen die Routerkonsolidierung stattfindet und Kunden bereit sind, SD-WAN als Edge-Gerät zu ermöglichen, das Verbindungen beendet.
2. Eine großartige Netzwerkarchitektur kann mit einem gewissenhaften Design gerendert werden, wenn ein Projekt von Grund auf neu erstellt wird.

Hinweis

Der Gateway-Modus kann auf der Rechenzentrumsseite für die vorhandenen Projekte mit einigen Infrastrukturunterbrechungen verwendet werden.

Vorteile/Anwendungsfälle

Im Folgenden sind die Vorteile/Anwendungsfälle für die Bereitstellung des Gateway-Modus aufgeführt:

1. Bester Anwendungsfall für die Konsolidierung von Router/Firewall/Netzwerkelementen in der Kundenfiliale.
2. Einfache und einfache LAN-Hostverwaltung über DHCP.
 - Ermöglicht es SD-WAN, zum nächsten Hop zu werden und DHCP-basierte IP-Adressierung für alle LAN-Hosts für Datenports anzubieten.
3. Alle Verbindungen enden am SD-WAN Edge/Gateway und die Verwaltung wird einfach.
4. SD-WAN ist der Brennpunkt des Edge-Routing und wird vom gesamten Datenverkehr gesteuert. Die Entscheidungen werden über die Kante zu Breakout oder Backhaul oder Overlay einschließlich der Bandbreite/Kapazität Accounting getroffen.

5. Alle LAN-Subnetz-Hosts als LAN-Hosts dürfen SD-WAN LAN VIP als nächster Hop haben. Wenn SD-WAN LAN eine Verbindung zu einem Core-Switch herstellt, können Sie dynamisches Routing ausführen, um Transparenz für alle LAN-Subnetze zu erhalten.
6. Große Flexibilität für hohe Verfügbarkeit (HA) - Strenge Empfehlung für den Gateway -Modus, damit der Standort im Aktiv-/Standby-Modus betrieben wird. Außerdem hilft es, ein Verkehrs-blackhole zu verhindern, wenn das SD-WAN-Gerät ausfällt.
 - Switches in der Filiale verfügbar - Parallele Hochverfügbarkeit kann im Gateway Modus funktionieren.
 - Switches in der Zweigstelle nicht verfügbar - SD-WAN kann auch im SD-WAN-Edge-Hochverfügbarkeitsmodus (Fail-to-Wire-Hochverfügbarkeitsmodus) betrieben werden, wobei die beiden SD-WAN-Boxen in Daisy-Chain geschaltet sind, um Fail-to-Wire-Ports als konvergiertes Hochverfügbarkeitspaar zu nutzen.
7. Erlauben Sie, dass das Internet als **UNTRUSTED-Schnittstellen** definiert wird, die automatisch eine dynamische NAT für Breakout und Quell-NAT die Verbindung erstellen, sodass die Antwort auf SD-WAN zurückkommt.
8. Sicherheitsüberlegungen zu **UNTRUSTED** Schnittstellen sind natürlich impliziert, da nur ICMP/ARP/UDP-Steuerungspakete auf 4980 zulässig sind.

Vorsicht

Im Folgenden finden Sie die Informationen, mit denen Sie im Gateway-Modus vorsichtig sein müssen:

- **Sorgfältiges Design und Netzwerkarchitektur** - Der Gateway-Modus erfordert möglicherweise sorgfältige Überlegungen zum Design und zur Vernetzung, da das gesamte Branch/Edge-Netzwerk in SD-WAN ist. Was zu blockieren, was zu routen ist, wie man LAN vernetzt, wie man WANs beendet, und so weiter.
- **Fehler des Geräts** - Der Edge-Modus kann nicht über die Fail-to-Wire-Fähigkeit verfügen. Der gesamte Zweig geht nach unten, wenn das Gerät ausfällt.
- **Sicherheitslage** - Da das Routing am Edge verwaltet wird, sind die Sicherheitshaltungen wie Firewall, Breakout/Backhaul Überlegungen entscheidend und das muss mit dem Kunden konzipiert werden.
- **Hohe Verfügbarkeit** —Fail-to-Wire-Hochverfügbarkeit muss einige Überlegungen zur Portverfügbarkeit haben und je nach Bereitstellung kann es schwierig werden, sie zu entwerfen.
 - SD-WAN 110 ist keine Option, da es keine Fail-to-Wire-Ports hat.

Wenn Sie zum Beispiel 2 WAN-Verbindungen benötigen, benötigen Sie 5 Ports, einschließlich eines dedizierten Ports für die Hochverfügbarkeitsschnittstelle einschließlich der LAN-Schnittstelle.

Inline-Modus — Fail-to-Wire/Fail-to-Block

Empfehlungen

Im Folgenden finden Sie die Empfehlungen für die Bereitstellung im **Inlinemodus** :

1. Der Inline-Modus eignet sich am besten für die Zweige, in denen die vorhandene Infrastruktur nicht geändert werden soll und das SD-WAN transparent im LAN-Segment liegt.
2. Rechenzentren können auch Inline-Fail-to-Wire- oder Inline-parallele Hochverfügbarkeit nutzen, da es immens wichtig ist, um sicherzustellen, dass die Rechenzentrums-Workloads aufgrund von Geräteabsturz nicht verdunkelt werden.

Vorteile und Anwendungsfälle

Im Folgenden sind die Vorteile/Anwendungsfälle für die Bereitstellung im Inline-Modus aufgeführt:

1. Halten Sie den MPLS-Router daher Fail-to-Wire ist eine schöne Funktion. Fail-to-Wire-fähige Geräte ermöglichen ein nahtloses Failover zur Unterlagen-Infrastruktur, wenn die Box ausfällt.
 - Wenn Ihre Geräte Fail-to-Wire (SD-WAN 210 und höher) unterstützen, ermöglicht dies die Platzierung eines einzelnen SD-WAN Inline zur Hardware, um den LAN-Datenverkehr zum Customer Edge-Router zu umgehen, wenn das SD-WAN abstürzt/ausfällt.
 - Wenn die MPLS-Links vorhanden sind, die eine natürliche Erweiterung des LAN/Intranets des Kunden ergeben, ist der Fail-to-Wire-Bridge-Paar-Port die beste Wahl (Fail-to-Wire-fähige Paare), so dass, wenn das Gerät abstürzt oder herunterfährt, der LAN-Verkehr per Hardware an den Customer Edge-Router umgangen wird (nächste Hop bleibt erhalten).
2. Die Vernetzung ist einfach.
3. SD-WAN sieht den gesamten Datenverkehr im Inline-Modus, daher ist es das beste Szenario für die richtige Bandbreite/Kapazitätsrechnung.
4. Wenige Integrationsanforderungen, da Sie nur eine IP des L2-Segments benötigen. LAN-Segmente sind bekannt, da Sie einen Arm zur LAN-Schnittstelle haben. Wenn Sie eine Verbindung zu einem Core-Switch herstellen, können Sie auch dynamisches Routing ausführen, um Transparenz für alle LAN-Subnetze zu erhalten.
5. Die Erwartungen des Kunden sind, dass SD-WAN als neuer Netzknoten in die bestehende Infrastruktur integriert werden muss (sonst ändert sich nichts).

6. **Proxy ARP** - Im Inlinemodus ist es für SD-WAN ein Segen, ARP-Anfragen an LAN-Next-Hop zu proxieren, wenn das Gateway ausfällt oder die SD-WAN-Schnittstelle zum nächsten Hop ausfällt.
- Im Inline-Modus mit Bridge-Pair (Fail-to-Block oder Fail-to-Wire) mit mehreren WAN-Verbindungen (MPLS/Internet) wird empfohlen, Proxy ARP für die Bridge-Paarschnittstelle zu aktivieren, die die LAN-Hosts mit ihrem Next-Hop-Gateway verbindet.
 - Aus irgendeinem Grund, wenn der nächste Hop heruntergefahren ist oder die SD-WAN-Schnittstelle zum nächsten Hop heruntergefahren ist, wodurch das Gateway nicht erreichbar ist, fungiert SD-WAN als Proxy für ARP-Anforderungen, so dass die LAN-Hosts weiterhin nahtlos Pakete senden und die verbleibenden WAN-Verbindungen verwenden können, die den virtuellen Pfad beibehalten.
7. **Hohe Verfügbarkeit** - Wenn Fail-to-Wire keine Option ist, können Geräte in parallele Hochverfügbarkeitsgeräte (gemeinsame LAN- und WAN-Schnittstellen für Active/Standby) platziert werden, um Redundanz zu erreichen.
- Wenn Ihre Appliances keine Fail-to-Wire unterstützen, wie das SD-WAN 110, müssen Sie eine parallele Inline-Hochverfügbarkeit verwenden, die es ermöglicht, dass ein Standby-Gerät eintritt, wenn das primäre Gerät ausfällt.

Vorsicht

Im Folgenden sind die Informationen aufgeführt, mit denen Sie im **Inline-Modus** vorsichtig sein müssen:

- Sanitär-Netzwerk mit zwei Armen zum SD-WAN (LAN- und WAN-Seite), benötigt einige Ausfallzeiten, da das Netzwerk in zwei Armen verstopft werden muss.
- Muss sicherstellen, dass, wenn Fail-to-Wire verwendet wird, es sich hinter einem Kunden-Edge-Router/einer Firewall in einer **VERTRAUENSWÜRDIGEN** Zone befindet, damit die Sicherheit nicht gefährdet wird.
- MPLS QoS ändert sich ein wenig, da die vorherigen QoS-Richtlinien möglicherweise von den Quell-IP-Adressen oder DSCP-basierten abhängig waren, die jetzt aufgrund einer Überlagerung maskiert werden.
- Es muss darauf geachtet werden, den MPLS-Router mit einer gut gestalteten, reservierten SD-WAN-spezifischen Bandbreite mit einem spezifischen DSCP-Tag neu zu verwenden, so dass das QoS von SD-WAN sich um die Priorisierung des Datenverkehrs kümmert und Anwendungen mit hoher Priorität sendet, die unmittelbar von anderen Klassen gefolgt sind (aber in der Lage sein, den gesamten Bandbreite, die für SD-WAN auf dem MPLS-Router reserviert

ist). MPLS-Warteschlangen sind eine Alternative oder MPLS mit einem einzigen DSCP in der Auto-Pfadgruppe festgelegt, die sich darum kümmern kann.

- Wenn die Internetschnittstellen **VERTRAUENSWÜRDIG** sind, da die Links auf dem Kunden-Edge-Router enden, müssen Sie zur Nutzung des Internetdienstes eine exklusive dynamische NAT-Regel schreiben, um das Ausbrechen des Internets von der Appliance zu ermöglichen.
- Wenn die Internetverbindungen die einzigen WAN-Verbindungen sind und weiterhin auf dem Customer Edge-Router enden, ist es immer noch in Ordnung, die Verbindungen zu umgehen, wenn der Customer Edge-Router Vorsichtsmaßnahmen trifft, um die Pakete über seine vorhandene Unterlage-Infrastruktur zu steuern.
 - Bei der Umgehung des LAN-Datenverkehrs über Bridge-Paar mit einer Internetverbindung und beim Ausfall der Appliance ist die richtige Vorsicht zu beachten. Da es sich um einen sensiblen Unternehmens-Intranetverkehr handelt, muss der Kunde am Vorabend des Ausfalls wissen, wie er damit umgehen soll.

Virtueller Inline/Einarm-Modus

Empfehlungen

Im Folgenden finden Sie die Empfehlungen für die Bereitstellung im **virtuellen Inlinemodus** :

1. Der virtuelle Inline-Modus eignet sich am besten für Rechenzentrumsnetzwerke, da die SD-WAN-Netzwerkinstallationen parallel ausgeführt werden können, während das Rechenzentrum seine vorhandenen Arbeitslasten mit vorhandener Infrastruktur bedient.
2. SD-WAN befindet sich in einer einarmigen Schnittstelle, die mit einem SLA-Tracking auf VIPs verwaltet wird. Wenn die Verfolgung ausfällt, wird der Datenverkehr das Routing über die vorhandene Unterlay-Infrastruktur fortgesetzt.
3. Zweige können auch im virtuellen Inline-Modus bereitgestellt werden, sind jedoch bei Inline/Gateway-Bereitstellungen überwiegender.

Vorteile und Anwendungsfälle

Im Folgenden werden die Vorteile/Anwendungsfälle für die Bereitstellung im **virtuellen Inlinemodus** aufgeführt:

1. Einfachste und empfohlene Möglichkeit, SD-WAN im Rechenzentrum zu vernetzen.
 - Der virtuelle Inline-Modus ermöglicht parallele Netzwerkinstallationen von SD-WAN mit dem Head-End-Core-Router.

- Der virtuelle Inline-Modus ermöglicht es uns, einfach PBRs definieren, um LAN-Datenverkehr umzulenken muss durch SD-WAN gehen und erhalten Overlay-Vorteile.
- 2. Nahtloses Failover zur zugrunde liegenden Infrastruktur, wenn SD-WAN ausfällt, und nahtlose Weiterleitung an SD-WAN für Overlay-Vorteile unter normalen Bedingungen.
- 3. Einfache Anforderungen an **Netzwerke** und **Integration**. Die einarmige Schnittstelle vom Head-end Router zu SD-WAN im virtuellen Inline.
- 4. Einfach zu implementierendes dynamisches Routing im **Nur-Importmodus** (nichts exportieren), um die Sichtbarkeit von LAN-Subnetzen zu erhalten, damit sie an Remote-SD-WAN-Peer-Appliances gesendet werden können.
- 5. Einfach zu definieren PBR auf den Routern (1 pro WAN VIP), um anzugeben, wie das physische zu wählen ist.

Vorsicht

Im Folgenden finden Sie die Informationen, bei denen Sie im **Virtual Inline-Modus** vorsichtig sein müssen:

- Es muss darauf geachtet werden, die logische SD-WAN-VIP einer WAN-Verbindung, die mit der richtigen physikalischen Schnittstelle definiert ist, deutlich zu MAP (sonst kann dies zu unerwünschten Problemen bei der WAN-Metrikbewertung und der Wahl der WAN-Pfade führen).
- Richtige Entwurfsüberlegungen sind zu berücksichtigen, um zu wissen, ob der gesamte Datenverkehr über SD-WAN oder nur bestimmten Datenverkehr umgeleitet wird.
- Das bedeutet, dass SD-WAN einen Teil der Bandbreite ausschließlich für sich selbst dediziert sein muss, der auf den Schnittstellen so eingestellt werden muss, dass die Kapazität von SD-WAN nicht von anderen Nicht-SD-WAN-Datenverkehr genutzt wird, was zu unerwünschten Ergebnissen führt.
 - Probleme bei der Bandbreitenbuchhaltung und Engpässe können auftreten, wenn die Kapazität der SD-WAN-Verbindungen falsch definiert ist.
- Dynamisches Routing kann einige Probleme verursachen, wenn die SD-WAN-Routen Rechenzentrum und Zweigstellen-VIPs in das Headend exportiert werden und wenn das Routing in Richtung SD-WAN beeinflusst wird, beginnen Overlay-Pakete mit der Schleife und verursachen unerwünschte Ergebnisse.
- Dynamisches Routing muss unter Berücksichtigung aller potenziellen Faktoren, was zu lernen/was zu bewerben ist, ordnungsgemäß verwaltet werden.
- Eine einarmige physikalische Schnittstelle könnte manchmal zu einem Engpass werden. Benötigt einige Entwurfsüberlegungen in diesen Zeilen, da es sowohl für Upload/Download

geeignet ist und auch als LAN zu LAN und LAN zu WAN/WAN zu LAN-Datenverkehr von SD-WAN fungiert.

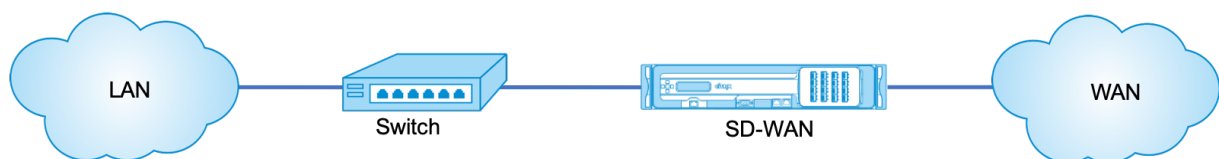
- Übermäßiger LAN-zu-LAN-Datenverkehr kann während des Entwurfs ein Punkt sein.
- Wenn das dynamische Routing nicht verwendet wird, muss bei der Verwaltung aller LAN-Subnetze die richtige Vorsicht gegeben sein. Wenn dies nicht der Fall ist, kann dies zu unerwünschten Routingproblemen führen.
- Es gibt mögliche Routingschleifenprobleme, wenn Sie eine Standardroute (0.0.0.0/0) auf dem SD-WAN im virtuellen Inline definieren, um auf den Headend-Router zurückzuverweisen. In solchen Situationen, wenn der virtuelle Pfad ausfällt, wird der Datenverkehr, der vom Rechenzentrums-LAN kommt (wie der Überwachungsdatenverkehr), zurück zum Headend und zurück zum SD-WAN geschoben, was zu unerwünschten Routingproblemen führt (wenn der virtuelle Pfad ausgefallen ist, werden die Subnetze der Remote-Branche **nicht** erreichbar Standardroute als HIT, die die Loop-Probleme verursacht).

Gateway-Modus

May 10, 2021

Gateway -Modus platziert die SD-WAN-Appliance physisch in den Pfad (Zwei-Arm-Bereitstellung) und erfordert Änderungen in der vorhandenen Netzwerkinfrastruktur, damit die SD-WAN-Appliance zum Standard-Gateway für das gesamte LAN-Netzwerk für diesen Standort wird. Gateway-Modus für neue Netzwerke und Routerersatz. Gateway-Modus ermöglicht SD-WAN-Geräte:

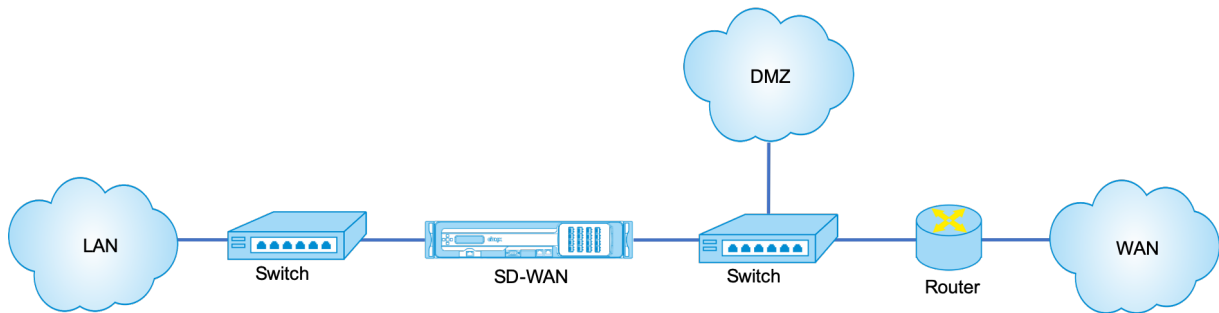
- So zeigen Sie den gesamten Datenverkehr zum und vom WAN an
- So führen Sie lokale Weiterleitung durch



Hinweis

Ein im Gateway-Modus bereitgestelltes SD-WAN fungiert als Layer 3-Gerät und kann keine Fail-to-Wire-Funktion ausführen. Alle beteiligten Schnittstellen werden für **Fail-to-Block** konfiguriert. Im Falle eines Geräteausfalls schlägt auch das Standard-Gateway für die Site fehl, was zu einem Ausfall führt, bis die Appliance und das Standard-Gateway wiederhergestellt sind.

Im **Inline-Modus** scheint die SD-WAN-Appliance eine Ethernet-Bridge zu sein. Die meisten SD-WAN-Appliance-Modelle verfügen über eine Fail-to-Wire-Funktion (Ethernet-Bypass) für den Inline-Modus. Wenn die Stromversorgung ausfällt, schließt sich ein Relais und die Eingangs- und Ausgangsanschlüsse werden elektrisch angeschlossen, so dass das Ethernet-Signal von einem Port zum anderen weitergeleitet wird. Im Fail-to-Wire-Modus sieht die SD-WAN-Appliance wie ein Cross-Over-Kabel aus, das die beiden Anschlüsse verbindet. Inline-Modus für die Integration in bereits definierte Netzwerke.

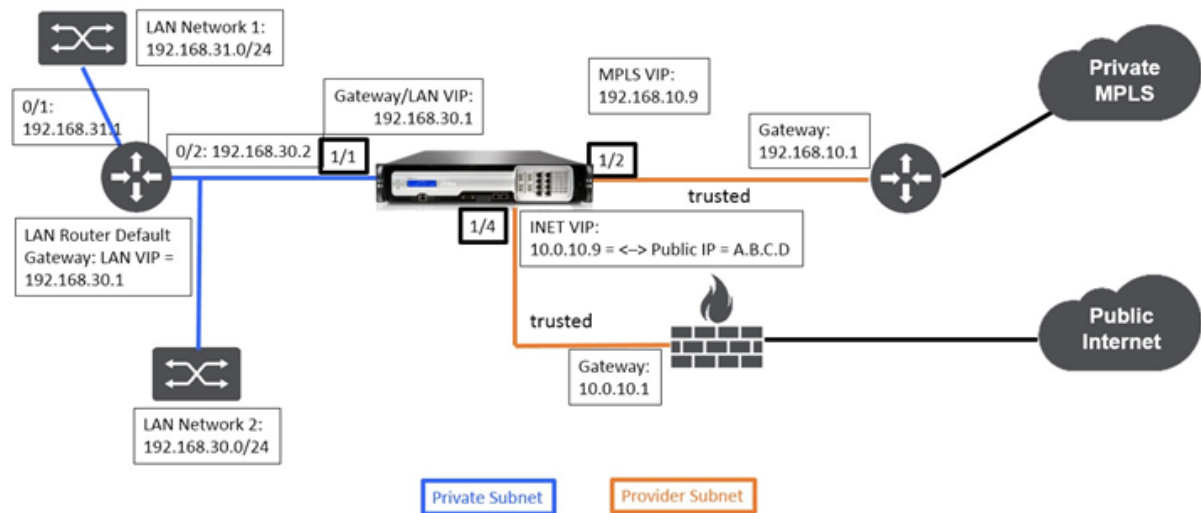


Dieser Artikel enthält schrittweise Verfahren zum Konfigurieren einer SD-WAN-Appliance im Gateway-Modus in einem Beispielnetzwerk-Setup. Die Inline-Bereitstellung wird auch für die Zweigseite beschrieben, um die Konfiguration abzuschließen. Ein Netzwerk kann weiterhin funktionieren, wenn ein Inline-Gerät entfernt wird, verliert jedoch jeglichen Zugriff, wenn das Gateway-Gerät entfernt wird.

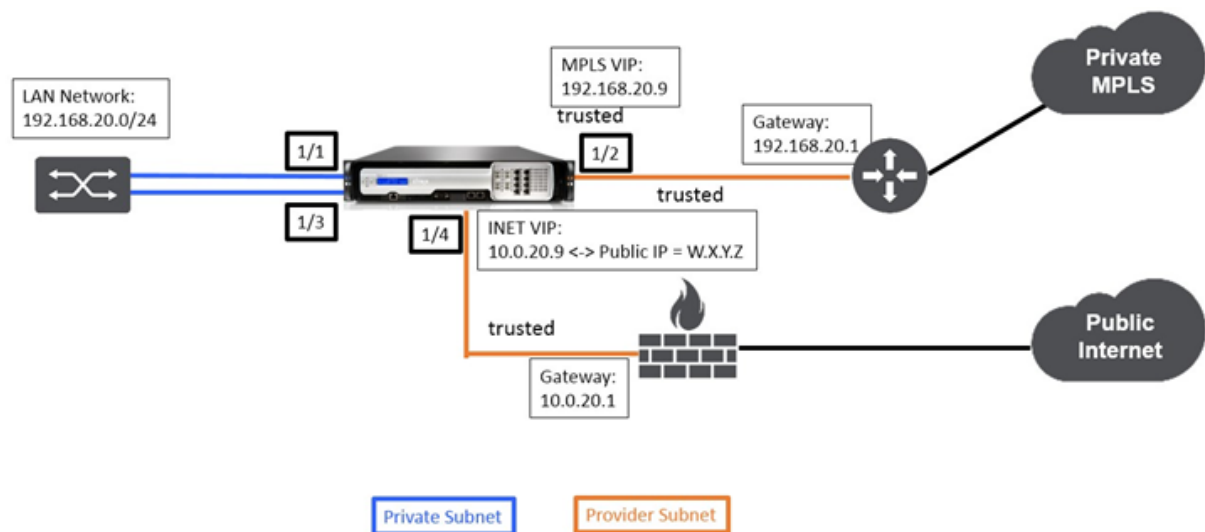
Topologie

In den folgenden Abbildungen werden die Topologien beschrieben, die in einem SD-WAN-Netzwerk unterstützt werden.

Rechenzentrum bei Gateway Bereitstellung



Zweig in der Inline-Bereitstellung



Bereitstellungsanforderungen

Bereitstellungsanforderungen und zugehörige Informationen werden im Folgenden beschrieben, um Sie beim Erstellen der Konfiguration zu unterstützen.

| Sitename | Rechenzentrums-Standort | Niederlassungsstandort |
|----------------|-------------------------|------------------------|
| Appliance-Name | A_DC1 | A_BR1 |

| Sitename | Rechenzentrums-Standort | Niederlassungsstandort |
|----------------------------|--|---|
| Management-IP | 172.30.2.10/24 | 172.30.2.20/24 |
| Sicherheitsschlüssel | Falls vorhanden | Falls vorhanden |
| Modell/Edition | 4000 | 2000 |
| Modus | Gateway | Inline |
| Topologie | 2 x WAN-Pfad | 2 x WAN-Pfad |
| VIP-Adresse | 192.168.10.9/24 –MPLS, 10.0.10.9/24 –Internet (Public IP –A.B.C.D), 192.168.30.1/24 - LAN | 192.168.20.9/24 - MPLS, 10.0.20.9/24 –Internet (Public IP –W.X.Y.Z) |
| Gateway-MPLS | 192.168.10.1 | 192.168.20.1 |
| Gateway-Internet | 10.0.10.1 | 10.0.20.1 |
| Verbindungsgeschwindigkeit | MPLS —100 Mbit/s, Internet — 20 Mbit/s | MPLS —10 Mbit/s, Internet —2 Mbit/s |
| Route | Netzwerk-IP-Adresse - 192.168.31.0/24, Diensttyp - Lokal, Gateway-IP-Adresse - 192.168.30.2 | Falls vorhanden |
| VLANs | Falls vorhanden | Falls vorhanden |

Konfigurationsvoraussetzungen

- Aktivieren Sie die SD-WAN-Appliance als Master Control Node.
- Die Konfiguration erfolgt nur auf dem Master Control Node (MCN) der SD-WAN-Appliance.

So aktivieren Sie eine Appliance als Master-Control-Knoten:

1. Navigieren Sie in der SD-WAN-Webverwaltungsschnittstelle zu **Konfiguration > Einheiteneinstellungen > Administratorschnittstelle > Registerkarte Sonstiges > Konsole wechseln**.

Hinweis

Wenn **Switch to Client Console** angezeigt wird, befindet sich die Appliance bereits im MCN-Modus. Es darf nur ein aktives MCN in einem SD-WAN-Netzwerk vorhanden sein.

2. Starten Sie die Konfiguration, indem Sie zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor** navigieren. Klicken Sie auf **Neu**, um mit der Konfiguration zu beginnen.

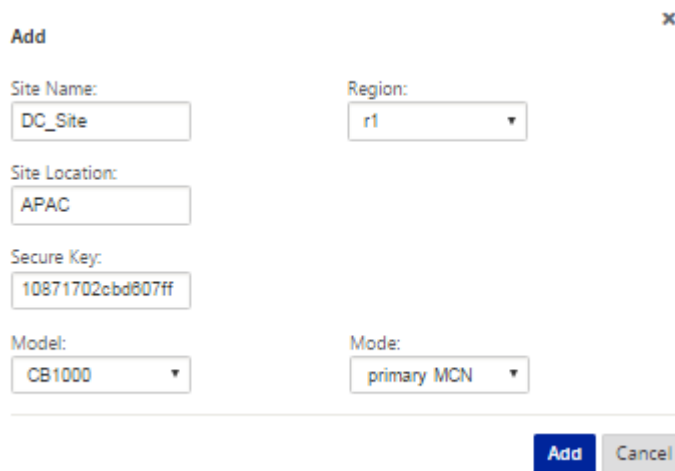
Konfiguration des Sitegatewaymodus für Rechenzentren

Im Folgenden werden die Konfigurationsschritte auf hoher Ebene zum Konfigurieren der Gateway-Bereitstellung des Rechenzentrums beschrieben:

1. Erstellen Sie einen DC-Standort.
2. Füllen Sie Schnittstellengruppen basierend auf angeschlossenen Ethernet-Schnittstellen aus.
3. Erstellen Sie eine virtuelle IP-Adresse für jede virtuelle Schnittstelle.
4. Füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht mit Burst-Geschwindigkeiten mithilfe von Internet- und MPLS-Links.
5. Füllen Sie Routen aus, wenn mehr Subnetze in der LAN-Infrastruktur vorhanden sind.

So erstellen Sie einen DC-Standort

1. Navigieren Sie zu **Konfigurationseditor > Sites** und klicken Sie auf die Schaltfläche **+ Hinzufügen**.
2. Füllen Sie die Felder wie unten gezeigt.
3. Behalten Sie die Standardeinstellungen bei, wenn Sie nicht dazu aufgefordert werden.



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following fields:

- Site Name:** A text input field containing "DC_Site".
- Region:** A dropdown menu showing "r1".
- Site Location:** A text input field containing "APAC".
- Secure Key:** A text input field containing "10871702ebd807ff".
- Model:** A dropdown menu showing "CB1000".
- Mode:** A dropdown menu showing "primary MCN".

At the bottom right of the dialog are two buttons: "Add" (in blue) and "Cancel" (in grey).

The screenshot displays the 'Basic Settings' configuration page for a site named 'MCN-5100'. On the left, a sidebar lists various configuration categories: Sites, Basic Settings (selected), Centralized Licensing, Routing Domains, Interface Groups, Virtual IP Addresses, VRRP, DHCP, WAN Links, Certificates, and High Availability. The main area contains the following fields and controls:

- Site Name:** MCN-5100
- Appliance Name:** Appliance
- Secure Key:** 2e0867413a24728 (with a 'Regenerate' button)
- Model:** CB5100 (dropdown menu)
- Mode:** primary MCN (dropdown menu)
- Site Location:** (empty text field)
- Default Direct Route Cost:** 5
- Gateway ARP Timer (ms):** 1000
- ☐ **Enable Source MAC Learning**
- Buttons:** 'Apply' and 'Revert'

So konfigurieren Sie Schnittstellengruppen basierend auf verbundenen Ethernet-Schnittstellen

1. Navigieren Sie im **Konfigurations-Editor** zu **Sites > Site anzeigen > [Site-Name]** > **Interface-Gruppen**. Klicken Sie auf **+**, um Schnittstellen hinzuzufügen, die verwendet werden sollen. Für den Gateway-Modus wird jeder Schnittstellengruppe eine einzige Ethernet-Schnittstelle zugewiesen.
2. Der Umgehungsmodus ist auf **Fail-to-Blockierung** eingestellt, da nur eine Ethernet/physische Schnittstelle pro virtueller Schnittstelle verwendet wird. Es gibt auch keine Brückenpaare.
3. In diesem Beispiel werden drei Interface-Gruppen erstellt, eine mit Blick auf das LAN und zwei weitere mit jedem jeweiligen WAN-Link. Weitere Informationen finden Sie im Beispiel "DC-Gateway-Modus" Topologie oben und füllen Sie die Schnittstellengruppen Felder wie unten dargestellt.

Virtual Interfaces

Ethernet Interfaces

12345678

Bypass Mode

Fail-to-Block

WCCP

Security

Trusted

Delete

Virtual Interfaces

| Name | Firewall Zone | VLAN ID | DHCP Client | Delete |
|------------|-----------------|---------|--------------------------|--------|
| DC-LAN-1-1 | Default_LAN_Zon | 0 | <input type="checkbox"/> | |

Bridge Pairs

| Interfaces | LSP | Delete |
|------------|--------------------------|--------|
| 1 ↔ 2 | <input type="checkbox"/> | |

VirtualInterface-1 (0)

12345678

Fail-to-Block

Trusted

Virtual Interfaces

| Name | Firewall Zone | VLAN ID | DHCP Client | Delete |
|-----------------|---------------|---------|--------------------------|--------|
| INET_DC-WAN-1-4 | <Default> | 0 | <input type="checkbox"/> | |

Bridge Pairs

| Interfaces | LSP | Delete |
|------------|--------------------------|--------|
| 1 ↔ 2 | <input type="checkbox"/> | |

VirtualInterface-2 (0)

12345678

Fail-to-Block

Trusted

Virtual Interfaces

| Name | Firewall Zone | VLAN ID | DHCP Client | Delete |
|-----------------|---------------|---------|--------------------------|--------|
| MPLS-DC-WAN-1-2 | <Default> | 0 | <input type="checkbox"/> | |

Bridge Pairs

| Interfaces | LSP | Delete |
|------------|-----|--------|
| | | |

Apply

Revert

So erstellen Sie VIP-Adresse (Virtual IP) für jede virtuelle Schnittstelle

1. Erstellen Sie für jeden WAN-Link im entsprechenden Subnetz eine VIP. VIPs werden für die Kommunikation zwischen zwei SD-WAN-Appliances in der virtuellen WAN-Umgebung verwendet.

2. Erstellen Sie eine virtuelle IP-Adresse, die als Gateway-Adresse für das LAN-Netzwerk verwendet werden soll.

| IP Address / Prefix | Virtual Interface | Firewall Zone | Identity | Private | Security | Delete |
|---------------------|---------------------|------------------|-------------------------------------|--------------------------|----------|--------|
| 10.0.10.9/24 | INET_DC-WAN-1-4 (0) | Default_LAN_Zone | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Trusted | |
| 192.168.10.9/24 | MPLS-DC-WAN-1-2 (0) | Default_LAN_Zone | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Trusted | |
| 192.168.30.1/24 | DC-LAN-1-1 (0) | Default_LAN_Zone | <input type="checkbox"/> | <input type="checkbox"/> | Trusted | |

Apply

Refresh

So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten mithilfe des Internetlinks aus:

1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+ Link hinzufügen**, um einen WAN-Link für den Internet-Link hinzuzufügen.

2. Geben Sie Informationen zum Internetlink ein, einschließlich der angegebenen öffentlichen IP-Adresse, wie unten dargestellt. AutoDetect **Public IP** kann nicht für SD-WAN-Appliance ausgewählt werden, die als MCN konfiguriert ist.
3. Navigieren Sie im Dropdown-Menü des Abschnitts zu **Access Interfaces** und klicken Sie auf die Schaltfläche **+ Hinzufügen**, um für den Internet-Link spezifische Schnittstellendetails hinzuzufügen.
4. Füllen Sie das Access Interface für IP- und Gateway Adressen wie unten dargestellt aus.

WAN Link: **BR571-WL-1** Section: **Settings** **+ Add Link** **Delete Link**

Basic Settings ?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name: **BR571-WL-1**

Access Type: **Public Internet** WAN Link Template: **<None>**

LAN to WAN

Physical Rate (kbps): **10000**

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): **10000**

WAN to LAN

Physical Rate (kbps): **10000**

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): **10000**

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Delete |
|------------------|-------------------|------------|--------------------|-------------------|--------------------------|--------|
| SJC_DC-INET-AI-1 | INET_DC-WAN-1-4 | 10.0.10.9 | 10.0.10.1 | Primary | <input type="checkbox"/> | |

So erstellen Sie eine MPLS-Verbindung

1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+**, um einen WAN-Link für den MPLS-Link hinzuzufügen.
2. Füllen Sie MPLS-Link-Details wie unten gezeigt.

- 3. Navigieren Sie zu **Access Interfaces**, klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails hinzuzufügen, die für den MPLS-Link spezifisch sind.
- 4. Füllen Sie das Access Interface für IP- und Gateway Adressen wie unten dargestellt aus.

Basic Settings ?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:
BR571-WL-1

Access Type:
Private MPLS

WAN Link Template:
<None>

LAN to WAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

Permitted Rate (kbps):
10000

WAN to LAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

Permitted Rate (kbps):
10000

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Delete |
|-----------------|-------------------|--------------|--------------------|-------------------|--------------------------|--------|
| SJC_DC-MPLS-... | MPLS-DC-WAN-1-2 | 192.168.10.9 | 192.168.10.1 | Primary | <input type="checkbox"/> | |

So füllen Sie Routen aus

Routen werden automatisch basierend auf der obigen Konfiguration erstellt. Die oben gezeigte DC-LAN-Beispieltopologie verfügt über ein zusätzliches LAN-Subnetz, das **192.168.31.0/24** ist. Für dieses Subnetz muss eine Route erstellt werden. Gateway-IP-Adresse muss sich im selben Subnetz wie die DC LAN VIP befinden, wie unten dargestellt.

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

280

Search:

| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|-------|--------------|--------------|--------------------|------|------|--------|
| 1 | 192.168.31.0/24 | 5 | Local | | 192.168.30.2 | | | |
| 2 | 192.175.58.0/24 | 5 | Virtual Path | BR571 | | | | |
| 3 | 192.175.59.0/24 | 5 | Virtual Path | BR572 | | | | |
| 4 | 192.175.60.0/24 | 5 | Virtual Path | BR573 | | | | |
| 5 | 192.175.61.0/24 | 5 | Virtual Path | BR574 | | | | |
| 6 | 192.175.62.0/24 | 5 | Virtual Path | BR575 | | | | |
| 7 | 172.111.64.5/24 | 5 | Local | | | | | |
| 8 | 172.111.65.5/24 | 5 | Local | | | | | |
| 9 | 0.0.0.0/0 | 65535 | Passthrough | | | | | |

Konfiguration der Inline-Bereitstellung von Zweigstandort

Im Folgenden sind die Konfigurationsschritte auf hoher Ebene zum Konfigurieren von Zweigstandort für die Inline-Bereitstellung aufgeführt:

1. Erstellen Sie eine Zweigwebsite.
2. Füllen Sie Schnittstellengruppen basierend auf angeschlossenen Ethernet-Schnittstellen aus.
3. Erstellen Sie eine virtuelle IP-Adresse für jede virtuelle Schnittstelle.
4. Füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht mit Burst-Geschwindigkeiten mithilfe von Internet- und MPLS-Links.
5. Füllen Sie Routen aus, wenn mehr Subnetze in der LAN-Infrastruktur vorhanden sind.

So erstellen Sie eine Zweigwebsite

1. Navigieren Sie zu **Konfigurationseditor** > **Sites** und klicken Sie auf die Schaltfläche **“+” Hinzufügen**.
2. Füllen Sie die Felder wie unten gezeigt.
3. Behalten Sie die Standardeinstellungen bei, wenn Sie nicht dazu aufgefordert werden.

Add

Site Name:

BR_Site

Secure Key:

dd40529b4c910e...

Model:

210

Sub Model:

BASE

Mode:

client

Site Location:

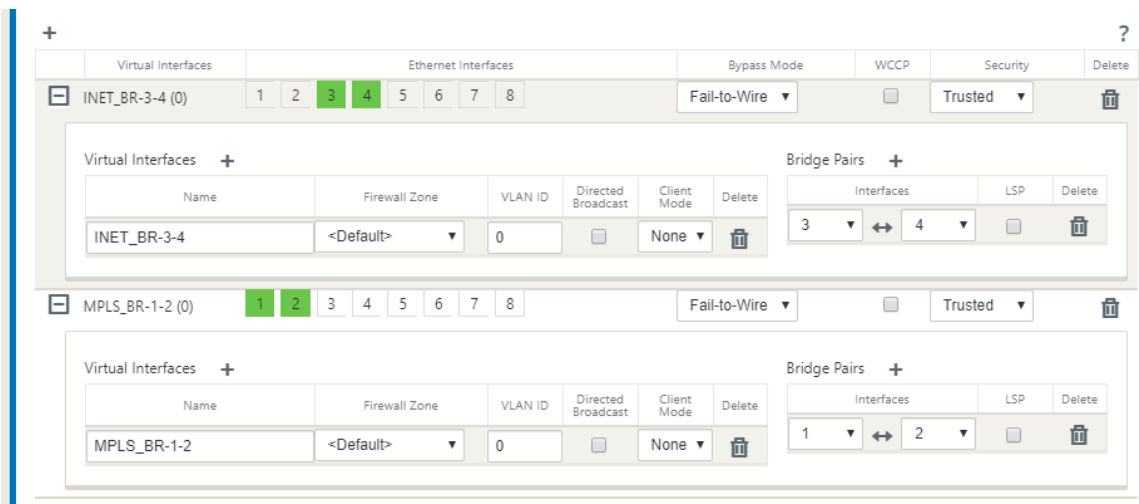
Add

Cancel

The screenshot shows the Citrix SD-WAN configuration interface. At the top, there are tabs: Basic, Global, Sites (selected), Connections, Optimization, and Provisioning. Below the tabs, the 'Region' is set to 'Default_Region'. The 'Site' dropdown is set to 'BR_Site'. To the right of the dropdown are buttons: '+ Site', 'Site' (with a copy icon), and 'Site' (with a delete icon). Below these is a list of configuration options for the selected site: Basic Settings (selected), Centralized Licensing, Routing Domains, Link Aggregation Groups, Interface Groups, Virtual IP Addresses, VRRP, DHCP, DNS, Proxy Auto-config settings, WAN Links, Certificates, and High Availability. To the right of this list is a detailed configuration form for the 'BR_Site'. The form includes fields for Site Name (BR_Site), Appliance Name (BR_Site-210), Secure Key (dd40529b4c910e... with a Regenerate button), Model (210), Sub Model (BASE), Mode (client), Site Location, Default Direct Route Cost (5), Gateway ARP Timer (ms) (1000), Host ARP Timer (ms) (1000), and a checkbox for 'Enable Source MAC Learning'. At the bottom of the form are 'Apply' and 'Refresh' buttons.

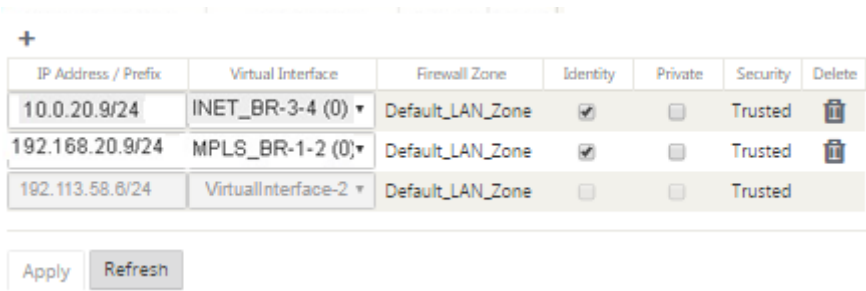
So füllen Sie Schnittstellengruppen basierend auf angeschlossenen Ethernet-Schnittstellen aus

1. Navigieren Sie im **Konfigurations-Editor** zu **Sites > Site anzeigen > [Client-Site-Name] > Schnittstellengruppen**. Klicken Sie auf **+**, um Schnittstellen hinzuzufügen, die verwendet werden sollen. Für den Inline-Modus werden jeder Schnittstellengruppe zwei Ethernet-Schnittstellen zugewiesen.
2. Der Bypass-Modus ist auf **Fail-to-Wire-Modus** eingestellt und Bridge Pair wird über die beiden Ethernet-Schnittstellen erstellt.
3. Lesen Sie das Beispiel Remote Site Inline Mode Topologie oben und füllen Sie die Schnittstellengruppen Felder wie unten dargestellt.



So erstellen Sie VIP-Adresse (Virtual IP) für jede virtuelle Schnittstelle

- 1. Erstellen Sie für jeden WAN-Link eine virtuelle IP-Adresse im entsprechenden Subnetz. VIPs werden für die Kommunikation zwischen zwei SD-WAN-Appliances in der virtuellen WAN-Umgebung verwendet.



So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten mithilfe des Internetlinks aus:

- 1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+**, um einen WAN-Link für den Internetlink hinzuzufügen.
- 2. Füllen Sie Details zum Internetlink, einschließlich der öffentlichen IP-Adresse Auto Detect, wie unten dargestellt.
- 3. Navigieren Sie zu **Access Interfaces**, klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den Internetlink hinzuzufügen.
- 4. Fügen Sie das Access Interface für IP-Adresse und Gateway wie unten gezeigt ein.

WAN Link: **BR571-WL-1** Section: **Settings** [+ Add Link](#) [Delete Link](#)

Basic Settings ?

Note: Changing the access type of this WAN Link may cause automatically generated **Paths** to this link to be added or removed.

Link Name:

Access Type: **Public Internet** WAN Link Template: **<None>**

LAN to WAN

Physical Rate (kbps):

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps):

WAN to LAN

Physical Rate (kbps):

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps):

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Delete |
|------------------|-------------------|------------|--------------------|-------------------|-------------------------------------|------------------------|
| SJC_BR-INET-AI-1 | INET_BR-3-4 | 10.0.20.9 | 10.0.20.1 | Primary | <input checked="" type="checkbox"/> | Delete |

So erstellen Sie MPLS-Verknüpfung

1. Navigieren Sie zu WAN-Links, klicken Sie auf die Schaltfläche **+**, um einen WAN-Link für den MPLS-Link hinzuzufügen.
2. Füllen Sie MPLS-Link-Details wie unten gezeigt.
3. Navigieren Sie zu Access Interfaces und klicken Sie auf die Schaltfläche **+**, um für den MPLS-Link spezifische Schnittstellendetails hinzuzufügen.
4. Fügen Sie das Access Interface für IP-Adresse und Gateway wie unten gezeigt ein.

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Private MPLS

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Delete |
|-----------------|-------------------|--------------|--------------------|-------------------|-------------------------------------|--------|
| SJC_BR-MPLS-... | MPLS_BR-1-2 | 192.168.20.9 | 192.168.20.1 | Primary | <input checked="" type="checkbox"/> | |

So füllen Sie Routen aus

Routen werden automatisch basierend auf der obigen Konfiguration erstellt. Falls es mehr Subnetze für diese Remote-Zweigstelle gibt, müssen bestimmte Routen hinzugefügt werden, die angeben, welches Gateway den Datenverkehr leitet, um diese Back-End-Subnetze zu erreichen.

Search:

| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|-------|--------------|--------------|--------------------|------|------|--------|
| 1 | 10.0.20.9/24 | 5 | Local | | | | | |
| 2 | 192.168.20.9/24 | 5 | Local | BR571 | | | | |
| 3 | 192.175.59.0/24 | 5 | Virtual Path | BR572 | | | | |
| 4 | 192.175.60.0/24 | 5 | Virtual Path | BR573 | | | | |
| 5 | 192.175.61.0/24 | 5 | Virtual Path | BR574 | | | | |
| 6 | 192.175.62.0/24 | 5 | Virtual Path | BR575 | | | | |
| 7 | 172.111.64.5/24 | 5 | Local | | | | | |
| 8 | 172.111.65.5/24 | 5 | | | | | | |
| 9 | 0.0.0.0/0 | 65535 | Passthrough | | | | | |

1

Beheben von Überwachungsfehlern

Nach Abschluss der Konfiguration für DC- und Zweigstandorte werden Sie benachrichtigt, um Überwachungsfehler auf DC- und BR-Standorten zu beheben.

Standardmäßig generiert das System Pfade für WAN-Links, die als Zugriffstyp Public Internet definiert sind. Sie müssen die Autopfad-Gruppenfunktion verwenden oder Pfade manuell für WAN-Links mit dem Zugriffstyp Privates Internet aktivieren. Pfade für MPLS-Links können durch Klicken auf Operator hinzufügen (im grünen Rechteck) aktiviert werden.

The screenshot shows the 'Add Path' dialog box. It has a title bar with 'Add Path' and a close button. Inside, there are four dropdown menus arranged in a 2x2 grid. The first row contains 'From Site' (selected: DC_site) and 'From WAN Link' (selected: DC_site-MPLS). The second row contains 'To Site' (selected: BR_site) and 'To WAN Link' (selected: BR_site-MPLS). Below these dropdowns is a checkbox labeled 'Reverse Also' which is checked. At the bottom of the dialog are two buttons: 'Add' (highlighted in blue) and 'Cancel'.

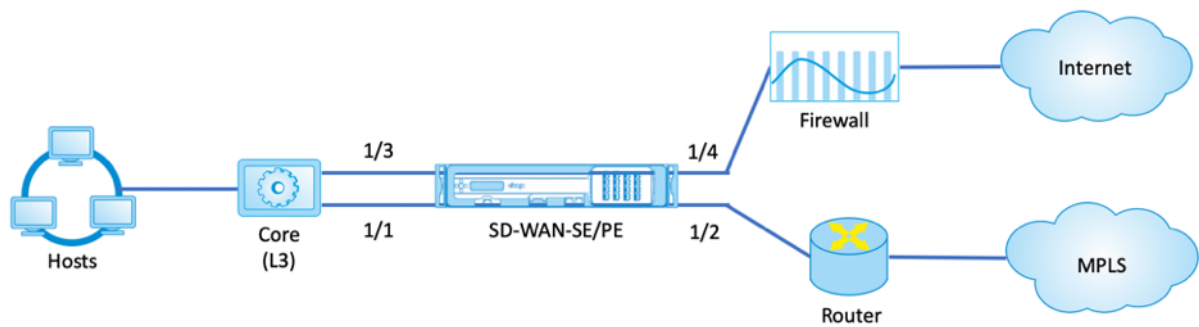
Nachdem Sie alle oben genannten Schritte ausgeführt haben, fahren Sie mit fort [Vorbereiten der SD-WAN-Appliance-Pakete](#).

Inlinemodus

May 10, 2021

Dieser Artikel enthält die Details zur Konfiguration eines Zweigs mit dem **Inline-Bereitstellungsmodus**. In diesem Modus scheint die SD-WAN-Appliance eine Ethernet-Brücke zu sein. Die meisten SD-WAN-Appliance-Modelle verfügen über eine **Fail-to-Wire-Feature** (Ethernet-Bypass) für den Inlinemodus. Wenn die Stromversorgung ausfällt, schließt sich ein Relais und die Eingangs- und Ausgangsanschlüsse werden elektrisch angeschlossen, so dass das Ethernet-Signal von einem Port zum anderen weitergeleitet wird. Im Fail-to-Wire-Modus sieht die SD-WAN-Appliance wie ein Cross-Over-Kabel aus, das die beiden Anschlüsse verbindet.

Im folgenden Diagramm Schnittstellen 1/1 und 1/2 sind Hardware-Bypass-Paare und werden Fail-to-Wire verbinden den Core mit der Kante MPLS Router. Die Schnittstellen 1/3 und 1/4 sind auch Hardware-Bypass-Paare und werden Fail-to-Wire verbinden den Core mit der Edge-Firewall.



Konfiguration der Inline-Bereitstellung von Zweigstandort

Im Folgenden sind die Konfigurationsschritte auf hoher Ebene zum Konfigurieren von Zweigstandort für die Inline-Bereitstellung aufgeführt:

1. Erstellen Sie eine Zweigwebsite.
2. Füllen Sie Schnittstellengruppen basierend auf angeschlossenen Ethernet-Schnittstellen aus.
3. Erstellen Sie eine virtuelle IP-Adresse für jede virtuelle Schnittstelle.
4. Füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht mit Burst-Geschwindigkeiten mithilfe von Internet- und MPLS-Links.
5. Füllen Sie Routen aus, wenn mehr Subnetze in der LAN-Infrastruktur vorhanden sind.

So erstellen Sie eine Zweigwebsite

1. Navigieren Sie zu **Konfigurationseditor > Sites** und klicken Sie auf **+ Schaltfläche Hinzufügen**.
2. Behalten Sie die Standardeinstellungen bei, wenn Sie nicht dazu aufgefordert werden.

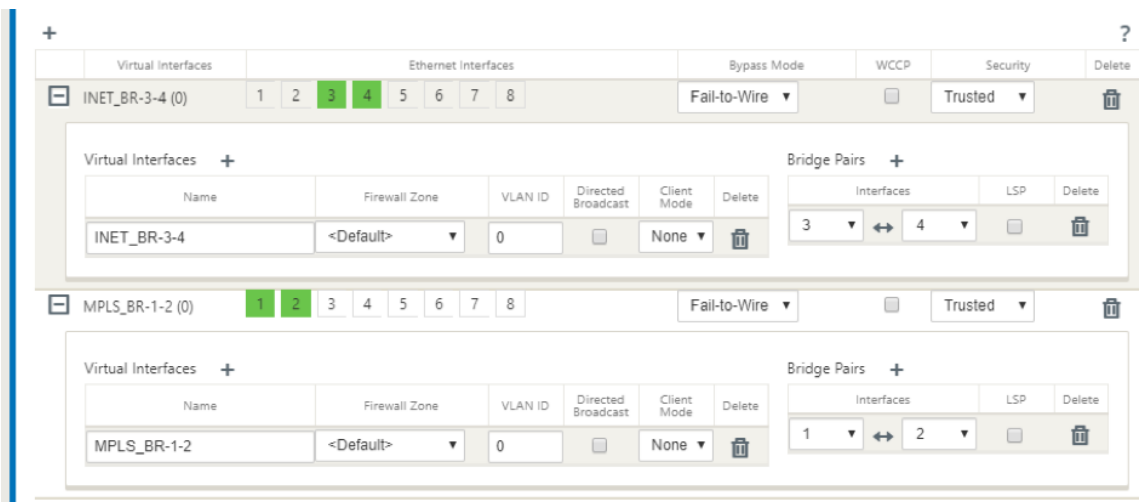
The screenshot displays the Citrix SD-WAN configuration interface. At the top, there are tabs for 'Basic', 'Global', 'Sites' (selected), 'Connections', 'Optimization', and 'Provisioning'. Below the tabs, the 'Region' is set to 'Default_Region'. The 'Site' dropdown is set to 'BR_Site', with buttons for '+ Site', 'Site', and 'Site'. A sidebar on the left lists various configuration options under the 'Sites' heading, with 'Basic Settings' selected. The main configuration area on the right shows the following fields:

- Site Name:** BR_Site
- Appliance Name:** BR_Site-210
- Secure Key:** dd40529b4c910e... (with a 'Regenerate' button)
- Model:** 210
- Sub Model:** BASE
- Mode:** client
- Site Location:** (empty field)
- Default Direct Route Cost:** 5
- Gateway ARP Timer (ms):** 1000
- Host ARP Timer (ms):** 1000
- ☐ **Enable Source MAC Learning**

At the bottom of the configuration area, there are 'Apply' and 'Refresh' buttons.

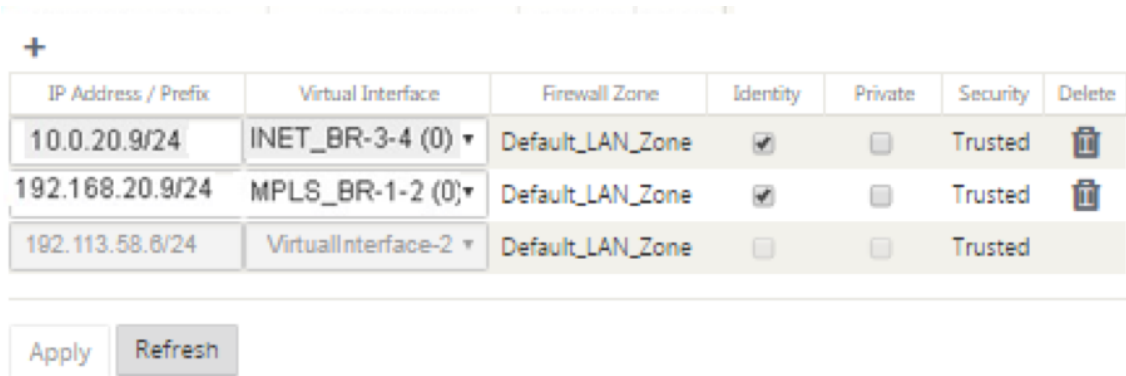
So füllen Sie Schnittstellengruppen basierend auf angeschlossenen Ethernet-Schnittstellen aus

1. Navigieren Sie im Konfigurations-Editor zu **Sites > Site anzeigen > [Client-Site-Name] > Schnittstellengruppen**. Klicken Sie auf **+**, um Schnittstellen hinzuzufügen, die verwendet werden sollen. Für den Inline-Modus werden jeder Schnittstellengruppe zwei Ethernet-Schnittstellen zugewiesen.
2. Der Bypass-Modus ist auf **Fail-to-Wire-Modus** eingestellt und Bridge Pair wird über die beiden Ethernet-Schnittstellen erstellt.
3. Sehen Sie sich die Beispieltopologie oben an, und füllen Sie die Felder "Schnittstellengruppen" wie unten dargestellt aus.



So erstellen Sie VIP-Adresse (Virtual IP) für jede virtuelle Schnittstelle

- 1. Erstellen Sie für jeden WAN-Link eine virtuelle IP-Adresse im entsprechenden Subnetz. VIPs werden für die Kommunikation zwischen zwei SD-WAN-Appliances in der virtuellen WAN-Umgebung verwendet.



So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten über Internetlinks aus

- 1. Navigieren Sie zu **WAN-Links**, klicken Sie auf +, um einen WAN-Link für den Internetlink hinzuzufügen.
- 2. Füllen Sie Details zum Internetlink, einschließlich der öffentlichen IP-Adresse Auto Detect, wie unten dargestellt.
- 3. Navigieren Sie zu **Access Interfaces**, klicken Sie auf +, um für den Internetlink spezifische Schnittstellendetails hinzuzufügen.
- 4. Fügen Sie das Access Interface für IP-Adresse und Gateway wie unten gezeigt ein.

WAN Link: BR571-WL-1

Section: Settings

+ Add Link

Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Public Internet

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):

10000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Delete |
|------------------|-------------------|------------|--------------------|-------------------|-------------------------------------|--------|
| SJC_BR-INET-AI-1 | INET_BR-3-4 | 10.0.20.9 | 10.0.20.1 | Primary | <input checked="" type="checkbox"/> | |

So erstellen Sie MPLS-Verknüpfung

1. Navigieren Sie zu **WAN-Links**, klicken Sie auf **+**, um einen WAN-Link für den MPLS-Link hinzuzufügen.
2. Füllen Sie MPLS-Link-Details wie unten gezeigt.
3. Navigieren Sie zu **Access Interfaces**, klicken Sie auf **+**, um für den MPLS-Link spezifische Schnittstellendetails hinzuzufügen.
4. Fügen Sie das Access Interface für IP-Adresse und Gateway wie unten gezeigt ein.

Basic Settings?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Private MPLS

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy/ARP | Delete |
|-----------------|-------------------|--------------|--------------------|-------------------|-------------------------------------|--------|
| SJC_BR-MPLS-... | MPLS_BR-1-2 | 192.168.20.9 | 192.168.20.1 | Primary | <input checked="" type="checkbox"/> | |

So füllen Sie Routen aus

Routen werden automatisch basierend auf der obigen Konfiguration erstellt. Falls es mehr Subnetze für diese Remote-Zweigstelle gibt, müssen bestimmte Routen hinzugefügt werden, die angeben, welches Gateway den Datenverkehr leitet, um diese Back-End-Subnetze zu erreichen.

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

292

Search:

| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|-------|--------------|--------------|--------------------|------|------|--------|
| 1 | 10.0.20.9/24 | 5 | Local | | | | | |
| 2 | 192.168.20.9/24 | 5 | Local | BR571 | | | | |
| 3 | 192.175.59.0/24 | 5 | Virtual Path | BR572 | | | | |
| 4 | 192.175.60.0/24 | 5 | Virtual Path | BR573 | | | | |
| 5 | 192.175.61.0/24 | 5 | Virtual Path | BR574 | | | | |
| 6 | 192.175.62.0/24 | 5 | Virtual Path | BR575 | | | | |
| 7 | 172.111.64.5/24 | 5 | Local | | | | | |
| 8 | 172.111.65.5/24 | 5 | | | | | | |
| 9 | 0.0.0.0/0 | 65535 | Passthrough | | | | | |

1

Virtueller Inline-Modus

October 28, 2021

Im virtuellen Inlinemodus verwendet der Router ein Routing-Protokoll wie PBR, OSPF oder BGP, um eingehenden und ausgehenden WAN-Verkehr an die Appliance umzuleiten, und die Appliance leitet die verarbeiteten Pakete zurück an den Router.

Im folgenden Artikel wird die schrittweise Vorgehensweise zum Konfigurieren von zwei SD-WAN (SD-WAN SE) -Appliances beschrieben:

- Rechenzentrums-Appliance im virtuellen Inlinemodus
- Gerät im Inline-Modus verzweigen
- Das Routing-Protokoll muss entweder am Core-Switch oder weiter stromaufwärts am Router konfiguriert werden. Der Router muss den Zustand der SD-WAN-Appliance überwachen, damit die Appliance bei einem Ausfall umgangen werden kann.
- Im virtuellen Inlinemodus wird die SD-WAN-Appliance physisch aus dem Pfad versetzt (ein-armige Bereitstellung), dh es muss nur eine einzige Ethernet-Schnittstelle verwendet werden (Beispiel: Schnittstelle 1/5), wobei der Bypass-Modus auf Fail-to-Block (FTB) eingestellt ist. Die Citrix SD-WAN Appliance muss so konfiguriert sein, dass Datenverkehr an das richtige Gateway weitergeleitet wird. Der für den virtuellen Pfad vorgesehene Datenverkehr wird auf die SD-WAN-Appliance gerichtet und dann gekapselt und an die entsprechende WAN-Verbindung

geleitet.

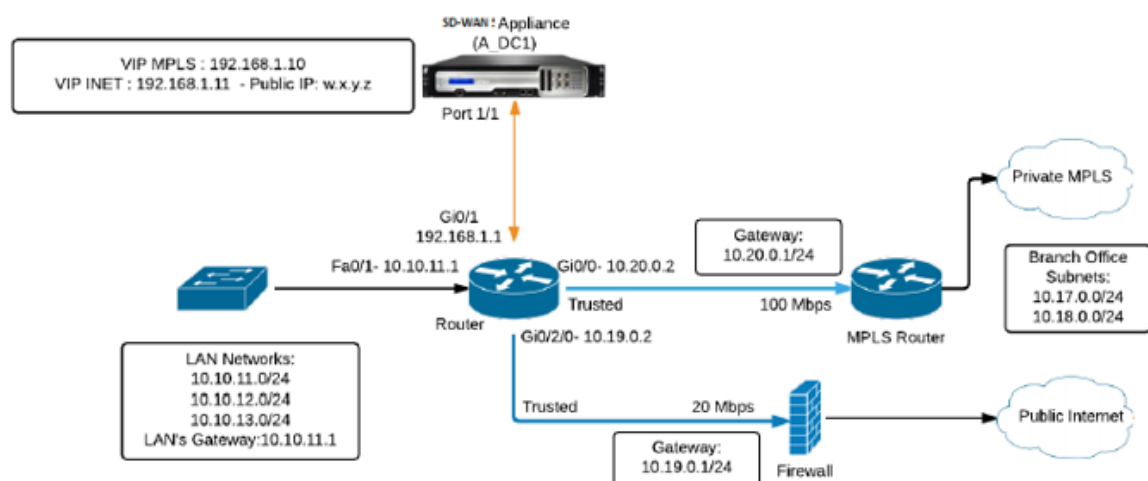
Sammeln Sie Informationen

Sammeln Sie die folgenden Informationen, die für die Konfiguration des virtuellen Inlinemodus erforderlich sind:

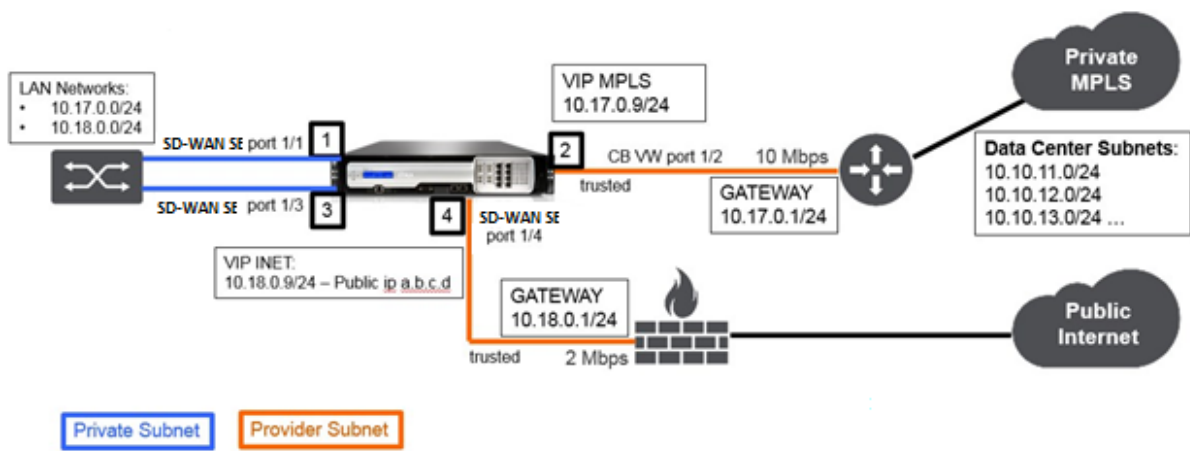
- Genaues Netzwerkschema Ihrer lokalen und Remotestandorte, einschließlich:
 - Lokale und Remote-WAN-Verbindungen und ihre Bandbreiten in beide Richtungen, ihre Subnetze, virtuellen IP-Adressen und Gateways von jeder Verbindung, Routen und VLANs.
- Tabelle für die Bereitstellung

Das Folgende ist ein Beispiel für ein Netzwerkschema und eine Bereitstellungstabelle:

Rechenzentrumstopologie — Virtueller Inline-Modus



Zweigtopologie —Inline-Modus



| Sitename | Rechenzentrums-Standort | Niederlassungsstandort |
|----------------------------|--|---|
| Appliance-Name | SJC-DC | SJC-BR |
| Management-IP | 172.30.2.10/24 | 172.30.2.20/24 |
| Sicherheits-Schlüssel | Falls vorhanden | Falls vorhanden |
| Modell/Edition | 4000 | 2000 |
| Modus | Virtueller Inlinemodus | Inline |
| Topologie | 2 x WAN-Pfad | 2 x WAN-Pfad |
| VIP-Adresse | 192.168.1.10/24 —MPLS, 192.168.2.10/24 —Internet, öffentliche IP w.x.y.z | 10.17.0.9/24 - MPLS, 10.18.0.9/24 —Internet, öffentliche IP a.b.c.d |
| Gateway-MPLS | 10.20.0.1 | 10.17.0.1 |
| Gateway-Internet | 10.19.0.1 | 10.18.0.1 |
| Verbindungsgeschwindigkeit | MPLS —100 Mbit/s, Internet — 20 Mbit/s | MPLS —10 Mbit/s, Internet —2 Mbit/s |

| Sitename | Rechenzentrums-Standort | Niederlassungsstandort |
|----------|---|---|
| Route | Sie müssen eine Route auf der SD-WAN SE Appliance hinzufügen, wie Sie die LAN-Subnetze (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24 usw.) über eine der physischen Schnittstellen erreichen: Gi0/1 - 192.168.1.1, Konfiguration > Virtuelles WAN > Konfigurationseditor > SJC_DC\ > Routes . In diesem Beispiel wurde die Schnittstelle 192.168.1.1 verwendet n/w Adresse: 10.10.13.0/24, 10.10.12.0/24, 10.10.11.0/24, - Servicetyp: lokal, - Gateway-IP-Adresse: 192.168.1.1 | Es wurden keine zusätzlichen Strecken hinzugefügt |
| VLANs | MPLS - VLAN 10, Internet - VLAN 20 | Keine (Standard 0) |

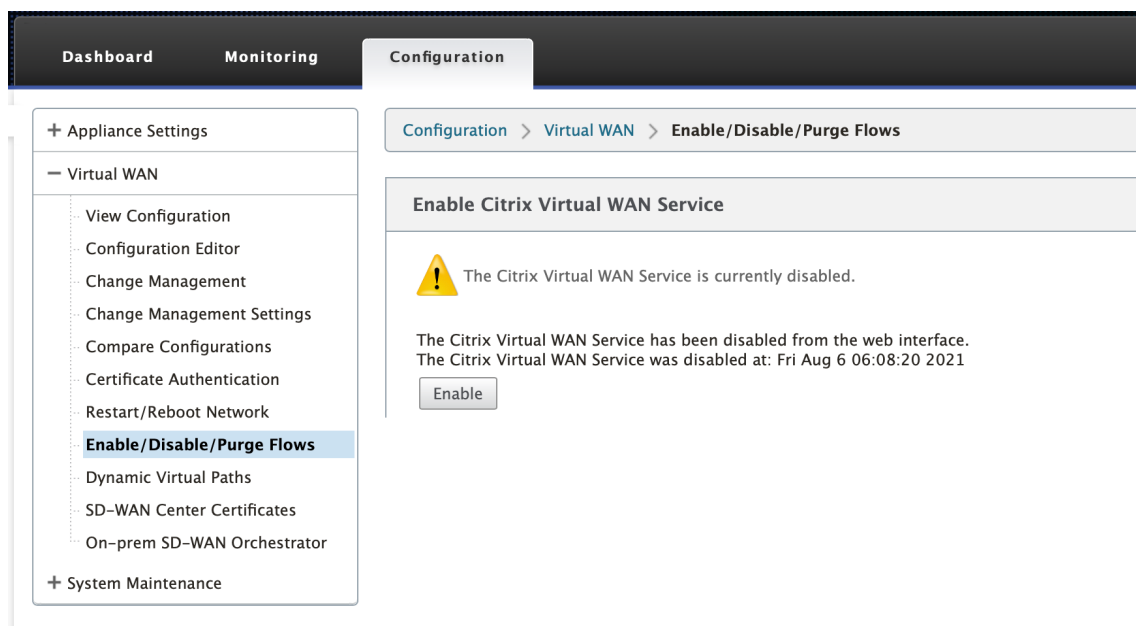
Voraussetzungen

1. Navigieren Sie in der Webverwaltungsoberfläche der SD-WAN-Appliance zu **Konfiguration > Appliance-Einstellungen > Administratorschnittstelle > Verschiedenes** und klicken Sie auf **Switch-Konsole**.

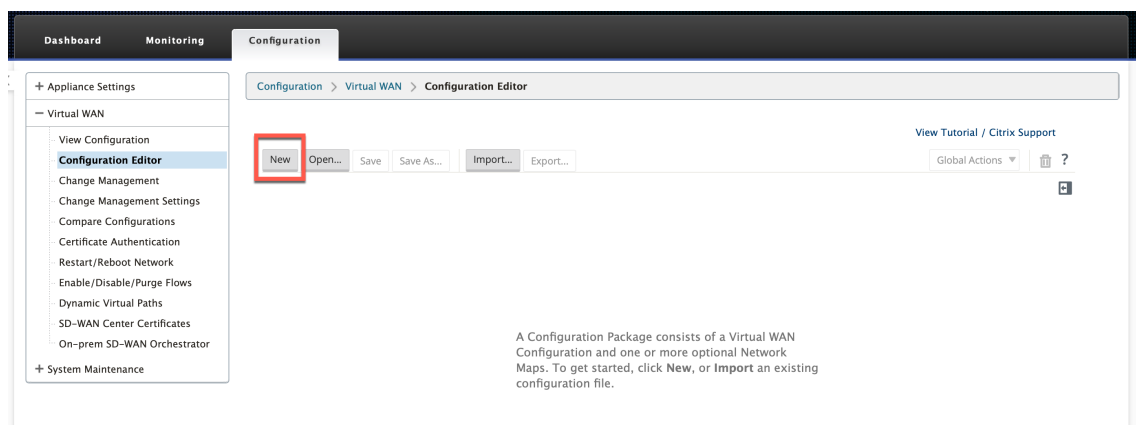
Hinweis

Wenn **Switch to Client Console** angezeigt wird, befindet sich die Appliance bereits im MCN-Modus. Sie müssen nur einen aktiven MCN in einem SD-WAN-Netzwerk haben.

2. Navigieren Sie zu **Konfiguration > Virtuelles WAN > Aktivieren/Deaktivieren/Bereinigen von Flows** und klicken Sie im Abschnitt **Citrix Virtual WAN-Dienst aktivieren** auf **Aktivieren**.



3. Starten Sie Konfiguration, indem Sie zu **Konfiguration > Virtuelles WAN > Konfigurationseditor** navigieren. Klicken Sie auf **Neu**, um mit der Konfiguration zu beginnen. Durch Klicken auf **Neu** wird eine anfängliche Konfigurationsdatei mit **Untitled_1** als Dateinamen erstellt. Sie können die Datei später [optional] mit der Schaltfläche **Speichern** unter umbenennen.



Rechenzentrumsstandort —Konfiguration des virtuellen Inlinemodus

Erstellen eines Rechenzentrumsstandorts

1. Navigieren Sie zu **Konfiguration > Virtual WAN > Konfigurationseditor > Sites** und klicken Sie auf **+ Site**.
2. Geben Sie den Site-Namen und den Standort ein. Wählen Sie das **Appliance-Modell** aus der Dropdownliste Modell und **Primärer MCN** aus der Dropdownliste Modus aus.
3. Klicken Sie auf **Hinzufügen**.

Add

Site Name:
SJC-DC

Secure Key:
f7944db45d32ca14

Model:
4000 ▼

Mode:
primary MCN ▼

Site Location:
AMER

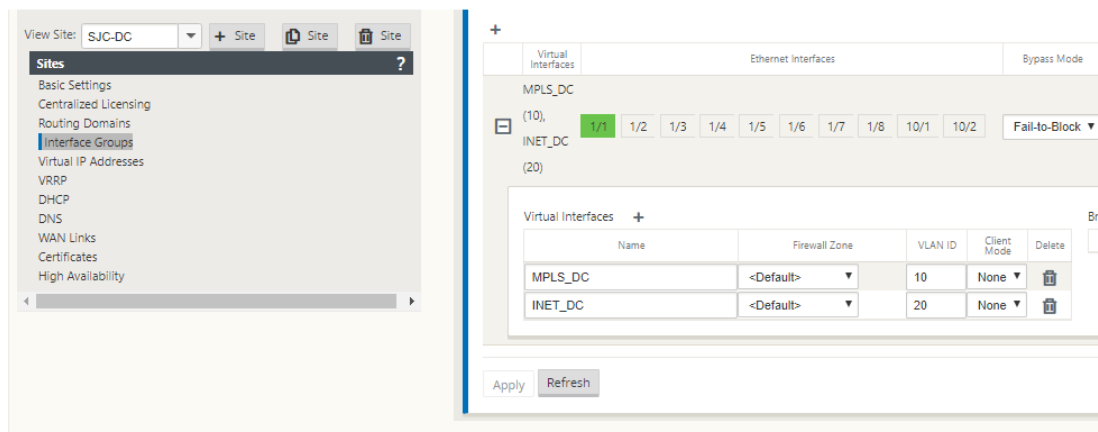
☒ Enable Site as Intermediate Node

Add **Cancel**

Konfigurieren von Schnittstellengruppen basierend auf verbundenen Ethernet-Schnittstellen

In der Konfiguration des virtuellen Inlinemodus wird nur eine Ethernet-Schnittstelle verwendet, dh die Schnittstelle, die den Upstream-Router verbindet, was Auswirkungen auf die Routing-Richtlinie bietet (Beispiel-Interface 1/5). Der Bypass-Modus ist auf Fail-to-Block (FTB) eingestellt, da nur eine Ethernet/physische Schnittstelle pro virtueller Schnittstelle verwendet wird. Außerdem gibt es keine Bridge Pairs.

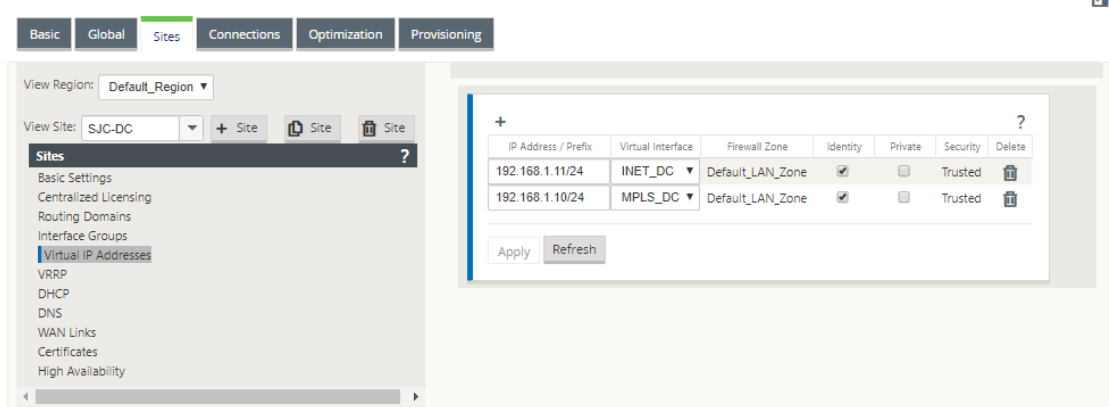
1. Navigieren Sie im **Konfigurationseditor** zu **Sites > [Site-Name] > Schnittstellengruppen**. Klicken Sie auf **+**, um Schnittstellen hinzuzufügen, die verwendet werden sollen.
2. Wählen Sie die Ethernet-Schnittstelle aus, die mit dem Upstream-Router verbunden wird, und klicken Sie neben Virtuelle Schnittstellen auf **+**. Fügen Sie die virtuellen Schnittstellen für MPLS- und Internetverbindungen hinzu. Fügen Sie gemäß der Beispieltopologie Folgendes hinzu:
 - Virtuelle Schnittstelle **MPLS** konfiguriert auf **VLAN 10**
 - Virtuelle Schnittstelle **INTERNET** konfiguriert auf **VLAN 20**
3. Wählen Sie in der Dropdownliste **Bypass-Modus** die Option **Fail-to-block** aus. Klicken Sie auf **Apply**.



Erstellen Sie eine virtuelle IP-Adresse für jede virtuelle Schnittstelle

Erstellen Sie für jeden WAN-Link eine virtuelle IP (VIP) -Adresse im entsprechenden Subnetz. VIPs werden für die Kommunikation zwischen zwei SD-WAN-Appliances in der virtuellen WAN-Umgebung verwendet.

1. Navigieren Sie im **Konfigurationseditor** zu **Sites >[Site-Name] > Virtuelle IP-Adressen**. Klicken Sie auf **+**, um VIPs zu erstellen.
2. Geben Sie die IP-Adresse/das Präfix ein und wählen Sie die entsprechende virtuelle Schnittstelle für MPLS und Internet aus.
3. Klicken Sie auf **Apply**.



Internet-WAN-Link erstellen

Erstellen Sie eine Internet-WAN-Verbindung basierend auf der physischen Rate und nicht auf Burst-Geschwindigkeiten.

1. Navigieren Sie im **Konfigurationseditor** zu **Sites > [Site-Name] > WAN-Links** und klicken Sie auf **+ Link**. Geben Sie einen Namen ein und wählen Sie **Zugriffstyp** als **öffentliches Internet**. Klicken Sie auf **Hinzufügen**.
2. Geben Sie den physikalischen Tarif ein. Aktivieren Sie nicht das Kontrollkästchen **Öffentliche IP automatisch erkennen**. Für die SD-WAN-Appliance, die als MCN konfiguriert ist, kann das Kontrollkästchen **Öffentliche IP automatisch erkennen** nicht aktiviert werden.

The screenshot displays the 'Basic Settings' configuration page for a WAN link. At the top, the 'WAN Link' dropdown is set to 'SJC-DC-INET' and the 'Section' dropdown is set to 'Settings'. There are buttons for '+ Add Link' and 'Delete Link'.

Basic Settings

- Link Name:** SJC-DC-INET
- Access Type:** Public Internet
- WAN Link Template:** <None>

LAN to WAN

- Physical Rate (kbps):** 20000
- ☒ Set Permitted From Physical
- Permitted Rate (kbps):** 20000

WAN to LAN

- Physical Rate (kbps):** 20000
- ☒ Set Permitted From Physical
- Permitted Rate (kbps):** 20000

Tracking IP Address: [Empty text box]

☐ Autodetect Public IP

Public IP Address: [Empty text box]

Advanced Settings

- Eligibility**
- Metered/Standby Link**
- Provisioning**

At the bottom, there are 'Apply' and 'Revert' buttons.

3. Wählen Sie in der Dropdownliste **Abschnitt** die Option **Zugriffsschnittstellen** aus und klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den Internetlink hinzuzufügen.

4. Geben Sie die virtuelle Internet-WAN-IP-Adresse und die Gateway-Adresse ein. Der Proxy ARP wird nicht auf weniger als zwei Ethernet-Schnittstellen überprüft.
5. Klicken Sie auf **Apply**.

The screenshot shows the 'WAN Link' configuration page for 'SJC-DC-INET'. The 'Section' is set to 'Access Interfaces'. There are buttons for '+ Add Link' and 'Delete Link'. Below is a table with one entry:

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Gateway MAC Address Binding | Delete |
|------------------|-------------------|--------------|--------------------|-------------------|--------------------------|-------------------------------------|--------|
| SJC-DC-INET-AI-1 | INET_DC | 192.168.1.11 | 192.168.1.1 | Primary | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

At the bottom of the table are 'Apply' and 'Refresh' buttons.

Erstellen Sie einen MPLS-Link

1. Wählen Sie auf der Seite **Sites > [Site-Name] > WAN-Links** in der Dropdownliste **Abschnitt** die Option **Einstellungen** aus. Klicken Sie auf die Schaltfläche **+ Link**, um einen WAN-Link für MPLS hinzuzufügen.
2. Geben Sie den Namen des MPLS WAN Link ein und wählen Sie **Zugriffstyp** als **privates Intranet** aus. Klicken Sie auf **Hinzufügen**.
3. Geben Sie den physischen Tarif und andere Details ein. Klicken Sie auf **Apply**.

Basic Settings?

LAN to WAN

Physical Rate (kbps):
100000

☒ Set Permitted From Physical

Permitted Rate (kbps):
100000

WAN to LAN

Physical Rate (kbps):
100000

☒ Set Permitted From Physical

Permitted Rate (kbps):
100000

Access Type:
Private Intranet

☐ Autodetect Public IP

Public IP Address:

Tracking IP Address:

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Gateway MAC Address Binding | Delete |
|------------------|-------------------|--------------|--------------------|-------------------|--------------------------|-------------------------------------|--------|
| SJC-DC-MPLS-A... | MPLS_DC | 192.168.1.10 | 192.168.1.9 | Primary | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

4. Wählen Sie in der Dropdownliste **Abschnitt** die Option **Zugriffsschnittstellen** aus und klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den MPLS-Link hinzuzufügen.
5. Geben Sie die MPLS Virtual IP-Adresse und Gateway-Adresse ein. Der Proxy ARP wird nicht auf weniger als zwei Ethernet-Schnittstellen überprüft.
6. Klicken Sie auf **Apply**.

WAN Link: SJC-DC-MPLS ⌵ Section: Access Interfaces (IPv4) ⌵

+ Link

Link

+

?

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Gateway MAC Address Binding | Delete |
|------------------|-------------------|--------------|--------------------|-------------------|--------------------------|-------------------------------------|--------|
| SJC-DC-MPLS-A... | MPLS_DC | 192.168.1.10 | 192.168.1.1 | Primary | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

Apply

Revert

Routen auffüllen

Fügen Sie auf der Seite des Rechenzentrums eine Route auf der SD-WAN-Appliance hinzu, wie Sie die LAN-Subnetze (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24 usw.) über eine der physischen Schnittstellen erreichen können.

0/1/0.1 —192.168.1.1 auf VLAN 10

0/1/0.2 —192.168.2.1 auf VLAN 20

In diesem Beispiel wird das Interface 192.168.1.1 verwendet.

Navigieren Sie im **Konfigurationseditor** zu **Verbindungen > Routen** und klicken Sie auf **+**, um die Routen hinzuzufügen.

Geben Sie die **Netzwerk-IP-Adresse**, die **Kosten** und die **Gateway-Adresse** ein. Klicken Sie auf **Hinzufügen**.

Edit?×

Network IP Address

10.10.11.0/24

Routing Domain

Default_RoutingD

Cost

5

Service Type

Local

Gateway IP Address

192.168.1.1

☒ Export Route

☐ Summary Route

☐ Eligibility Based On Path

Path:

<None>

☐ Eligibility Based On Gateway

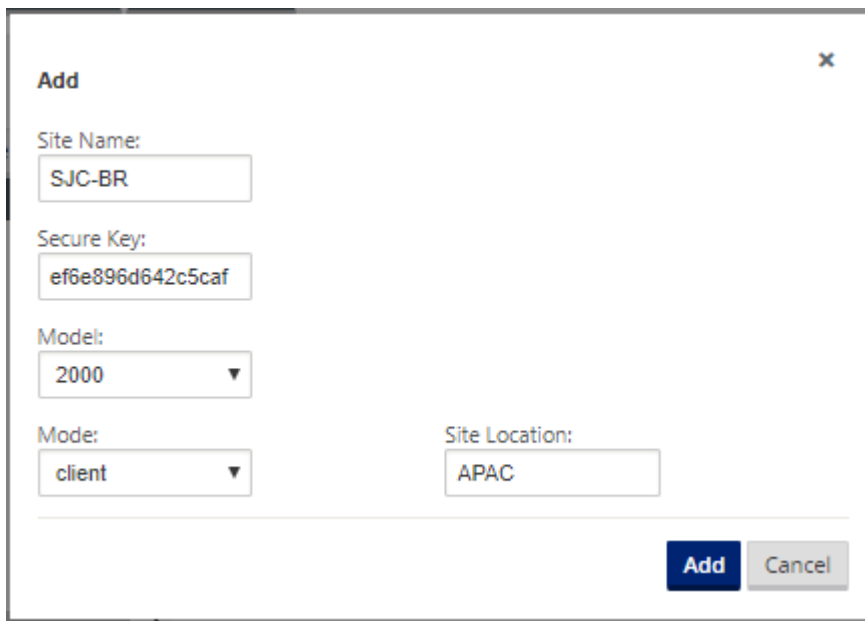
Apply

Cancel

Konfiguration der Inline-Bereitstellung von Zweigstandort

Erstellen eines Zweigstandorts

1. Navigieren Sie zu **Configuration Editor > Sites** und klicken Sie auf **+ Site**.
2. Geben Sie den Site-Namen und den Standort ein. Wählen Sie das **Appliance-Modell** aus der Dropdownliste Modell und **Client** aus der Dropdownliste Modus aus.
3. Klicken Sie auf **Hinzufügen**.



Add

Site Name:
SJC-BR

Secure Key:
ef6e896d642c5caf

Model:
2000

Mode:
client

Site Location:
APAC

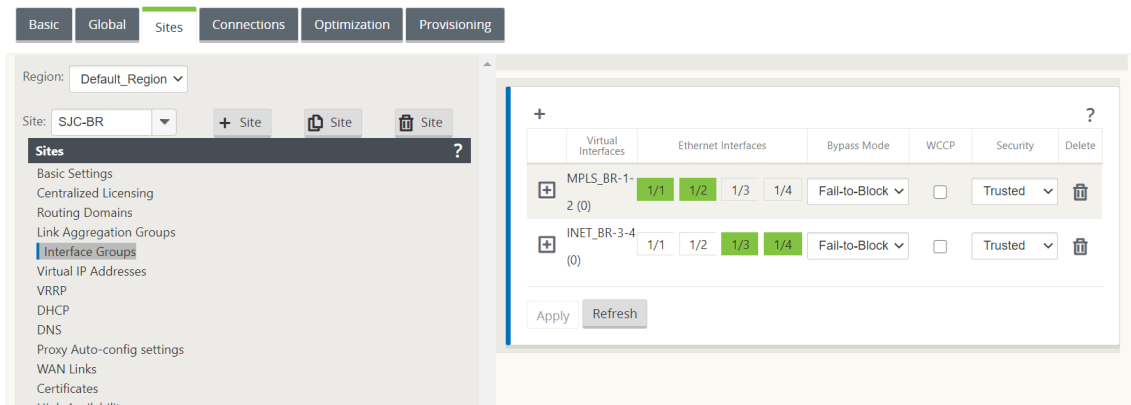
Add Cancel

Konfigurieren von Schnittstellengruppen basierend auf verbundenen Ethernet-Schnittstellen

1. Navigieren Sie im **Konfigurationseditor** zu **Sites > [Client-Site-Name] > Schnittstellengruppen**. Klicken Sie auf **+**, um Schnittstellen hinzuzufügen, die verwendet werden sollen. Für die Inline-Moduskonfiguration werden vier Ethernet-Schnittstellen verwendet; Schnittstellenpaar 1/3, 1/4 und Schnittstellenpaar 1/1 und 1/2.
2. Stellen Sie den **Bypass-Modus** auf Fail-to-Wire ein, da zwei Ethernet/physische Schnittstellen pro virtueller Schnittstelle verwendet werden. Es gibt zwei Brückenpaare.
3. Klicken Sie neben **Virtuelle Schnittstellen** auf **+** und füllen Sie WAN-Verbindungen basierend auf der physischen Rate und nicht auf Burst-Geschwindigkeiten mithilfe von Internet- und MPLS-Links.
 - Virtuelle Schnittstelle **INTERNET** konfiguriert auf Bridge-Paar 1/3 und 1/4
 - Virtuelle Schnittstelle **MPLS** konfiguriert auf Bridge Pair 1/1 und 1/2.

4. Klicken Sie neben **Bridge Pairs** auf **+** und erstellen Sie das Bridge-Paar, indem Sie die entsprechenden Schnittstellen auswählen.

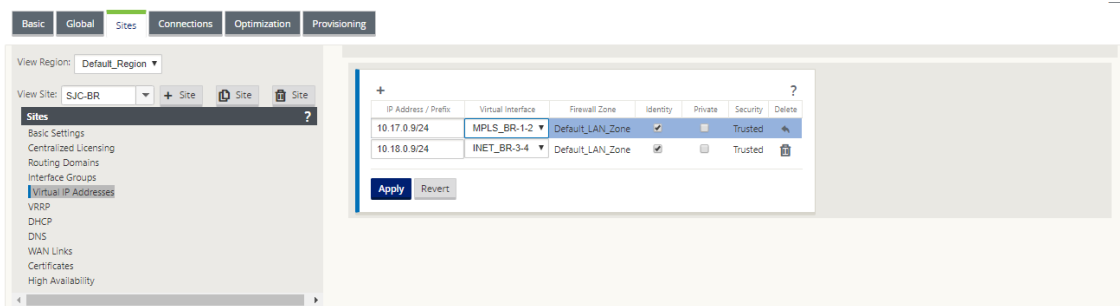
Lesen Sie das Diagramm **Zweigtopologie —Inline-Modus-Topologie** im Abschnitt [Voraussetzungen](#), und füllen Sie die Schnittstellengruppen aus.



Virtuelle IP-Adresse (VIP) für jede virtuelle Schnittstelle erstellen

Erstellen Sie für jeden WAN-Link eine virtuelle IP-Adresse im entsprechenden Subnetz. VIPs werden für die Kommunikation zwischen zwei SD-WAN-Appliances in der virtuellen WAN-Umgebung verwendet.

1. Navigieren Sie im **Konfigurationseditor** zu **Sites > [Site-Name] > Virtuelle IP-Adressen**. Klicken Sie auf **+**, um VIPs zu erstellen.
2. Geben Sie die IP-Adresse/das Präfix ein und wählen Sie die entsprechende virtuelle Schnittstelle für MPLS und Internet aus.
3. Klicken Sie auf **Apply**.



Internet-WAN-Link erstellen

So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten über Internetlinks aus

1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+ Link**, um einen WAN-Link für den Internetlink hinzuzufügen. Geben Sie einen Namen ein und wählen Sie **Zugriffstyp** als **öffentliches Internet**. Klicken Sie auf **Hinzufügen**.
2. Füllen Sie die Internetverbindungsdetails aus und aktivieren Sie das Kontrollkästchen **Öffentliche IP-Adresse automatisch erkennen**.
3. Wählen Sie in der Dropdownliste **Abschnitt** die Option **Zugriffsschnittstellen** aus und klicken Sie auf das **+**, um Schnittstellendetails für den Internetlink hinzuzufügen.
4. Geben Sie die virtuelle Internet-WAN-IP-Adresse und die Gateway-Adresse ein. Der Proxy ARP wird nicht auf weniger als zwei Ethernet-Schnittstellen überprüft.

The screenshot displays the Citrix SD-WAN configuration interface. At the top, there's a header bar with 'WAN Link: SJC-BR-INET', 'Section: Settings', and buttons for '+ Add Link' and 'Delete Link'.

The main content area is titled 'Basic Settings'. It includes a note: 'Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.' Below this, the 'Link Name' is 'SJC-BR-INET'. The 'Access Type' is set to 'Public Internet' and the 'WAN Link Template' is '<None>'. There are two sections for 'LAN to WAN' and 'WAN to LAN' settings, each with 'Physical Rate (kbps)' and 'Permitted Rate (kbps)' set to 2000, and checkboxes for 'Set Permitted From Physical' (checked) and 'Auto Learn' (unchecked). A 'Tracking IP Address' field is present. The 'Autodetect Public IP' checkbox is checked, and a 'Public IP Address' field is shown.

At the bottom, there's a navigation bar with tabs: 'Basic', 'Global', 'Sites', 'Connections', 'Optimization', and 'Provisioning'. The 'Sites' tab is active, showing a 'View Region' dropdown set to 'Default_Region'. Below this, there's a 'View Site' dropdown set to 'SJC-BR' and buttons for '+ Site', 'Site', and 'Delete Site'. A sidebar on the left lists various configuration options under 'Sites', with 'Virtual IP Addresses' selected. The main area shows a table of virtual interfaces:

| IP Address / Prefix | Virtual Interface | Firewall Zone | Identity | Private | Security | Delete |
|---------------------|-------------------|------------------|-------------------------------------|--------------------------|----------|--------|
| 10.17.0.9/24 | MPLS_BR-1-2 | Default_LAN_Zone | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Trusted | |
| 10.16.0.9/24 | INET_BR-3-4 | Default_LAN_Zone | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Trusted | |

Buttons for 'Apply' and 'Revert' are at the bottom of the table.

Erstellen Sie eine MPLS-WAN-Verbindung

1. Navigieren Sie zu **WAN-Links** und wählen Sie **Einstellungen** aus der Dropdownliste **Abschnitt** aus. Klicken Sie auf die Schaltfläche **+ Link**, um einen WAN-Link für den MPLS-Link hinzuzufügen.
2. Geben Sie den Namen des MPLS WAN Link und andere Details ein. Wählen Sie **Zugriffstyp** als **privates Intranet** aus.

WAN Link: **SJC-BR-MPLS** Section: **Settings** **+ Add Link** **Delete Link**

Basic Settings

Link Name: **SJC-BR-MPLS**

Access Type: **Private MPLS** WAN Link Template: **<None>**

LAN to WAN

Physical Rate (kbps): **10000**

☒ Set Permitted From Physical

Permitted Rate (kbps): **10000**

WAN to LAN

Physical Rate (kbps): **10000**

☒ Set Permitted From Physical

Permitted Rate (kbps): **10000**

MPLS Queues **+ Add**

Advanced Settings

Metered/Standby Link

Provisioning

Apply **Revert**

3. Wählen Sie in der Dropdownliste **Abschnitt** die Option **Zugriffsschnittstellen** aus und klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den MPLS-Link hinzuzufügen.
4. Geben Sie die MPLS Virtual IP-Adresse und Gateway-Adresse ein. Der Proxy ARP wird nicht auf weniger als zwei Ethernet-Schnittstellen überprüft.

WAN Link: SJC-BR-MPLS Section: Access Interfaces + Add Link Delete Link

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Gateway MAC Address Binding | Delete |
|------------------|-------------------|------------|--------------------|-------------------|--------------------------|-------------------------------------|--------|
| SJC-BR-MPLS-AI-1 | MPLS_BR-1-2 | 10.17.0.9 | 10.17.0.1 | Primary | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

Apply Revert

Routen auffüllen

Routen werden basierend auf der vorhergehenden Konfiguration automatisch erstellt. Wenn es mehr Subnetze gibt, die für diese Remote-Zweigstelle spezifisch sind, müssen bestimmte Routen hinzugefügt werden, um zu identifizieren, welches Gateway den Datenverkehr leiten soll, um diese Back-End-Subnetze zu erreichen.

Erstellen von Autopath-Gruppen

1. Navigieren Sie im **Konfigurationseditor** zu **Global > Autopath-Gruppen**. Klicken Sie auf **+**.
2. Geben Sie einen Namen ein und klicken Sie auf **Übernehmen**.
3. Konfigurieren Sie die Autopath-Gruppe gemäß Ihren Anforderungen und klicken Sie auf **Übernehmen**.

Global ?

Network Settings
Regions
Centralized Licensing
Routing Domains
Applications
Firewall Zones
Firewall Policy Templates
Rule Groups
Network Objects
Route Learning Import Template
Route Learning Export Template
Virtual Path Default Sets
Dynamic Virtual Path Default Sets
Intranet Default Sets
DHCP Option Sets
Autopath Groups
WAN-to-WAN Forwarding Groups
WAN-to-WAN Forwarding Groups

+ Name Edit Delete

| | | |
|---------------|--|--|
| Default_Group | | |
| MPLS | | |

Apply Refresh

Edit x

☒ Set as Default

IP DSCP Tagging:
Any

Bad Loss Sensitive:
Enable (Default)

Silence Period (ms):
DEFAULT

Path Probation Period (ms):
10000 (Default)

☒ Instability Sensitive

Apply Cancel

4. Navigieren Sie zu **Verbindungen > WAN-Links**. Wählen Sie den Internet-WAN-Link aus der Dropdownliste **WAN-Links** und **virtuelle Pfade** aus der Dropdownliste **Abschnitt** aus.

5. Aktivieren Sie das Kontrollkästchen **Verwenden** und wählen Sie das neu erstellte Autopath-Gruppe aus der **Autopath-Gruppe** Kontrollkästchen für die Intranet-WAN-Links an den jeweiligen Standorten (sowohl Rechenzentrum als auch Zweig).

Keine zwei Autopath-Gruppen können als Standard markiert werden. Wenn markiert, würde dies zu einem Audit-Fehler führen.

| Virtual Path Service | Use | Tunnel Header Size (bytes) | Active MTU Detect | UDP Port | UDP Hole Punching | Enable | Alt Port | Interval (min) | Autopath Group |
|----------------------|-------------------------------------|----------------------------|--------------------------|----------|--------------------------|--------------------------|----------|----------------|----------------|
| SJC_DC-SJC-BR | <input checked="" type="checkbox"/> | 0 | <input type="checkbox"/> | 4980 | <input type="checkbox"/> | <input type="checkbox"/> | | 1440 | <None> |

Apply Revert

Nachdem die virtuellen Pfade für WAN-Verbindungen mit Zugriffstyp manuell als **Privates Intranet** hinzugefügt wurden, werden virtuelle Pfade unter **Pfade** gefüllt.

Nachdem Sie alle vorherigen Schritte abgeschlossen haben, fahren Sie mit [Vorbereiten der SD-WAN-Appliance-Paket](#) fort.

Beheben von Überwachungsfehlern

Nach Abschluss der Konfiguration für Rechenzentrums- und Zweigstandorte werden Sie darauf hingewiesen, die Überwachungsfehler an DC- und BR-Standorten zu beheben. Beheben Sie die Audit-Fehler (falls vorhanden).

Erstellen eines SD-WAN-Netzwerks

May 10, 2021

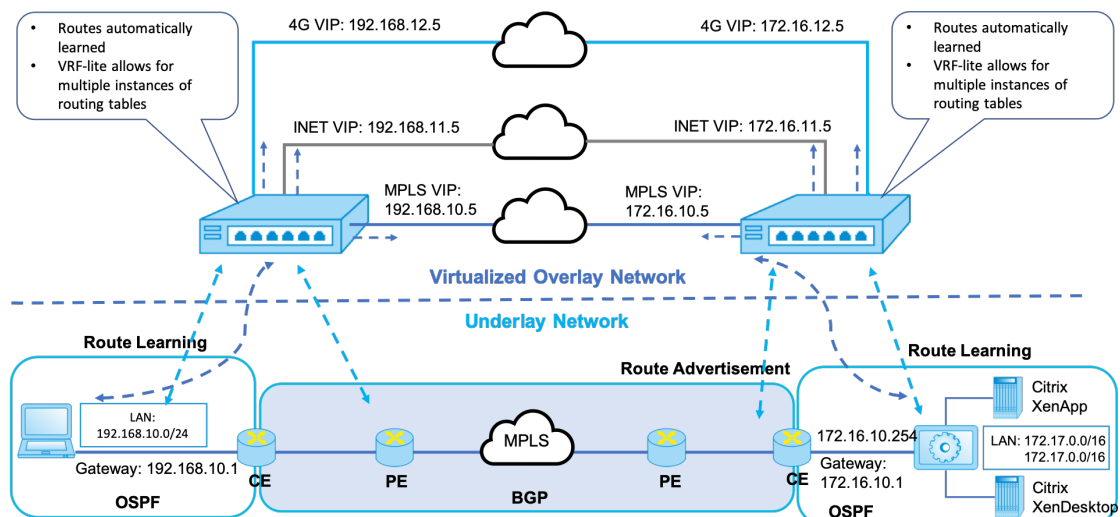
So erstellen Sie ein SD-WAN-Overlay-Netzwerk ohne die Notwendigkeit, SD-WAN-Overlay-Routentabellen zu erstellen:

1. Erstellen Sie einen WAN-Pfad-Tunnel über jede WAN-Verbindung zwischen zwei SD-WAN-Appliances.
2. Konfigurieren Sie Virtual IP, um den Endpunkt für jede WAN-Verbindung darzustellen. Sie können verschlüsselte WAN-Pfade über das aktuelle L3-Netzwerk einrichten.
3. Aggregieren Sie 2, 3 und 4 WAN-Pfade (physische Verbindungen) in einem einzigen virtuellen Pfad, sodass Pakete das WAN mithilfe des SD-WAN-Overlay-Netzwerks anstelle der vorhandenen Unterlage durchlaufen können, die am wenigsten intelligent und kostengünstig ist.

SD-WAN-Routingkomponenten und Netzwerktopologie

- Lokal —Subnetz befindet sich an diesem Standort (bekannt für SD-WAN-Umgebung)
- Virtueller Pfad —über den virtualisierten Pfad an die ausgewählte Standort-Appliance gesendet
- Intranet —Standorte ohne SD-WAN-Appliance
- Internet —Internet-gebundener Datenverkehr
- Pass-Through —unberührter Verkehr, in einer Brücke Schnittstelle zum anderen
- Default-Route (0.0.0.0/0) definiert - Wird für Pass-Through-Datenverkehr verwendet, der nicht von der SD-WAN-Overlay Routingtabelle erfasst oder am MCN verwendet wird, um Clientsites anzuweisen, den gesamten Datenverkehr an den MCN-Knoten weiterzuleiten.

SD-WAN overlay dynamic network routing



WAN-Optimierung nur mit Premium (Enterprise) Edition

May 10, 2021

Die SD-WAN Premium (Enterprise) Edition-Appliances enthalten zusätzlich zur WAN-Virtualisierung voll funktionsfähige WAN-Optimierungsfunktionen. Einige Kunden ziehen es vor, WAN-Optimierungsfunktionen zu implementieren, bevor sie zu SD-WAN-Services migrieren. Dieser Anwendungsfall für die Bereitstellung enthält die Schritte zum Verwenden von Premium Edition-Appliances zur Verwendung von WAN-Optimierungsdiensten.

Die Citrix SD-WAN Product Platform Editions enthalten die folgenden Appliances:

- SD-WAN: SD-WAN Standard Edition
- Premium (Enterprise): SD-WAN Premium Edition-Gerät
- WANOP: SD-WAN WANOP Edition Appliance

Um Premium (Enterprise) Edition-Appliances in ein vorhandenes verteiltes WANOP-Netzwerk zu integrieren, können Sie die SD-WAN-Appliance (Physical oder Virtual) am DC-Standort als MCN konfigurieren. Die SD-WAN-Appliance verwaltet die gesamte Konfiguration des Netzwerks. Zwischen dem Zweigstandort und MCN am DC-Standort wird ein virtueller Pfad eingerichtet. Dieser virtuelle Pfad wird nur zum Senden von Steuerdatenverkehr zwischen den Appliances verwendet. Bei der Zweige-Appliance wird der Datenverkehr als Intranetdienst verarbeitet. Der Intranetverkehr ist nicht gekapselt und durchläuft die vorhandene WAN-Verbindung, um den DC-Site zu erreichen. Eine WANOP-Appliance am DC-Standort sollte sich im Datenverkehrspfad befinden, um eine End-to-End-Datenverkehrsoptimierung zu ermöglichen.

Für Kundenstandorte, die keine SD-WAN-Hardware-Appliance am Headend haben, können VPX-Appliances in einem HA-Paar (zwei virtuelle WAN-VPXs) als MCN im Einarmmodus verwendet werden. Für den Einarmmodus sind PBR-Regeln auf dem Drittanbieter-Router erforderlich, um den Datenverkehr an die SD-WAN-Appliance umzuleiten.

In diesem Dokument wird davon ausgegangen, dass die DC-Standort-Appliances im HA-Modus zur Redundanz bereitgestellt werden. Der HA-Modus ist für diese Bereitstellung nicht obligatorisch.

Voraussetzungen

- Ein Paar WANOP-Appliances und ein Paar SD-WAN-Appliances, die im HA-Modus am DC-Standort bereitgestellt werden.
- Eine Premium Edition-Appliance am Standort der Zweigstelle.

Netzwerktopologie

SD-WAN Standard Edition und WANOP Appliances in PBR-Bereitstellung:

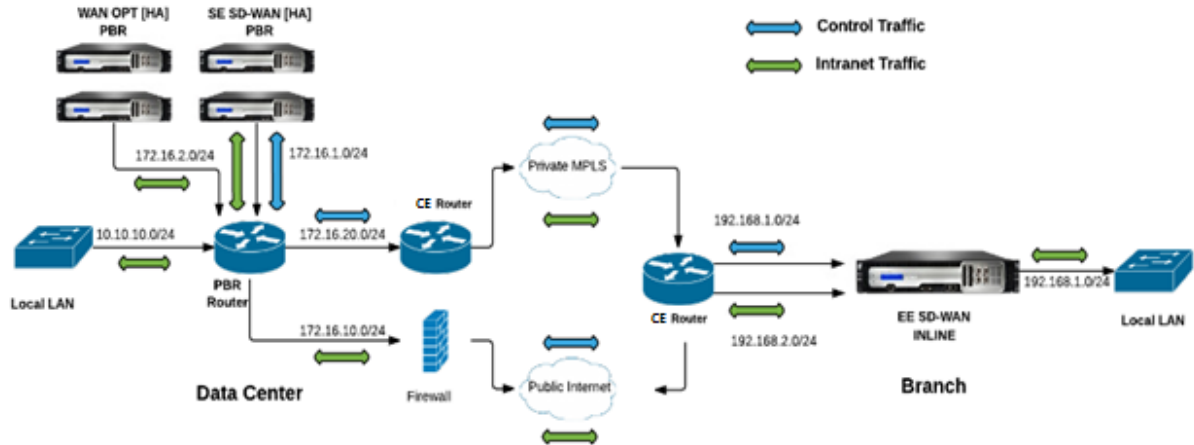
In der folgenden Abbildung werden sowohl die SD-WAN SE als auch die WAN OP Appliances am DC-Standort im Einarmmodus bereitgestellt. Die SD-WAN-Appliance unterstützt die PBR-Bereitstellung, während die WANOP-Appliance sowohl PBR als auch WCCP unterstützt. Der vom WAN am DC-Standort empfangene Steuerdatenverkehr (Virtual Path Traffic) wird vom PBR-Router an die SD-WAN-Appliance umgeleitet. Der Datenverkehr wird vom PBR-Router zur WAN-Optimierungs-Appliance umgeleitet.

Verkehrsfluss für WAN zu DC LAN:

- CE (Customer Edge) Router -> PBR Router -> SD-WAN -> PBR Router -> LAN

- CE (Customer Edge) Router -> PBR Router -> WAN OPT -> PBR Router-> LAN

Der gleiche Verkehrsfluss wird in umgekehrter Richtung verfolgt.



SD-WAN Standard Edition im PBR-Modus und WANOP im Inline-Einsatz:

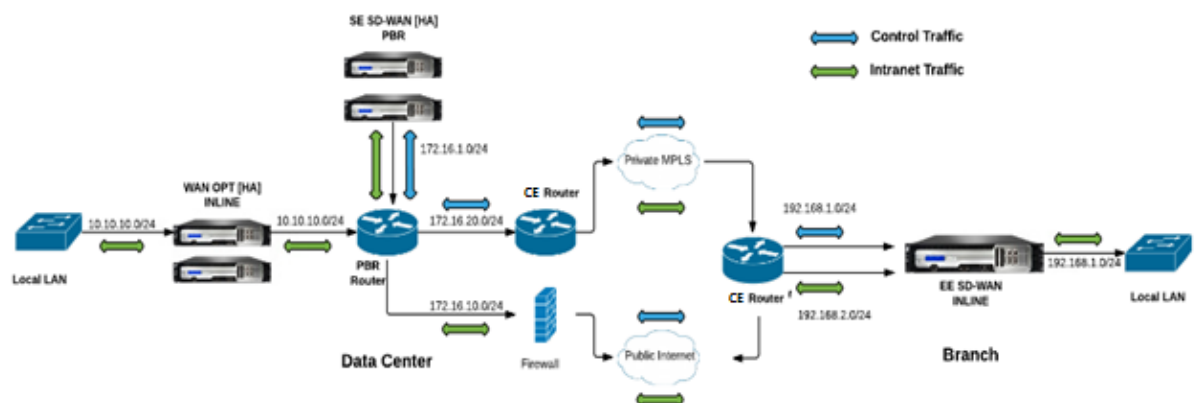
In der folgenden Abbildung wird die SD-WAN-Appliance am DC-Standort im Einarmmodus bereitgestellt, während die WANOP-Appliance im Inline-Modus bereitgestellt wird.

Der vom WAN am DC-Standort empfangene Steuerdatenverkehr (Virtual Path Traffic) wird vom PBR-Router an die SD-WAN-Appliance umgeleitet. Der Datenverkehr wird vom PBR-Router an die WAN Optimization Appliance (inline) weitergeleitet.

Verkehrsfluss für WAN zu DC LAN:

- CE (Customer Edge) Router -> PBR Router -> SD-WAN -> PBR Router -> LAN
- CE (Customer Edge) Router -> PBR Router -> WAN OPT -> LAN

Der gleiche Verkehrsfluss wird in umgekehrter Richtung verfolgt.



Konfigurationsschritte

1. Konfigurieren Sie die SD-WAN-Appliance unter DC [MCN], um virtuelle Pfade zwischen DC- und Zweigstandorten einzurichten.

Siehe [Konfigurieren des virtuellen Pfaddiensts zwischen MCN und Clients](#).

2. Konfigurieren Sie den Intranetdienst am DC-Standort.
 - a) Wechseln Sie am MCN (DC-Standort) zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor > Verbindungen > Standort (DC) > Intranetdienste**. Klicken Sie auf das **[+]**Zeichen, um einen Intranetdienst hinzuzufügen.
 - b) Wählen Sie eine oder mehrere WAN-Links für **Intranetdienstauss**, und klicken Sie dann auf **Übernehmen**.
 - c) Navigieren Sie zu Routen unter demselben **Standort (DC)**, klicken Sie auf **[+]**Zeichen, um das Remote-Netzwerk mit niedrigeren Kosten als 5 hinzuzufügen, und wählen Sie auf **Hinzufügen**.

Beispiel: - Geben Sie **192.168.1.0/24** in das Feld **Netzwerk-IP-Adresse** mit Kosten 4 ein, und wählen Sie **Servicetyp** als **Intranet** aus.

Hinweis

Die Kosten an jedem Standort sollten unter 5 liegen, damit die Intranetroute Vorrang hat.

3. Konfigurieren Sie den Intranetdienst am Zweigstandort.
 - a) Wiederholen Sie die Unterschritte a bis c von **Schritt 2** oben auf der Zweigwebsite.

Beispiel: - Geben Sie **172.16.1.0/24** in das Feld Netzwerk-IP-Adresse mit Kosten 4 ein, und wählen Sie **Diensttyp** als **Intranet** aus.
4. Führen Sie die **Änderungsverwaltung** aus, um die Konfiguration auf den Zweigstandort hochzuladen und zu verteilen.

Siehe, [Exportieren von Konfigurationspaketen und Änderungsverwaltung](#)

Standardmäßig wird der Datenverkehr über den virtuellen Pfad von Zweig an DC gesendet.

Hinweis

Der PBR-Router sollte so konfiguriert werden, dass der Datenverkehr gemäß den bereitgestellten Bereitstellungsschritten umgeleitet wird.

Weitere Informationen zum Konfigurieren der WAN-Optimierung finden Sie unter: [Aktivieren-Konfigurations-WAN-Optimierung](#).

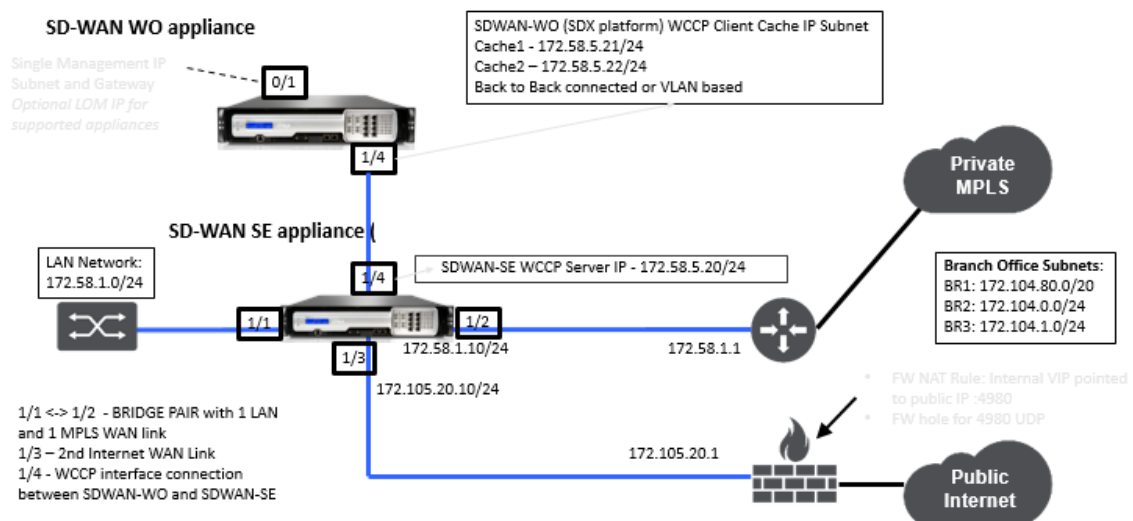
Zwei-Box-Modus

May 10, 2021

Der Zwei-Box-Modus ist eine WCCP-Einarm-basierte Bereitstellung, bei der die SD-WAN SE-Appliance als WCCP-Router fungiert und die SDWAN-WANOP (4000/5000) Appliances als WCCP-Clients fungieren und dabei helfen, WCCP-Konvergenz zu etablieren. Auf diese Weise werden alle virtuellen Pfad-/Intranet-Service-orientierten TCP-Pakete, die die SD-WAN SE-Appliance erreichen, zur Optimierung weitergeleitet, indem sie sowohl SD-WAN SE als auch WANOP Vorteile für den Kundenverkehr bieten.

Der Zwei-Box-Modus wird nur bei den folgenden Appliance-Modellen unterstützt:

- SD-WAN SE-Appliances —4000, 4100 und 5100
- SD-WAN WANOP-Geräte —4000, 4100, 5000 und 5100



Hinweis

Auf Hochverfügbarkeits- und WCCP-Bereitstellungsmodi kann nicht zugegriffen werden, wenn der Zwei-Box-Modus aktiviert ist. Diese Bereitstellungsmodi sind jedoch für den Benutzer zur Verwaltung verfügbar.

Wichtig

- Obwohl die Legacy-WCCP-Bereitstellung deaktiviert ist, wenn der Zwei-Box-Modus aktiviert ist, kann die Konvergenz der Dienstgruppen nur auf der WCCP-Überwachungsseite überprüft werden. Es gibt keine separate GUI-Seite unter dem Monitoring-Abschnitt für den Zwei-Box-Modus.
- Wenn der WCCP-Prozess, der auf der Standard Edition-Appliance ausgeführt wird,

mehrmals innerhalb eines kurzen Zeitraums neu gestartet wird, z. B. dreimal in einer Minute, wird die Servicegruppe automatisch heruntergefahren. Um die WCCP-Konvergenz auf der WANOP-Appliance abrufen zu können, aktivieren Sie in diesem Szenario die WCCP-Funktion in der Web-GUI der WANOP-Appliance erneut.

- Wenn sich die WCCP-Konfiguration oder die WAN-Optimierung im Zusammenhang mit der Konfiguration auf der Standard Edition-Appliance ändert, wird die externe WANOP-Appliance neu gestartet. Wenn Sie beispielsweise das Kontrollkästchen WCCP in der Schnittstellengruppe des Konfigurations-Editors, gefolgt vom Change Management-Prozess, aktivieren/deaktivieren, startet auch die WANOP-Appliance neu.

Hinweis

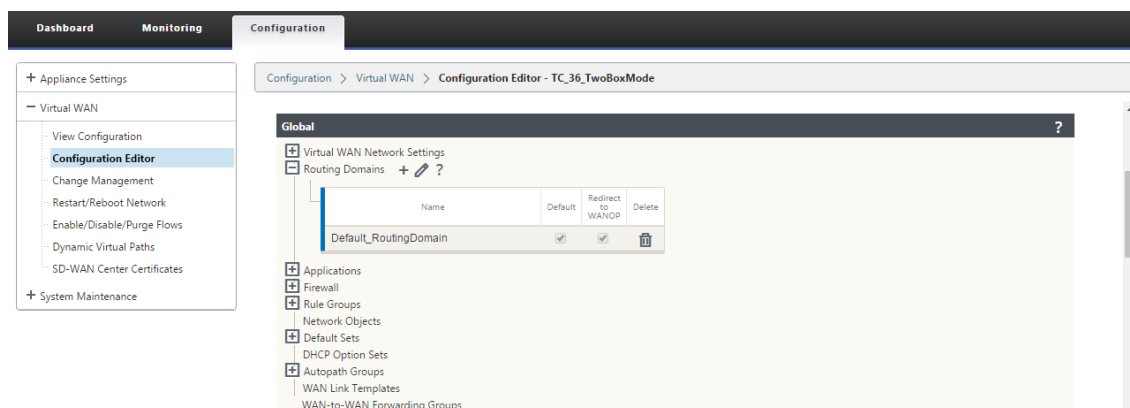
Beachten Sie auch die folgenden Punkte, die bei der Implementierung des Zwei-Box-Modus zu beachten sind:

- Wenn eine Routingdomäne aus dem Konfigurations-Editor zur WANOP-Appliance ausgewählt ist, sollte sie der Schnittstellengruppe hinzugefügt werden, für die WCCP aktiviert ist.
- Der Datenverkehr derselben Routingdomäne sollte auch auf der Partnerseite ausgewählt werden. Beispiel: **MCN > Branch01**, um die Vorteile der WAN-Optimierung zu beobachten.
- Wenn eine Routingdomäne in der Schnittstellengruppe ausgewählt ist, für die WCCP aktiviert ist, sollte eine andere Schnittstellengruppe, die die überbrückten Schnittstellen enthält, dieselbe Routingdomäne konfiguriert sein. Nur wenn die WCCP-aktivierte Schnittstellengruppe die Routingdomäne konfiguriert hat, reicht es nicht aus, den End-to-End-Datenverkehr mit WAN-Optimierungsvorteilen zu übertragen.

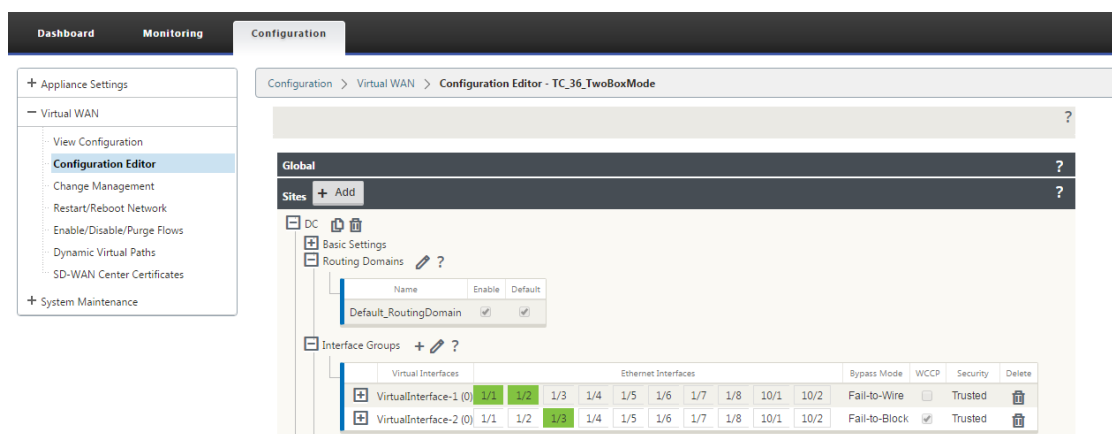
Citrix SD-WAN Standard Edition

So konfigurieren Sie die Lösung im Zwei-Box-Modus in der Standard Edition-Appliance am DC- oder Zweigstandort:

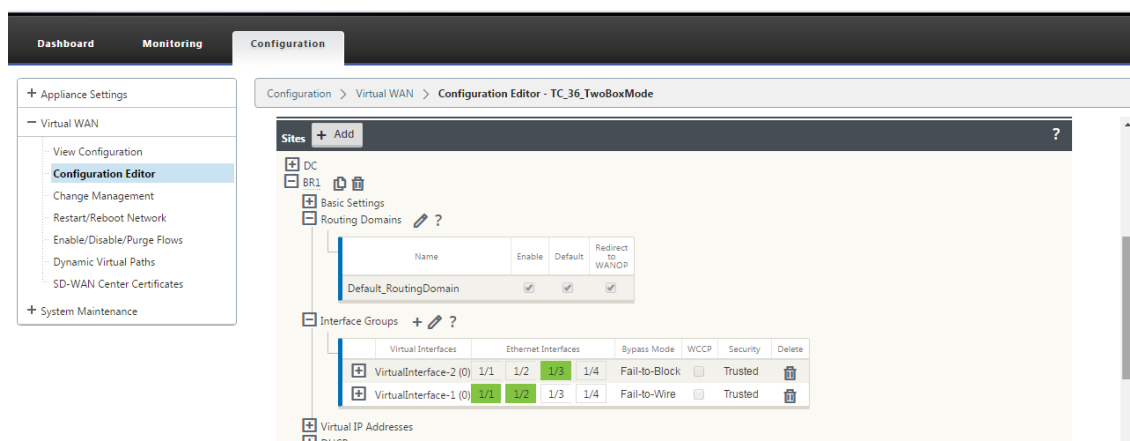
1. Wechseln Sie in der SD-WAN SE-Webverwaltungsschnittstelle zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor**. Öffnen Sie ein vorhandenes Konfigurationspaket oder erstellen Sie ein Paket.
2. Wechseln Sie im ausgewählten Konfigurationspaket zur Registerkarte **Erweitert**, um die Konfigurationsdetails anzuzeigen.
3. Öffnen Sie **Globale** Einstellungen, und erweitern Sie **Routingdomänen, um anzuzeigen, dass das Kontrollkästchen An WANOP umleiten** aktiviert ist.



4. Erweitern Sie DC, um **WCCP** für die **virtuelle Schnittstelle** unter **Schnittstellengruppeneinstellungen** zu aktivieren, die anzeigen, für welche virtuelle Netzwerkschnittstelle die Appliance aktiviert ist.



5. Erweitern Sie **Sites+ Hinzufügen**, um die Einstellungen der Zweigroutingdomäne und der Schnittstellengruppeneinstellungen anzuzeigen. Unter dem Zweigstandort ist das Kontrollkästchen **An WANOP umleiten** für Routingdomänen aktiviert.



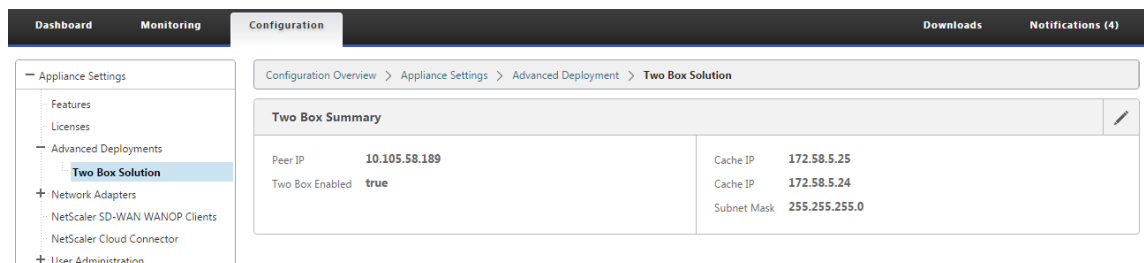
Hinweis

Der WCCP-Listener sollte nur für die virtuellen Netzwerkschnittstellen aktiviert werden, für die nur EINE Ethernet-Schnittstelle konfiguriert ist. Aktivieren Sie den WCCP-Listener nicht auf einem BRIDGED-Paar. Es soll auf der ONE-ARM-Schnittstelle zwischen den SD-WAN SE und SD-WAN WANOP-Einheiten aktiviert werden.

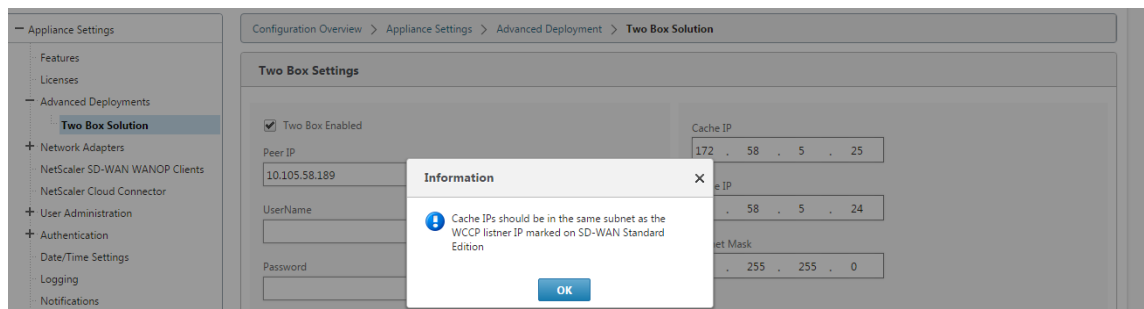
Citrix SD-WAN WANOP-Konfiguration

So konfigurieren Sie den Zwei-Box-Bereitstellungsmodus in der Web-GUI der SD-WAN WANOP Appli-
ance:

1. Wechseln Sie in der SD-WAN WANOP-Webverwaltungsschnittstelle zu **Konfiguration > Appliance-Einstellungen > Erweiterte Bereitstellungen > Zwei-Box-Lösung**.



2. Klicken Sie auf das Symbol **Bearbeiten**, um die beiden Einstellungen für den Boxmodus zu bearbeiten. Der Informationsdialog zu **Cache-IPs** wird angezeigt. Klicken Sie auf **OK**.



3. Aktivieren Sie das **Kontrollkästchen Zwei Kästchen aktiviert**.
4. Geben Sie die **Peer-IP** ein. Peer IP ist die IP-Adresse der SD-WAN Standard Edition Appliance.
5. Geben Sie die Benutzeranmeldeinformationen ein, und klicken Sie auf **Übernehmen**.

Two Box Settings

☒ Two Box Enabled

Peer IP

UserName

Password

Cache IP

Cache IP

Subnet Mask

Apply

Cancel

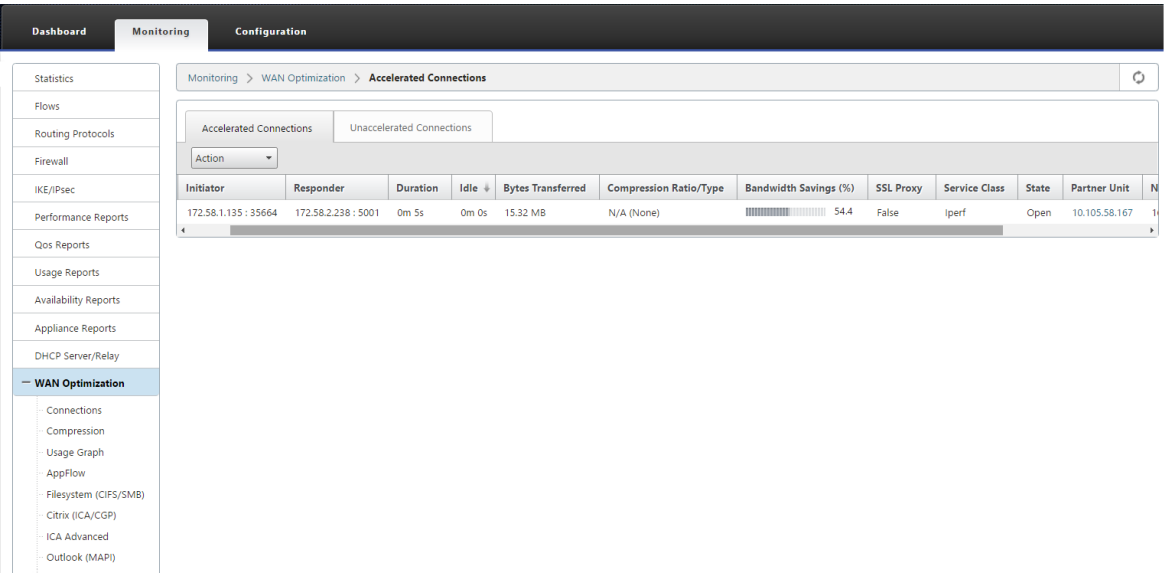
Konfiguration und Verwaltbarkeit im Zwei-Box-Modus

Im Folgenden sind einige der beiden Boxmoduskonfigurations- und Verwaltbarkeitspunkte aufgeführt, die für die Bereitstellung in Betracht gezogen werden sollten:

- SD-WAN WANOP Konfigurationen, die unten erwähnt werden, können vom SD-WAN SE Konfigurationseditor als einheitlichen Bereich konfiguriert werden
 - SERVICE CLASS
 - APPLICATION CLASSIFIER
 - FEATURES
 - SYSTEM TUNING

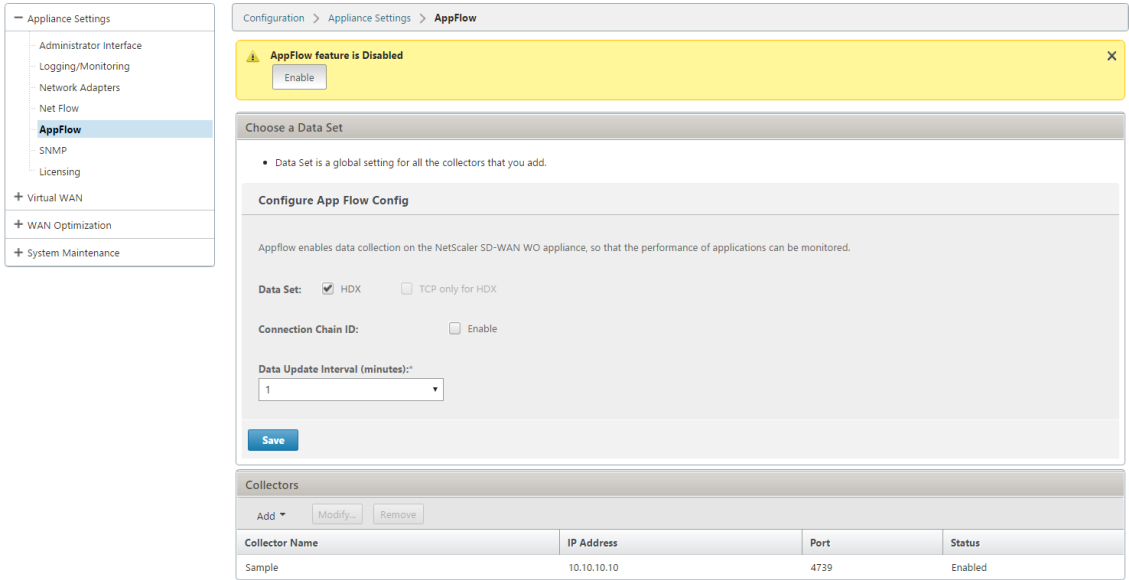
Überwachen

Sie können den SD-WANOP-Datenverkehr direkt über die Seite “Überwachung” der Web-Benutzeroberfläche der SD-WAN SE Appliance überwachen. Auf diese Weise können sowohl die SDWAN-SE als auch die SDWAN-WO Appliances in einem einzigen Bereich überwacht werden, während der Datenverkehr verarbeitet wird. Sie können die Verbindungsdetails, Details zu sicheren Partnern usw. unter dem Knoten WAN-Optimierung in der SDWAN-SE-Benutzeroberfläche anzeigen.



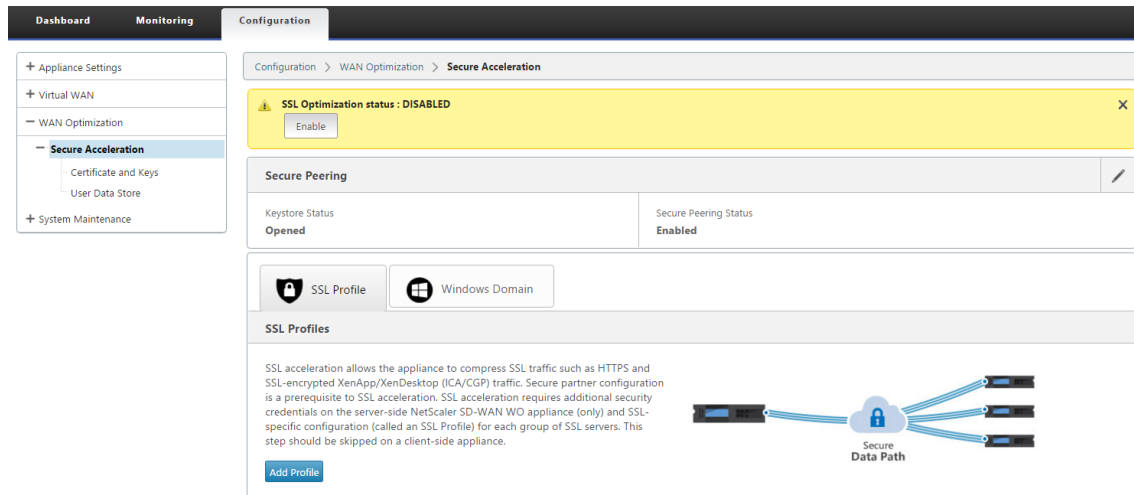
Konfiguration

Sie können APPFLOW direkt über die SDWAN-SE-Konfigurationsseite unter **APPFLOW**-Knoten konfigurieren. Dadurch kann SDWAN-SE als ein einziger Bereich für die Konfiguration von APPFLOW und anderen Datenverarbeitungskonfigurationsattributen wie Service Class, Application Classifiers fungieren. Die Konfiguration auf der SDWAN-SE spiegelt die SDWAN-WO-Konfiguration wider, wodurch eine nahtlose APPFLOW Funktionalität unterstützt wird.



SD-WAN WANOP, die bereits von Citrix Application Delivery Management (ADM) erkannt wurde, sollte isoliert und nicht mit Citrix ADM konfiguriert werden, bis dieser Modus ausgeschaltet ist. Dies liegt daran, dass die Konfiguration von WANOP für die Datenverarbeitung von der SD-WAN SE-Appliance im Zwei-Box-Modus verwaltet wird.

Erweiterte Optimierungen oder Secure Acceleration sollten direkt auf der SDWAN-SE-Appliance konfiguriert werden, wie wir es auf der SDWAN-WO Appliance konfigurieren würden. Dies hilft, einen einzelnen Bereich der Konfiguration von Konfigurationen wie Domain Join oder Secure Acceleration/SSL-Profilerstellung für erweiterte Optimierungen oder SSL-Proxy aufrechtzuerhalten.



- Die Lizenzierung sollte für jede SD-WAN SE und SD-WAN WANOP Appliances separat verwaltet werden.
- Software-Upgrade sollte für jede SD-WAN SE und SD-WAN WANOP Appliances mit den entsprechenden Softwarepaketen separat verwaltet werden. Zum Beispiel tar.gz für SD-WAN SE und Upgrade für SD-WAN WANOP.
- Die Datenpfadintegration sollte zwischen SD-WAN SE und externen WANOP-Appliances über den WCCP-Bereitstellungsmodus konfiguriert werden.
 - Auf Datenpfad-Ebene werden sowohl WCCP- als auch Virtual WAN-Funktionen durch Datenpfadintegration zwischen WANOP und SE extern im Einarmmodus angeboten, um Optimierungsvorteile zu erzielen.

Einheitliche Konfiguration und Überwachung

Wenn Sie den Zwei-Box-Modus mit SD-WAN SE und SDWAN-WANOP-Appliances aktivieren, können Sie die Konfiguration in der SD-WAN SE-Appliance ähnlich anzeigen, wie Sie zwei Box-Konfigurationen mit der SD-WAN-EE-Appliance anzeigen können.

1. Gehen Sie zu **Konfiguration > Virtuelles WAN > WAN-Optimierung**
2. Appflow-Knoten unter **Konfiguration > Appliance-Einstellungen**
3. WAN-Optimierungsknoten unter Konfiguration.

Diese Informationen werden von der SD-WAN WANOP-Appliance umgeleitet, die sich im Zwei-Box-Modus mit der SD-WAN SE-Appliance befindet.

Konfigurationen im Zusammenhang mit WANOP, wie SSL Acceleration und AppFlow können nun von der SD-WAN SE Web-GUI durchgeführt werden.

Statistiken zu Datenverkehr wie Connections, Compression, CIFS/SMB, ICA Advanced, MAPI und Partnern können jetzt ähnlich wie bei der SD-WAN Premium (Enterprise)-Edition über die Web-GUI von SD-WAN SE unter **Überwachung > WAN-Optimierung** überwacht werden.

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

- WAN Optimization

+ Secure Acceleration

+ System Maintenance

Configuration > WAN Optimization

SSL Optimization status : DISABLED

Enable

Secure Peering

Keystore Status

Opened

Secure Peering Status

Enabled

SSL Profile

Windows Domain

DashboardMonitoringConfiguration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Monitoring > Statistics

Statistics

Show: Paths (Summary) ☐ Enable Auto Refresh 5 seconds Refresh ☒ Show latest data.

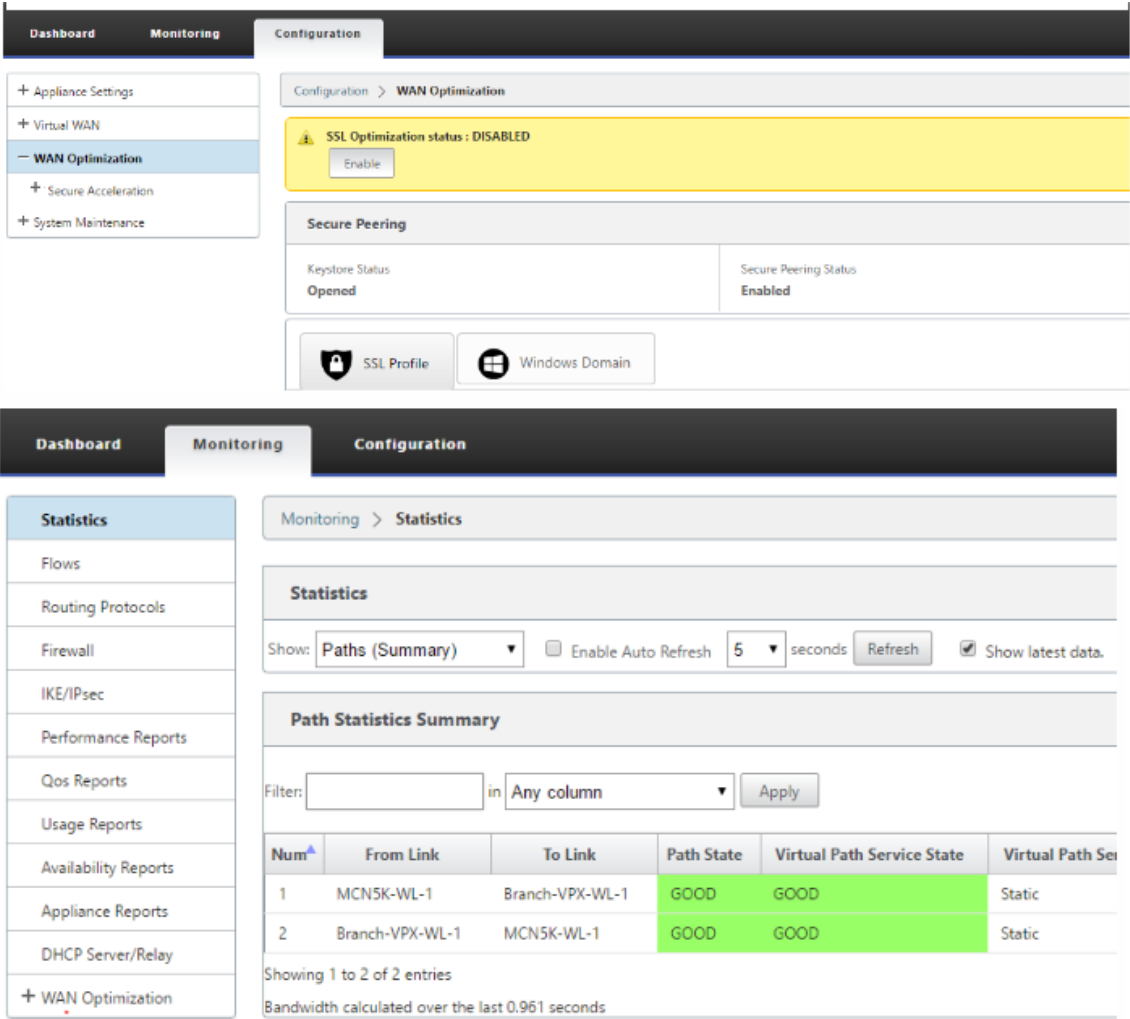
Path Statistics Summary

Filter: in Any column Apply

| Num | From Link | To Link | Path State | Virtual Path Service State | Virtual Path Se |
|-----|-----------------|-----------------|------------|----------------------------|-----------------|
| 1 | MCN5K-WL-1 | Branch-VPX-WL-1 | GOOD | GOOD | Static |
| 2 | Branch-VPX-WL-1 | MCN5K-WL-1 | GOOD | GOOD | Static |

Showing 1 to 2 of 2 entries

Bandwidth calculated over the last 0.961 seconds



Änderung der Verwaltungs-IP-Adresse für die SD-WAN WANOP Appliance im Zwei-Box-Modus

So ändern Sie die Verwaltungs-IP-Adresse der SDWAN-WANOP-Appliance im Zwei-Box-Modus:

1. Führen Sie den Befehl `clear_wo_sync` auf der SD-WAN SE-Appliance aus. Es stellt sicher, dass die SD-WAN WANOP IP-Adressinformationen für die GUI-Umleitung gelöscht werden.
2. Deaktivieren und aktivieren Sie die Konfiguration des Zwei-Box-Modus auf der SD-WAN WANOP-Appliance. Die neue IP-Adresse (geänderte IP) der SD-WAN WANOP Appliance wird an SD-WAN SE gesendet. Die neue geänderte IP-Adresse wird in den URL-Umleitungsseiten angezeigt.

Die Verwaltungs-IP-Adresse wird für die Konfiguration der Peer-IP-Adresse verwendet.

Deaktivieren Sie den Zwei-Box-Modus auf der SD-WAN WANOP-Appliance

So deaktivieren oder entkoppeln Sie die SD-WAN WANOP- und SD-WAN SE-Geräte aus dem Zwei-Box-Modus:

1. Deaktivieren Sie den Zwei-Box-Modus von der SD-WAN WANOP-Appliance.
2. Es wird erwartet, dass die SD-WAN WANOP-Appliance zwei Box-Mode-Seiten in der Web-GUI SD-WAN SE angezeigt wird. Um diese Seiten zu löschen, führen Sie den Befehl `clear_wo_syncaus`.

Hohe Verfügbarkeit

October 28, 2021

In diesem Thema werden die Bereitstellungen und Konfigurationen mit hoher Verfügbarkeit (Hochverfügbarkeit) behandelt, die von SD-WAN-Appliances unterstützt werden (Standard Edition und Premium (Enterprise) Edition).

Citrix SD-WAN Appliances können in der Hochverfügbarkeitskonfiguration als Appliances in Active/Standby-Rollen bereitgestellt werden. Es gibt drei Modi für die Bereitstellung von Hochverfügbarkeit:

- Parallele Inline-Hochverfügbarkeit
- Hochverfügbarkeit von Fail-to-Wire
- Einarmige Hochverfügbarkeit

Diese Hochverfügbarkeitsbereitstellungsmodi ähneln dem Virtual Router Redundancy Protocol (VRRP) und verwenden ein proprietäres SD-WAN-Protokoll. Sowohl Clientknoten (Clients) als auch Master Control Nodes (MCNs) in einem SD-WAN-Netzwerk können in einer Hochverfügbarkeitskonfiguration bereitgestellt werden. Die primäre und sekundäre Appliance müssen dieselben Plattformmodelle aufweisen.

Bei Hochverfügbarkeitskonfiguration wird eine SD-WAN-Appliance am Standort als aktive Appliance bezeichnet. Die Standby-Appliance überwacht die aktive Appliance. Die Konfiguration wird über beide Appliances hinweg gespiegelt. Wenn die Standby-Appliance für einen definierten Zeitraum die Verbindung mit der Active Appliance verliert, übernimmt die Standby-Appliance die Identität der Active Appliance und übernimmt die Datenverkehrslast. Je nach Bereitstellungsmodus hat dieses schnelle Failover nur minimale Auswirkungen auf den Anwendungsverkehr, der durch das Netzwerk fließt.

Bereitstellungsmodi für Hochverfügbarkeit

Einarm-Modus:

Im Einarmmodus befindet sich das Hochverfügbarkeits-Appliance-Paar außerhalb des Datenpfads. Der Anwendungsdatenverkehr wird an das Appliance-Paar mit Policy Based Routing (PBR) umgeleitet. Der Einarm-Modus wird implementiert, wenn ein einzelner Einfügepunkt im Netzwerk nicht möglich ist oder um den Herausforderungen von Fail-to-Wire entgegenzuwirken. Die Standby-Appliance kann demselben VLAN oder Subnetz wie die Active Appliance und der Router hinzugefügt werden.

Im Einarmmodus wird empfohlen, dass sich die SD-WAN-Appliances nicht in den Datennetzsubnetzen befinden. Der virtuelle Pfadverkehr muss den PBR nicht durchqueren und vermeidet Routenschleifen. Die SD-WAN-Appliance und der Router müssen direkt verbunden sein, entweder über einen Ethernet-Port oder im selben VLAN.

- **IP-SLA-Überwachung für Rückfall:**

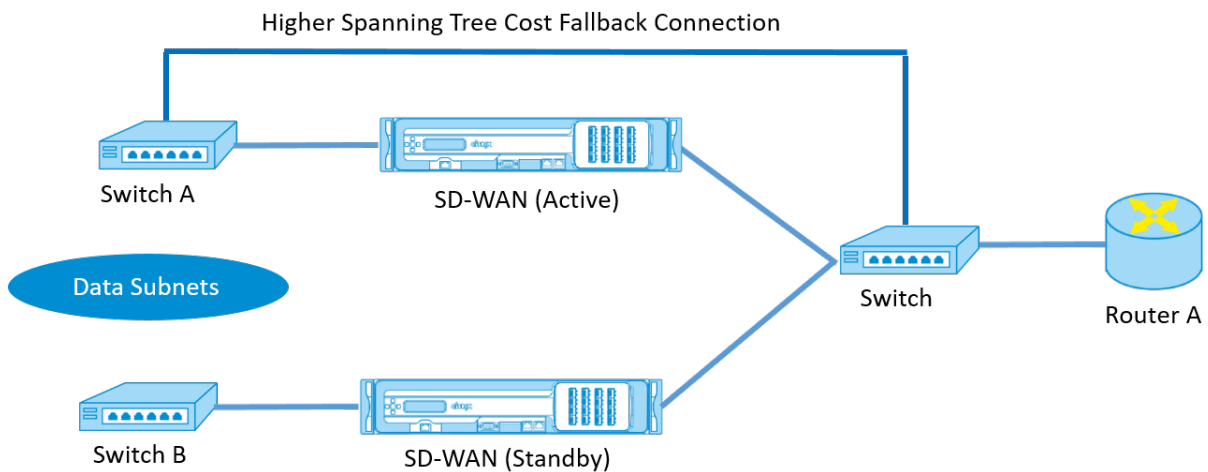
Der aktive Datenverkehr fließt auch dann, wenn der virtuelle Pfad ausgefallen ist, solange eine der SD-WAN-Appliances aktiv ist. Die SD-WAN-Appliance leitet den Datenverkehr als Intranetverkehr zurück an den Router um. Wenn jedoch beide aktive/Standby-SD-WAN-Appliances inaktiv werden, versucht der Router, den Datenverkehr an die Appliances umzuleiten. Die IP-SLA-Überwachung kann am Router so konfiguriert werden, dass die PBR deaktiviert wird, wenn die nächste Appliance nicht erreichbar ist. Dadurch kann der Router zurückgreifen, um eine Routensuche durchzuführen und Pakete entsprechend weiterzuleiten.

Paralleler Inline-Hochverfügbarkeitsmodus:

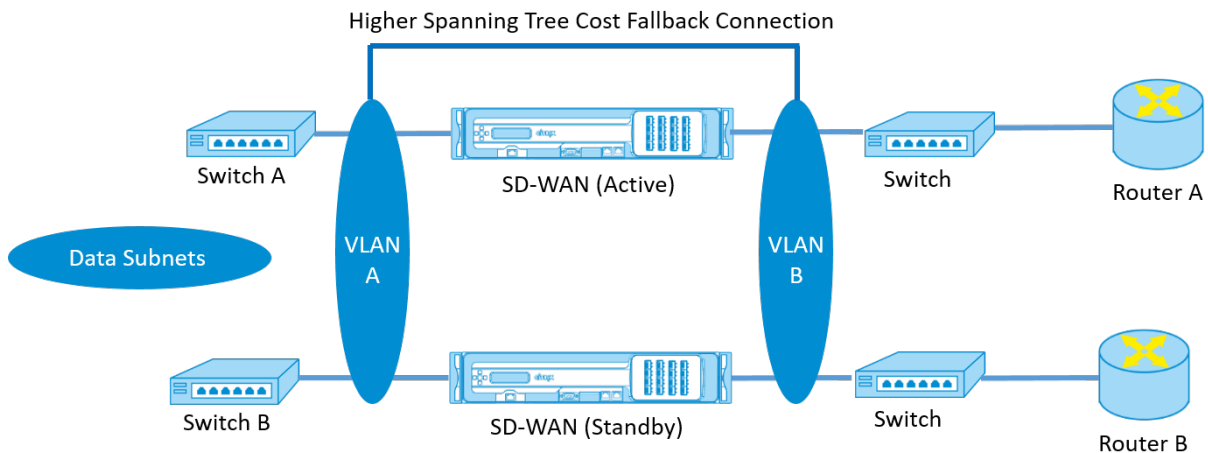
Im parallelen Inline-Hochverfügbarkeitsmodus werden die SD-WAN-Appliances inline mit dem Datenpfad nebeneinander bereitgestellt. Es wird nur ein Pfad durch die Active Appliance verwendet. Es ist wichtig zu beachten, dass Bypass-Schnittstellengruppen so konfiguriert sind, dass sie Failto-Block sind, um Brückenschleifen während eines Failovers zu vermeiden.

Der Hochverfügbarkeitsstatus kann über die Inline-Schnittstellengruppen oder über eine direkte Verbindung zwischen den Appliances überwacht werden. Externes Tracking kann verwendet werden, um die Erreichbarkeit der vor- oder nachgelagerten Netzwerkinfrastruktur zu überwachen. Zum Beispiel; Switch-Port kann bei Bedarf keine Statusänderung der Hochverfügbarkeit steuern.

Wenn sowohl aktive als auch Standby-SD-WAN-Appliances deaktiviert sind oder fehlschlagen, kann ein tertiärer Pfad direkt zwischen Switch und Router verwendet werden. Dieser Pfad muss höhere Spanning Tree-Kosten haben als die SD-WAN-Pfade, damit er unter normalen Bedingungen nicht verwendet wird. Das Failover im parallelen Inline-Hochverfügbarkeitsmodus hängt von der konfigurierten Failover-Zeit ab, die standardmäßige Failover-Zeit beträgt 1000 ms. Ein Failover hat jedoch eine Verkehrsauswirkung von 3-5 Sekunden. Der Rückfall auf den Tertiärpfad wirkt sich auf den Verkehr für die Dauer der Spanning Tree-Konvergenz aus. Wenn keine Verbindungen zu anderen WAN-Links vorhanden sind, müssen beide Appliances mit ihnen verbunden sein.



In komplexeren Szenarien, in denen mehrere Router VRRP verwenden, werden nicht routbare VLANs empfohlen, um sicherzustellen, dass der LAN-seitige Switch und Router auf Layer 2 erreichbar sind.



Fail-to-Wire-Modus:

Im Fail-to-Wire-Modus befinden sich die SD-WAN-Appliances im selben Datenpfad. Die Bypass-Schnittstellengruppen müssen sich im Fail-to-Wire-Modus befinden, wobei sich die Standby-Appliance im Passthrough- oder Bypass-Status befindet. Für die hochverfügbare Schnittstellengruppe muss eine direkte Verbindung zwischen den beiden Appliances an einem separaten Port konfiguriert und verwendet werden.

Hinweis

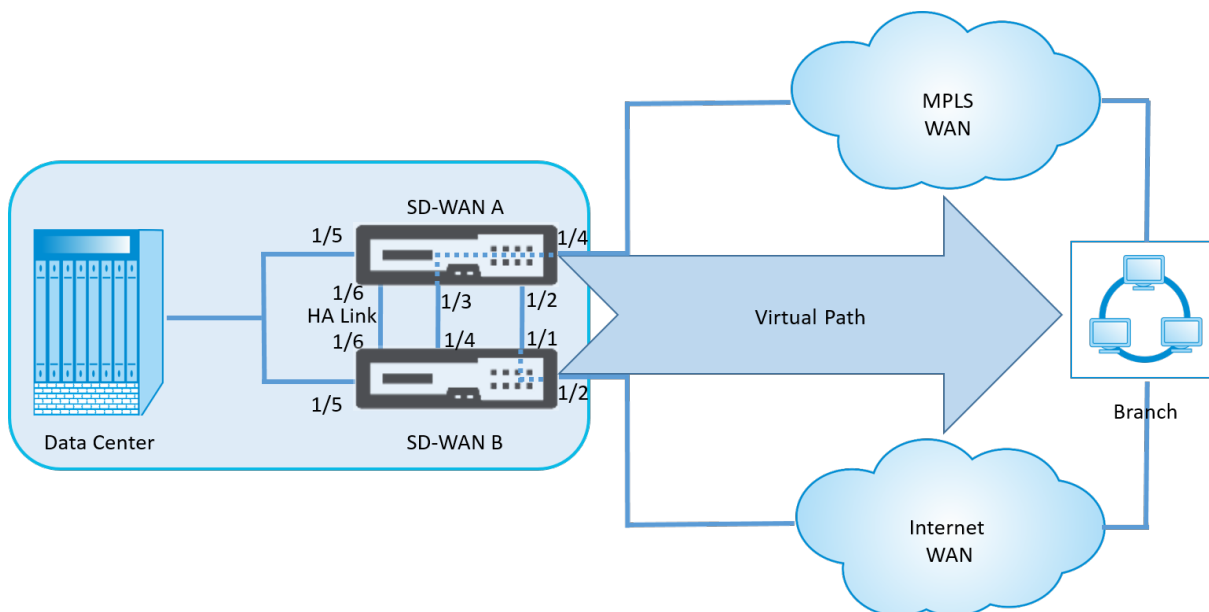
- Der Switchover mit hoher Verfügbarkeit im Fail-to-Wire-Modus dauert etwa 10 bis 12 Sekunden, da die Ports bei der Wiederherstellung aus dem Fail-to-Wire-Modus verzögert werden.
- Wenn die Hochverfügbarkeitsverbindung zwischen den Appliances fehlschlägt, wechseln beide Appliances in den Status Aktiv und verursachen eine Dienstunterbrechung. Um die Di-

enstunterbrechung zu minimieren, weisen Sie mehrere Hochverfügbarkeitsverbindungen zu, damit kein einziger Fehlerpunkt auftritt.

- Es ist zwingend erforderlich, dass im Fail-to-Wire-Modus für hohe Verfügbarkeit ein separater Port in den Hardware-Appliance-Paaren für den Hochverfügbarkeitskontroll-Austauschmechanismus verwendet wird, um bei der Zustandskonvergenz zu helfen.

Aufgrund einer Änderung des physischen Zustands beim Umschalten der SD-WAN-Appliances von Active auf Standby kann ein Failover zu einem teilweisen Verlust der Konnektivität führen, je nachdem, wie lange die automatische Aushandlung für die Ethernet-Ports dauert.

Die folgende Abbildung zeigt ein Beispiel für die Fail-to-Wire-Bereitstellung.



Die Einarm-Hochverfügbarkeitskonfiguration oder die Parallele Inline-Hochverfügbarkeitskonfiguration wird für Rechenzentren oder Sites empfohlen, die ein hohes Datenvolumen weiterleiten, um Unterbrechungen während des Failovers zu minimieren.

Wenn während eines Failovers ein minimaler Service-Verlust akzeptabel ist, ist der Fail-to-Wire-Hochverfügbarkeitsmodus eine bessere Lösung. Der Fail-to-Wire-Hochverfügbarkeitsmodus schützt vor Ausfällen der Appliance und die parallele Inline-Hochverfügbarkeit schützt vor allen Ausfällen. In allen Szenarien ist eine hohe Verfügbarkeit wertvoll, um die Kontinuität des SD-WAN-Netzwerks während eines Systemausfalls zu erhalten.

Konfigurieren der Hochverfügbarkeit

So konfigurieren Sie Hochverfügbarkeit:

1. Navigieren Sie im Konfigurationseditor zu **Sites > Site-Name** > **Hochverfügbarkeit**. Wählen Sie **Hochverfügbarkeit aktivieren** aus, und klicken Sie auf **Übernehmen**.

The screenshot shows the 'High Availability' configuration page for site 'MCN-5100'. The left sidebar lists various configuration categories, with 'High Availability' selected. The main panel has a tabbed interface with 'Basic', 'Global', 'Sites', 'Connections', 'Optimization', and 'Provisioning'. The 'Sites' tab is active, showing a list of sites with 'MCN-5100' selected. A modal dialog is open, prompting the user to 'Enable High Availability' and click the 'Apply' button. Below the dialog, the 'Enable High Availability' checkbox is checked. The configuration fields are as follows:

| HA Appliance Name: | Failover Time (ms): | Shared Base MAC: |
|--------------------|---------------------|-------------------|
| MATRIZ-1 | 1000 | AA:AA:AA:00:00:00 |

Below these fields are three unchecked checkboxes: 'Swap Primary/Secondary', 'Primary Reclaim', and 'HA Fail-to-Wire Mode'. At the bottom, there is a section for 'HA IP Interfaces' with a '+' icon. Below this is a table of IP interfaces:

| Virtual Interface | Control IP Addresses | | Delete |
|-------------------|----------------------|--------------|--------|
| | Primary | Secondary | |
| LAN (100) | 10.0.15.241 | 10.0.15.240 | |
| INET (0) | 10.213.16.35 | 10.213.16.34 | |

2. Geben Sie Werte für den folgenden Parameter ein:

- **Appliance-Name für hohe Verfügbarkeit:** Der Name der (sekundären) Appliance für hohe Verfügbarkeit.
- **Failover-Zeit:** Die Wartezeit (in Millisekunden) nach dem Kontakt mit der primären Appliance geht verloren, bevor die Standby-Appliance aktiv wird.
- **Shared Base-MAC:** Die gemeinsam genutzte MAC-Adresse für die Hochverfügbarkeitspaare. Wenn ein Failover auftritt, verfügt die sekundäre Appliance über dieselben virtuellen MAC-Adressen wie die fehlgeschlagene primäre Appliance.
- **Swap Primary/Secondary:** Wenn diese Option ausgewählt ist und beide Appliances des Hochverfügbarkeitspaares gleichzeitig auftauchen, wird die sekundäre Appliance zur primären Appliance und hat Vorrang.
- **Primäre Rückgewinnung:** Wenn diese Option ausgewählt ist, gewinnt die designierte primäre

Appliance die Kontrolle beim Neustart nach einem Failover-Ereignis zurück.

- **Hochverfügbarkeits-Fail-to-Wire-Modus:** Wählen Sie diese Option aus, um den Fail-to-wire-Hochverfügbarkeit

Hinweis

Für Hypervisor- und Cloud-basierte Plattformen wählen Sie die Option **Shared Base MAC** deaktivieren, um die gemeinsam genutzte virtuelle MAC-Adresse zu deaktivieren.

Stellen Sie für Hypervisor basierte Plattformen sicher, dass der Promiscuous-Modus auf den Hypervisoren aktiviert ist, um Paketbeschaffung von freigegebenen MAC-Adressen mit hoher Verfügbarkeit zu ermöglichen. Wenn der Promiscuous-Modus nicht aktiviert ist, können Sie die Option **Shared Base-MAC deaktivieren** aktivieren.

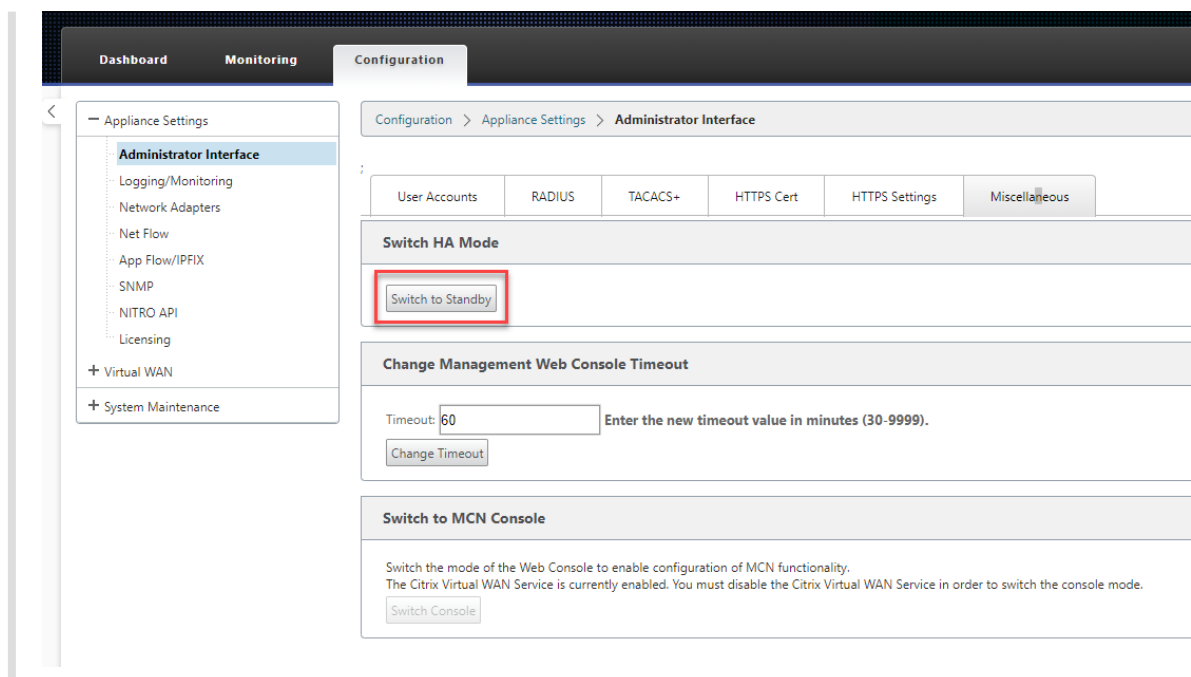
Klicken Sie neben **Hochverfügbarkeits-IP-Schnittstellen** auf **+**, um Schnittstellengruppen zu konfigurieren. Geben Sie Werte für die folgenden Parameter ein:

- **Virtual Interface** —Das virtuelle Interface, das für die Kommunikation zwischen den Appliances im Hochverfügbarkeitspaar verwendet wird. Es überwacht die Active Appliance auf Erreichbarkeit. Für den Einarm-Hochverfügbarkeitsmodus ist nur eine Schnittstellengruppe erforderlich.
- **Primär** —Die eindeutige virtuelle IP-Adresse für das primäre Gerät. Die sekundäre Appliance verwendet die primäre virtuelle IP-Adresse, um mit der primären Appliance zu kommunizieren.
- **Sekundär** —Die eindeutige virtuelle IP-Adresse für das sekundäre Gerät. Die primäre Appliance verwendet die sekundäre virtuelle IP-Adresse, um mit der sekundären Appliance zu kommunizieren.

Klicken Sie links neben dem neuen Eintrag für **Hochverfügbarkeits-IP-Schnittstellen** auf **+**. Geben Sie im Feld Externe **Sendungsverfolgungs-IP-Adresse** die IP-Adresse des externen Geräts ein, das auf ARP-Anforderungen reagiert, um den Status der primären Appliance zu bestimmen, und klicken Sie dann auf **Übernehmen**.

Hinweis:

Sie können eine HA-Umschaltung auch manuell von der Appliance aus auslösen. Navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Administratorschnittstelle > Verschiedenes**. Klicken Sie im Abschnitt HA-Modus **wechseln je nach HA-Appliance auf In Standbywechseln oder Zu Aktiv** wechseln.



Überwachen

So überwachen Sie die Konfiguration mit hoher Verfügbarkeit:

Melden Sie sich bei der SD-WAN-Webverwaltungsschnittstelle für die Active und Standby-Appliance an, für die eine hohe Verfügbarkeit implementiert ist. Zeigen Sie den Status der hohen Verfügbarkeit auf der Registerkarte **Dashboard** an.

DashboardMonitoringConfiguration

System Status

Name:

BLR_DC-Appliance

Model:

4000

Appliance Mode:

MCN

Management IP Address:

10.105.58.172

Appliance Uptime:

3 days, 7 hours, 1 minutes, 43.0 seconds

Service Uptime:

3 days, 6 hours, 39 minutes, 51.0 seconds

Routing Domain Enabled:

Default_RoutingDomain

High Availability Status

Local Appliance:

Active

Peer Appliance:

Standby

Last Update Received:

0 seconds ago

DashboardMonitoringConfiguration

System Status

Name:

BLR_DC-BLR_DC_HA

Model:

4000

Appliance Mode:

MCN

Management IP Address:

10.105.58.142

Appliance Uptime:

1 weeks, 1 days, 12 hours, 41 minutes, 5.3 seconds

Service Uptime:

3 days, 6 hours, 50 minutes, 31.0 seconds

Routing Domain Enabled:

Default_RoutingDomain

High Availability Status

Local Appliance:

Standby

Peer Appliance:

Active

Last Update Received:

0 seconds ago

Informationen zu Netzwerkadaptern zu Active und Standby-Hochverfügbarkeits-Appliances finden Sie unter **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Ethernet**.

DashboardMonitoringConfiguration

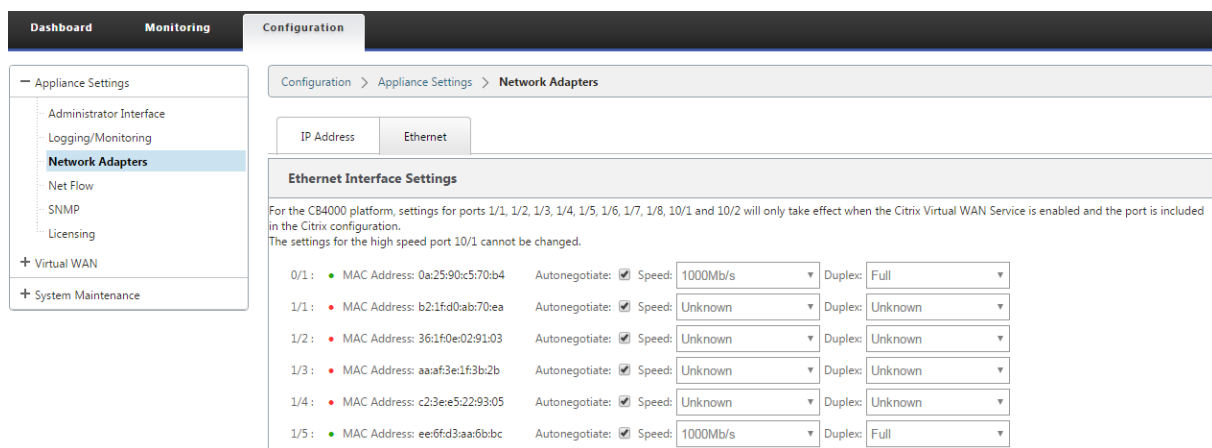
Configuration > Appliance Settings > Network Adapters

IP AddressEthernet

Ethernet Interface Settings

For the CB4000 platform, settings for ports 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 10/1 and 10/2 will only take effect when the Citrix Virtual WAN Service is in the Citrix configuration.
The settings for the high speed port 10/1 cannot be changed.

| | | | | | | | |
|-------|--------------------------------|----------------|-------------------------------------|--------|----------|---------|---------|
| 0/1 : | MAC Address: 0a:c4:7a:14:c9:d6 | Autonegotiate: | <input checked="" type="checkbox"/> | Speed: | 1000Mb/s | Duplex: | Full |
| 1/1 : | MAC Address: 5a:4c:f8:f0:71:b2 | Autonegotiate: | <input checked="" type="checkbox"/> | Speed: | Unknown | Duplex: | Unknown |
| 1/2 : | MAC Address: d6:1e:72:d5:d1:18 | Autonegotiate: | <input checked="" type="checkbox"/> | Speed: | 1000Mb/s | Duplex: | Full |
| 1/3 : | MAC Address: 66:4f:9d:c5:48:d2 | Autonegotiate: | <input checked="" type="checkbox"/> | Speed: | Unknown | Duplex: | Unknown |
| 1/4 : | MAC Address: 46:63:cb:5d:39:db | Autonegotiate: | <input checked="" type="checkbox"/> | Speed: | 1000Mb/s | Duplex: | Full |
| 1/5 : | MAC Address: 06:7b:ce:9a:c5:dd | Autonegotiate: | <input checked="" type="checkbox"/> | Speed: | 1000Mb/s | Duplex: | Full |



Problembehandlung

Führen Sie die folgenden Schritte zur Fehlerbehebung durch, während Sie die SD-WAN-Appliance im Hochverfügbarkeitsmodus (HA) konfigurieren:

1. Der Hauptgrund für Split-Brain-Problem ist auf Kommunikationsprobleme zwischen den HA-Appliances zurückzuführen.
 - Überprüfen Sie, ob ein Problem mit der Konnektivität (z. B. die Ports der beiden SD-WAN-Appliance sind hoch- oder heruntergefahren) zwischen den SD-WAN-Appliances.
 - Der SD-WAN-Dienst muss auf einer der SD-WAN-Appliances deaktiviert werden, um sicherzustellen, dass nur eine SD-WAN-Appliance aktiv ist.
2. Sie können die HA-bezogenen Protokolle überprüfen, die in der Datei **SDWAN_common.log** angemeldet sind.

HINWEIS

Alle HA-bezogenen Protokolle werden mit dem Schlüsselwort **racpp** protokolliert.

3. Sie können die portbezogenen Ereignisse in der Datei **SDWAN_common.log** überprüfen (z. B. gehen die HA-fähigen Ports aus oder nach oben).
4. Bei jeder HA-Statusänderung wird ein SD-WAN-Ereignis protokolliert. Wenn also die Protokolle überrollt werden, können Sie die Ereignisprotokolle überprüfen, um die Ereignisdetails abzurufen.

Hochverfügbarkeit des Edge-Modus mit Glasfaser-Y-Kabel aktivieren

September 26, 2023

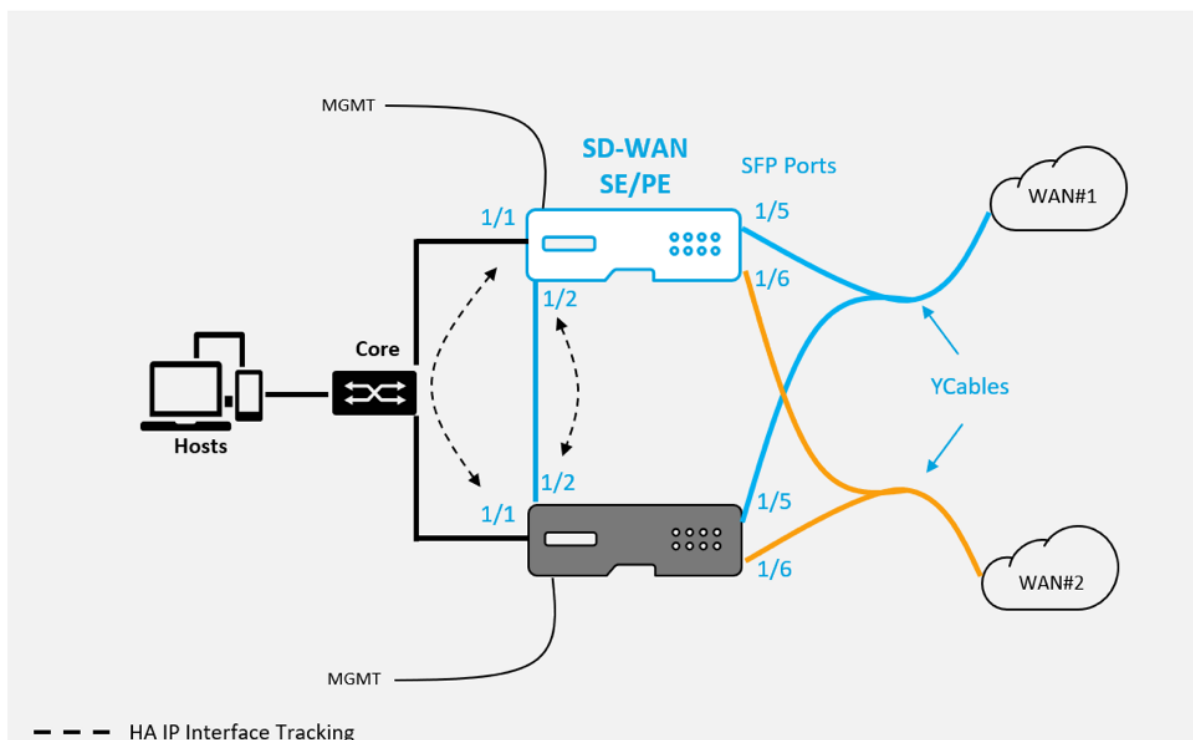
Hinweis: In Version 10.2, Version 2, ist diese Funktionalität nur für die 1100 SE/PE-Appliance anwendbar.

Im folgenden Verfahren werden die Schritte zum Aktivieren von High Availability (HA) auf 1100 SE/PE-Appliances beschrieben, die im Edge-Modus bereitgestellt werden, wobei die Übergabe von den WAN-Link-Diensteanbietern Glasfaser erfolgt.

Die verfügbaren SFP-Ports (Small Form-Factor Pluggable) auf 1100 Appliances können mit Glasfaser-Y-Kabeln verwendet werden, um eine Hochverfügbarkeitsfunktion für die Edge-Modus-Bereitstellung zu ermöglichen.

Auf der 1100 SE/PE-Einheit verbindet das Splitterkabel Splitting mit Glasfaseranschlüssen von zwei 1100 Einheiten, die im HA-Paar konfiguriert sind.

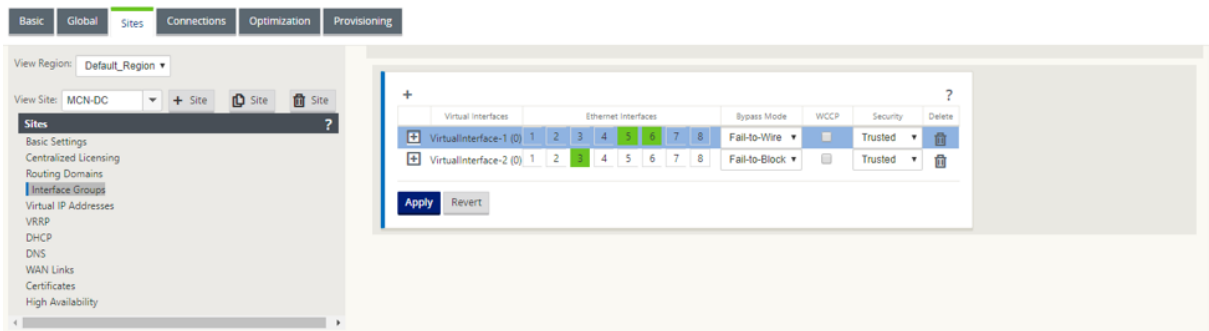
Das Glasfaser-Y-Kabel hat drei Enden. Ein Ende verbindet sich mit der Glasfaser-Übergabe des Anbieters, und die anderen beiden Enden verbinden sich mit SFP-Ports, die für diese WAN-Verbindung konfiguriert sind, auf zwei 1100 SE/PE-Appliances, die im HA-Paar bereitgestellt werden. Das Splitterkabel wird verwendet, um ein eingehendes Signal in mehrere Signale zu teilen.



Voraussetzungen:

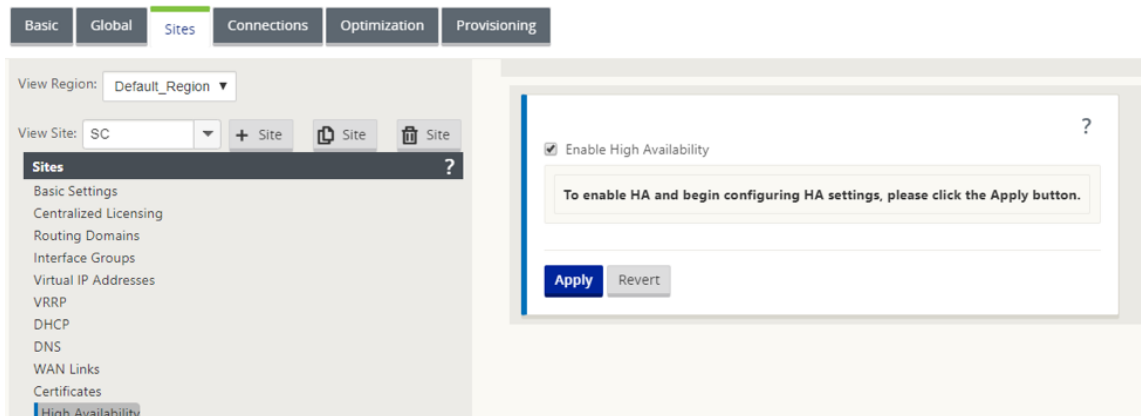
1. Auf der 1100 SE/PE-Appliance sind die Ports 1/5 und 1/6 SFP-Ports. Schließen Sie die Splitterenden des Y-Kabels an einen dieser Ports an beiden Geräten im HA-Paar an. [1100 SE](#) Weitere Informationen finden Sie unter.
2. Fügen Sie der SD-WAN-Appliance-Konfiguration SFP-Ports hinzu. Die Konfiguration der SFP-Ports entspricht dem Konfigurieren von Netzwerkschnittstellenports. Weitere Informationen

finden Sie unter [Konfigurieren von Schnittstellengruppen](#). Durch das Hinzufügen von 1/5 oder 1/6 Ports zur Konfiguration können Sie die Y-Kabelunterstützungsfunktion aktivieren.

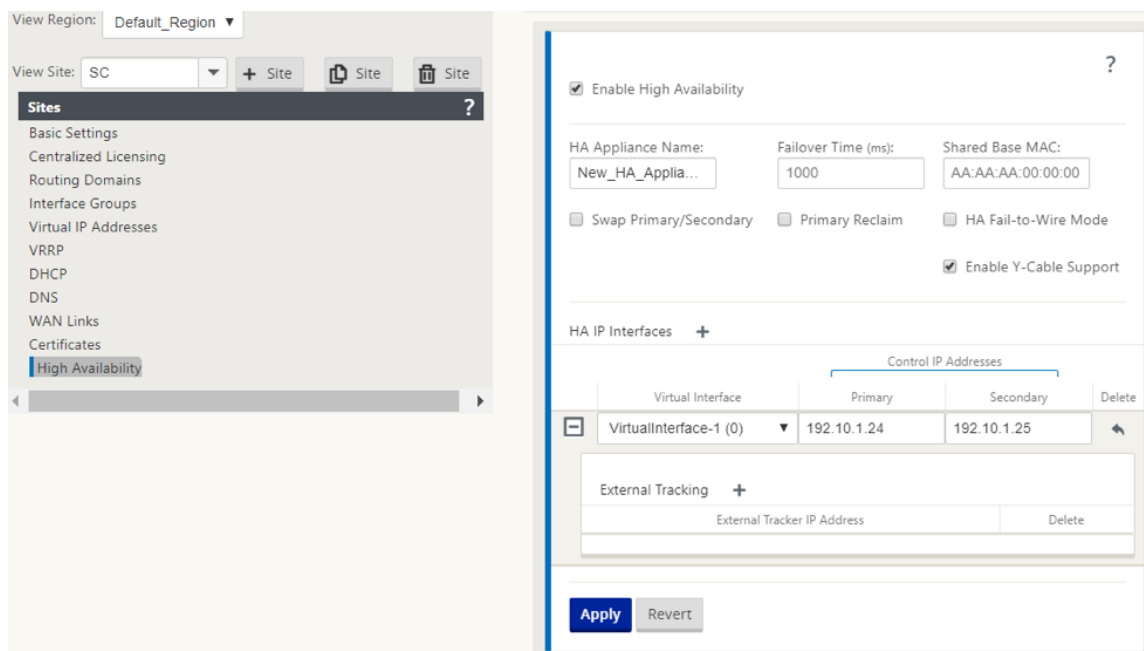


So aktivieren Sie Hochverfügbarkeit mit Y-Kabel:

1. Navigieren Sie in der GUI der 1100 SE/PE-Einheit zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor > Sites**. Klicken Sie auf **Hochverfügbarkeit aktivieren**.



2. Klicken Sie auf **Y-Kabelunterstützung aktivieren**.
3. Fügen Sie HA IP Interfaces hinzu, indem Sie neben den Schnittstellen, die an die Y-Kabel angeschlossen sind (z. B. 1/1 LAN-Schnittstelle oder 1/2 direkt angeschlossene Schnittstellen) verwenden. Wenn die Y-Kabel-Funktion aktiviert ist, können keine SFP-Ports für die HA-IP-Schnittstellen verwendet werden.



4. Übernehmen, Stage und Aktivieren der Konfiguration.

Einschränkungen:

- HA Fail-to-Wire-Modus Konfiguration mit Y-Kabel wird nicht unterstützt.
- Die SFPs, die mit dem Y-Kabel verbunden sind, können nicht als HA-IP-Schnittstellenverfolgung verwendet werden.
- Softwareversion 10.2.2 oder höher und 11.0 oder höher ist erforderlich, um diese Bereitstellung zu unterstützen.

Keine Berührung

October 28, 2021

Hinweis

Der Zero Touch-Bereitstellungsdienst wird nur auf ausgewählten Citrix SD-WAN-Appliances unterstützt:

- SD-WAN 110 Standard Edition
- SD-WAN 210 Standard Edition
- SD-WAN 410 Standard Edition
- SD-WAN 2100 Standard Edition
- SD-WAN 1000 Standard Edition (Reimaging erforderlich)

- SD-WAN 1000 Enterprise Edition (Premium Edition) (Reimaging erforderlich)
- SD-WAN 1100 Standard Edition
- SD-WAN 1100 Premium (Enterprise) Edition
- SD-WAN 2000 Standard Edition (Reimaging erforderlich)
- SD-WAN 2000 Enterprise Edition (Premium Edition) (Reimaging erforderlich)
- SD-WAN 2100 Enterprise Edition (Premium Edition)
- SD-WAN AWS VPX-Instanz

Zero-Touch-Bereitstellung Cloud Service ist ein von Citrix betriebener und verwalteter cloud-basierter Dienst, der die Erkennung neuer Appliances im Citrix SD-WAN-Netzwerk ermöglicht und sich hauptsächlich auf die Rationalisierung des Bereitstellungsprozesses für Citrix SD-WAN an Zweigstellen- oder Cloud-Servicebüros konzentriert. Der Zero-Touch-Bereitstellungs-Cloud-Service ist von jedem beliebigen Punkt im Netzwerk über den öffentlichen Internetzugang zugänglich. Auf den Zero-Touch-Bereitstellungs-Cloud-Dienst wird über das Secure Socket Layer (SSL)-Protokoll zugegriffen.

Die Null-Touch-Bereitstellung Cloud Services kommunizieren sicher mit Back-End-Citrix Diensten, die eine gespeicherte Identifikation von Citrix Kunden hosten, die Zero Touch-fähige Geräte erworben haben (z. B. SD-WAN 410-SE, 2100-SE). Die Back-End-Dienste sind vorhanden, um jede Zero Touch Deployment-Anforderung zu authentifizieren, wobei die Zuordnung zwischen dem Kundenkonto und den Seriennummern von Citrix SD-WAN Appliances ordnungsgemäß überprüft wird.

ZTD High-Level-Architektur und Workflow:

Standort des Rechenzentrums:

Citrix SD-WAN-Administrator —Ein Benutzer mit Administratorrechten für die SD-WAN-Umgebung mit den folgenden primären Zuständigkeiten:

- Konfigurationserstellung mit dem Citrix SD-WAN Center Netzwerkkonfigurationstool oder Import der Konfiguration von der Master Control Node (MCN) SD-WAN-Appliance
- Citrix Cloud Login, um den Zero Touch Deployment Service für die Bereitstellung neuer Standortknoten zu initiieren.

Hinweis

Wenn Ihr SD-WAN Center über einen Proxyserver mit dem Internet verbunden ist, müssen Sie die Proxyserver-Einstellungen im SD-WAN Center konfigurieren. Weitere Informationen finden Sie unter [Proxyserver-Einstellungen für die Zero Touch-Bereitstellung](#).

Netzwerkadministrator —Ein Benutzer, der für die Verwaltung des Unternehmensnetzwerks verantwortlich ist (DHCP, DNS, Internet, Firewall usw.)

- Konfigurieren Sie ggf. Firewalls für die ausgehende Kommunikation mit dem FQDN ***sd-wanzt.citrixnetworkapi.net*** vom SD-WAN Center.

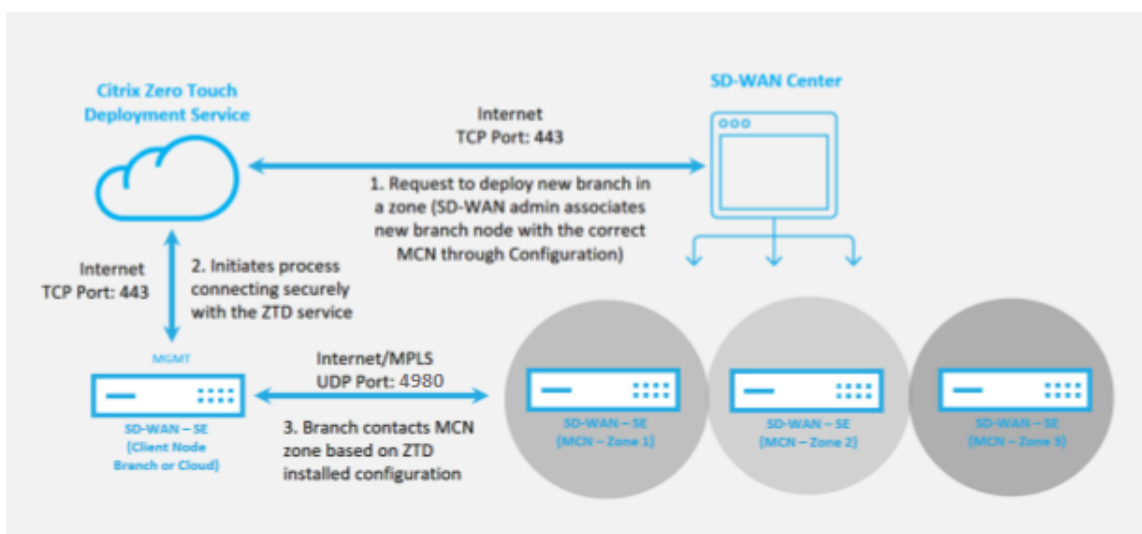
Remotestandort:

Vor-Ort-Installateur —Ein lokaler Ansprechpartner oder ein angestellter Installateur für Aktivitäten vor Ort mit den folgenden Hauptaufgaben:

- Entpacken Sie die Citrix SD-WAN-Appliance physisch.
- Reimaging nicht-ZTD-fähiger Appliances.
 - Benötigt für: SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
 - Nicht erforderlich für: SD-WAN 410-SE, 2100-SE
- Netzkabel der Appliance.
- Verdrahten Sie die Appliance für die Internetverbindung auf der Verwaltungsschnittstelle (z. B. MGMT oder 0/1).
- Verkabeln Sie die Appliance für die WAN-Link-Konnektivität auf den Datenschnittstellen (z. B. APA.wan, APB.wan, APC.wan, 0/2, 0/3, 0/5 usw.).

Hinweis

Das Schnittstellenlayout ist für jedes Modell unterschiedlich. Verweisen Sie daher auf die Dokumentation zur Identifizierung von Daten und Management-Ports.

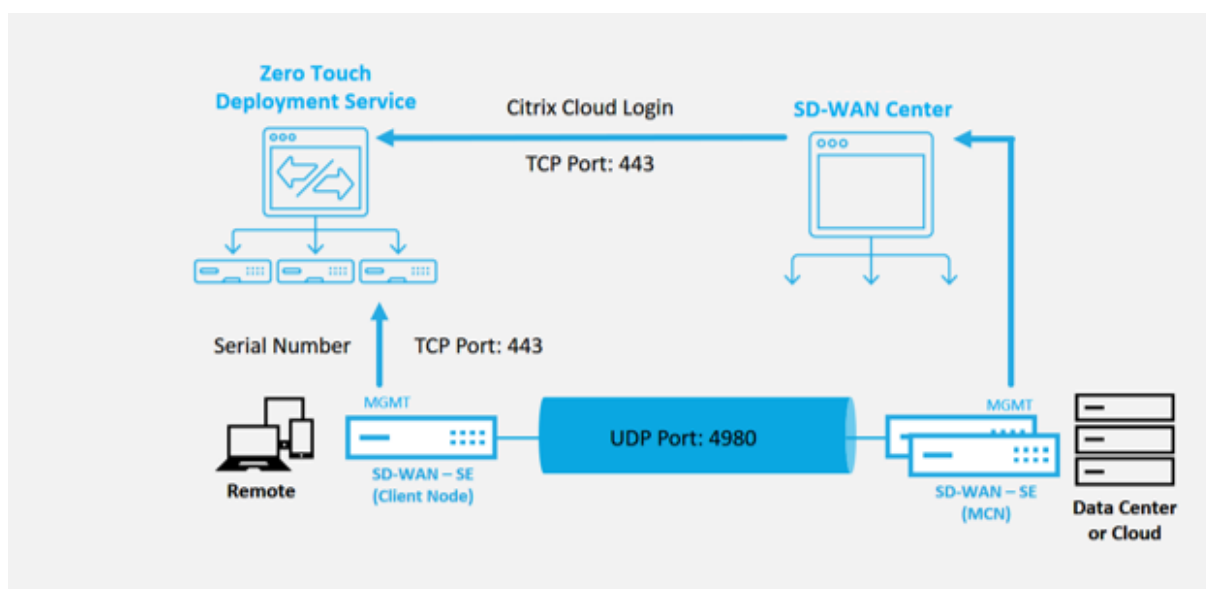


Die folgenden Voraussetzungen sind erforderlich, bevor Sie einen Zero Touch-Bereitstellungsdienst starten:

- Aktive Ausführung von SD-WAN auf Master Control Node (MCN) heraufgestuft.
- Aktives Ausführen von SD-WAN Center mit Konnektivität zum MCN über Virtual Path.
- Citrix Cloud-Anmeldeinformationen, die auf <https://onboarding.cloud.com> erstellt wurden (verweisen Sie auf die nachstehende Anleitung zur Kontoerstellung).

- Verwaltungsnetzwerkonnektivität (SD-WAN Center und SD-WAN-Appliance) mit dem Internet an Port 443, entweder direkt oder über einen Proxyserver.
- (optional) Mindestens eine aktiv ausgeführte SD-WAN-Appliance, die in einer Zweigstelle im Clientmodus mit gültiger Virtual Path-Konnektivität zu MCN betrieben wird, um die erfolgreiche Pfadeinrichtung im bestehenden Unterlagennetzwerk zu überprüfen.

Die letzte Voraussetzung ist keine Anforderung, ermöglicht es dem SD-WAN-Administrator jedoch zu überprüfen, ob das Unterlagennetzwerk die Einrichtung virtueller Pfade ermöglicht, wenn die Zero Touch-Bereitstellung mit einer neu hinzugefügten Site abgeschlossen ist. Dies bestätigt in erster Linie, dass die entsprechenden Firewall- und Routenrichtlinien vorhanden sind, um entweder den NAT-Verkehr entsprechend zu erreichen, oder um zu bestätigen, dass der UDP-Port 4980 erfolgreich in das Netzwerk eindringen kann, um den MCN zu erreichen.



Überblick über den Zero Touch-Bereitstellungsdienst:

Der Zero Touch Deployment Service arbeitet zusammen mit dem SD-WAN Center, um eine einfachere Bereitstellung von SD-WAN-Appliances in Zweigstellen zu ermöglichen. SD-WAN Center wird als zentrales Verwaltungstool für die SD-WAN Standard und Enterprise (Premium) Edition-Appliances konfiguriert und verwendet. Um den Zero Touch Deployment Service (oder den Zero-Touch-Bereitstellungs-Cloud-Dienst) zu verwenden, muss ein Administrator zunächst das erste SD-WAN-Gerät in der Umgebung bereitstellen und dann das SD-WAN Center als zentralen Verwaltungspunkt konfigurieren und bereitstellen. Wenn das SD-WAN Center, Version 9.1 oder höher, mit Konnektivität zum öffentlichen Internet auf Port 443 installiert ist, initiiert SD-WAN Center automatisch den Cloud-Dienst und installiert die erforderlichen Komponenten, um die Zero Touch Deployment-Funktionen freizuschalten und die Zero Touch Deployment Option in der GUI von SD-WAN Center. Die Zero Touch-Bereitstellung ist in der SD-WAN Center-Software standardmäßig nicht verfügbar. Dies wurde absichtlich entwickelt, um sicherzustellen, dass die richtigen vorläufigen Komponenten im Unterlagennetzwerk vorhanden sind,

bevor ein Administrator Vor-Ort-Aktivitäten im Zusammenhang mit Zero Touch Deployment initiieren kann.

Nachdem eine funktionierende SD-WAN-Umgebung eingerichtet wurde und die Registrierung beim Zero Touch Deployment Service ausgeführt wurde, erfolgt durch Erstellen eines Citrix Cloud-Kontos. Da SD-WAN Center mit dem Zero-Touch-Bereitstellungsservice kommunizieren kann, stellt die Benutzeroberfläche die Zero Touch Deployment Optionen auf der Registerkarte **Konfiguration** bereit. Die Anmeldung beim Zero Touch Service authentifiziert die Kunden-ID, die der jeweiligen SD-WAN-Umgebung zugeordnet ist, und registriert das SD-WAN-Center, zusätzlich zum Entsperren des Kontos für die weitere Authentifizierung von Null-Touch-Bereitstellungs-Appliance-Bereitstellungen.

Mithilfe des Netzwerkkonfigurationstools im SD-WAN Center muss der SD-WAN-Administrator dann die Vorlagen- oder Klon-Site-Funktionen verwenden, um die SD-WAN-Konfiguration zu erstellen und neue Sites hinzuzufügen. Die neue Konfiguration wird vom SD-WAN Center verwendet, um die Bereitstellung der Zero-Touch-Bereitstellung für die neu hinzugefügten Sites zu initiieren. Wenn der SD-WAN-Administrator mithilfe des Zero-Touch-Bereitstellungsprozesses einen Standort zur Bereitstellung initiiert, hat er die Möglichkeit, die für die Zero-Touch-Bereitstellung zu verwendende Appliance vorab zu authentifizieren, indem er die Seriennummer vorab ausfüllt und die E-Mail-Kommunikation mit dem Installationsprogramm vor Ort initiiert, um vor Ort zu beginnen Aktivität.

Der Onsite-Installer erhält E-Mail-Kommunikation, dass der Standort für die Zero Touch Deployment bereit ist, und kann mit dem Installationsvorgang für das Einschalten und Verkabeln der Appliance für die DHCP-IP-Adresszuweisung und den Internetzugriff über den MGMT-Anschluss beginnen. Verkabelung in allen LAN- und WAN-Ports. Alles andere wird vom Zero-Touch-Bereitstellungsdienst initiiert und der Fortschritt wird mithilfe der Aktivierungs-URL überwacht. Falls es sich bei dem zu installierenden Remote-Knoten um eine Cloud-Instanz handelt, startet das Öffnen der Aktivierungs-URL den Workflow, um die Instanz automatisch in der dafür vorgesehenen Cloud-Umgebung zu installieren. Ein lokaler Installer benötigt keine Aktion.

Der Zero Touch Deployment Cloud Service automatisiert die folgenden Aktionen:

Laden Sie den Zero-Touch-Bereitstellungs-Agent herunter und aktualisieren Sie diesen, wenn neue Funktionen auf der Zweigeinheit verfügbar sind.

- Authentifizieren Sie die Zweigstellenappliance, indem Sie die Seriennummer überprüfen.
- Authentifizieren Sie, dass der SD-WAN-Administrator die Site für die Null-Touch-Bereitstellung mit dem SD-WAN-Center akzeptiert hat.
- Ziehen Sie die für die Ziel-Appliance spezifische Konfigurationsdatei aus dem SD-WAN-Center.
- Schieben Sie die für die Ziel-Appliance spezifische Konfigurationsdatei an die Zweigeinheit.
- Installieren Sie die Konfigurationsdatei auf der Zweigeinheit.
- Schieben Sie alle fehlenden SD-WAN-Softwarekomponenten oder erforderlichen Updates auf die Zweigeinheit.

- Push einer temporären 10-Mbit/s-Lizenzdatei zum Bestätigen der Herstellung virtueller Pfade zur Zweigstellenappliance.
- Aktivieren Sie den SD-WAN-Dienst auf der Zweigseinheit.

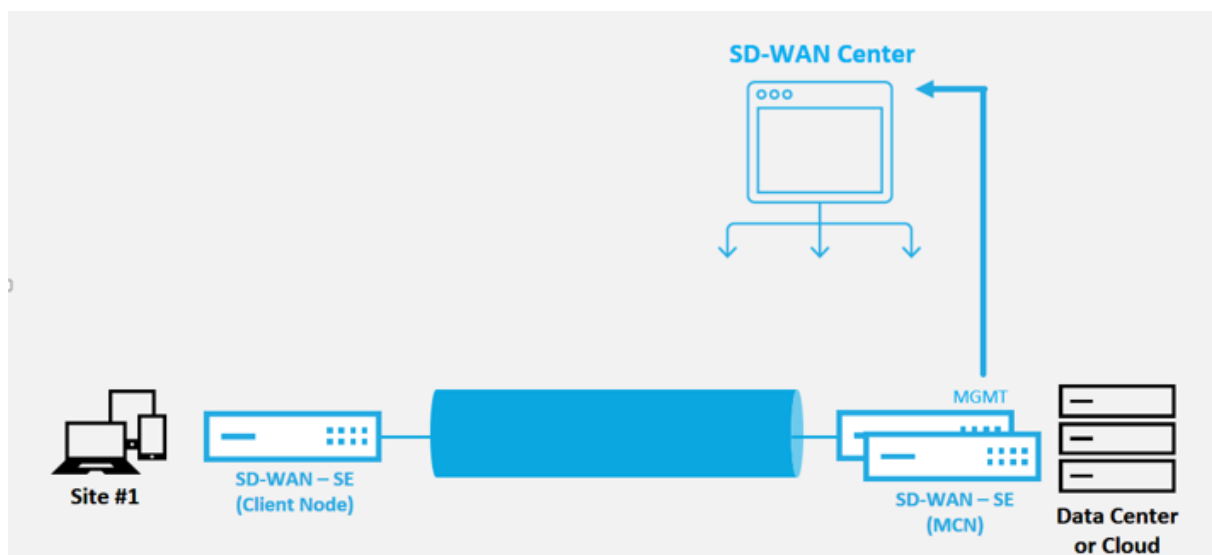
Der SD-WAN-Administrator benötigt weitere Schritte, um eine permanente Lizenzdatei auf der Appliance zu installieren.

Hinweis

Während der Durchführung einer Zweigstellenkonfiguration, die bereits die gleiche Version der Appliance-Software enthält, die in MCN verwendet wird, lädt der Zero-Touch-Deployment-Prozess die Appliance-Softwaredatei nicht erneut herunter. Diese Änderung gilt für neu ausgelieferte Appliances, Appliances, die auf Werkseinstellungen zurückgesetzt und die Konfiguration administrativ zurückgesetzt werden. Wenn die Konfiguration zurückgesetzt wird, aktivieren Sie das Kontrollkästchen **Nach dem Wiederherstellen neu starten**, um den Zero-Touch-Bereitstellungsprozess zu starten.

Zero Touch-Bereitstellungsverfahren

Im folgenden Verfahren werden die Schritte beschrieben, die zum Bereitstellen einer neuen Site mit dem Zero Touch Deployment Service erforderlich sind. Lassen Sie einen laufenden MCN und einen Clientknoten bereits mit ordnungsgemäßer Kommunikation zum SD-WAN Center arbeiten, und etablieren Sie virtuelle Pfade, die die Konnektivität über das Unterlagennetzwerk bestätigen. Die folgenden Schritte sind für den SD-WAN-Administrator erforderlich, um die Bereitstellung von Zero Touch zu initiieren:



Konfigurieren des Zero Touch-Bereitstellungsdienstes

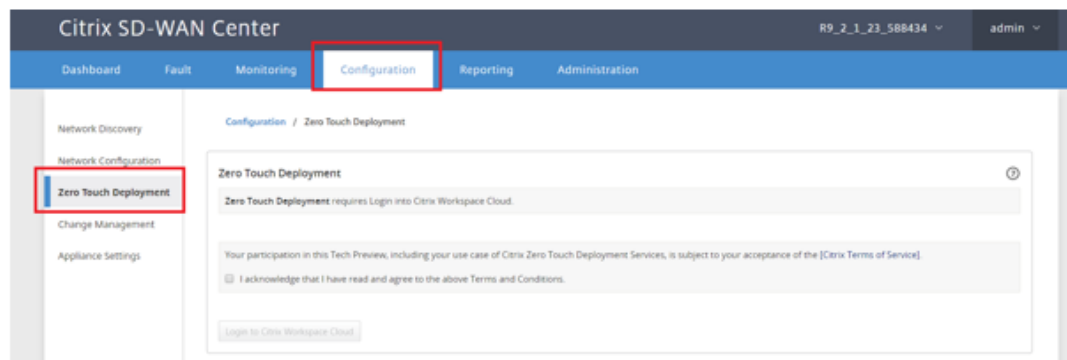
Das SD-WAN-Center verfügt über die Funktionalität, um Anforderungen von neu verbundenen Appliances zu akzeptieren, um dem SD-WAN Enterprise-Netzwerk beizutreten. Die Anforderung wird über den Zero-Touch-Bereitstellungsdienst an das Webinterface weitergeleitet. Sobald die Appliance eine Verbindung zum Dienst herstellt, werden Konfigurations- und Software-Upgrade-Pakete heruntergeladen.

Konfigurations-Workflow:

- Greifen Sie auf **SD-WAN Center** zu > **Neue Standortkonfiguration erstellen** oder Importieren Sie die vorhandene Konfiguration und speichern Sie sie.
- Melden Sie sich bei Citrix Cloud an, um den Zero-Touch-Bereitstellungsdienst zu aktivieren. Die Menüoption Zero Touch Deployment wird nun in der Web-Management-Oberfläche des SD-WAN Centers angezeigt.
- Navigieren Sie im SD-WAN Center zu **Konfiguration** > **Zero Touch-Bereitstellung** > **Neuen Standort bereitstellen**.
- Wählen Sie eine Appliance aus, klicken Sie auf **Aktivieren** und dann auf **Bereitstellen**.
- Das Installationsprogramm erhält die Aktivierungs-E-Mail > Geben Sie die Seriennummer ein > **Aktivieren** > Appliance wurde erfolgreich bereitgestellt.

So konfigurieren Sie Zero Touch-Bereitstellungsdienst:

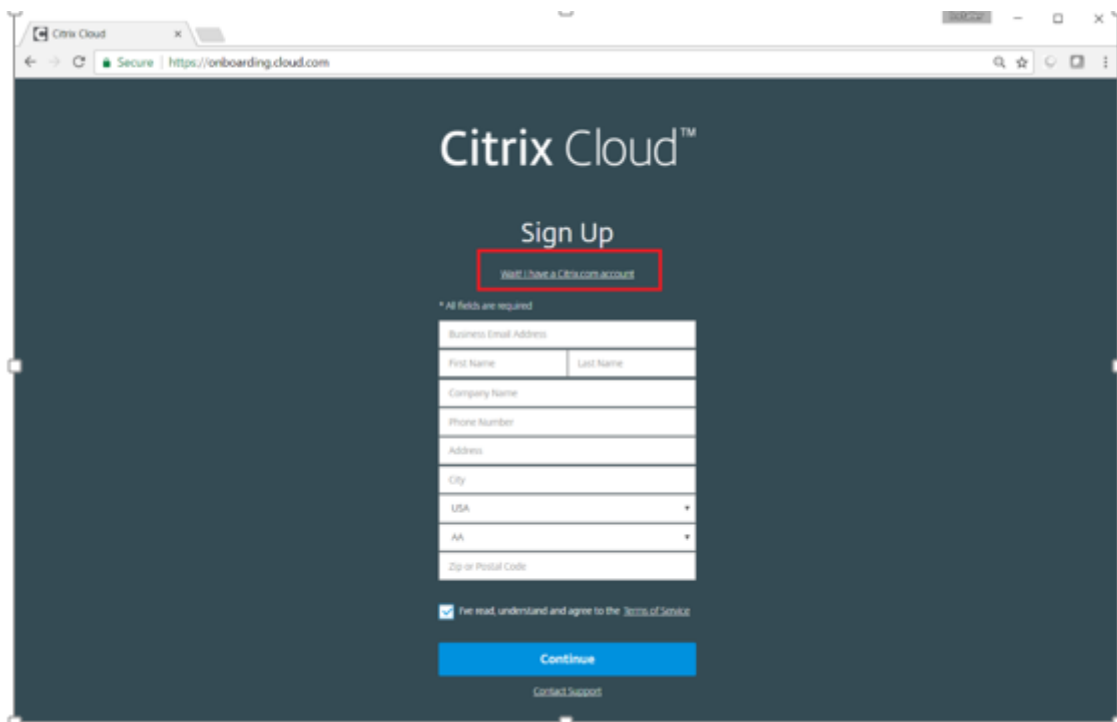
1. Installieren Sie das SD-WAN Center mit aktivierten Zero Touch Deployment-Funktionen:
 - a) Installieren Sie SD-WAN Center mit der zugewiesenen DHCP-IP-Adresse.
 - b) Stellen Sie sicher, dass das SD-WAN Center eine ordnungsgemäße Management-IP-Adresse und Netzwerk-DNS-Adresse mit Konnektivität zum öffentlichen Internet im Verwaltungsnetzwerk zuweist.
 - c) Aktualisieren Sie das SD-WAN Center auf die neueste Version der SD-WAN-Software.
 - d) Bei ordnungsgemäßer Internetverbindung initiiert das SD-WAN Center den Cloud-Dienst für die Zero-Touch-Bereitstellung und lädt automatisch alle Firmware-Updates herunter und installiert sie, die für die Zero-Touch-Bereitstellung spezifisch sind. Wenn dieses Call Home-Verfahren fehlschlägt, ist die folgende Zero Touch-Bereitstellungsoption in der GUI nicht verfügbar.



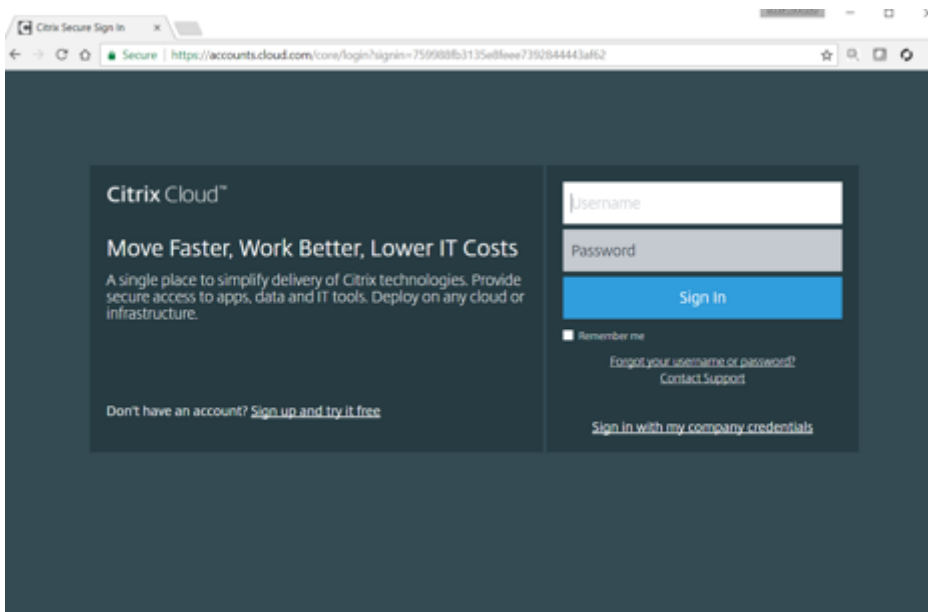
- e) Lesen Sie die Allgemeinen Geschäftsbedingungen und wählen Sie dann **Ich bestätige, dass ich die oben genannten Geschäftsbedingungen gelesen habe und damit einverstanden bin.**
- f) Klicken Sie auf die Schaltfläche Bei **Citrix Workspace Cloud anmelden**, wenn bereits ein Citrix Cloud-Konto erstellt wurde.
- g) Melden Sie sich beim Citrix Cloud-Konto an, und nachdem Sie die folgende Meldung über die erfolgreiche Anmeldung erhalten haben, **SCHLIESSEN SIE BITTE DIESES FENSTER NICHT. DER PROZESS BENÖTIGT WEITERE 20 SEKUNDEN, BIS DIE SD-WAN CENTER GUI AKTUALISIERT WIRD.** Das Fenster muss von selbst geschlossen werden, wenn es fertig ist.



2. Gehen Sie folgendermaßen vor, um ein Cloud-Anmeldekonto zu erstellen: Öffnen Sie einen Webbrowser auf <https://onboarding.cloud.com>
3. Klicken Sie auf den Link für **Wait, ich habe ein Citrix.com-Konto.**



4. Melden Sie sich mit einem vorhandenen Citrix Konto an.



5. Sobald Sie sich bei der SD-WAN Center Zero Touch Deployment angemeldet haben, stellen Sie möglicherweise fest, dass keine Sites für die Zero-Touch-Bereitstellung verfügbar sind, da die folgenden Gründe folgende Ursachen haben:

- Die aktive Konfiguration wurde nicht im Dropdownmenü Konfiguration ausgewählt.
- Alle Standorte für die aktuell aktive Konfiguration wurden bereits bereitgestellt

- Die Konfiguration wurde nicht mit dem SD-WAN Center erstellt, sondern mit dem Konfigurationseditor, der im MCN
 - Sites wurden nicht in der Konfiguration erstellt, die auf Null-Touch-fähige Appliances verweisen (z. B. 410-SE, 2100-SE, Cloud VPX)
6. Aktualisieren Sie die Konfiguration, um einen **neuen Remote-** Standort mit einer **ZTD-fähigen SD-WAN-Appliance** mithilfe der SD-WAN-Center-Netzwerkkonfiguration hinzuzufügen.

Wenn die SD-WAN-Konfiguration nicht mit der SD-WAN-Center-Netzwerkkonfiguration erstellt wurde, importieren Sie die aktive Konfiguration aus dem MCN und beginnen Sie mit der Änderung der Konfiguration mit dem SD-WAN Center. Für die Zero Touch-Bereitstellung muss der SD-WAN-Administrator die Konfiguration mithilfe des SD-WAN-Centers erstellen. Das folgende Verfahren muss verwendet werden, um einen neuen Standort hinzuzufügen, der für die Null-Touch-Bereitstellung vorgesehen ist.

- a) Entwerfen Sie die neue Site für die SD-WAN-Appliance-Bereitstellung, indem Sie zunächst die Details der neuen Site skizzieren (Appliance-Modell, Verwendung von Schnittstellen-gruppen, virtuelle IP-Adressen, WAN-Verbindungen mit Bandbreite und deren jeweiligen Gateways).

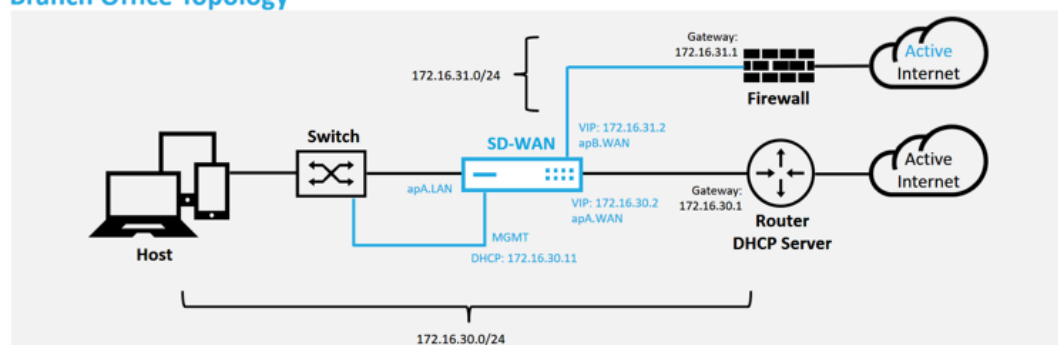
Wichtig

Möglicherweise stellen Sie jeden Standortknoten fest, für den VPX ausgewählt ist, da das Modell ebenfalls aufgeführt ist, aber derzeit ist die Null-Touch-Bereitstellungsunterstützung nur für die AWS VPX-Instanz verfügbar.

Hinweis

- Stellen Sie sicher, dass Sie einen Support-Webbrowser für Citrix SD-WAN Center verwenden
- Stellen Sie sicher, dass der Webbrowser während der Citrix Workspace-Anmeldung keine Popup-Fenster blockiert

Branch Office Topology



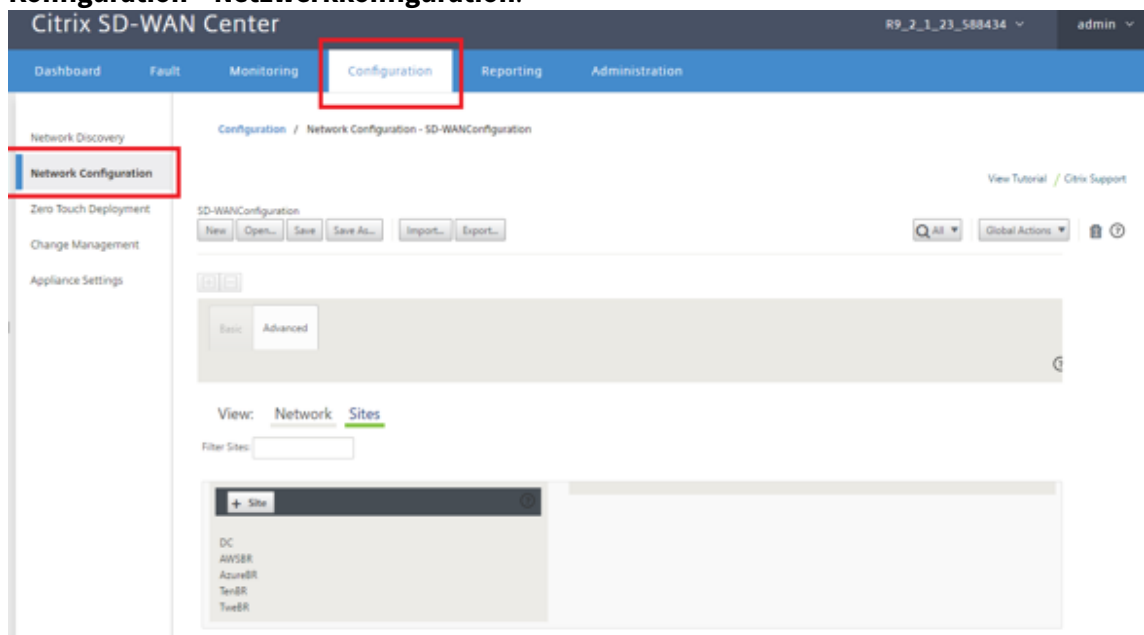
Dies ist ein Beispiel für die Bereitstellung eines Zweigstellenstandorts. Die SD-WAN-Appliance wird physisch im Pfad der vorhandenen MPLS-WAN-Verbindung über ein 172.16.30.0/24-Netzwerk bereitgestellt und eine vorhandene Backupverbindung verwendet, indem sie in einen aktiven Zustand aktiviert und diese zweite WAN-Verbindung direkt in die SD-WAN-Appliance auf ein anderes Subnetz 172.16.31.0/24.

Hinweis

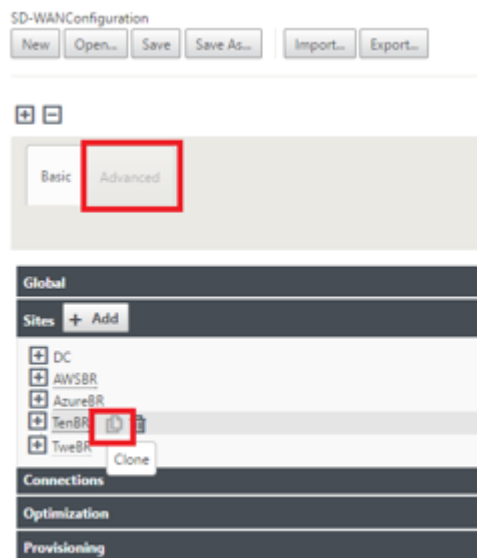
Die SD-WAN-Appliances weisen automatisch eine Standard-IP-Adresse 192.168.100.1/16 zu. Wenn DHCP standardmäßig aktiviert ist, stellt der DHCP-Server im Netzwerk der Appliance möglicherweise eine zweite IP-Adresse in einem Subnetz bereit, das den Standardwert überlappt. Dies kann möglicherweise zu einem Routingproblem auf der Appliance führen, bei dem die Appliance möglicherweise keine Verbindung zum Clouddienst für die Zero-Touch-Bereitstellung herstellen kann. Konfigurieren Sie den DHCP-Server so, dass IP-Adressen außerhalb des Bereichs 192.168.0.0/16 zugewiesen werden.

Für die Platzierung von SD-WAN-Produkten in einem Netzwerk stehen verschiedene Bereitstellungsmodi zur Verfügung. Im obigen Beispiel wird SD-WAN als Overlay auf der vorhandenen Netzwerkinfrastruktur bereitgestellt. Bei neuen Standorten können SD-WAN-Administratoren das SD-WAN im Edge- oder Gateway-Modus bereitstellen, wodurch die Notwendigkeit eines WAN-Edge-Routers und einer Firewall entfällt und die Netzwerkanforderungen des Edge-Routing und der Firewall auf der SD-WAN-Lösung konsolidiert werden.

7. Öffnen Sie die Web-Management-Schnittstelle des SD-WAN Center, und navigieren Sie zur Seite **Konfiguration > Netzwerkkonfiguration**.



8. Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration vom MCN.
9. Navigieren Sie zur Registerkarte Erweitert, um eine Site zu erstellen.
10. Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.
11. Erstellen Sie schnell die Konfiguration für die neue Site, indem Sie die Klonfunktion einer vorhandenen Site verwenden.



12. Füllen Sie alle erforderlichen Felder aus der Topologie aus, die für diesen neuen Zweigstandort entwickelt wurde

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name: **ThiBR** Appliance Name: **EE1000** Secure Key: 752a7ebe58cdd9a6

Routing Domains

| Name | Enable | Default |
|-----------------------|-------------------------------------|-------------------------------------|
| Default_RoutingDomain | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Virtual Interfaces

| Name | VLAN ID | DHCP |
|-------------|---------|--------------------------|
| ThiBR_Link1 | 0 | <input type="checkbox"/> |
| ThiBR_Link2 | 0 | <input type="checkbox"/> |

Virtual IP Addresses

| Include | Virtual Interface | Virtual IP Address/Prefix |
|-------------------------------------|-------------------|---------------------------|
| <input checked="" type="checkbox"/> | ThiBR_Link1 | 172.16.30.2/24 |
| <input checked="" type="checkbox"/> | ThiBR_Link2 | 172.16.31.2/24 |

Local Routes

Include Network Address Routing Domain Gateway

WAN Links

| Include Link | WAN Link | Access Type |
|-------------------------------------|-------------|-----------------|
| <input checked="" type="checkbox"/> | ThiBR-Link2 | Public Internet |

Access Interfaces

| Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway |
|-------------------------------------|------------------|-------------------|--------------------|-------------|
| <input checked="" type="checkbox"/> | ThiBR-Link2-AI-1 | ThiBR_Link2 | 172.16.31.2 | 172.16.31.1 |

ThiBR-Link1 Public Internet

Access Interfaces

| Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway |
|-------------------------------------|------------------|-------------------|--------------------|-------------|
| <input checked="" type="checkbox"/> | ThiBR-Link1-AI-1 | ThiBR_Link1 | 172.16.30.2 | 172.16.30.1 |

GRE Tunnels

Include Name Source IP Destination IP Tunnel IP / Prefix

Clone Cancel

13. Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen** der Site und vergewissern Sie sich, dass das SD-WAN-Modell korrekt ausgewählt ist, das den Zero-Touch-Dienst unterstützen würde.

Global

Sites **+ Add**

- DC
- AWSBR
- AzureBR
- TenBR
- ThiBR **Basic Settings** ?

Appliance Name: EE1000 Secure Key: 548d734bda6d306d **Regenerate**

Model: CB1000 Mode: client

Default Direct Route Cost: 5

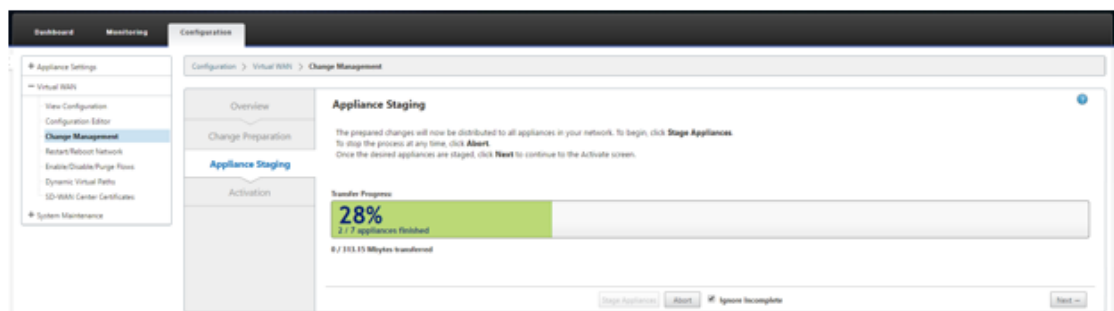
Gateway ARP Timer (ms): 1000

☐ Enable Source MAC Learning

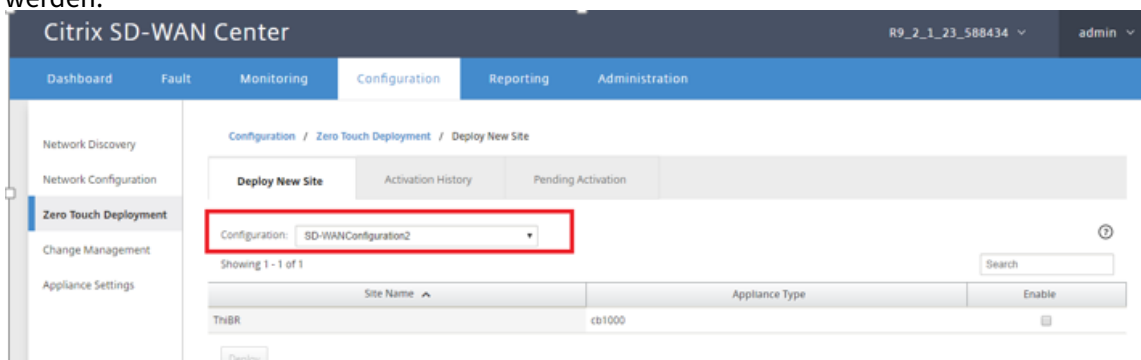
Routing Domains

Das SD-WAN-Modell für die Site kann aktualisiert werden, aber beachten Sie, dass die Schnittstellengruppen möglicherweise neu definiert werden müssen, da die aktualisierte Appliance möglicherweise ein neues Schnittstellenlayout hat als das, was zum Klonen verwendet wurde.

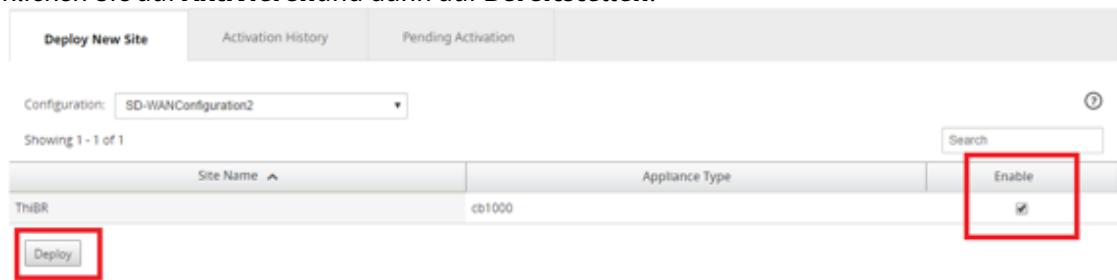
14. Speichern Sie die neue Konfiguration im SD-WAN Center, und verwenden Sie den Export in den **Change Management-Posteingang**, um die Konfiguration mithilfe von Change Management zu übertragen.
15. Folgen Sie dem Änderungsverwaltungsverfahren, um für die neue Konfiguration ordnungsgemäß ein Staging durchzuführen, wodurch die vorhandenen SD-WAN-Geräte auf die neue Site aufmerksam gemacht werden, die per Zero Touch bereitgestellt werden soll. Sie müssen die Option “Unvollständig ignorieren” verwenden, um den Versuch zu überspringen, die Konfiguration auf die neue Site zu übertragen, die noch den Zero-Touch-Bereitstellungs-Workflow durchlaufen muss.



16. Navigieren Sie zurück zur Seite “Zero Touch Deployment” von SD-WAN Center, und wenn die neue aktive Konfiguration ausgeführt wird, steht die neue Site für die Bereitstellung zur Verfügung.
17. Wählen Sie auf der Seite “Zero Touch Deployment” auf der Registerkarte **Neue Site bereitstellen** die laufende Netzwerkkonfigurationsdatei aus
18. Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit nicht bereitgestellten SD-WAN-Geräten angezeigt, die für keine Berührung unterstützt werden.



19. Wählen Sie die Zweigstellen aus, die Sie für den Zero Touch-Dienst konfigurieren möchten, klicken Sie auf **Aktivieren** und dann auf **Bereitstellen**.



20. Es wird ein Popupfenster Neue Site bereitstellen angezeigt, in dem der Administrator bei Bedarf die Seriennummer, die Straßenadresse der Zweigstelle, die E-Mail-Adresse des Installers und weitere Hinweise angeben kann.

Hinweis

Das Eingabefeld Seriennummer ist optional und führt je nachdem, ob es ausgefüllt ist oder nicht, zu einer Änderung der Aktivitäten vor Ort, für die der Installateur verantwortlich ist.

- Wenn das Feld Seriennummer ausgefüllt ist - der Installateur muss keine Seriennummer in die Aktivierungs-URL eingeben, die mit dem Befehl `deploy site` generiert wurde
- Wenn das Feld "Seriennummer" schwarz bleibt - Der Installer ist für die Eingabe des Korrigieren Sie die Seriennummer der Appliance in die Aktivierungs-URL, die mit dem Befehl `deploy site` generiert wurde

21. Nachdem Sie auf die Schaltfläche **Bereitstellen** geklickt haben, wird eine Meldung angezeigt, dass "Die Sitekonfiguration wurde bereitgestellt". Diese Aktion löst das SD-WAN-Center aus, das zuvor beim Clouddienst für die Zero-Touch-Bereitstellung registriert war, die Konfiguration dieser bestimmten Site so zu teilen, dass sie im Clouddienst der Zero-Touch-Bereitstellung gespeichert ist.

22. Navigieren Sie zur Registerkarte Ausstehende Aktivierung, um zu bestätigen, dass die Informationen der Zweigstands-site Site erfolgreich ausgefüllt wurden und in den Status der ausstehenden Installationsaktivität versetzt wurden.

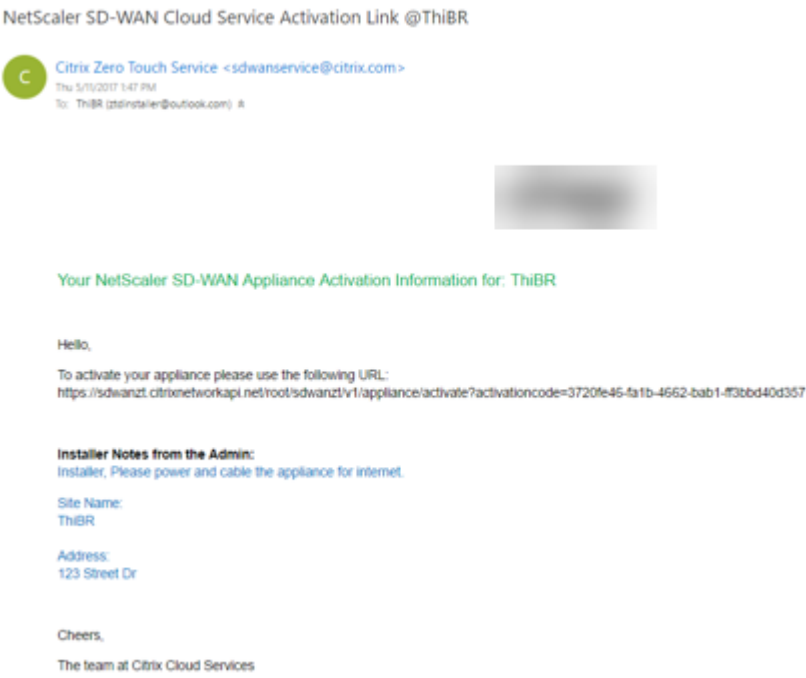
| Pending Activation | | | | | |
|-------------------------------------|-----------|------------------------|---------------|------------|--------|
| Showing 1 - 1 of 1 | | | | | |
| Site Name | Serial No | Installer Email | Address | Status | Action |
| ThiBR | ***** | ztdinstaller@*****.com | 123 Street Dr | Connecting | |
| <div>Delete</div> <div>Modify</div> | | | | | |

Hinweis

Eine Zero-Touch-Bereitstellung im Status “Ausstehende Aktivierung” kann optional zum Löschen oder Ändern gewählt werden, wenn die Informationen falsch sind. Wenn eine Site von der ausstehenden Aktivierungsseite gelöscht wird, kann sie auf der Registerkarte Neue Site bereitstellen bereitgestellt werden. Sobald Sie die Zweig-Site aus der ausstehenden Aktivierung löschen möchten, wird der Aktivierungslink, der an das Installationsprogramm gesendet wird, ungültig.

Wenn das Feld Seriennummer nicht vom SD-WAN-Administrator ausgefüllt wurde, zeigt das Statusfeld “Warten auf Installer” anstelle von “Verbinden” an.

23. Die nächste Reihe von Aktivitäten wird vom On-Site-Installer durchgeführt.
- a) Das Installationsprogramm überprüft das Postfach für die E-Mail-Adresse, die der SD-WAN-Administrator beim Bereitstellen der Site verwendet hat.



- b) Öffnen Sie zum Beispiel <https://sdwanzt.citrixnetworkapi.net> die Aktivierungs-URL der Zero-Touch-Bereitstellung in einem Internetbrowser-Fenster.
- c) Wenn der SD-WAN-Administrator die Seriennummer im Schritt Bereitstellungsstandort nicht vorausgefüllt hat, ist der Installer dafür verantwortlich, die Seriennummer auf der physischen Appliance zu finden und die Seriennummer manuell in die Aktivierungs-URL einzugeben, und klicken Sie dann auf die Schaltfläche **Aktivieren**.



- d) Wenn der Administrator die Seriennummerninformationen vorab ausfüllt, ist die Aktivierungs-URL bereits zum nächsten Schritt weitergegangen.



- e) Der Installer muss physisch vor Ort sein, um die folgenden Aktionen auszuführen:
- Kabel alle WAN- und LAN-Schnittstellen entsprechend der Topologie und Konfiguration, die in früheren Schritten erstellt wurden.
 - Kabel die Verwaltungsschnittstelle (MGMT, 0/1) im Segment des Netzwerks, das DHCP-IP-Adresse und Konnektivität zum Internet mit DNS und FQDN zur IP-Adressauflösung bereitstellt.
 - Stromkabel die SD-WAN-Appliance.
 - Schalten Sie den Netzschalter des Geräts ein.

Hinweis

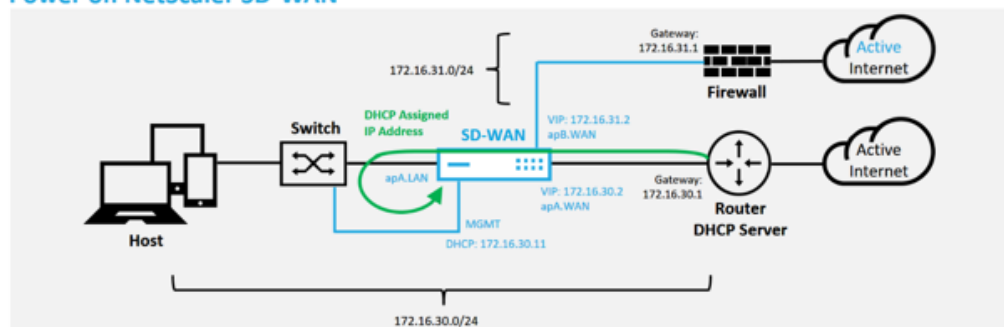
Die meisten Appliances schaltet sich automatisch ein, wenn das Netzkabel angeschlossen ist. Einige Appliance muss möglicherweise über den Netzschalter an der Vorderseite der Appliance eingeschaltet werden, andere haben möglicherweise den Netzschalter auf der Rückseite der Appliance. Einige Netzschalter müssen den Netzschalter gedrückt halten, bis das Gerät

hochgeschaltet wird.

24. Die nächste Reihe von Schritten wird mit Hilfe des Zero Touch Deployment Service automatisiert, erfordert jedoch, dass die folgenden Voraussetzungen zur Verfügung stehen.

- Die Zweigereinheit muss eingeschaltet sein
 - DHCP muss im vorhandenen Netzwerk verfügbar sein, um Verwaltungs- und DNS-IP-Adresse zuzuweisen
 - Jede DHCP-zugewiesene IP-Adresse erfordert Konnektivität zum Internet mit der Fähigkeit, FQDNs aufzulösen
 - Die IP-Zuweisung kann manuell konfiguriert werden, solange die anderen Voraussetzungen erfüllt sind
- a) Die Appliance erhält eine IP-Adresse vom Netzwerk DHCP-Server. In dieser Beispieltopologie wird dies über die umgangenen Datenschnittstellen einer werkseitigen Standardzustandsanwendung erreicht.

Power on NetScaler SD-WAN



- b) Wenn die Appliance die Webverwaltung und die DNS-IP-Adressen vom DHCP-Server des Unterlay-Netzwerkes abrufen, initiiert die Appliance den Zero Touch-Bereitstellungsdienst und lädt alle Softwareupdates für die Null-Touch-Bereitstellung herunter.
- c) Bei erfolgreicher Konnektivität mit dem Cloud Service für die Zero-Touch-Bereitstellung führt der Bereitstellungsprozess automatisch Folgendes aus:
- Laden Sie die Konfigurationsdatei herunter, die zuvor vom SD-WAN Center gespeichert ist
 - Anwenden der Konfiguration auf die lokale Appliance
 - Laden Sie eine temporäre Lizenzdatei mit 10 MB herunter und installieren Sie sie
 - Laden Sie bei Bedarf Softwareupdates herunter und installieren Sie sie
 - Aktivieren Sie den SD-WAN-Dienst



d) Eine weitere Bestätigung kann in der Web-Management-Oberfläche des SD-WAN Center erfolgen, das Zero Touch Deployment Menü zeigt erfolgreich aktivierte Appliances auf der Registerkarte **Aktivierungsverlauf an**.

| Dashboard | Fault | Monitoring | Configuration | Reporting | Administration |
|-----------------------|-------|------------|--|--------------------|--------------------|
| Network Discovery | | | Configuration / Zero Touch Deployment / Activation History | | |
| Network Configuration | | | Deploy New Site | Activation History | Pending Activation |
| Zero Touch Deployment | | | | | |
| Change Management | | | | | |
| Appliance Settings | | | | | |

Showing 1 - 1 of 1

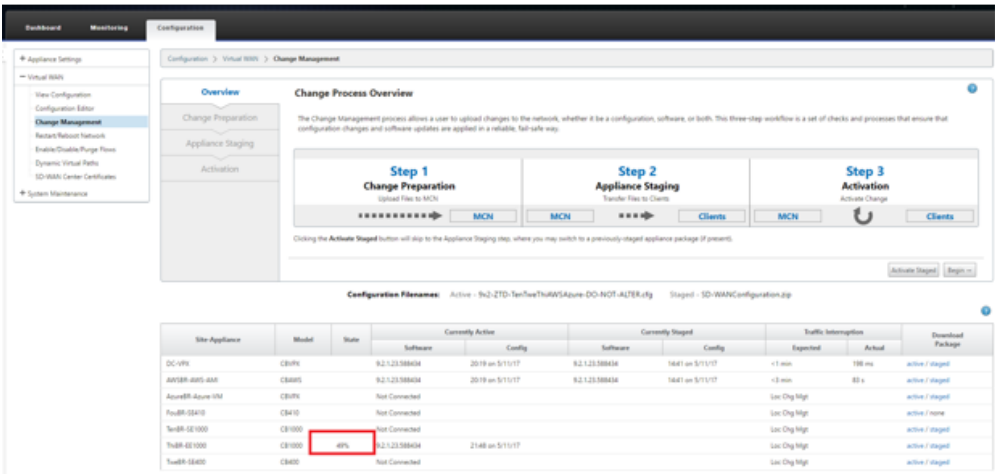
| Site Name | Serial No | Installer Email | Address | Status Details | Activation Date | Status | Action |
|-----------|-----------|--------------------------|---------------|---------------------|--------------------------|-----------|--------|
| ThBR | 3F6P82307 | ztdinstaller@outlook.com | 123 Street Dr | Appliance Activated | May 11 22:18:03 2017 UTC | Activated | |

e) Die virtuellen Pfade werden möglicherweise nicht sofort in einem verbundenen Zustand angezeigt, da das MCN der Konfiguration, die vom Clouddienst für die Zero-Touch-Bereitstellung übergeben wurde, nicht vertraut und meldet “Konfigurationsversion nicht übereinstimmen”im MCN-Dashboard.

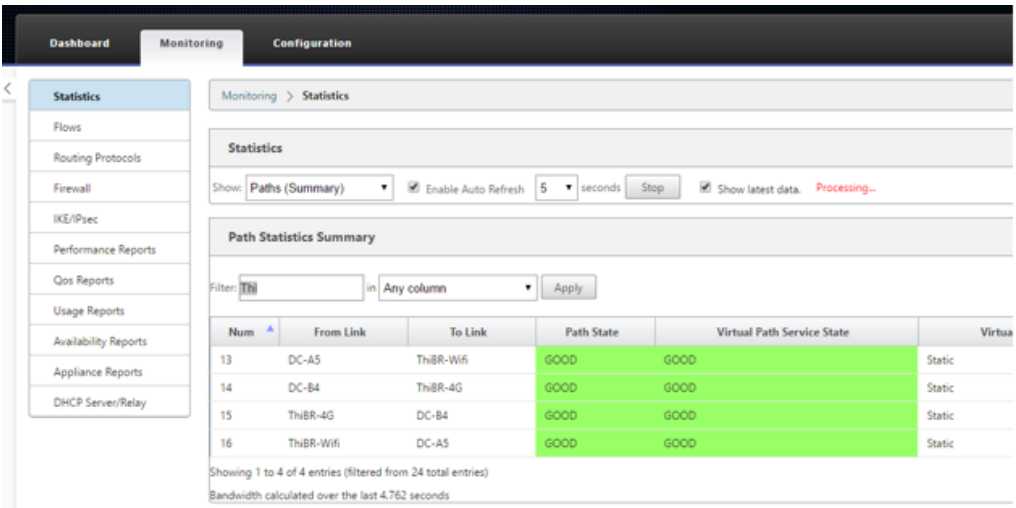
| Dashboard | Monitoring | Configuration |
|---|---|--|
| System Status | | |
| Name: | DC | |
| Model: | VPX | |
| Appliance Mode: | MCN | |
| Serial Number: | 1079975b-b067-ae77-1718-d7bdf0375a2b | |
| Management IP Address: | 172.16.10.51 | |
| Appliance Uptime: | 3 weeks, 5 days, 22 hours, 45 minutes, 35.2 seconds | |
| Service Uptime: | 1 weeks, 2 days, 20 hours, 58 minutes, 57.0 seconds | |
| Routing Domain Enabled: | Default_RoutingDomain | |
| Local Versions | | |
| Software Version: | 9.2.1.23.588434 | |
| Built On: | Apr 21 2017 at 05:23:29 | |
| Hardware Version: | VPX | |
| OS Partition Version: | 4.6 | |
| Virtual Path Service Status | | |
| Virtual Path DC-AWSBR: | | Uptime: 1 hours, 12 minutes, 48.0 seconds. |
| Virtual Path 'DC-AzureBR' is currently dead. | | |
| Virtual Path 'DC-ThBR' is currently dead. | | |
| Virtual Path 'DC-ThBR' is currently dead (Configuration version mismatch) | | |
| Virtual Path 'DC-FouBR' is currently dead. | | |

f) Die Konfiguration wird erneut an die neu installierte Zweigstelleneinheit übermit-

telt und der Status wird auf der Seite **MCN > Konfiguration > Virtuelles WAN > Änderungsverwaltung** überwacht (dieser Vorgang kann einige Minuten dauern).



g) Der SD-WAN-Administrator kann die Head-End-MCN-Webverwaltungsseite für die etablierten virtuellen Pfade der Remotesite überwachen.



h) SD-WAN Center kann auch verwendet werden, um die DHCP-zugewiesene IP-Adresse der Vor-Ort-Appliance auf der Seite **Konfiguration > Netzwerkerkennung > Inventar und Status** zu identifizieren.

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Network Discovery

Network Configuration

Zero Touch Deployment

Change Management

Appliance Settings

Configuration / Network Discovery / Inventory And Status

SSL Certificate

Discovery Settings

Inventory And Status

Showing 1 - 7 of 7

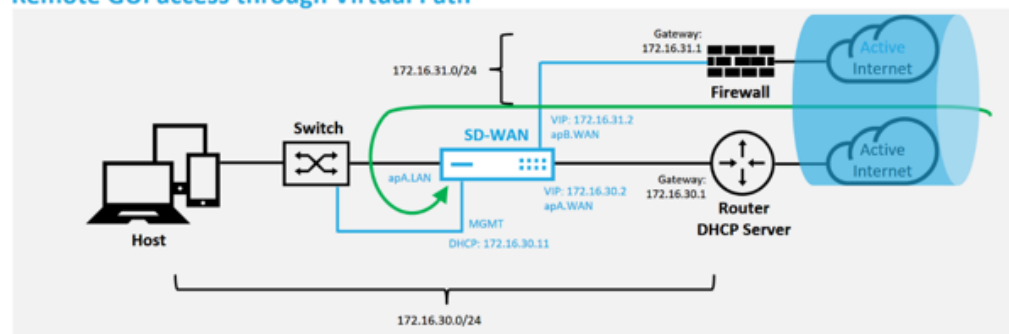
Search

| <input checked="" type="checkbox"/> | Poll | State | Name | MGT IP Address | Model | Serial Number | Software | Registry Timestamp | Last Successful Poll | Latest Record | Download |
|-------------------------------------|------|---------------|---------|----------------|-------|--------------------------------------|------------------|--------------------|----------------------|----------------|----------|
| <input checked="" type="checkbox"/> | | State in Sync | DC | 172.16.10.51 | cdvpx | 1079975b-b067-ae77-171b-d70df0375a2b | R9_2_1_23_588434 | 1494551952 | 05/11/17 19:02 | 05/11/17 19:01 | |
| <input checked="" type="checkbox"/> | | Unknown | AWSBR | | | | | | | | |
| <input checked="" type="checkbox"/> | | Not Reachable | AzureBR | 192.168.202.4 | | | | | | | |
| <input checked="" type="checkbox"/> | | Unknown | FouBR | | | | | | | | |
| <input checked="" type="checkbox"/> | | Not Reachable | TenBR | 192.168.10.11 | | | | | | | |
| <input checked="" type="checkbox"/> | | Not Reachable | ThnBR | 192.168.30.11 | | | | | | | |
| <input checked="" type="checkbox"/> | | Unknown | TweBR | | | | | | | | |

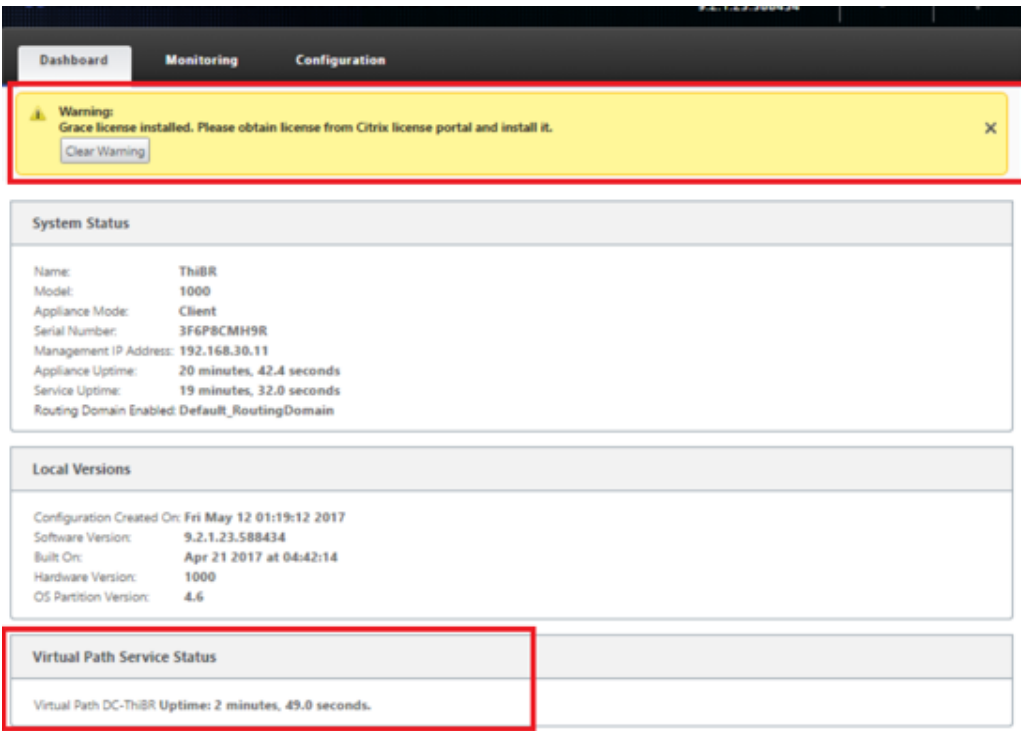
Apply

- i) Zu diesem Zeitpunkt kann der SD-WAN-Netzwerkadministrator mithilfe des SD-WAN-Overlay-Netzwerks auf die Appliance vor Ort Zugriff auf die Appliance vor Ort erhalten.

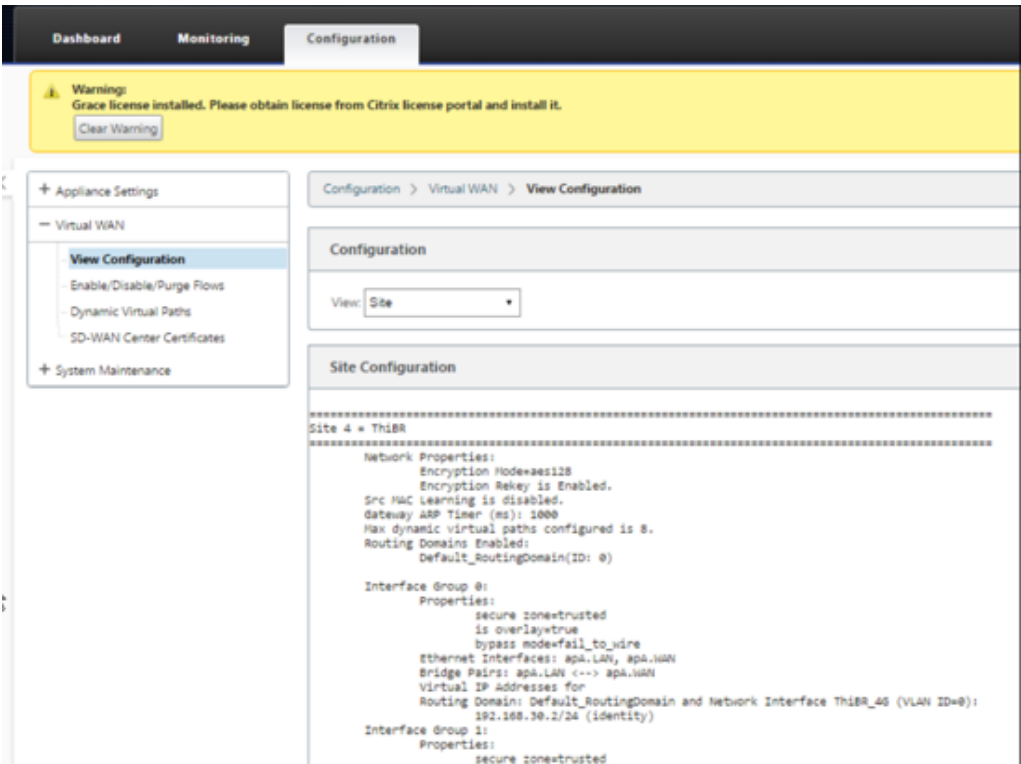
Remote GUI access through Virtual Path



- j) Der Webverwaltungszugriff auf die Remotestandort-Appliance zeigt an, dass die Appliance mit einer temporären Gnadenlizenz von 10 Mbit/s installiert wurde, wodurch der Status des Virtual Path Service als aktiv gemeldet werden kann.

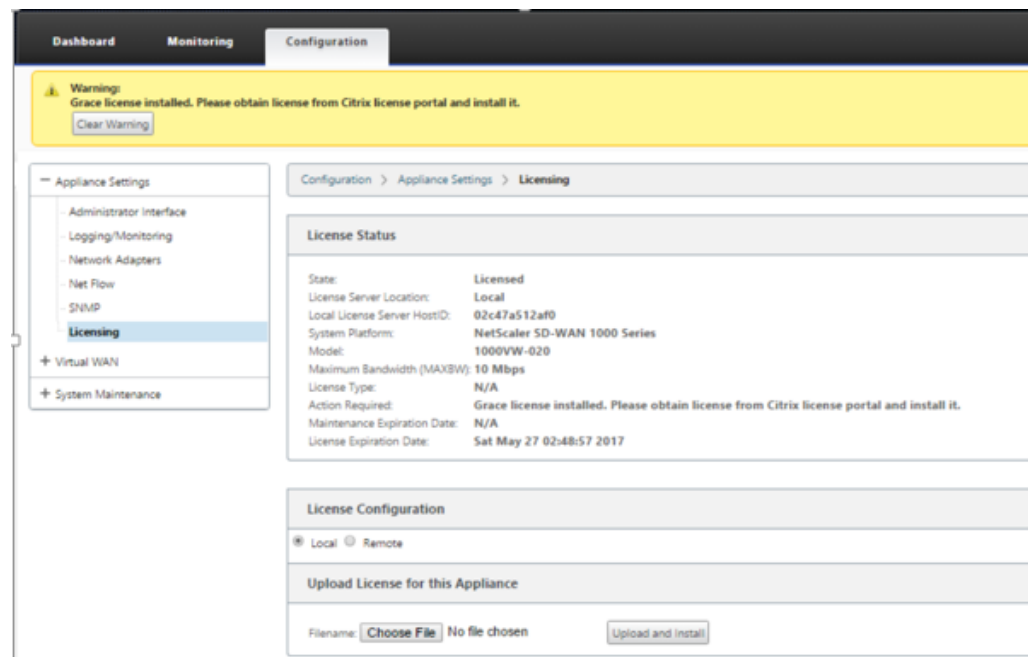


k) Die Appliance-Konfiguration kann über die Seite **Konfiguration > Virtuelles WAN > Konfiguration anzeigen** validiert werden.



l) Die Appliance-Lizenzdatei kann auf der Seite **Konfiguration > Appliance-**

Einstellungen > Lizenzierung auf eine permanente Lizenz aktualisiert werden.



Nach dem Hochladen und Installieren der permanenten Lizenzdatei verschwindet das Warnbanner Grace License und während des Lizenzinstallationsvorgangs tritt kein Verlust der Konnektivität mit dem Remotestandort auf (Null Pings werden gelöscht).

On-Prem Zero-Touch

May 10, 2021

Anweisungen zum Bereitstellen einer SD-WAN-Appliance mit Zero Touch Service finden Sie im Thema; [Konfigurieren des Zero Touch-Bereitstellungsdiensts](#).

AWS

May 10, 2021

In den folgenden Abschnitten wird beschrieben, wie ZTD in einer AWS-Umgebung bereitgestellt wird.

Bereitstellung in AWS:

Mit SD-WAN Version 9.3 wurden die Null-Touch-Bereitstellungsfunktionen auf Cloud-Instanzen erweitert. Das Verfahren zum Bereitstellen von Zero Touch-Bereitstellungsprozess vier Cloud-Instanzen unterscheidet sich geringfügig von der Appliance-Bereitstellung für den Zero Touch-Dienst.

1. Aktualisieren Sie die Konfiguration, um mithilfe der SD-WAN-Center-Netzwerkconfiguration einen neuen Remote-Standort mit einem ZTD-fähigen SD-WAN-Cloud-Gerät hinzuzufügen.

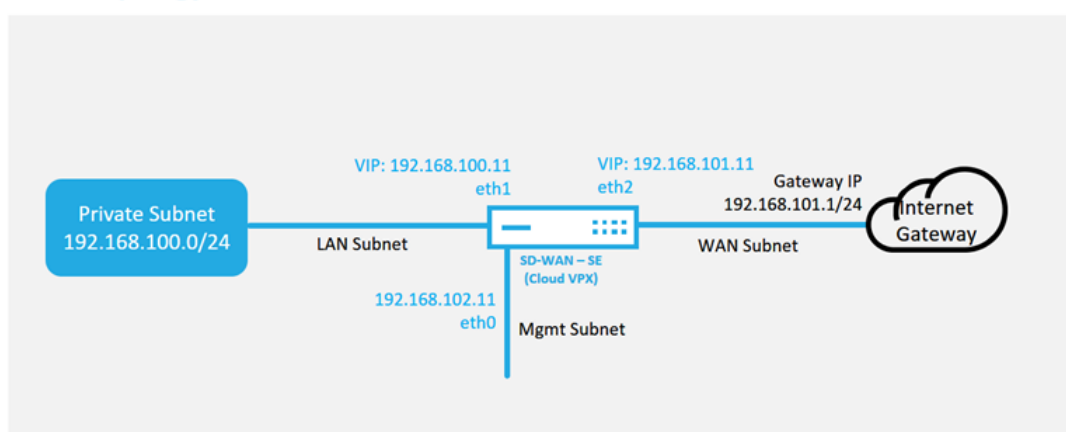
Wenn die SD-WAN-Konfiguration nicht mit der SD-WAN-Center-Netzwerkconfiguration erstellt wurde, importieren Sie die aktive Konfiguration aus dem MCN und beginnen Sie mit der Änderung der Konfiguration mit dem SD-WAN Center. Für die Zero Touch-Bereitstellung muss der SD-WAN-Administrator die Konfiguration mithilfe des SD-WAN-Centers erstellen. Das folgende Verfahren sollte verwendet werden, um einen neuen Cloud-Knoten hinzuzufügen, der für die Null-Touch-Bereitstellung vorgesehen ist.

- a) Entwerfen Sie die neue Site für die SD-WAN-Cloud-Bereitstellung, indem Sie zunächst die Details der neuen Site skizzieren (z. B. die VPX-Größe, die Verwendung von Schnittstellen-gruppen, virtuelle IP-Adressen, WAN-Link (s) mit Bandbreite und deren jeweiligen Gateways).

Hinweis

- In der Cloud bereitgestellte SD-WAN-Instanzen müssen im Edge/Gateway -Modus bereitgestellt werden.
- Die Vorlage für die Cloud-Instanz ist auf drei Schnittstellen beschränkt: Management, LAN und WAN (in dieser Reihenfolge).
- Die verfügbaren Cloud-Vorlagen für SD-WAN VPX sind derzeit hart festgelegt, um die #. #. #.11 IP-Adresse der verfügbaren Subnetze in der VPC zu erhalten.

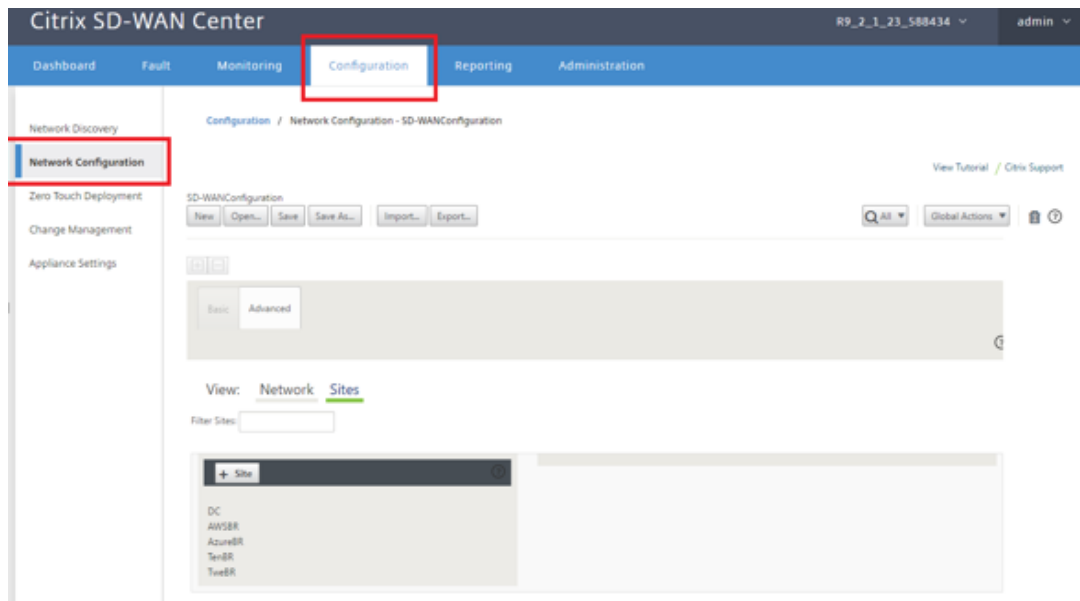
Cloud Topology with NetScaler SD-WAN



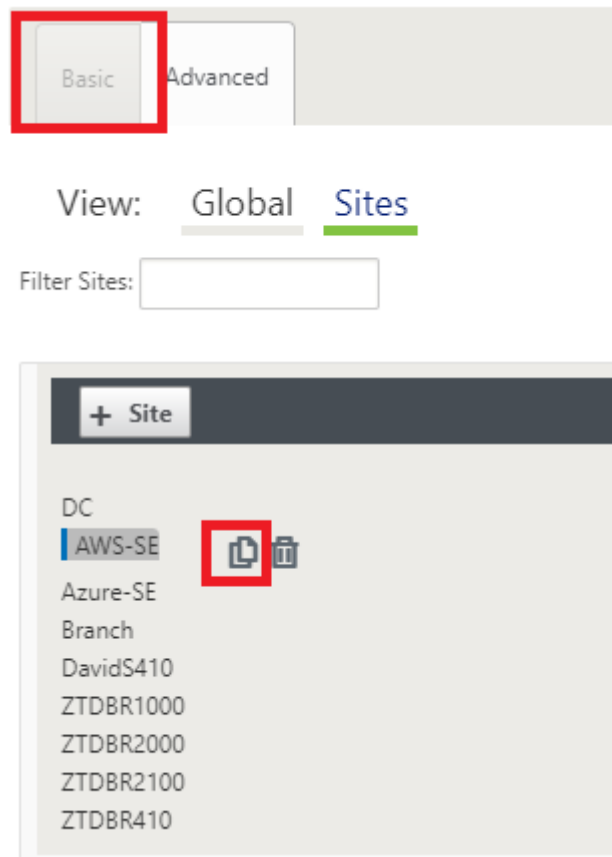
Dies ist ein Beispiel für die Bereitstellung einer SD-WAN-Cloud bereitgestellten Site. Das Citrix SD-WAN Gerät wird als Edge-Gerät bereitgestellt, das eine einzelne Internet-WAN-Verbindung in diesem Cloud-Netzwerk bedient. Remote-Standorte können mehrere un-

terschiedliche Internet-WAN-Verbindungen nutzen, die sich mit demselben Internet Gateway für die Cloud verbinden. Dadurch können Ausfallsicherheit und aggregierte Bandbreitenkonnektivität von jedem SD-WAN-Bereitstellungsstandort in die Cloud-Infrastruktur bereitgestellt werden. Dies bietet kostengünstige und äußerst zuverlässige Konnektivität zur Cloud.

- b) Öffnen Sie die Web-Management-Schnittstelle des SD-WAN Center, und navigieren Sie zur Seite **Konfiguration > Netzwerkkonfiguration**.



- c) Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration aus dem MCN.
- d) Navigieren Sie zur Registerkarte Basic, um eine neue Website zu erstellen.
- e) Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.
- f) Erstellen Sie schnell die Konfiguration für die neue Cloud-Site, indem Sie die Clone-Funktion einer vorhandenen Site verwenden oder manuell eine neue Site erstellen.



- g) Füllen Sie alle erforderlichen Felder aus der zuvor für diese neue Cloud-Site entwickelten Topologie aus.

Beachten Sie, dass die für Cloud-ZTD-Bereitstellungen verfügbare Vorlage für die Verwendung der #. #.11 IP-Adresse für die Mgmt, LAN- und WAN-Subnetze schwierig ist. Wenn die Konfiguration nicht so eingestellt ist, dass sie mit der erwarteten IP-Adresse .11 für jede Schnittstelle übereinstimmt, kann das Gerät nicht ordnungsgemäß ARP zu den Cloud-Umgebungsgateways und IP-Konnektivität zum virtuellen Pfad des MCN einrichten.

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name: ! Appliance Name: Secure Key:

Routing Domains

| Name | Enable | Default |
|-----------------------|-------------------------------------|-------------------------------------|
| Default_RoutingDomain | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Virtual Interfaces

| Name | VLAN ID | DHCP |
|---------|---------|--------------------------|
| E1Vlan0 | 0 | <input type="checkbox"/> |
| E2Vlan0 | 0 | <input type="checkbox"/> |

Virtual IP Addresses

| Include | Virtual Interface | Virtual IP Address/Prefix |
|-------------------------------------|-------------------|---|
| <input checked="" type="checkbox"/> | E1Vlan0 | 192.168.100.11/2 ! |
| <input checked="" type="checkbox"/> | E2Vlan0 | 192.168.101.11/2 ! |

Local Routes

| Include | Network Address | Routing Domain | Gateway |
|---------|-----------------|----------------|---------|
|---------|-----------------|----------------|---------|

WAN Links

| Include Link | WAN Link | Access Type |
|-------------------------------------|---|-----------------|
| <input checked="" type="checkbox"/> | AWS-INET ! | Public Internet |

Access Interfaces

| Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway |
|-------------------------------------|------------------|-------------------|---|--|
| <input checked="" type="checkbox"/> | AWS-INET-AI-1 | E2Vlan0 | 192.168.101.11 ! | 192.168.101.1 ! |

h) Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen** der Site, und überprüfen Sie, ob das SD-WAN-Modell korrekt ausgewählt ist, was den Null-Touch-Dienst unterstützen würde.

Edit Site Settings

Appliance Name:

☐ Enable Site as Intermediate Node

☐ Enable Dynamic Virtual Paths

Model:

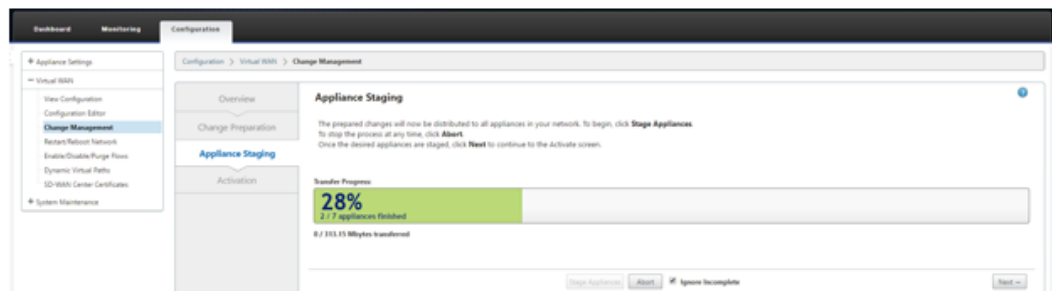
Appliance: AWS-SE-CBVPX

Interfaces:

Ethernet Port 2:
VLANs: 0 (192.168.101.11/24)

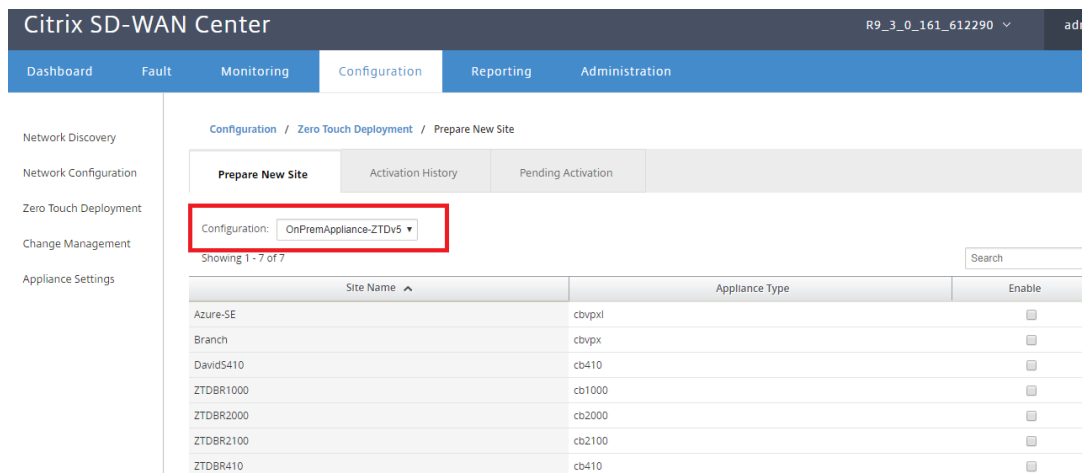
i) Speichern Sie die neue Konfiguration im SD-WAN Center, und verwenden Sie den Export in den **Change Management-Posteingang**, um die Konfiguration mithilfe von Change Management zu übertragen.

- j) Befolgen Sie das Change Management-Verfahren, um für die neue Konfiguration das Staging richtig durchzuführen, wodurch die vorhandenen SD-WAN-Geräte über den neuen Standort informiert werden, der per Zero Touch bereitgestellt werden soll. Sie müssen die Option *Unvollständig ignorieren* verwenden, um den Versuch zu überspringen, die Konfiguration an die neue Site zu übertragen, die muss immer noch den ZTD-Workflow durchlaufen.



2. Navigieren Sie zurück zur Seite Zero Touch Deployment von SD-WAN Center. Wenn die neue aktive Konfiguration ausgeführt wird, steht die neue Site für die Bereitstellung zur Verfügung.

- a) Wählen Sie auf der Seite “Zero Touch Deployment” unter der Registerkarte **Neue Site bereitstellen** die ausgeführte Netzwerkkonfigurationsdatei aus.
- b) Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit nicht bereitgestellten Citrix SD-WAN Geräten angezeigt, die für keine Berührung unterstützt werden.



- c) Wählen Sie die Ziel-Cloud-Site aus, die Sie mit dem Zero Touch-Dienst bereitstellen möchten, klicken Sie auf **Aktivieren** und dann auf **Provisioning und Bereitstellen**.

| Site Name ^ | Appliance Type | Enable |
|-------------|----------------|-------------------------------------|
| AWS-SE | cbvpxl | <input checked="" type="checkbox"/> |
| Azure-SE | cbvpxl | <input type="checkbox"/> |
| Branch | cbvpx | <input type="checkbox"/> |
| DavidS410 | cb410 | <input type="checkbox"/> |
| ZTDBR1000 | cb1000 | <input type="checkbox"/> |
| ZTDBR2000 | cb2000 | <input type="checkbox"/> |
| ZTDBR2100 | cb2100 | <input type="checkbox"/> |
| ZTDBR410 | cb410 | <input type="checkbox"/> |

- d) Es erscheint ein Popup-Fenster, in dem der Citrix SD-WAN Admin die Bereitstellung für Zero Touch initiieren kann.

Geben Sie eine E-Mail-Adresse ein, an die die Aktivierungs-URL übermittelt werden kann, und wählen Sie den **Bereitstellungstyp** für die gewünschte Cloud aus.

Provision and Deploy ✕

Site Name:
AWS-SE

Installer Email:
ztdinstaller@outlook.com

Provision Type
AWS ▼

Next

- e) Nachdem Sie auf **Weiter** geklickt haben und die entsprechende Region und Instanzgröße gewählt, füllen Sie die Felder SSH-Schlüsselname und Rollen-ARN entsprechend aus.

Provision and Deploy AWS ✕

AWS Region
US West (Oregon) ▼

AWS Instance Size
m4.2xlarge ▼

SSH Key Name:
aws-ztd ⓘ

Role ARN:
arn:aws:iam::*****:role/ZeroTouch ⓘ

Back **Deploy**

Hinweis

Nutzen Sie die Hilfe-Links, um Anleitungen zum Einrichten des SSH-Schlüssels und der Rollen-ARN für das Cloud-Konto zu erhalten. Stellen Sie außerdem sicher, dass die ausgewählte Region mit dem übereinstimmt, was auf dem Konto verfügbar ist

und dass die ausgewählte Instanzgröße VPX oder VPXL als ausgewähltes Modell in der SD-WAN-Konfiguration übereinstimmt.

- f) Klicken Sie auf **Deploy** und lösen Sie das SD-WAN Center aus, das zuvor beim ZTD Cloud Service registriert wurde, um die Konfiguration dieser Site so freizugeben, dass sie temporär im ZTD Cloud Service gespeichert ist.
- g) Navigieren Sie zur Registerkarte **Ausstehende Aktivierung**, um zu bestätigen, dass die Standortinformationen erfolgreich ausgefüllt wurden und in einen Bereitstellungsstatus versetzt wurden.

Configuration / Zero Touch Deployment / Pending Activation

| | | | |
|------------------|--------------------|--------------------|--|
| Prepare New Site | Activation History | Pending Activation | |
|------------------|--------------------|--------------------|--|

Showing 1 - 1 of 1 Search

| Site Name ^ | Serial No | Installer Email | Address | Status | Action |
|-------------|--------------------------------------|--------------------------|------------------------|--------------|--------|
| AWS-SE | 2E20EFCF-1A26-42DC-86D0-5624FD27C37F | ztdinstaller@outlook.com | AWS - US West (Oregon) | Provisioning | |

Delete Modify

3. Starten Sie den Zero Touch-Bereitstellungsprozess als Cloud-Administrator.

- a) Der Installer muss das Postfach der E-Mail-Adresse überprüfen, die der SD-WAN-Administrator bei der Bereitstellung der Site verwendet hat.

NetScaler SD-WAN Cloud Service Activation Link @AWS-SE



Citrix Zero Touch Service <sdwanservice@citrix.com>

Today, 11:01 AM

You 3



Reply all | v

Inbox

NetScaler SD-WAN Appliance Activation InformationTo begin the process of activating your appliance, [click here](#) .

(Or paste this URL into your browser

<https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate?activationcode=67940818-abb8-47f0-9f17-9a20a3955d57>)**Site Name** AWS-SE**Address** AWS - US West (Oregon)**Additional Notes**

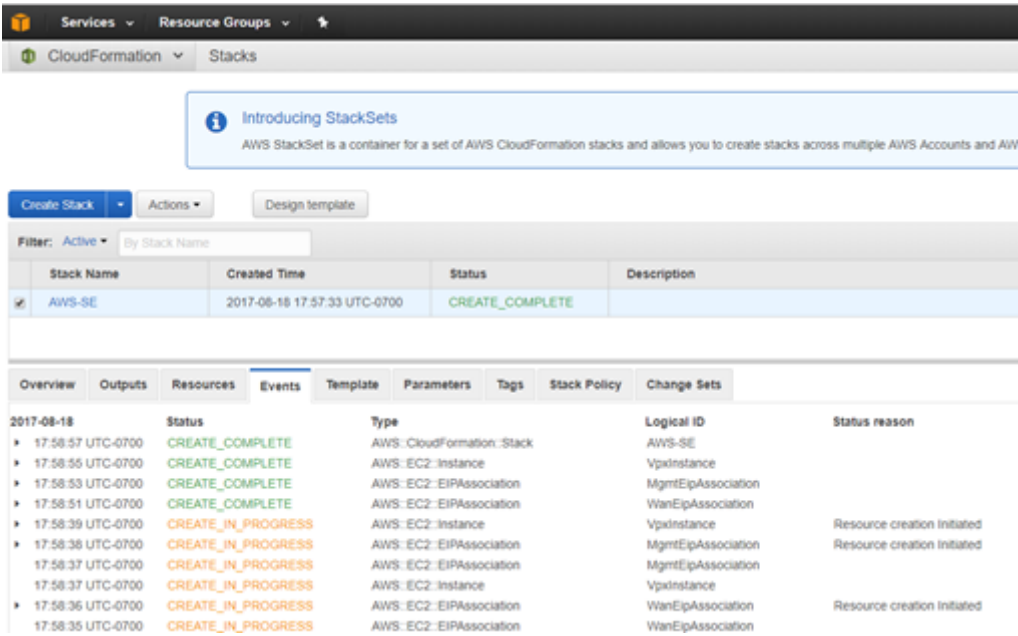
The NetScaler SD-WAN Team

*** This is an automatically generated email, please do not reply ***

- b) Öffnen Sie die Aktivierungs-URL, die in der E-Mail in einem Internet-Browser-Fenster gefunden wurde (Beispiel;<https://sdwanzt.citrixnetworkapi.net>).
- c) Wenn der SSH-Schlüssel und die Rollen-ARN ordnungsgemäß eingegeben werden, beginnt der Zero Touch-Bereitstellungsdienst sofort mit der Bereitstellung der SD-WAN-Instanz. Andernfalls werden Verbindungsfehler sofort angezeigt.



d) Zur weiteren Fehlerbehebung in der AWS-Konsole kann der Cloud Formation-Dienst zum Abfangen von Ereignissen verwendet werden, die während des Bereitstellungsvorgangs auftreten.



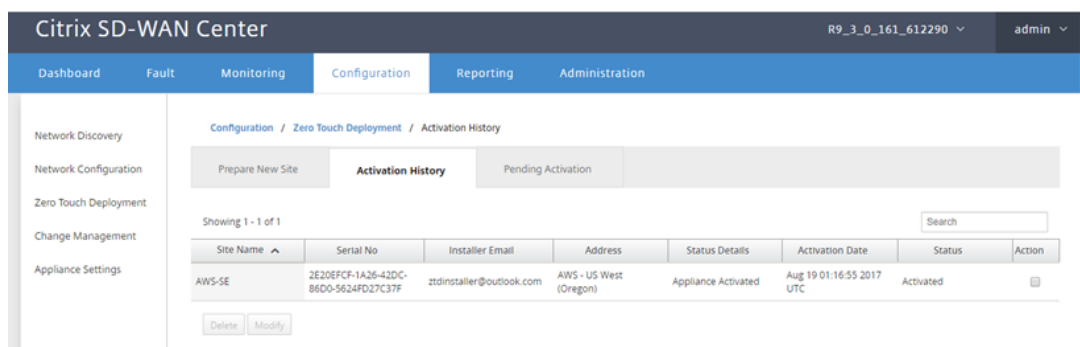
e) Erlauben Sie den Bereitstellungsprozess ca. 8-10 Minuten und die Aktivierung weiterer ~ 3-5 Minuten, um vollständig abzuschließen.

f) Bei erfolgreicher Konnektivität der SD-WAN-Cloud-Instanz mit dem ZTD Cloud Service führt der Dienst automatisch Folgendes aus:

- Laden Sie die standortspezifische Konfigurationsdatei herunter, die zuvor vom SD-WAN-Center gespeichert wurde.
- Anwenden der Konfiguration auf die lokale Instanz
- Laden Sie eine temporäre Lizenzdatei mit 10 MB herunter und installieren Sie sie
- Herunterladen und Installieren von Softwareupdates bei Bedarf
- Aktivieren Sie den SD-WAN-Dienst



g) Eine weitere Bestätigung kann über die Webverwaltungsschnittstelle des SD-WAN Centers erfolgen. Im Menü “Zero Touch Deployment” werden erfolgreich aktivierte Appliances auf der Registerkarte **Aktivierungsverlauf** angezeigt.



- h) Die virtuellen Pfade werden möglicherweise nicht sofort in einem verbundenen Zustand angezeigt. Dies liegt daran, dass der MCN der Konfiguration nicht vertraut, die vom ZTD Cloud Service übergeben wurde, und meldet, dass die *Konfigurationsversion im MCN Dashboard nicht übereinstimmt*.

The screenshot displays the MCN Dashboard with three tabs: Dashboard, Monitoring, and Configuration. The 'Dashboard' tab is active, showing the following sections:

- System Status:**
 - Name: DC
 - Model: VPX
 - Appliance Mode: MCN
 - Serial Number: b536a38c-5f48-b720-4f8d-b3f50b23f69f
 - Management IP Address: 172.16.10.30
 - Appliance Uptime: 1 weeks, 2 days, 3 hours, 50 minutes, 18.3 seconds
 - Service Uptime: 1 weeks, 2 days, 3 hours, 42 minutes, 19.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions:**
 - Software Version: 9.3.0.161.612290
 - Built On: Aug 8 2017 at 14:45:01
 - Hardware Version: VPX
 - OS Partition Version: 4.6
- Virtual Path Service Status:**
 - Virtual Path DC-Branch: Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.
 - Virtual Path 'DC-DavidS410' is currently dead.
 - Virtual Path DC-ZTDBR1000: Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.
 - Virtual Path 'DC-ZTDBR2000' is currently dead.
 - Virtual Path 'DC-ZTDBR2100' is currently dead.
 - Virtual Path 'DC-ZTDBR410' is currently dead.
 - Virtual Path 'DC-AWS-SE' is currently dead (Configuration version mismatch)** (highlighted with a red box)
 - Virtual Path 'DC-Azure-SE' is currently dead.

- i) Die Konfiguration wird automatisch an die neu installierte Zweigstellen-Appliance weitergeleitet. Der Status dieser Konfiguration kann auf der Seite **MCN > Konfiguration > Virtuelles WAN > Änderungsverwaltung** überwacht werden (abhängig von der Konnektivität wird diese -Prozess kann einige Minuten dauern).

DashboardMonitoringConfiguration

+ Appliance Settings

- Virtual WAN

View Configuration

Configuration Editor

Change Management

Change Management Settings

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

+ System Maintenance

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Change Process Overview

The Change Management process allows a user to upload changes to the network, whether it processes that ensure that configuration changes and software updates are applied in a reliable

Step 1

Change Preparation

Upload Files to MCN

MCN

Step 2

Appliance

Transfer Files

MCN

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a pr

Configuration Filenames: Active - OnPremAppliance-ZTDv5.zip Stag

Search

| Site-Appliance | Model | State | Currently Active | | Current |
|-------------------------|--------|---------------|------------------|------------------|------------------|
| | | | Software | Config | Software |
| DC-DC_SDWAN | CBVPX | | 9.3.0.161.612290 | 10:55 on 8/18/17 | 9.3.0.161.612290 |
| AWS-SE-AWS-SE-CBVPX | CBVPXL | 6% | 9.3.0.161.612290 | | |
| Azure-SE-Azure-SE-CBVPX | CBVPXL | Not Connected | | | |
| Branch-Branch_SDWAN | CBVPX | | 9.3.0.161.612290 | 10:55 on 8/18/17 | 9.3.0.161.612290 |

j) Der SD-WAN-Administrator kann die Head-End-MCN-Webverwaltungsseite für die etablierten virtuellen Pfade der neu hinzugefügten Cloud-Site überwachen.

DashboardMonitoringConfiguration

Statistics

Flows

Routing Protocols

Firewall

IKL/Ipsec

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

Monitoring > Statistics

Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Start Show latest data.

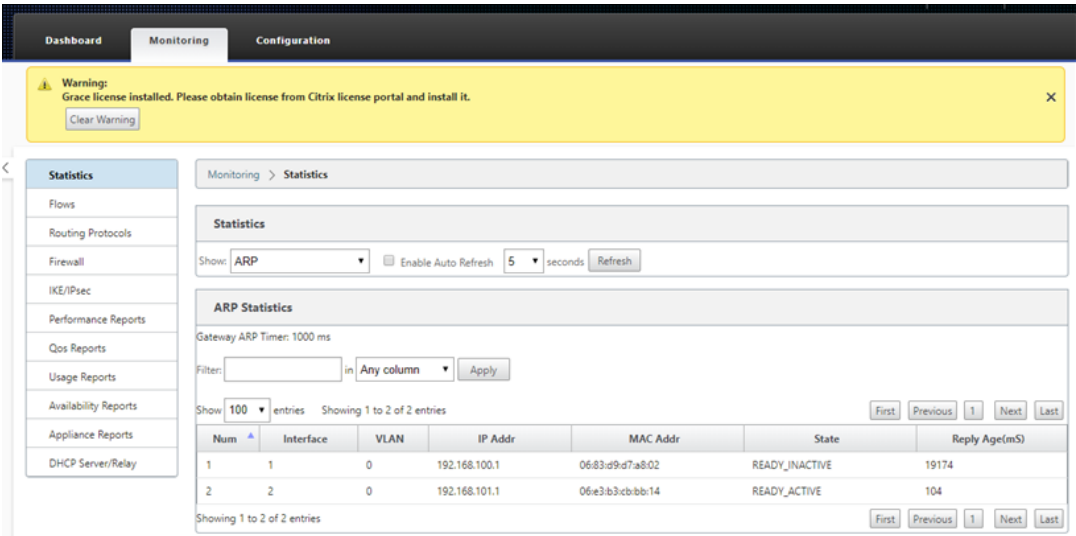
Path Statistics Summary

Filter: AWS in Any column Apply

| Num | From Link | To Link | Path State | Virtual Path Service State | Virtual Path Service Type | BOWT | Jitter (mS) | Loss % | kbps | Congestion |
|-----|-----------|----------|------------|----------------------------|---------------------------|------|-------------|--------|-------|------------|
| 27 | DC-INET | AWS-INET | GOOD | GOOD | Static | 26 | 2 | 0.00 | 16.20 | NO |
| 28 | AWS-INET | DC-INET | GOOD | GOOD | Static | 26 | 2 | 0.00 | 15.13 | NO |

Showing 1 to 2 of 2 entries (filtered from 30 total entries)
Bandwidth calculated over the last 0.956 seconds

k) Wenn eine Fehlerbehebung erforderlich ist, öffnen Sie die Benutzeroberfläche von SD-WAN-Instanzen mit der öffentlichen IP-Adresse, die von der Cloud-Umgebung während der Bereitstellung zugewiesen wurde, und verwenden Sie die ARP-Tabelle auf der Seite **Überwachung > Statistiken**, um Probleme zu identifizieren, die mit den erwarteten Gateways verbunden sind, oder verwenden Sie die Optionen zur Verfolgung von Routen und Paketerfassung in der Diagnose.



Azure

May 10, 2021

Das Verfahren zum Bereitstellen von Zero Touch-Bereitstellungsprozess für Cloud-Instanzen unterscheidet sich geringfügig von der Appliance-Bereitstellung für Zero Touch-Dienst.

Aktualisieren Sie die Konfiguration, um eine neue Remote-Site mit einem ZTD-fähigen SD-WAN-Cloud-Gerät mit SD-WAN Center-Netzwerkkonfiguration hinzuzufügen

Wenn die SD-WAN-Konfiguration nicht mit der SD-WAN-Center-Netzwerkkonfiguration erstellt wurde, importieren Sie die aktive Konfiguration aus dem MCN und beginnen Sie mit der Änderung der Konfiguration mit dem SD-WAN Center. Für die Zero Touch-Bereitstellung muss der SD-WAN-Administrator die Konfiguration mithilfe des SD-WAN-Centers erstellen. Das folgende Verfahren sollte verwendet werden, um einen neuen Cloud-Knoten hinzuzufügen, der für die Null-Touch-Bereitstellung vorgesehen ist.

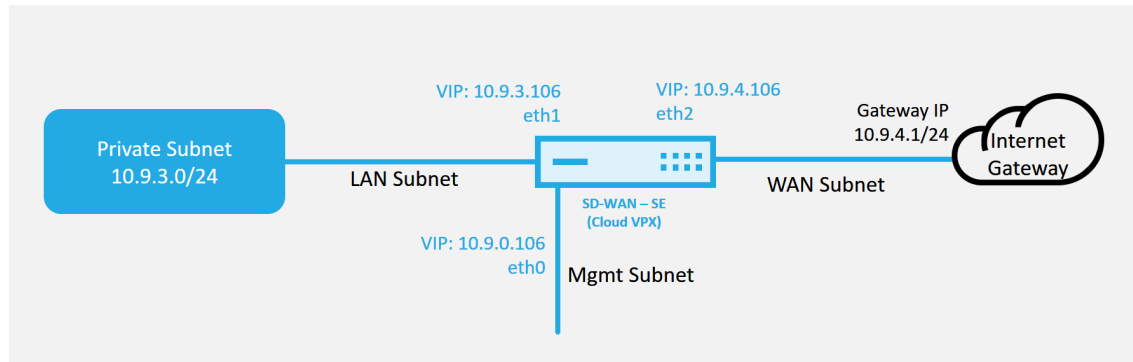
1. Entwerfen Sie die neue Site für die SD-WAN-Cloud-Bereitstellung, indem Sie zunächst die Details der neuen Site skizzieren (z. B. die VPX-Größe, die Verwendung von Schnittstellengruppen, virtuelle IP-Adressen, WAN-Link (s) mit Bandbreite und deren jeweiligen Gateways).

Hinweis

- In der Cloud bereitgestellte SD-WAN-Instanzen müssen im Edge/Gateway -Modus bereitgestellt werden.
- Die Vorlage für die Cloud-Instanz ist auf drei Schnittstellen beschränkt: Management, LAN und WAN (in dieser Reihenfolge).

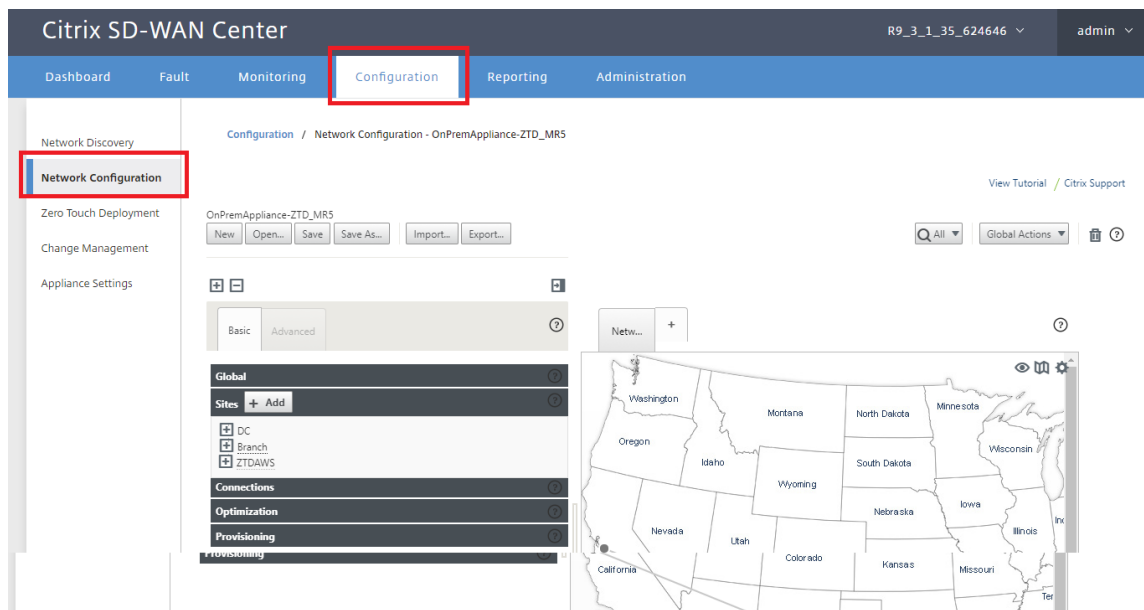
- Die verfügbaren Azure-Cloudvorlagen für SD-WAN VPX sind derzeit hart festgelegt, um die 10.9.4.106 IP für das WAN, 10.9.3.106 IP für das LAN und 10.9.0.16 IP für die Verwaltungsadresse zu erhalten. Die SD-WAN-Konfiguration für den Azure-Knoten für Zero Touch muss mit diesem Layout übereinstimmen.
- Der Azure-Site-Name in der Konfiguration muss alle Kleinbuchstaben ohne Sonderzeichen enthalten (z. B. ztdazure).

Azure Cloud Topology with NetScaler SD-WAN

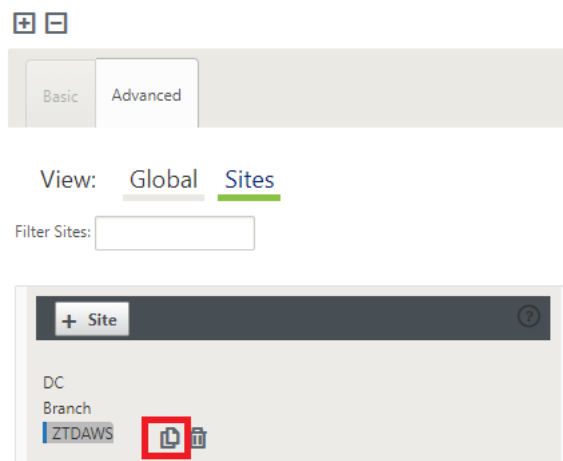


Dies ist ein Beispiel für die Bereitstellung einer SD-WAN-Cloud bereitgestellten Site. Das Citrix SD-WAN Gerät wird als Edge-Gerät bereitgestellt, das eine einzelne Internet-WAN-Verbindung in diesem Cloud-Netzwerk bedient. Remote-Standorte können mehrere unterschiedliche Internet-WAN-Verbindungen nutzen, die sich mit demselben Internet Gateway für die Cloud verbinden. Dadurch können Ausfallsicherheit und aggregierte Bandbreitenkonnektivität von jedem SD-WAN-Bereitstellungsstandort in die Cloud-Infrastruktur bereitgestellt werden. Dies bietet kostengünstige und äußerst zuverlässige Konnektivität zur Cloud.

2. Öffnen Sie die Web-Management-Schnittstelle des SD-WAN Center, und navigieren Sie zur Seite **Konfiguration > Netzwerkkonfiguration**.



3. Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration aus dem MCN.
4. Navigieren Sie zur Registerkarte Basic, um eine neue Website zu erstellen.
5. Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.
6. Erstellen Sie schnell die Konfiguration für die neue Cloud-Site, indem Sie die Clone-Funktion einer vorhandenen Site verwenden oder manuell eine neue Site erstellen.



7. Füllen Sie alle erforderlichen Felder aus der zuvor für diese neue Cloud-Site entwickelten Topologie aus.

Beachten Sie, dass die für Azure Cloud ZTD-Bereitstellungen verfügbare Vorlage derzeit fest festgelegt ist, um die 10.9.4.106 IP für das WAN, 10.9.3.106 IP für das LAN und 10.9.0.16 IP für die Verwaltungsadresse zu erhalten. Wenn die Konfiguration nicht so eingestellt ist, dass sie mit der erwarteten VIP-Adresse für jede Schnittstelle übereinstimmt, kann das Gerät nicht ordnungs-

gemäß ARP für die Cloud-Umgebung Gateways und IP-Konnektivität zum virtuellen Pfad des MCN einrichten.

Es wird importiert, dass der Websitenamen mit dem übereinstimmt, was Azure erwartet. Der Website-Name muss in Kleinbuchstaben, mindestens 6 Zeichen, ohne Sonderzeichen, er muss dem folgenden regulären Ausdruck bestätigen `^[a-z][a-z0-9-]{1,61}[a-z0-9]$`.

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name:
ztdazure

Appliance Name:
azure-CBVPXL

Secure Key:
f6796bba4d1c8da2

Routing Domains

| Name | Enable | Default |
|-----------------------|-------------------------------------|-------------------------------------|
| Default_RoutingDomain | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Virtual Interfaces

| Name | VLAN ID | DHCP |
|---------|---------|--------------------------|
| E1Vlan0 | 0 | <input type="checkbox"/> |
| E2Vlan0 | 0 | <input type="checkbox"/> |

Virtual IP Addresses

| Include | Virtual Interface | Virtual IP Address/Prefix |
|-------------------------------------|-------------------|---------------------------|
| <input checked="" type="checkbox"/> | E1Vlan0 | 10.9.3.106/24 |
| <input checked="" type="checkbox"/> | E2Vlan0 | 10.9.4.106/24 |

Local Routes

| Include | Network Address | Routing Domain | Gateway |
|---------|-----------------|----------------|---------|
|---------|-----------------|----------------|---------|

WAN Links

| Include Link | WAN Link | Access Type |
|-------------------------------------|------------|-----------------|
| <input checked="" type="checkbox"/> | Azure-INET | Public Internet |

Access Interfaces

| Include Interface | Access Interface | Virtual Interface | Virtual IP Address | Gateway |
|-------------------------------------|------------------|-------------------|--------------------|----------|
| <input checked="" type="checkbox"/> | Azure-WL-1-AI-1 | E2Vlan0 | 10.9.4.106 | 10.9.4.1 |

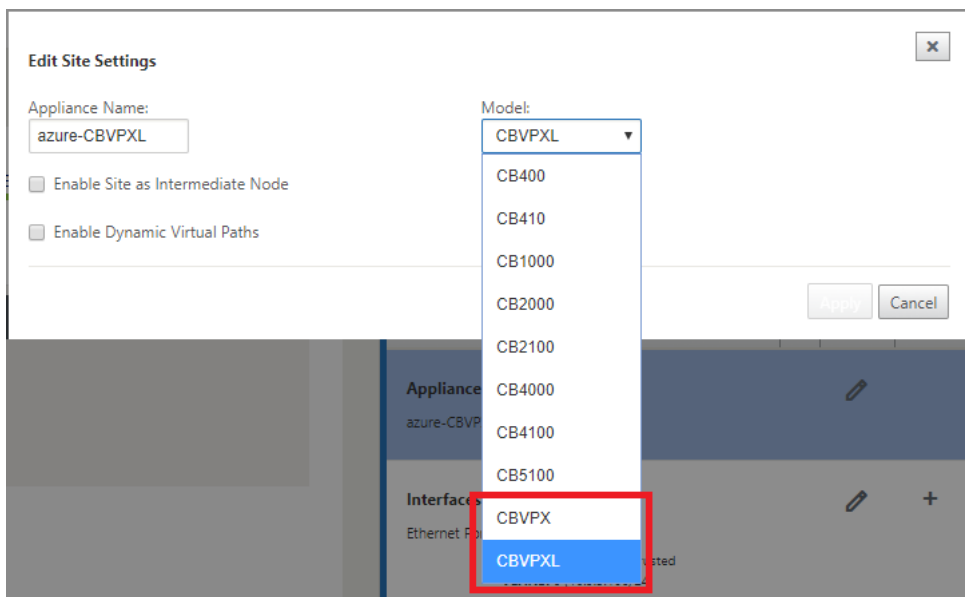
GRE Tunnels

| Include | Name | Source IP | Destination IP | Tunnel IP / Prefix |
|---------|------|-----------|----------------|--------------------|
|---------|------|-----------|----------------|--------------------|

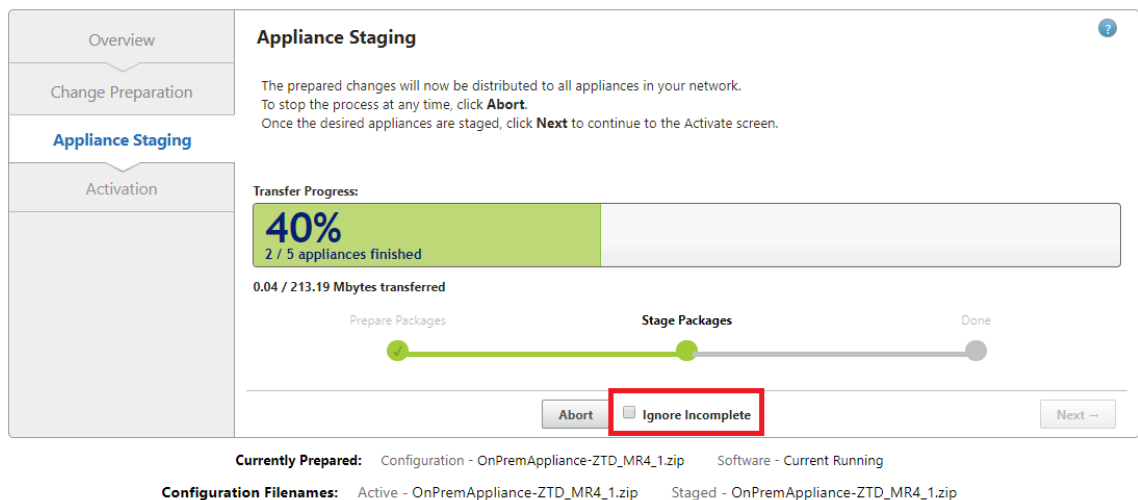
Clone

Cancel

8. Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellung**ender Site, und überprüfen Sie, ob das SD-WAN-Modell korrekt ausgewählt ist, was den Null-Touch-Dienst unterstützen würde.

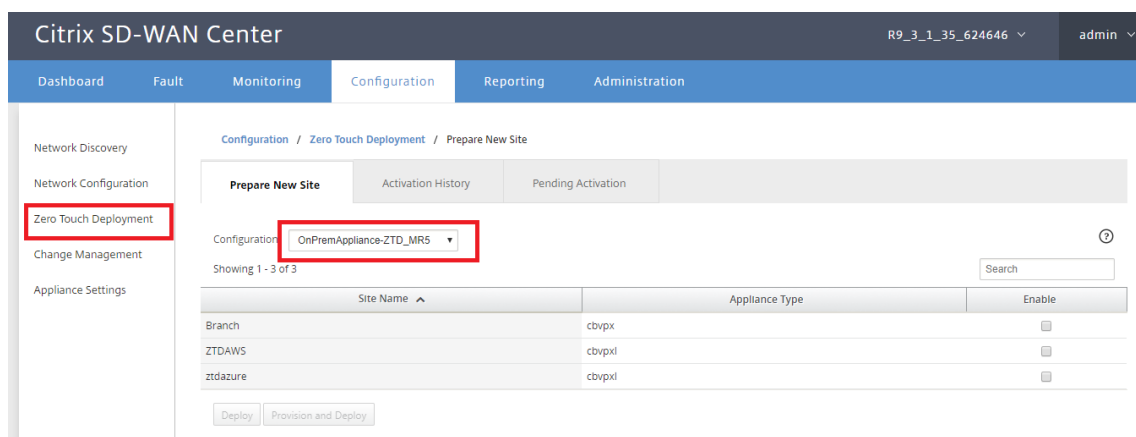


9. Speichern Sie die neue Konfiguration im SD-WAN Center, und verwenden Sie den Export in den **Change Management-Posteingang**, um die Konfiguration mithilfe von Change Management zu übertragen.
10. Befolgen Sie das Change Management-Verfahren, um für die neue Konfiguration das Staging richtig durchzuführen, wodurch die vorhandenen SD-WAN-Geräte über den neuen Standort informiert werden, der per Zero Touch bereitgestellt werden soll. Sie müssen die Option *Unvollständig ignorieren* verwenden, um den Versuch zu überspringen, die Konfiguration an die neue Site zu übertragen, die muss immer noch den ZTD-Workflow durchlaufen.

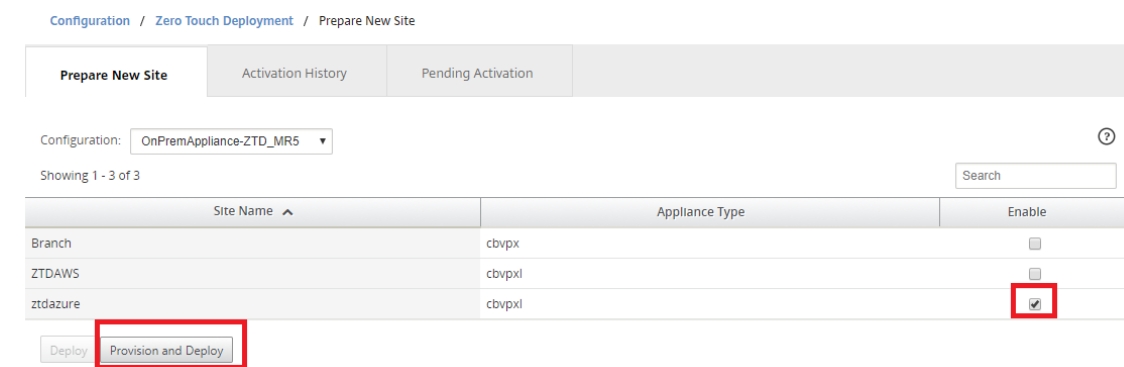


Navigieren Sie zur Zero Touch Deployment Seite des SD-WAN Centers, und wenn die neue aktive Konfiguration ausgeführt wird, wird die neue Site für die Bereitstellung und Bereitstellung von Azure SD-WAN Center verfügbar sein (Schritt 1 von 2)

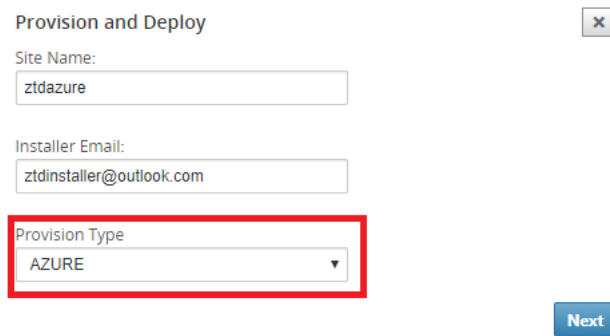
1. Melden Sie sich auf der Seite Zero Touch Deployment mit den Anmeldeinformationen Ihres Citrix Kontos an. Wählen Sie auf der Registerkarte **Neue Site bereitstellen** die ausgeführte Netzwerkkonfigurationsdatei aus.
2. Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit ZTD-fähigen Citrix SD-WAN Geräten angezeigt.



3. Wählen Sie die Ziel-Cloud-Site aus, die Sie mit dem Zero Touch-Dienst bereitstellen möchten, klicken Sie auf **Aktivieren** und dann auf **Provisioning und Bereitstellen**.



4. Es erscheint ein Popup-Fenster, in dem der Citrix SD-WAN Admin die Bereitstellung für Zero Touch initiieren kann. Überprüfen Sie, ob der Site-Name den Anforderungen in Azure entspricht (Kleinbuchstaben ohne Sonderzeichen). Geben Sie eine E-Mail-Adresse auf, an die die Aktivierungs-URL bereitgestellt werden kann, und wählen Sie Azure als **Bereitstellungstyp** für die gewünschte Cloud aus, bevor Sie auf **Weiterklicken**.



Provision and Deploy

Site Name:
ztdazure

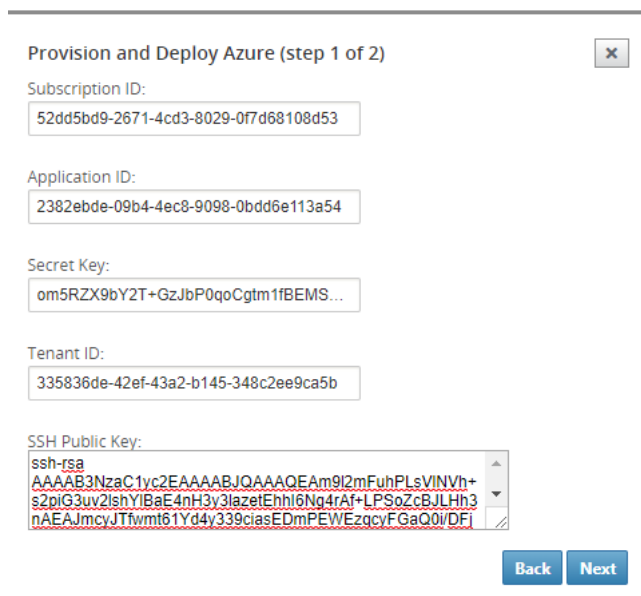
Installer Email:
ztdinstaller@outlook.com

Provision Type
AZURE

Next

5. Nachdem Sie auf **Weiter** geklickt haben, erfordert das Fenster “Provisioning und Bereitstellen von Azure (Schritt 1 von 2)” die Eingabe von vom Azure-Konto erhalten.

Kopieren Sie alle erforderlichen Felder, nachdem Sie die Informationen von Ihrem Azure-Konto erhalten haben, und fügen Sie sie ein. In den folgenden Schritten wird beschrieben, wie Sie die erforderliche Abonnement-ID, die Anwendungs-ID, den geheimen Schlüssel und die Mandanten-ID von Ihrem Azure-Konto erhalten, und klicken Sie dann auf **Weiter**.



Provision and Deploy Azure (step 1 of 2)

Subscription ID:
52dd5bd9-2671-4cd3-8029-0f7d68108d53

Application ID:
2382ebde-09b4-4ec8-9098-0bdd6e113a54

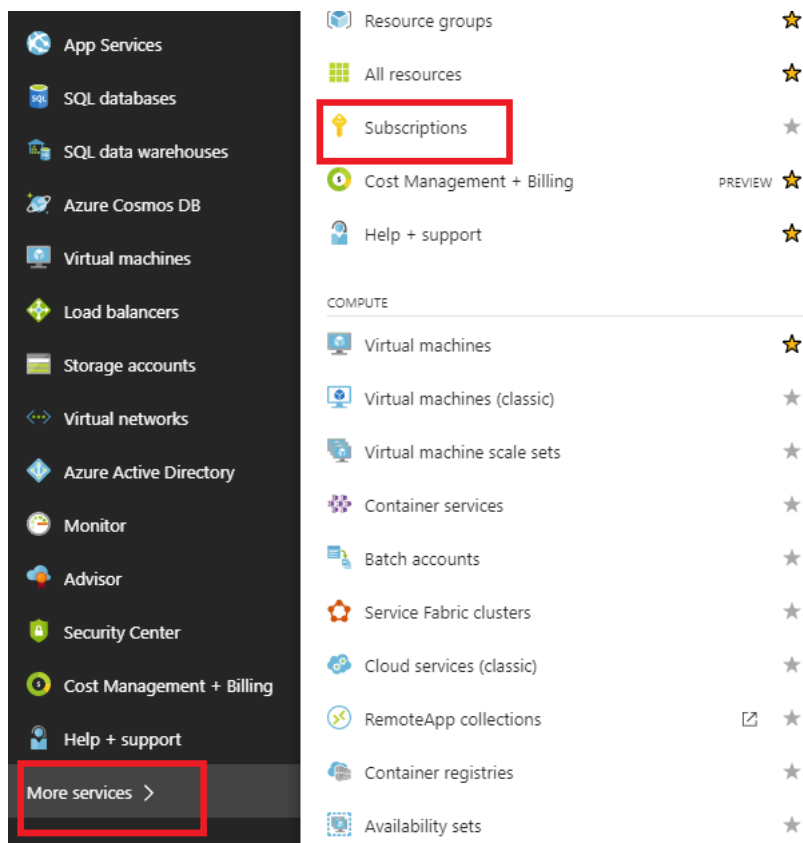
Secret Key:
om5RZX9bY2T+GzJbP0qoCgtm1fBEMS...

Tenant ID:
335836de-42ef-43a2-b145-348c2ee9ca5b

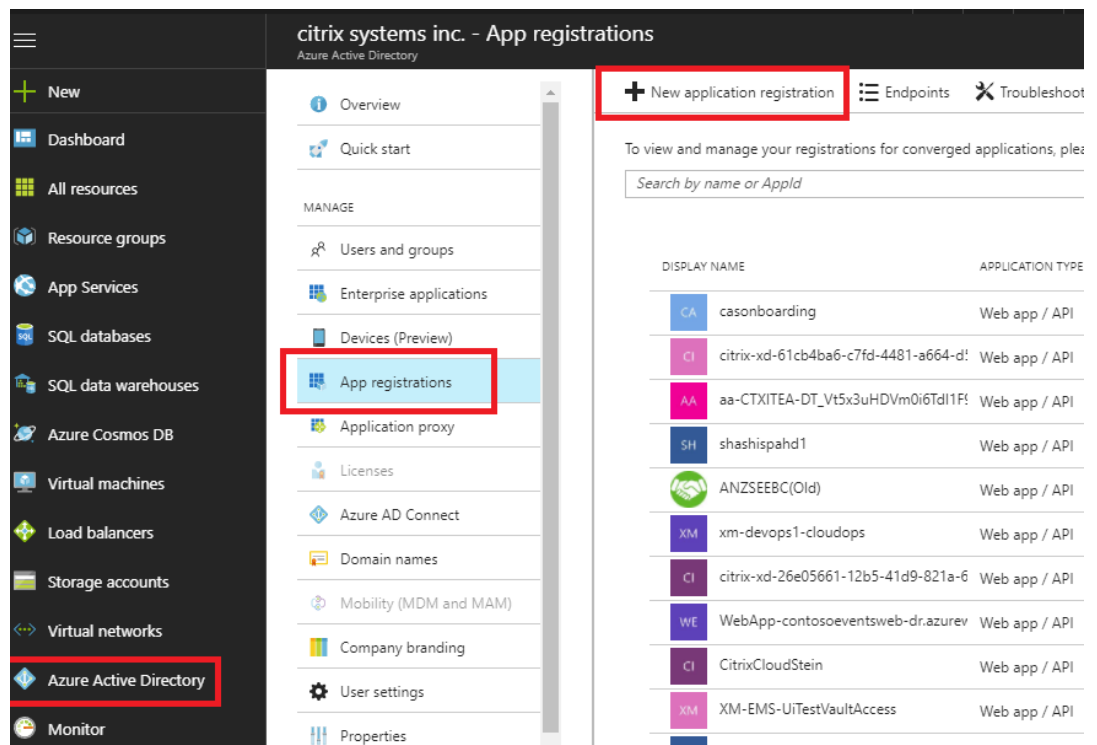
SSH Public Key:
ssh-rsa
AAAAB3NzaC1vc2EAAAABJQAAAAQEA9I2mFuhPLsVINVh+
s2piG3uv2lshYlBaE4nH3y3lazeEhhl6Ng4rAf+LPSoZcBJLHh3
nAEAJmcyJTfwmt61Yd4y339ciasEDmPEWEzqcyFGaQ0i/DFi

Back Next

- a) Auf dem Azure-Konto können wir die erforderliche **Abonnement-ID** identifizieren, indem Sie zu “Weitere Dienste” navigieren und **Abonnements auswählen**.



- b) Um die erforderliche ***Anwendungs-ID** zu identifizieren, navigieren Sie zu Azure Active Directory, Anwendungsregistrierungen, und klicken Sie auf **Neue Anwendungsregistrierung**.



- c) Geben Sie im Menü zum Erstellen der App-Registrierung einen Namen und eine Anmelde-URL ein (dies kann eine beliebige URL sein, die einzige Voraussetzung ist, dass sie gültig sein muss) und klicken Sie dann auf **Erstellen**.

Create

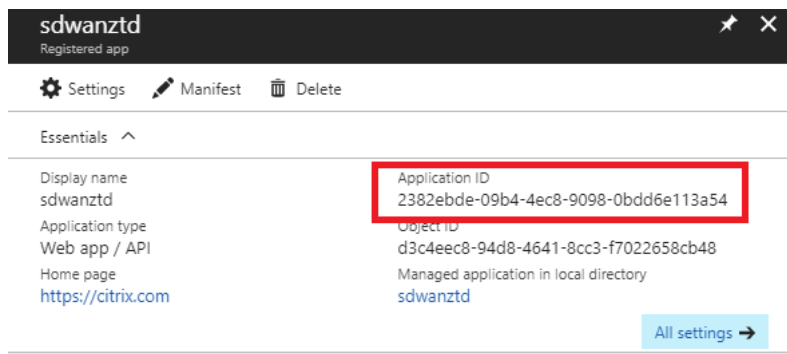
* Name *?*
sdwanztd ✓

Application type *?*
Web app / API ▼

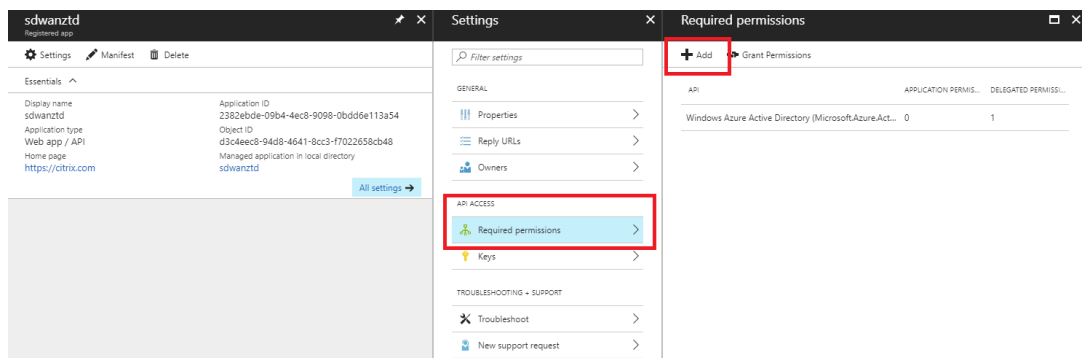
* Sign-on URL *?*
https://citrix.com ✓

Create

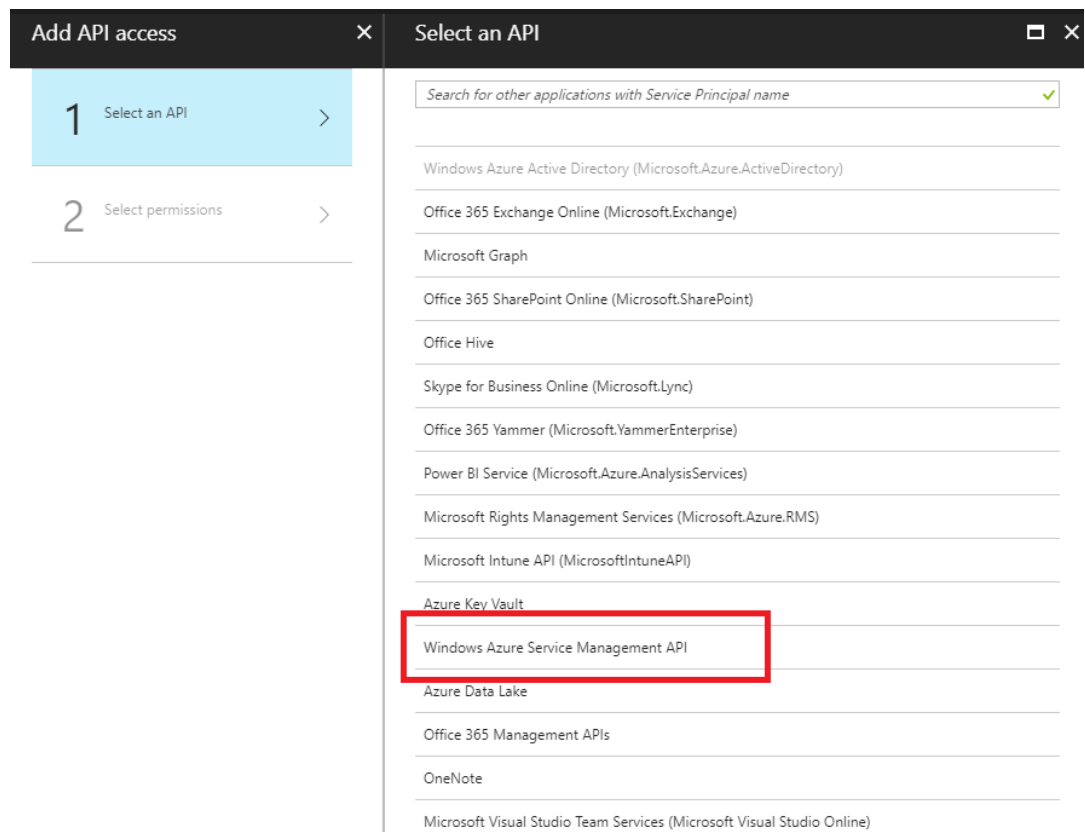
- d) Suchen Sie nach der neu erstellten registrierten App und öffnen Sie sie, und notieren Sie sich die Anwendungs-ID.



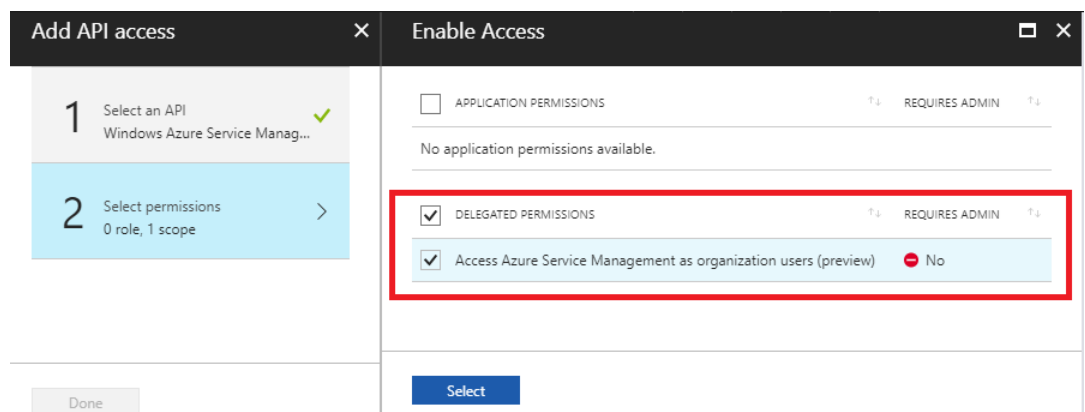
- e) Öffnen Sie erneut die neu erstellte Registrierungs-App, und um den erforderlichen *Sicherheitsschlüssel* zu identifizieren, wählen Sie unter API-Zugriff **Erforderliche Berechtigungen** aus, um einem Drittanbieter die Bereitstellung und Instanzerstellung zu erlauben. Wählen Sie dann **Hinzufügen** aus.



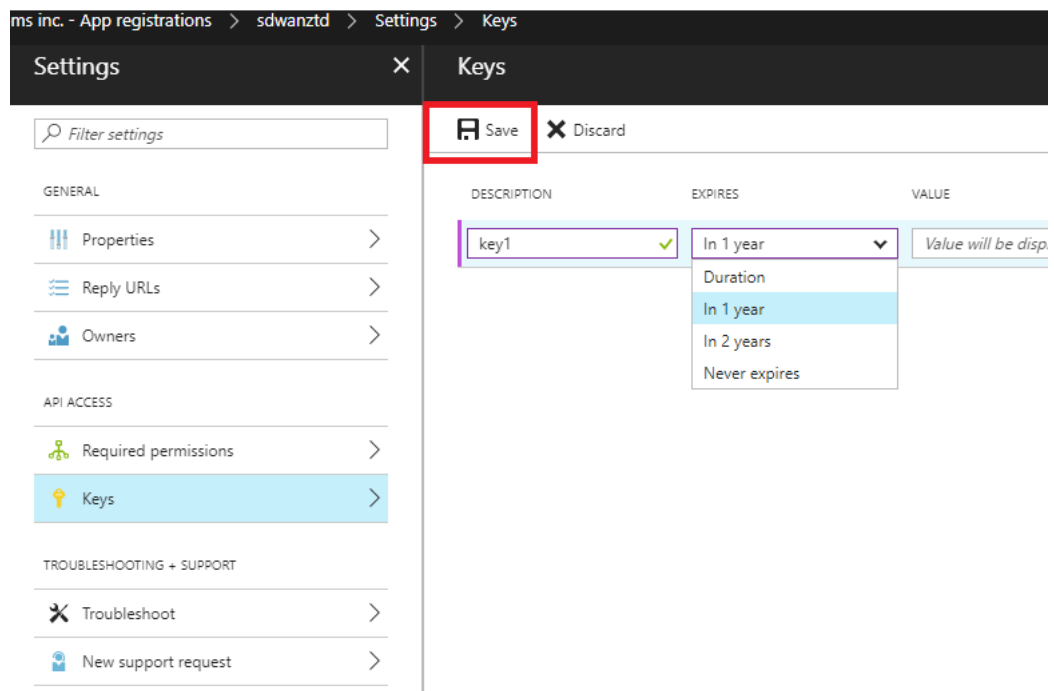
- f) Wenn Sie die erforderlichen Berechtigungen hinzufügen, wählen Sie eine **API** aus, und markieren Sie dann die **Windows Azure-Dienstverwaltungs-API**.



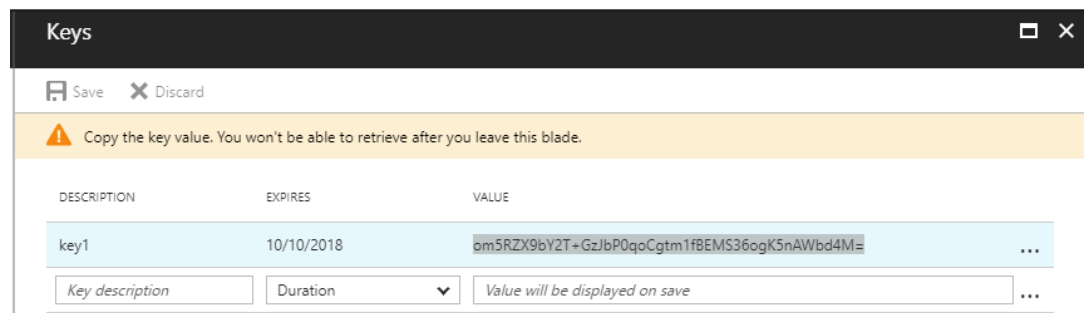
- g) Aktivieren Sie **Sie Stellvertreterberechtigungen**, um Instanzen bereitzustellen, und klicken Sie dann auf **Auswählen** und **Fertig**.



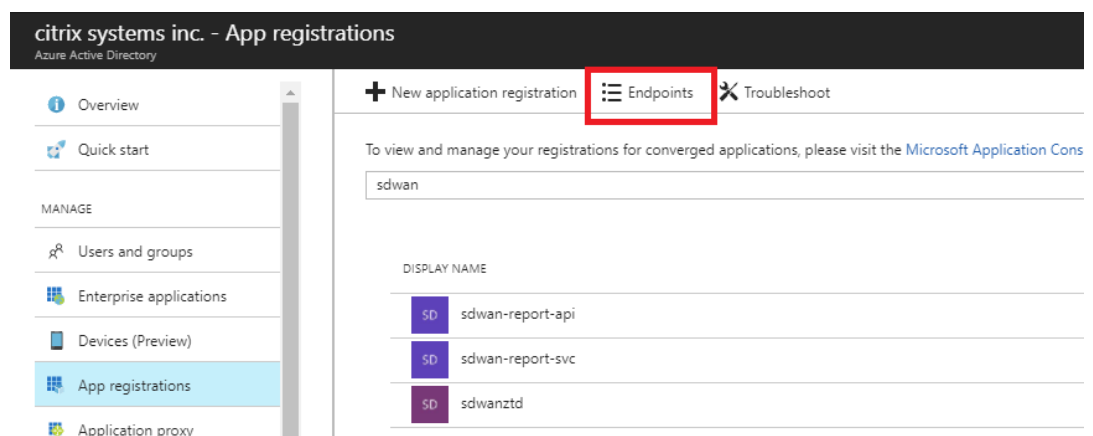
- h) Wählen Sie für diese registrierte App unter API-Zugriff die Option **Schlüssel** aus, und erstellen Sie eine geheime **Schlüsselbeschreibung** und die gewünschte **Dauer** für die Gültigkeit des Schlüssels. Klicken Sie dann auf **Speichern**, der einen **geheimen Schlüssel** erzeugt (der Schlüssel wird nur für den Provisioning Prozess benötigt, er kann gelöscht werden, nachdem die Instanz verfügbar ist).



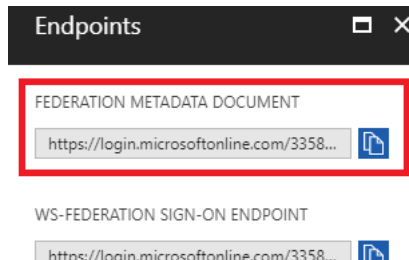
- i) Kopieren und speichern Sie den geheimen Schlüssel (beachten Sie, dass Sie diesen später nicht abrufen können).



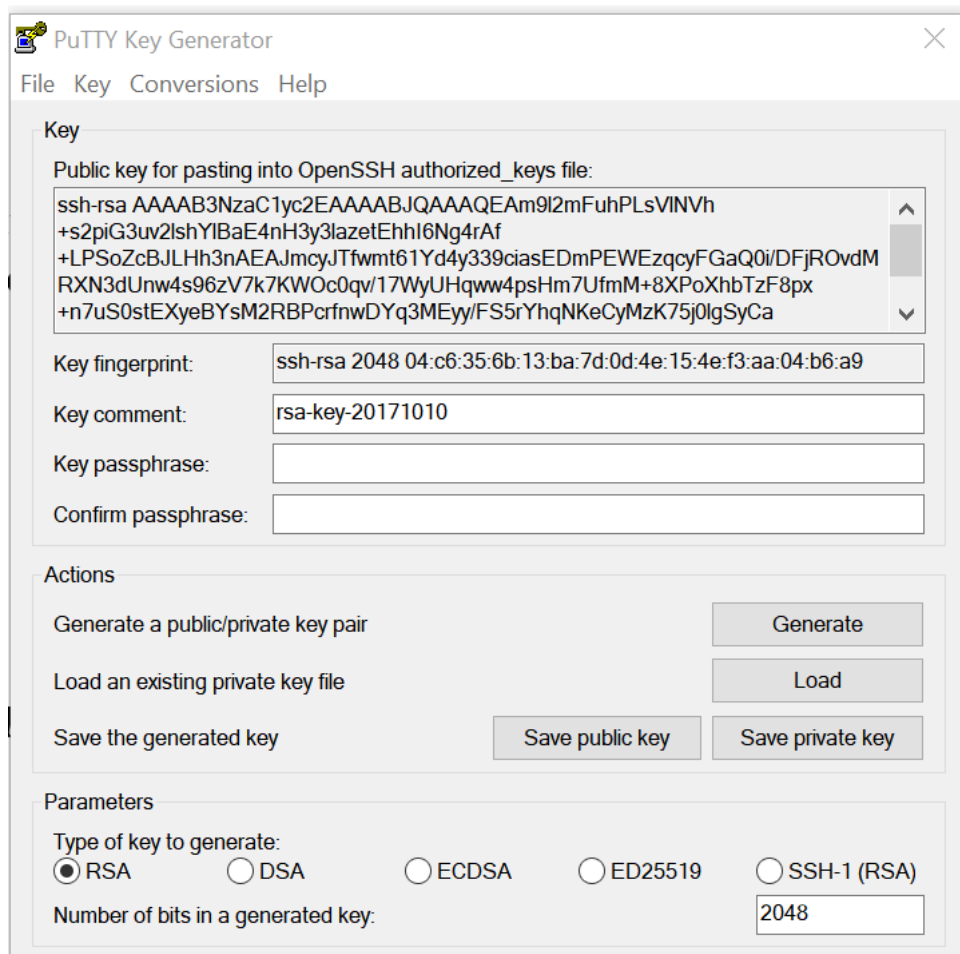
- j) Um die erforderliche **Mandanten-ID** zu identifizieren, navigieren Sie zurück zum Anwendungsregistrierungsbereich, und wählen Sie **Endpunkte** aus.



- k) Kopieren Sie das **Verbundmetadatendokument**, um Ihre Mandanten-ID zu identifizieren (beachten Sie, dass die Mandanten-ID eine 36-stellige Zeichenfolge ist, die zwischen dem `online.com/` und dem `/federation` in der URL ist).

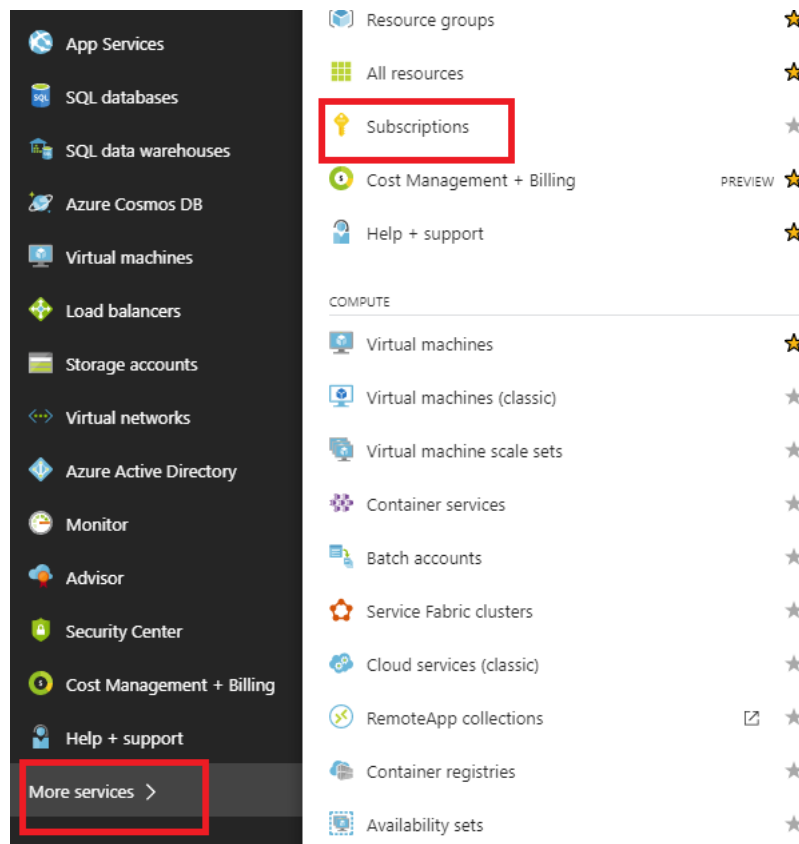


- l) Das letzte erforderliche Element ist der **öffentliche SSH-Schlüssel**. Dies kann mit dem Putty Key Generator oder `ssh-keygen` erstellt werden und wird für die Authentifizierung verwendet, so dass Passwörter sich anmelden müssen. Der öffentliche SSH-Schlüssel kann kopiert werden (einschließlich der Überschrift `ssh-rsa` und nachfolgende `rsa-key` strings). Dieser öffentliche Schlüssel wird über die SD-WAN Center-Eingabe für den Citrix Zero Touch Deployment Service freigegeben.

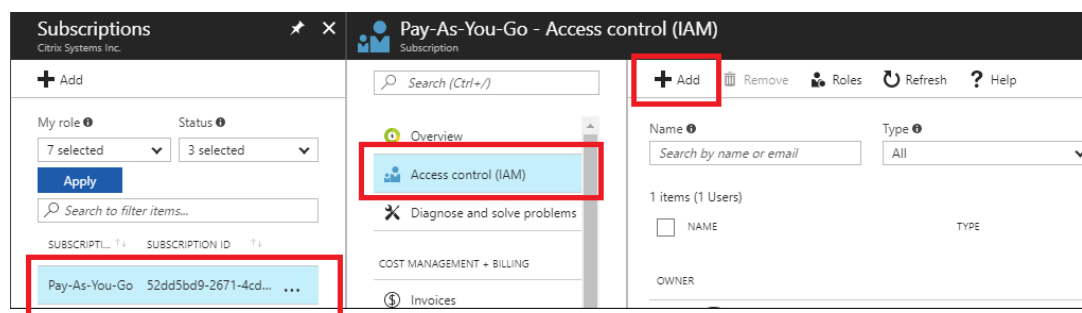


- m) Zusätzliche Schritte sind erforderlich, um der Anwendung eine Rolle zuzuweisen.

Navigieren Sie zurück zu Weitere Dienste und dann zu Abonnements.



- n) Wählen Sie das aktive Abonnement aus, dann **Zugriffskontrolle (IAM)**, und klicken Sie dann auf **Hinzufügen**.



- o) Wählen Sie im Bereich Berechtigungen hinzufügen die Option **Besitzerrolle** aus, weisen Sie Zugriff auf **Azure AD-Benutzer, -Gruppe oder -Anwendung** zu und suchen Sie im Feld **Auswählen** nach der registrierten App, damit der Zero Touch Deployment Cloud Service die Instanz auf Azure erstellen und konfigurieren kann. Abonnement. Sobald die App identifiziert wurde, wählen Sie sie aus und stellen Sie sicher, dass sie als ausgewähltes Element ausgefüllt wird, bevor Sie auf **Speichern** klicken.

Add permissions ✕

Role ⓘ
Owner ▼

Assign access to ⓘ
Azure AD user, group, or application ▼

Select ⓘ
ztd ✓

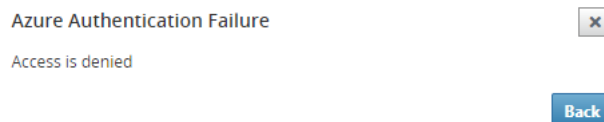
mbx_ztduser
mbx_ztduser@citrite.net

Selected members:

ztd [Remove](#)

[Save](#) [Discard](#)

- p) Nachdem Sie die erforderlichen Eingaben gesammelt und in SD-WAN Center eingegeben haben, klicken Sie auf **Weiter**. Wenn die Eingaben nicht korrekt sind, tritt ein Authentifizierungsfehler auf.



Bereitstellung und Bereitstellung von Azure im SD-WAN Center (Schritt 2 von 2)

1. Sobald die Azure-Authentifizierung erfolgreich ist, füllen Sie die entsprechenden Felder aus, um die gewünschte Azure-Region und die entsprechende Instanzgröße auszuwählen, und klicken Sie dann auf **Bereitstellen**.

Provision and Deploy Azure (step 2 of 2)

Azure Region

West US

Azure Instance Size

Standard_D4_v2

WAN subnet address prefix:

10.9.4.0/24

LAN subnet address prefix:

10.9.3.0/24

Management subnet prefix:

10.9.0.0/24

Back

Deploy

2. Navigieren Sie zur Registerkarte **Ausstehende Aktivierung** im SD-WAN Center, um den aktuellen Status der Bereitstellung zu verfolgen.

Citrix SD-WAN Center

R9_3_1_35_624646

admin

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Network Discovery

Network Configuration

Zero Touch Deployment

Change Management

Appliance Settings

Configuration / Zero Touch Deployment / Pending Activation

Prepare New Site

Activation History

Pending Activation

Showing 1 - 1 of 1

Site Name

Serial No

Installer Email

Address

Status

Action

ztdazure

B0F20EC1-9DEE-4902-B072-D593536C6C02

ztdinstaller@outlook.com

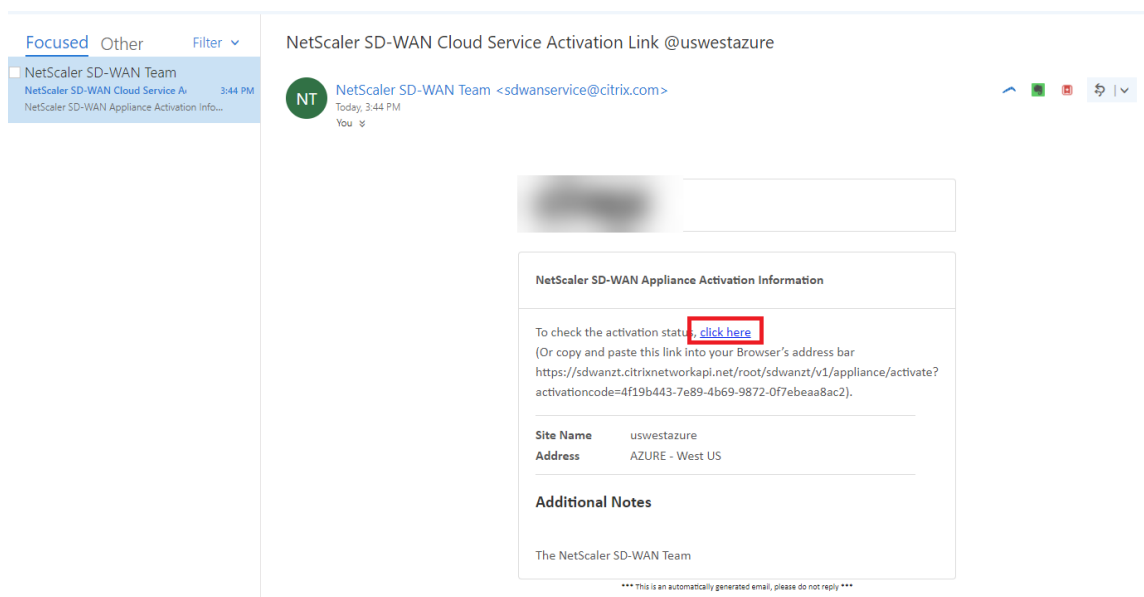
AZURE - West US 2

Provisioning

Delete

Modify

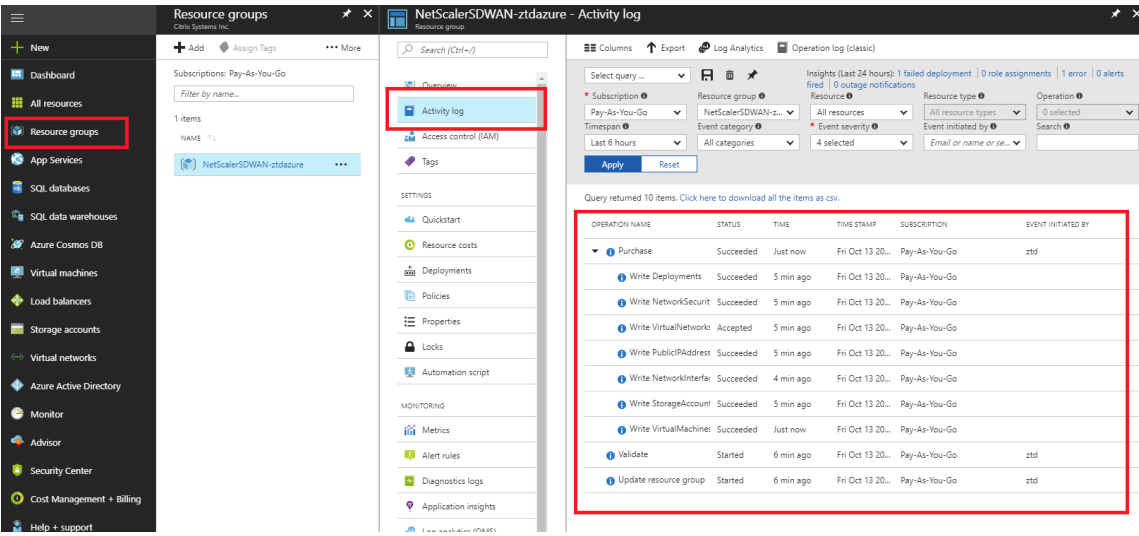
3. Eine E-Mail mit einem Aktivierungscode wird an die in Schritt 1 eingegebene E-Mail-Adresse gesendet, die E-Mail abgerufen und die **Aktivierungs-URL** geöffnet, um den Prozess auszulösen und den Aktivierungsstatus zu überprüfen.



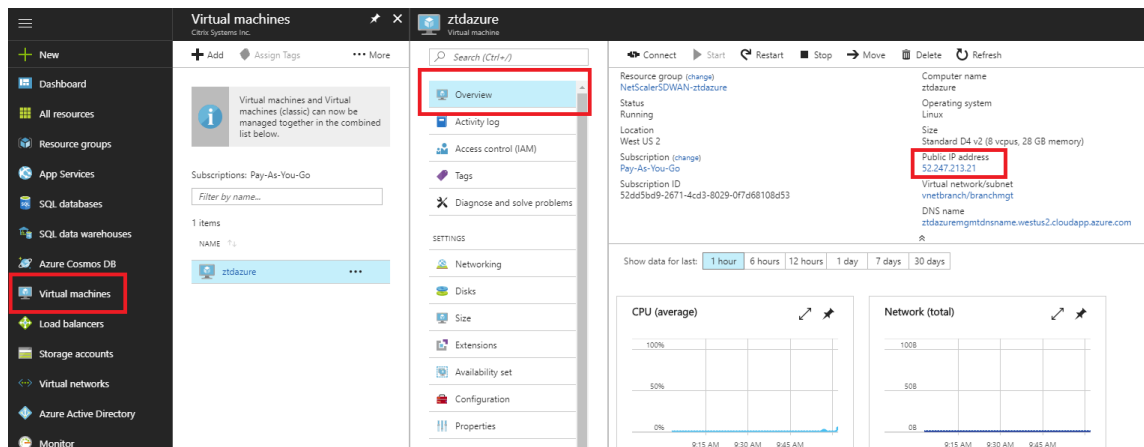
4. Eine E-Mail mit einer Aktivierungs-URL wird an die in Schritt 1 eingegebene E-Mail-Adresse gesendet. Rufen Sie die E-Mail ab und öffnen Sie die **Aktivierungs-URL**, um den Prozess auszulösen und den Aktivierungsstatus zu überprüfen.



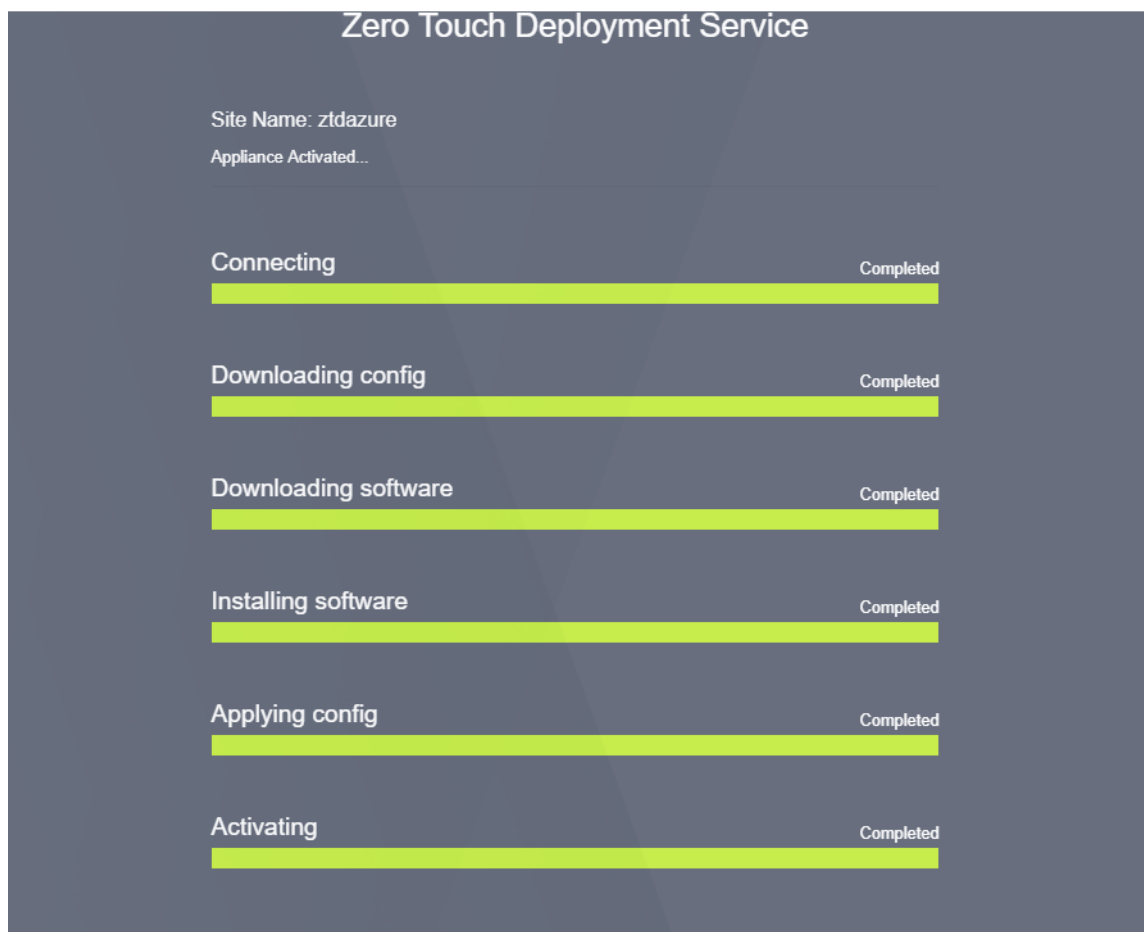
5. Es dauert einige Minuten, bis die Instanz vom SD-WAN Cloud Service bereitgestellt wird. Sie können die Aktivität im Azure-Portal unter **Aktivitätsprotokoll** für die automatisch erstellte **Ressourcengruppe** überwachen. Alle Probleme oder Fehler bei der Provisioning werden hier aufgefüllt und in das SD-WAN Center im Aktivierungsstatus repliziert.



6. Im Azure-Portal ist die erfolgreich gestartete Instanz unter **Virtuelle Maschinen verfügbar**. Um die zugewiesene öffentliche IP zu erhalten, navigieren Sie zur Übersicht für die Instanz.

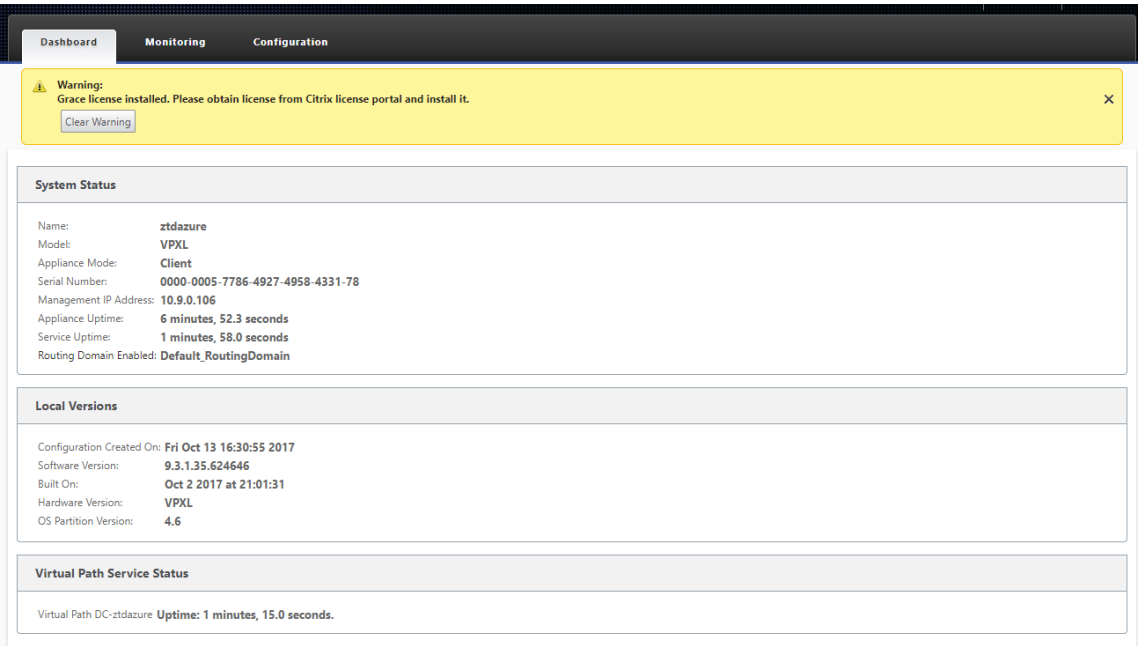


7. Nachdem sich die VM in einem laufenden Zustand befindet, geben Sie sie eine Minute, bevor der Dienst sich anspricht und den Prozess des Herunterladens der Konfiguration, der Software und der Lizenz startet.

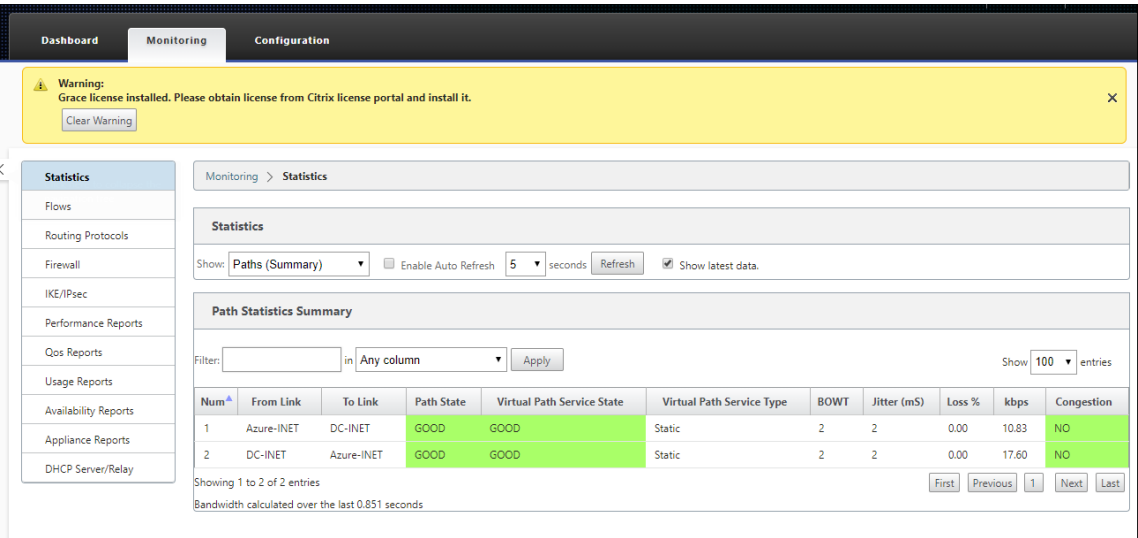


8. Nachdem die einzelnen SD-WAN-Cloud-Dienstschritte automatisch kompliziert sind, melden

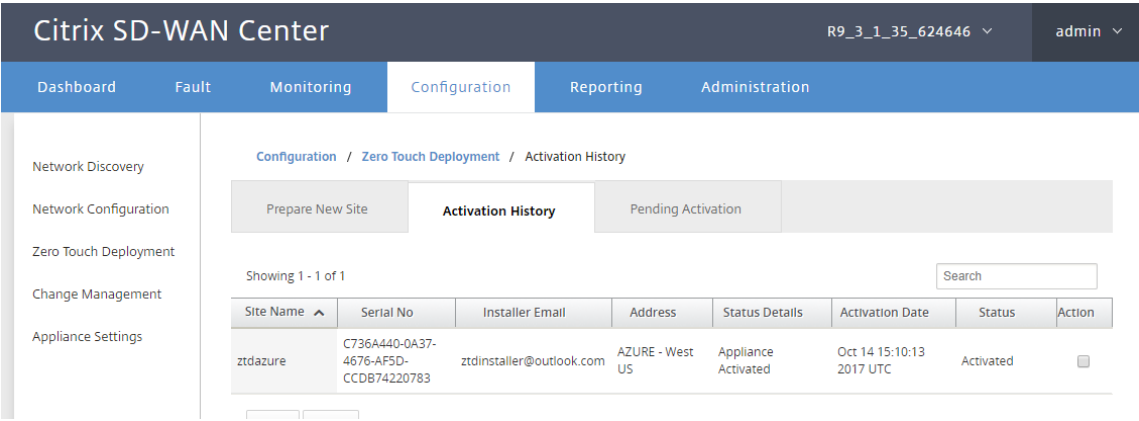
Sie sich bei der Webschnittstelle von SD-WAN-Instanzen mit der öffentlichen IP-Adresse an, die vom Azure-Portal abgerufen wurde.



9. Auf der Seite “Citrix SD-WAN Überwachungsstatistiken” werden erfolgreiche Verbindungen vom MCN zur SD-WAN-Instanz in Azure identifiziert.



10. Darüber hinaus wird der erfolgreiche (oder erfolglose) Bereitstellungsversuch auf der Aktivierungsverlaufsseite des SD-WAN-Centers protokolliert.



Bereitstellung in einer Region

May 10, 2021

Mit Regionen können Sie eine Netzwerkhierarchie mit verteilter Verwaltung definieren. Eine Region muss einen Regional Control Node (RCN) definieren, der Funktionen übernimmt, die vom Network Control Node (MCN) für seine Region ausgeführt werden. Der MCN ist der Controller für die Standard-region.

Statische und dynamische virtuelle Pfade sind zwischen Regionen nicht zulässig. RCNs verwalten den Datenverkehr zwischen Regionen.

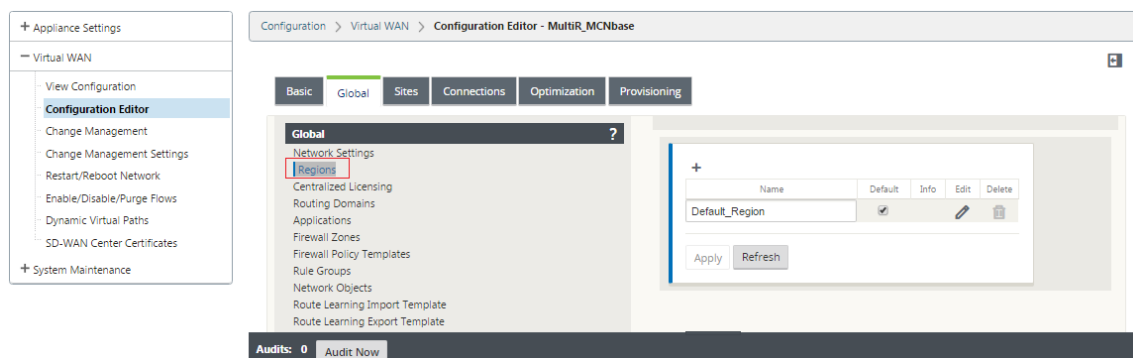
Eine Bereitstellung in einer Region in einem SD-WAN-Netzwerk kann Netzwerkstandorte mit weniger als 550 unterstützen.

Sie können einen Standardbereich im Konfigurationseditor der Benutzeroberfläche der SD-WAN-Appliance konfigurieren. Der Basic-Editor ist nützlich, um nur ein kleines Netzwerk mit MCN- und Client-SD-WAN-Knoten zu erstellen. Verwenden Sie andere Konfigurationsoptionen im Konfigurationseditor, um ein Netzwerk mit mehreren Regionen mit MCN, RCN, Clients oder erweiterten Funktionen zu konfigurieren.

So konfigurieren Sie die Bereitstellung einer einzelnen Region:

1. Navigieren Sie im Konfigurations-Editor zur Registerkarte **Global**. Wählen Sie **Regionen** aus. Die standardmäßigen Regionskonfigurationsoptionen werden angezeigt.

Sie können den Namen und die Beschreibung für den Standardbereich ändern, indem Sie ihn bearbeiten.



2. Bearbeiten Sie die **Default_Region**, um den Namen zu ändern und Subnetze zu konfigurieren.
3. Aktivieren Sie den Intervall-VIP-Abgleich je nachdem, ob Sie einen **erzwungenen internen VIP-Abgleich** oder **einen externen VIP-Abgleich**
 - Erzwungene interne VIP: Wenn diese Option aktiviert ist, müssen alle nicht-privaten virtuellen IP-Adressen in der Region mit den konfigurierten Subnetzen übereinstimmen.
 - Zulässige externe VIP - Wenn diese Option aktiviert ist, dürfen nicht-private virtuelle IP-Adressen aus anderen Regionen mit den konfigurierten Subnetzen übereinstimmen.
4. Klicken Sie auf +, um Subnetze hinzuzufügen.

Edit

Name:

Default_Region

Description:

☐ Force Internal VIP Matching

☐ Allow External VIP Matching

Subnets +

| Routing Domain | Network | Delete |
|-----------------------|---------|--------|
| Default_RoutingDomain | | |

Apply

Cancel

5. Wählen Sie eine **Routingdomäne** aus, geben Sie die **Netzwerkadresse** ein. Klicken Sie auf **Übernehmen**. Die Netzwerkadresse ist die IP-Adresse und die Maske für das Subnetz.

Bereitstellung in mehreren Regionen

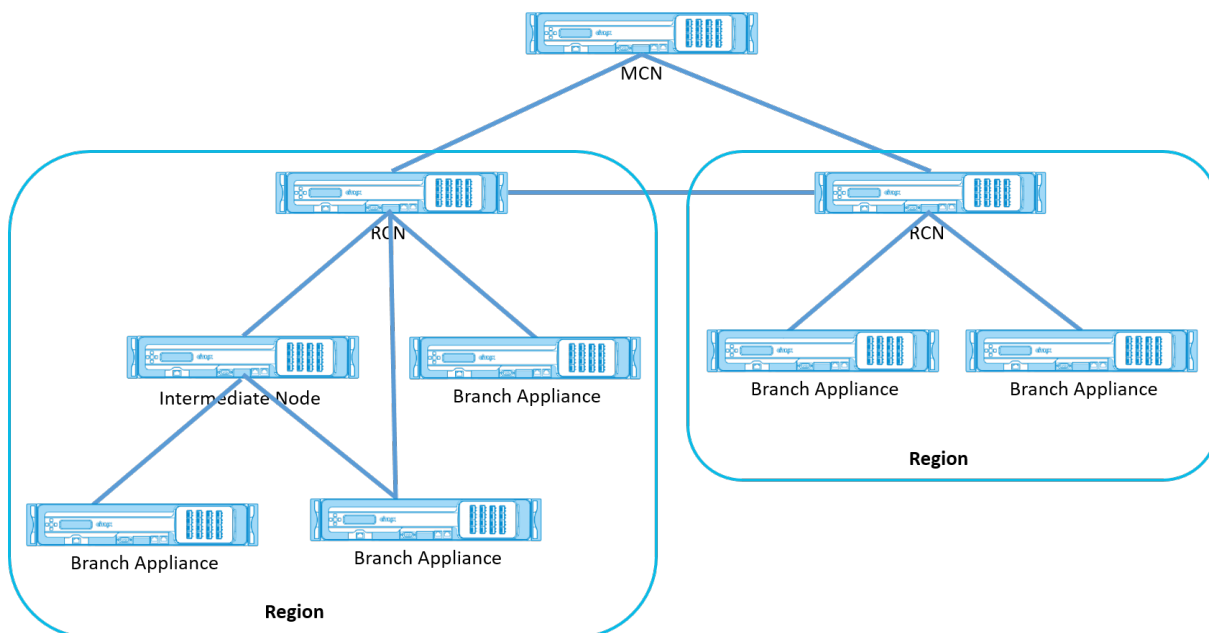
May 10, 2021

Eine SD-WAN-Appliance, die als Master Control Node (MCN) konfiguriert ist, unterstützt die Bereitstellung mehrerer Regionen. Der MCN verwaltet mehrere Regional Control Nodes (RCNs). Jeder RCN wiederum verwaltet mehrere Client-Sites. Der MCN kann auch verwendet werden, um einige der Client-Standorte direkt zu verwalten.

Mit MCN als Kontrollknoten des Netzwerks und RCNs als Kontrollknoten der Regionen kann SD-WAN bis zu 6000 Standorte verwalten.

Die Bereitstellung mit mehreren Regionen ermöglicht es Ihnen, ein Netzwerk in Regionen zu fragmentieren und ein abgestuftes Netzwerk einzurichten, z. B. Branch (Client) > RCN > MCN.

Ein MCN mit einer einzigen Region kann mit maximal 550 Standorten konfiguriert werden. Sie können die vorhandenen Sites in der Standardregion beibehalten und neue Regionen mit RCNs und deren Sites für die Bereitstellung mehrerer Regionen hinzufügen.



Die folgende Tabelle enthält eine Liste der Plattformen, die für die Konfiguration des primären und sekundären MCN/RCN unterstützt werden.

HINWEIS:

- Die Premium Edition (PE) -Appliance wird früher als Enterprise Edition (EE) bezeichnet.
- Verwenden Sie das Citrix SD-WAN 210 SE-Gerät nur in den verwalteten SD-WAN Orchestrator Netzwerken als MCN.

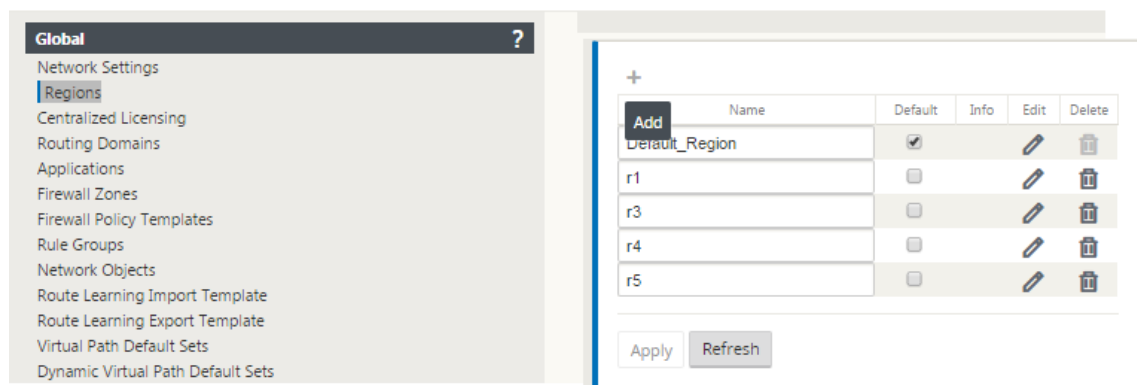
| Plattform-Edition | Primär/Sekundär-MCN | Primär/Sekundär-RCN |
|---|---------------------|---------------------|
| 110-SE | Nein | Nein |
| 210-SE | Ja | Ja |
| 400-SE | Ja | Nein |
| 410-SE | Ja | Nein |
| 1000-SE, 1000-PE | Ja | Nein |
| 1100-SE, 1100-PE | Ja | Ja |
| VPX-SE, VPXL-SE | Ja | Ja |
| 2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE | Ja | Ja |

So konfigurieren Sie die Bereitstellung mehrerer Regionen für ein SD-WAN-Netzwerk:

1. Navigieren Sie im Konfigurations-Editor zur Registerkarte **Global**. Wählen Sie **Regionen** aus. Die standardmäßigen Regionskonfigurationsoptionen werden angezeigt.

Sie können den Namen und die Beschreibung für den Standardbereich ändern, indem Sie ihn bearbeiten.

2. Klicken Sie auf **+ Hinzufügen**, um eine neue Region hinzuzufügen.



? x

Add

Name:

Description:

☐ Force Internal VIP Matching

☐ Allow External VIP Matching

Subnets +

| Network | Delete |
|---------|--------|
| | |

Add Cancel

3. Geben Sie einen Namen und eine Beschreibung für den Teilsektor ein.
4. Aktivieren Sie den internen VIP-Abgleich je nachdem, ob Sie einen **erzwungenen internen VIP-Abgleich** oder **einen externen VIP-Abgleich zulassen** möchten
 - Erzwungene interne VIP: Wenn diese Option aktiviert ist, müssen alle nicht-privaten virtuellen IP-Adressen in der Region mit den konfigurierten Subnetzen übereinstimmen.
 - Zulässige externe VIP - Wenn diese Option aktiviert ist, dürfen nicht-private virtuelle IP-Adressen aus anderen Regionen mit den konfigurierten Subnetzen übereinstimmen.
5. Klicken Sie auf +, um Subnetze hinzuzufügen. Wählen Sie eine Routingdomäne aus.

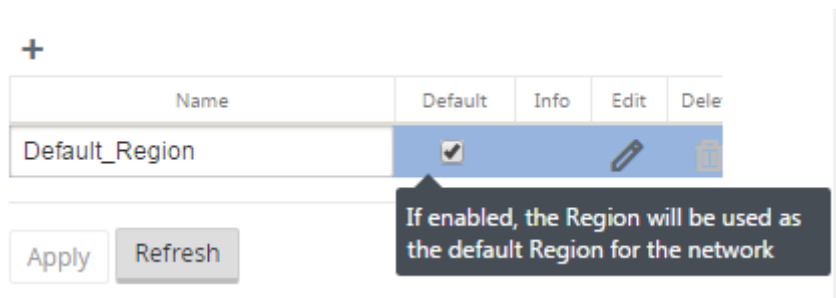
Subnets +

| Routing Domain | Network | Delete |
|-----------------------|---------|--------|
| <Default> | | |
| <Default> | | |
| Default_RoutingDomain | | |
| WCCP_RoutingDomain | | |

Add Cancel

6. Geben Sie eine **Netzwerkadresse** ein. Klicken Sie auf **Hinzufügen**. Die Netzwerkadresse ist die IP-Adresse und die Maske für das Subnetz. Der neu erstellte Bereich wird der vorhandenen Liste der Regionen hinzugefügt.

Sie können das Kontrollkästchen **Standard** aktivieren, um einen gewünschten Bereich als Standard zu verwenden.



Hinweis

Sie können MCN auf einen GEO- oder Client-Site klonen.

Das SD-WAN Center unterstützt die Bereitstellung mehrerer Regionen. Weitere Informationen finden Sie unter [SD-WAN Center Bereitstellung und Berichterstellung über mehrere Regionen](#).

Übersichtsansicht des Änderungsmanagements

Wenn Sie den Änderungsverwaltungsprozess für Appliances durchführen, die in der Bereitstellung mit mehreren Regionen konfiguriert sind, wird die Übersichtstabelle für das Änderungsmanagement in der Benutzeroberfläche der SD-WAN-Appliance angezeigt.

In der Spalte **Region** wird eine Liste der Regionen angezeigt, die derzeit im Netzwerk konfiguriert sind. Sie können die Änderungsverwaltungsübersicht für eine bestimmte Region anzeigen, indem Sie sie in der Übersichtstabelle auswählen.

Standardregionsübersicht:

Global Multi-Region Summary

| Region | Total Sites | Not Connected | Preparing/Staging | Staged | Failed |
|----------------|--------------------|---------------|-------------------|--------|--------|
| Default_Region | 5 | 1 | 0 | 4 | 0 |
| AMEA_r1 | 32 | 0 | 0 | 32 | 0 |
| APAC_r1 | 2 | 0 | 0 | 2 | 0 |
| AMER-1 | Data not available | | | | |

Region - Default_Region Details

Show 25 entries

| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Traffic Interruption | | Download Package |
|-------------------------------|--------|------------|------------------|------------------|------------------|------------------|----------------------|--------|------------------|
| | | | Software | Config | Software | Config | Expected | Actual | |
| MCN1-MCN1-CB4100 | CB4100 | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 min | | active / staged |
| APAC_RCN-APAC_RCN-CB1000 | CB1000 | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | | active / staged |
| BR1-BR1-CBVPXL | CBVPXL | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | | active / staged |
| RCN01-2000-RCN01-2000 | CB2000 | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | | active / staged |
| AMER-1RCN-5100-AMER-1RCN-5100 | CB5100 | Not Needed | Not Connected | | | | Loc Chg Mgt | | none / staged |

Previous 1 Next

Regionsübersicht:

Global Multi-Region Summary

Search

| Region | Total Sites | Not Connected | Preparing/Staging | Staged | Failed |
|----------------|--------------------|---------------|-------------------|--------|--------|
| Default Region | 5 | 1 | 0 | 4 | 0 |
| AMEA_r1 | 32 | 0 | 0 | 32 | 0 |
| APAC_r1 | 2 | 0 | 0 | 2 | 0 |
| AMER-1 | Data not available | | | | |

Region - AMEA_r1 Details

Show25entries

Search

CustomizeRefresh

| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Traffic Interruption | | Download Package |
|-----------------------------|-------|-------|------------------|------------------|------------------|------------------|----------------------|--------|------------------|
| | | | Software | Config | Software | Config | Expected | Actual | |
| AMEA_r1_vpx01-AMEA_r1_vpx01 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx02-AMEA_r1_vpx02 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx03-AMEA_r1_vpx03 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx04-AMEA_r1_vpx04 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx05-AMEA_r1_vpx05 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx06-AMEA_r1_vpx06 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx07-AMEA_r1_vpx07 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx08-AMEA_r1_vpx08 | CBVPX | Done | 10.1.0.14.661523 | 15:54 on 2/28/18 | 10.1.0.14.661523 | 16:11 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx13-AMEA_r1_vpx13 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx14-AMEA_r1_vpx14 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx15-AMEA_r1_vpx15 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx16-AMEA_r1_vpx16 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx17-AMEA_r1_vpx17 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx18-AMEA_r1_vpx18 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx19-AMEA_r1_vpx19 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx20-AMEA_r1_vpx20 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx33-AMEA_r1_vpx20 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx34-AMEA_r1_vpx20 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx35-vpx35 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx36-vpx36 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx37-vpx37 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx38-vpx38 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx39-vpx39 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx40-vpx40 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |
| AMEA_r1_vpx49-vpx49 | CBVPX | Done | 10.1.0.14.661523 | 16:11 on 2/28/18 | 10.1.0.14.661523 | 21:14 on 2/28/18 | <1 sec | 0 ms | active / staged |

Previous12Next

Hinweis

In einigen Fällen ist der Wert **Gesamtzahl Sites**, der in der Tabelle **Globale Übersicht über mehrere Regionen** angezeigt wird, kleiner als die Summe der verbleibenden Spalten.

Wenn beispielsweise ein Zweigknoten nicht verbunden ist, ist es möglich, dass der Zweig zweimal gezählt wird; einmal als “Nicht verbunden” und einmal als “Vorbereitung/Staging”.

Konfigurationshandbuch für Citrix Virtual Apps and Desktops Workloads

June 8, 2022

Citrix SD-WAN ist eine WAN-Edge-Lösung der nächsten Generation, die die digitale Transformation

mit flexibler, automatisierter, sicherer Konnektivität und Leistung für SaaS-, Cloud- und virtuelle Anwendungen beschleunigt, um eine stets aktive Workspace Erfahrung zu gewährleisten.

Citrix SD-WAN ist die empfohlene und beste Möglichkeit für Unternehmen, die den Citrix Virtual Apps and Desktops Service verwenden, eine Verbindung zu Workloads von Citrix Virtual Apps and Desktops in der Cloud herzustellen. Weitere Informationen finden Sie unter [Citrix Blog](#).

Dieses Dokument konzentriert sich auf die Konfiguration von Citrix SD-WAN für die Konnektivität zu/von Citrix Virtual Apps and Desktops Workloads auf Azure.

Vorteile

- Einfache Einrichtung von SD-WAN in Citrix Virtual Apps and Desktops über einen geführten Workflow
- Ständig eingeschaltete, leistungsstarke Konnektivität durch fortschrittliche SD-WAN-Technologien
- Vorteile über alle Verbindungen hinweg (VDA-zu-DC, Benutzer-zu-VDA, VDA-zu-Cloud, Benutzer-zu-Cloud)
- Reduziert die Latenz im Vergleich zum Backhauling-Datenverkehr zum Rechenzentrum
- Verkehrsmanagement zur Sicherstellung der Quality of Service (QoS)
 - QoS über HDX/ICA-Datenverkehrsströme (HDX AutoQoS mit einem Port)
 - QoS zwischen HDX und anderem Datenverkehr
 - HDX QoS Fairness zwischen Benutzern
 - End-to-End-QoS
- Link-Bonding bietet mehr Bandbreite für schnellere Leistung
- Hohe Verfügbarkeit mit nahtlosem Link-Failover und SD-WAN-Redundanz in Azure
- Optimiertes VoIP-Erlebnis (Paketrennen für reduzierten Jitter und minimalen Paketverlust, QoS, lokaler Ausbruch für reduzierte Latenz)
- Größere Kosteneinsparungen und müssen im Vergleich zu Azure ExpressRoute schneller und einfacher bereitgestellt werden

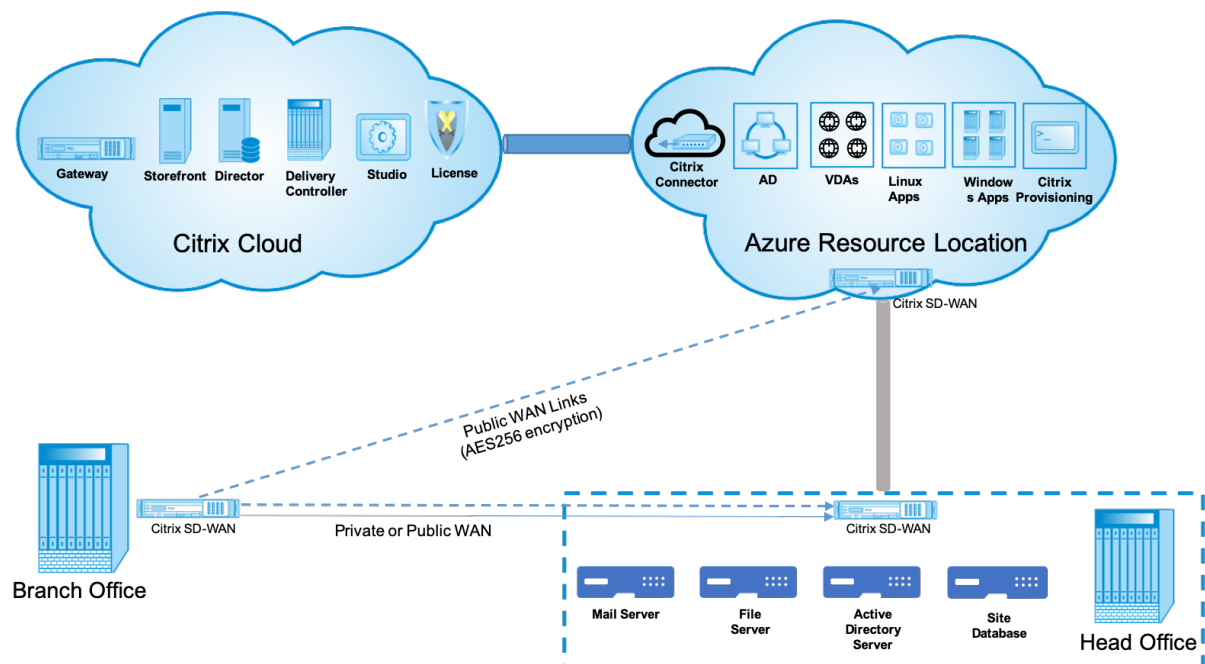
Voraussetzungen

Befolgen Sie die folgenden Voraussetzungen, um die Workload-Funktionen von Citrix Virtual Apps and Desktops zu bewerten und bereitzustellen:

- Sie müssen entweder über ein vorhandenes SD-WAN-Netzwerk verfügen oder ein neues erstellen.
- Sie müssen ein Abonnement für Citrix Virtual Apps and Desktops Service haben.

- Um SD-WAN-Funktionen wie Multistream-HDX-AutoQoS und tiefe Sichtbarkeit nutzen zu können, muss der Network Location Service (NLS) für alle SD-WAN-Sites in Ihrem Netzwerk konfiguriert sein.
- Sie müssen einen DNS-Server und AD bereitstellen, auf dem die Clientendpunkte vorhanden sind (häufig in Ihrer Rechenzentrums Umgebung), oder Sie können Azure Active Directory (AAD) verwenden.
- Der DNS-Server muss in der Lage sein, sowohl interne (private) als auch externe (öffentliche) IPs aufzulösen.
- Stellen Sie sicher, dass der FQDN (sdwan-location.citrixnetworkapi.net) der Zulassungsliste in der Firewall hinzugefügt wird. Dies ist der FQDN für den Netzwerkstandortdienst, der für das Senden von Datenverkehr über den virtuellen SD-WAN-Pfad von entscheidender Bedeutung ist. Eine bessere Möglichkeit, wenn Sie mit Positivlisten von Wildcard-FQDNs vertraut sind, wäre es auch möglich *.citrixnetworkapi.net zur zulässigen Liste hinzuzufügen, da dies die Subdomain für andere Citrix Cloud-Dienste wie Zero-Touch-Provisioning ist.
- Melden Sie sich bei sdwan.cloud.com an, um den SD-WAN Orchestrator für die Verwaltung Ihres SD-WAN-Netzwerks zu verwenden. SD-WAN Orchestrator ist eine auf Citrix Cloud basierende Multitenant-Verwaltungsplattform für Citrix SD-WAN.

Bereitstellungsarchitektur



Die folgenden Entitäten sind für die Bereitstellung erforderlich:

- Ein on-premises Standort, der die SD-WAN-Appliance hostet, die entweder im Zweigstellenmodus oder als MCN (Master Control Node) bereitgestellt werden kann. Der Zweigmodus

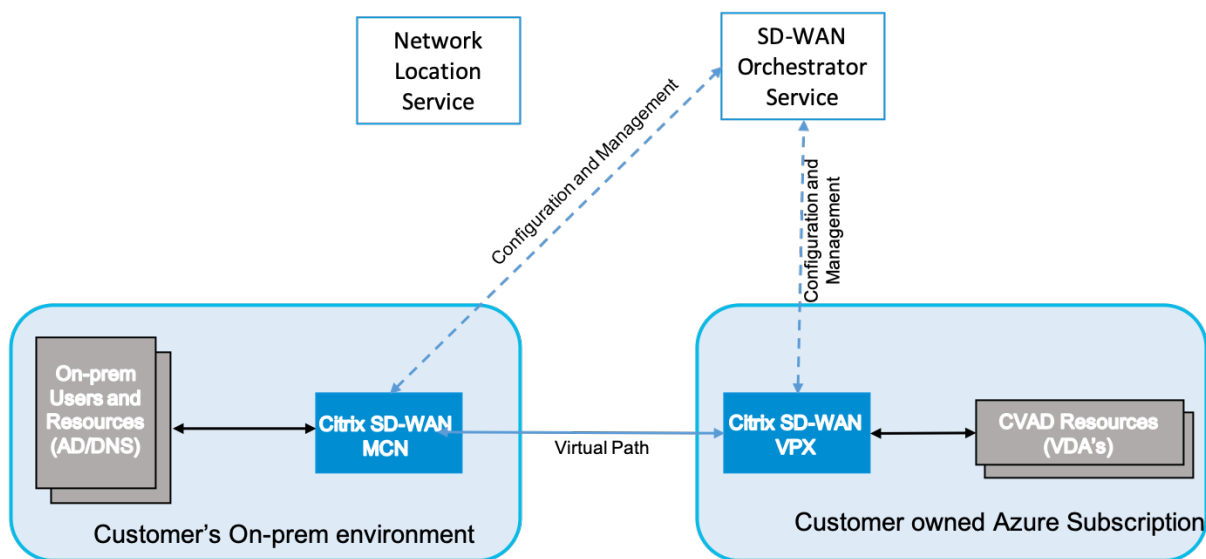
oder MCN enthält die Clientcomputer, das Active Directory und DNS. Sie können jedoch auch die Verwendung von Azure DNS und AD wählen. In den meisten Szenarien dient der lokale Standort als Rechenzentrum und beherbergt das MCN.

- **Cloud-Service für Citrix Virtual Apps and Desktops** —Citrix Virtual Apps and Desktops bietet Virtualisierungslösungen, die der IT die Kontrolle über virtuelle Maschinen, Anwendungen und Sicherheit ermöglichen und überall Zugriff für jedes Gerät bieten. Endbenutzer können Anwendungen und Desktops unabhängig vom Betriebssystem und der Benutzeroberfläche des Geräts verwenden.

Mit dem Citrix Virtual Apps and Desktops s-Dienst können Sie sichere virtuelle Apps und Desktops auf jedem Gerät bereitstellen und den Großteil der Produktinstallation, Setup, Konfiguration, Upgrades und Überwachung von Citrix überlassen. Sie behalten die vollständige Kontrolle über Anwendungen, Richtlinien und Benutzer und bieten auf jedem Gerät die beste Benutzererfahrung.

- **Citrix Connector/Cloud Connector** - Sie verbinden Ihre Ressourcen über Citrix Cloud Connector mit dem Service, der als Kanal für die Kommunikation zwischen Citrix Cloud und Ihren Ressourcenstandorten dient. Mit Cloud Connector kann die Cloud ohne komplexe Netzwerk- oder Infrastrukturkonfiguration (VPNs, IPsec-Tunnel o. Ä.) verwaltet werden. Ressourcenstandorte enthalten die Maschinen und andere Ressourcen, die Anwendungen und Desktops für Ihre Abonnenten bereitstellen.
- **SD-WAN Orchestrator** —Citrix SD-WAN Orchestrator ist ein Cloud-gehosteter Multitenant-Management-Service, der **Do It Yourself** Unternehmen und Citrix Partnern zur Verfügung steht. Citrix Partner können Citrix SD-WAN Orchestrator verwenden, um mehrere Kunden mit einer einzigen Glasscheibe und geeigneten rollenbasierten Zugriffskontrollen zu verwalten.
- **Virtuelle und physische SD-WAN-Appliances** —Dies läuft als mehrere Instanzen in der Cloud (VMs) und on-premises im Rechenzentrum und in den Zweigstellen (physische Geräte oder VMs), um Konnektivität zwischen diesen Standorten und zum/vom öffentlichen Internet bereitzustellen. Die SD-WAN-Instanz in Citrix Virtual Apps and Desktops wird als eine oder eine Reihe virtueller Appliances (in HA-Bereitstellung) erstellt, indem diese Instanzen über den Azure Marketplace Provisioning werden. SD-WAN-Appliances an anderen Standorten (DC und Niederlassungen) werden vom Kunden erstellt. Alle diese SD-WAN-Appliances werden (in Bezug auf Konfiguration und Software-Upgrades) von SD-WAN-Administratoren über SD-WAN Orchestrator verwaltet.

Bereitstellung und Konfiguration



In einer gemeinsamen Bereitstellung würde ein Kunde die Citrix SD-WAN Appliance (H/W oder VPX) als MCN in seinem DC/Large Office bereitstellen. Der Kunden-DC würde normalerweise lokale Benutzer und Ressourcen wie AD- und DNS-Server hosten. In einigen Szenarien kann der Kunde Azure Active Directory Dienste (AADS) und DNS nutzen, die beide von der Citrix SD-WAN - und CMD-Integration unterstützt werden.

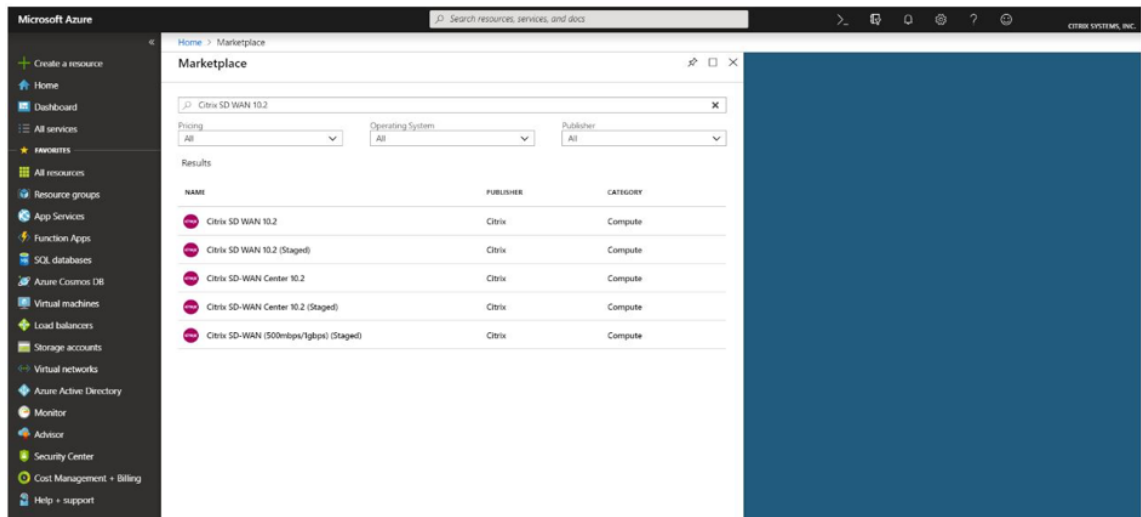
Innerhalb des vom Kunden verwalteten Azure-Abonnements muss der Kunde die virtuelle Citrix SD-WAN Appliance und die VDAs bereitstellen. Die SD-WAN-Appliances werden über SD-WAN Orchestrator verwaltet. Sobald die SD-WAN-Appliance konfiguriert wurde, stellt sie eine Verbindung zum vorhandenen Citrix SD-WAN Netzwerk her. Weitere Aufgaben wie Konfiguration, Transparenz und Verwaltung werden über SD-WAN Orchestrator erledigt.

Die dritte Komponente dieser Integration ist der **Network Location Service (NLS)**, der es internen Benutzern ermöglicht, das Gateway zu Bypass und sich direkt mit den VDAs zu verbinden, wodurch die Latenz für den internen Netzwerkverkehr reduziert wird. Sie können NLS manuell oder über Citrix SD-WAN Orchestrator konfigurieren. Weitere Informationen finden Sie unter [NLS](#).

Konfiguration

Die Citrix SD-WAN VM wird in einer bestimmten Region bereitgestellt (je nach Kundenwunsch) und kann über MPLS, Internet oder 4G/LTE mit mehreren Zweigstellen verbunden werden. Innerhalb einer VNET (Virtual Network) -Infrastruktur wird die SD-WAN Standard Edition (SE) -VM im Gateway Modus bereitgestellt. Das VNET verfügt über Routen zum Azure-Gateway. Die SD-WAN-Instanz verfügt über eine Route zum Azure-Gateway für die Internetverbindung. Diese Route muss manuell erstellt werden.

1. Navigieren Sie in einem Webbrowser zu [Azure-Portal](#). Melden Sie sich bei Microsoft Azure-Konto an und suchen Sie nach Citrix SD-WAN Standard Edition.
2. Wählen Sie in den Suchergebnissen die Citrix SD-WAN Standard Edition-Lösung aus. Klicken Sie auf **Erstellen**, nachdem Sie die Beschreibung durchlaufen und sichergestellt haben, dass die gewählte Lösung korrekt ist.

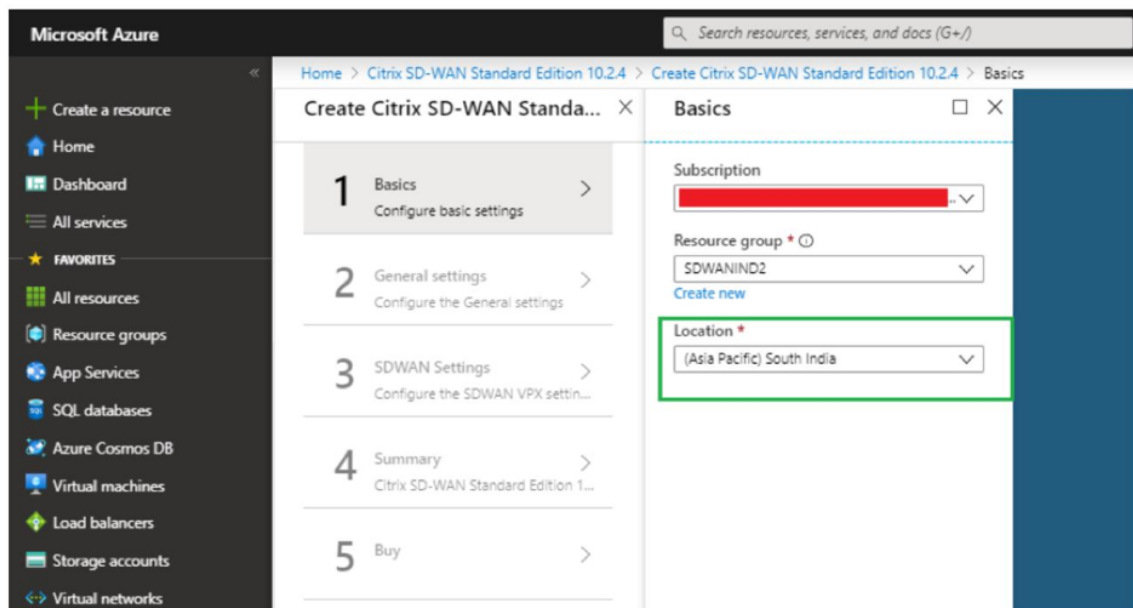


Klicken Sie auf **Erstellen**, einen Assistenten, der mit den erforderlichen Details zum Erstellen der virtuellen Maschine auffordert.

3. Wählen Sie auf der Seite **Grundeinstellungen** die Ressourcengruppe aus, in der Sie die SD-WAN SE-Lösung bereitstellen möchten.

Eine Ressourcengruppe ist ein Container, der zugehörige Ressourcen für eine Azure-Lösung enthält. Die Ressourcengruppe kann alle Ressourcen für die Lösung oder nur die Ressourcen enthalten, die Sie als Gruppe verwalten möchten. Sie können auf der Grundlage Ihrer Bereitstellung festlegen, wie Ressourcen Ressourcengruppen zugewiesen werden sollen.

Für Citrix SD-WAN wird empfohlen, dass die ausgewählte Ressourcengruppe leer sein muss. Wählen Sie in ähnlicher Weise die Azure-Region aus, in der Sie die SD-WAN-Instanz bereitstellen möchten. Die Region muss mit der Region identisch sein, in der Ihre Citrix Virtual Apps and Desktops Ressourcen bereitgestellt werden.



4. Geben Sie auf der Seite **Administratoreinstellungen** einen Namen für die virtuelle Maschine an. Wählen Sie einen Benutzernamen und ein sicheres Kennwort. Das Kennwort muss aus einem Großbuchstaben und einem Sonderzeichen bestehen und aus mehr als neun Zeichen bestehen. Klicken Sie auf **OK**.

Dieses Kennwort ist erforderlich, um sich als Gastbenutzer an der Verwaltungsoberfläche der Instanz anzumelden. Um Admin-Zugriff auf die Instanz zu erhalten, verwenden Sie admin als Benutzernamen und das Kennwort, das während der Provisioning der Instanz erstellt wurde. Wenn Sie den Benutzernamen verwenden, der während der Provisioning der Instanz erstellt wurde, erhalten Sie schreibgeschützten Zugriff. Wählen Sie hier auch den Bereitstellungstyp aus.

Wenn Sie eine einzelne Instanz bereitstellen möchten, stellen Sie sicher, dass Sie deaktiviert über die Option HA-Bereitstellungsmodus wählen, andernfalls die Auswahl aktiviert ist. Für Produktionsnetzwerke empfiehlt Citrix immer die Bereitstellung von Instanzen im HA-Modus, da das Netzwerk vor Ausfällen der Instanz geschützt wird.

Create Citrix SD-WAN Standa... X

1 Basics Done ✓

2 Administrator settings Configure deployment settings >

3 SDWAN settings Configure Netscaler SD-WAN a... >

4 SDWAN Route settings Configure the route settings >

Administrator settings □ X

* Virtual Machine name ⓘ
SDWSEA ✓

HA Deployment Mode ⓘ
Enabled Disabled

* Username ⓘ
ctsdwadmin ✓

* Password ⓘ
..... ✓

* Confirm password
..... ✓

5. Wählen Sie auf der **SD-WAN-Einstellungsseite** die Instanz aus, in der Sie das Image ausführen möchten. Wählen Sie den folgenden Instanz-Typ gemäß Ihrer Anforderung:

- Instanztyp D3_V2 für maximalen unidirektionalen Durchsatz von 200 Mbit/s mit direkter Konnektivität zu maximal 16 Zweigen.
- Instanztyp D4_V2 für maximalen unidirektionalen Durchsatz von 500 Mbit/s mit direkter Konnektivität zu maximal 16 Zweigen.
- Instanztyp F8 Standard für maximalen unidirektionalen Durchsatz von 1 Gbit/s mit direkter Konnektivität zu maximal 64 Zweigen.
- Instanztyp F16 Standard für maximalen unidirektionalen Durchsatz von 1 Gbit/s mit direkter Konnektivität zu maximal 128 Zweigen.

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function Apps

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing

Help + support

Home > Marketplace > Citrix SD-WAN 10.2 > Create Citrix SD-WAN 10.2 > SDWAN Settings > Choose a size

SDWAN Settings

* Virtual machine size ⓘ
1x Standard D3 v2

* Virtual networks ⓘ
(new) vnet

Subnets ⓘ
Configure subnets

Choose a size

Search

Compute type
Current generation

Disk type
All disk types

vCPUs
1 128

RECOMMENDED

SKU

TYPE

COMPUTE

VCPUS

GB RAM

DATA DISKS

MAX IOPS

LOCAL SSD

PREMIUM

ADDITIONAL

USD/MON

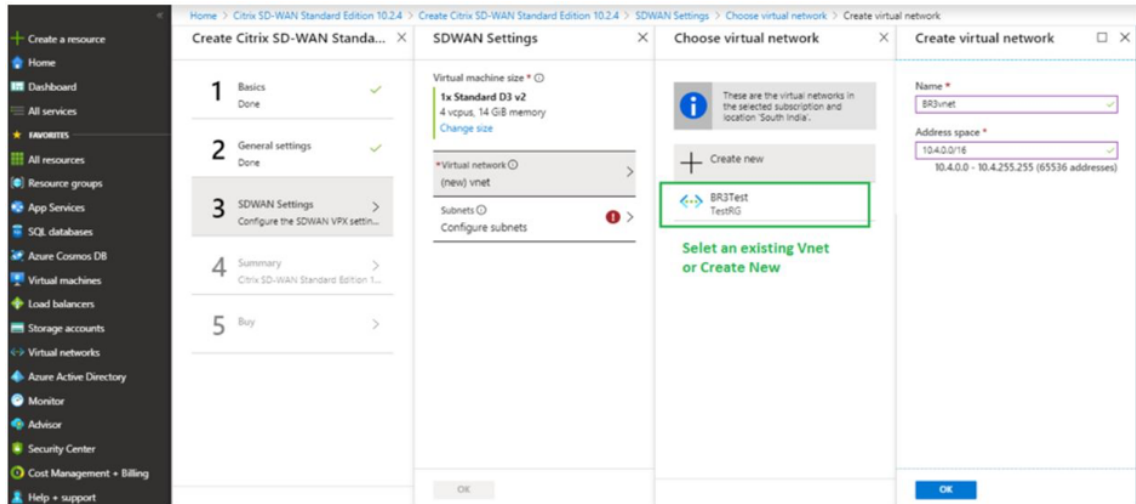
Available

| | | | | | | | | | | |
|---|-------|----------|-----------------|----|----|----|--------|--------|----|----------|
| ★ | D3_v2 | Standard | General purpose | 4 | 14 | 16 | 16x500 | 200 GB | No | \$209.06 |
| ★ | D4_v2 | Standard | General purpose | 8 | 28 | 32 | 32x500 | 400 GB | No | \$415.13 |
| ★ | F8 | Standard | Compute optim | 8 | 16 | 32 | 32x500 | 128 GB | No | \$282.72 |
| | F16 | Standard | Compute optim | 16 | 32 | 64 | 64x500 | 256 GB | No | \$565.44 |

Prices presented are estimates in your local currency that include Azure infrastructure applicable software costs, as well as any discounts for the subscription and location. Final charges will appear in your local currency in cost analysis and billing views. If you purchased Azure services through a reseller, contact your reseller for full pricing details. Recommended sizes are determined by the publisher of the selected image based on hardware and software requirements.

OK Select

6. Erstellen Sie ein neues virtuelles Netzwerk (VNet) oder verwenden Sie ein vorhandenes VNet. Dies ist der wichtigste Schritt für die Bereitstellung, da in diesem Schritt die Subnetze ausgewählt werden, die den Schnittstellen der SD-WAN VPX-VM zugewiesen werden sollen.



Das Aux-Subnetz wird nur benötigt, wenn Sie die Instanzen im HA-Modus bereitstellen. Stellen Sie sicher, dass die SD-WAN-Instanz im selben VNet wie Ihre Citrix Virtual Apps and Desktops-Ressourcen bereitgestellt wird und sich im selben Subnetz wie die LAN-Schnittstelle der SD-WAN VPX-Appliance befindet.

SDWAN Settings

Virtual machine size * ⓘ
1x Standard D3 v2
4 vcpus, 14 GiB memory
[Change size](#)

*Virtual network ⓘ
(new) BR3vnet

Subnets ⓘ
Configure subnets ⓘ

OK

Subnets

Manangement subnet name *
snet-mgmt ✓

Manangement subnet address prefix *
10.4.0.0/24 ✓

LAN subnet name *
snet-lan ✓

LAN subnet address prefix *
10.4.1.0/24 ✓

WAN subnet name *
snet-wan ✓

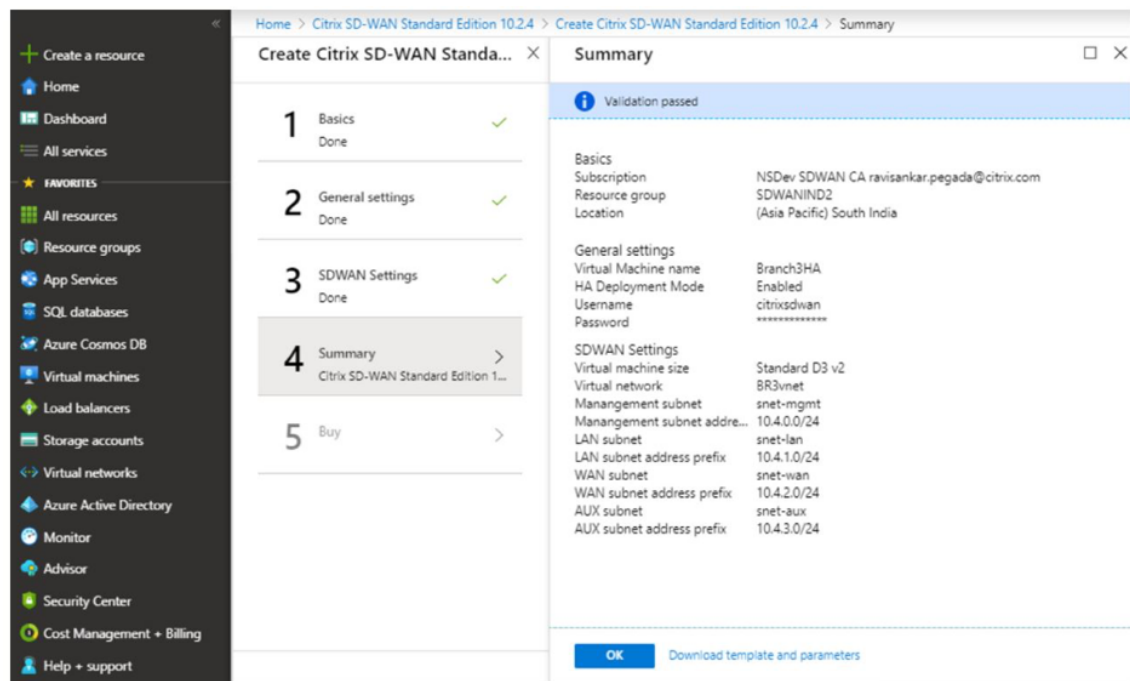
WAN subnet address prefix *
10.4.2.0/24 ✓

AUX subnet name *
snet-aux ✓

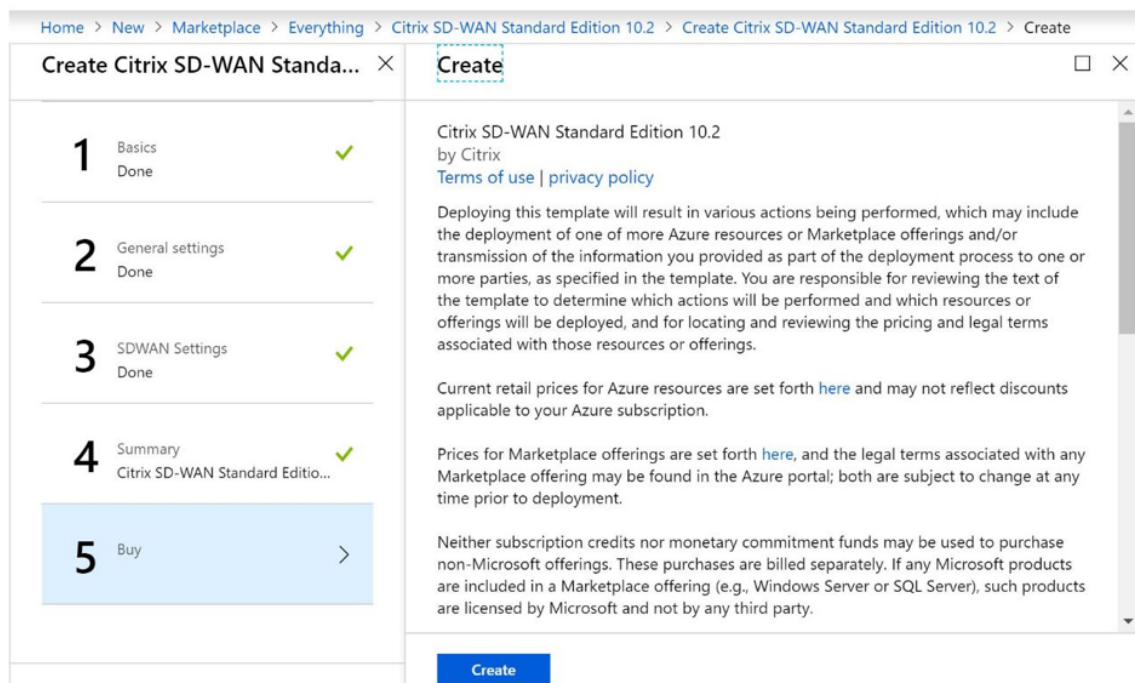
AUX subnet address prefix *
10.4.3.0/24 ✓

OK

7. Überprüfen Sie die Konfiguration auf der **Zusammenfassungsseite** und klicken Sie auf **OK**.



8. Klicken Sie auf der Seite **Kaufen auf Erstellen**, um den Bereitstellungsprozess für die Instanzen zu starten. Es kann etwa 10 Minuten dauern, bis die Instanz bereitgestellt wird. Sie erhalten eine Benachrichtigung im Azure-Verwaltungsportal, in der der Erfolg/Fehler bei der Instanzerstellung vorgeschlagen wird.



Nachdem die Instanz erfolgreich erstellt wurde, rufen Sie die öffentliche IP ab, die der Verwaltungsschnittstelle der SD-WAN-Instanz zugewiesen ist. Sie finden sie unter dem Netzwerkab-

schnitt der Ressourcengruppe, in der die Instanz bereitgestellt wurde. Nach dem Abrufen können Sie es verwenden, um sich bei der Instanz anzumelden.

HINWEIS

Für den Admin-Zugriff lautet der Benutzername **admin** und das Kennwort, das Sie während der Instanzerstellung festgelegt haben.

9. Sobald die Site bereitgestellt wurde, melden Sie sich bei SD-WAN Orchestrator an, um sie zu konfigurieren. Wie in den Voraussetzungen erwähnt, müssen Sie über die Berechtigung für SD-WAN Orchestrator verfügen, um die Site zu konfigurieren. Wenn Sie es noch nicht haben, lesen Sie weiter [Onboarding von Citrix SD-WAN Orchestrator](#).
10. Wenn Sie bereits über ein SD-WAN-Netzwerk verfügen, fahren Sie mit der Erstellung der Konfiguration für die Site fort, die Sie in Azure bereitgestellt haben. Andernfalls müssen Sie ein MCN erstellen. Weitere Informationen finden Sie unter [Netzwerkkonfiguration](#).
11. Sobald Sie Zugriff auf SD-WAN Orchestrator haben und bereits einen MCN eingerichtet haben, melden Sie sich bei SD-WAN Orchestrator an und klicken Sie auf **+Neue Site**, um mit der Konfiguration der SD-WAN VPX Appliance zu beginnen (die Sie in Azure bereitgestellt haben).

New Site

Site Details

Site Name *

Name

Site Address *

Search for Site Address

☐ Lat/Lng

Cancel Next ➔

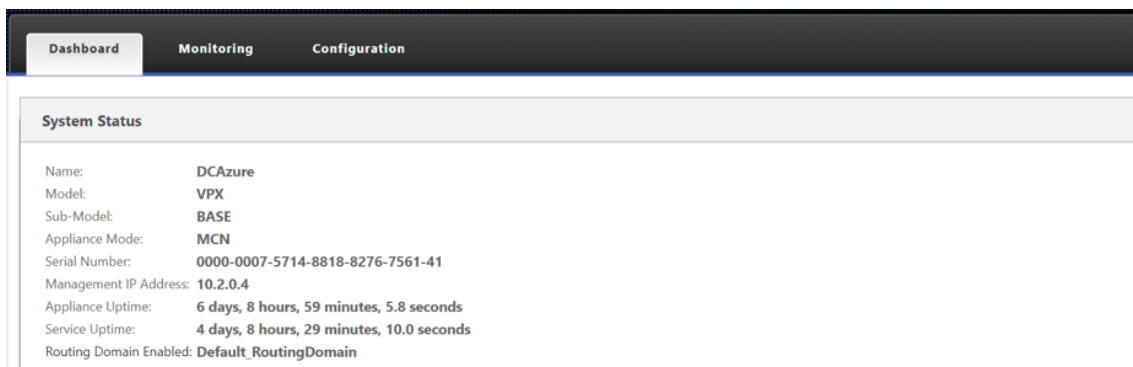
12. Geben Sie einen eindeutigen Site-Namen an, und geben Sie die Adresse basierend auf der Region ein, in der Sie das Image Provisioning. Informationen zum Einrichten der Instanz in Azure finden Sie unter [Grundeinstellungen](#).

HINWEIS

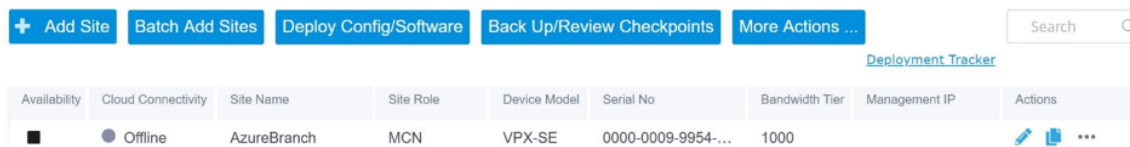
Um die Seriennummer der Instanz in Azure abzurufen, melden Sie sich über die IP der öffentlichen Verwaltung bei der Instanz an. Sie können die Seriennummer auf dem Dashboard-Bildschirm sehen. Wenn Sie Instanzen in HA konfigurieren, müssen beide Seriennummern erfasst werden. Stellen Sie außerdem beim Konfigurieren der Instanz

sicher, dass die Schnittstellen als **Vertrauenswürdig** ausgewählt werden.

13. Zum Abrufen der IP-Adressen, die mit LAN- und WAN-Schnittstellen in Azure verknüpft sind. Navigieren Sie zum **Azure-Portal > Ressourcengruppen > Ressourcengruppe**, in der das SD-WAN **bereitgestellt wird > SD-WAN VM > Networking**.



14. Sobald Sie mit der Konfiguration der Instanz fertig sind. Klicken Sie auf **Config/Software bereitstellen**, indem Sie zu **Konfiguration > Netzwerkkonfiguration Homenavigieren**.



15. Wenn es keine Probleme gibt und die Konfiguration korrekt ist, müssen Sie die virtuellen Pfade zwischen der Instanz in Azure und Ihrem MCN haben, sobald die Konfigurationsbereitstellung ausgeführt wurde.

Konfiguration von Citrix Virtual Apps and Desktops

Wie im [Bereitstellung und Konfiguration](#) Abschnitt hervorgehoben, ist das AD/DNS on-premises Standort vorhanden und fungiert als DC und in einer Bereitstellung mit SD-WAN, die hinter dem SD-WAN im LAN-Netzwerk angezeigt wird. Es ist die IP-Adresse Ihres AD/DNS, die Sie hier konfigurieren müssen. Falls Sie Azure Active Directory-Service/DNS verwenden, konfigurieren Sie **168.63.129.16** als DNS-IP.

Wenn Sie eine lokale AD/DNS verwenden, überprüfen Sie, ob Sie in der Lage sind, die IP-Adresse Ihres DNS von Ihrer SD-WAN-Appliance aus zu pingen. Sie können dies tun, indem Sie zu **Problembehandlung > Diagnosen** navigieren. Aktivieren Sie das Kontrollkästchen **Ping** und initiieren Sie einen Ping von der LAN-Schnittstelle/Standardschnittstelle der SD-WAN-Appliance zur IP Ihrer AD/DNS.

The screenshot shows the Citrix Cloud SD-WAN Orchestrator interface. The top navigation bar includes the Citrix Cloud logo and SD-WAN Orchestrator. Below the navigation bar, there's a breadcrumb trail: Customer cloudDNATest / Site All Sites. The left sidebar contains navigation links: Dashboard, Reports, Configuration, Troubleshooting (with sub-links for Audit Logs, Device Logs, and Diagnostics), and Administration. The main content area is titled 'Network Troubleshooting : Diagnostics'. It features a form with the following elements:

- Checkboxes for Ping (checked), Traceroute, Packet Capture, and Bandwidth Test.
- A 'Source Site' section with a dropdown menu showing 'cDNTestCMD'.
- A 'PING' section with a dropdown menu.
- Fields for 'IP Address', 'Interface' (set to 'Default'), and 'Gateway IP (Optional)' (set to 'Default').
- Fields for 'Routing Domain' (set to 'Default_RoutingDomain') and 'Packet Size (KB)' (set to '70').

Wenn der Ping erfolgreich ist, bedeutet dies, dass Ihr AD/DNS erfolgreich erreicht werden kann. Wenn nicht, bedeutet dies, dass es ein Routing-Problem in Ihrem Netzwerk gibt, das die Erreichbarkeit Ihres AD/DNS verhindert. Versuchen Sie, wenn möglich, Ihre AD- und SD-WAN-Appliance auf demselben LAN-Segment zu hosten.

Falls es immer noch ein Problem gibt, wenden Sie sich an Ihren Netzwerkadministrator. Ohne diesen Schritt erfolgreich abzuschließen, wird der Schritt zur Katalogerstellung nicht erfolgreich sein und Sie erhalten eine Fehlermeldung, da **Global DNS IP nicht konfiguriert ist**.

HINWEIS Stellen Sie

sicher, dass das DNS sowohl interne als auch externe IPs auflösen kann.

Netzwerkstandort-Service

Mit dem Dienst **Network Location** in Citrix Cloud können Sie den internen Datenverkehr zu den Apps und Desktops optimieren, die Sie den Arbeitsbereichen der Abonnenten zur Verfügung stellen, um HDX-Sitzungen schneller zu machen. Benutzer in internen und externen Netzwerken müssen über ein externes Gateway eine Verbindung mit VDAs herstellen. Während dies für externe Benutzer zu erwarten ist, können sich interne Benutzer dadurch langsamer mit virtuellen Ressourcen verbinden. Der **Network Location-Dienst** ermöglicht es internen Benutzern, das Gateway zu Bypass und sich direkt mit den VDAs zu verbinden, wodurch die Latenz für den internen Netzwerkverkehr reduziert wird.

Konfiguration

Verwenden Sie eine der folgenden Methoden, um den **Network Location-Dienst** einzurichten:

- **Citrix SD-WAN Orchestrator:** Detaillierte Informationen zur Konfiguration von NLS mit Citrix SD-WAN Orchestrator finden Sie unter [Netzwerkstandort-Service](#).
- **PowerShell-Modul für den Netzwerkstandortdienst, das Citrix bereitstellt:** Detaillierte Informationen zur Konfiguration von NLS mit dem PowerShell-Modul finden Sie unter [PowerShell-Modul und -Konfiguration](#).

Die Netzwerkstandorte teilen sich die öffentlichen IP-Bereiche der Netzwerke, von denen Ihre internen Benutzer eine Verbindung herstellen. Wenn Abonnenten Virtual Apps and Desktops-Sitzungen über ihren Workspace starten, erkennt Citrix Cloud anhand der öffentlichen IP-Adresse des Netzwerks, von dem aus sie eine Verbindung herstellen, ob Abonnenten intern oder außerhalb des Unternehmensnetzwerks sind.

Wenn ein Abonnent sich über das interne Netzwerk verbindet, leitet Citrix Cloud die Verbindung direkt an den VDA weiter und umgeht Citrix Gateway. Wenn ein Abonnent eine externe Verbindung herstellt, leitet Citrix Cloud den Abonnenten erwartungsgemäß über Citrix Gateway und dann an den VDA im internen Netzwerk.

HINWEIS

Die öffentliche IP, die im Netzwerkstandortdienst konfiguriert werden muss, muss die öffentliche IP sein, die den WAN-Verbindungen zugewiesen ist.

Domänennamensystem

May 10, 2021

Domain Name System (DNS) übersetzt menschlich lesbare Domänennamen in maschinenlesbare IP-Adressen und umgekehrt. Citrix SD-WAN bietet die folgenden DNS-Funktionen:

- DNS-Proxy
- Transparente DNS-Weiterleitung

Sie können einen DNS-Proxy oder eine transparente DNS-Weiterleitung mit den folgenden beiden Arten von DNS-Diensten konfigurieren:

- **Statischer DNS-Dienst:** Interkt die DNS-Anforderungen, die an die SD-WAN-IP-Adresse bestimmt sind, und leitet sie an die angegebenen DNS-Server weiter. Sie können interne, ISP, Google oder einen anderen Open-Source-DNS-Dienst erstellen. Statischer DNS-Dienst kann auf globaler und Standortebene konfiguriert werden.

- **Dynamischer DNS-Dienst:** Interkt die DNS-Anforderungen, die an die SD-WAN-IP-Adresse bestimmt sind, und leitet sie an einen der DNS-Server um, die von den DHCP-basierten WAN-Verbindungen gelernt wurden. Wenn die WAN-Verbindung untergeht, wird ein anderer DHCP-basierter WAN-Verbindungen DNS-Server ausgewählt. Diese Funktion ist in der Bereitstellung nützlich, bei der ISPs DNS-Anforderungen nur an DNS-Server zulassen, die von ihnen gehostet werden. Dynamischer DNS-Dienst kann nur auf Standortebene konfiguriert werden. Pro Standort ist nur ein dynamischer DNS-Dienst zulässig.

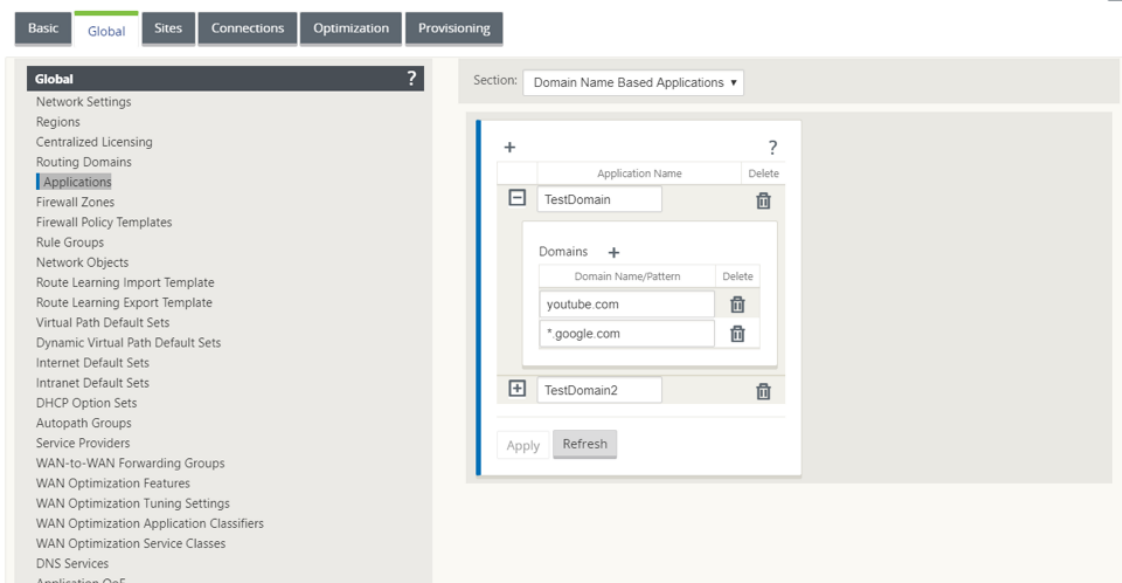
DNS-Proxy

Sie können einen Proxy mit mehreren Weiterleitungen konfigurieren, mit denen DNS-Anfragen basierend auf Anwendungsdomännennamen gesteuert werden können. Die DNS-Weiterleitung funktioniert für die Anforderungen, die über UDP-Verbindungen empfangen werden.

So konfigurieren Sie SD-WAN als DNS-Proxy:

1. Definieren Sie die auf Domännennamen basierenden Anwendungen. Navigieren Sie im Konfigurations-Editor zu **Global > Anwendungen > Domännennamen-basierte Anwendungen**.

Geben Sie den Anwendungsnamen und die erforderlichen Domännennamen oder -muster ein. Sie können mehrere Domännennamen als Anwendung gruppieren. Sie können entweder den vollständigen Domainnamen eingeben oder am Anfang Wildcards verwenden. Zum Beispiel - *.google.com



2. Definieren Sie die erforderlichen DNS-Dienste. Sie können statischen oder dynamischen DNS-Dienst definieren.

Um einen statischen DNS-Dienst zu konfigurieren, navigieren Sie zu **Global > DNS Service** und wählen Sie den **Typ** als **Statisch** aus. Geben Sie den **Dienstnamen** und ein Paar primäre und sekundäre DNS-Server-IP-Adressen ein.

| Service Name | Type | Service Type | Service Instance | Primary DNS |
|--------------|--------|--------------|------------------|-------------|
| Google | Static | | | 8.8.8.8 |

Hinweis

Wenn Sie Office 365-Breakout-Richtlinie konfiguriert haben, wird automatisch ein Quad9-DNS-Dienst erstellt. Weitere Informationen finden Sie unter [Office 365-Optimierung](#).

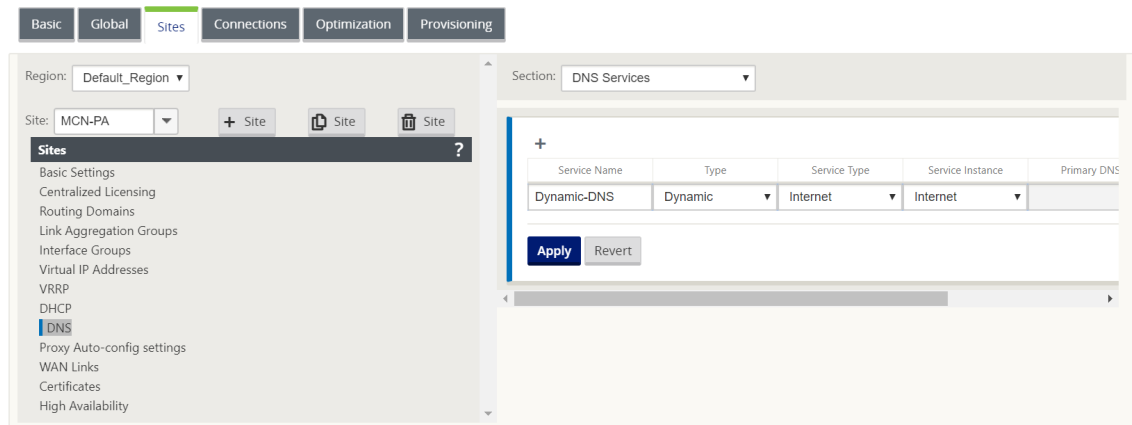
Alternativ können Sie die statischen DNS-Dienste auch auf individueller Standortebene definieren. Die Konfiguration des DNS-Dienstes auf Standortebene überschreibt die globale Konfiguration. Um den standortspezifischen statischen DNS-Dienst zu konfigurieren, navigieren Sie zu **Sites > DNS > DNS Services** und wählen Sie den **Typ** als **Statisch** aus.

| Service Name | Type | Service Type | Service Instance | Primary DNS |
|--------------|--------|--------------|------------------|---------------|
| Internal | Static | | | 172.103.3.100 |

Um einen Dynamic DNS-Dienst zu konfigurieren, navigieren Sie zu **Sites > DNS > DNS Services** und wählen Sie den **Typ** als **dynamisch** aus. Geben Sie den **Dienstnamen** ein und wählen Sie **Internet** als **Diensttyp** und **Dienstinstanz** aus.

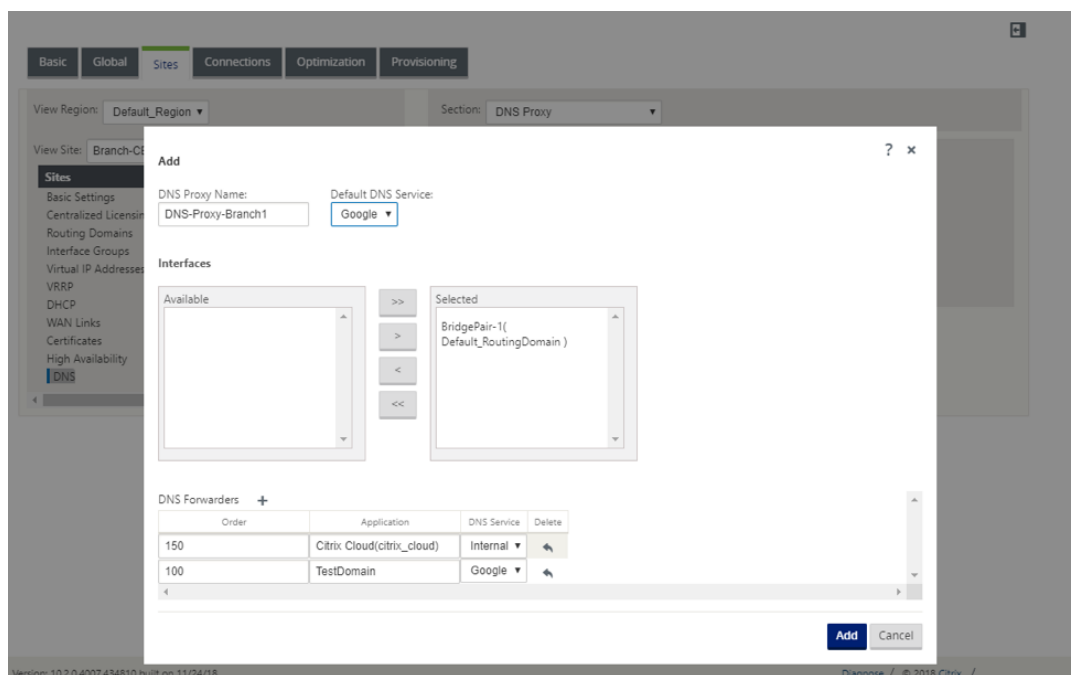
Hinweis

Dynamischer DNS-Dienst kann nur auf Standortebene konfiguriert werden. Pro Standort ist nur ein dynamischer DNS-Dienst zulässig.



3. Konfigurieren Sie den DNS-Proxy für die Site. Navigieren Sie zu **Sites > DNS > DNS Proxy**. Klicken Sie auf **+**. Geben Sie Werte für die folgenden Parameter ein:

- **DNS-Proxyname:** Name des DNS-Proxy.
- **Standard-DNS-Dienst:** Der Standard-DNS-Dienst, an den die DNS-Anfragen weitergeleitet werden, wenn keine der Anwendungen im DNS-Forwarder-Lookup übereinstimmt.
- **Interfaces:** Die Schnittstellen, auf denen die DNS-Anfragen abgefangen werden. Nur vertrauenswürdige Schnittstellen sind zulässig.
- **DNS-Weiterleitungen:** Liste der DNS-Weiterleitungen.
 - **Auftrag:** Die Priorität der Weiterleitung.
 - **Anwendung:** Anwendungen, für die DNS-Anfragen an den ausgewählten DNS-Dienst weitergeleitet werden müssen.
 - **DNS-Dienst:** Der DNS-Dienst, an den die DNS-Anfragen für die angegebene Anwendung weitergeleitet werden.

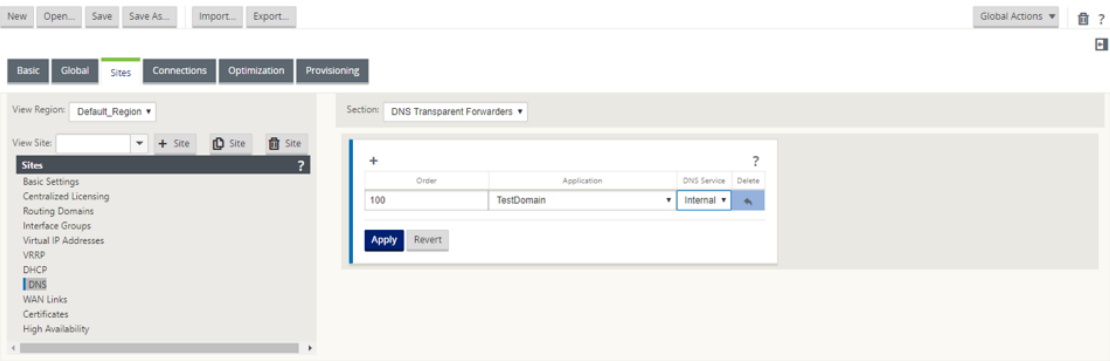


Transparente DNS-Weiterleitung

Citrix SD-WAN kann als transparente DNS-Weiterleitung konfiguriert werden. In diesem Modus kann SD-WAN DNS-Anforderungen abfangen, die nicht an seine IP-Adresse bestimmt sind, und sie an den angegebenen DNS-Dienst weiterleiten. Nur die DNS-Anforderungen, die vom lokalen Dienst auf vertrauenswürdigen Schnittstellen stammen, werden abgefangen. Wenn die DNS-Anforderungen mit Anwendungen in der DNS-Weiterleitungsliste übereinstimmen, wird sie an den konfigurierten DNS-Dienst weitergeleitet. Die DNS-Weiterleitung wird nur für Anforderungen unterstützt, die über UDP-Verbindungen kommen.

So konfigurieren Sie SD-WAN als transparente DNS-Weiterleitung:

1. Navigieren Sie zu **Websites > DNS > Transparente DNS-Weiterleitungen**. Klicken Sie auf **+**.
2. Geben Sie Werte für die folgenden Parameter ein:
 - **Auftrag:** Die Priorität der Weiterleitung.
 - **Anwendung:** Anwendungen, für die DNS-Anfragen an den ausgewählten DNS-Dienst weitergeleitet werden müssen.
 - **DNS-Dienst:** Der DNS-Dienst, an den die DNS-Anfragen für die angegebene Anwendung weitergeleitet werden.



Ebenso fügen Sie bei Bedarf weitere transparente DNS-Weiterleitungen hinzu.

3. Klicken Sie auf **Übernehmen**.

Überwachen

Um Proxystatistiken und Transparente Weiterleitungsstatistiken anzuzeigen, navigieren Sie zu **Überwachung > DNS**.

Sie können den Anwendungsnamen, den DNS-Dienstnamen, den DNS-Dienststatus und die Anzahl der Zugriffe auf den DNS-Dienst anzeigen.

Proxystatistik

| Dashboard | Monitoring | Configuration |
|----------------------|------------------|---------------|
| Statistics | Monitoring > DNS | |
| Flows | | |
| Routing Protocols | | |
| Firewall | | |
| IKE/IPsec | | |
| ICMP | | |
| Performance Reports | | |
| Qos Reports | | |
| Usage Reports | | |
| Availability Reports | | |
| Appliance Reports | | |
| DHCP Server/Relay | | |
| VRRP | | |
| PPPoE | | |
| DNS | | |

DNS Statistics

Refresh

Proxy Statistics

Search:

| Proxy Name | Application Name | DNS Service Name | DNS Service Active | Hits |
|------------|--------------------|------------------|--------------------|------|
| DNS_Proxy1 | office365_optimize | Quad9 | YES | 2 |
| DNS_Proxy1 | office365_allow | Quad9 | YES | 8 |
| DNS_Proxy1 | office365_default | Quad9 | YES | 6 |
| DNS_Proxy1 | Any | Google | YES | 17 |

Showing 1 to 4 of 4 entries

Transparent Forwarder Statistics

Search:

| Application Name | DNS Service Name | DNS Service Active | Hits |
|--------------------|------------------|--------------------|------|
| office365_allow | Quad9 | YES | 0 |
| office365_default | Quad9 | YES | 0 |
| office365_optimize | Quad9 | YES | 0 |

Showing 1 to 3 of 3 entries

Transparente Weiterleitungsstatistiken

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

| Proxy Name | Application Name | DNS Service Name | DNS Service Active | Hits |
|------------------------------|------------------|------------------|--------------------|------|
| No Proxy Stats at this time. | | | | |
| Showing 0 to 0 of 0 entries | | | | |

Transparent Forwarder Statistics

Search:

| Application Name | DNS Service Name | DNS Service Active | Hits |
|--------------------|------------------|--------------------|------|
| SocialMedia | Google | YES | 5 |
| OnlineShopping | Google | YES | 2 |
| office365_optimize | Quad9 | YES | 1 |
| office365_default | Quad9 | YES | 11 |
| office365_allow | Quad9 | YES | 8 |

Showing 1 to 5 of 5 entries

DHCP-Server und DHCP-Relay

May 10, 2021

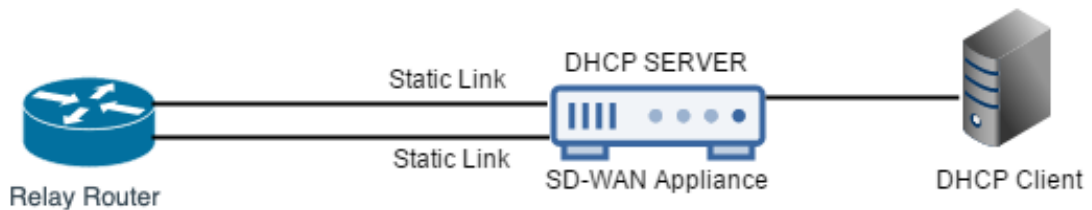
Citrix SD-WAN bietet die Möglichkeit, Standard- oder Premium Edition-Appliances entweder als DHCP-Server oder DHCP-Relay-Agents zu verwenden. Mit der DHCP-Serverfunktion können Geräte im gleichen Netzwerk wie die LAN/WAN -Schnittstelle der SD-WAN-Appliance ihre IP-Konfiguration von der SD-WAN-Appliance abrufen. Mit der DHCP-Relayfunktion können Ihre SD-WAN-Appliances DHCP-Pakete zwischen DHCP-Client und Server weiterleiten.

Im Folgenden sind die Vorteile der Verwendung der DHCP-Server- und DHCP-Relay-Funktionen aufgeführt:

- Reduzieren Sie die Anzahl der Geräte am Kundenstandort.
- Ersetzen des Routers am Client-Standort (Einfache Bereitstellung von Edge-Router-Diensten).
- Vereinfachen Sie das Clientstandsnetzwerk.
- Konfiguration des Routers ohne CLI-Befehle.
- Reduzieren Sie die manuelle Konfiguration auf einfachen Client-Sites.

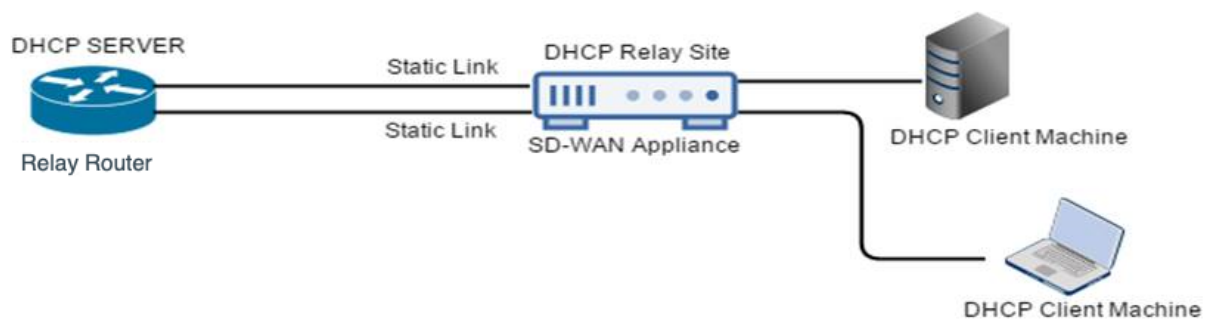
DHCP-Server

Citrix SD-WAN-Appliances können als DHCP-Server konfiguriert werden. Es kann IP-Adressen von angegebenen Adresspools innerhalb des Netzwerks DHCP-Clients zuweisen und verwalten. Der DHCP-Server kann so konfiguriert werden, dass weitere Parameter wie die IP-Adresse des DNS-Servers (Domain Name System) und des Standard-Routers zugewiesen werden. Der DHCP-Server akzeptiert Adressenzuweisungsanforderungen und Verlängerungen. Der DHCP-Server akzeptiert auch Übertragungen von lokal angeschlossenen LAN-Segmenten oder von DHCP-Anforderungen, die von anderen DHCP-Relay-Agents im Netzwerk weitergeleitet werden.



DHCP-Relais

Ein DHCP-Relay-Agent ist ein Host oder Router, der DHCP-Pakete zwischen Clients und Servern weiterleitet. Netzwerkadministratoren können den DHCP-Relay-Dienst der SD-WAN-Appliances verwenden, um Anfragen und Antworten zwischen lokalen DHCP-Clients und einem entfernten DHCP-Server weiterzuleiten. Es ermöglicht lokalen Hosts, dynamische IP-Adressen vom Remote-DHCP-Server zu erfassen. Der Relay-Agent empfängt DHCP-Nachrichten und generiert eine neue DHCP-Nachricht, die auf einer anderen Schnittstelle gesendet wird.



Konfigurieren von DHCP-Server und DHCP-Relay

May 10, 2021

Konfigurieren von DHCP-Server und DHCP-Relay mit dem Konfigurationseditor

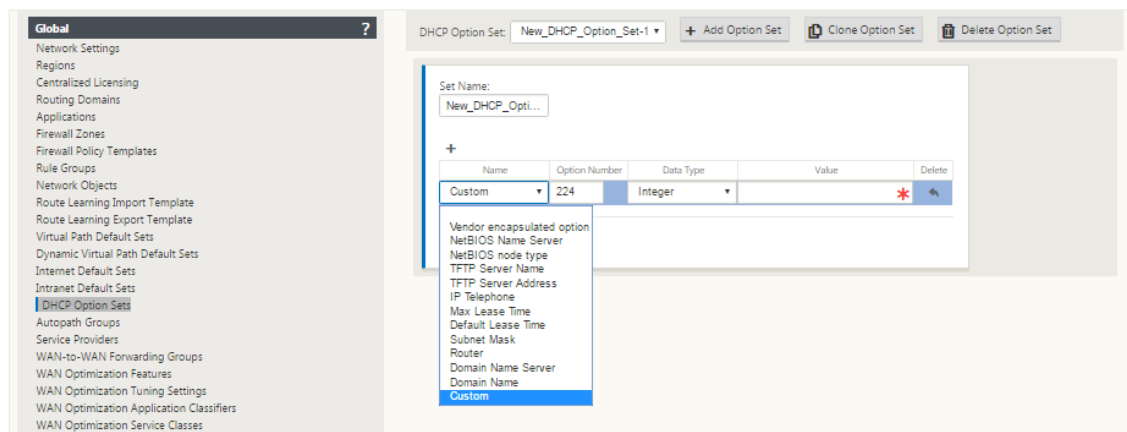
Sie können die DHCP-Server- und DHCP-Relay-Einstellungen für die Appliances im Netzwerk mithilfe des Konfigurations-Editors konfigurieren. Die Konfiguration wird über den Änderungsverwaltungsprozess an die Appliances im SD-WAN-Netzwerk übertragen.

So konfigurieren Sie einen Standort mit dem Konfigurationseditor als DHCP-Server:

1. Navigieren Sie zu **Konfigurations-Editor > Standorte > [Sitenamen] > DHCP > Server-Subnetze**. Klicken Sie auf **+**.
2. Wählen Sie eine konfigurierte Routingdomäne aus, wenn mehrere Domänen vorhanden sind.
3. Wählen Sie die **virtuelle Schnittstelle** aus, die zum Empfangen der DHCP-Anforderungen verwendet werden soll. Das IP-Subnetz, das vom DHCP-Server zur Bereitstellung von Adressen verwendet wird, wird automatisch ausgefüllt.
4. Geben Sie den **Domännennamen**, den **primären DNS** und den **sekundären DNS** ein. Der DHCP-Server leitet diese Informationen an die Clients weiter.
5. Klicken Sie auf **Aktivieren**, um das Subnetz zu aktivieren.
6. Konfigurieren Sie dynamische IP-Adresspools, die zum Zuweisen von IP-Adressen zu Clients verwendet werden. Geben Sie die Start- und Endadresse des Bereichs an, und wählen Sie den **Optionssatz** aus.

Hinweis

Die DHCP-Optionssätze sind Gruppen von DHCP-Einstellungen, die auf einzelne IP-Adressbereiche angewendet werden können. Um DHCP-Optionssätze zu erstellen, navigieren Sie zu **Global > DHCP-Optionssätze**. Wählen Sie die erforderlichen DHCP-Optionen aus, und geben Sie einen Wert dafür an.



7. Konfigurieren Sie einzelne Hosts, für die eine feste IP-Adresse basierend auf der MAC-Adresse erforderlich ist. Wählen Sie die **feste IP-Adresse**, die **MAC-Adresse** und den **Optionssatz** aus.

| Ranges + | | | | |
|----------------|----------------|--------------|---------------------|--------|
| Range Start IP | Range End IP | Gateway IP | Option Set | Delete |
| 10.200.247.200 | 10.200.247.205 | 10.200.247.1 | New DHCP Option Set | |

| Hosts + | | | |
|------------------|-------------------|------------|--------|
| Fixed IP Address | MAC Address | Option Set | Delete |
| 10.200.247.206 | 1a:0a:45:14:e1:52 | <None> | |

Hinweis

Bei festen IP-Adressen wird die **Gateway-IP** durch Konfigurieren der **Router-Option** im **DHCP-Optionssatz festgelegt**.

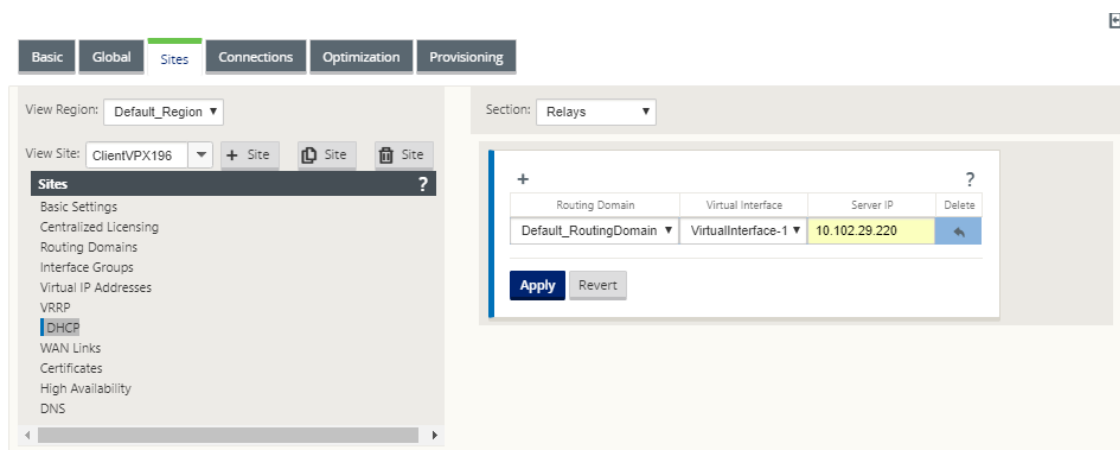
So konfigurieren Sie einen Standort mit dem Konfigurationseditor als DHCP-Relay:

1. Navigieren Sie zu **Konfigurations-Editor > Standorte Site Name[Site name] > DHCP > Relays**. Klicken Sie auf **+**.

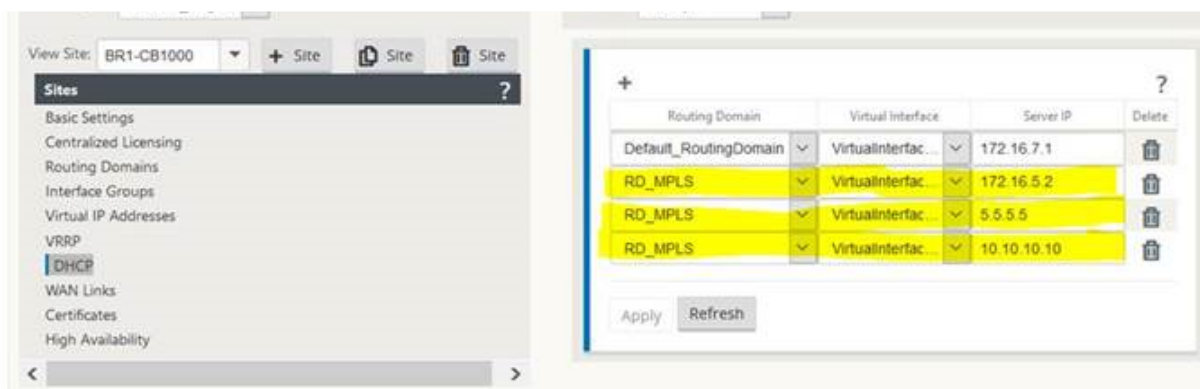
Hinweis:

Sie können maximal 16 DHCP-Relays konfigurieren.

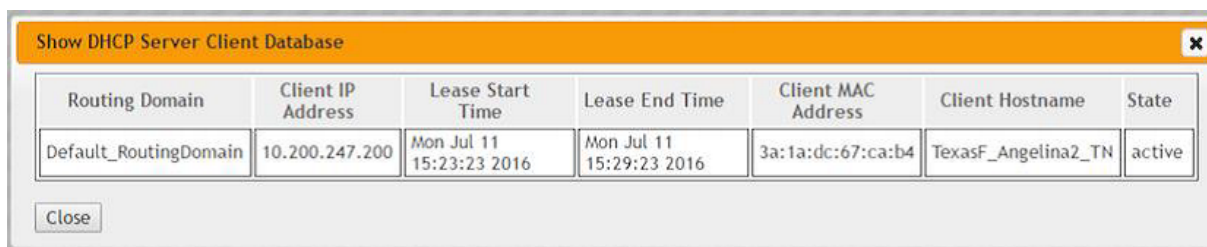
2. Wählen Sie eine konfigurierte Routingdomäne aus, wenn mehrere Domänen vorhanden sind.
3. Wählen Sie eine virtuelle Schnittstelle aus, die mit einem Remote-DHCP-Server kommuniziert.
4. Geben Sie die DHCP-Server-IP ein, mit der das Relay die Anforderung und Antwort von den Clients weiterleitet.



Sie können ein einzelnes DHCP-Relay über eine gemeinsame virtuelle Netzwerkschnittstelle konfigurieren und auf mehrere DHCP-Server verweisen.



Um eine Liste der Clients aus der DHCP-Serverdatenbank anzuzeigen, navigieren Sie in der Webverwaltungsschnittstelle zu **Monitor > DHCP-Server/Relay**.



Konfigurieren einer SD-WAN-Appliance als DHCP-Server oder DHCP-Relay mithilfe von Appliance-Einstellungen

Sie können eine einzelne SD-WAN-Appliance manuell als DHCP-Server oder als DHCP-Wiedergabe auf der Seite mit den Appliance-Einstellungen konfigurieren.

So aktivieren Sie den DHCP-Server auf einer SD-WAN-Appliance:

1. Navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter**. Suchen Sie auf der Seite **Netzwerkadapter** nach dem Bereich **Management Interface DHCP-Server**.
2. Klicken Sie auf **DHCP-Server aktivieren**, um den Server zu starten, geben Sie dann die **Lease-Zeit** (in Minuten) und den **Domännennamen** ein, und definieren Sie den **IP-Adressbereich**, indem Sie eine **Start-IP-Adresse** und eine **End-IP-Adresse** eingeben.

Hinweis

Der IP-Adresspool des Servers sollte sich innerhalb des Verwaltungsnetzwerks befinden.

| Management Interface DHCP Server | |
|--|---|
| <p>If you plan to use the DHCP Server or DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead to duplicate IP addresses on the defined management network.</p> <p>When HA switches from the Active to the Standby Citrix Appliance, the DHCP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working.</p> <p>The Management Interface DHCP Server will use the current Management Interface IP settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server IP range, defined by Start and End IP Address, must be valid in the Management Interface subnet.</p> | |
| DHCP Server Status: | stopped |
| Enable DHCP Server: | <input checked="" type="checkbox"/> |
| Lease Time (minutes): | <input type="text" value="1440"/> |
| Domain Name: | <input type="text" value="as-cx"/> |
| Start IP Address: | <input type="text" value="10.3.1.1"/> |
| End IP Address: | <input type="text" value="10.3.1.254"/> |
| <input type="button" value="Change Settings"/> | |

3. Klicken Sie auf **Einstellungen ändern**, um die Konfiguration des DHCP-Servers abzuschließen.

Hinweis

Wenn Sie DHCP-Server auf einer für Hochverfügbarkeit (High Availability) konfigurierten SD-WAN-Appliance verwenden möchten, konfigurieren Sie den Dienst nicht sowohl auf der aktiven als auch auf der Standby-Appliance. Dies führt zu doppelten IP-Adressen im definierten Verwaltungsnetzwerk.

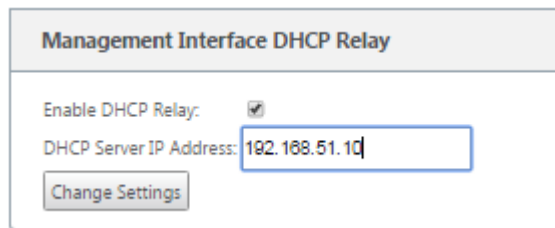
4. Klicken Sie auf **Client anzeigen**, um die aktuellen DHCP-Clients anzuzeigen, und klicken Sie auf **Clients löschen**, um die DHCP-Client-Leases freizugeben.

So aktivieren Sie den DHCP-Relay-Dienst auf einer SD-WAN-Appliance:

1. Navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter**. Suchen Sie auf der Seite **Netzwerkadapter** nach dem Bereich **DHCP-Relay der Verwaltungsschnittstelle**.
2. **Aktivieren Sie das Kontrollkästchen DHCP-Relay** aktivieren, um den Dienst zu aktivieren. Geben Sie die **IP-Adresse des DHCP-Servers** ein, und klicken Sie auf **Einstellungen ändern**, um Ihre Appliance als DHCP-Relay-Agent zu verwenden.

Hinweis

Wenn Sie den DHCP-Relaydienst auf einer Appliance verwenden möchten, die für hohe Verfügbarkeit (HA) konfiguriert ist, konfigurieren Sie den Dienst nicht sowohl auf den aktiven als auch auf den Standby-Appliances. Dies führt zu doppelten IP-Adressen im definierten Verwaltungsnetzwerk.



WAN-Link-IP-Adressen-Lernen über DHCP-Client

May 10, 2021

Citrix SD-WAN Appliances unterstützen das Lernen von WAN-Link-IP-Adressen über DHCP-Clients. Diese Funktionalität reduziert den Umfang der manuellen Konfiguration, die für die Bereitstellung von SD-WAN-Appliances erforderlich ist, und senkt die ISP-Kosten, da keine statischen IP-Adressen gekauft werden müssen. SD-WAN-Appliances können dynamische IP-Adressen für WAN-Links auf nicht vertrauenswürdigen Schnittstellen abrufen. Dadurch entfällt die Notwendigkeit, dass ein zwischengeschalteter WAN-Router diese Funktion ausführen kann.

Hinweis

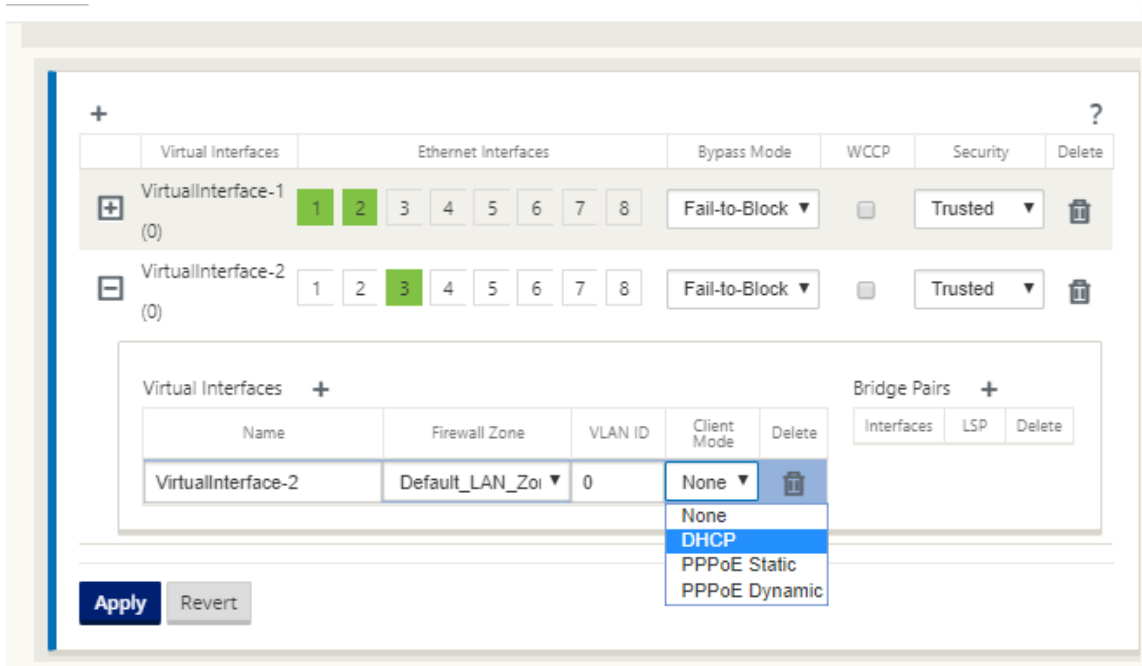
- DHCP-Client kann nur für nicht vertrauenswürdige, nicht überbrückte Schnittstellen konfiguriert werden, die als Clientknoten konfiguriert sind.
- DHCP-Client für Datenport kann nur auf Nicht-MCN/Nicht-RCN-Websites aktiviert werden.
- Die Bereitstellung von Einarm- oder Richtlinienbasiertem Routing (PBR) wird auf dem Standort mit der DHCP-Clientkonfiguration nicht unterstützt.
- DHCP-Ereignisse werden nur aus Sicht des Clients protokolliert, und es werden keine DHCP-Serverprotokolle generiert.

So konfigurieren Sie DHCP für eine nicht vertrauenswürdige virtuelle Schnittstelle im Fail-to-block-Modus:

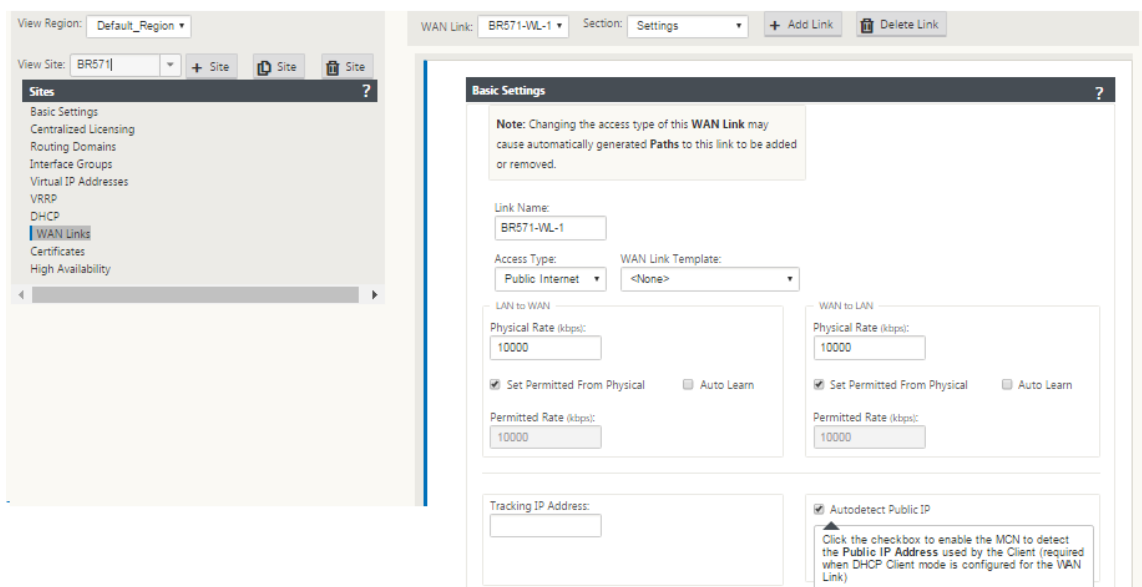
1. Wechseln Sie im **Konfigurations-Editor** zu **Sites>[Sitename]> Schnittstellengruppen> Virtuelle Schnittstellen**.

Hinweis

Die physische Schnittstelle in der Schnittstellengruppe muss ein nicht überbrücktes Paar auf einer einzigen Schnittstelle sein.



2. Wählen Sie DHCP als **Client-Modus** aus.
3. Navigieren Sie zu **WAN-Links > [WAN-Linkname] > Einstellungen > Grundeinstellungen**.
4. Aktivieren Sie das Kontrollkästchen **Öffentliche IP automatisch erkennen**, damit der MCN die vom Client verwendete öffentliche IP-Adresse erkennen kann. Dies ist erforderlich, wenn der DHCP-Clientmodus für den WAN-Link konfiguriert ist.

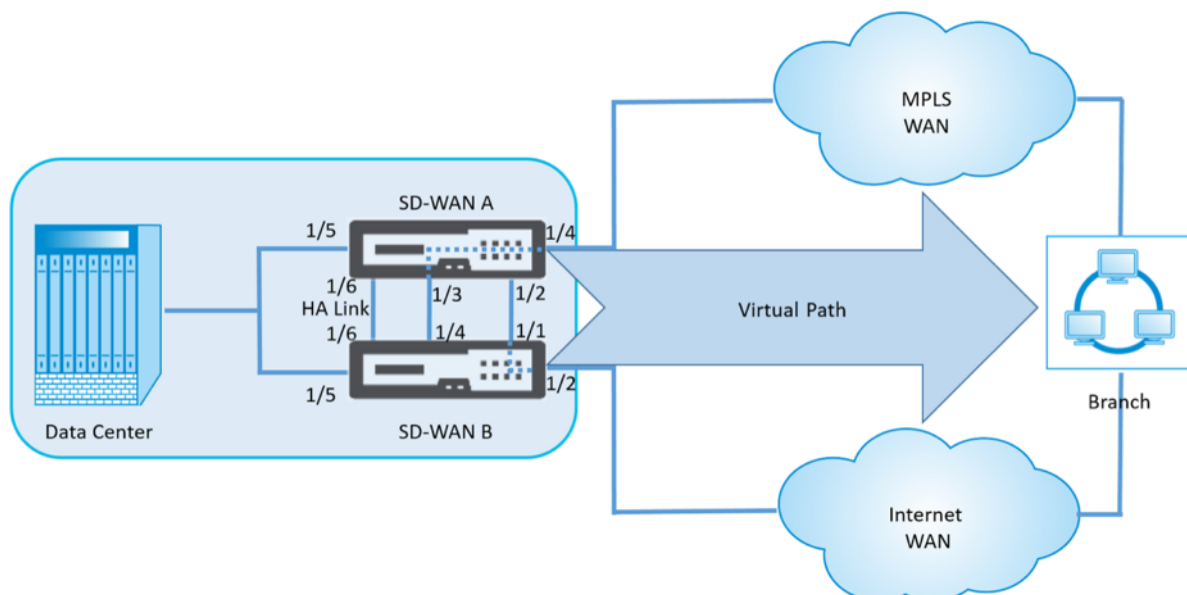


DHCP-Unterstützung für Fail-to-Wire-Port

Früher wurde der DHCP-Client nur auf Fail-to-block-Port unterstützt. Ab Version 11.2.0 wird die DHCP-Clientfunktion auf Fail-to-Wire-Port für den Zweigstandort mit serieller Hochverfügbarkeit (HA) -Bereitstellungen erweitert. Diese Erweiterung:

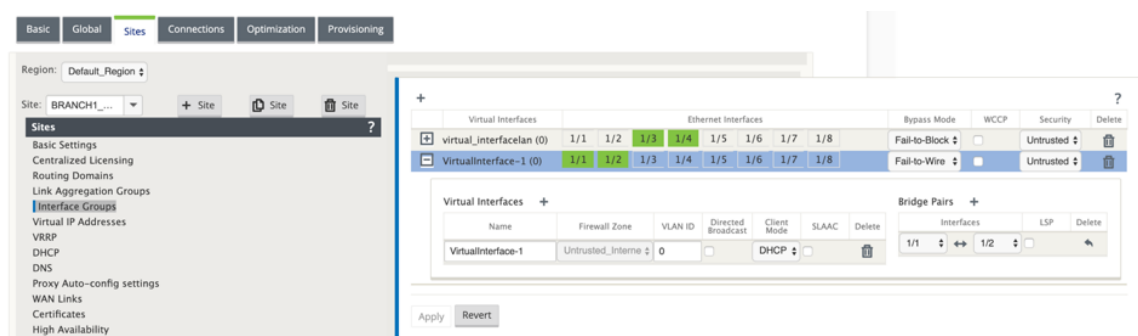
- Ermöglicht die DHCP-Clientkonfiguration für nicht vertrauenswürdige Schnittstellengruppe, die über Fail-to-Wire-Bridge-Paare und serielle HA-Bereitstellungen verfügt
- Ermöglicht die Auswahl von DHCP-Schnittstellen als Teil von **privaten Intranet-WAN-Verbindungen**.

Der DHCP-Client wird nun auf dem privaten Intranetlink unterstützt.

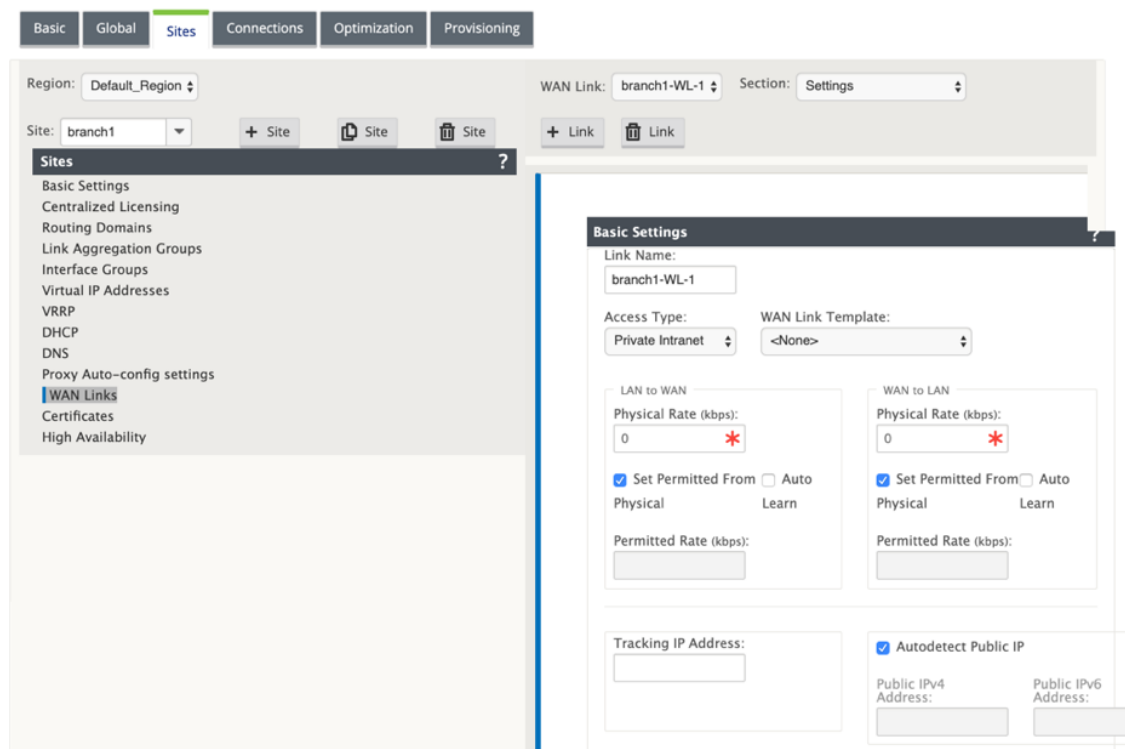


So konfigurieren Sie DHCP für eine nicht vertrauenswürdige virtuelle Schnittstelle im Fail-to-Wire-Modus:

1. Wechseln Sie im **Konfigurations-Editor** zu **Sites > [Sitename] > Schnittstellengruppen > Virtuelle Schnittstellen**.



2. Wählen Sie DHCP als **Client-Modus** und fügen Sie **Bridge-Paare** hinzu.
3. Gehen Sie zu **WAN-Links** klicken Sie auf **+** wählen Sie **WAN-Link-Name** aus der Dropdown-Liste > wählen Sie **Einstellungen** im Feld **Abschnitt > Grundeinstellungen** aus.
4. Aktivieren Sie das Kontrollkästchen **Öffentliche IP automatisch erkennen**, damit der MCN die vom Client verwendete öffentliche IP-Adresse erkennen kann. Dies ist erforderlich, wenn der DHCP-Clientmodus für den WAN-Link konfiguriert ist.



Hinweis

Eine LAN-Schnittstelle darf nicht mit dem Fail-to-Wire-Paar verbunden sein, da Pakete zwischen den Schnittstellen überbrückt werden könnten.



Überwachung von WAN-Verbindungen für DHCP-Clients

Die Laufzeit-IP-Adresse, Subnetzmaske und Gateway-Einstellungen werden protokolliert und in einer Protokolldatei namens *SDWANVW_IP_Learned.log* archiviert. Ereignisse werden generiert, wenn Dynamic Virtual IPs erlernt, freigegeben oder abgelaufen sind und wenn ein Kommunikationsproblem mit dem erlernten Gateway oder DHCP-Server vorliegt. Oder wenn doppelte IP-Adressen in der archivierten Protokolldatei erkannt werden. Wenn doppelte IPs an einem Standort erkannt werden, werden dynamische virtuelle IP-Adressen freigegeben und erneuert, bis alle virtuellen Schnittstellen am Standort eindeutige virtuelle IP-Adressen erhalten.

So überwachen Sie die WAN-Links des DHCP-Clients:

1. Auf SD-WAN-Appliance auf der Seite **Flows aktivieren/deaktivieren/löschen/löschen** enthält die Tabelle DHCP-Client-WAN-Links den Status der gelernten IPs.
2. Sie können die Verlängerung der IP beantragen, wodurch die Leasingzeit aktualisiert wird. Sie können auch die **Erneuerung freigeben**, die eine neue IP-Adresse mit einer neuen Lease ausgibt.

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 | SPWL3-Inter | 10.30.30.55/24 | 10.30.30.2 | 1800 | 1640 | 9:13 on 1/8/2016 | Renew  | Submit |
| X2 | VLAN350 | SPWL4-Inter | 10.20.20.53/24 | 10.20.20.2 | 86400 | 71035 | 4:29 on 1/9/2016 | Renew  | Submit |

Dynamische PAC-Dateianpassung

May 10, 2021

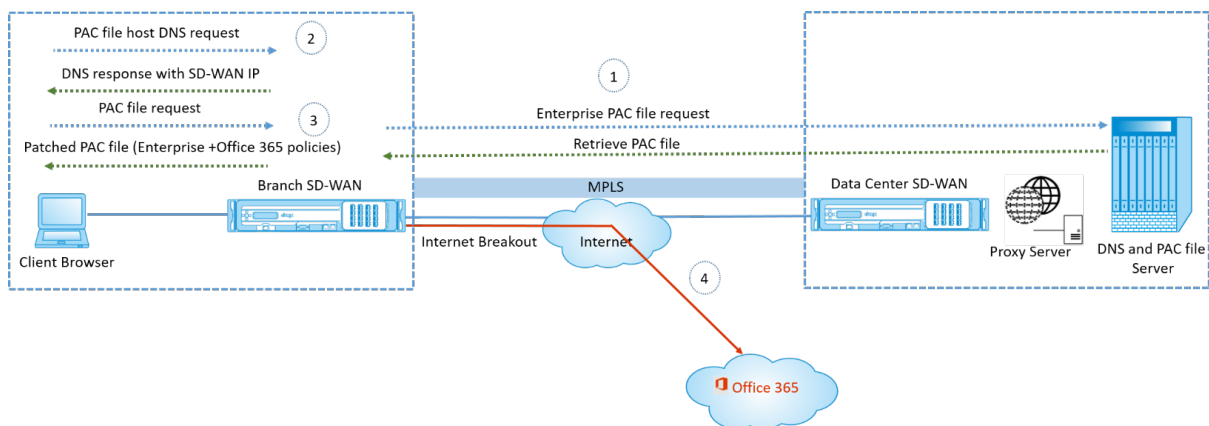
Mit der zunehmenden Einführung von unternehmenskritischen SaaS-Anwendungen und verteilten Mitarbeitern wird es äußerst wichtig, Latenz und Überlastung zu reduzieren. Latenz und Überlastung sind in traditionellen Methoden der Backhauling von Datenverkehr durch das Rechenzentrum inhärent. Citrix SD-WAN ermöglicht das direkte Internetbreakout von SaaS-Anwendungen wie Office 365. Weitere Informationen finden Sie unter [Office 365-Optimierung](#).

Wenn explizite Webproxys in der Enterprise-Bereitstellung konfiguriert sind, wird der gesamte Datenverkehr an den Web-Proxy gelenkt, was die Klassifizierung und das direkte Internetbreakout erschwert. Die Lösung besteht darin, SaaS-Anwendungsdatenverkehr durch Anpassen der PAC-Datei (Proxy Auto-Config) vom Proxy auszuschließen.

Citrix SD-WAN 11.0 ermöglicht Proxy-Umgehung und lokale Internetausbrüche für Office 365-Anwendungsdatenverkehr, indem benutzerdefinierte PAC-Dateien dynamisch generiert und bereitgestellt werden. PAC-Datei ist eine JavaScript-Funktion, die definiert, ob Webbrowser-Anforderungen direkt an das Ziel oder an einen Web-Proxy-Server gehen.

Funktionsweise der PAC-Dateianpassung

Idealerweise die PAC-Datei des Unternehmensnetzwerks auf dem internen Webserver, werden diese Proxyeinstellungen über eine Gruppenrichtlinie verteilt. Der Client-Browser fordert PAC-Dateien vom Enterprise-Webserver an. Die Citrix SD-WAN Appliance dient die angepassten PAC-Dateien für Standorte, an denen Office 365-Breakout aktiviert ist.



1. Citrix SD-WAN fordert regelmäßig die neueste Kopie der Enterprise-PAC-Datei vom Enterprise-Webserver an und ruft sie ab. Die Citrix SD-WAN Appliance patcht Office 365-URLs in die Unternehmens-PAC-Datei. Die Enterprise-PAC-Datei wird voraussichtlich einen Platzhalter (SD-WAN-spezifisches Tag) haben, in dem die Office 365-URLs nahtlos gepatcht werden.
2. Der Client-Browser löst eine DNS-Anforderung für den unternehmenseigenen PAC-Dateihost aus. Citrix SD-WAN fängt die Anforderung für den FQDN der Proxy-Konfigurationsdatei ab und antwortet mit Citrix SD-WAN VIP.
3. Der Client-Browser fordert die PAC-Datei an. Die Citrix SD-WAN Appliance bedient die gepatchte PAC-Datei lokal. Die PAC-Datei enthält Enterprise-Proxy-Konfiguration und Office 365-URL-Ausschlussrichtlinien.
4. Beim Empfang einer Anforderung für Office 365-Anwendung führt die Citrix SD-WAN Appliance ein direktes Internetbreakout durch.

Voraussetzungen

1. Die Unternehmen sollten eine PAC-Datei gehostet haben.
2. Die PAC-Datei sollte einen Platzhalter *SDWAN_TAG* oder ein Vorkommen der Funktion *findproxy-forurl* zum Patchen von Office 365-URLs haben.
3. Die PAC-Datei-URL sollte domänenbasiert und nicht IP-basiert sein.
4. Die PAC-Datei wird nur über die vertrauenswürdigen Identitäts-VIPs bereitgestellt.
5. Die Citrix SD-WAN Appliance sollte in der Lage sein, die Unternehmens-PAC-Datei über die Verwaltungsschnittstelle herunterzuladen.

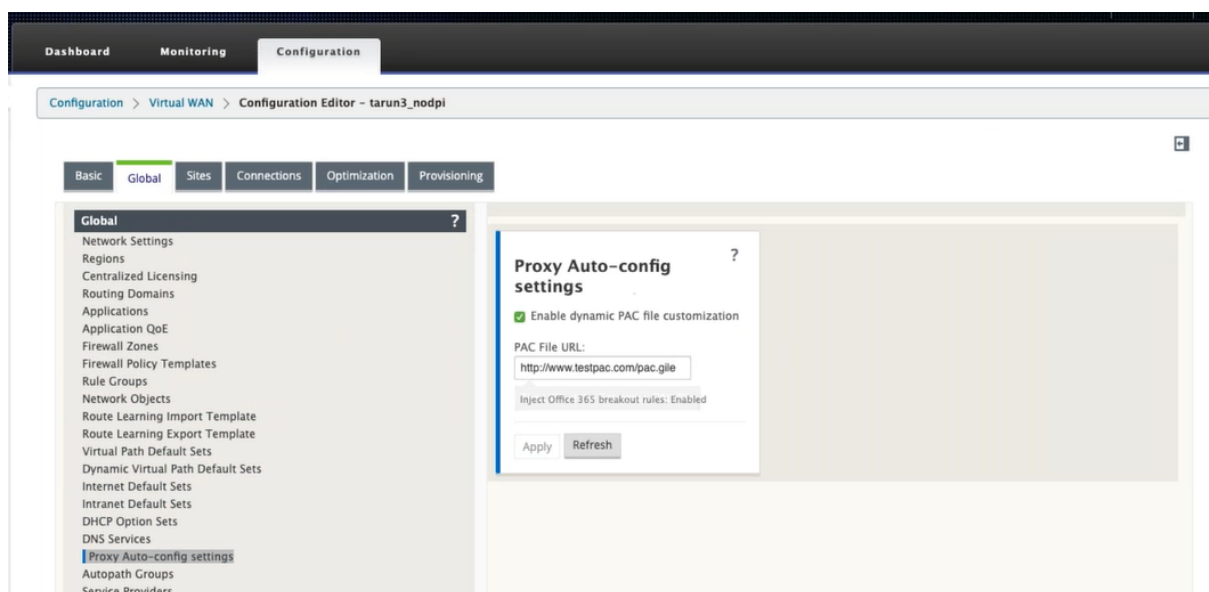
Konfiguration der PAC-Dateianpassung

Sie können die PAC-Dateianpassung global oder auf Standortebene aktivieren.

Hinweis:

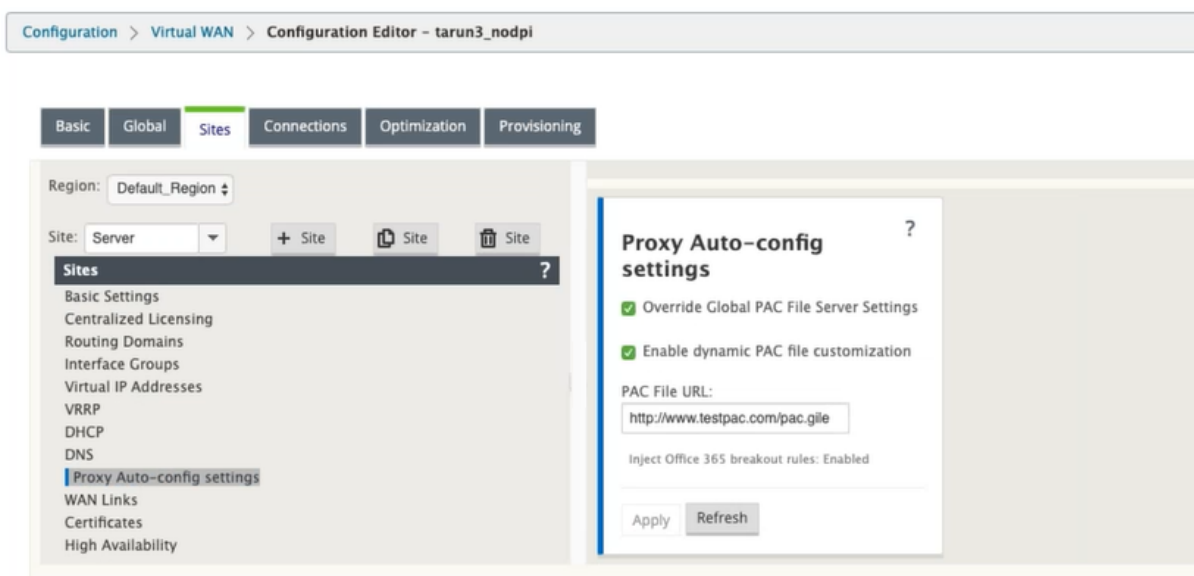
Die Office 365-Breakout-Option muss für die dynamische PAC-Dateianpassung aktiviert sein. Informationen zum Aktivieren von Office 365-Breakout finden Sie unter [Office 365-Optimierung](#).

Um die dynamische PAC-Dateianpassung global für alle Standorte zu konfigurieren, navigieren Sie im Konfigurationseditor zu **Global > Einstellungen für die automatische Proxy-Konfiguration**.



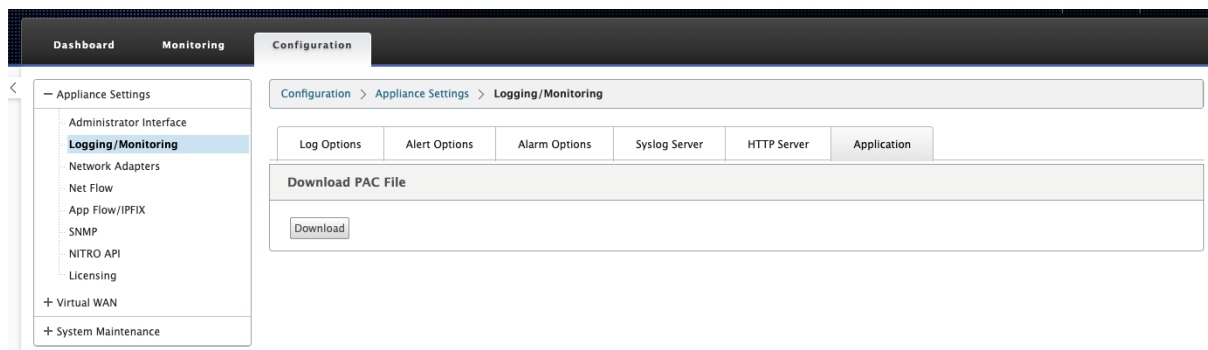
Wählen Sie **Dynamische PAC-Dateianpassung aktivieren** aus. Geben Sie im Feld **PAC-Datei-URL** die URL des Enterprise PAC-Dateiservers ein. Die Office 365-Breakout-Regeln werden dynamisch in die Enterprise-PAC-Datei gepatcht.

Um die dynamische PAC-Dateianpassung für eine Site zu konfigurieren, navigieren Sie zu **Sites > [Site] > Proxy-Autokonfigurationseinstellungen**. Sie können auch globale PAC-Dateiserver-Einstellungen außer Kraft setzen und eine andere PAC-Dateiserver-URL angeben.

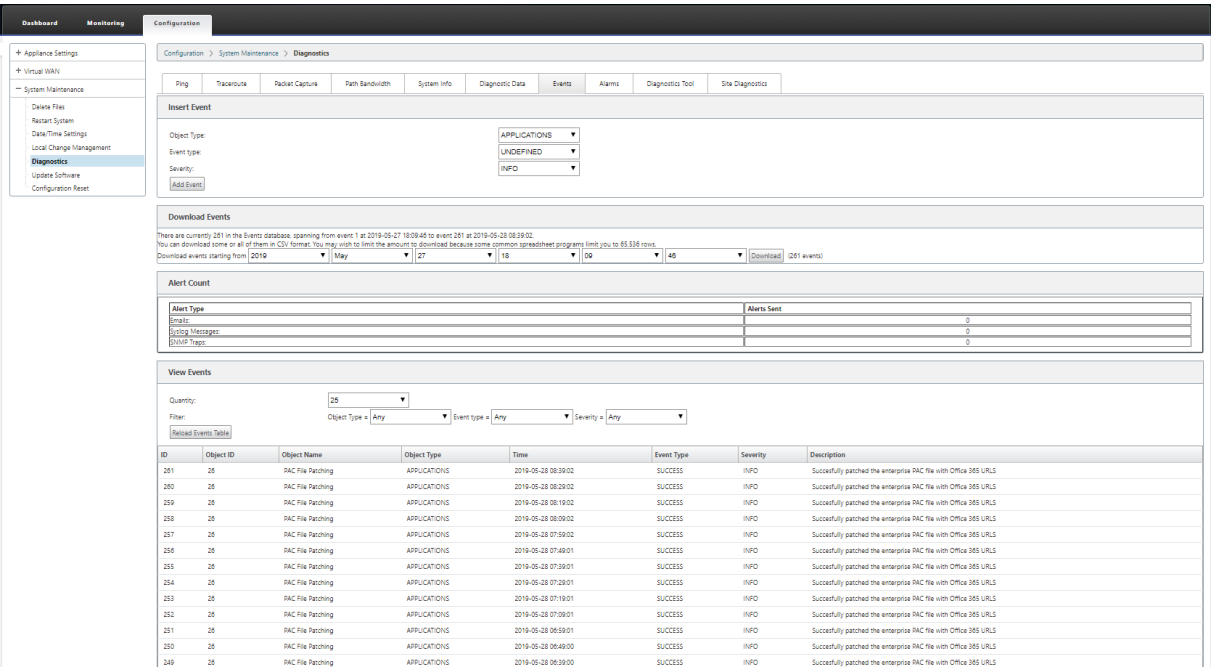


Problembehandlung

Sie können die angepasste PAC-Datei von der Citrix SD-WAN Appliance zur Fehlerbehebung herunterladen. Navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Logging/Überwachung > Anwendung**, und klicken Sie auf **Download**.



Sie können den Patch-Status der PAC-Datei auch im Abschnitt **Ereignisse** anzeigen, zu **Konfiguration > Systemwartung > Diagnose** navigieren, und klicken Sie auf die Registerkarte **Ereignisse**.



Einschränkungen

- HTTPS-PAC-Dateiserver-Anforderungen werden nicht unterstützt.
- Mehrere PAC-Dateien in einem Netzwerk werden nicht unterstützt, einschließlich PAC-Dateien für Routingdomänen oder Sicherheitszonen.
- Das Generieren von PAC-Dateien auf Citrix SD-WAN von Grund auf wird nicht unterstützt.
- WPAD über DHCP wird nicht unterstützt.

GRE Tunnel

May 10, 2021

Mit der GRE-Tunnelfunktion können Sie Citrix SD-WAN Appliances so konfigurieren, dass GRE-Tunnel im LAN oder Intranet beendet werden. Wenn Sie den Standort nicht als GRE Tunnel Terminierungsknoten konfigurieren möchten, können Sie diesen Schritt überspringen und mit dem Abschnitt [Konfigurieren der WAN-Links für die MCN-Site](#) fortfahren.

So konfigurieren Sie einen GRE Tunnel:

Klicken Sie in der Ansicht **Sites** für die neue MCN-Site auf **+** links neben dem Label **GRE Tunnel**. Die Tabelle **GRE Tunnel** für den neuen Standort wird geöffnet. Weitere Informationen finden Sie in den GRE-Themen.

Konfigurieren von GRE-Tunneln der MCN-Site.

[GRE-Tunnel für den Zweigstandort konfigurieren.](#)

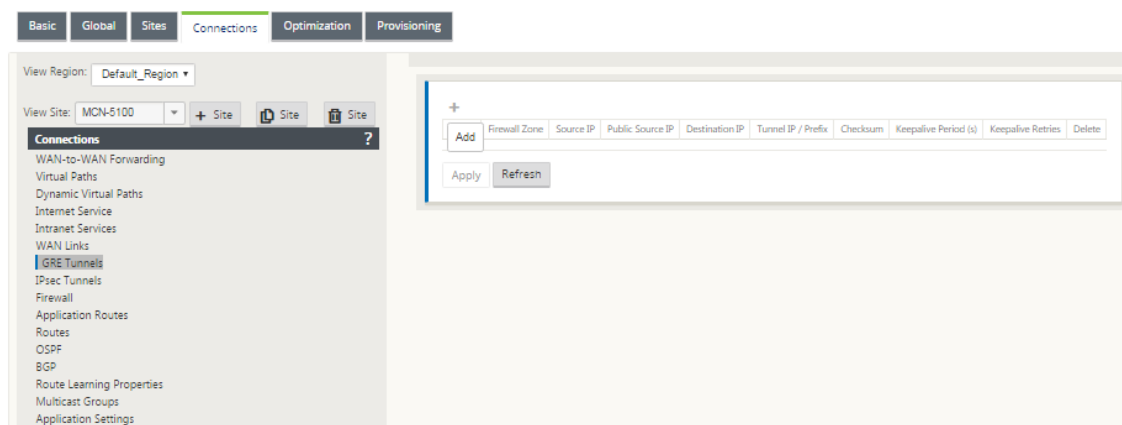
GRE-Tunnel für den MCN-Standort konfigurieren (optional)

October 28, 2021

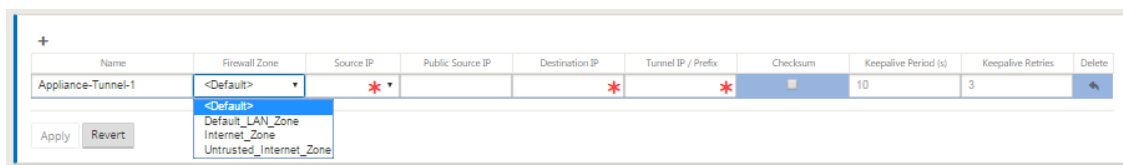
Mit der GRE-Tunnelfunktion können Sie Citrix SD-WAN Appliances so konfigurieren, dass GRE-Tunnel im LAN oder Intranet beendet werden. Wenn Sie diesen Standort nicht als GRE-Tunnel-Abschlussknoten konfigurieren möchten, können Sie diesen Schritt überspringen und mit dem Abschnitt [Konfigurieren der WAN-Links für den MCN-Site](#) fortfahren.

Gehen Sie folgendermaßen vor, um einen GRE-Tunnel zu konfigurieren:

1. Klicken Sie auf der Registerkarte Verbindungen für den neuen MCN-Site auf **GRE-Tunnel**. Dadurch wird die Tabelle **GRE Tunnel** für den neuen Standort geöffnet.



2. Klicken Sie auf **+** rechts neben den **GRE-Tunneln**. Dadurch wird der Tabelle ein neuer leerer GRE Tunnel Eintrag hinzugefügt und zur Bearbeitung geöffnet.



3. Konfigurieren Sie die GRE Tunneleinstellungen.

Geben Sie Folgendes ein:

- **Servicetyp** - Wählen Sie den Dienstyp entweder Intranet oder LAN aus der Dropdownliste aus.

- **Bezeichnung:**
 - Wenn der Dienstyp Intranet ist, wählen Sie aus der Liste der konfigurierten Intranetdienste im Dropdownmenü aus.
 - Wenn der Dienstyp LAN ist, geben Sie einen Namen für den neuen GRE-Tunnel ein, oder übernehmen Sie die Standardeinstellung.
 - Standard verwendet ein Benennungsformat **Appliance-Tunnel-*<number>*** - wobei *<number>* die Anzahl der für diese Site konfigurierten GRE-Tunnel ist, die um eins erhöht werden.
 - **Intranetdiensttyp** - Für einen Intranetdiensttyp wählen Sie **Standard** oder **ZScaler** aus der Dropdownliste.
 - **Firewall-Zone** - Wählen Sie die Dateizone für den GRE-Tunnel zu Ihnen.
 - **Quell-IP** — Wählen Sie eine Quell-IP-Adresse für den Tunnel aus dem Dropdownmenü für dieses Feld aus. Die Menüoptionen sind die Liste der für diese Site konfigurierten virtuellen Schnittstellen. Konfigurieren Sie mindestens eine virtuelle Schnittstelle, bevor Sie einen GRE Tunnel konfigurieren können. Anweisungen finden Sie unter [Konfigurieren der virtuellen Schnittstellengruppen für die MCN-Site](#) und [Konfigurieren der virtuellen IP-Adressen für die MCN-Site](#).
 - **Public Source IP:** Geben Sie die IP-Adresse ein, die als Quelladresse für Pakete im GRE-Tunnel verwendet werden soll. Die Quell-IP-Adresse ist der Ausgangspunkt des GRE-Tunnels.
 - **Ziel-IP** — Geben Sie die IP-Adresse ein, die als Host-Ziel verwendet werden soll. Die Ziel-IP-Adresse ist der Endpunkt des GRE-Tunnels.
 - **Tunnel IP/ Präfix** — Geben Sie die IP-Adresse und das Präfix ein, die für die GRE-Tunnelschnittstelle verwendet werden.
 - **Prüfsumme** — Wählen Sie das Feld **Prüfsumme** aus, um Prüfsumme für den GRE-Header des Tunnels zu
 - **Keepalive-Zeitraum** — Geben Sie das Wartezeitintervall (in Sekunden) zwischen Keepalive-Nachrichten ein. Wenn auf 0 konfiguriert, werden keine Keepalive-Pakete gesendet, aber der Tunnel bleibt oben. Der Standardwert ist 10.
 - **Keepalive-Wiederholungen** — Geben Sie die Anzahl der Keepalive-Wiederholungen ein, die die Virtual WAN Appliance versuchen muss, bevor sie den Tunnel zum Fall bringt. Der Standardwert ist 3 Tage.
4. Klicken Sie auf **Apply**. Dadurch werden Ihre Einstellungen übermittelt und der neue GRE Tunnel zur Tabelle hinzugefügt.

| Name | Firewall Zone | Source IP | Public Source IP | Destination IP | Tunnel IP / Prefix | Checksum | Keepalive Period (s) | Keepalive Retries | Delete |
|--------------------|----------------|--------------|------------------|----------------|--------------------|----------|----------------------|-------------------|--------|
| Appliance-Tunnel-1 | Default_LAN_Zo | 192.113.59.5 | 192.113.59.6 | 10.199.81.237 | 10.199.106.2/20 | x | 10 | 3 | |

- Um weitere GRE-Tunnel zu konfigurieren, klicken Sie auf **+** rechts neben den **GRE-Tunneln** und fahren Sie wie in den vorherigen Schritten fort.

Der nächste Schritt besteht darin, die [WAN-Verbindungen für die MCN-Site zu konfigurieren](#).

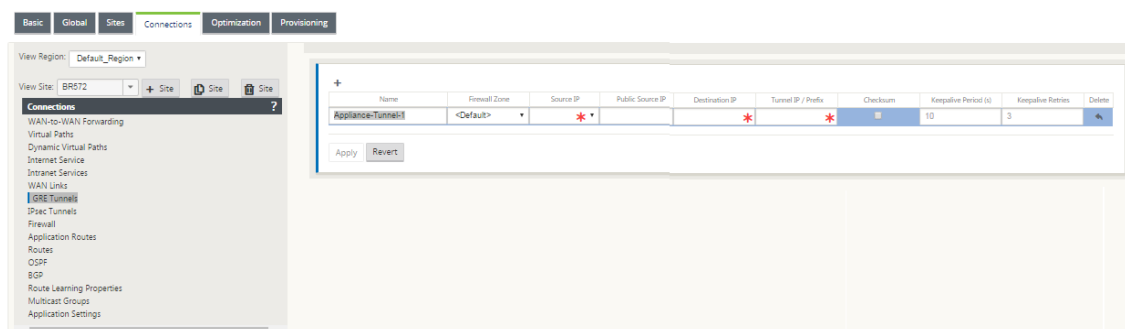
GRE-Tunnel für einen Zweigstandort konfigurieren

October 28, 2021

Mit der GRE-Tunnelfunktion können Sie Citrix SD-WAN Appliances so konfigurieren, dass GRE-Tunnel im LAN oder Intranet beendet werden. Wenn Sie diesen Zweigstandort nicht als LAN GRE-Tunnelabschlussknoten konfigurieren möchten, können Sie diesen Schritt überspringen und mit dem Abschnitt [Konfigurieren von WAN-Links für den Zweigstandort](#) fortfahren.

So konfigurieren Sie einen LAN-GRE-Tunnel für den Zweigstandort:

- Klicken Sie in der Ansicht Verbindungen für den neuen Zweigstandort auf **GRE-Tunnel**. Die **GRE-Tunnels-Ansicht** für den neuen Standort wird geöffnet.
- Klicken Sie auf **+** rechts neben den **GRE-Tunneln**. Dadurch wird der Tabelle ein neuer leerer GRE Tunnel Eintrag hinzugefügt und zur Bearbeitung geöffnet.



- Konfigurieren Sie die GRE Tunneleinstellungen. Geben Sie Folgendes ein:

- Service** - Wählen Sie den Dienstyp entweder Intranet oder LAN aus der Dropdownliste aus.
- Bezeichnung:**
 - Wenn der Dienstyp Intranet ist, wählen Sie aus der Liste der konfigurierten Intranet-dienste im Dropdownmenü aus.

- Wenn der Diensttyp LAN ist, geben Sie einen Namen für den neuen GRE-Tunnel ein, oder übernehmen Sie die Standardeinstellung.
 - Standard verwendet ein Benennungsformat **Appliance-Tunnel-*<number>*** - wobei *<number>* die Anzahl der für diese Site konfigurierten GRE-Tunnel ist, die um eins erhöht werden.
- **Intranetdiensttyp** - Für einen Intranetdiensttyp wählen Sie **Standard** oder **ZScaler** aus der Dropdownliste.
 - **Firewallzone** - Wählen Sie eine Firewallzone für den GRE-Tunnel aus.
 - **Quell-IP** —Wählen Sie eine Quell-IP-Adresse für den Tunnel aus dem Dropdownmenü für dieses Feld aus. Die Menüoptionen sind die Liste der virtuellen IP-Adressen, die Sie für diese Site konfiguriert haben. Konfigurieren Sie mindestens eine virtuelle Schnittstelle und eine virtuelle IP-Adresse, bevor Sie einen LAN GRE Tunnel konfigurieren können. Anweisungen finden Sie in den Abschnitten [Konfigurieren der virtuellen Schnittstellengruppen für den Zweigstandort](#) und [Konfigurieren der virtuellen IP-Adressen für den Zweigstandort](#).
 - **Public Source IP** - Geben Sie die IP-Adresse ein, die als Quelladresse für Pakete im GRE-Tunnel verwendet werden soll. Die Quell-IP-Adresse ist der Ausgangspunkt des GRE-Tunnels.
 - **Ziel-IP** —Geben Sie die IP-Adresse ein, die als Host-Ziel verwendet werden soll. Die Ziel-IP-Adresse ist der Endpunkt des GRE-Tunnels.
 - **Tunnel IP/ Präfix** — Geben Sie die IP-Adresse und das Präfix ein, die für die GRE-Tunnelschnittstelle verwendet werden.
 - **Prüfsumme** — Wählen Sie das Feld **Prüfsumme** aus, um Prüfsumme für den GRE-Header des Tunnels zu
 - **Keepalive-Perioden** —Geben Sie das Wartezeitintervall (in Sekunden) zwischen Keepalive-Nachrichten ein. Wenn auf 0 konfiguriert, werden keine Keepalive-Pakete gesendet, aber der Tunnel bleibt oben. Der Standardwert ist 10.
 - **Keepalive-Wiederholungen** — Geben Sie die Anzahl der Keepalive-Wiederholungen ein, die die Virtual WAN Appliance versuchen muss, bevor sie den Tunnel zum Fall bringt. Der Standardwert ist 3 Tage.
4. Klicken Sie auf **Apply**. Dadurch werden Ihre Einstellungen übermittelt und der Tabelle der neue GRE Tunnel hinzugefügt.

| Name | Firewall Zone | Source IP | Public Source IP | Destination IP | Tunnel IP / Prefix | Checksum | Keepalive Period (s) | Keepalive Retries | Delete |
|--------------------|----------------|--------------|------------------|----------------|--------------------|-------------------------------------|----------------------|-------------------|--------|
| Appliance-Tunnel-1 | Default_LAN_Zo | 192.113.59.5 | 192.113.59.6 | 10.199.81.237 | 10.199.108.2/20 | <input checked="" type="checkbox"/> | 10 | 3 | |

Apply Revert

5. Um weitere GRE-Tunnel zu konfigurieren, klicken Sie auf **+** rechts neben dem **GRE-Tunnels-Label** und fahren Sie wie in den vorangegangenen Schritten fort.

Der nächste Schritt besteht darin, die [WAN-Verbindungen für den Zweigstandort](#) zu konfigurieren.

In-Band- und Backup-Management

May 10, 2021

In-Band-Verwaltung

Mit Citrix SD-WAN können Sie die SD-WAN-Appliance auf zwei Arten verwalten: Out-of-Band-Verwaltung und In-Band-Verwaltung. Mit der Out-of-Band-Verwaltung können Sie eine Verwaltungs-IP mit einem für die Verwaltung reservierten Port erstellen, der nur den Verwaltungsdatenverkehr trägt. Mit der In-Band-Verwaltung können Sie die SD-WAN-Datenports für die Verwaltung verwenden. Es überträgt sowohl Daten- als auch Verwaltungsdatenverkehr, ohne einen zusätzlichen Verwaltungspfad konfigurieren zu müssen.

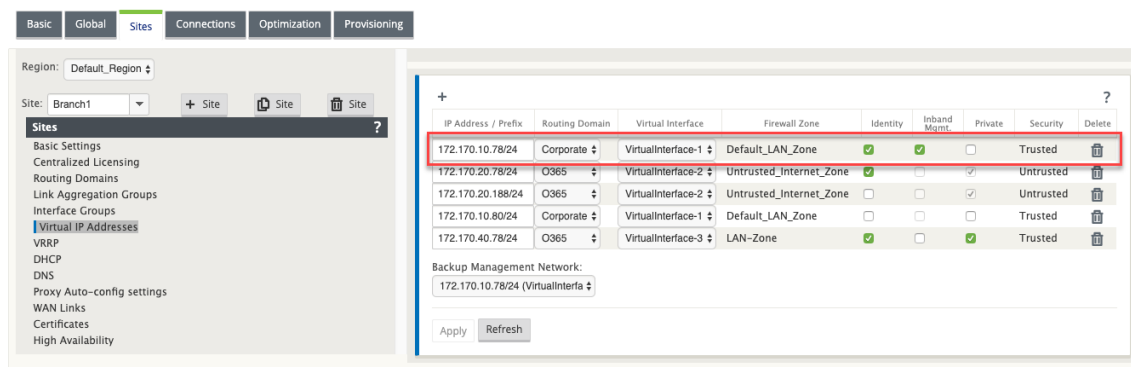
Durch die In-Band-Verwaltung können virtuelle IP-Adressen mit Verwaltungsdiensten wie Web-UI und SSH verbunden werden. Sie können die In-Band-Verwaltung auf mehreren vertrauenswürdigen Schnittstellen aktivieren, die für IP-Dienste aktiviert sind. Sie können auf die Web-UI und SSH über die Management-IP und virtuelle In-Band-IPs zugreifen.

So aktivieren Sie die In-Band-Verwaltung auf einer virtuellen IP:

1. Navigieren Sie im Konfigurations-Editor zu **Sites > Virtuelle IP-Adressen**.
2. Wählen Sie **Inband-Verwaltung** für die virtuellen IPs, für die Sie die In-Band-Verwaltung aktivieren möchten.

Hinweis:

Stellen Sie sicher, dass der Sicherheitstyp der Schnittstelle **Trusted** und **Identity** aktiviert ist.



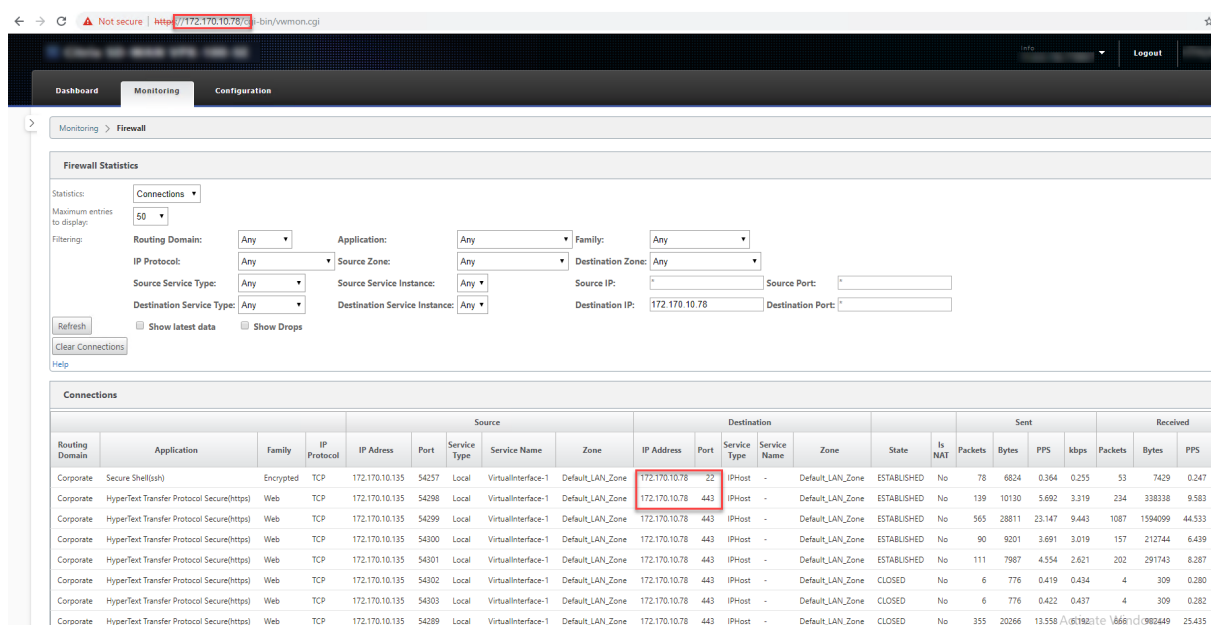
3. Klicken Sie auf **Anwenden**

Ausführliche Vorgehensweise zum Konfigurieren der virtuellen IP-Adresse finden Sie unter [So konfigurieren Sie virtuelle IP](#).

Überwachung der In-Band-Verwaltung

Im vorangegangenen Beispiel haben wir die In-Band-Verwaltung auf der virtuellen IP 172.170.10.78 aktiviert. Sie können diese IP verwenden, um auf die Web-UI und SSH zuzugreifen.

Navigieren Sie in der Web-Benutzeroberfläche zu **Überwachung > Firewall**. Sie können SSH und Web-UI sehen, auf die über die virtuelle IP auf Port 22 bzw. 443 in der Spalte **Ziel-IP-Adresse** zugegriffen wird.



In-Band-Provisioning

Die Notwendigkeit, SD-WAN-Appliances in einfacheren Umgebungen wie zu Hause oder in kleinen Zweigstellen bereitzustellen, ist deutlich gestiegen. Das Konfigurieren separater Verwaltungszugriff für einfachere Bereitstellungen stellt einen zusätzlichen Overhead dar. Die Zero-Touch-Bereitstellung (ZTD) und die In-Band-Verwaltungsfunktion ermöglichen Provisioning und Konfigurationsverwaltung über bestimmte Datenports. ZTD wird nun auf den dafür vorgesehenen Datenports unterstützt und es besteht keine Notwendigkeit, einen separaten Management-Port für ZTD zu verwenden. Citrix SD-WAN ermöglicht außerdem das nahtlose Failover des Verwaltungsdatenverkehrs zum Verwaltungsport, wenn der Datenport ausfällt und umgekehrt.

Eine Appliance im werkseitig ausgelieferten Zustand, die In-Band-Provisioning unterstützt, kann durch einfaches Verbinden der Daten oder des Verwaltungsports mit dem Internet bereitgestellt werden. Die Appliances, die die In-Band-Provisioning unterstützen, verfügen über spezifische Ports für LAN und WAN. Die Appliance im Zurücksetzungszustand auf Werkseinstellungen verfügt über eine Standardkonfiguration, die es ermöglicht, eine Verbindung mit dem Zero-Touch-Bereitstellungsdienst herzustellen. Der LAN-Port fungiert als DHCP-Server und weist dem WAN-Port, der als DHCP-Client fungiert, eine dynamische IP zu. Die WAN-Verbindungen überwachen den Quad 9-DNS-Dienst, um WAN-Konnektivität zu ermitteln.

Hinweis

Die In-Band-Provisioning gilt nur für SD-WAN 110 SE- und SD-WAN VPX-Plattformen.

Sobald die IP-Adresse abgerufen und eine Verbindung mit dem Zero-Touch-Bereitstellungsdienst hergestellt wurde, werden die Konfigurationspakete heruntergeladen und auf der Appliance installiert. Informationen zur Zero-Touch-Bereitstellung über das SD-WAN Center finden Sie unter [Zero Touch-Bereitstellung](#). Weitere Informationen zur Zero-Touch-Bereitstellung über SD-WAN Orchestrator finden Sie unter [Zero Touch-Bereitstellung](#).

Hinweis: Für die Day-0-Bereitstellung von SD-WAN-Appliances über die Daten-Ports sollte die Appliance-Softwareversion SD-WAN 11.1.0 oder höher sein.

Die Standardkonfiguration einer Appliance im Zurücksetzungsstatus auf Werkseinstellungen umfasst die folgenden Konfigurationen:

- DHCP-Server auf LAN-Anschluss
- DHCP-Client auf WAN-Port
- QUAD9-Konfiguration für DNS
- Standard-LAN-IP ist 192.168.0.1
- Grace Lizenz von 35 Tagen.

Sobald die Appliance bereitgestellt wurde, wird die Standardkonfiguration deaktiviert und durch die Konfiguration überschrieben, die vom Zero-Touch-Bereitstellungsdienst empfangen wurde. Wenn

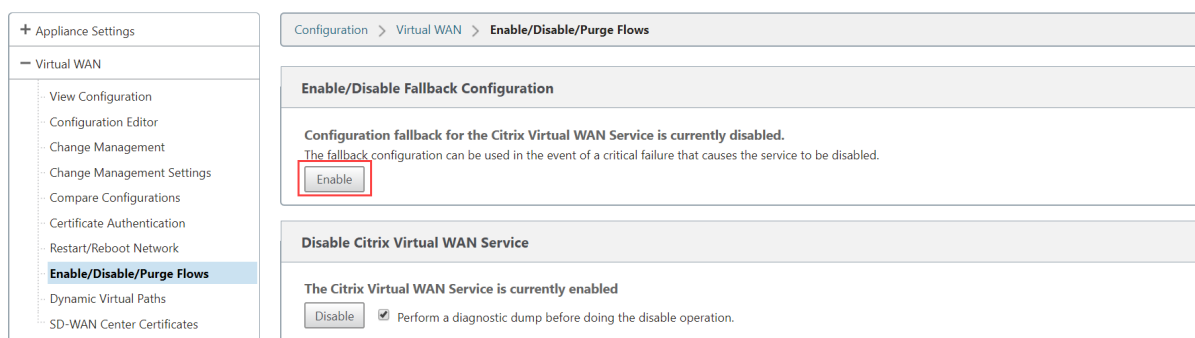
eine Appliance-Lizenz oder eine Kulanzlizenz abläuft, wird die Standardkonfiguration aktiviert, um sicherzustellen, dass die Appliance weiterhin mit dem Zero-Touch-Bereitstellungsdienst verbunden bleibt und Lizenzen erhält, die über eine Zero-Touch-Bereitstellung verwaltet werden.

Fallback-Konfiguration

Die Fallbackkonfiguration stellt sicher, dass die Appliance mit dem Zero-Touch-Bereitstellungsdienst verbunden bleibt, wenn Verbindungsfehler, Konfigurationskonflikt oder Softwarevereinstimmung vorliegen. Die Fallbackkonfiguration ist standardmäßig auf den Appliances aktiviert, die über ein Standardkonfigurationsprofil verfügen. Sie können die Fallback-Konfiguration auch gemäß Ihren vorhandenen LAN-Netzwerkeinstellungen bearbeiten.

Hinweis: Stellen Sie nach der anfänglichen Appliance-Bereitstellung sicher, dass die Fallback-Konfiguration für die Zero-Touch-Bereitstellungsdienstkonnektivität aktiviert ist.

Wenn die Rückfallkonfiguration deaktiviert ist, können Sie sie aktivieren, indem Sie zu **Konfiguration > Virtuelles WAN > Enable /Disable/Purge Flows> Fallback-Konfiguration aktivieren/deaktivieren** navigieren und auf **Aktivieren** klicken.



So passen Sie die Fallbackkonfiguration gemäß Ihrem LAN-Netzwerk an:

1. Navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Fallback-Konfiguration**.
2. Bearbeiten Sie Werte für die folgenden LAN-Einstellungen gemäß Ihren Netzwerkanforderungen. Dies ist die Mindestkonfiguration, die erforderlich ist, um eine Verbindung mit dem Zero-Touch-Bereitstellungsdienst herzustellen.
 - **VLAN-ID:** Die VLAN-ID, in die der LAN-Port gruppiert werden muss.
 - **IP-Adresse:** Die dem LAN-Port zugewiesene virtuelle IP-Adresse.
 - **DHCP aktiviert:** Aktiviert den LAN-Port als DHCP-Server. Der DHCP-Server weist den Clients am LAN-Port dynamische IP-Adressen zu.
 - **DHCP Start und DHCP End:** Der Bereich der IP-Adressen, den DHCP verwendet, um den Clients am LAN-Port dynamisch eine IP zuzuweisen.
 - **DNS-Server:** Die IP-Adresse des primären DNS-Servers.

- **Alt DNS Server:** Die IP-Adresse des sekundären DNS-Servers.
- **Internetzugang:** Erlaubt allen LAN-Clients den Internetzugang ohne weitere Filterung.

Die folgende Tabelle enthält die Details der vordefinierten WAN- und LAN-Ports für die Fallback-konfiguration auf verschiedenen Plattformen:

| Plattform | WAN-Ports | LAN-Ports |
|-----------|-----------------|-----------|
| 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 |
| 410 | 1/4, 1/5, 1/6 | 1/3 (FTB) |
| 1100 | 1/4, 1/5, 1/6 | 1/3 (FTB) |

Fallback Configuration

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

WAN Settings (Ports: 1)

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

LAN Settings (Ports: 2)

VLAN ID:

0

IP Address:

192.168.0.1/24

DHCP Enabled:

☐

DHCP Start:

192.168.0.50

DHCP End:

192.168.0.250

DNS Server:

9.9.9.9

Alt DNS Server:

149.112.112.112

Internet Access:

☐ ?

Port Settings

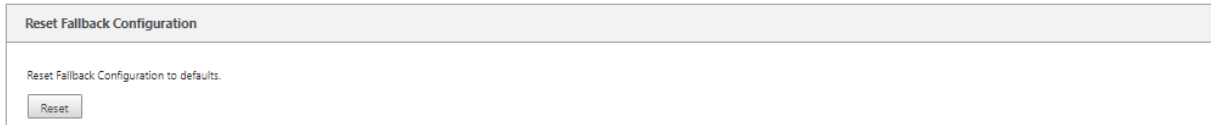
| Port Name | Mode |
|-----------|---|
| 1 | <input checked="" type="radio"/> WAN <input type="radio"/> LAN <input type="radio"/> Disabled |
| 2 | <input type="radio"/> WAN <input checked="" type="radio"/> LAN <input type="radio"/> Disabled |
| 3 | <input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled |
| 4 | <input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled |
| 5 | <input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled |
| 6 | <input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled |
| 7 | <input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled |
| 8 | <input type="radio"/> WAN <input type="radio"/> LAN <input checked="" type="radio"/> Disabled |

Unassigned Port Bypass Mode: Fail-to-Block

Apply

3. Konfigurieren Sie den Modus für jeden Port. Der Port kann entweder LAN- oder WAN-Port sein oder deaktiviert werden. Die angezeigten Ports hängen vom Appliance-Modell ab. Stellen Sie außerdem den Port-Bypass-Modus auf **Fail-to-Blockierung** oder **Fail-to-Wire** ein.

Um die Fallback-Konfiguration jederzeit auf die Standardkonfiguration zurückzusetzen, klicken Sie auf **Zurücksetzen**.



Konfigurierbare Verwaltung oder Datenport

Durch die In-Band-Verwaltung können die Datenports sowohl Daten- als auch Verwaltungsdatenverkehr übertragen, wodurch ein dedizierter Management-Port überflüssig wird. Dadurch bleibt der Management-Port auf den Low-End-Appliances, die bereits eine geringe Portdichte aufweisen, ungenutzt. Mit Citrix SD-WAN können Sie den Verwaltungsport so konfigurieren, dass er entweder als Datenport oder als Verwaltungsport verwendet wird.

Hinweis

Sie können den Verwaltungsport nur auf den folgenden Plattformen in Datenport konvertieren.

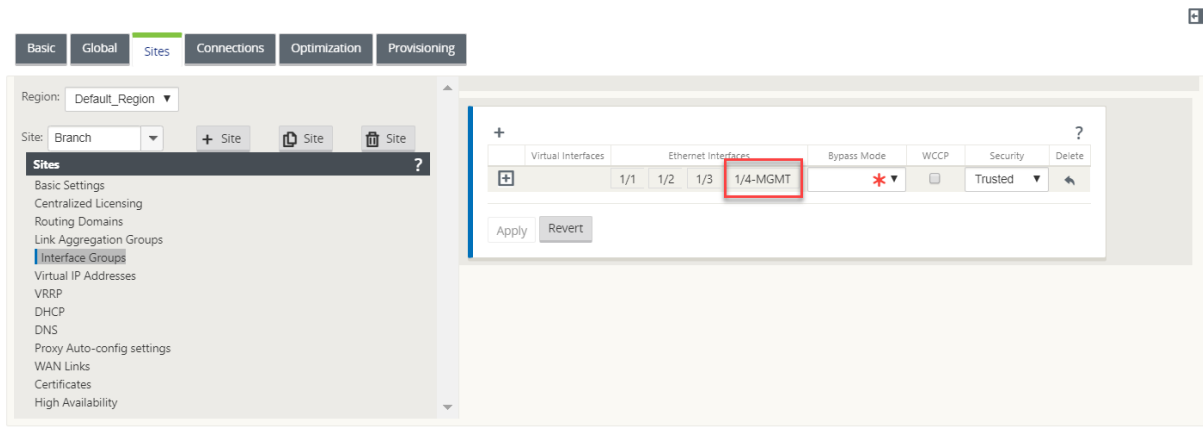
- Citrix SD-WAN 110 SE/LTE
- Citrix SD-WAN 210 SE/LTE

Verwenden Sie im Konfigurationseditor den Verwaltungsport in Ihrer Konfiguration. Nachdem die Konfiguration aktiviert wurde, wird der Management-Port in einen Datenport konvertiert.

Hinweis

Sie können einen Verwaltungsport nur konfigurieren, wenn die In-Band-Verwaltung auf anderen vertrauenswürdigen Schnittstellen der Appliance aktiviert ist.

Um eine Verwaltungsschnittstelle zu konfigurieren, navigieren Sie im Konfigurationseditor zu **Sites**, wählen Sie eine Site aus und klicken auf **Interface-Gruppen**. Die MGMT-Schnittstelle kann konfiguriert werden. Weitere Informationen zum Konfigurieren von Schnittstellengruppen finden Sie unter [Konfigurieren von Schnittstellengruppen](#).



Um den Verwaltungsport neu zu konfigurieren, um Verwaltungsfunktionen auszuführen, entfernen Sie die Konfiguration. Erstellen Sie eine Konfiguration, ohne den Management-Port zu verwenden, und aktivieren Sie sie.

Backup-Management-Netzwerk

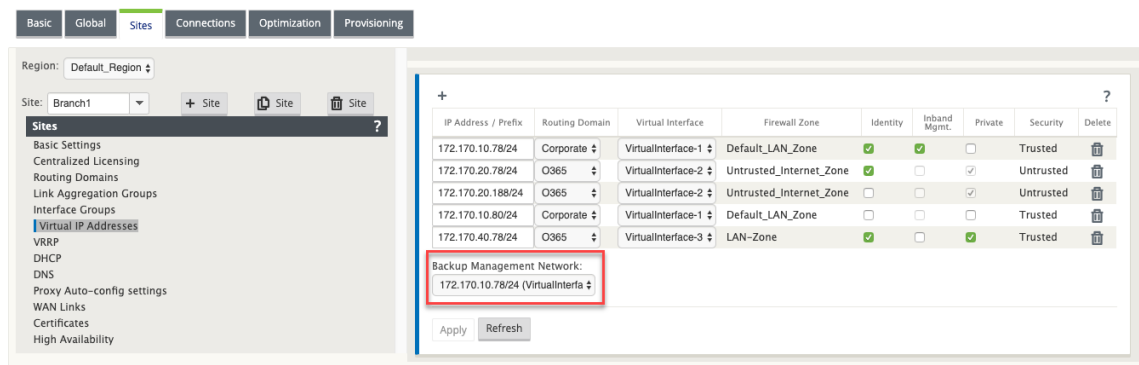
Sie können eine virtuelle IP-Adresse als Backup-Management-Netzwerk konfigurieren. Sie wird als Verwaltungs-IP-Adresse verwendet, wenn der Verwaltungsport nicht mit einem Standard-Gateway konfiguriert ist.

Hinweis

Wenn ein Standort Internetdienst mit einer einzelnen Routingdomäne konfiguriert ist, wird standardmäßig eine vertrauenswürdige Schnittstelle mit aktivierter Identität als Sicherungsverwaltungsnetzwerk ausgewählt.

So wählen Sie eine virtuelle IP als Sicherungsverwaltungsnetzwerk aus:

1. Navigieren Sie im Konfigurations-Editor zu **Sites > Virtuelle IP-Adressen**.
2. Wählen Sie eine virtuelle IP-Adresse als Backup-Management-Netzwerk aus.



3. Wählen Sie den DNS-Proxy aus, an den alle DNS-Anfragen über die In-Band- und Backup-Managementebene weitergeleitet werden.

Hinweis

Der DNS-Proxy kann nur ausgewählt werden, wenn sowohl die In-Band-Verwaltung als auch das Backup-Management-Netzwerk für eine virtuelle IP aktiviert sind.

4. Klicken Sie auf **Übernehmen**.

Ausführliche Vorgehensweisen zur Konfiguration der virtuellen IP-Adresse finden Sie unter [So konfigurieren Sie eine virtuelle IP-Adresse](#)

Überwachung der Backup-Verwaltung

Im vorangegangenen Beispiel haben wir 172.170.10.78 virtuelle IP als Backup-Management-Netzwerk ausgewählt. Wenn die Verwaltungs-IP-Adresse nicht mit einem Standard-Gateway konfiguriert ist, können Sie diese IP verwenden, um auf die Web-Benutzeroberfläche und SSH zuzugreifen.

Navigieren Sie in der Web-Benutzeroberfläche zu **Überwachung > Firewall**. Sie können diese virtuelle IP-Adresse als Quell-IP-Adresse für SSH- und Web-UI-Zugriff sehen.

Monitoring > Firewall

Firewall Statistics

Statistics: Connections
Maximum entries to display: 50
Filtering:
Routing Domain: Any Application: Any Family: Any
IP Protocol: Any Source Zone: Any Destination Zone: Any
Source Service Type: Any Source Service Instance: Any Source IP: 172.170.10.78 Source Port: *
Destination Service Type: Any Destination Service Instance: Any Destination IP: * Destination Port: *
Refresh Clear Connections Help
Show latest data Show Drops

Connections

| Routing Domain | Application | Family | IP Protocol | Source | | | | Destination | | | | State | Is NAT | Sent | | | Received | | | | | |
|----------------|---|-----------------|-------------|---------------|-------|--------------|--------------|------------------|---------------|------|--------------|------------------|-------------------------|--------------|------|---------|----------|-------|-------|---------|-------|-------|
| | | | | IP Address | Port | Service Type | Service Name | Zone | IP Address | Port | Service Type | | | Service Name | Zone | Packets | Bytes | PPS | kpps | Packets | Bytes | PPS |
| Corporate | Transmission Control Protocol(tcp) | Network Service | TCP | 172.170.10.78 | 49818 | IPHost | - | Default_LAN_Zone | 18.210.2.11 | 443 | Internet | Branch1-Internet | Untrusted_Internet_Zone | SYN_SENT | Yes | 1 | 60 | - | - | 0 | 0 | - |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 58939 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | NEW | Yes | 2 | 148 | - | - | 0 | 0 | - |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 43012 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 168 | 0.070 | 0.047 | 2 | 297 | 0.070 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 36558 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 148 | 0.011 | 0.007 | 2 | 277 | 0.011 |
| Corporate | HyperText Transfer Protocol Secure(https) | Web | TCP | 172.170.10.78 | 60624 | IPHost | - | Default_LAN_Zone | 18.235.40.8 | 443 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 9 | 1271 | 0.176 | 0.199 | 7 | 4069 | 0.137 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 60585 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 1 | 80 | 0.003 | 0.002 | 1 | 128 | 0.003 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 58010 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 1 | 80 | 0.020 | 0.013 | 1 | 80 | 0.020 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 36684 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 1 | 80 | 0.006 | 0.004 | 1 | 161 | 0.006 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 33173 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 1 | 80 | 0.003 | 0.002 | 1 | 80 | 0.003 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 53914 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 1 | 80 | 0.006 | 0.004 | 1 | 128 | 0.006 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 53708 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 128 | 0.013 | 0.006 | 2 | 144 | 0.013 |
| Corporate | Domain Name Service(dns) | Network Service | UDP | 172.170.10.78 | 43704 | IPHost | - | Default_LAN_Zone | 10.105.147.14 | 53 | Internet | Branch1-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 1 | 80 | 0.020 | 0.013 | 1 | 128 | 0.020 |

Internetzugriff

May 10, 2021

Der Internetdienst wird für den Datenverkehr zwischen einer Endbenutzer-Website und Websites im öffentlichen Internet verwendet. Internetdienstdatenverkehr wird nicht von SD-WAN gekapselt und verfügt nicht über die gleichen Funktionen wie Datenverkehr, der über den Virtual Path Service bereitgestellt wird. Es ist jedoch wichtig, diesen Datenverkehr auf dem SD-WAN zu klassifizieren und zu berücksichtigen. Datenverkehr, der als Internetdienst identifiziert wird, ermöglicht die zusätzliche Möglichkeit, dass SD-WAN in der Lage ist, die WAN-Verbindungsbandbreite aktiv zu verwalten, indem der Internetverkehr im Verhältnis zum Datenverkehr über den virtuellen Pfad und den Intranetverkehr gemäß der vom Administrator festgelegten Konfiguration eingeschränkt wird. Zusätzlich zu den Funktionen zum Bandbreitenprovisioning verfügt SD-WAN über die zusätzliche Möglichkeit, den über den Internetdienst bereitgestellten Datenverkehr über mehrere Internet-WAN-Verbindungen oder optional die Verwendung der Internet-WAN-Verbindungen in einer primären oder sekundären Konfiguration auszugleichen.

Die Steuerung des Internetverkehrs mithilfe des Internetdienstes auf SD-WAN-Appliances kann in den folgenden Bereitstellungsmodi konfiguriert werden:

- Direktes Internetbreakout in Branch mit integrierter Firewall
- Direktes Internetbreakout bei Zweigweiterleitung an Secure Web Gateway
- Backhaul Internet to Data Center MCN

Internet Traffic Control

Direct Internet Breakout at Branch with Integrated Firewall



Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



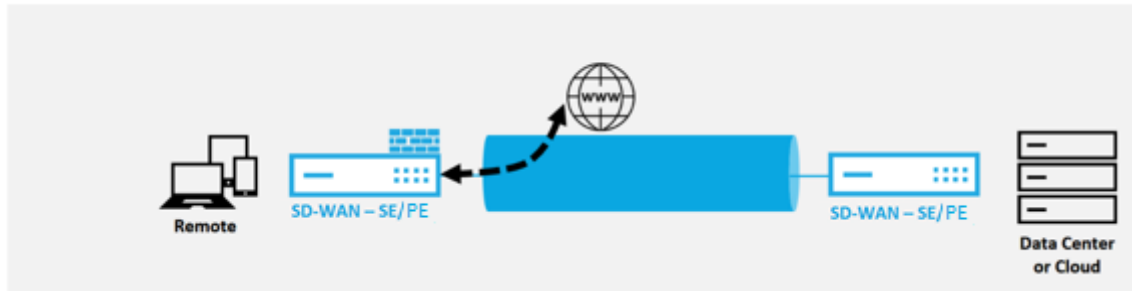
Backhaul Internet to Data Center MCN



Direkter Internetbreakout in Branch mit integrierter Firewall

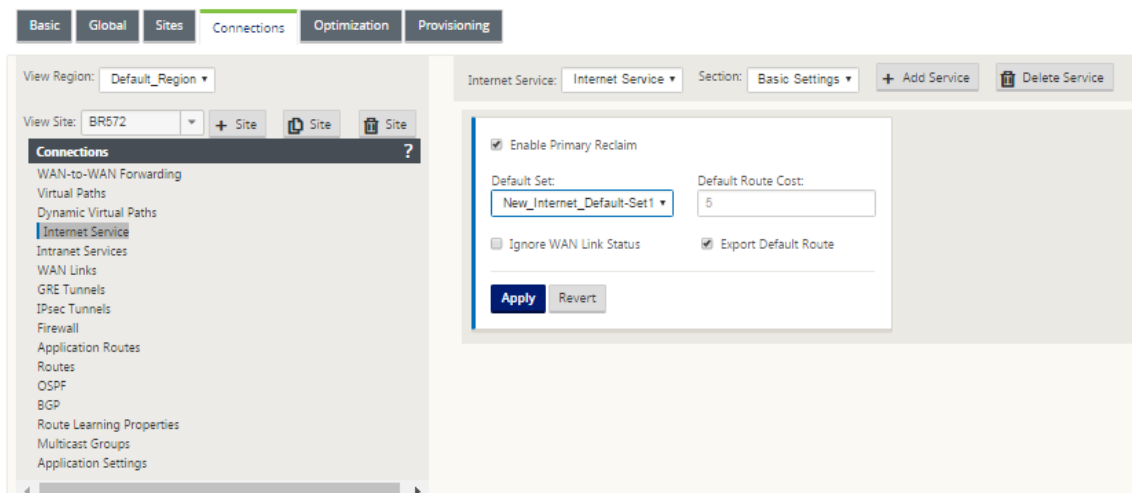
May 10, 2021

Direct Internet Breakout at Branch with Integrated Firewall



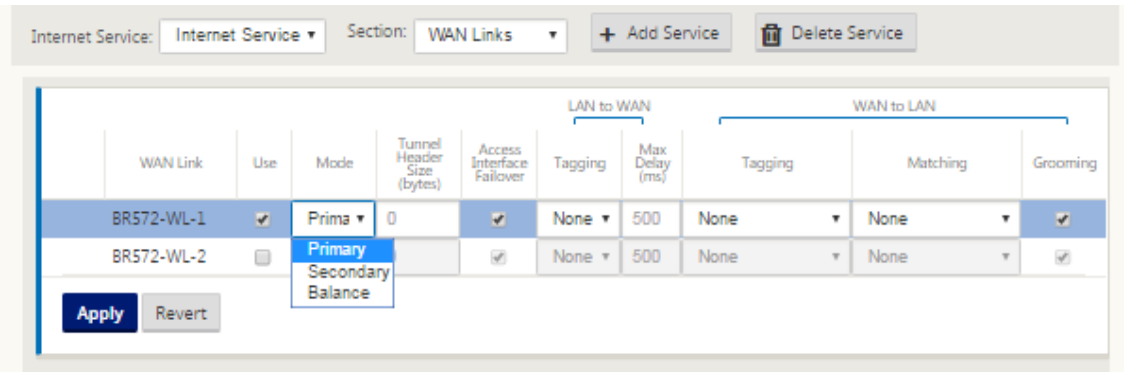
Führen Sie die folgenden Schritte aus, um Internetdienst für einen beliebigen Standort (Clientknoten oder MCN) zu aktivieren:

1. Navigieren Sie im **Konfigurations-Editor** zur Kachel **Verbindungen**. Klicken Sie auf das Symbol Hinzufügen (+), um einen Internetdienst für diese Site hinzuzufügen. Pro Site kann nur ein Internetdienst erstellt werden.
2. In den **Grundeinstellungen** für den Internetdienst gibt es mehrere Optionen, wie sich der Internetdienst während der Nichtverfügbarkeit von WAN-Verbindungen verhalten soll. Ein Internet-Standardsatz kann in der Kachel Global mit einem Satz von Regeln definiert werden, die auf jeden Knoten in der Konfiguration angewendet werden können, für den Internetdienst aktiviert ist. Dies ermöglicht eine zentrale Steuerung für die Verwaltung von Internetdiensten, ohne dass jeder Knoten separat konfiguriert werden muss.

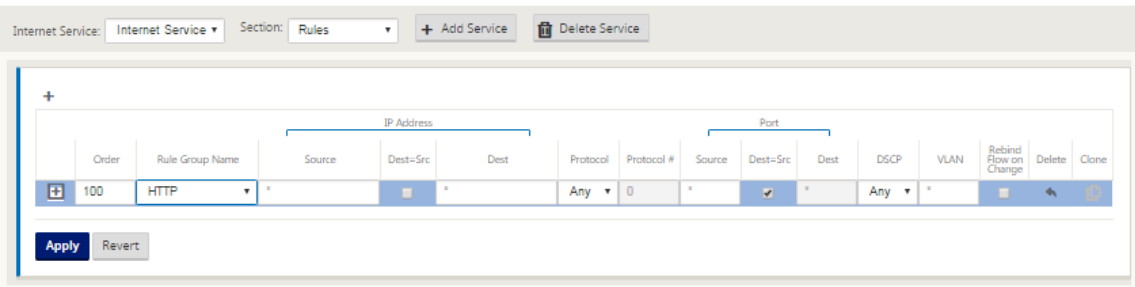


3. Im Knoten Internetdienst-WAN-Links werden die in der Site-Kachel erstellten WAN-Links zur Verfügung gestellt, um auszuwählen, welche WAN-Verbindung Sie für den Internetverkehr verwenden möchten. Zusätzlich zu anderen Optionen sind die verfügbaren Modi Primary, Secondary

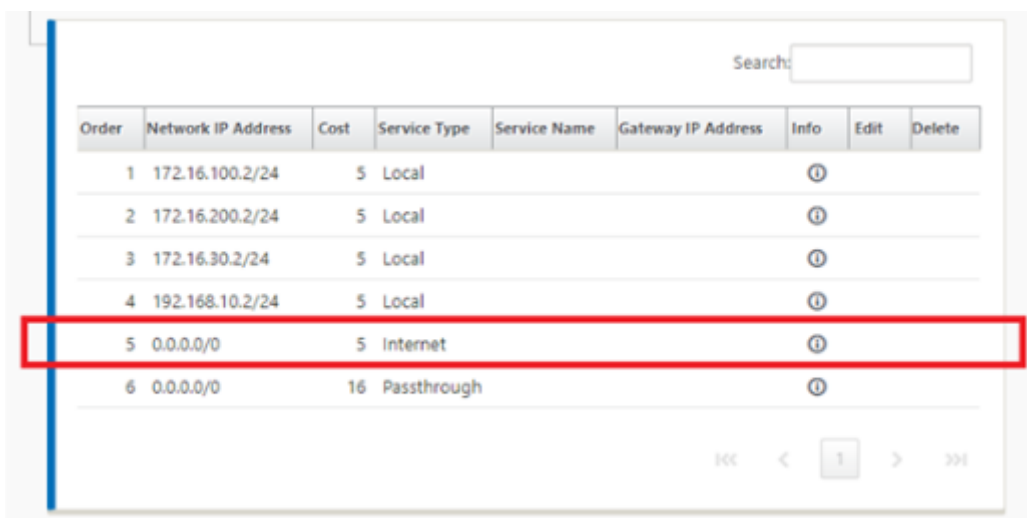
und Balanced, sodass der Administrator die verfügbaren WAN-Verbindungen gleichzeitig oder in einer aktiven/passiven Rolle verwenden kann.



4. Es stehen Standortknotenspezifische Regeln zur Verfügung, die die Möglichkeit der Anpassung jeder Site ermöglichen, alle allgemeinen Einstellungen, die im globalen Standardsatz konfiguriert sind, eindeutig außer Kraft zu setzen. Die Modi umfassen die gewünschte Zustellung über eine bestimmte WAN-Verbindung oder als Override-Dienst, der den gefilterten Datenverkehr ermöglicht.

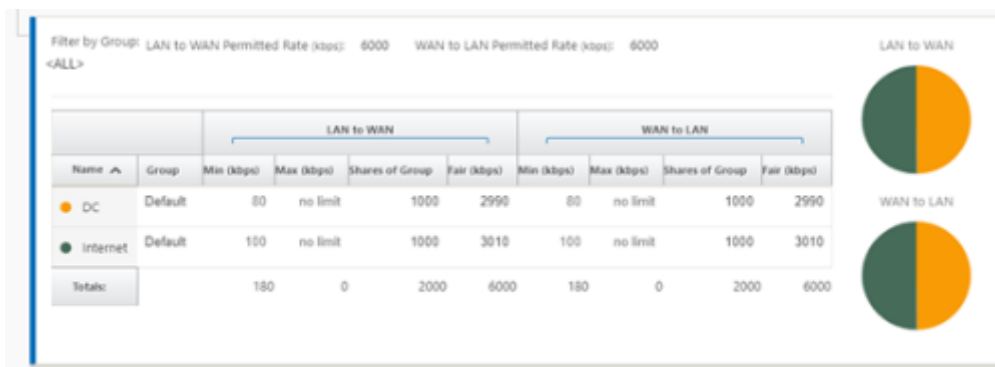


Da ein Internetdienst für einen Knoten erstellt wird, wird die Routentabelle für diesen bestimmten Knoten automatisch mit einer Route 0.0.0.0/0 für Diensttyp gleich Internet und einer Routenkosten von 5 aktualisiert. Andernfalls würde die Standardroute mit Kosten 16 mit Passthrough als Diensttyp übernommen und der Internetverkehr würde an das Unterlagennetz weitergegeben werden.



| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|------|--------------|--------------|--------------------|------|------|--------|
| 1 | 172.16.100.2/24 | 5 | Local | | | ⓘ | | |
| 2 | 172.16.200.2/24 | 5 | Local | | | ⓘ | | |
| 3 | 172.16.30.2/24 | 5 | Local | | | ⓘ | | |
| 4 | 192.168.10.2/24 | 5 | Local | | | ⓘ | | |
| 5 | 0.0.0.0/0 | 5 | Internet | | | ⓘ | | |
| 6 | 0.0.0.0/0 | 16 | Passthrough | | | ⓘ | | |

Wenn Internet Service für einen Standortknoten aktiviert ist, wird die Provisioning-Kachel verfügbar gemacht, um die bidirektionale (LAN zu WAN/WAN zu LAN) Verteilung der Bandbreite für eine WAN-Verbindung zwischen den verschiedenen Diensten, die die WAN-Verbindung verwenden, zu ermöglichen. Der Abschnitt Dienste ermöglicht es Benutzern, die Bandbreitenzuweisung weiter zu optimieren. Darüber hinaus kann Fair Share aktiviert werden, so dass alle Dienste ihre minimale reservierte Bandbreite erhalten, bevor eine faire Verteilung in Kraft tritt.



Der Internetdienst kann in den verschiedenen Bereitstellungsmodi verwendet werden, die von Citrix SD-WAN unterstützt werden.

- Inline-Bereitstellungsmodus (SD-WAN-Overlay)

Citrix SD-WAN kann als Overlay-Lösung in jedem Netzwerk bereitgestellt werden. Als Overlay-Lösung wird SD-WAN im Allgemeinen hinter bestehenden Edge-Routern und/oder Firewalls eingesetzt. Wenn SD-WAN hinter einer Netzwerk-Firewall bereitgestellt wird, kann die Schnittstelle als vertrauenswürdig konfiguriert werden und der Internetverkehr kann als Internet-Gateway an die Firewall übermittelt werden.

- Edge- oder Gateway-Modus

Citrix SD-WAN kann als Edge-Gerät bereitgestellt werden und ersetzt vorhandene Edge-Router und/oder Firewall-Geräte. Die integrierte Firewall-Funktion ermöglicht SD-WAN, das Netzwerk vor direkter Internetverbindung zu schützen. In diesem Modus wird die Schnittstelle, die mit der öffentlichen Internetverbindung verbunden ist, als nicht vertrauenswürdig konfiguriert, wodurch die Verschlüsselung aktiviert wird, und Firewall- und Dynamische NAT-Funktionen sind aktiviert, um das Netzwerk zu schützen.

Direkter Internetzugang mit Secure Web Gateway

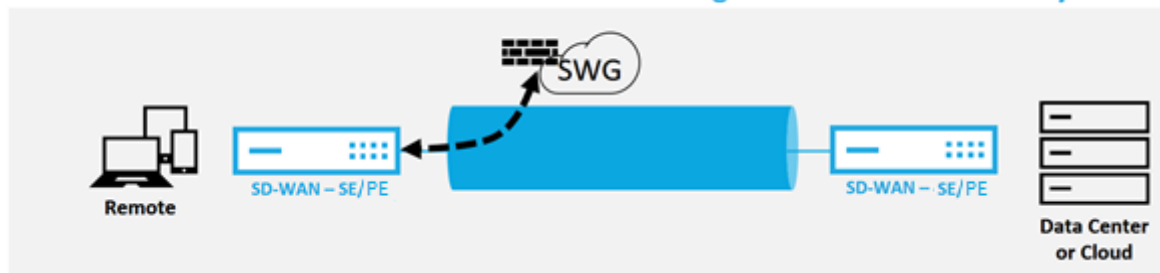
October 28, 2021

Um Datenverkehr zu sichern und Richtlinien durchzusetzen, verwenden Unternehmen häufig MPLS-Links, um Zweigdatenverkehr in das Unternehmens-Rechenzentrum zurückzuleiten. Das Rechenzentrum wendet Sicherheitsrichtlinien an, filtert den Datenverkehr durch Sicherheitsanwendungen, um Malware zu erkennen, und leitet den Datenverkehr über einen ISP weiter. Ein solches Backhauling über private MPLS-Verbindungen ist teuer. Dies führt auch zu einer erheblichen Latenz, was zu einer schlechten Benutzererfahrung am Zweigstellenstandort führt. Es besteht auch das Risiko, dass Benutzer Ihre Sicherheitskontrollen Bypass.

Eine Alternative zum Backhauling ist das Hinzufügen von Sicherheits-Appliances in der Filiale. Die Kosten und Komplexität steigen jedoch, wenn Sie mehrere Appliances installieren, um konsistente Richtlinien über die Standorte hinweg aufrechtzuerhalten. Am wichtigsten ist, dass das Kostenmanagement unpraktisch wird, wenn Sie viele Niederlassungen haben.

Eine Alternative besteht darin, die Sicherheit ohne zusätzliche Kosten, Komplexität oder Latenz durchzusetzen, darin, den gesamten Internetverkehr der Zweigstelle mit Citrix SD-WAN an den Secure Web Gateway Service weiterzuleiten. Ein Secure Web Gateway Service eines Drittanbieters ermöglicht die Erstellung detaillierter und zentraler Sicherheitsrichtlinien für alle verbundenen Netzwerke. Die Richtlinien werden konsistent angewendet, unabhängig davon, ob sich der Benutzer im Rechenzentrum oder an einem Zweigstandort befindet. Da Secure Web Gateway-Lösungen Cloud-basiert sind, müssen Sie dem Netzwerk keine teureren Sicherheitsgeräte hinzufügen.

Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



Citrix SD-WAN unterstützt die folgenden Secure Web Gateway-Lösungen von Drittanbietern:

- [Zscaler](#)
- [Forcepoint](#)
- [Palo Alto](#)
- [Citrix Secure Internet Access](#)

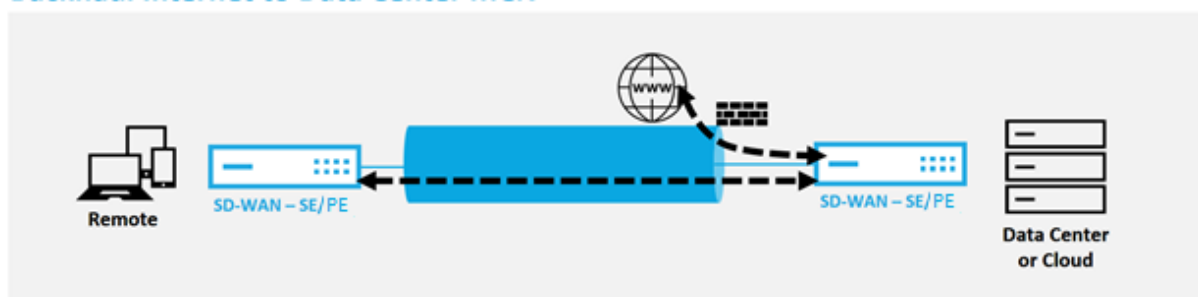
Backhaul Internet

May 10, 2021

Die Citrix SD-WAN Lösung kann den Internetverkehr an den MCN-Standort oder andere Zweigstellenstandorte zurückleiten. Backhaul zeigt an, dass der für das Internet bestimmte Datenverkehr über eine andere vordefinierte Site zurückgesendet wird, die auf das Internet zugreifen kann. Dies ist nützlich für Netzwerke, die aufgrund von Sicherheitsbedenken oder der Topologie der Unterlagennetze keinen direkten Internetzugang zulassen. Ein Beispiel wäre ein Remote-Standort, an dem keine externe Firewall vorhanden ist, bei dem die integrierte SD-WAN-Firewall die Sicherheitsanforderungen für diesen Standort nicht erfüllt. In einigen Umgebungen ist das Backhauling des gesamten Internetverkehrs von Remotesite durch die gehärtete DMZ im Rechenzentrum möglicherweise der beste Ansatz, um Benutzern in Remoteniederlassungen Internetzugang zu ermöglichen. Dieser Ansatz hat jedoch seine Einschränkungen, sich der folgenden und der unterlegten WAN-Links Größe entsprechend bewusst zu sein.

- Die Backhaul des Internetverkehrs erhöht die Latenz der Internetverbindung und ist abhängig von der Entfernung des Zweigstandorts für das Rechenzentrum variabel.
- Backhaul des Internetverkehrs verbraucht Bandbreite auf dem virtuellen Pfad und wird bei der Dimensionierung von WAN-Verbindungen berücksichtigt.
- Die Backhaul des Internetverkehrs kann den Internet-WAN-Link im Rechenzentrum überzeichnen.

Backhaul Internet to Data Center MCN



Alle Citrix SD-WAN Geräte können bis zu acht verschiedene Internet-WAN-Verbindungen in einem einzigen Gerät beenden. Lizenzierte Durchsatzfunktionen für die aggregierten WAN-Verbindungen werden

pro entsprechender Appliance im Citrix SD-WAN Datenblatt aufgeführt.

Die Citrix SD-WAN Lösung unterstützt die Backhaul des Internetverkehrs mit der folgenden Konfiguration.

1. Aktivieren Sie den Internetdienst am MCN-Standortknoten oder jede andere Standortnotiz, an der Internetdienst gewünscht ist.

Hinweis

Aktivieren Sie Internetdienst- und Exportrouten, wenn sich alle anderen Standorte in der WAN-zu-WAN-Weiterleitungsgruppe befinden.

2. Fügen Sie auf den Zweigknoten, auf denen der Internetverkehr zurückgeführt wird, manuell eine Route 0.0.0.0/0 hinzu, um den gesamten Standarddatenverkehr an den Virtual Path-Service zu leiten. Der nächste Hop wird als MCN bezeichnet, oder zwischengeschaltete Site.

3. Stellen Sie sicher, dass die Routentabelle des Zweigstandorts keine anderen kostengünstigeren Routen aufweist, die den Verkehr außer der gewünschten Backhaul-Route steuern würden.

Search:

| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|------|--------------|--------------|--------------------|------|------|--------|
| 1 | 172.16.100.2/24 | 5 | Local | | | | | |
| 2 | 172.16.30.2/24 | 5 | Local | | | | | |
| 3 | 192.168.10.2/24 | 5 | Local | | | | | |
| 4 | 0.0.0.0/0 | 5 | Virtual Path | DC | | | | |
| 5 | 0.0.0.0/0 | 16 | Passthrough | | | | | |

<<

<

1

>

>>

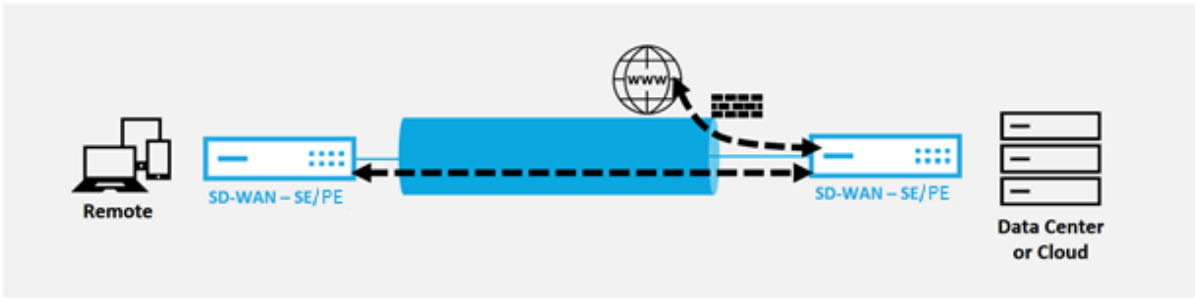
Hairpin-Modus

May 10, 2021

Mit der Hairpin Deployment können Sie die Nutzung einer Remote Hub-Site für den Internetzugang über Backhaul oder Hairpin implementieren, wenn lokale Internetdienste nicht verfügbar sind oder langsamer Datenverkehr auftreten. Sie können Routing mit hoher Bandbreite zwischen Clientstandorten anwenden, indem Sie Backhauling von bestimmten Standorten zulassen.

Der Zweck einer Hairpin Bereitstellung von einem Nicht-WAN zu einem WAN-Weiterleitungsstandort besteht darin, einen effizienteren Bereitstellungsprozess und eine effizientere technische Implementierung bereitzustellen. Sie können bei Bedarf eine Remote-Hub-Site für den Internetzugang verwenden und Flows durch den virtuellen Pfad zum SD-WAN-Netzwerk weiterleiten.

Backhaul Internet to Data Center MCN



Betrachten Sie beispielsweise einen Administrator mit mehreren SD-WAN-Sites, A und B. Standort A verfügt über einen schlechten Internetdienst. Site B verfügt über einen nutzbaren Internetdienst, mit dem Sie den Datenverkehr nur von Standort A zu Standort B zurückholen möchten. Sie können versuchen, dies zu erreichen, ohne die Komplexität strategisch gewichteter Routenkosten und die Weitergabe an Websites, die den Datenverkehr nicht erhalten sollten.

Außerdem wird die Routingtabelle nicht für alle Standorte in einer Hairpin-Bereitstellung freigegeben. Wenn der Datenverkehr beispielsweise zwischen Standort A und Standort B durch Standort C ausgesteckt wird, sind die Routen von Standort A und B nur Standort C bekannt. Standort A und Standort B teilen sich nicht gegenseitig die Routingtabelle im Gegensatz zu WAN-zu-WAN-Weiterleitung.

Wenn der Datenverkehr zwischen Standort A und Standort B bis Standort C verläuft, müssen die statischen Routen in Standort A und Standort B hinzugefügt werden, was angibt, dass der nächste Hop für beide Standorte der Zwischenstandort C ist.

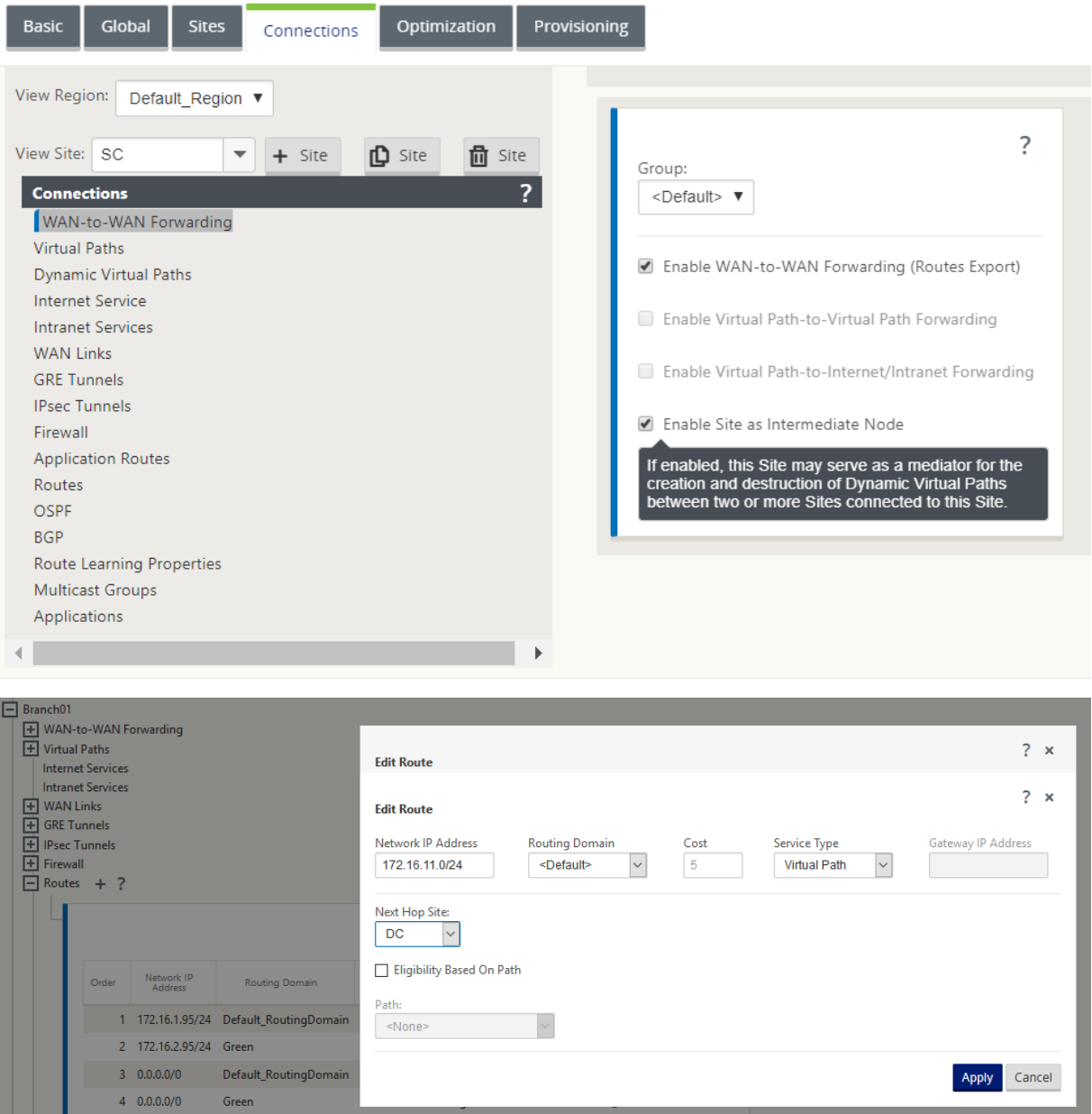
WAN-to-WAN Forwarding und Hairpin Bereitstellung weisen bestimmte Unterschiede auf:

1. Dynamische virtuelle Pfade sind nicht konfiguriert. Immer sieht der Zwischenstandort den gesamten Datenverkehr zwischen den beiden Standorten.
2. Teilt nicht an WAN-to-WAN-Weiterleitungsgruppen teil.

WAN-to-WAN Forwarding und Hairpin Bereitstellung schließen sich gegenseitig aus. Nur einer von ihnen kann zu einem bestimmten Zeitpunkt konfiguriert werden.

Citrix SD-WAN SE/PE und VPX (virtuelle) Appliances unterstützen die Hairpinbereitstellung. Sie können jetzt eine 0.0.0.0/0 Route zum Hairpin Datenverkehr zwischen zwei Standorten konfigurieren, ohne dass zusätzliche Standorte betroffen sind. Wenn das Hairpinning für den Intranetverkehr verwendet wird, werden dem Clientstandort bestimmte Intranetrouten hinzugefügt, um den Intranetverkehr über den virtuellen Pfad zur Hairpin-Site weiterzuleiten. Die Aktivierung der WAN-zu-WAN-Weiterleitung zur Erreichung der Hairpin Funktionalität ist nicht mehr erforderlich.

Sie können die Hairpinbereitstellung über die Citrix SD-WAN Webverwaltungsschnittstelle im Konfigurationseditor konfigurieren.



Gehostete Firewalls

May 10, 2021

Derzeit unterstützt Citrix SD-WAN die folgenden gehosteten Firewalls:

- [Palo Alto Netzwerke](#)
- [Check Point](#)

Palo Alto Networks Firewall-Integration auf SD-WAN 1100 Plattform

May 10, 2021

Citrix SD-WAN unterstützt das Hosten von Palo Alto Networks Virtual Machine (VM) -Firewall der nächsten Generation auf der SD-WAN 1100 Plattform. Im Folgenden werden die unterstützten VM-Modelle aufgeführt:

- VM 50
- VM 100

Die Firewall der virtuellen Maschinenserie Palo Alto Network wird als virtuelle Maschine auf der SD-WAN 1100 Plattform ausgeführt. Die virtuelle Firewall-Maschine ist im **Virtual Wire-Modus** integriert, mit zwei virtuellen Datenschnittstellen verbunden. Erforderlicher Datenverkehr kann durch Konfigurieren von Richtlinien auf SD-WAN an die virtuelle Firewall-Maschine umgeleitet werden.

Vorteile

Im Folgenden sind die wichtigsten Ziele oder Vorteile der Integration von Palo Alto Networks auf der SD-WAN 1100 Plattform aufgeführt:

- Zweiggerätekonsolidierung: Eine einzige Appliance, die sowohl SD-WAN als auch erweiterte Sicherheit bietet
- Sicherheit in Zweigstellen mit On-Prem NGFW (Next Generation Firewall) zum Schutz von LAN-zu-LAN-, LAN-zu-Internet- und Internet-zu-LAN-Datenverkehr

Konfigurationsschritte

Die folgenden Konfigurationen sind erforderlich, um die virtuelle Maschine Palo Alto Networks auf SD-WAN zu integrieren:

- Bereitstellen der virtuellen Firewall-Maschine
- Aktivieren der Datenverkehrsumleitung zur virtuellen Sicherheitsmaschine

Hinweis:

Die virtuelle Maschine der Firewall muss zuerst bereitgestellt werden, bevor die Datenverkehrsumleitung aktiviert wird.

Provisioning virtueller Maschine Palo Alto Network

Es gibt zwei Möglichkeiten, die virtuelle Firewall-Maschine bereitzustellen:

- Provisioning über SD-WAN Center
- Provisioning über die Benutzeroberfläche der SD-WAN-Appliance

Provisioning virtueller Maschinen in der Firewall über das SD-WAN Center

Voraussetzungen

- Fügen Sie dem SD-WAN Center den sekundären Speicher hinzu, um die Firewall-VM-Imagedateien zu speichern. Weitere Informationen finden Sie unter [Systemanforderungen und Installation](#).
- Reservieren Sie den Speicher von der sekundären Partition für die Firewall-VM-Imagedateien. Um das Speicherlimit zu konfigurieren, navigieren Sie zu **Administration > Speicherwartung**.
 - Wählen Sie den erforderlichen Speicherbetrag aus der Liste aus.
 - Klicken Sie auf **Übernehmen**.

The screenshot shows the 'Administration / Storage Maintenance' page in the SD-WAN Center. The left sidebar contains navigation links: Dashboard, Fault, Monitoring, Configuration, Reporting, Administration (selected), and Nitro API. Under Administration, there are links for User/Authentication Settings, Global Settings, Database Maintenance, Storage Maintenance (selected), and Diagnostics.

The main content area is titled 'Administration / Storage Maintenance' and shows the 'Region' as 'Default_Region'. Below this is a 'Storage Systems' table with columns: Host, File System, Type, Size (MB), Available (MB), and Active/Migrate Data.

| Host | File System | Type | Size (MB) | Available (MB) | Active/Migrate Data |
|--------|-------------|------|-----------|----------------|---------------------|
| Local* | /dev/xvda2 | ext3 | 7288 | 3471 | |
| Local | /dev/xvdb | ext3 | 14910 | 12921 | |

Below the table is an 'Apply' button and a note: 'Note: Software image storage reserved will be reduced while calculating the secondary partition Size(MB) and Available(MB)'.

The next section is 'Software Image Storage Reservation'. It includes a note: 'Note: User can modify the storage reservation only if the SD-WAN Center has secondary partition mounted and it should operate in headend mode'. Below this, there is a dropdown menu for 'Amount of storage to reserve from secondary partition storage(Active)' with '10GB' selected. An 'Apply' button is also present.

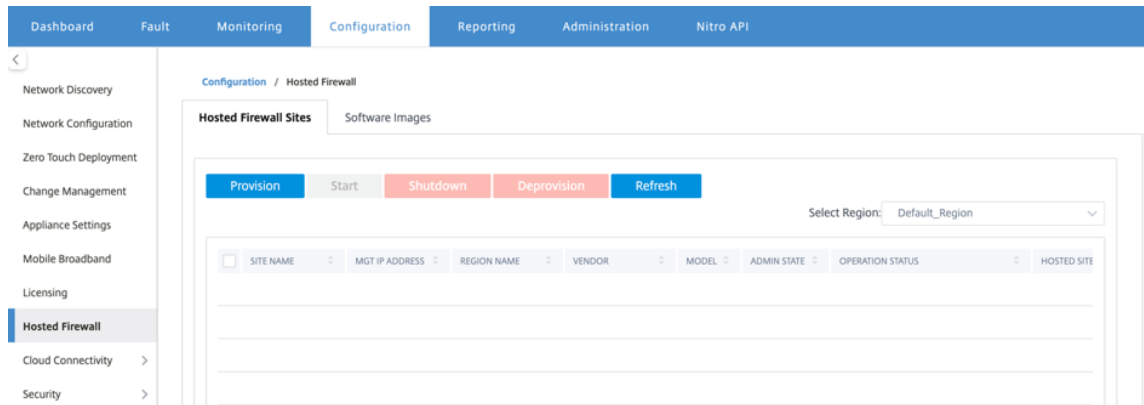
The final section is 'Thresholds'. It contains a warning: 'SD-WAN Center Database Storage and Auto Cleanup settings are misconfigured, SD-WAN Center will reach auto cleanup threshold before the configured 6 months.' Below this, there are two settings: 'Stop stats polling when storage usage exceeds 55% of active storage size' and 'Notify user when storage usage exceeds 10% of active storage size'. An 'Apply' button is at the bottom.

Hinweis:

Speicher ist für die sekundäre Partition reserviert, die aktiv ist, wenn die Bedingung erfüllt ist.

Führen Sie die folgenden Schritte aus, um Provisioning Firewall-Maschine über die SD-WAN Center-Plattform bereitzustellen:

1. Navigieren Sie in der Citrix SD-WAN Center-GUI zu **Konfiguration** > Wählen Sie **Gehostete Firewall** aus.



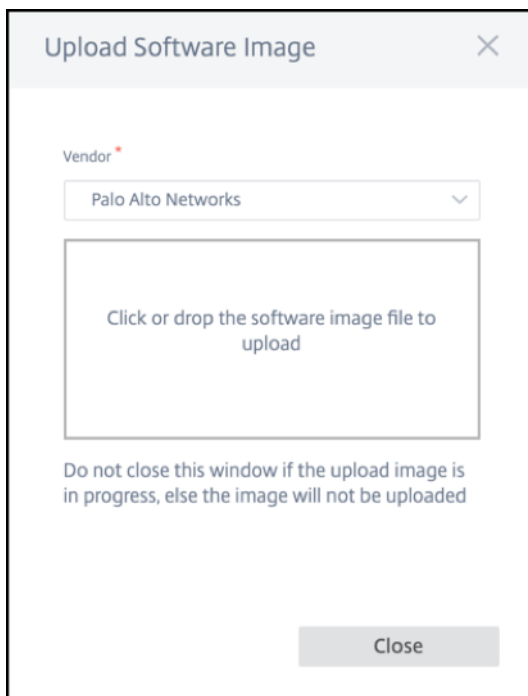
Sie können die **Region** aus der Dropdown-Liste auswählen, um die bereitgestellten Site-Details für diese ausgewählte Region anzuzeigen.

2. Laden Sie das Softwareimage hoch.

Hinweis

Stellen Sie sicher, dass Sie über genügend Speicherplatz verfügen, um das Software-Image hochzuladen.

Navigieren Sie zu **Konfiguration** > **Gehostete Firewall** > **Software-Images** und wählen Sie den Namen des Anbieters als Palo Alto Networks aus der Dropdown-Liste aus. Klicken oder legen Sie die Softwareimage-Datei in das Feld für den Upload ab.



Eine Statusleiste mit dem laufenden Upload-Prozess wird angezeigt. Klicken Sie auf **Aktualisieren** oder führen Sie keine andere Aktion aus, bis die Imagedatei 100% hochgeladen zeigt.

- **Aktualisieren:** Klicken Sie auf die Option **Aktualisieren**, um die neuesten Imagedateideails zu erhalten.
- **Löschen:** Klicken Sie auf die Option **Löschen**, um eine vorhandene Imagedatei zu löschen.

Hinweis

- Wenn Sie die virtuelle Firewall-Maschine auf den Sites bereitstellen möchten, die Teil des Nicht-Standardbereichs sind, laden Sie die Imagedatei auf jedem der Collector-Knoten hoch.
- Wenn Sie das Palo Alto VM-Image aus dem SDWAN Center löschen, wird das Image aus dem SDWAN Center-Speicher und NICHT aus der Appliance gelöscht.

3. Gehen Sie zur Provisioning zurück zur Registerkarte **Gehostete Firewall-Sites** und klicken Sie auf **Bereitstellen**.

Provision Virtual Machine

Vendor *

Palo Alto Networks

Vendor Virtual Machine Model *

VM50

Software Image *

PA-VM-KVM-9.0.1.qcow2

Please ensure to upload this image in the collector, for non-default region sites provisioning

Region *

Region1

Sites for Firewall Hosting *

DC () X

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Management Server Secondary IP Address/Domain Name

Enter Management Server Secondary IP Address or domain name

Virtual Machine Authentication Key

Enter the virtual authentication key to be used in the Management server

Authentication Code

Enter the authentication code to be used for licensing

Start Provision

Cancel

- **Anbieter:** Wählen Sie den **Anbieternamen** als **Palo Alto Networks** aus der Dropdown-Liste aus.
- **Vendor Virtual Machine Model:** Wählen Sie die Modellnummer der virtuellen Maschine aus der Liste aus.
- **Software-Image:** Wählen Sie die zu bereitzustellende Imagedatei aus.
- **Region:** Wählen Sie den Teilsektor aus der Liste aus.
- **Sites für Firewall-Hosting:** Wählen Sie Sites für die Liste für Firewall-Hosting aus. Sie

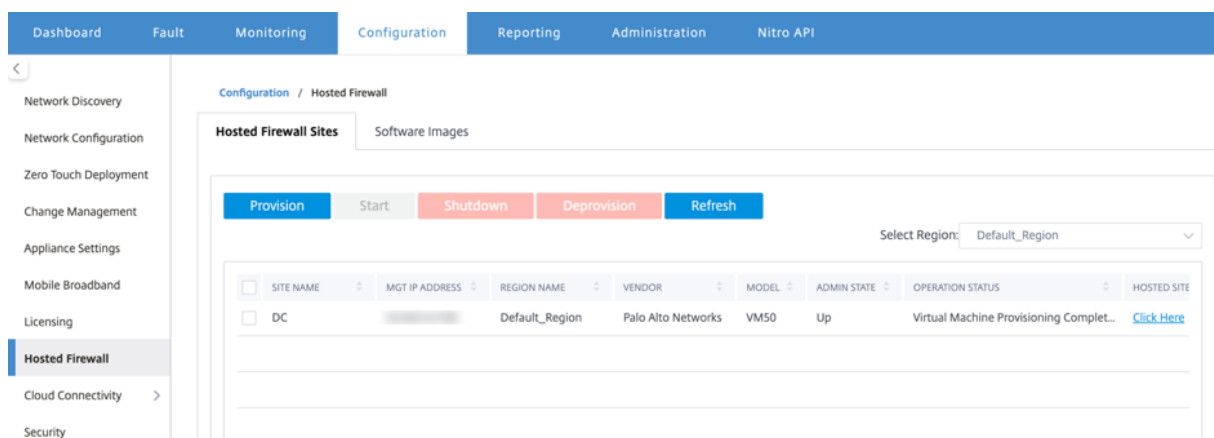
müssen sowohl primäre als auch sekundäre Standorte auswählen, wenn sich die Standorte im Hochverfügbarkeitsmodus befinden.

- **Primäre IP-Adresse/Domänenname des Management Servers:** Geben Sie die primäre IP-Adresse des Managements oder den vollqualifizierten Domännennamen ein (optional).
- **Sekundäre IP-Adresse/Domänenname des Management Servers:** Geben Sie die sekundäre IP-Adresse des Management-Servers oder den vollqualifizierten Domännennamen ein (optional).
- **Authentifizierungsschlüssel für virtuelle Maschinen:** Geben Sie den virtuellen Authentifizierungsschlüssel ein, der im Verwaltungsserver verwendet werden soll.
- **Authentifizierungscode:** Geben Sie den virtuellen Authentifizierungscode ein, der für die Lizenzierung verwendet werden soll.

4. Klicken Sie auf **Bereitstellung starten**.

5. Klicken Sie auf **Aktualisieren**, um den neuesten Status zu erhalten. Nachdem die virtuelle Maschine Palo Alto Networks vollständig gestartet wurde, reflektiert sie die Benutzeroberfläche des SD-WAN Centers.

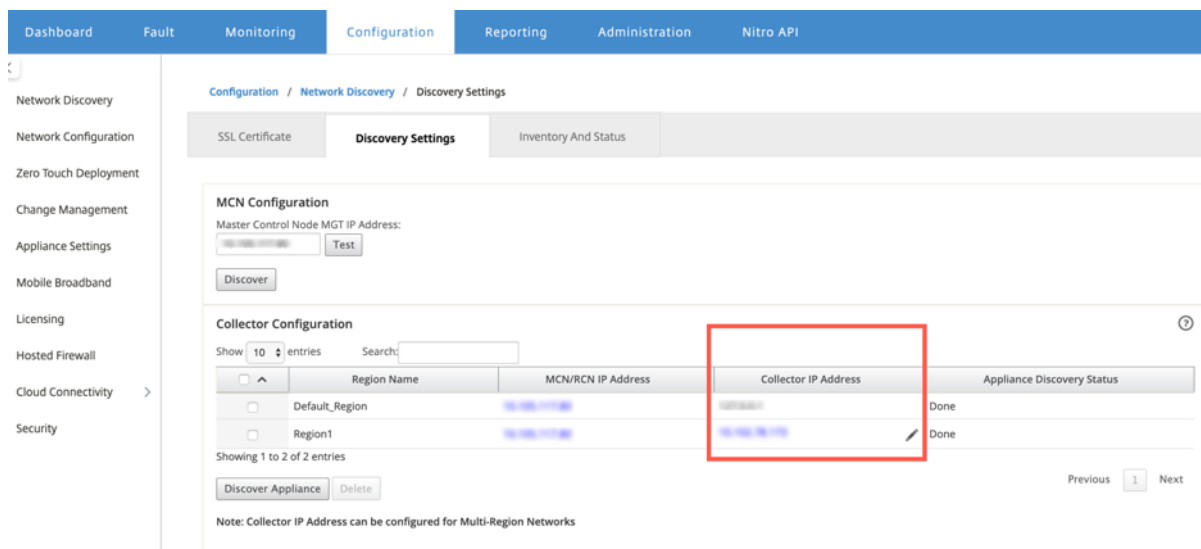
Sie können die virtuelle Maschine nach Bedarf **starten, herunterfahren** und **deaktivieren**.



- **Standortname:** Zeigt den Standortnamen an.
- **Verwaltungs-IP:** Zeigt die Verwaltungs-IP-Adresse des Standorts an.
- **Regionsname:** Zeigt die Regionsbezeichnung an.
- **Lieferant:** Zeigt den Herstellernamen an (Palo Alto Networks).
- **Modell:** Zeigt die Modellnummer (VM50/VM100) an.
- **Administratorstatus:** Status der virtuellen Maschine des Herstellers (Up/Down).
- **Arbeitsvorgangstatus:** Zeigt die Meldung Betriebsstatus an.
- **Gehostete Site:** Verwenden Sie den Link **Hier klicken**, um auf die Benutzeroberfläche der virtuellen Maschine von Palo Alto Networks zuzugreifen.

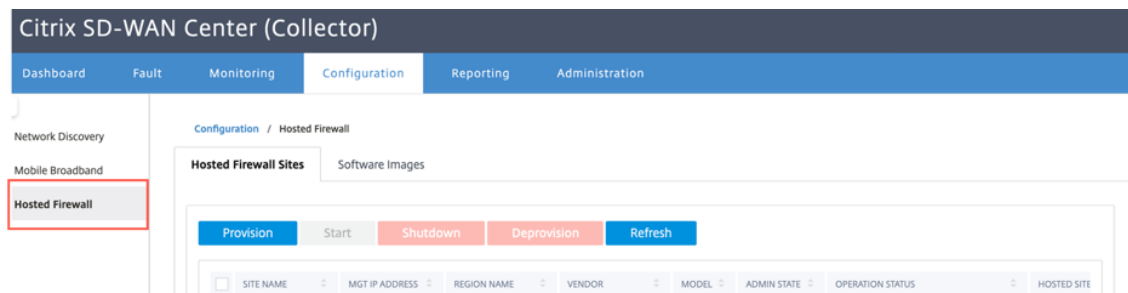
Um die nicht standardmäßigen Regionssites bereitzustellen, müssen Sie das Software-Image auf den SD-WAN Center Collector hochladen. Sie können die Palo Alto Networks sowohl von der SD-WAN Center Head End GUI als auch vom SD-WAN Center Collector bereitstellen.

Um die IP-Adresse des SD-WAN Center Collectors abzurufen, navigieren Sie zu **Konfiguration > Netzwerkerkennung >** wählen Sie die Registerkarte **Ermittlungseinstellungen** aus.



So stellen Sie die Palo Alto Networks vom SD-WAN Collector her:

1. Navigieren Sie in der SD-WAN Collector-GUI zu **Konfiguration >** Wählen Sie **Gehostete Firewall** aus.



2. Wechseln Sie zur Registerkarte **Software-Images**, um das Software-Image hochzuladen.
3. Klicken Sie auf der Registerkarte **Gehostete Firewall-Sites** auf **Bereit**
4. Geben Sie die folgenden Details an und klicken Sie auf **Bereitstellung starten**.

Vendor *

Palo Alto Networks

Vendor Virtual Machine Model *

VM50

Software Image *

PA-VM-KVM-8.1.3.qcow2

Please ensure to upload this image in the collector, for non-default region sites provisioning

Sites for Firewall Hosting *

BRANCH-PA (10.10.10.10) X

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Management Server Secondary IP Address/Domain Name

Enter Management Server Secondary IP Address or domain name

Virtual Machine Authentication Key

Enter the virtual authentication key to be used in the Management server

Authentication Code

Enter the authentication code to be used for licensing

Start Provision Cancel

- **Anbieter:** Wählen Sie den **Anbieternamen** als **Palo Alto Networks** aus der Dropdown-Liste aus.
- **Vendor Virtual Machine Model:** Wählen Sie die Modellnummer der virtuellen Maschine aus der Liste aus.
- **Software-Image:** Wählen Sie die zu bereitzustellende Imagedatei aus.
- **Region:** Wählen Sie den Teilsektor aus der Liste aus.
- **Sites für Firewall-Hosting:** Wählen Sie Sites für die Liste für Firewall-Hosting aus. Sie müssen sowohl primäre als auch sekundäre Standorte auswählen, wenn sich die Standorte im Hochverfügbarkeitsmodus befinden.
- **Primäre IP-Adresse/Domänenname des Management Servers:** Geben Sie die primäre IP-Adresse des Managements oder den vollqualifizierten Domännennamen ein (optional).
- **Sekundäre IP-Adresse/Domänenname des Management Servers:** Geben Sie die

sekundäre IP-Adresse des Management-Servers oder den vollqualifizierten Domännennamen ein (optional).

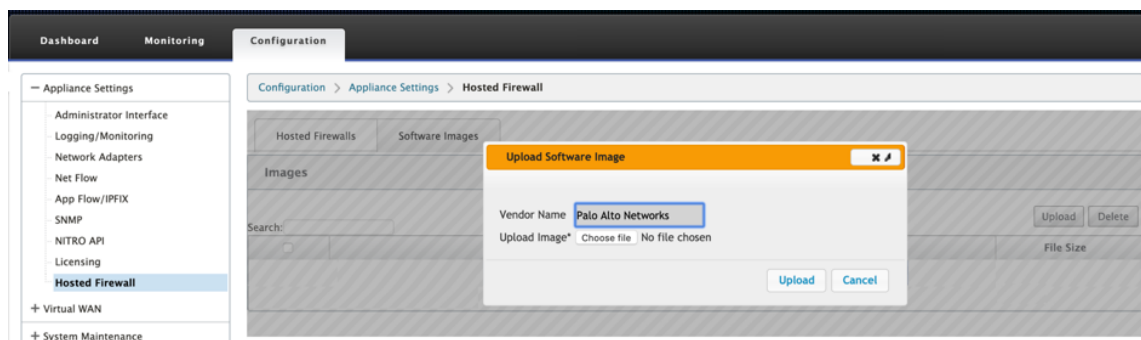
- **Authentifizierungsschlüssel für virtuelle Maschinen:** Geben Sie den virtuellen Authentifizierungsschlüssel ein, der im Verwaltungsserver verwendet werden soll.
- **Authentifizierungscode:** Geben Sie den virtuellen Authentifizierungscode ein, der für die Lizenzierung verwendet werden soll.

5. Klicken Sie auf **Bereitstellung starten**.

Bereitstellung virtueller Maschinen durch die Benutzeroberfläche der SD-WAN-Appliance

Stellen Sie auf der SD-WAN-Plattform die gehostete virtuelle Maschine bereit und starten Sie sie. Führen Sie die folgenden Schritte für die Provisioning:

1. Navigieren Sie in der Citrix SD-WAN GUI zu **Konfiguration > Appliance-Einstellungen** erweitern **>Gehostete Firewall** auswählen.
2. Laden Sie das Softwareimage hoch:
 - Wählen Sie die Registerkarte **Software-Images** . Wählen Sie den Namen des Anbieters als **Palo Alto Networks** aus.
 - Wählen Sie die Softwareimagedatei aus.
 - Klicken Sie auf **Upload**.

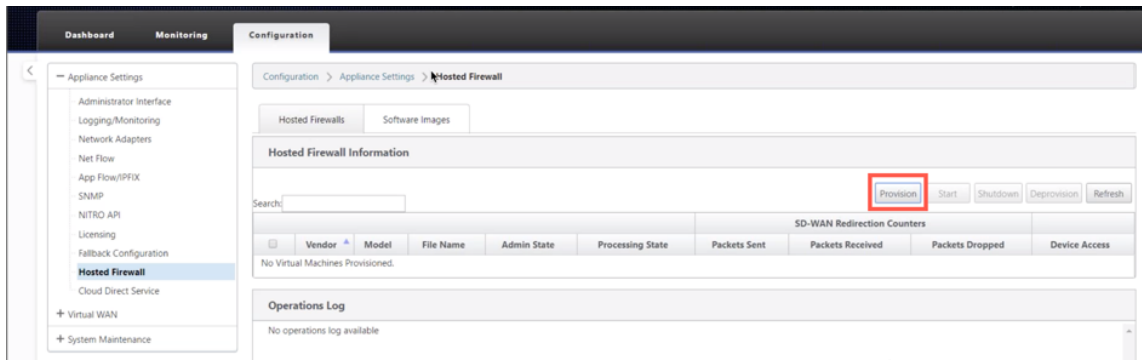


Hinweis:

Es können maximal zwei Software-Images hochgeladen werden. Das Hochladen des Images der virtuellen Maschine Palo Alto Networks kann je nach Verfügbarkeit der Bandbreite länger dauern.

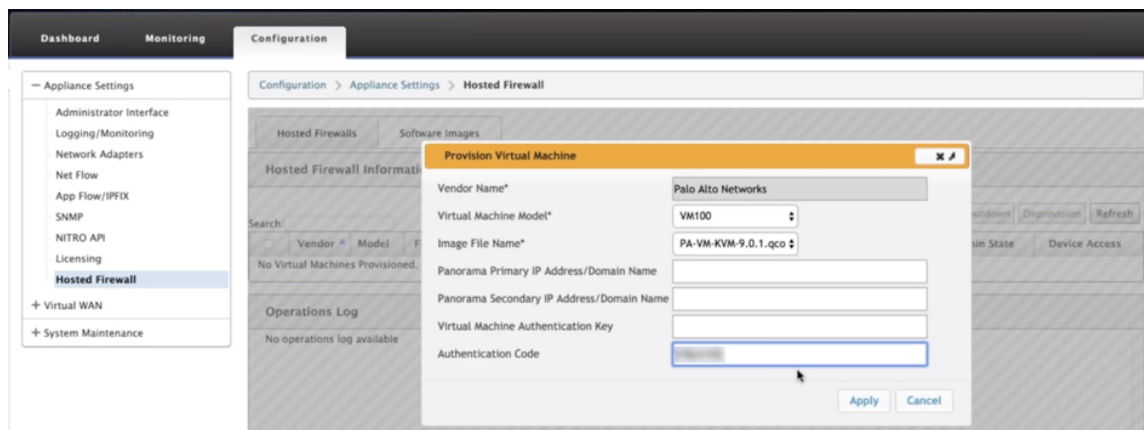
Sie können eine Statusleiste sehen, um den Upload-Prozess zu verfolgen. Das Dateidetail spiegelt sich wieder, sobald das Image erfolgreich hochgeladen wurde. Das für die Provisioning verwendete Image kann nicht gelöscht werden. Führen Sie keine Aktion aus oder gehen Sie zurück zu einer anderen Seite, bis die Imagedatei 100% hochgeladen zeigt.

3. Wählen Sie für die Provisioning die Registerkarte **Gehostete Firewalls** aus und klicken Sie auf **die Schaltfläche Bereitstellen**.

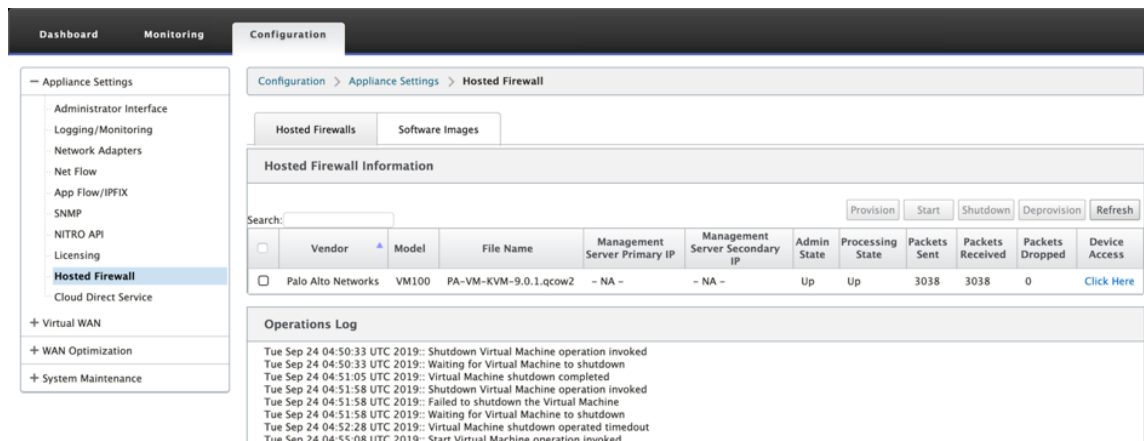


4. Geben Sie die folgenden Details für die Provisioning.

- **Anbietername:** Wählen Sie den Anbieter als **Palo Alto Networks** aus.
- **Modell der virtuellen Maschine:** Wählen Sie die Modellnummer der virtuellen Maschine aus der Liste aus.
- **Name der Imagedatei:** Wählen Sie die Imagedatei aus.
- **Primäre Panorama-IP-Adresse/Domänenname:** Geben Sie die primäre Panorama-IP-Adresse oder den vollqualifizierten Domännennamen an (optional).
- **Sekundäre Panorama-IP-Adresse/Domänenname:** Geben Sie die sekundäre Panorama-IP-Adresse oder den vollqualifizierten Domännennamen an (optional).
- **Authentifizierungsschlüssel für virtuelle Maschinen:** Geben Sie den Authentifizierungsschlüssel für die virtuelle Maschine an (optional).
Der Authentifizierungsschlüssel für virtuelle Maschinen wird für die automatische Registrierung der virtuellen Maschine Palo Alto Networks im Panorama benötigt.
- **Authentifizierungscode:** Geben Sie den Authentifizierungscode (Lizenzcode für virtuelle Maschinen) ein (Optional).
- Klicken Sie auf **Übernehmen**.



5. Klicken Sie auf **Aktualisieren**, um den neuesten Status zu erhalten. Nachdem die virtuelle Maschine Palo Alto Networks vollständig gestartet wurde, reflektiert sie die SD-WAN-Benutzeroberfläche mit den Operations-Protokolldetails.



- **Admin-Status:** Gibt an, ob die virtuelle Maschine hoch- oder heruntergefahren ist.
- **Verarbeitungsstatus:** Datenpfad Verarbeitungsstatus der virtuellen Maschine.
- **Gesendete Pakete:** Pakete, die von SD-WAN an die virtuelle Sicherheitsmaschine gesendet werden.
- **Empfangenes Paket:** Pakete, die von SD-WAN von der virtuellen Sicherheitsmaschine empfangen werden.
- **Paket gelöscht:** Von SD-WAN abgelegte Pakete (z. B. wenn die virtuelle Sicherheitsmaschine ausgefallen ist).
- **Gerätezugriff:** Klicken Sie auf den Link, um den GUI-Zugriff auf die virtuelle Sicherheitsmaschine zu erhalten.

Sie können die virtuelle Maschine nach Bedarf **starten**, **herunterfahren** und **deaktivieren**. Verwenden Sie **hier klicken**, um auf die GUI der virtuellen Maschine von Palo Alto Networks zuzugreifen, oder verwenden Sie Ihre Management-IP zusammen mit 4100 Port (Management-IP: 4100).

Hinweis

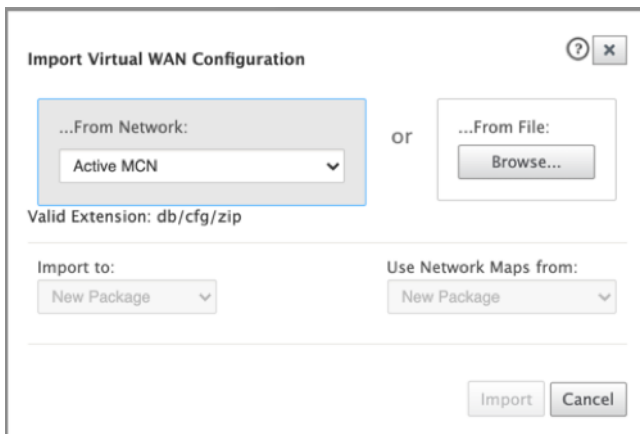
Verwenden Sie immer den Inkognito-Modus, um auf die Palo Alto Networks GUI zuzugreifen.

Traffic-Umleitung

Die Konfiguration der Datenverkehrsumleitung kann sowohl über den Konfigurationseditor auf MCN als auch den Konfigurationseditor im SD-WAN Center erfolgen.

So navigieren Sie im SD-WAN Center durch den Konfigurationseditor:

1. Öffnen Sie Citrix SD-WAN Center UI, navigieren Sie zu **Konfiguration > Netzwerkkonfigurationsimport**. Importieren Sie die virtuelle WAN-Konfiguration aus dem aktiven MCN und klicken Sie auf **Importieren**.



Die restlichen Schritte sind ähnlich wie folgt - die Konfiguration der Datenverkehrsumleitung über MCN.

So navigieren Sie durch den Konfigurationseditor auf MCN:

1. Setzen Sie **Verbindungsanpassungstyp** unter **Global > Netzwerkeinstellungen** auf **Symmetrisch**.

Global

- Network Settings
- Regions
- Centralized Licensing
- Hosted Firewall Template
- Routing Domains
- Applications
- Application QoS
- Firewall Zones
- Firewall Policy Templates
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- DNS Services
- Proxy Auto-config settings
- Autopath Groups
- Service Providers
- WAN-to-WAN Forwarding Groups
- WAN Optimization Features
- WAN Optimization Tuning Settings
- WAN Optimization Application Classifiers
- WAN Optimization Service Classes

Global Security Settings

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode: AES 128-Bit

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type: 32-Bit Checksum

☐ Enable FIPS Mode

☐ Enable Appliance Authentication

Network Secure Key: 72d050ce5ca54c... **Regenerate**

Global Firewall Settings

Global Policy Template: New_Firewall_... Default Firewall Action: Allow ☒ Default Connection State Tracking

Connection Match Type: Symmetric

Denied Timeout (s): 30

TCP Initial Timeout (s): 120 TCP Idle Timeout (s): 7440

TCP Closing Timeout (s): 60 TCP Time Wait Timeout (s): 120 TCP Closed Timeout (s): 10

UDP Initial Timeout (s): 30 UDP Idle Timeout (s): 300

ICMP Initial Timeout (s): 30 ICMP Idle Timeout (s): 60

Generic Initial Timeout (s): 30 Generic Idle Timeout (s): 300

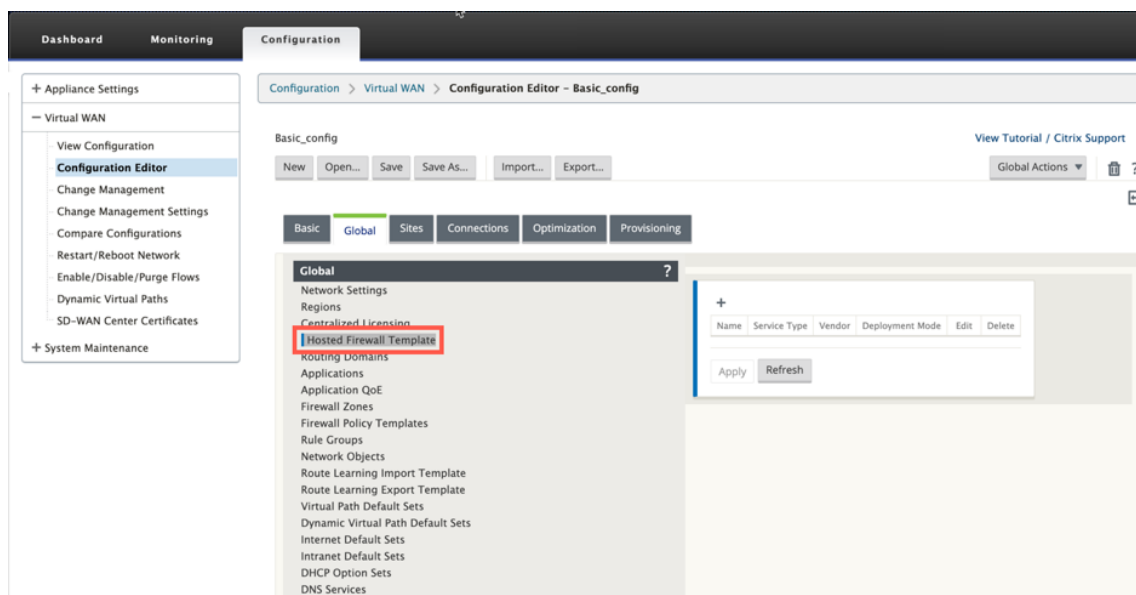
Global On-Demand Bandwidth Limit Setting

Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%): 120

Apply **Revert**

Standardmäßig sind SD-WAN-Firewallrichtlinien richtungsspezifisch. Der symmetrische Übereinstimmungstyp entspricht den Verbindungen anhand der angegebenen Übereinstimmungskriterien und wendet die Richtlinienaktion in beide Richtungen an.

- Öffnen Sie **Citrix SD-WAN UI**, navigieren Sie zu **Konfiguration** erweitern **Virtual WAN** wählen Sie **Konfigurationseditor** > wählen Sie **Gehostete Firewall-Vorlage** im Abschnitt **Global**



3. Klicken Sie auf + und geben Sie die erforderlichen Informationen an, die im folgenden Screenshot verfügbar sind, um die Vorlage **Hosted Firewall** hinzuzufügen, und klicken Sie auf **Hinzufügen**.

Edit

Name:

PaloAlto-NGFW

Vendor:

Palo Alto Networks

Model:

VM50

Deployment Mode:

Virtual Wire

Primary Management Server IP/FQDN:

Secondary Management Server IP/FQDN:

Service Redirection Interfaces

+

| Name | Input Interface | Output Interface | VLAN ID | Delete |
|--------------|-----------------|------------------|---------|--------|
| INTERNET-OUT | Interface-1 | Interface-2 | 0 | |
| INTERNET-IN | Interface-2 | Interface-1 | 0 | |

Apply

Cancel

Mit der **gehosteten Firewall-Vorlage** können Sie die Verkehrsanleitung zu der **virtuellen Firewall-Maschine** konfigurieren, die auf der SD-WAN-Appliance gehostet wird. Die folgenden Eingaben sind für die Konfiguration der Vorlage erforderlich:

- **Name:** Name der gehosteten Firewall-Vorlage.
- **Hersteller:** Name des Firewall-Herstellers.
- **Bereitstellungsmodus:** Das Feld “**Bereitstellungsmodus**” wird automatisch ausgefüllt und ausgegraut. Für den Anbieter von **Palo Alto Networks** ist der Bereitstellungsmodus **Virtual**

Wire.

- **Modell:** Virtual Machine-Modell der gehosteten Firewall. Sie können die Modellnummer der virtuellen Maschine als VM 50/VM 100 für den Palo Alto Networks-Anbieter auswählen.
- **Primärer Managementserver IP/FQDN:** Primärer Managementserver IP/FQDN von Panorama.
- **Sekundärer Managementserver IP/FQDN:** Sekundärer Managementserver IP/FQDN von Panorama.
- **Dienstumleitungsschnittstellen:** Dies sind logische Schnittstellen, die für die Verkehrsumleitung zwischen SD-WAN und gehosteter Firewall verwendet werden.

Interface-1, Interface-2 bezieht sich auf die ersten beiden Schnittstellen auf der gehosteten Firewall. Wenn VLANs für die Verkehrsumleitung verwendet werden, müssen dieselben VLANs auf der gehosteten Firewall konfiguriert werden. VLANs, die für die Verkehrsumleitung konfiguriert sind, sind intern zum SD-WAN und zur gehosteten Firewall.

Hinweis

Die Umleitungseingabeschnittstelle muss aus der Richtung des Verbindungsinitiators ausgewählt werden, die Umleitungsschnittstelle wird automatisch für den Antwortverkehr ausgewählt. Wenn beispielsweise ausgehender Internetverkehr an die gehostete Firewall auf Schnittstellen1 umgeleitet wird, wird der Antwortverkehr automatisch zur gehosteten Firewall auf Schnittstellen2 umgeleitet. Es besteht keine Notwendigkeit von Interface-2 im obigen Beispiel, wenn kein eingehender Internet-Datenverkehr vorhanden ist.

Zum Hosten der Palo Alto Networks-Firewall sind nur zwei physikalische Schnittstellen zugewiesen. Wenn Datenverkehr aus mehreren Zonen an die gehostete Firewall weitergeleitet werden muss, können mithilfe interner VLANs mehrere Unterschnittstellen erstellt und verschiedenen Firewallzonen auf der gehosteten Firewall zugeordnet werden.

Über SD-WAN-Firewallrichtlinien oder Richtlinien auf Standortebene können Sie den gesamten Datenverkehr auf die virtuelle Maschine Palo Alto Networks umleiten.

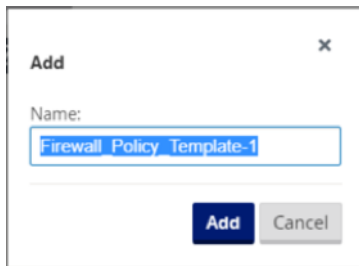
Hinweis

SD-WAN-Firewall-Richtlinien werden automatisch erstellt, um den Datenverkehr zu/von gehosteten Firewall-Verwaltungsservern **Zulassen**. Dadurch wird eine Umleitung des Verwaltungsdatenverkehrs vermieden, der von einer gehosteten Firewall stammt (oder).

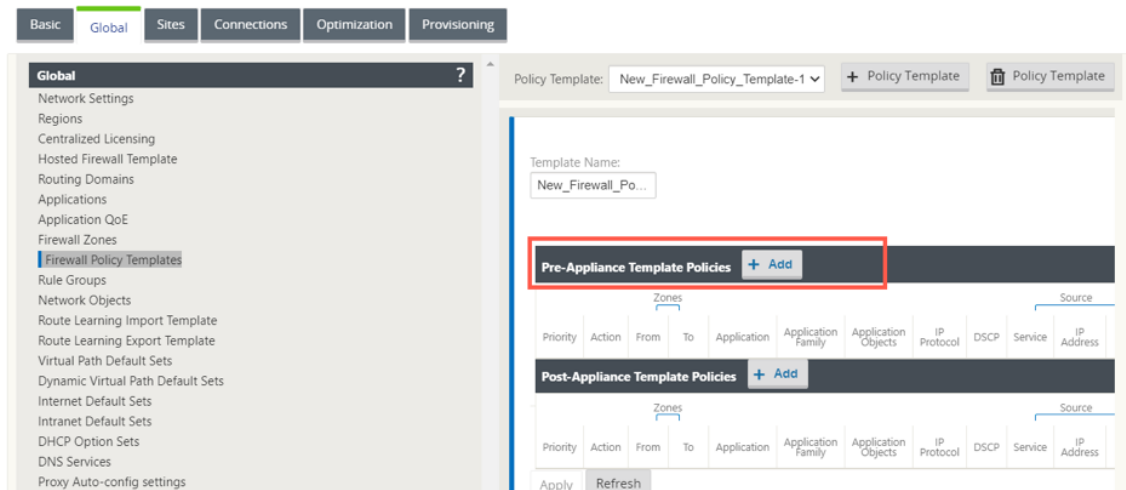
Die Umleitung des Datenverkehrs zur virtuellen Firewall-Maschine kann mithilfe von SD-WAN-Firewall-Richtlinien erfolgen. Es gibt zwei Methoden zum Erstellen von SD-WAN-Firewall-Richtlinien - entweder über Firewall-Richtlinienvorlagen im **globalen** Abschnitt oder auf Site-Ebene.

Methode - 1

1. Navigieren Sie von Citrix SD-WAN GUI zu **Konfiguration** erweitern Sie **Virtual WAN > Konfigurations-Editor**. Navigieren Sie zur Registerkarte **Global** und wählen Sie **Firewall-Richtlinienvorlagen** aus. Klicken Sie auf **+ Richtlinienvorlage**. Geben Sie der Richtlinienvorlage einen Namen an und klicken Sie auf **Hinzufügen**.



2. Klicken Sie auf **+ Hinzufügen** neben **Richtlinien für Pre-Appliance-Vorlagen**.



3. Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch auf **Redirect** gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdown-Liste aus. Füllen Sie die anderen Übereinstimmungskriterien nach Bedarf aus.

Priority: Policy Type: **Hosted Firewall** ▼

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

Traffic Match Type: **IP Protocol** ▼ IP Protocol: **Any** ▼ DSCP: **Any** ▼ ☐ Match Established

Application Objects: **Any** ▼

Source Service Type: **Any** ▼ Source Service Name: **Any** ▼ Source IP: Source Port:

Dest Service Type: **Any** ▼ Dest Service Name: **Any** ▼ Dest IP: Dest Port:

Actions

Action: **Redirect** ▼ ☒ Allow Fragments Connection State Tracking: **No Tracking** ▼

Hosted Firewall Template: **PaloAlto-NGFW** ▼ Service Redirection Interface: **INTERNET-OUT** ▼

4. Navigieren Sie zu den **Verbindungen > Firewall** und wählen Sie dann die Firewall-Richtlinie (die Sie erstellt haben) unter dem Namensfeld aus. Klicken Sie auf **Übernehmen**.

Basic Global Sites **Connections** Optimization Provisioning

Region: **Default_Region** ▼

Site: **BR1100** ▼ [+ Site](#) [Site](#) [Site](#)

Connections ?

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall**
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups

Section: **Settings** ▼

Policy Templates + ?

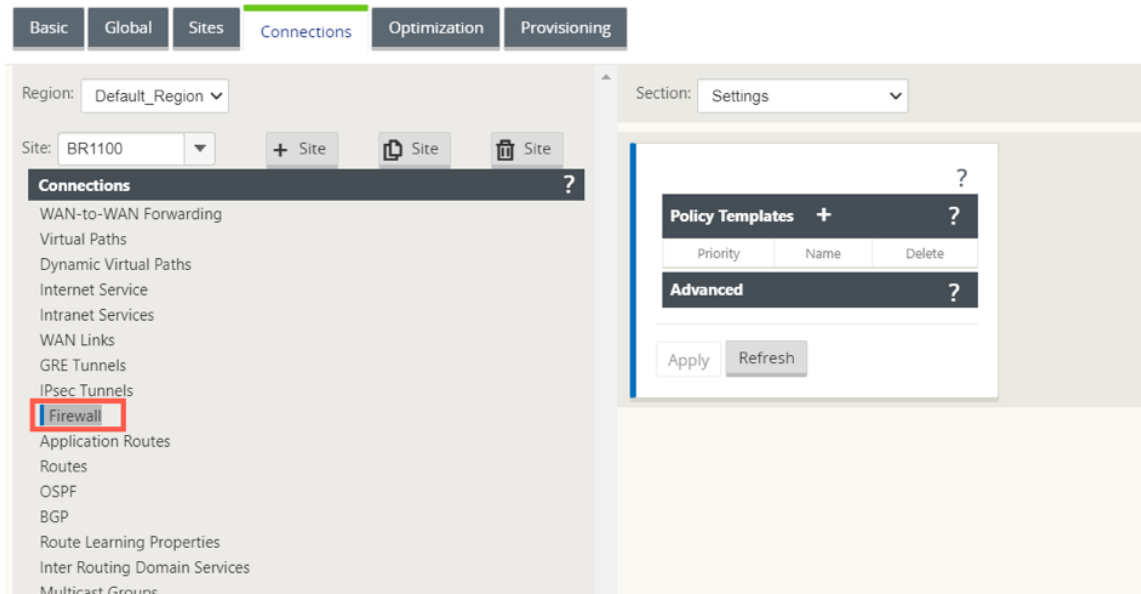
| Priority | Name | Delete |
|----------|----------------------------|-------------------|
| 100 | New_Firewall_P... ▼ | ↶ |

Advanced ?

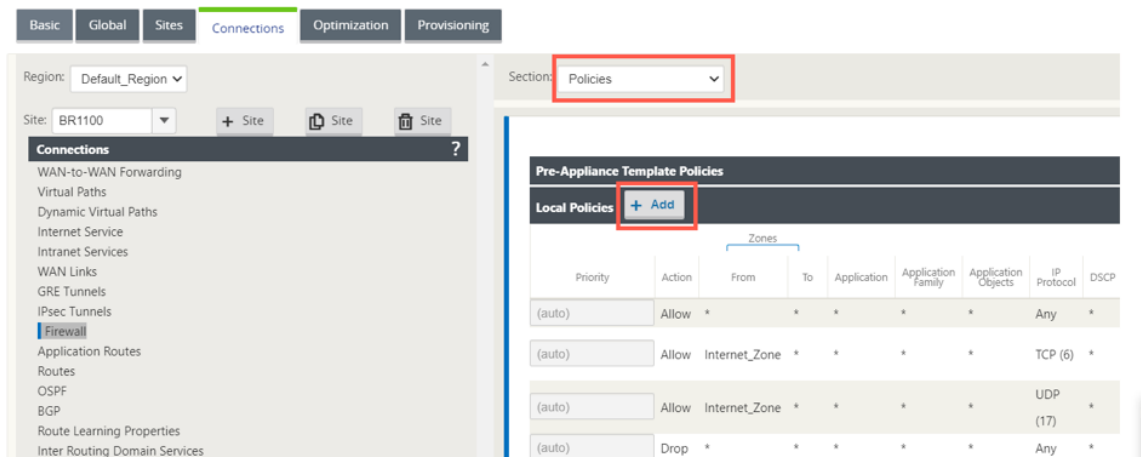
[Apply](#) [Revert](#)

Methode - 2

- Um den gesamten Datenverkehr umzuleiten, navigieren Sie unter dem **Konfigurationseditor** > **Virtual WAN** zur Registerkarte **Verbindung** und wählen Sie **Firewall** aus.



- Wählen Sie in der Dropdown-Liste **Abschnitt** die Option **Richtlinien** aus und klicken Sie auf **+Hinzufügen**, um eine neue Firewall-Richtlinie zu erstellen.



- Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch auf **Redirect** gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdown-Liste aus. Klicken Sie auf **Hinzufügen**.

Priority:
100

Policy Type:
Hosted Firewall

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

Traffic Match Type:
IP Protocol

IP Protocol:
Any

DSCP:
Any

☐ Match Established

Application Objects:
Any

Source Service Type:
Any

Source Service Name:
Any

Source IP:
*

Source Port:
*

Dest Service Type:
Any

Dest Service Name:
Any

Dest IP:
*

Dest Port:
*

Actions

Action:
Redirect

☒ Allow Fragments

Connection State Tracking:
No Tracking

Hosted Firewall Template:
PaloAlto-NGFW

Service Redirection Interface:
INTERNET-OUT

Während die gesamte Netzwerkkonfiguration ausgeführt wird, können Sie die Verbindung unter **Überwachung > Firewall** > unter **Statistikliste** überwachen und **Richtlinien filtern**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Firewall

Firewall Statistics

Statistics: Filter Policies

Maximum entries to display: 50

Filtering: Application: Any Family: Any IP Protocol: Any

Filter Policy Action: Any Source Service Type: Any Source Service Name: Any Source IP: *

Destination Service Type: Any Destination Service Name: Any Destination IP: *

Source Port: * Destination Port: * Source Zone: Any Destination Zone: Any DSCP: Any

Refresh

Show latest data.

Help

Filter Policies

Default Policy=Allow(Not Tracked) Packets=42 Bytes=3528

Match In Progress Packets=0 Bytes=0

| ID | Application | Family | IP Protocol | DSCP | Service Type | Service Name | IP Address | Port or ICMP Type | Zone | Service Type | Service Name | IP Address | Port or ICMP Code | Zone | Action | Conn Match Type | Track Connection | Allow Fragments |
|----|-------------|--------|-------------|------|--------------|--------------|------------|-------------------|---------------|--------------|--------------|-------------------|-------------------|------|----------|-----------------|------------------|-----------------|
| 1 | * | * | * | * | * | - | * | NA | * | Internet | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 2 | * | * | * | * | Internet | - | * | NA | * | * | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 3 | * | * | * | * | * | - | * | NA | * | Virtual Path | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 4 | * | * | * | * | Virtual Path | - | * | NA | * | * | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 5 | * | * | * | * | IPHost | - | * | NA | * | * | - | * | NA | * | Allow | Symmetric | No | Yes |
| 6 | * | * | TCP | * | Internet | - | * | * | Internet_Zone | * | - | 172.147.93.174/32 | 5001 | * | Allow | Symmetric | No | Yes |
| 7 | * | * | UDP | * | Internet | - | * | * | Internet_Zone | * | - | 172.147.93.174/32 | 5001 | * | Allow | Symmetric | No | Yes |
| 8 | * | * | * | * | Internet | - | * | NA | * | * | - | * | NA | * | Drop | Symmetric | No | Yes |

Filter Policies Displayed: 8

Filter Policies In Use: 8/1000

Sie können die Zuordnung zwischen der Konfiguration, die Sie in der SD-WAN-Servicekettenvorlage vorgenommen haben, und der Konfiguration von Palo Alto Network mithilfe der Benutzeroberfläche von Palo Alto Networks überprüfen.

paloalto

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Commit

Config

Search

Interfaces

VLANs

Virtual Wires

Virtual Routers

IPSec Tunnels

GRE Tunnels

DHCP

DNS Proxy

GlobalProtect

Portals

Gateways

MDM

Device Block List

Clientless Apps

Clientless App Groups

QoS

LLDP

Network Profiles

GlobalProtect IPSec Crypto

IKE Gateways

IPSec Crypto

IKE Crypto

Monitor

Interface Mgmt

Zone Protection

QoS Profile

LLDP Profile

MBFD Profile

Ethernet

VLAN

Loopback

Tunnel

| Interface | Interface Type | Management Profile | Link State | IP Address | Virtual Router | Tag | VLAN / Virtual Wire | Security Zone | Features | Comment |
|----------------|----------------|--------------------|------------|------------|----------------|----------|---------------------|---------------|----------|---------|
| ethernet1/1 | Virtual Wire | | none | none | none | Untagged | VWIRE-INET | LAN | | |
| ethernet1/1.10 | Virtual Wire | | none | none | none | 10 | VWIRE-INTRANET | LAN | | |
| ethernet1/2 | Virtual Wire | | none | none | none | Untagged | VWIRE-INET | Internet | | |
| ethernet1/2.10 | Virtual Wire | | none | none | none | 10 | VWIRE-INTRANET | Internet | | |
| ethernet1/3 | | | none | none | none | Untagged | none | none | | |
| ethernet1/4 | | | none | none | none | Untagged | none | none | | |
| ethernet1/5 | | | none | none | none | Untagged | none | none | | |
| ethernet1/6 | | | none | none | none | Untagged | none | none | | |
| ethernet1/7 | | | none | none | none | Untagged | none | none | | |
| ethernet1/8 | | | none | none | none | Untagged | none | none | | |
| ethernet1/9 | | | none | none | none | Untagged | none | none | | |
| ethernet1/10 | | | none | none | none | Untagged | none | none | | |
| ethernet1/11 | | | none | none | none | Untagged | none | none | | |
| ethernet1/12 | | | none | none | none | Untagged | none | none | | |
| ethernet1/13 | | | none | none | none | Untagged | none | none | | |
| ethernet1/14 | | | none | none | none | Untagged | none | none | | |
| ethernet1/15 | | | none | none | none | Untagged | none | none | | |
| ethernet1/16 | | | none | none | none | Untagged | none | none | | |

HINWEIS:

Die virtuelle Maschine von Palo Alto Networks kann nicht bereitgestellt werden, wenn **Cloud Direct** oder **SD-WAN WANOP (PE)** bereits auf der 1100 Appliance bereitgestellt werden.

Anwendungsfälle —Hosted Firewall auf SD-WAN 1100

Im Folgenden sind einige der Anwendungsfallszenarien aufgeführt, die mithilfe der Citrix SD-WAN 1100 -Appliance implementiert werden:

Anwendungsfall 1: Umleiten des gesamten Datenverkehrs in die Hosted Firewall

Dieser Anwendungsfall gilt für Anwendungsfälle in kleinen Zweigstellen, in denen der gesamte Datenverkehr von der gehosteten Firewall der nächsten Generation verarbeitet wird. Die Bandbreitenanforderungen müssen berücksichtigt werden, da der Durchsatz des umgeleiteten Datenverkehrs auf 100 Mbit/s begrenzt ist.

Um dies zu erreichen, erstellen Sie eine Firewall-Regel, die mit jedem Datenverkehr und **Action** as **Redirect** übereinstimmt, wie im folgenden Screenshot gezeigt:

Priority: 100

Policy Type: Hosted Firewall

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

☐ Match Established

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: *

Dest IP: *

Dest Port: *

Actions

Action: Redirect

☒ Allow Fragments

Connection State Tracking: No Tracking

Hosted Firewall Template: PA-Template

Service Redirection Interface: PA-Intf

Anwendungsfall 2: Nur Internetverkehr in die Hosted Firewall umleiten

Dieser Anwendungsfall gilt für alle Zweigstellen, bei denen Internet-gebundener Datenverkehr den Umfang des unterstützten umgeleiteten Datenverkehrs nicht überschreitet. In diesem Fall wird der Datenverkehr zwischen Rechenzentren von Sicherheitsgeräten/-diensten verarbeitet, die in Rechenzentren bereitgestellt werden.

Um dies zu erreichen, erstellen Sie eine Firewall-Regel, die mit jedem Datenverkehr und **Action** als **Redirect** übereinstimmt, wie im folgenden Screenshot gezeigt:

Priority: 100

Policy Type: Hosted Firewall

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

Match Established: ☐

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Internet

Dest Service Name: Any

Dest IP: *

Dest Port: *

Actions

Action: Redirect

Allow Fragments: ☒

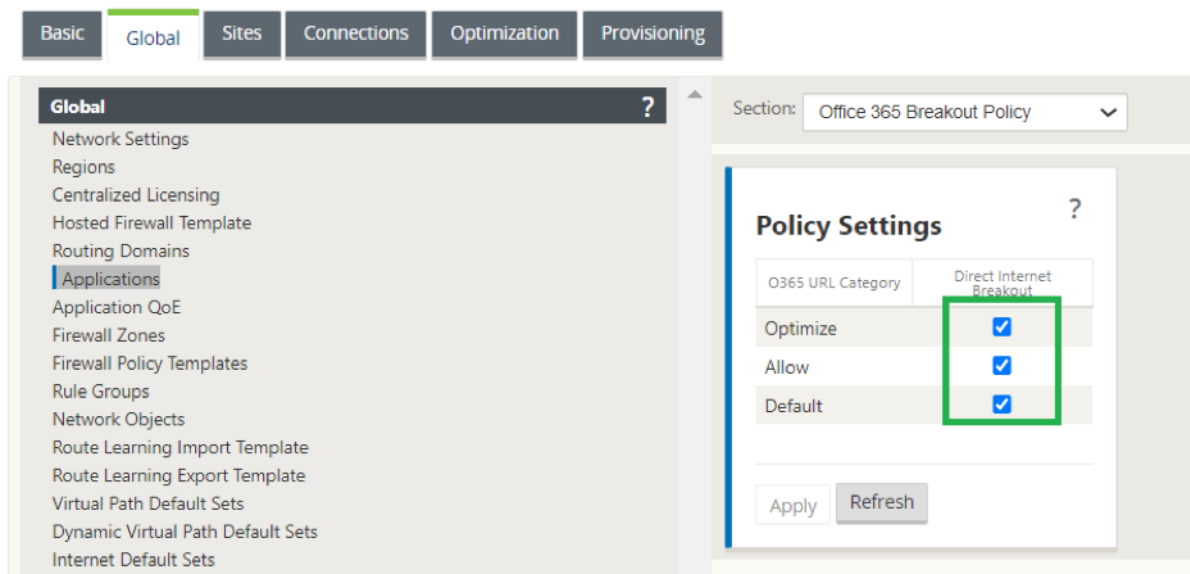
Connection State Tracking: No Tracking

Hosted Firewall Template: PA-Template

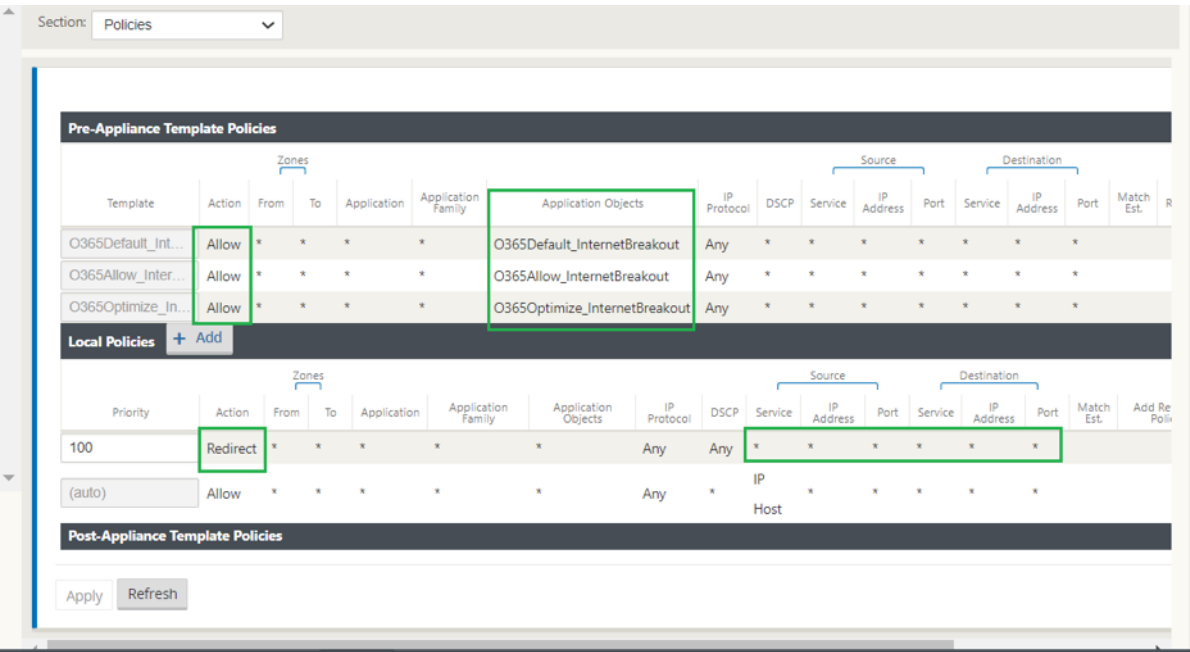
Service Redirection Interface: PA-Intf

Anwendungsfall 3: Direkter Internet-Breakout für vertrauenswürdige Internet-SaaS-Anwendungen und Weiterleitung des verbleibenden gesamten Datenverkehrs auf die gehostete VM

In diesem Anwendungsfall wird eine Firewallregel hinzugefügt, um einen direkten Internet-Breakout für vertrauenswürdige SaaS-Anwendungen wie Office 365 durchzuführen. Aktivieren Sie zunächst Office 365 Breakout Policy, wie im folgenden Screenshot gezeigt:



Dadurch werden automatisch **Richtlinien für Pre-Appliance-Vorlagen** hinzugefügt, um Office 365-Datenverkehr zuzulassen, wie im folgenden Screenshot gezeigt. Fügen Sie nun eine Firewall-Regel hinzu, um den verbleibenden gesamten Datenverkehr an die gehostete Firewall umzuleiten, wie



Hinweis:

Die Konfiguration der gehosteten Firewall ist unabhängig von der Citrix SD-WAN SD-WAN-Konfiguration. Daher kann die gehostete Firewall gemäß den Sicherheitsanforderungen des Unternehmens konfiguriert werden.

Check Point Firewall-Integration auf SD-WAN 1100 Plattform

May 10, 2021

Citrix SD-WAN unterstützt das Hosten von **Check Point CloudGuard Edge** auf der SD-WAN 1100 Plattform.

Der **Check Point CloudGuard Edge** wird als virtuelle Maschine auf der SD-WAN 1100 Plattform ausgeführt. Die virtuelle Firewall-Maschine ist im Bridge-Modus mit zwei virtuellen Datenschnittstellen integriert. Erforderlicher Datenverkehr kann durch Konfigurieren von Richtlinien auf SD-WAN an die virtuelle Firewall-Maschine umgeleitet werden.

Vorteile

Im Folgenden werden die wichtigsten Ziele oder Vorteile der Check Point-Integration auf der SD-WAN 1100 Plattform aufgeführt:

- Zweigerätekonsolidierung: Eine einzige Appliance, die sowohl SD-WAN als auch erweiterte Sicherheit bietet
- Sicherheit in Zweigstellen mit On-Prem NGFW (Next Generation Firewall) zum Schutz von LAN-zu-LAN-, LAN-zu-Internet- und Internet-zu-LAN-Datenverkehr

Konfigurationsschritte

Die folgenden Konfigurationen sind erforderlich, um die virtuelle Check Point-Firewall-Maschine auf SD-WAN zu integrieren:

- Bereitstellen der virtuellen Firewall-Maschine
- Aktivieren der Datenverkehrsumleitung zur virtuellen Sicherheitsmaschine

Hinweis:

Die virtuelle Maschine der Firewall muss zuerst bereitgestellt werden, bevor die Datenverkehrsumleitung aktiviert wird.

Bereitstellen der virtuellen Maschine der Check Point Firewall

Es gibt zwei Möglichkeiten, die virtuelle Firewall-Maschine bereitzustellen:

- Provisioning über SD-WAN Center
- Provisioning über die Benutzeroberfläche der SD-WAN-Appliance

Provisioning virtueller Maschinen in der Firewall über das SD-WAN Center

Voraussetzungen

- Fügen Sie dem SD-WAN Center den sekundären Speicher hinzu, um die Firewall-VM-Imagedateien zu speichern. Weitere Informationen finden Sie unter [Systemanforderungen und Installation](#).
- Reservieren Sie den Speicher von der sekundären Partition für die Firewall-VM-Imagedateien. Um das Speicherlimit zu konfigurieren, navigieren Sie zu **Administration > Speicherwartung**.
 - Wählen Sie den erforderlichen Speicherbetrag aus der Liste aus.
 - Klicken Sie auf **Übernehmen**.

Administration / Storage Maintenance

Region: Default_Region

| Host | File System | Type | Size (MB) | Available (MB) | Active/Migrate Data |
|--------|-------------|------|-----------|----------------|---------------------|
| Local* | /dev/xvda2 | ext3 | 7288 | 3471 | |
| Local | /dev/xvdb | ext3 | 14910 | 12921 | |

Apply

Note: Software image storage reserved will be reduced while calculating the secondary partition Size(MB) and Available(MB)

Software Image Storage Reservation

Note: User can modify the storage reservation only if the SD-WAN Center has secondary partition mounted and it should operate in headend mode

Amount of storage to reserve from secondary partition storage(Active) is: 10GB

Apply

Thresholds

SD-WAN Center Database Storage and Auto Cleanup settings are misconfigured. SD-WAN Center will reach auto cleanup threshold before the configured 6 months.

Stop stats polling when storage usage exceeds 55% of active storage size

☐ Notify user when storage usage exceeds 10% of active storage size

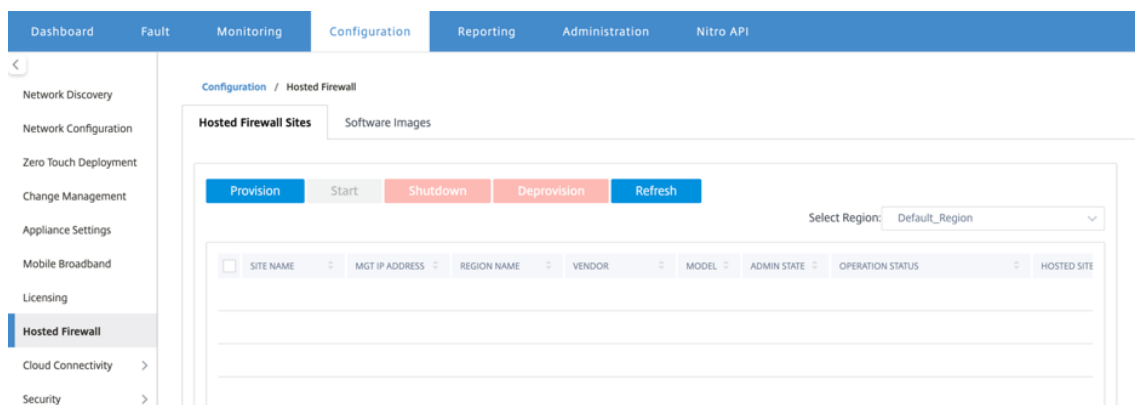
Apply

Hinweis:

Speicher ist einer sekundären Partition reserviert, die aktiv ist, wenn die Bedingung erfüllt ist.

Führen Sie die folgenden Schritte aus, um Provisioning Firewall-Maschine über die SD-WAN Center-Plattform bereitzustellen:

1. Navigieren Sie in der Citrix SD-WAN Center-GUI zu **Konfiguration** > Wählen Sie **Gehostete Firewall** aus.



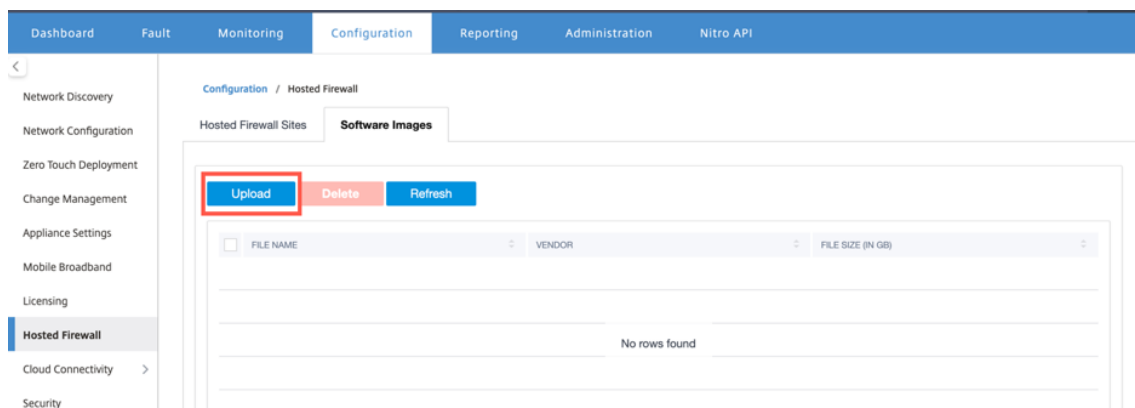
Sie können die **Region** aus der Dropdown-Liste auswählen, um die bereitgestellten Site-Details für diese ausgewählte Region anzuzeigen.

2. Laden Sie das Softwareimage hoch.

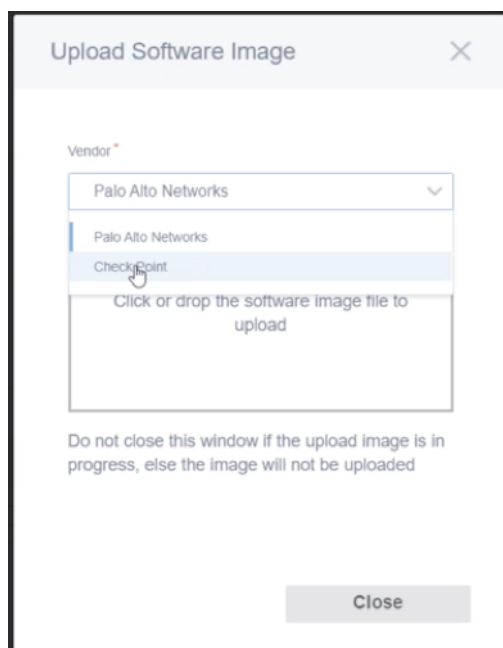
Hinweis

Stellen Sie sicher, dass Sie über genügend Speicherplatz verfügen, um das Software-Image hochzuladen.

Navigieren Sie zu **Konfiguration > Gehostete Firewall > Software-Images** und klicken Sie auf **Hochladen**.



3. Wählen Sie in der Dropdown-Liste den Namen des Anbieters als **Check Point** aus. Klicken oder legen Sie die Softwareimage-Datei in das Feld für den Upload ab.



Eine Statusleiste mit dem laufenden Upload-Prozess wird angezeigt. Klicken Sie auf **Aktualisieren** oder führen Sie keine andere Aktion aus, bis die Imagedatei 100% hochgeladen zeigt.

- **Aktualisieren:** Klicken Sie auf **Aktualisieren**, um die neuesten Imagedateidetails abzurufen.
- **Löschen:** Klicken Sie auf **Löschen**, um eine vorhandene Imagedatei zu löschen.

Hinweis

Um die virtuelle Firewall-Maschine auf dem Site-Teil einer nicht standardmäßigen Region bereitzustellen, laden Sie die Image-Datei auf jedem Collector-Knoten hoch.

4. Gehen Sie zur Provisioning zurück zur Registerkarte **Gehostete Firewall-Sites** und klicken Sie auf **Bereitstellen**.

Provision Virtual Machine

Vendor *

Check Point

Vendor Virtual Machine Model *

EDGE

Region *

Region where the sites available

Software Image *

Choose the Image to provision

Please ensure to upload this image in the collector for non-default region sites provisioning

Sites for Firewall Hosting *

Sites to host the firewall

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Virtual Machine SIC Key

Enter the SIC key

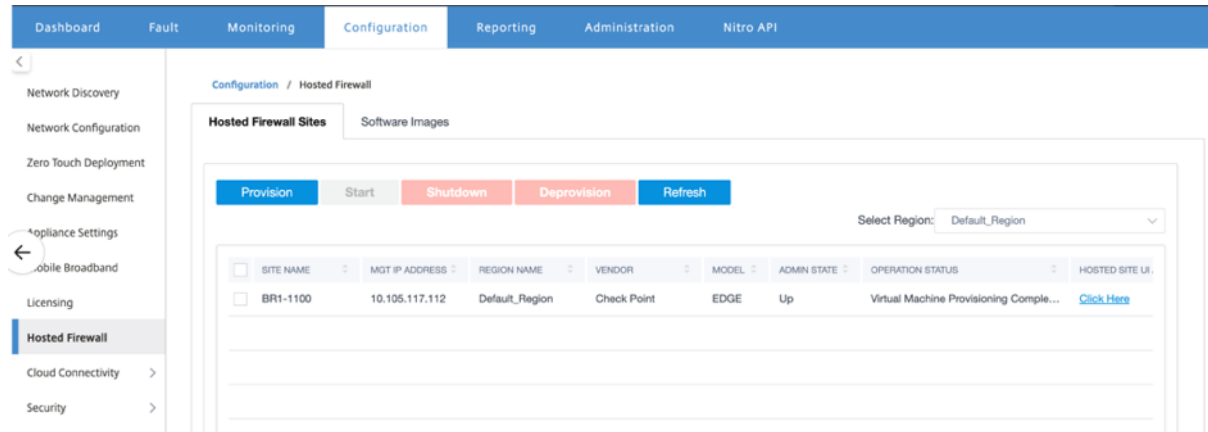
Start Provision Cancel

- **Anbieter:** Wählen Sie den Namen des Anbieters als **Check Point** aus der Dropdown-Liste aus.
- **Vendor Virtual Machine Model:** Das Feld “VM-Modell” wird automatisch als Edge gefüllt.
- **Region:** Wählen Sie den Teilsektor aus der Liste aus.
- **Software-Image:** Wählen Sie die zu bereitzustellende Imagedatei aus.
- **Sites für Firewall-Hosting:** Wählen Sie Sites für die Liste für Firewall-Hosting aus. Sie müssen sowohl primäre als auch sekundäre Standorte auswählen, wenn sich die Standorte im Hochverfügbarkeitsmodus befinden.
- **Primäre IP-Adresse/Domänenname des Management Servers:** Geben Sie die primäre IP-Adresse des Managements oder den vollqualifizierten Domännennamen ein (optional).
- **SIC-Schlüssel der virtuellen Maschine:** Geben Sie den Secure Internal Communication (SIC) -Schlüssel der virtuellen Maschine ein. SIC schafft vertrauenswürdige Verbindungen zwischen **Check Point-Komponenten**.

5. Klicken Sie auf **Bereitstellung starten**.

6. Klicken Sie auf **Aktualisieren**, um den neuesten Status zu erhalten. Nachdem die virtuelle Check Point-Maschine vollständig gestartet wurde, wird sie auf der Benutzeroberfläche des SD-WAN Centers angezeigt.

Sie können die virtuelle Maschine nach Bedarf **starten**, **herunterfahren** und **deaktivieren**.

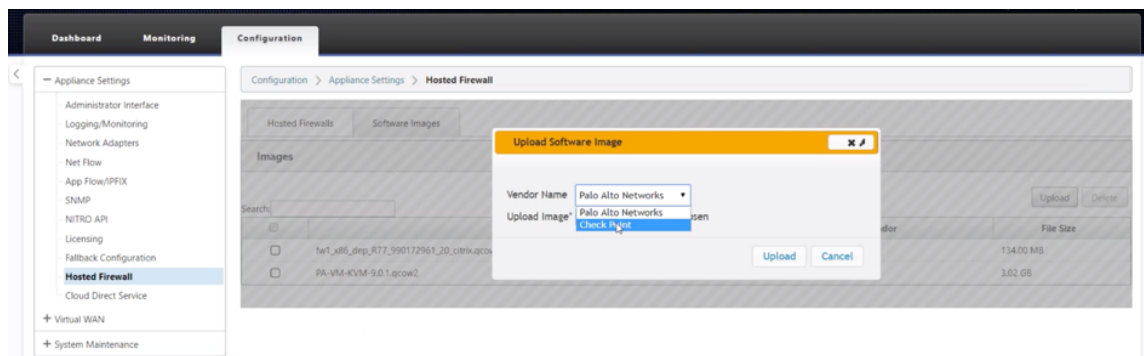


- **Standortname:** Zeigt den Standortnamen an.
- **Verwaltungs-IP:** Zeigt die Verwaltungs-IP-Adresse des Standorts an.
- **Regionsname:** Zeigt die Regionsbezeichnung an.
- **Anbieter:** Zeigt den Namen des Anbieters (Check Point) an.
- **Modell:** Zeigt das Modell - **Edge**.
- **Administratorstatus:** Status der virtuellen Maschine des Herstellers (Up/Down).
- **Betriebsstatus:** Zeigt die letzte Meldung zum Betriebsstatus an.
- **Zugriff auf die Benutzeroberfläche für gehostete Sites:** Verwenden Sie den Link **Hier klicken**, um auf die GUI der virtuellen Check Point-Maschine

Bereitstellung virtueller Maschinen durch die Benutzeroberfläche der SD-WAN-Appliance

Stellen Sie auf der SD-WAN-Plattform die gehostete virtuelle Maschine bereit und starten Sie sie. Führen Sie die folgenden Schritte für die Provisioning:

1. Navigieren Sie von Citrix SD-WAN GUI zu **Konfiguration > Appliance-Einstellungen** wählen Sie **Gehostete Firewall** aus.
2. Laden Sie das Softwareimage hoch:
 - Wählen Sie die Registerkarte **Software-Images** . Wählen Sie den **Namen des Anbieters** als Kontrollpunkt aus.
 - Wählen Sie die Softwareimagedatei aus.
 - Klicken Sie auf **Upload**.

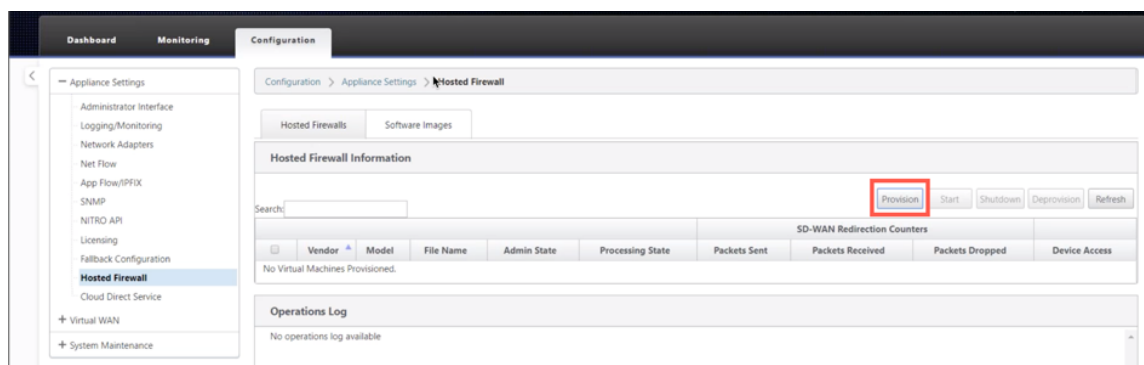


Hinweis:

Es können maximal zwei Images hochgeladen werden. Das Hochladen des Images der Check Point virtuellen Maschine kann je nach Bandbreitenverfügbarkeit länger dauern.

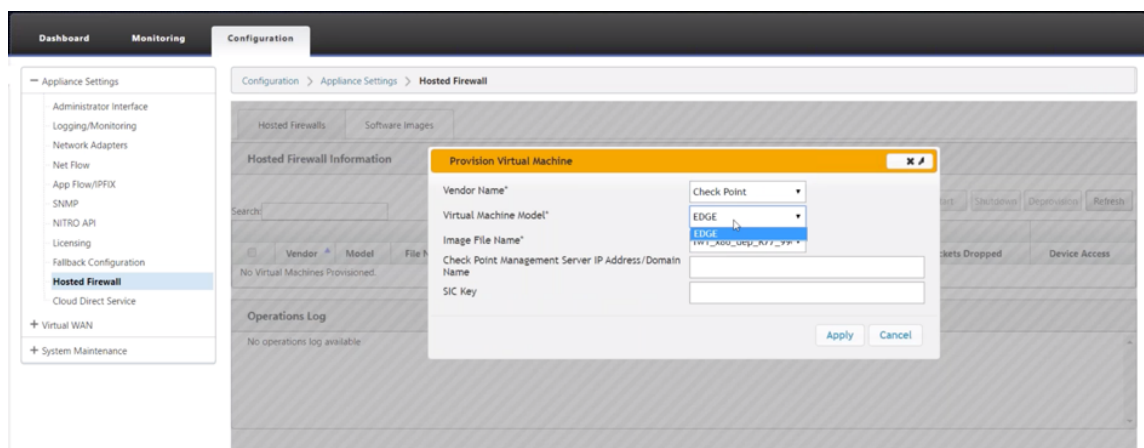
Sie können eine Statusleiste sehen, um den Upload-Prozess zu verfolgen. Das Dateidetail spiegelt sich wieder, sobald das Image erfolgreich hochgeladen wurde. Das für die Provisioning verwendete Image kann nicht gelöscht werden. Führen Sie keine Aktion aus oder gehen Sie zurück zu einer anderen Seite, bis die Imagedatei 100% hochgeladen zeigt.

3. Für die Provisioning wählen Sie die Registerkarte **Gehostete Firewall** > klicken Sie auf die Schaltfläche **Bereitstellen**.

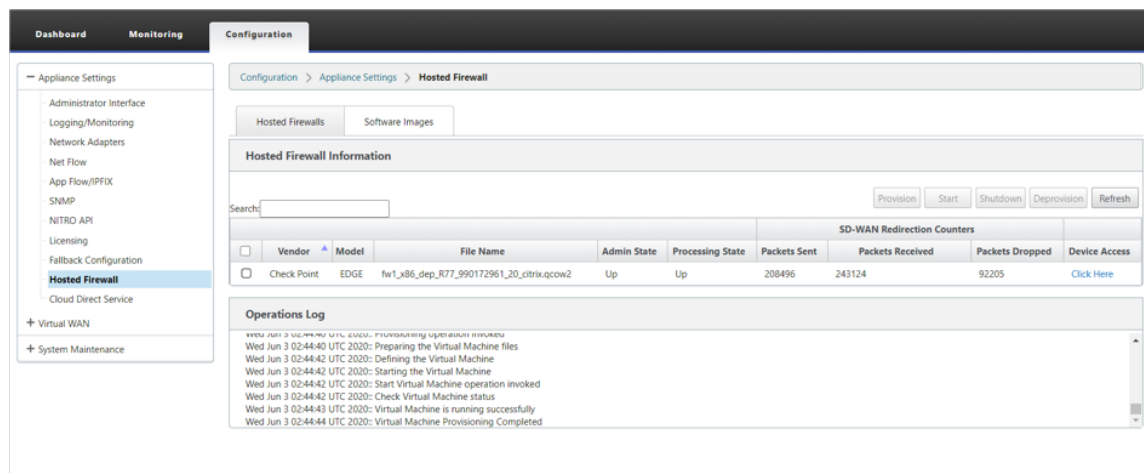


4. Geben Sie die folgenden Details für die Provisioning.

- **Anbietername:** Wählen Sie den **Namen des Anbieters** als Check Point aus.
- **Modell der virtuellen Maschine:** Das Modell der virtuellen Maschine wird automatisch als **Edge** ausgefüllt.
- **Imagedateiname:** Der Name der Imagedatei wird automatisch ausgefüllt.
- **Überprüfen Sie die IP Adresse/Domäne des Point Management Servers:** Geben Sie die IP-Adresse/Domäne des Checkpoint Management Servers an.
- **SIC-Schlüssel:** Geben Sie den SIC-Schlüssel an (optional). SIC schafft vertrauenswürdige Verbindungen zwischen **Check Point-Komponenten**. Klicken Sie auf **Übernehmen**.



5. Klicken Sie auf **Aktualisieren**, um den neuesten Status zu erhalten. Nachdem die virtuelle Check Point-Maschine vollständig gestartet wurde, wird sie auf der SD-WAN-Benutzeroberfläche mit den Vorgängen Protokolldetails reflektiert.



- **Admin-Status:** Gibt an, ob die virtuelle Maschine hoch- oder heruntergefahren ist.
- **Verarbeitungsstatus:** Datenpfad Verarbeitungsstatus der virtuellen Maschine.
- **Gesendete Pakete:** Pakete, die von SD-WAN an die virtuelle Sicherheitsmaschine gesendet werden.
- **Empfangenes Paket:** Pakete, die von SD-WAN von der virtuellen Sicherheitsmaschine empfangen werden.
- **Paket gelöscht:** Von SD-WAN abgelegte Pakete (z. B. wenn die virtuelle Sicherheitsmaschine ausgefallen ist).
- **Gerätezugriff:** Klicken Sie auf den Link, um den GUI-Zugriff auf die virtuelle Sicherheitsmaschine zu erhalten.

Sie können die virtuelle Maschine nach Bedarf **starten**, **herunterfahren** und **deaktivieren**. Verwenden Sie die **Option Hier klicken**, um auf die GUI der virtuellen Check Point-Maschine zuzugreifen, oder verwenden Sie Ihre Verwaltungs-IP zusammen mit 4100-Port (Management-IP: 4100).

Hinweis: Verwenden Sie

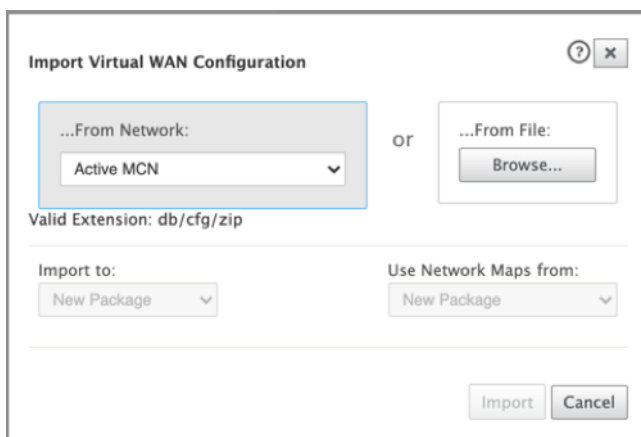
immer den Inkognito-Modus, um auf die Checkpoint-GUI zuzugreifen.

Datenverkehr an Edge umleiten

Die Konfiguration der Datenverkehrsumleitung kann sowohl über den Konfigurationseditor auf MCN als auch den Konfigurationseditor im SD-WAN Center erfolgen.

So navigieren Sie im SD-WAN Center durch den Konfigurationseditor:

1. Öffnen Sie Citrix SD-WAN Center UI, navigieren Sie zu **Konfiguration > Netzwerkkonfigurationsimport**. Importieren Sie die virtuelle WAN-Konfiguration aus dem aktiven MCN und klicken Sie auf **Importieren**.



Die restlichen Schritte sind ähnlich wie folgt - die Konfiguration der Datenverkehrsumleitung über MCN.

So navigieren Sie durch den Konfigurationseditor auf MCN:

1. Setzen Sie **Verbindungsanpassungstyp** unter **Global > Netzwerkeinstellungen** auf **Symmetrisch**.

Global

- Network Settings
- Regions
- Centralized Licensing
- Hosted Firewall Template
- Routing Domains
- Applications
- Application QoE
- Firewall Zones
- Firewall Policy Templates
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- DNS Services
- Proxy Auto-config settings
- Autopath Groups
- Service Providers
- WAN-to-WAN Forwarding Groups
- WAN Optimization Features
- WAN Optimization Tuning Settings
- WAN Optimization Application Classifiers
- WAN Optimization Service Classes

Global Security Settings

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode: AES 128-Bit

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type: 32-Bit Checksum

☐ Enable FIPS Mode

☐ Enable Appliance Authentication

Network Secure Key: 72d050ce5ca54c... **Regenerate**

Global Firewall Settings

Global Policy Template: New_Firewall_... Default Firewall Action: Allow ☒ Default Connection State Tracking

Connection Match Type: Symmetric

Denied Timeout (s): 30

TCP Initial Timeout (s): 120 TCP Idle Timeout (s): 7440

TCP Closing Timeout (s): 60 TCP Time Wait Timeout (s): 120 TCP Closed Timeout (s): 10

UDP Initial Timeout (s): 30 UDP Idle Timeout (s): 300

ICMP Initial Timeout (s): 30 ICMP Idle Timeout (s): 60

Generic Initial Timeout (s): 30 Generic Idle Timeout (s): 300

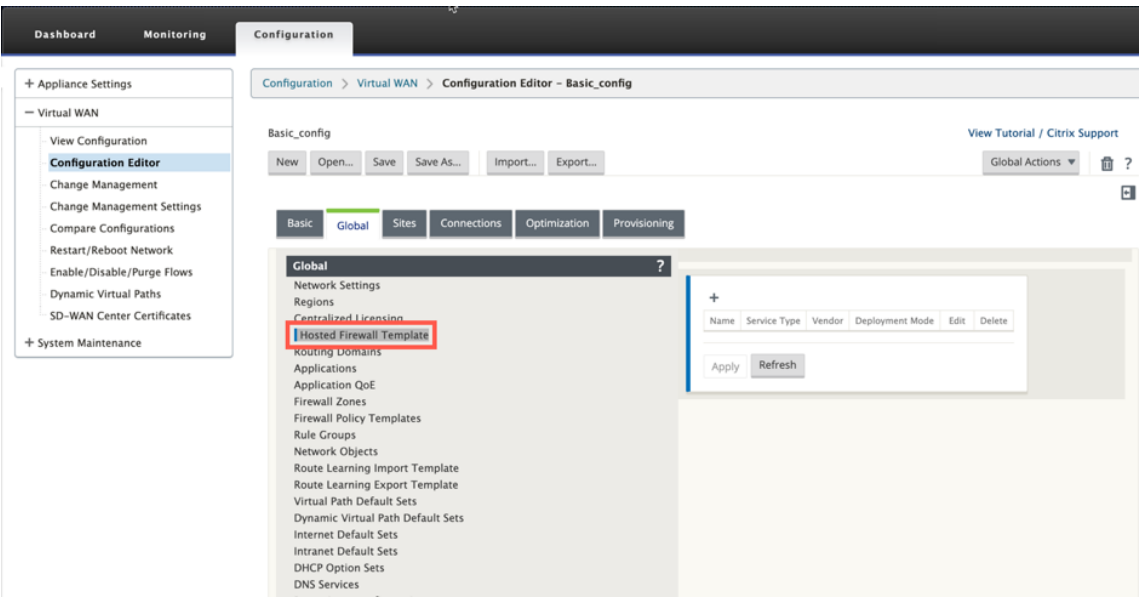
Global On-Demand Bandwidth Limit Setting

Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%): 120

Apply **Revert**

Standardmäßig sind SD-WAN-Firewallrichtlinien richtungsspezifisch. Der symmetrische Übereinstimmungstyp entspricht den Verbindungen anhand der angegebenen Übereinstimmungskriterien und wendet die Richtlinienaktion in beide Richtungen an.

- Öffnen Sie Citrix SD-WAN UI, navigieren Sie zu **Konfiguration** erweitern **Virtual WAN** wählen Sie **Konfigurationseditor** wählen Sie **Gehostete Firewall-Vorlage** im Abschnitt **Global**



3. Klicken Sie auf + und geben Sie die erforderlichen Informationen an, die im folgenden Screen-shot verfügbar sind, um die **Vorlage für gehostete Firewall** hinzuzufügen. Klicken Sie auf **Hinzufügen**.

Edit

Name:

CheckPoint-NGFW

Vendor

Check Point

Model:

Edge

Deployment Mode:

Bridge

Primary Management Server IP/FQDN:

Secondary Management Server IP/FQDN:

Service Redirection Interfaces

+

| Name | Input Interface | Output Interface | VLAN ID | Delete |
|--------------|-----------------|------------------|---------|--------|
| INTERNET-OUT | Interface-1 | Interface-2 | 0 | |
| INTERNET-IN | Interface-2 | Interface-1 | 0 | |

Apply

Cancel

Mit der **gehosteten Firewall-Vorlage** können Sie die Datenverkehrsumleitung zur **virtuellen Firewall-Maschine** konfigurieren, die auf der SD-WAN-Plattform gehostet wird. Die folgenden Eingaben sind für die Konfiguration der Vorlage erforderlich:

- **Name:** Der Name der gehosteten Firewall-Vorlage.
- **Anbieter:** Der Name des Firewall-Anbieters —Check Point.
- **Bereitstellungsmodus:** Das Feld “**Bereitstellungsmodus** “wird automatisch ausgefüllt und

ausgegraut. Für den **Check Point-Anbieter** ist der Bereitstellungsmodus **Bridge**.

- **Modell:** Virtual Machine-Modell der gehosteten Firewall. Nachdem Sie den Anbieter als **Kontrollpunkt** ausgewählt haben, wird das Modellfeld automatisch mit **Edge** gefüllt.
- **Primärer Managementserver IP/FQDN:** Primärer Managementserver IP/FQDN.
- **Sekundärer Managementserver IP/FQDN:** Sekundärer Managementserver IP/FQDN.
- **Dienstumleitungsschnittstellen:** Dies sind logische Schnittstellen, die für die Verkehrsumleitung zwischen SD-WAN und gehosteter Firewall verwendet werden.

Hinweis

Die Eingabeschnittstelle für die Umleitung muss aus der Richtung des Verbindungsinitiators ausgewählt werden, die Ausgabeschnittstelle wird automatisch für den Antwortverkehr ausgewählt. Wenn beispielsweise ausgehender Internetverkehr an die gehostete Firewall auf Schnittstellen1 umgeleitet wird, wird der Antwortverkehr automatisch zur gehosteten Firewall auf Schnittstellen2 umgeleitet. Außerdem ist Interface-2 nicht erforderlich, wenn kein eingehender Internet-Datenverkehr vorhanden ist.

Der virtuellen Maschine Check Point sind nur zwei Datenschnittstellen zugewiesen.

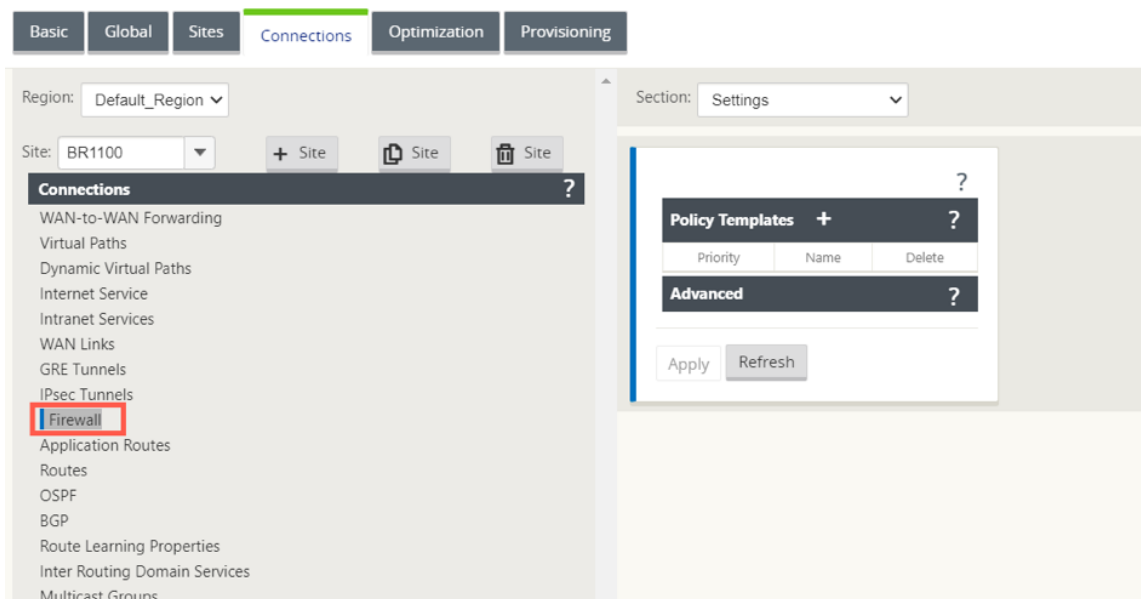
Hinweis:

SD-WAN-Firewall-Richtlinien werden automatisch erstellt, um den Datenverkehr zu/von gehosteten Firewall-Verwaltungsservern **zulassen**. Dadurch wird die Umleitung des Verwaltungsdatenverkehrs vermieden, der von (oder) für die gehostete Firewall bestimmt ist.

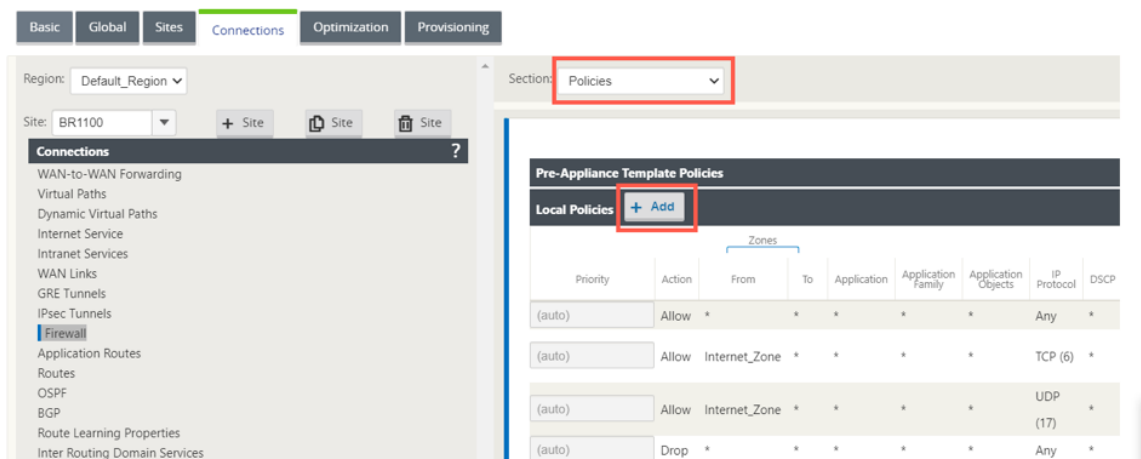
Die Umleitung des Datenverkehrs zur virtuellen Firewall-Maschine kann mithilfe von SD-WAN-Firewall-Richtlinien erfolgen. Es gibt zwei Methoden zum Erstellen von SD-WAN-Firewall-Richtlinien - entweder über Firewall-Richtlinienvorlagen im **globalen** Abschnitt oder auf Site-Ebene.

Methode - 1

1. Navigieren Sie von Citrix SD-WAN GUI zu **Konfiguration** erweitern Sie **Virtual WAN > Konfigurations-Editor**. Wählen Sie **Firewall** unter **Verbindungen** aus.



2. Wählen Sie in der Dropdown-Liste **Abschnitt** die Option **Richtlinien** aus und klicken Sie auf **+Hinzufügen**, um eine neue Firewall-Richtlinie zu erstellen.



3. Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch auf **Redirect** gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdown-Liste aus. Klicken Sie auf **Hinzufügen**.

Priority: 400

Policy Type: **Hosted Firewall**

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

☐ Match Established

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: Any

Dest IP: *

Dest Port: *

Actions

Action: **Redirect**

☒ Allow Fragments

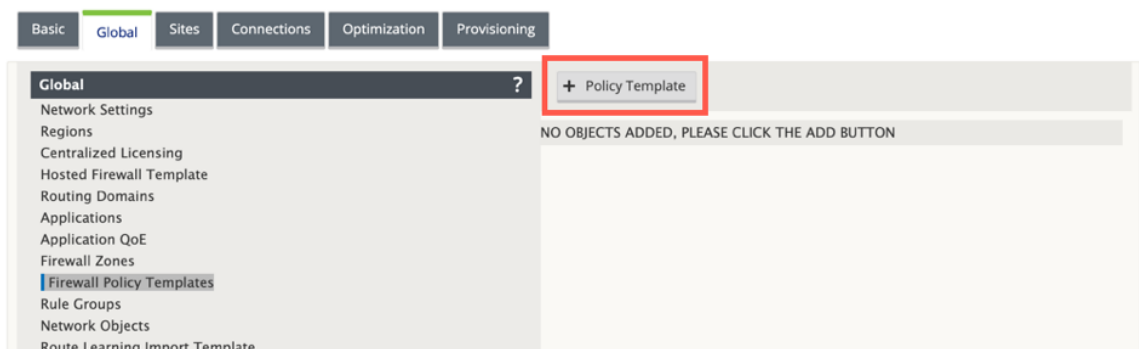
Connection State Tracking: No Tracking

Hosted Firewall Template: CheckPoint-NGFW

Service Redirection Interface: INTERNET-OUT

Methode - 2

1. Navigieren Sie zur Registerkarte **Global** und wählen Sie **Firewall-Richtlinienvorlagen** aus. Klicken Sie auf **+ Richtlinienvorlage**.



2. Geben Sie der Richtlinienvorlage einen Namen und klicken Sie auf **Hinzufügen**.

Add

Name:

New_Firewall_Policy_Template-1

Add **Cancel**

3. Klicken Sie auf **+ Hinzufügen** neben **Richtlinien für Pre-Appliance-Vorlagen**.

Basic Global Sites Connections Optimization Provisioning

Global ?

- Network Settings
- Regions
- Centralized Licensing
- Hosted Firewall Template
- Routing Domains
- Applications
- Application QoS
- Firewall Zones
- Firewall Policy Templates**
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- DNS Services
- Proxy Auto-config settings

Policy Template: New_Firewall_Policy_Template-1 **+ Policy Template** **Policy Template**

Template Name: New_Firewall_Po...

Pre-Appliance Template Policies **+ Add**

| Priority | Action | From | To | Application | Application Family | Application Objects | IP Protocol | DSCP | Service | IP Address | | | | | | | | | | | | | | | | | | | | | | |
|--|--------|------|----|-------------|--------------------|---------------------|-------------|------|---------|------------|----------|--------|------|----|-------------|--------------------|---------------------|-------------|------|---------|------------|--------------------------|--|--|--|--|--|--|--|--|--|--|
| Post-Appliance Template Policies + Add | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Priority</th> <th>Action</th> <th>From</th> <th>To</th> <th>Application</th> <th>Application Family</th> <th>Application Objects</th> <th>IP Protocol</th> <th>DSCP</th> <th>Service</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td colspan="11"> <div>Apply Refresh</div> </td> </tr> </tbody> </table> | | | | | | | | | | | Priority | Action | From | To | Application | Application Family | Application Objects | IP Protocol | DSCP | Service | IP Address | <div>Apply Refresh</div> | | | | | | | | | | |
| Priority | Action | From | To | Application | Application Family | Application Objects | IP Protocol | DSCP | Service | IP Address | | | | | | | | | | | | | | | | | | | | | | |
| <div>Apply Refresh</div> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

4. Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch auf **Redirect** gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdown-Liste aus. Klicken Sie auf **Hinzufügen**.

Priority: Policy Type: **Hosted Firewall**

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Inter_Routing_Domain_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |

Traffic Match Type: **IP Protocol** IP Protocol: **Any** DSCP: **Any** ☐ Match Established

Application Objects: **Any**

Source Service Type: **Any** Source Service Name: **Any** Source IP: Source Port:

Dest Service Type: **Any** Dest Service Name: **Any** Dest IP: Dest Port:

Actions

Action: **Redirect** ☒ Allow Fragments Connection State Tracking: **No Tracking**

Hosted Firewall Template: **CheckPoint-NGFW** Service Redirection Interface: **INTERNET-OUT**

5. Navigieren Sie zu den **Verbindungen > Firewall** und wählen Sie dann die Firewall-Richtlinie (die Sie erstellt haben) unter dem Namensfeld aus. Klicken Sie auf **Übernehmen**.

Basic Global Sites **Connections** Optimization Provisioning

Region: **Default_Region**

Site: **BR1100** **+ Site** **Site** **Site**

Connections

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall**
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups

Section: **Settings**

Policy Templates **+**

| Priority | Name | Delete |
|----------|--------------------------|--------|
| 100 | New_Firewall_P... | |

Advanced

Apply **Revert**

Während die gesamte Netzwerkkonfiguration ausgeführt wird, können Sie die Verbindung unter **Überwachung > Firewall** > unter **Statistikliste** überwachen und **Richtlinien filtern**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Firewall

Firewall Statistics

Statistics:

Filter Policies

Maximum entries to display:

50

Filtering:

Application: Any

Family: Any

IP Protocol: Any

Filter Policy Action: Any

Source Service Type: Any

Destination Service Type: Any

Source Port: *

Destination Port: *

Source IP: *

Destination IP: *

Source Zone: Any

Destination Zone: Any

DSCP: Any

Refresh

Show latest data.

Help

Filter Policies

Default Policy - Allow(Not Tracked) Packets - 42 Bytes - 3528

Match In Progress Packets - 0 Bytes - 0

| ID | Application | Family | IP Protocol | DSCP | Service Type | Service Name | IP Address | Port or ICMP Type | Zone | Service Type | Service Name | IP Address | Port or ICMP Code | Zone | Action | Conn Match Type | Track Connection | Allow Fragments |
|----|-------------|--------|-------------|------|--------------|--------------|------------|-------------------|---------------|--------------|--------------|-------------------|-------------------|------|----------|-----------------|------------------|-----------------|
| 1 | * | * | * | * | * | - | * | NA | * | Internet | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 2 | * | * | * | * | Internet | - | * | NA | * | * | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 3 | * | * | * | * | * | - | * | NA | * | Virtual Path | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 4 | * | * | * | * | Virtual Path | - | * | NA | * | * | - | * | NA | * | Redirect | Symmetric | No | Yes |
| 5 | * | * | * | * | * | - | * | NA | * | * | - | * | NA | * | Allow | Symmetric | No | Yes |
| 6 | * | * | TCP | * | Internet | - | * | * | Internet_Zone | * | - | 172.147.93.174/32 | 5001 | * | Allow | Symmetric | No | Yes |
| 7 | * | * | UDP | * | Internet | - | * | * | Internet_Zone | * | - | 172.147.93.174/32 | 5001 | * | Allow | Symmetric | No | Yes |
| 8 | * | * | * | * | Internet | - | * | NA | * | * | - | * | NA | * | Drop | Symmetric | No | Yes |

Filter Policies Displayed: 8

Filter Policies In Use: 8/1000

Verknüpfungsaggregationsgruppen

October 28, 2021

Mit der LAG-Funktion (Link Aggregation Groups) können Sie zwei oder mehr Ports auf Ihrer SD-WAN-Appliance gruppieren, um als einen einzigen Port zusammenzuarbeiten. Dies gewährleistet eine erhöhte Verfügbarkeit, Link-Redundanz und verbesserte Leistung.

Citrix SD-WAN unterstützt einfache LAG (ACTIVE-BACKUP). Die 802.3ad LACP-Protokoll-basierten Verhandlungen werden in der aktuellen Version nicht unterstützt. Zu jeder Zeit ist nur ein Port aktiv und die anderen Ports sind im Backupmodus. Die aktiven und Backupunterstützungen basieren auf dem Data Plane Development Kit (DPDK) -Paket für die LAG-Funktionalität. Die LAG-Funktionalität ist nur auf den folgenden von DPDK unterstützten Plattformen verfügbar:

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

- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 4000, 4100 und 5100 SE
- Citrix SD-WAN 6100 SE
- Citrix SD-WAN 2100 SE

Hinweis

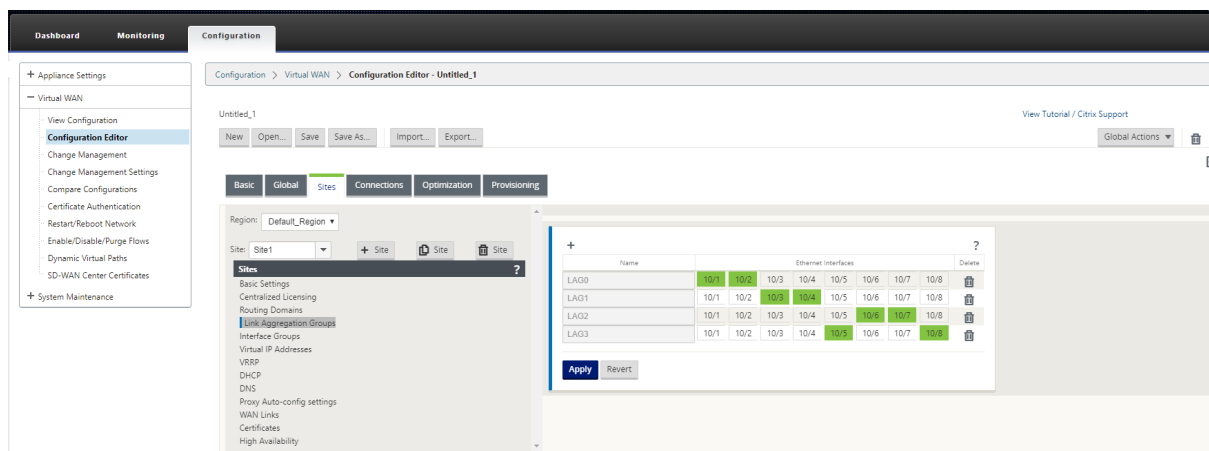
Die LAG-Funktionalität wird auf VPX/VPXL-Plattformen nicht unterstützt.

Sie können maximal vier LAGs mit maximal vier Ports erstellen, die in jeder LAG auf den Citrix SD-WAN-Appliances gruppiert sind.

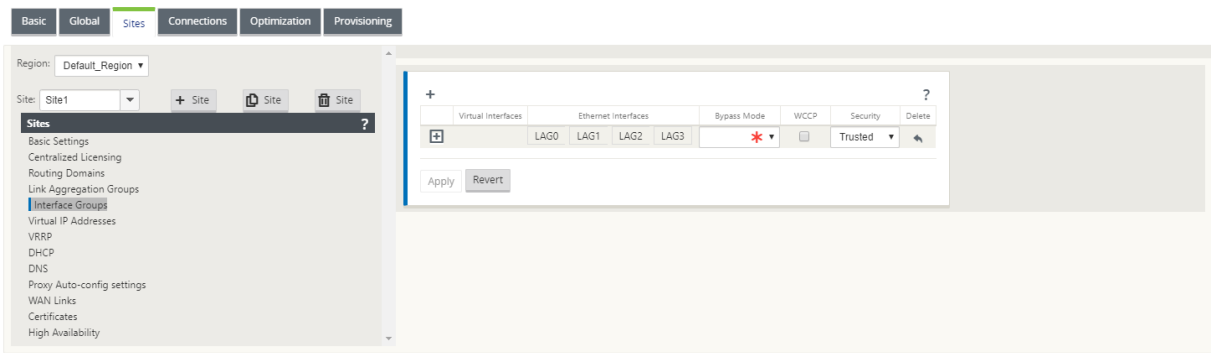
Hinweis

Für Citrix SD-WAN 210 und 410 Appliances können Sie nur eine LAG mit maximal drei darin gruppierten Ports erstellen.

Um Link-Aggregationsgruppen zu konfigurieren, navigieren Sie im **Konfigurationseditor** zu **Sites** > **Link-Aggregationsgruppen**. Sie können alle verfügbaren physischen Ports und Ethernet-Schnittstellen anzeigen. Klicken Sie auf **+**, um eine LAG zu erstellen.



Wählen Sie die Mitglieds-Ports aus und klicken Sie auf **Übernehmen**. Sobald die Ports zur LAG hinzugefügt wurden, können Sie nur die LAGs in der **Schnittstellengruppe** anstelle der Mitgliedsports sehen.

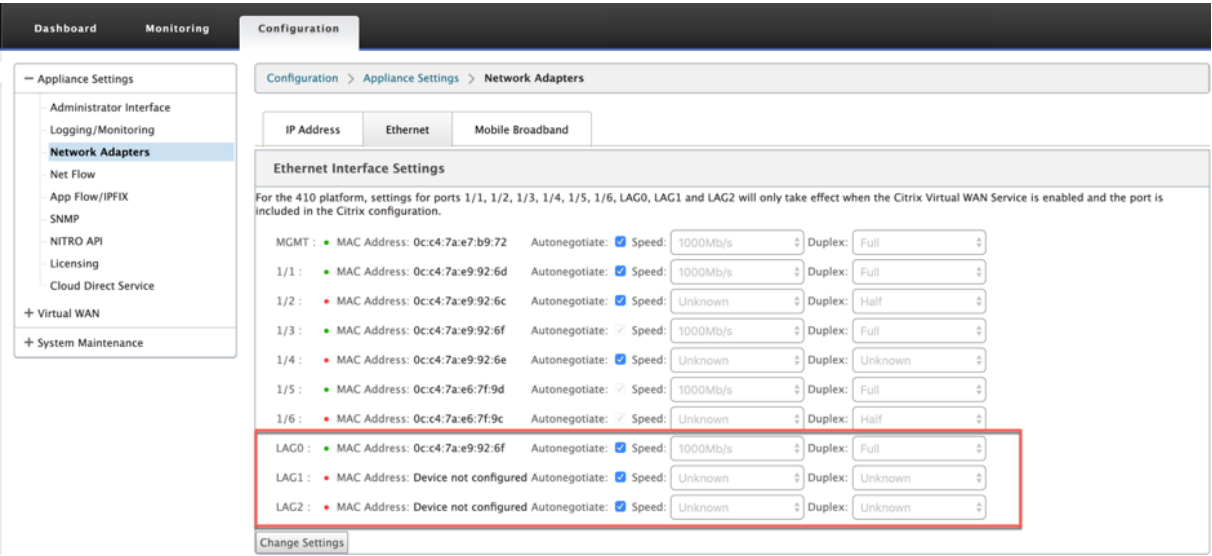


Sie können virtuelle Schnittstellen mit LAGs erstellen und diese Schnittstellen werden weiter verwendet, um LAN/WAN-Verbindungen und HA zu konfigurieren.

Hinweis

Die Funktion [Link State Propagation \(LSP\)](#) wird nicht unterstützt, wenn LAGs als Ethernet-Schnittstellen in Schnittstellengruppen verwendet werden.

Sie können die aktiven und Standby-LAG-Ports anzeigen und zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Ethernet** navigieren.



Hinweis

Sie können die Einstellungen für einzelne Mitglieds-Ports nicht ändern. Konfigurationsänderungen, die an der LAG vorgenommen wurden, werden automatisch an die Mitglieds-Ports übertragen.

Verknüpfen Zustandspropagierung

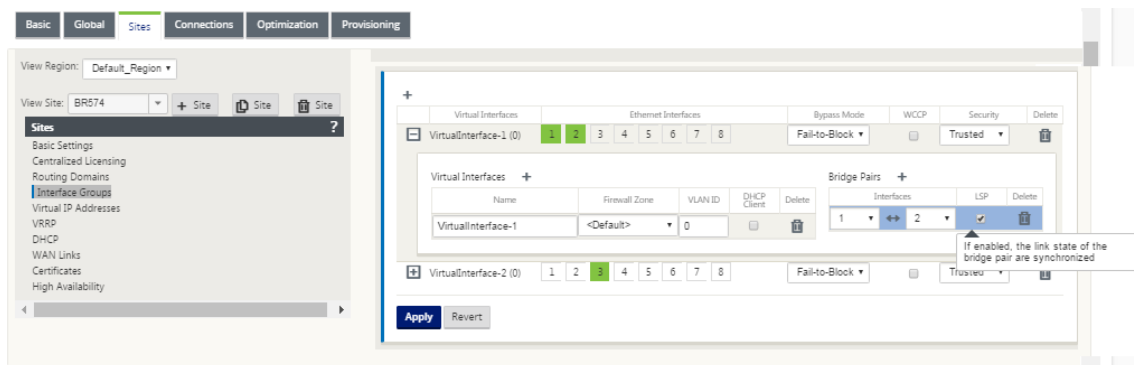
May 10, 2021

Mit der LSP-Funktion (Link State Propagation) können Netzwerkadministratoren den Verbindungsstatus eines Bypass-Paares synchronisieren, sodass angeschlossene Geräte auf der anderen Seite des Links anzeigen können, wenn Links inaktiv sind. Wenn ein Port eines Bypass-Paares inaktiv wird, wird der gekoppelte Link administrativ deaktiviert. Wenn Ihre Netzwerkarchitektur ein paralleles Failover-Netzwerk enthält, wird der Datenverkehr auf dieses Netzwerk umgestellt. Sobald der unterbrochene Link wiederhergestellt ist, wird der entsprechende Link automatisch aktiviert.

Konfigurieren der Hyperlinkstatuspropagierung

So konfigurieren Sie die Hyperlinkstatuspropagierung:

1. Navigieren Sie zu **Konfigurations-Editor > Standorte > [Standortname] > Schnittstellen-gruppen**.
2. Erweitern Sie **Virtuelle Schnittstellen**, und klicken Sie unter **Bridge-Paare** auf das Kontrollkästchen **LSP**, um die **Hyperlinkstatuspropagierung** für ein Bridge-Paar zu aktivieren. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.



Überwachung der Linkstatistiken

So überwachen Sie Linkstatistiken:

1. Wählen Sie auf der Seite **Monitor > Statistik** aus dem Dropdownmenü **Anzeigen** die Option **Ethernet**, um den Status des Bypass-Port-Paares mit aktivierter Linkstatus-Propagierung anzuzeigen. Beachten Sie, dass die LAN-Seiten-Verbindung ausgefallen ist und später die WAN-Seiten-Verbindung des Bypass-Paares administrativ DEAKTIVIERT ist.

Statistics

Show: Ethernet ☐ Enable Auto Refresh 5 seconds Refresh

Ethernet Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries

| Port | Link State | Frames Sent | Bytes Sent | Frames Received | Bytes Received | Errors |
|------|------------|-------------|------------|-----------------|----------------|--------|
| 1 | DOWN | 132885 | 8755483 | 212584 | 15332801 | 0 |
| 2 | DISABLED | 17984552 | 1531084459 | 18189043 | 1584612144 | 3258 |

Showing 1 to 2 of 2 entries

2. Navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Registerkarte Ethernet**. Die Ports, die administrativ abgeschaltet sind, werden in der Liste **Ethernet Interface Settings** durch ein rotes Sternchen (*) gekennzeichnet.

Ethernet Interface Settings

| | | | | |
|-------|----------------------------------|--|----------------|-----------------|
| 1 : | MAC Address: 0c:c4:7a:12:bc:8d | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| 2 : | * MAC Address: 0c:c4:7a:12:bc:8c | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| 3 : | MAC Address: 0c:c4:7a:12:bc:8f | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| 4 : | MAC Address: 0c:c4:7a:12:bc:8e | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| 5 : | MAC Address: 0c:c4:7a:12:bc:91 | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| MGT : | MAC Address: 0c:c4:7a:12:bc:90 | Autonegotiate: <input checked="" type="checkbox"/> | Speed: 100Mb/s | Duplex: Full |
| X1 : | MAC Address: 00:25:90:ed:22:9f | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| X2 : | MAC Address: 00:25:90:ed:22:9e | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| X3 : | MAC Address: 00:25:90:ed:22:9d | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |
| X4 : | MAC Address: 00:25:90:ed:22:9c | Autonegotiate: <input checked="" type="checkbox"/> | Speed: Unknown | Duplex: Unknown |

* interface disabled by Port State Reflection

Change Settings

Mess- und Standby-WAN-Verbindungen

May 10, 2021

Citrix SD-WAN unterstützt die Aktivierung von getakteten Links, die so konfiguriert werden können, dass Benutzerdatenverkehr nur über eine bestimmte Internet-WAN-Verbindung übertragen wird, wenn alle anderen verfügbaren WAN-Verbindungen deaktiviert sind.

Metered Links sparen Bandbreite für Links, die basierend auf der Nutzung abgerechnet werden. Mit den getakteten Links können Sie die Links als Letzter Resort-Link konfigurieren, der die Verwendung des Links nicht zulässt, bis alle anderen nicht getakteten Links heruntergefahren oder verschlechtert sind. Letztes Resort festlegen ist in der Regel aktiviert, wenn drei WAN-Links zu einer Site vorhanden sind (MPLS, Breitband Internet, 4G/LTE) und eine der WAN-Verbindungen 4G/LTE ist und für ein Unternehmen zu teuer ist, um die Nutzung zuzulassen, es sei denn, dies ist erforderlich. Die Messung ist

standardmäßig nicht aktiviert und kann auf einer WAN-Verbindung eines beliebigen Zugriffstyps (Public Internet, Private MPLS, Private Intranet) aktiviert werden. Wenn die Messung aktiviert ist, können Sie optional Folgendes konfigurieren:

- Datenkappe
- Abrechnungszeitraum (wöchentlich/monatlich)
- Startdatum
- Standby-Modus
- Priorität
- Aktives Heartbeat-Intervall - Intervall, in dem eine Heartbeat-Nachricht von einer Appliance an ihren Peer am anderen Ende des virtuellen Pfads gesendet wird, wenn für mindestens ein Heartbeat-Intervall kein Datenverkehr (Benutzer/Steuerung) auf dem Pfad vorhanden ist.

Bei einem lokalen getakteten Link zeigt das Dashboard einer Appliance unten eine **WAN-Link-Metering-Tabelle** mit Messinformationen an.

Die Bandbreitennutzung auf einer lokalen getakteten Verbindung wird anhand des konfigurierten Datendeckels verfolgt. Wenn die Nutzung 50%, 75% oder 90% des konfigurierten Datendeckels überschreitet, generiert die Appliance ein Ereignis, um den Benutzer zu warnen, und oben im Dashboard der Appliance wird ein Warnbanner angezeigt. Dieses Nutzungswarnungsereignis kann auch im SD-WAN Center angezeigt werden. Ein gemessener Pfad kann mit 1 oder 2 gemessenen Links gebildet werden. Wenn zwischen zwei gemessenen Links ein Pfad gebildet wird, ist das aktive Heartbeat-Intervall, das auf dem gemessenen Pfad verwendet wird, das größere der beiden konfigurierten aktiven Heartbeat-Intervalle auf den Links.

Ein gemessener Pfad ist ein Nicht-Standby-Pfad und ist immer für den Benutzerverkehr berechtigt. Wenn mindestens ein nicht getakterter Pfad im Status GOOD vorhanden ist, trägt ein gemessener Pfad die reduzierte Menge an Steuerverkehr und wird vermieden, wenn die Weiterleitungsebene nach einem Pfad nach einem doppelten Paket sucht.

Standbymodus

Der Standby-Modus einer WAN-Verbindung ist standardmäßig deaktiviert. Um den Standby-Modus zu aktivieren, müssen Sie angeben, in welchem der beiden folgenden Modi die Standby-Verbindung funktioniert

- **AufAnforderung:** Der Standby-Link, der aktiv wird, wenn eine der Bedingungen erfüllt ist.

Wenn die verfügbare Bandbreite im virtuellen Pfad kleiner ist als das konfigurierte Bandbreitenlimit bei Bedarf UND eine ausreichende Nutzung vorhanden ist. Ausreichende Auslastung ist definiert als mehr als 95% (ON_DEMAND_USAGE_THRESHOLD_PCT) der aktuellen verfügbaren Bandbreite, oder die Differenz zwischen der aktuellen verfügbaren Bandbreite und der aktuellen Nutzung beträgt weniger als 250 kbps (ON_DEMAND_THRESHOLD_GAP_KBPS), beide

Parameter können mit `t2_variables` geändert werden, wenn alle Nicht-Standby Pfade sind tot oder deaktiviert.

- **Last-Resort** - ein Standby-Link, der nur aktiv wird, wenn alle Nicht-Standby-Links und On-Demand-Standby-Links deaktiviert oder deaktiviert sind.
- Standby-Priorität gibt die Reihenfolge an, in der eine Standby-Verbindung aktiv wird, wenn mehrere Standby-Links vorhanden sind:
 - ein Priority 1 Standby-Link wird zuerst aktiv, während ein Priority 3 Standby-Link zuletzt aktiv wird
 - Mehrere Standby-Links können die gleiche Priorität zugewiesen werden

Wenn Sie eine Standby-Verbindung konfigurieren, können Sie die Standby-Priorität und zwei Taktintervalle angeben:

- **Aktives Heartbeat Intervall** - das Heartbeat Intervall, das verwendet wird, wenn der Standby-Pfad aktiv ist (Standard 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- **Standby-Heartbeat-Intervall** - das Heartbeat-Intervall, das verwendet wird, wenn der Standby-Pfad inaktiv ist (Standard 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/deaktiviert)

Ein Standby-Pfad wird mit 1 oder 2 Standby-Links gebildet.

- **Auf Anforderung** - Ein On-Demand-Standby-Pfad wird gebildet zwischen:
 - eine Nicht-Standby-Verbindung und eine On-Demand-Standby-Verbindung
 - 2 On-Demand-Standby-Links
- **Last-Resort** - Ein Last-Resort-Standby-Pfad wird gebildet zwischen:
 - eine Nicht-Standby-Verbindung und eine Last-Resort-Standby-Verbindung
 - einen On-Demand-Standby-Link und einen Last-Resort-Standby-Link
 - 2 Last-Resort-Standby-Links

Die Taktintervalle, die auf einem Standby-Pfad verwendet werden, werden wie folgt bestimmt:

- Wenn der Standby-Heartbeat auf mindestens 1 der 2 Links deaktiviert ist, wird der Heartbeat im Standby-Pfad deaktiviert, während er inaktiv ist.
- Wenn der Standby-Heartbeat für beide Links nicht deaktiviert ist, wird der größere der beiden Werte verwendet, wenn der Standby-Pfad Standby-Pfad ist.
- Wenn aktives Heartbeat-Intervall für beide Links konfiguriert ist, wird der größere der beiden Werte verwendet, wenn der Standby-Pfad aktiv ist.

Heartbeat (Keep alive) Nachrichten:

- In einem Nicht-Standby-Pfad werden Heartbeat-Nachrichten nur gesendet, wenn mindestens ein Heartbeat-Intervall kein Datenverkehr (Steuerung oder Benutzer) vorhanden ist. Das Heartbeat-Intervall variiert je nach Pfadzustand. Für **Nicht-Standby-, nicht getaktete** Pfade:
 - 50 ms, wenn der Pfadzustand GOOD ist
 - 25 ms, wenn der Pfadzustand BAD ist

Auf einem Standby-Pfad hängt das verwendete Heartbeat-Intervall vom Aktivitätsstatus und dem Pfadstatus ab:

- Wenn der Heartbeat nicht deaktiviert ist, werden Heartbeat-Nachrichten regelmäßig im konfigurierten Standby-Heartbeat-Intervall gesendet, da kein anderer Datenverkehr darauf zulässig ist.
- das konfigurierte aktive Heartbeat-Intervall wird verwendet, wenn der Pfadstatus GOOD ist.
- 1/2 das konfigurierte aktive Heartbeat-Intervall wird verwendet, wenn der Pfadzustand BAD ist.
- Während aktiv, wie Nicht-Standby-Pfade, werden Heartbeat-Nachrichten nur gesendet, wenn für mindestens das konfigurierte aktive Heartbeat-Intervall kein Datenverkehr (Steuerung oder Benutzer) vorhanden ist.
- das konfigurierte Standby-Heartbeat-Intervall wird verwendet, wenn der Pfadstatus GOOD ist.
- 1/2 das konfigurierte Standby-Heartbeat-Intervall wird verwendet, wenn der Pfadzustand BAD ist.

Während inaktiv, sind Standby-Pfade nicht für den Benutzerverkehr geeignet. Die einzigen Kontrollprotokollmeldungen, die auf inaktiven Standby-Pfaden gesendet werden, sind Heartbeat-Nachrichten, die zur Erkennung von Verbindungsfehlern und zur Erfassung von Qualitätsmetriken dienen. Wenn Standby-Pfade aktiv sind, sind sie für den Benutzerverkehr mit zusätzlichen Zeitkosten berechtigt. Dies geschieht, damit die Nicht-Standby-Pfade, falls verfügbar, bei der Weiterleitungspfadtauswahl bevorzugt werden.

Der Pfadstatus eines Standbypfads mit deaktiviertem Heartbeat (inaktiv) wird angenommen, dass er GOOD ist und in der Tabelle Pfadstatistiken unter **Überwachung** als GOOD angezeigt wird. Wenn es aktiv wird, im Gegensatz zu einem Nicht-Standby-Pfad, der im DEAD Zustand beginnt, bis es von seinem virtuellen Pfad-Peer hört, wird es im GOOD- Zustand gestartet. Wenn keine Verbindung mit dem Virtual Path Peer erkannt wird, wird der Pfad BAD und dann DEAD. Wenn die Konnektivität mit dem Virtual Path Peer wieder hergestellt wird, wird der Pfad BAD und dann wieder GOOD.

Wenn ein solcher Standby-Pfad DEAD wird und dann inaktiv wird, ändert sich der Pfadzustand nicht sofort in (angenommen) GOOD. Stattdessen wird es für die Zeit im DEAD Zustand gehalten, so dass es nicht sofort verwendet werden kann. Dies soll verhindern, dass Aktivität zwischen einer Pfadgruppe mit niedrigerer Priorität mit angenommenen guten DEAD Pfaden und einer Pfadgruppe mit höherer Priorität mit tatsächlich GOOD-Pfaden oszilliert. Diese Wartezeit

(NO_HB_PATH_ON_HOLD_PERIOD_MS) ist auf 5 min eingestellt und kann über t2_variables geändert werden.

Wenn die Pfad-MTU-Erkennung auf einem virtuellen Pfad aktiviert ist, wird die MTU des Standby-Pfads nicht zur Berechnung der MTU des virtuellen Pfads verwendet, während der Pfad im Standby-Modus ist. Wenn der Standby-Pfad aktiv wird, wird die MTU des Virtual Path unter Berücksichtigung der MTU des Standby-Pfades neu berechnet. (Die MTU des virtuellen Pfades ist die kleinste MTU unter allen aktiven Pfaden innerhalb des virtuellen Pfades).

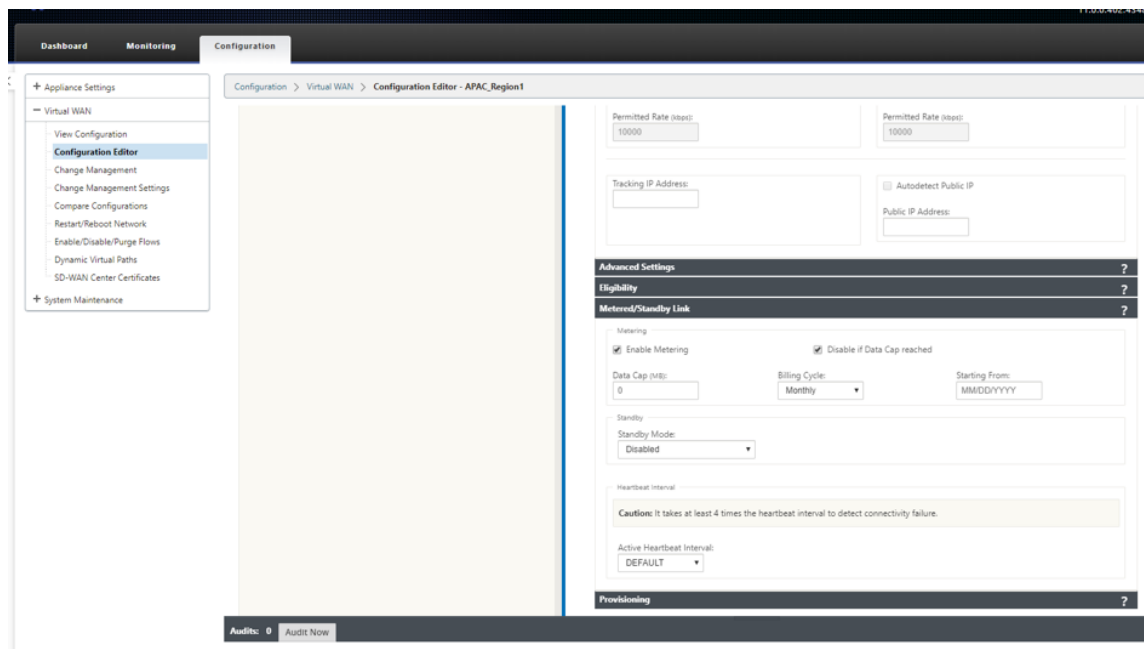
Ereignisse und Protokollmeldungen werden generiert, wenn ein Standby-Pfad zwischen Standby-Modus und Aktiv übergeht.

Konfigurationsvoraussetzungen:

- Eine Zählerverbindung kann von jedem Zugriffstyp sein.
- Alle Links an einem Standort können mit aktivierter Messung konfiguriert werden.
- Eine Standby-Verbindung kann vom Zugriffstyp Öffentliches Internet oder Privates Intranet sein. Eine WAN-Verbindung vom Privaten MPLS-Zugriffstyp kann nicht als Standby-Verbindung konfiguriert werden.
- Pro Standort muss mindestens ein Nicht-Standby-Link konfiguriert werden. Pro Site werden maximal 3 Standby-Links unterstützt.
- Internet-/Intranetdienste werden möglicherweise nicht für On-Demand-Standby-Links konfiguriert. On-Demand-Standby-Links unterstützen nur den Virtual Path Service.
- Der Internetdienst wird möglicherweise auf einer Standby-Verbindung mit letzter Instanz konfiguriert, aber nur der Lastausgleichsmodus wird unterstützt.
- Der Intranetdienst wird möglicherweise auf einer Standby-Verbindung mit letzter Instanz konfiguriert, es wird jedoch nur der sekundäre Modus unterstützt und die primäre Rückgewinnung muss aktiviert sein.

So konfigurieren Sie getaktete Links:

1. Navigieren Sie in der SD-WAN-Webverwaltungsoberfläche zu **Konfiguration > Virtuelles WAN** wählen Sie **Konfigurationseditor** Hinzufügen oder wählen Sie **Sites** aus der Dropdown-Liste aus > wählen Sie **WAN-Links** Klicken Sie auf **Metered/Standby Link**, um es zu erweitern.



2. Aktivieren Sie das Kontrollkästchen **Messung aktivieren** . Sie können Werte für die Datenobergrenze, das Startdatum des Abrechnungszyklus, die ungefähre Nutzung bereits verwendet und das aktive Heartbeat-Intervall angeben.

Metering

☒ Enable Metering ☒ Disable if Data Cap reached

Data Cap (MB): Billing Cycle: Starting From:

Standby

Standby Mode:

Heartbeat Interval

Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.

Active Heartbeat Interval:

3. Link deaktivieren, wenn die Datenobergrenze erreicht ist:

- Wenn das Kontrollkästchen **Link deaktivieren, wenn Data Cap erreicht** ist aktiviert ist, werden der gemessene Link und alle zugehörigen Pfade bis zum nächsten Abrechnungszyklus deaktiviert, wenn die Datennutzung die Datenobergrenze erreicht.
- Standardmäßig ist das Kontrollkästchen **Link deaktivieren, wenn die Datenbegrenzung erreicht** ist, deaktiviert, in dem der aktuelle Modus oder Status beibehalten wird, damit die gemessene Verbindung fortgesetzt wird, nachdem die Datenobergrenze bis zum näch-

sten Abrechnungszyklus erreicht ist.

4. Wenn der getaktete Link konfiguriert ist, können Sie die ungefähren Daten angeben, die bereits in MB für die getaktete Verknüpfung verwendet wurden.

Um die korrekte getaktete Link-Nutzung zu verfolgen, müssen Sie die ungefähre Nutzung auf dem getakteten Link eingeben, wenn der Link bereits seit einigen Tagen im aktuellen Abrechnungszeitraum verwendet wurde. Diese ungefähre Verwendung ist nur für den ersten Zyklus. Die Gesamtauslastung seit dem Startdatum bis zum aktuellen Datum wird berechnet und im Dashboard angezeigt.

Nachdem Sie das Konfigurationsupdate durchgeführt haben, können Sie die Verwendungsdetails im Dashboard anzeigen.

| | |
|----------------|-----------------------|
| WAN Link Name: | DC-WL-1 |
| Total Usage: | 999.35 MBs of 500 MBs |
| Data Usage: | 0.00 MBs |
| Control Usage: | 999.35 MBs |
| Usage(in %): | 199 |
| Billing Cycle: | MONTHLY |
| Starting From: | 05/06/2020 |
| Days Elapsed: | 8 days of 31 days |

So konfigurieren Sie Standby-Links:

1. Standardmäßig ist der Standby-Modus einer WAN-Verbindung deaktiviert. Um die WAN-Link als Standby zu konfigurieren, wählen Sie einen der Standby-Modi (Last-Resort/On-Demand) aus der Dropdownliste aus.

The screenshot displays the configuration page for a standby connection in Citrix SD-WAN 11.2. It features two main sections: 'Standby' and 'Heartbeat Interval'. In the 'Standby' section, 'Standby Mode' is set to 'Last-Resort' and 'Priority' is set to '1'. The 'Heartbeat Interval' section contains a caution box stating: 'Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.' Below this, 'Active Heartbeat Interval' and 'Standby Heartbeat Interval' are both set to '1 second'. A dark blue bar at the bottom of the configuration area is labeled 'Provisioning' with a question mark icon. At the very bottom, there are 'Apply' and 'Revert' buttons.

2. Sobald ein Standby-Modus ausgewählt ist, wählen Sie die Standby-Priorität, das aktive Heartbeat-Intervall und das Standby-Heartbeat-Intervall entsprechend aus. Klicken Sie auf **Anwenden**, um die Konfiguration zu überprüfen.
3. Wenn eine bedarfsabhängige Standby-Verbindung konfiguriert ist, wird der globale standardmäßige bedarfsabhängige Bandbreitenbeschränkung (120%) auf den virtuellen Pfad angewendet. Dies gibt die maximal zulässige WAN-zu-LAN-Bandbreite für den virtuellen Pfad an. Sie wird als Prozentsatz der gesamten Bandbreite angegeben, die von allen Nicht-Standby-Links im virtuellen Pfad bereitgestellt wird. Solange die verfügbare Bandbreite im virtuellen Pfad unterhalb des Grenzwerts liegt und eine ausreichende Nutzung vorliegt, versucht die Appliance, Pfade auf Anforderung zu aktivieren, um die Bandbreite zu ergänzen.
4. Öffnen Sie die Abschnitte Global > **Virtual WAN Network** Settings, um das **globale** standardmäßige Bandbreitenlimit auf Anforderung anzuzeigen oder zu ändern.

Global Security Settings

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode:

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type:

☐ Enable FIPS Mode

Network Secure Key:

Global Firewall Settings

Global Policy Template:

Default Firewall Action:

☐ Default Connection State Tracking

Denied Timeout (s):

TCP Initial Timeout (s):

TCP Idle Timeout (s):

TCP Closing Timeout (s):

TCP Time Wait Timeout (s):

TCP Closed Timeout (s):

UDP Initial Timeout (s):

UDP Idle Timeout (s):

ICMP Initial Timeout (s):

ICMP Idle Timeout (s):

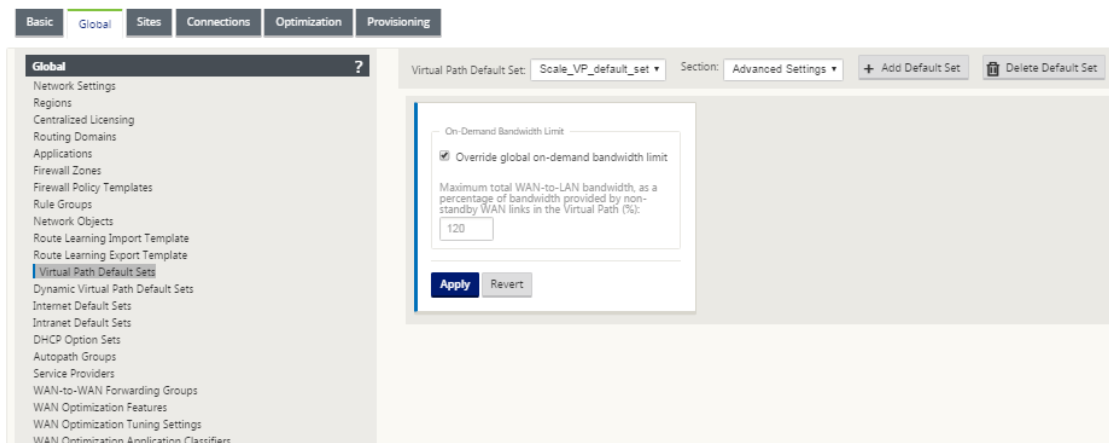
Generic Initial Timeout (s):

Generic Idle Timeout (s):

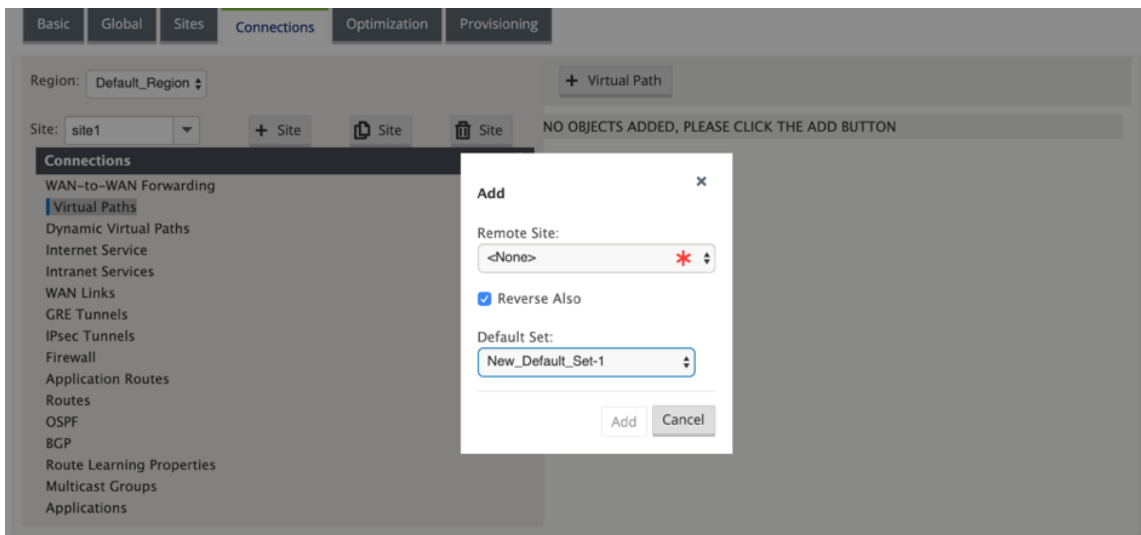
Global On-Demand Bandwidth Limit Setting

Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%):

- Wenn Sie ein bedarfsspezifisches Bandbreitenlimit für einen virtuellen Pfad anwenden und die globale Standardeinstellung unverändert beibehalten möchten, muss ein virtueller Pfadvorgabesatz erstellt und das bedarfsgesteuerte Bandbreitenlimit in den erweiterten Einstellungen geändert werden.



6. Um Einstellungen für einen bestimmten virtuellen Pfad anzuwenden, navigieren Sie zum Abschnitt **Verbindungen > Virtuelle Pfade**, und klicken Sie auf **+ Virtueller Pfad**.



Überwachung von getakteten und Standby-WAN-Verbindungen

- Die Seite Dashboard enthält die folgenden Informationen **zur WAN-Link Metering** mit den Verwendungswerten:
 - **WAN-Link-Name:** Zeigt den WAN-Link-Namen an.
 - **Gesamtauslastung:** Zeigt den gesamten Datenverkehr an (Datennutzung + Steuerungsbelegung).
 - **Datenverwendung:** Zeigt die Verwendung nach Benutzerdatenverkehr an.
 - **Steuerungsauslastung:** Zeigt die Verwendung nach Steuerdatenverkehr an.
 - **Verwendung (in%):** Zeigt den verwendeten Daten-Cap-Wert in Prozent (Gesamtnutzung/Daten-Cap) x 100 an.
 - **Abrechnungszeitraum:** Abrechnungsfrequenz (wöchentlich/monatlich)

- **Beginnend von:** Startdatum des Abrechnungszyklus
- **Verstrichene Tage:** Die verstrichene Zeit (in Tagen, Stunden, Minuten und Sekunden)

The screenshot shows the 'Monitoring' tab in the Citrix SD-WAN 11.2 interface. It displays several sections:

- System Status:** Name: MCN_DC, Model: VPX, Sub-Model: BASE, Appliance Mode: MCN, Serial Number: abd6562d-8259-d2b5-d81e-21b0296d0b9a, Management IP Address: 10.106.172.82, Appliance Uptime: 1 day, 19 hours, 16 minutes, 15.5 seconds, Service Uptime: 2 minutes, 2.0 seconds, Routing Domain Enabled: Default_RoutingDomain.
- Local Versions:** Software Version: 11.0.8.401.434810, Built On: Apr 12 2019 at 10:51:28, Hardware Version: VPX, OS Partition Version: 5.1.
- Virtual Path Service Status:** Virtual Path MCN_DC-BRANCH-1: Uptime: 1 minutes, 57.0 seconds.
- WAN Link Metering:** WAN Link Name: MCN_DC-WL-1, Total Usage: 35.23 MBs of 400 MBs, Data Usage: 34.91 MBs, Control Usage: 0.32 MBs, Billing Cycle: MONTHLY, Starting From: 05/13/2019, Days Elapsed: 12 days of 31 days.

- Wenn Pfadstatistiken (**Monitoring > Statistics > Paths**) angezeigt werden, werden gemessene Links und Standby-Links wie im Screenshot gezeigt markiert.

The screenshot shows the 'Monitoring > Statistics' page. The 'Path Statistics Summary' table displays the following data:

| Num | From Link | To Link | Path State | Virtual Path Service State | Virtual Path Service Type | BOWT | Jitter (mS) | Loss % | kbps | Congestion |
|-----|-------------------|-------------------|------------|----------------------------|---------------------------|------|-------------|--------|------|------------|
| 1 | Dallas_MCN-queue1 | ANZ_RCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 2 | ANZ_RCN-queue1 | Dallas_MCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 3 | Dallas_MCN-queue1 | APAC_RCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 4 | APAC_RCN-queue1 | Dallas_MCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 5 | Dallas_MCN-queue1 | California-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 6 | California-queue1 | Dallas_MCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 7 | Dallas_MCN-queue1 | EMEA_RCN-queue2 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 8 | EMEA_RCN-queue2 | Dallas_MCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 9 | Dallas_MCN-WL-2 | Newyork-WL-2 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 10 | Dallas_MCN-queue1 | Newyork-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 11 | Newyork-WL-2 | Dallas_MCN-WL-2 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 12 | Newyork-queue1 | Dallas_MCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 13 | Dallas_MCN-queue1 | Texas-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 14 | Texas-queue1 | Dallas_MCN-queue1 | DEAD | DEAD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |

Showing 1 to 14 of 14 entries
Bandwidth calculated over the last 73.55 seconds

- Wenn die Appliance über einen virtuellen Pfad verfügt, der über einen lokalen oder Remote-On-Demand-Standby-Link verfügt, wird bei der Anzeige der WAN-Link-Nutzungsstatistiken am unteren Rand der Seite eine zusätzliche Tabelle angezeigt (**Überwachung > Statistik > WAN-Link-Nutzung**).

Local WAN-to-LAN On Demand WAN Link Usages

Filter: in Any column

Apply

Show 100 entries Showing 0 to 0 of 0 entries

First Previous Next Last

| Adaptive Bandwidth Detection | | | | | | | | | | |
|------------------------------|---------------|------------------|------------|----------------------------|-------------------------|-------------------------|-------------------|---|---------------------------------------|--------|
| WAN Link | WAN Link Mode | Standby Priority | Configured | Minimum Acceptable BW Kbps | Maximum Allowed BW Kbps | Current Allowed BW Kbps | Virtual Path Name | Virtual Path On Demand Bandwidth Limit Kbps | Virtual Path Available Bandwidth Kbps | In Use |
| No data available in table | | | | | | | | | | |

Showing 0 to 0 of 0 entries

First Previous Next Last

Bandwidth calculated over the last 5.078 seconds

- Wenn die Verwendung eines getakteten Links 50% des konfigurierten Datendeckels überschreitet, wird oben im Dashboard ein Warnbanner angezeigt. Wenn die Verwendung 75% des konfigurierten Datendeckels überschreitet, werden außerdem die numerischen Messinformationen am unteren Rand des Dashboards hervorgehoben.

The data usage on the following Metered Wanlinks have reached the threshold:

- BR1-WL1-New : 75%.

| System Status | |
|-------------------------|--------------------------------------|
| Name: | BR1 |
| Model: | VPX |
| Sub-Model: | BASE |
| Appliance Mode: | Client |
| Serial Number: | aa4580cb-7527-8dee-f8ea-9824a89142e6 |
| Management IP Address: | 10.105.184.72 |
| Appliance Uptime: | 10 hours, 7 minutes, 34.6 seconds |
| Service Uptime: | 9 hours, 17 minutes, 53.0 seconds |
| Routing Domain Enabled: | Default, RoutingDomain |

| Local Versions | |
|---------------------------|--------------------------|
| Configuration Created On: | Thu Apr 18 20:06:57 2019 |
| Software Version: | 11.0.13.401.434810 |
| Built On: | Apr 18 2019 at 19:35:14 |
| Hardware Version: | VPX |
| OS Partition Version: | 5.1 |

| Virtual Path Service Status | |
|-----------------------------|--|
| Virtual Path DC-BR1 | Uptime: 9 hours, 17 minutes, 43.0 seconds. |

| WAN Link Metering | |
|----------------------------|-----------------------|
| WAN Link Name: BR1-WL1-New | |
| Total Usage: | 329.58 MBs of 400 MBs |
| Data Usage: | 258.09 MBs |
| Control Usage: | 71.48 MBs |
| Usage (%) | 82 |
| Billing Cycle: | MONTHLY |
| Starting From: | 07/17/2019 |
| Days Elapsed: | 3 days of 31 days |

Ein WAN-Link-Verwendungsereignis wird auch an der Appliance generiert, wenn die Verwendung 50%, 75% und 90% der konfigurierten Datenobergrenze überschreitet.

| | | | | | | | |
|-------|---|----------------|----------|---------------------|---------|---------|---|
| 17654 | 1 | RL-TB-CL1-WL-2 | WAN LINK | 2017-05-24 10:22:58 | USAGE_3 | WARNING | Total usage 1.84 Cbytes used (91% of limit 2.00 Cbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017 |
| 17653 | 1 | RL-TB-CL1-WL-2 | WAN LINK | 2017-05-24 10:17:58 | USAGE_2 | WARNING | Total usage 1.52 Cbytes used (75% of limit 2.00 Cbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017 |
| 17652 | 1 | RL-TB-CL1-WL-2 | WAN LINK | 2017-05-24 10:09:58 | USAGE_1 | WARNING | Total usage 1.00 Cbytes used (50% of limit 2.00 Cbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017 |

- Wenn ein Standby-Pfad zwischen dem Standby-Modus und dem aktiven Zustand wechselt, wird ein Ereignis von der Appliance generiert.

| | | | | | | | |
|-------|---|--------------------------------|--------------|---------------------|---------|--------|---|
| 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. Die konfigurierten aktiven und Standby-Taktintervalle für jeden Pfad können unter **Konfiguration > Virtuelles WAN > Konfiguration anzeigen > Pfade** angezeigt werden.

Dashboard

Monitoring

Configuration

+

Appliance Settings

-

Virtual WAN

View Configuration

Configuration Editor

Change Management

Change Management Settings

Compare Configurations

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

+

System Maintenance

Configuration > Virtual WAN > View Configuration

Configuration

View: Paths

Path Configuration

Paths on virtual path 3 'Dallas_MCN-ANZ_RCN':

| Path ID | From Link | To Link | Primary Src IP Address | Primary Dst IP Address | Secondary Src IP Address | Secondary Dst IP Address | Src Port | Dst Port | Alt Src |
|---------|-------------------|-------------------|------------------------|------------------------|--------------------------|--------------------------|----------|----------|---------|
| 0 | Dallas_MCN-queue1 | ANZ_RCN-queue1 | 192.168.1.10 | 192.168.90.10 | - | - | 4980 | 4980 | |
| 0 | ANZ_RCN-queue1 | Dallas_MCN-queue1 | 192.168.90.10 | 192.168.1.10 | - | - | 4980 | 4980 | |

| From Link | To Link | Realtime Eligible | Interactive Eligible | Bulk Eligible | Path Group | Standby Heartbeat Interval(ms) | Active Heartbeat Interval(ms) |
|-------------------|-------------------|-------------------|----------------------|---------------|------------|--------------------------------|-------------------------------|
| Dallas_MCN-queue1 | ANZ_RCN-queue1 | YES | YES | YES | 0 | n/a | n/a |
| ANZ_RCN-queue1 | Dallas_MCN-queue1 | YES | YES | YES | 0 | n/a | n/a |

Paths on virtual path 8 'Dallas_MCN-APAC_RCN':

| Path ID | From Link | To Link | Primary Src IP Address | Primary Dst IP Address | Secondary Src IP Address | Secondary Dst IP Address | Src Port | Dst Port | Alt Src |
|---------|-------------------|-------------------|------------------------|------------------------|--------------------------|--------------------------|----------|----------|---------|
| 0 | Dallas_MCN-queue1 | APAC_RCN-queue1 | 192.168.1.10 | 192.168.80.10 | - | - | 4980 | 4980 | |
| 0 | APAC_RCN-queue1 | Dallas_MCN-queue1 | 192.168.80.10 | 192.168.1.10 | - | - | 4980 | 4980 | |

| From Link | To Link | Realtime Eligible | Interactive Eligible | Bulk Eligible | Path Group | Standby Heartbeat Interval(ms) | Active Heartbeat Interval(ms) |
|-------------------|-------------------|-------------------|----------------------|---------------|------------|--------------------------------|-------------------------------|
| Dallas_MCN-queue1 | APAC_RCN-queue1 | YES | YES | YES | 0 | n/a | n/a |
| APAC_RCN-queue1 | Dallas_MCN-queue1 | YES | YES | YES | 0 | n/a | n/a |

Paths on virtual path 9 'Dallas_MCN-California':

| Path ID | From Link | To Link | Primary Src IP Address | Primary Dst IP Address | Secondary Src IP Address | Secondary Dst IP Address | Src Port | Dst Port | Alt Src |
|---------|-------------------|-------------------|------------------------|------------------------|--------------------------|--------------------------|----------|----------|---------|
| 0 | Dallas_MCN-queue1 | California-queue1 | 192.168.1.10 | 192.168.50.10 | - | - | 4980 | 4980 | |
| 0 | California-queue1 | Dallas_MCN-queue1 | 192.168.50.10 | 192.168.1.10 | - | - | 4980 | 4980 | |

| From Link | To Link | Realtime Eligible | Interactive Eligible | Bulk Eligible | Path Group | Standby Heartbeat Interval(ms) | Active Heartbeat Interval(ms) |
|-------------------|-------------------|-------------------|----------------------|---------------|------------|--------------------------------|-------------------------------|
| Dallas_MCN-queue1 | California-queue1 | YES | YES | YES | 0 | n/a | n/a |
| California-queue1 | Dallas_MCN-queue1 | YES | YES | YES | 0 | n/a | n/a |

Paths on virtual path 12 'Dallas_MCN-EMEA_RCN':

| Path ID | From Link | To Link | Primary Src IP Address | Primary Dst IP Address | Secondary Src IP Address | Secondary Dst IP Address | Src Port | Dst Port | Alt Src |
|---------|-------------------|-------------------|------------------------|------------------------|--------------------------|--------------------------|----------|----------|---------|
| 0 | Dallas_MCN-queue1 | EMEA_RCN-queue2 | 192.168.1.10 | 17.1.1.10 | - | - | 4980 | 4980 | |
| 0 | EMEA_RCN-queue2 | Dallas_MCN-queue1 | 17.1.1.10 | 192.168.1.10 | - | - | 4980 | 4980 | |

| From Link | To Link | Realtime Eligible | Interactive Eligible | Bulk Eligible | Path Group | Standby Heartbeat Interval(ms) | Active Heartbeat Interval(ms) |
|-------------------|-------------------|-------------------|----------------------|---------------|------------|--------------------------------|-------------------------------|
| Dallas_MCN-queue1 | EMEA_RCN-queue2 | YES | YES | YES | 0 | n/a | n/a |
| EMEA_RCN-queue2 | Dallas_MCN-queue1 | YES | YES | YES | 0 | n/a | n/a |

Paths on virtual path 13 'Dallas_MCN-Newyork':

| Path ID | From Link | To Link | Primary Src IP Address | Primary Dst IP Address | Secondary Src IP Address | Secondary Dst IP Address | Src Port | Dst Port | Alt Src |
|---------|-------------------|-------------------|------------------------|------------------------|--------------------------|--------------------------|----------|----------|---------|
| 1 | Dallas_MCN-queue1 | Newyork-queue1 | 192.168.1.10 | 192.168.70.10 | - | - | 4980 | 4980 | |
| 0 | Dallas_MCN-WL-2 | Newyork-WL-2 | 192.168.10.10 | 192.168.60.10 | - | - | 4980 | 4980 | |
| 0 | Newyork-WL-2 | Dallas_MCN-WL-2 | 192.168.60.10 | 192.168.10.10 | - | - | 4980 | 4980 | |
| 1 | Newyork-queue1 | Dallas_MCN-queue1 | 192.168.70.10 | 192.168.1.10 | - | - | 4980 | 4980 | |

| From Link | To Link | Realtime Eligible | Interactive Eligible | Bulk Eligible | Path Group | Standby Heartbeat Interval(ms) | Active Heartbeat Interval(ms) |
|-------------------|-------------------|-------------------|----------------------|---------------|------------|--------------------------------|-------------------------------|
| Dallas_MCN-queue1 | Newyork-queue1 | YES | YES | YES | 0 | n/a | n/a |
| Dallas_MCN-WL-2 | Newyork-WL-2 | YES | YES | YES | 0 | n/a | n/a |
| Newyork-WL-2 | Dallas_MCN-WL-2 | YES | YES | YES | 0 | n/a | n/a |
| Newyork-queue1 | Dallas_MCN-queue1 | YES | YES | YES | 0 | n/a | n/a |

Paths on virtual path 14 'Dallas_MCN-Texas':

| Path ID | From Link | To Link | Primary Src IP Address | Primary Dst IP Address | Secondary Src IP Address | Secondary Dst IP Address | Src Port | Dst Port | Alt Src |
|---------|-------------------|-------------------|------------------------|------------------------|--------------------------|--------------------------|----------|----------|---------|
| 0 | Dallas_MCN-queue1 | Texas-queue1 | 192.168.1.10 | 192.168.40.10 | - | - | 4980 | 4980 | |
| 0 | Texas-queue1 | Dallas_MCN-queue1 | 192.168.40.10 | 192.168.1.10 | - | - | 4980 | 4980 | |

| From Link | To Link | Realtime Eligible | Interactive Eligible | Bulk Eligible | Path Group | Standby Heartbeat Interval(ms) | Active Heartbeat Interval(ms) |
|-------------------|-------------------|-------------------|----------------------|---------------|------------|--------------------------------|-------------------------------|
| Dallas_MCN-queue1 | Texas-queue1 | YES | YES | YES | 0 | n/a | n/a |
| Texas-queue1 | Dallas_MCN-queue1 | YES | YES | YES | 0 | n/a | n/a |

Office 365-Optimierung

May 10, 2021

Die **Office 365-Optimierungsfunktionen** halten sich an die [Microsoft Office 365-Netzwerkverbindungsgrundsätze](#), um Office 365 zu optimieren. Office 365 wird als Service über mehrere Service-Endpunkte (Front-türen) bereitgestellt, die sich global befinden. Um eine optimale Benutzererfahrung für Office 365-Datenverkehr zu erzielen, empfiehlt Microsoft, Office365-Datenverkehr aus Zweigumgebungen direkt ins Internet umzuleiten und Praktiken wie Backhauling auf einen zentralen Proxy zu vermeiden. Dies liegt daran, dass Office 365-Datenverkehr wie Outlook, Word usw. empfindlich auf Latenz reagieren und Backhauling-Datenverkehr mehr Latenz führt, was zu einer schlechten Benutzererfahrung führt. Mit Citrix SD-WAN können Sie Richtlinien konfigurieren, um Office 365-Datenverkehr zum Internet auszuschalten.

Der Office 365-Datenverkehr wird an den nächsten Office 365-Dienstendpunkt weitergeleitet, der an den Rändern der Microsoft Office 365-Infrastruktur weltweit vorhanden ist. Sobald der Datenverkehr eine Haustür erreicht, geht er über das Microsoft-Netzwerk und erreicht das eigentliche Ziel. Dadurch wird die Latenz minimiert, da die Roundtrip Zeit vom Kundennetzwerk zum Office 365-Endpunkt reduziert wird.

Office 365-Endpunkte

Office 365-Endpunkte sind eine Reihe von Netzwerkadressen und Subnetzen. Endpunkte werden in die folgenden drei Kategorien unterteilt:

- **Optimieren** - Diese Endpunkte bieten Konnektivität zu jedem Office 365-Dienst und -Feature und sind empfindlich auf Verfügbarkeit, Leistung und Latenz. Es stellt über 75% der Office 365-Bandbreite, Verbindungen und Datenvolumen dar. Alle Endpunkte optimieren werden in Microsoft-Rechenzentren gehostet. Serviceanforderungen an diese Endpunkte sollten vom Zweig zum Internet ausbrechen und nicht über das Rechenzentrum gehen.
- **Zulassen** - Diese Endpunkte bieten nur Verbindungen zu bestimmten Office 365-Diensten und -Features und sind nicht so empfindlich auf Netzwerkleistung und Latenz. Die Darstellung der Office 365-Bandbreite und der Anzahl der Verbindungen ist ebenfalls geringer. Diese Endpunkte werden in Microsoft-Rechenzentren gehostet. Dienstanforderungen an diese Endpunkte können vom Zweig zum Internet ausbrechen oder das Rechenzentrum durchlaufen.
- **Standard** - Diese Endpunkte stellen Office 365-Dienste bereit, die keine Optimierung erfordern und als normaler Internetverkehr behandelt werden können. Einige dieser Endpunkte werden möglicherweise nicht in Microsoft-Rechenzentren gehostet. Der Datenverkehr in dieser Kategorie ist nicht anfällig für Latenzschwankungen. Daher führt ein direktes Ausbrechen

dieser Art von Datenverkehr zu keiner Leistungssteigerung im Vergleich zum Internetausfall. Darüber hinaus ist der Datenverkehr in dieser Kategorie möglicherweise nicht immer Office 365-Datenverkehr. Daher wird empfohlen, diese Option zu deaktivieren, wenn Office 365-Unterbrechung in Ihrem Netzwerk aktiviert wird.

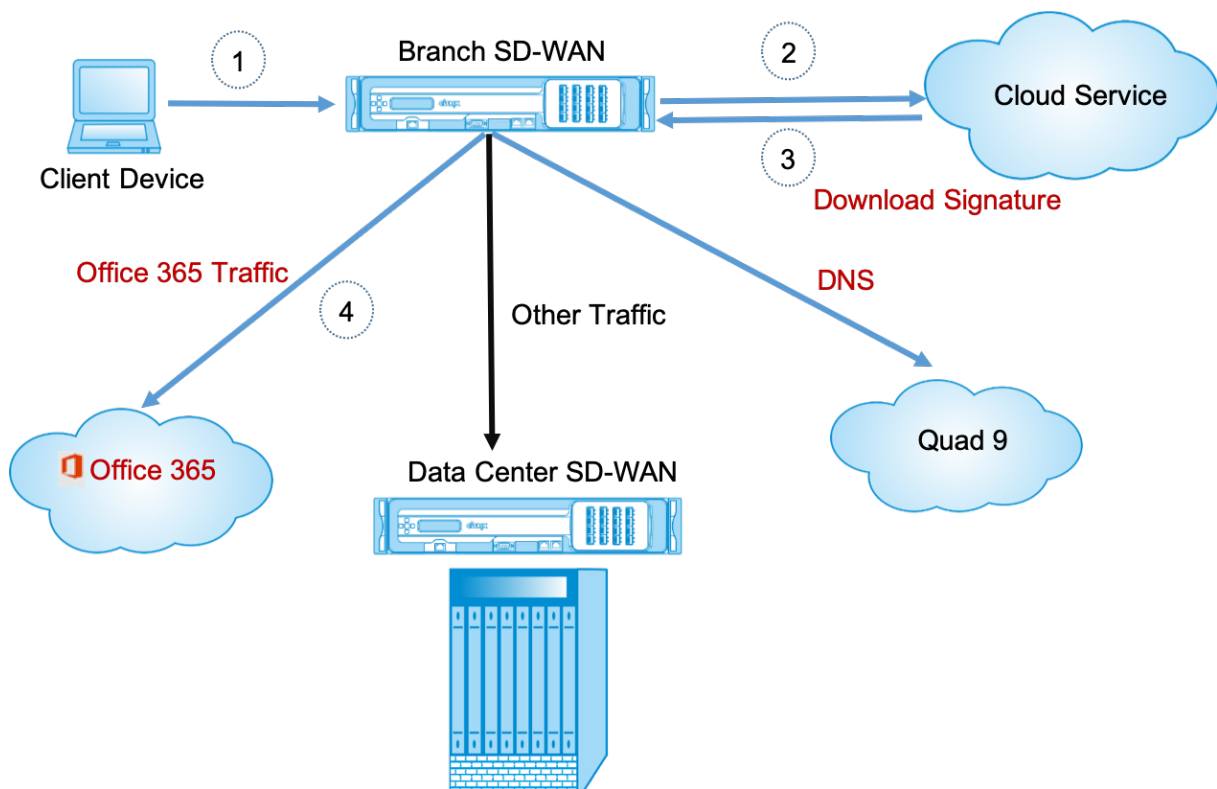
Funktionsweise der Office 365-Optimierung

Die Microsoft-Endpunktsignaturen werden höchstens einmal täglich aktualisiert. Der Agent auf der Appliance fragt täglich den Citrix Dienst (sdwan-app-routing.citrixnetworkapi.net) ab, um die neuesten Endpunktsignaturen zu erhalten. Die SD-WAN-Appliance fragt den Citrix Dienst (sdwan-app-routing.citrixnetworkapi.net) einmal täglich ab, wenn die Appliance eingeschaltet und Office 365-Optimierung aktiviert ist. Wenn neue Signaturen verfügbar sind, lädt die Appliance sie herunter und speichert sie in der Datenbank. Bei den Signaturen handelt es sich im Wesentlichen um eine Liste von URLs und IPs, die verwendet werden, um Office 365-Datenverkehr basierend auf den Verkehrssteuerungsrichtlinien zu erkennen, die konfiguriert werden können.

Hinweis

Erste Paketerkennung und Klassifizierung von Office 365-Datenverkehr wird nur durchgeführt, wenn das Office 365-Breakout-Feature aktiviert ist.

Wenn eine Anforderung für Office 365-Anwendung eintrifft, führt der Anwendungsklassifikator eine erste Paketklassifikatordatenbanksuche durch, identifiziert und markiert Office 365-Datenverkehr. Sobald der Office 365-Datenverkehr klassifiziert ist, werden die automatisch erstellten Anwendungsrouten und Firewallrichtlinien wirksam und unterbricht den Datenverkehr direkt zum Internet. Die Office 365-DNS-Anforderungen werden an bestimmte DNS-Dienste wie Quad9 weitergeleitet. Weitere Informationen finden Sie unter [Domänennamensystem](#).



Die Signaturen werden vom Cloud Service (sdwan-app-routing.citrixnetworkapi.net) heruntergeladen.

Konfigurieren von Office 365 - Breakout

Mit der Office 365-Richtlinie können Sie angeben, welche Kategorie von Office 365-Datenverkehr Sie direkt aus dem Zweig ausbrechen können. Beim Aktivieren von Office 365-Unterbrechung und Kompilieren der Konfiguration wird automatisch ein DNS-Objekt, ein Anwendungsobjekt, eine Anwendungsroute und eine Firewallrichtlinienvorlage erstellt und auf Zweigstandorte mit Internetdienst angewendet.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben:

1. Um Office 365 Breakout durchzuführen, muss ein Internetdienst auf der Appliance konfiguriert werden. Weitere Informationen zum Konfigurieren des Internetdienstes finden Sie unter [Internetzugriff](#).
2. Stellen Sie sicher, dass die Verwaltungsschnittstelle über eine Internetverbindung verfügt.
Sie können die Einstellungen der Verwaltungsschnittstelle mithilfe der Citrix SD-WAN - Webschnittstelle konfigurieren.

3. Stellen Sie sicher, dass das Management-DNS konfiguriert ist. Um das DNS der Verwaltungsschnittstelle zu konfigurieren, navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter**. Geben Sie im Abschnitt **DNS-Einstellungen** die Details des primären und sekundären DNS-Servers ein, und klicken Sie auf **Einstellungen ändern**.

The screenshot shows the 'Configuration > Appliance Settings > Network Adapters' page. The 'Management Interface IP' section is visible, with tabs for 'IP Address', 'Ethernet', and 'Mobile Broadband'. The 'DHCP' section has an 'Enable DHCP' checkbox. The 'Manual' section contains input fields for 'IP Address' (10.105.147.52), 'Subnet Mask' (255.255.255.0), and 'Gateway IP Address' (10.105.147.1). Below this, the 'DNS Settings' section is highlighted with a red box. It contains input fields for 'Primary DNS' and 'Secondary DNS', and 'Change Settings' and 'Clear Settings' buttons.

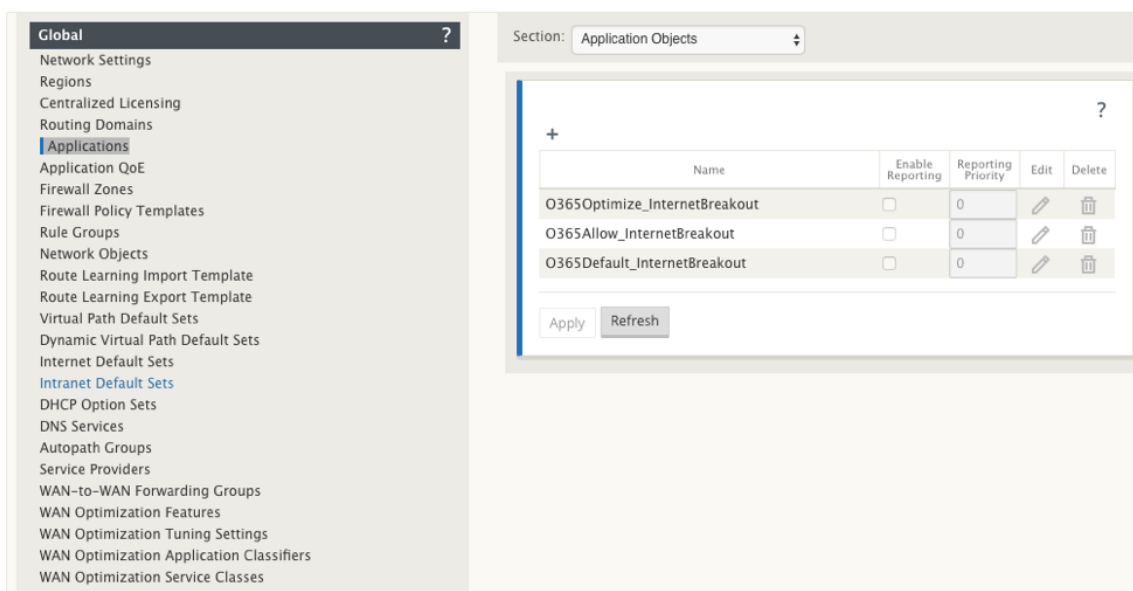
Die Einstellung **Office 365 Breakout Policy** ist unter globalen Einstellungen verfügbar, wählen Sie die erforderliche Office 365-Kategorie für Internetbreakout aus, und klicken Sie auf **Übernehmen**.

The screenshot shows the 'Global' settings page. The 'Section' dropdown is set to 'Office 365 Breakout Policy'. The 'Policy Settings' section is visible, with a table showing the 'O365 URL Category' and 'Direct Internet Breakout From Branch' settings. The 'Allow' category is selected, and the 'Direct Internet Breakout From Branch' checkbox is checked. The 'Apply' and 'Revert' buttons are at the bottom.

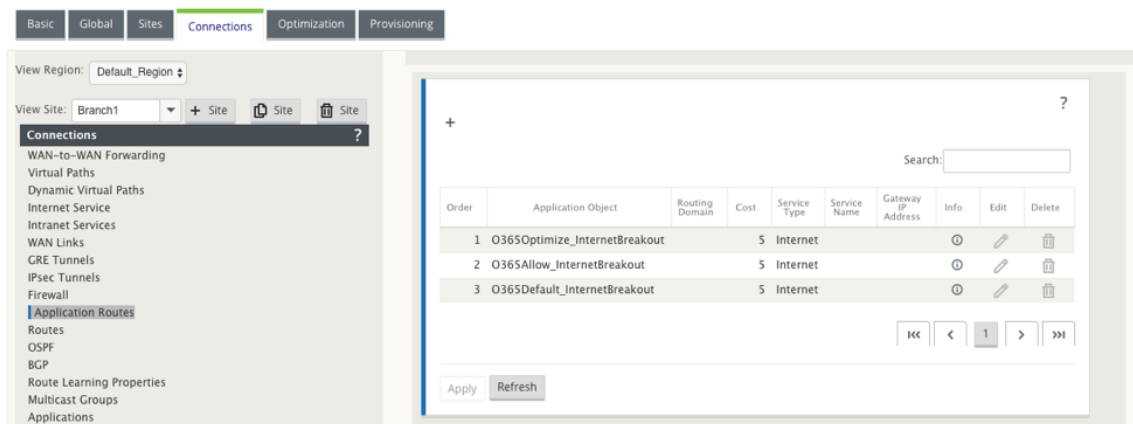
| O365 URL Category | Direct Internet Breakout From Branch |
|-------------------|--------------------------------------|
| Optimize | <input checked="" type="checkbox"/> |
| Allow | <input checked="" type="checkbox"/> |
| Default | <input type="checkbox"/> |

Nachdem Sie Office 365 konfiguriert haben, brechen Sie Richtlinieneinstellungen aus und kompilieren Sie die Konfiguration. Die folgenden Einstellungen werden automatisch ausgefüllt.

- **DNS-Objekt** - Das DNS-Objekt gibt an, welche Art von Datenverkehr an den DNS-Dienst weitergeleitet werden soll, den der Benutzer konfiguriert ist. Die DNS-Anforderungen werden auf allen vertrauenswürdigen Schnittstellen gehört, und DNS-Weiterleitungen sind enthalten, um Office 365-DNS-Anforderungen an den Quad9-Dienst zu leiten. Diese Weiterleitungsregel hat die höchste Priorität. Weitere Informationen finden Sie im Abschnitt **Domain Name Service**.
- **Anwendungsobjekt** - Ein Anwendungsobjekt mit der vom Benutzer ausgewählten Office 365-Kategorie wird erstellt. Wenn Sie die Kategorien Optimieren, Zulassen und Standardkategorien ausgewählt haben, werden die Anwendungsobjekte **O365Optimize_InternetBreakout**, **O365Allow_InternetBreakout** und **O365Default_InternetBreakout** erstellt.



- **Anwendungsroute:** Für jedes Office 365-Anwendungsobjekt mit dem Internetdiensttyp wird eine Anwendungsroute erstellt.



- **Firewall-Richtlinienvorlage für die Pre-Appliance:** Für jede konfigurierte Office 365-

Kategorie wird eine globale Richtlinienvorlage für die Pre-Appliance erstellt. Diese Vorlage wird auf alle Zweigwebsites angewendet, die über einen Internetdienst verfügen. Die Richtlinie vor der Appliance hat Vorrang vor lokalen Richtlinienvorlagen und Post-Appliance-Richtlinien.

Section: Policies

Pre-Appliance Template Policies

| Template | Routing Domain | Action | Zones | | Application | Application Family | Application Objects | IP Protocol | DSCP | Service | Source | | Destination | | | Match Est. | Reverse Also | Info |
|--------------------|----------------|--------|-------|----|-------------|--------------------|-------------------------------|-------------|------|---------|------------|------|-------------|------------|------|------------|--------------|------|
| | | | From | To | | | | | | | IP Address | Port | Service | IP Address | Port | | | |
| O365Optimize_In... | * | Allow | * | * | * | * | O365Optimize_InternetBreakout | Any | * | * | * | * | * | * | * | * | | ⓘ |
| O365Allow_Inter... | * | Allow | * | * | * | * | O365Allow_InternetBreakout | Any | * | * | * | * | * | * | * | * | | ⓘ |
| O365Default_Int... | * | Allow | * | * | * | * | O365Default_InternetBreakout | Any | * | * | * | * | * | * | * | * | | ⓘ |

Transparente Weiterleitung für Office 365

Der Zweig bricht für Office 365 beginnt mit einer DNS-Anforderung. Die DNS-Anforderung, die Office 365-Domänen durchläuft, muss lokal gesteuert werden. Wenn Office 365 Internet Breakout aktiviert ist, werden die internen DNS-Routen ermittelt und die Liste der transparenten Weiterleitungen automatisch aufgefüllt. Office 365-DNS-Anforderungen werden standardmäßig an den Open-Source-DNS-Dienst Quad9 weitergeleitet. Der Quad9-DNS-Dienst ist sicher, skalierbar und verfügt über Multi-Pop-Präsenz. Sie können den DNS-Dienst bei Bedarf ändern.

Transparente Weiterleitungen für Office 365-Anwendungen werden in jeder Zweigstelle erstellt, in der Internetdienst und Office 365-Breakout aktiviert sind.

Wenn Sie einen anderen DNS-Proxy verwenden oder SD-WAN als DNS-Proxy konfiguriert ist, wird die Weiterleitungsliste automatisch mit Weiterleitungen für Office 365-Anwendungen gefüllt.

BasicGlobalSitesConnectionsOptimizationProvisioning

View Region: Default_Region

View Site: Branch-CB2K + Site Site Site

Sites ?

Basic Settings
Centralized Licensing
Routing Domains
Interface Groups
Virtual IP Addresses
VRRP
DHCP
WAN Links
Certificates
High Availability
DNS

Section: DNS Transparent Forwarders

+ ?

| Order | Application | DNS Service | Delete |
|-------|------------------------------|-------------|--------|
| 100 | Office 365 Optimize(offic... | Quad9 | 🗑 |
| 200 | Office 365 Allow(offic36... | Quad9 | 🗑 |
| 300 | Office 365 Default(offic... | Quad9 | 🗑 |

Apply Refresh

Überwachen

Sie können die Office 365-Anwendungsstatistiken in den folgenden SD-WAN-Statistikberichten überwachen:

- Firewall-Statistiken

| Connections | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------------|--|--------|-------------|-------------|-------|--------------|--------------------|------------------|----------------|------|--------------|-------------------|---------------|-------------|-------|---------|-------|-------|----------|---------|-------|-------|--------|-----|---------------|---|
| | | Source | | | | | | | Destination | | | | | | | Sent | | | Received | | | | | | | |
| Routing Domain | Application | Family | IP Protocol | IP Address | Port | Service Type | Service Name | Zone | IP Address | Port | Service Type | Service Name | Zone | State | In MB | Packets | Bytes | PPS | Mbps | Packets | Bytes | PPS | Mbps | Age | Last Activity | Related Objects |
| Default_RoutingDomain | Windows LiveConnectSvc | 9966 | TCP | 172.17.0.10 | 80982 | Local | VirtualInterface-1 | Default_LAN_Zone | 104.127.201.20 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 10 | 1888 | 0.071 | 0.071 | 13 | 4761 | 0.062 | 0.236 | 21 | 3903 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 58078 | Local | VirtualInterface-1 | Default_LAN_Zone | 52.108.238.4 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 54 | 7076 | 0.737 | 0.772 | 56 | 13280 | 0.764 | 1.430 | 20 | 2893 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 80982 | Local | VirtualInterface-1 | Default_LAN_Zone | 13.107.6.171 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 1085 | 82353 | 5.411 | 22.493 | 1890 | 66909 | 6.418 | 18.274 | 20 | 4692 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 80945 | Local | VirtualInterface-1 | Default_LAN_Zone | 13.107.6.171 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 63 | 23012 | 0.231 | 0.796 | 72 | 14114 | 0.287 | 0.649 | 21 | 3902 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 80982 | Local | VirtualInterface-1 | Default_LAN_Zone | 13.107.6.156 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 381 | 13192 | 0.903 | 2.443 | 412 | 35662 | 0.953 | 6.608 | 20 | 4617 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 80901 | Local | VirtualInterface-1 | Default_LAN_Zone | 40.126.12.101 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 22 | 4238 | 0.073 | 0.116 | 17 | 14058 | 0.058 | 0.381 | 20 | 3904 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 58075 | Local | VirtualInterface-1 | Default_LAN_Zone | 52.108.238.4 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 28 | 8499 | 0.317 | 0.769 | 23 | 10359 | 0.260 | 0.910 | 20 | 2894 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 58076 | Local | VirtualInterface-1 | Default_LAN_Zone | 52.108.238.4 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 65 | 7864 | 0.747 | 0.717 | 73 | 14968 | 0.821 | 1.383 | 20 | 3901 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 62016 | Local | VirtualInterface-1 | Default_LAN_Zone | 52.108.26.1 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 27 | 4379 | 0.932 | 1.538 | 15 | 10058 | 0.658 | 3.745 | 20 | 3902 | (See FlowView for more details) |
| Default_RoutingDomain | Office 365 Common(PfxAll)_common | 9966 | TCP | 172.17.0.10 | 58082 | Local | VirtualInterface-1 | Default_LAN_Zone | 40.126.12.102 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 38 | 15423 | 0.217 | 0.743 | 39 | 24018 | 0.173 | 1.187 | 19 | 3902 | (See FlowView for more details) |
| Default_RoutingDomain | Microsoft(Microsoft) | 9966 | TCP | 172.17.0.10 | 80297 | Local | VirtualInterface-1 | Default_LAN_Zone | 13.107.6.163 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 37 | 7321 | 0.134 | 0.196 | 42 | 10408 | 0.141 | 0.279 | 20 | 3903 | (See FlowView for more details) |
| Default_RoutingDomain | Microsoft(Microsoft) | 9966 | TCP | 172.17.0.10 | 80247 | Local | VirtualInterface-1 | Default_LAN_Zone | 52.203.156.4 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 24 | 3618 | 0.096 | 0.115 | 19 | 9821 | 0.076 | 0.316 | 20 | 3903 | (See FlowView for more details) |
| Default_RoutingDomain | Microsoft(Microsoft) | 9966 | TCP | 172.17.0.10 | 80281 | Local | VirtualInterface-1 | Default_LAN_Zone | 23.58.14.151 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 14 | 1766 | 0.063 | 0.064 | 13 | 6869 | 0.059 | 0.230 | 21 | 4617 | (See FlowView for more details) |
| Default_RoutingDomain | Microsoft Skype for Business (Formerly Microsoft Lync Online) (Office 365)(ync_online) | 9966 | TCP | 172.17.0.10 | 58277 | Local | VirtualInterface-1 | Default_LAN_Zone | 13.107.1.128 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 21 | 2330 | 0.286 | 0.254 | 22 | 15247 | 0.299 | 1.441 | 74 | 7803 | (See FlowView for more details) |
| Default_RoutingDomain | Microsoft Skype for Business (Formerly Microsoft Lync Online) (Office 365)(ync_online) | 9966 | TCP | 172.17.0.10 | 62015 | Local | VirtualInterface-1 | Default_LAN_Zone | 52.114.74.44 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 18 | 3435 | 0.307 | 0.835 | 11 | 9605 | 0.211 | 1.475 | 20 | 3903 | (See FlowView for more details) |
| Default_RoutingDomain | Microsoft SharePoint Online (Office 365)(sharepoint_online) | 9966 | TCP | 172.17.0.10 | 60309 | Local | VirtualInterface-1 | Default_LAN_Zone | 13.107.6.168 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 56 | 8714 | 0.198 | 0.246 | 68 | 15272 | 0.240 | 0.642 | 20 | 3903 | (See FlowView for more details) |
| Default_RoutingDomain | Microsoft SharePoint Online (Office 365)(sharepoint_online) | 9966 | TCP | 172.17.0.10 | 60296 | Local | VirtualInterface-1 | Default_LAN_Zone | 13.107.138.9 | 443 | Internet | Branch-1-Internet | Internet_Zone | ESTABLISHED | Yes | 630 | 25070 | 2.116 | 6.735 | 750 | 38671 | 2.251 | 10.277 | 20 | 3902 | (See FlowView for more details) |

- Strömungen

| 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 |

- DNS-Statistiken

| Dashboard | Monitoring | Configuration |
|----------------------------------|--------------------|--------------------|
| Statistics | Monitoring > DNS | |
| Flows | | |
| Routing Protocols | | |
| Firewall | | |
| IKE/IPsec | | |
| ICMP | | |
| Performance Reports | | |
| Qos Reports | | |
| Usage Reports | | |
| Availability Reports | | |
| Appliance Reports | | |
| DHCP Server/Relay | | |
| VRRP | | |
| PPPoE | | |
| DNS | | |
| DNS Statistics | | |
| Refresh | | |
| Proxy Statistics | | |
| Search: | | |
| Proxy Name | Application Name | DNS Service Name |
| DNS_Proxy1 | office365_optimize | Quad9 |
| DNS_Proxy1 | office365_allow | Quad9 |
| DNS_Proxy1 | office365_default | Quad9 |
| DNS_Proxy1 | Any | Google |
| Showing 1 to 4 of 4 entries | | |
| Transparent Forwarder Statistics | | |
| Search: | | |
| Application Name | DNS Service Name | DNS Service Active |
| office365_allow | Quad9 | YES |
| office365_default | Quad9 | YES |
| office365_optimize | Quad9 | YES |
| Showing 1 to 3 of 3 entries | | |

• Anwendungs-Routenstatistiken

Monitoring > Statistics

Statistics

Show: Application Routes ☒ Enable Auto Refresh 5 seconds ☐ Clear Counters on Refresh Processing...

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 3 of 3 entries

| | | | | | | | | | | | | |
|-----|-------------------------------|--------------------|----------|---------------|-----------|---------|--------|------|-----------|----------|------------------|-------------------|
| Num | Application Object | Gateway IP Address | Service | Firewall Zone | Reachable | Site | Type | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
| 0 | O365Optimize_InternetBreakout | * | Internet | 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

Sie können Office 365-Anwendungsstatistiken auch im SD-WAN Center-Anwendungsbericht anzeigen.

Routing Domain: Any

Applications HDX App QoE MOS Services Classes Sites Virtual Paths Paths WAN Links MPLS Queues Ethernet GRE IPsec Events

Report Type: Top Applications Select Site:

Show Bandwidth/Data in Kbps/KB Filters: +

10 / page Showing 1 - 10 of 12

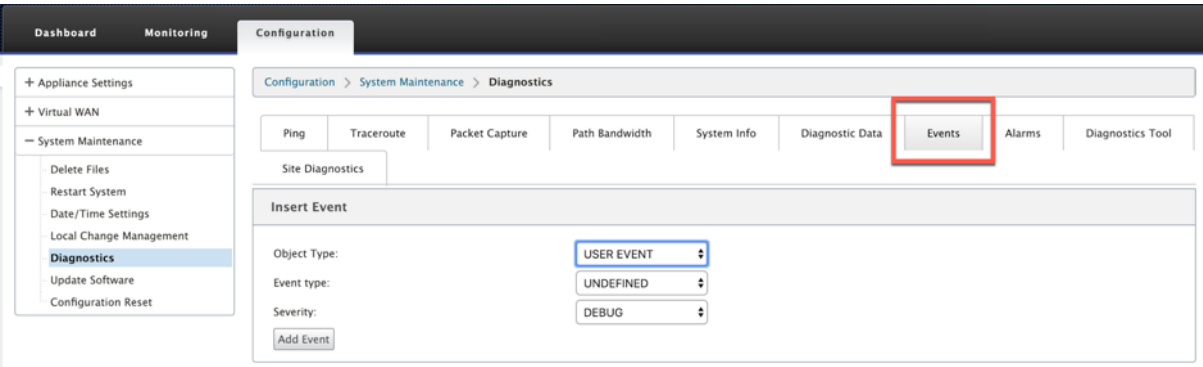
Search

| Application Name | Aggregate Data | Aggregate Outgoing Data | Aggregate Incoming Data | Average Bandwidth | Average Outgoing Bandwidth | Average Incoming Bandwidth | |
|--|----------------|-------------------------|-------------------------|-------------------|----------------------------|----------------------------|--|
| Office 365 Common | 644.22 | 445.29 | 198.93 | 28.63 | 19.79 | 8.84 | |
| Microsoft Office 365 | 440.82 | 21.42 | 419.40 | 19.59 | 0.95 | 18.64 | |
| Microsoft Outlook (Office 365) | 264.79 | 31.72 | 233.07 | 11.77 | 1.41 | 10.36 | |
| Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365) | 215.94 | 178.94 | 37.00 | 9.60 | 7.95 | 1.64 | |
| Microsoft SharePoint Online (Office 365) | 28.48 | 6.09 | 22.39 | 1.27 | 0.27 | 0.99 | |
| Google Generic | 24.09 | 3.63 | 20.46 | 3.21 | 0.48 | 2.73 | |
| Microsoft | 13.29 | 4.01 | 9.28 | 0.59 | 0.18 | 0.41 | |
| Domain Name Service | 6.30 | 6.30 | 0.00 | 0.42 | 0.42 | 0.00 | |

Problembehandlung

Sie können den Dienstfehler im Abschnitt **Ereignisse** der SD-WAN-Appliance anzeigen.

Um die Fehler zu überprüfen, navigieren Sie zu **Konfiguration > Systemwartung > Diagnose**, und klicken Sie auf die Registerkarte **Ereignisse**.



Wenn bei der Verbindung mit dem Citrix Dienst ein Problem auftritt (sdwan-app-routing.citrixnetworkapi.net), wird die Fehlermeldung in der Tabelle **Ereignisse anzeigen** angezeigt.

View Events

Quantity: 25

Filter: Object Type = APPLICATIONS Event type = FAILURE Severity = ERROR

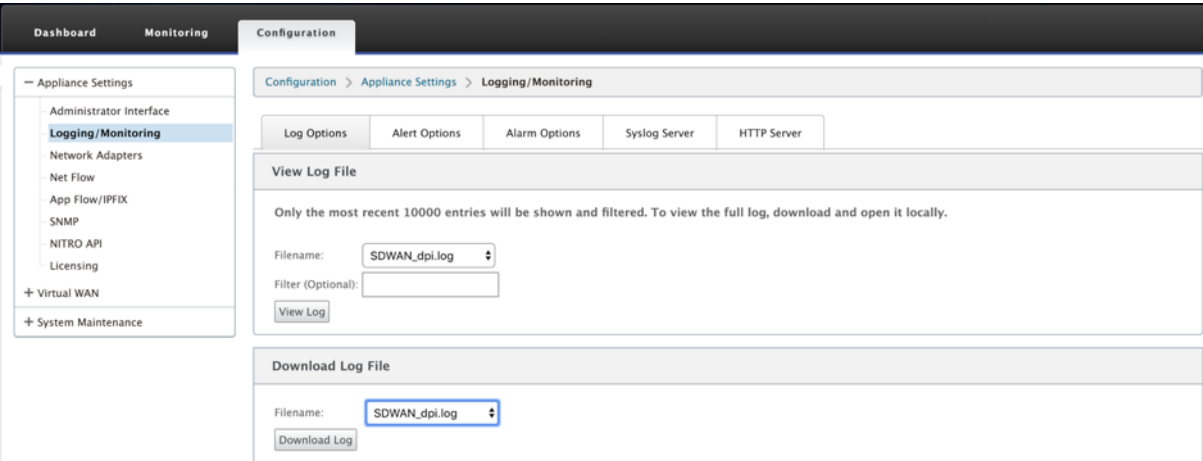
Reload Events Table

| ID | Object ID | Object Name | Object Type | Time | Event Type | Severity | Description |
|-------|-----------|------------------|--------------|---------------------|------------|----------|--------------------------------------|
| 13839 | 26 | Endpoints Update | APPLICATIONS | 2019-02-12 09:02:15 | FAILURE | ERROR | Failed to connect to the service API |

Times are in UTC

Die Verbindungsfehler werden auch in **SDWAN_DPI.log protokolliert**. Um das Protokoll anzuzeigen, navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Logging/Überwachung > Log-Optionen**. Wählen Sie **SDWAN_DPI.log** aus der Dropdown-Liste aus, und klicken Sie auf **Protokoll anzeigen**.

Sie können die Protokolldatei auch herunterladen. Um die Protokolldatei herunterzuladen, wählen Sie die erforderliche Protokolldatei aus der Dropdown-Liste unter dem Abschnitt **Protokolldatei herunterladen** aus und klicken Sie auf **Protokoll herunterladen**.



Einschränkungen

- Wenn Office 365-Breakout-Richtlinie konfiguriert ist, wird keine Deep Packet Inspection für Verbindungen durchgeführt, die für die konfigurierte Kategorie von IP-Adressen bestimmt sind.
- Die automatisch erstellte Firewallrichtlinie und die Anwendungsrouten können nicht bearbeitet werden.
- Die automatisch erstellte Firewallrichtlinie hat die niedrigste Priorität und kann nicht bearbeitet werden.
- Die Routenkosten für die automatisch erstellte Anwendungsrouten betragen fünf. Sie können es mit einer kostengünstigeren Route überschreiben.

Office 365-Beacon-Dienst

Microsoft bietet Office 365-Beacon-Dienst an, um die Erreichbarkeit von Office 365 über die WAN-Verbindungen zu messen. Der Beacon-Dienst ist im Grunde eine URL - `sdwan.measure.office.com/apc/trans.png`, die in regelmäßigen Abständen untersucht wird. Die Untersuchung erfolgt auf jeder Appliance für jede internetfähige WAN-Verbindung. Bei jedem Prüfpunkt wird eine HTTP-Anforderung an den Beacon-Dienst gesendet und eine HTTP-Antwort erwartet. Die HTTP-Antwort bestätigt die Verfügbarkeit und Erreichbarkeit des Office 365-Dienstes.

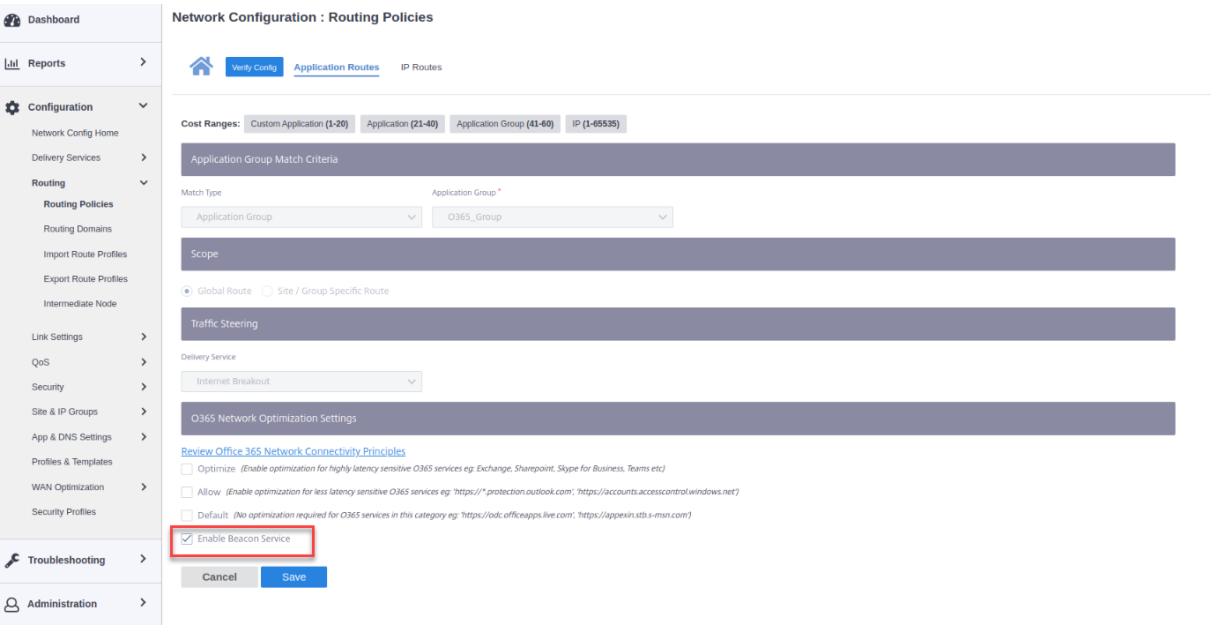
Mit Citrix SD-WAN können Sie nicht nur Beacon-Probing durchführen, sondern auch die Latenz bestimmen, mit der Office 365-Endpunkte über jede WAN-Verbindung erreicht werden. Die Latenz ist die Roundtrip-Zeit, die zum Senden einer Anfrage und zum Abrufen einer Antwort vom Office 365-Beacon-Dienst über eine WAN-Verbindung verwendet wird. Auf diese Weise können Netzwerkadministratoren den Bericht zur Beacon-Service-Latenz anzeigen und den besten Internetlink für den direkten Office 365-Breakout manuell auswählen. Die Beacon-Sondierung ist nur über SD-WAN Orchestrator aktiviert. Standardmäßig ist das Beacon-Probing für alle im Internet aktivierten WAN-Verbindungen aktiviert, wenn Office 365-Breakout über Orchestrator aktiviert ist.

Hinweis

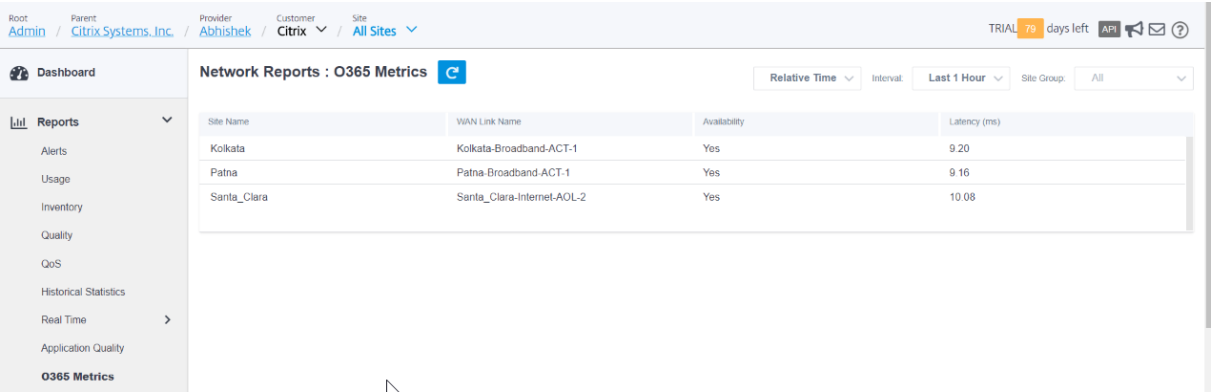
Office 365-Beacon-Probing ist für getaktete Links nicht aktiviert.

Sie können Office 365-Beacon-Probing deaktivieren und Latenzberichte im SD-WAN Orchestrator anzeigen. Weitere Informationen finden Sie unter [Office 365-Optimierung](#).

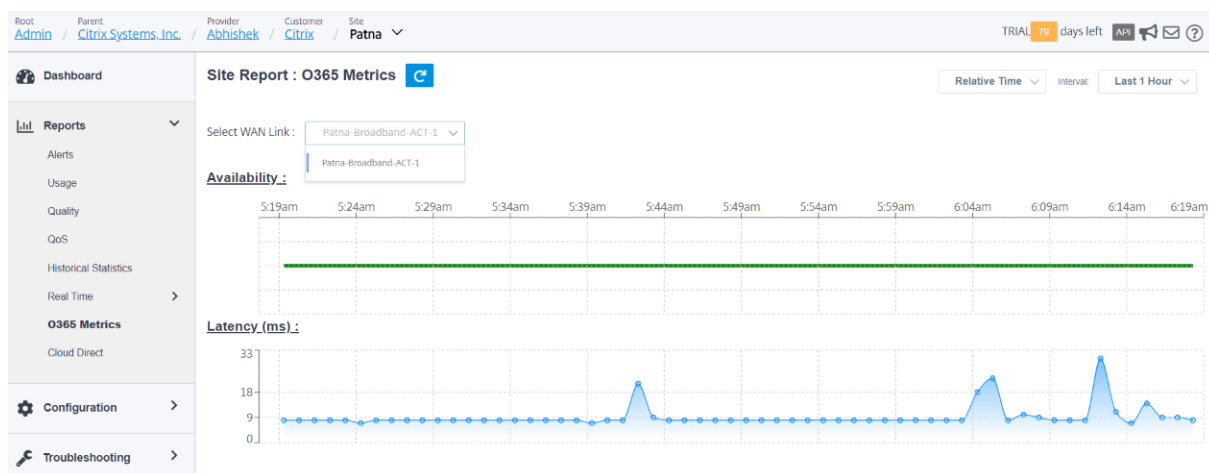
Um den Office 365 Beacon-Dienst zu deaktivieren, navigieren Sie in SD-WAN Orchestrator auf Netzwerkebene zu **Konfiguration > Routing > Routing Policies > O365 Network Optimization Settings** und deaktivieren Sie **Enable Beacon Service**.



Um die Beacon-Sondierungs- und Latenzberichte in SD-WAN Orchestrator auf Netzwerkebene anzuzeigen, navigieren Sie zu **Berichte > O365-Metriken**.



Um einen detaillierten Bericht auf Site-Ebene des Beacon-Service in SD-WAN Orchestrator auf Standortebene anzuzeigen, navigieren Sie zu **Berichte > O365-Metriken**.



Optimierung von Citrix Cloud und Gateway Service

November 16, 2022

Mit der Funktionserweiterung der **Citrix Cloud and Gateway Service-Optimierung** können Sie den für den Citrix Cloud und den Gateway Service bestimmten Datenverkehr erkennen und weiterleiten. Sie können Richtlinien erstellen, um den Datenverkehr entweder direkt ins Internet zu übergeben oder ihn über eine Backhaul-Route über den virtuellen Pfad zu senden. In Ermangelung dieser Funktion wird der Gateway-Dienst, wenn die Standardroute der virtuelle Pfad ist, an das Rechenzentrum des Kunden zurückkehren und dann ins Internet gehen und unnötige Latenz hinzufügen. Darüber hinaus erhalten Sie jetzt Einblick in den Citrix Gateway Service- und den Citrix Cloud-Datenverkehr und können QoS-Richtlinien erstellen, um ihn gegenüber dem virtuellen Pfad zu priorisieren.

Die **Breakout-Funktion für Citrix Cloud and Gateway Service** ist in der Citrix SD-WAN SD-WAN-Softwareversion 11.2.1 und höher standardmäßig aktiviert.

Ab Version 11.2.1 können Sie nun die erste Paketerkennung, Klassifizierung und selektives Routing (direkter Internet-Breakout oder über den virtuellen Pfad) des Datenverkehrs aktivieren, der für Citrix Cloud und Citrix Gateway Service (Steuerung und Daten) bestimmt ist.

Hinweis

- Sie können die Optimierung des Citrix Cloud- und Gateway Service nur über Citrix SD-WAN Orchestrator konfigurieren. Weitere Informationen finden Sie unter [Optimierung des Gateway Service](#).
- Die **Citrix SD-WAN Orchestrator-Verkehrsoptimierung** wird von Citrix SD-WAN SD-WAN-Softwareversion 11.2.3 oder höher eingeführt. Das Ziel besteht darin, eine detail-

liertere Klassifizierung bereitzustellen und somit den Datenverkehr von Citrix SD-WAN Orchestrator-Datenverkehr und den Datenverkehr anderer abhängiger Dienste von Citrix Cloud getrennt zu identifizieren und eine Internet-Breakout-Option bereitzustellen. Infolgedessen können Kunden jetzt nur den Citrix SD-WAN Orchestrator-Datenverkehr optimieren.

Citrix Cloud- und Gateway-Dienst

Im Folgenden sind die Verkehrskategorien aufgeführt, die zu Klassifizierungs- und Optimierungszwecken verwendet werden:

- **Citrix Cloud:** Ermöglicht die Erkennung und Weiterleitung von Datenverkehr, der für Citrix Cloud Web-Benutzeroberfläche und APIs bestimmt ist.
 - Citrix SD-WAN Orchestrator und abhängige kritische Services:
 - * **Citrix SD-WAN Orchestrator:** Ermöglicht direktes Internetbreakout von Heartbeat und anderem Datenverkehr, der zum Aufbau und zur Aufrechterhaltung der Konnektivität zwischen Citrix SD-WAN Appliance und Citrix SD-WAN Orchestrator erforderlich ist.
 - * **Citrix Cloud Download Service:** Ermöglicht den direkten Internet-Breakout zum Herunterladen von Appliance-Software, Konfiguration, Skripts usw. auf die Citrix SD-WAN SD-WAN-Appliance.
- **Citrix Gateway Service:** Aktivieren Sie diese Option, um Datenverkehr (Steuerung und Daten) zu erkennen und zu routen, der für den Citrix Gateway Service bestimmt ist.
 - **Gateway Service Client-Daten:** Ermöglicht direktes Internetbreakout von ICA-Datentunneln zwischen Clients und Citrix Gateway Service. Es erfordert hohe Bandbreite und niedrige Latenz.
 - **Gateway Service Server Data:** Ermöglicht direktes Internetbreakout von ICA-Datentunneln zwischen Virtual Delivery Agents (VDAs) und Citrix Gateway Service. Es erfordert hohe Bandbreite und niedrige Latenz und ist nur relevant für VDA-Ressourcenstandorte (VDA-zu-Citrix Gateway Service-Verbindungen).
 - **Gateway Service Control Traffic:** Ermöglicht direktes Internetbreakout des Steuerungsverkehrs. Keine spezifischen QoS-Überlegungen.
 - **Gateway Service Web Proxy Traffic:** Ermöglicht direktes Internetbreakout des Web-Proxydatenverkehrs. Es erfordert eine hohe Bandbreite, aber die Latenzanforderungen können variieren.

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

| Proxy Name | Application Name | DNS Service Name | DNS Service Active | Hits |
|------------|-------------------------|------------------|--------------------|-------|
| Default | office365_optimize | Quad9 | YES | 0 |
| Default | citrix_cloud_web_ui_api | Quad9 | YES | 4 |
| Default | ngs_client_data | Quad9 | YES | 14 |
| Default | ngs_server_data | Quad9 | YES | 0 |
| Default | ngs_control_traffic | Quad9 | YES | 2286 |
| Default | ngs_web_proxy | Quad9 | YES | 0 |
| Default | Any | azureDNS | YES | 51490 |

Showing 1 to 7 of 7 entries

Transparent Forwarder Statistics

Search:

| Application Name | DNS Service Name | DNS Service Active | Hits |
|-------------------------|------------------|--------------------|------|
| citrix_cloud_web_ui_api | Quad9 | YES | 0 |
| ngs_client_data | Quad9 | YES | 0 |
| ngs_control_traffic | Quad9 | YES | 0 |
| ngs_server_data | Quad9 | YES | 0 |
| ngs_web_proxy | Quad9 | YES | 0 |
| office365_optimize | Quad9 | YES | 0 |

Showing 1 to 6 of 6 entries

Transparent Forwarder Statistics

Search:

| Application Name | DNS Service Name | DNS Service Active | Hits |
|---------------------------|------------------|--------------------|------|
| citrix_cloud_download_svc | Quad9 | YES | 1 |
| citrix_sdwan_orchestrator | Quad9 | YES | 1 |

Showing 1 to 2 of 2 entries

• Anwendungs-Routenstatistiken

Monitoring > Statistics

Statistics

Show: Application Routes ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 6 of 6 entries

| Num | Application Object | Gateway IP Address | Service | Firewall Zone | Reachable | Site | Type | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|-------------------------------|--------------------|----------|------------------------|-----------|---------|--------|------|-----------|----------|------------------|-------------------|
| 0 | O365Optimize_InternetBreakout | * | Internet | Untrusted_Internet_Zon | YES | azure07 | Static | 50 | 7 | YES | N/A | N/A |
| 1 | NGS_WebProxy_Breakout | * | Internet | Untrusted_Internet_Zon | YES | azure07 | Static | 50 | 0 | YES | N/A | N/A |
| 2 | NGS_ServerData_Breakout | * | Internet | Untrusted_Internet_Zon | YES | azure07 | Static | 50 | 44 | YES | N/A | N/A |
| 3 | NGS_ControlTraffic_Breakout | * | Internet | Untrusted_Internet_Zon | YES | azure07 | Static | 50 | 72 | YES | N/A | N/A |
| 4 | NGS_ClientData_Breakout | * | Internet | Untrusted_Internet_Zon | YES | azure07 | Static | 50 | 0 | YES | N/A | N/A |
| 5 | CitrixCloud_Breakout | * | Internet | Untrusted_Internet_Zon | YES | azure07 | Static | 50 | 0 | YES | N/A | N/A |

Showing 1 to 6 of 6 entries

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show entries Showing 1 to 2 of 2 entries

| Num | Application Object | Gateway IP Address | Service | Firewall Zone | Reachable | Site | Type | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|----------------------------------|--------------------|----------|---------------|-----------|----------------|--------|------|-----------|----------|------------------|-------------------|
| 0 | CitrixSdwanOrchestrator_Breakout | * | Internet | Internet_Zone | YES | BRANCH1_KVMVPX | Static | 50 | 35 | YES | N/A | N/A |
| 1 | CitrixCloudDownloadSvc_Breakout | * | Internet | Internet_Zone | YES | BRANCH1_KVMVPX | Static | 50 | 8 | YES | N/A | N/A |

Showing 1 to 2 of 2 entries

Problembehandlung

Sie können den Dienstfehler im Abschnitt **Ereignisse** der SD-WAN-Appliance anzeigen.

Um die Fehler zu überprüfen, navigieren Sie zu **Konfiguration > Systemwartung > Diagnose**, und klicken Sie auf die Registerkarte **Ereignisse**.

Dashboard

Monitoring

Configuration

+ Appliance Settings

+ Virtual WAN

System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics**
- Update Software
- Configuration Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostics Data

Events

Alarms

Diagnostics Tool

Site Diagnostics

Insert Event

Object Type:

Event type:

Severity:

Wenn bei der Verbindung mit dem Citrix Dienst ein Problem auftritt (sdwan-app-routing.citrixnetworkapi.net), wird die Fehlermeldung in der Tabelle **Ereignisse anzeigen** angezeigt.

View Events

Quantity:

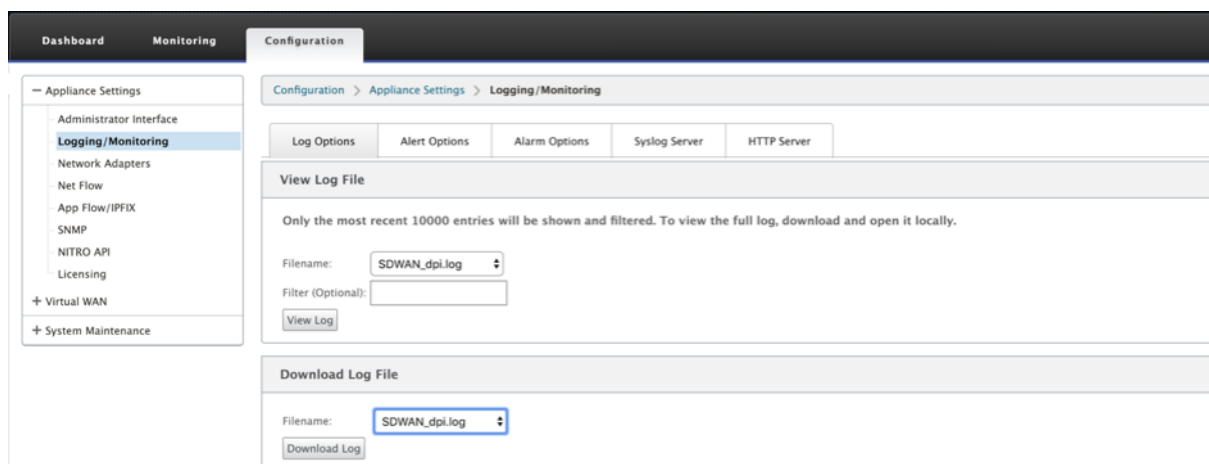
Filter: Object Type = Event type = Severity =

| ID | Object ID | Object Name | Object Type | Time | Event Type | Severity | Description |
|-------|-----------|------------------|--------------|---------------------|------------|----------|--------------------------------------|
| 13839 | 26 | Endpoints Update | APPLICATIONS | 2019-02-12 09:02:15 | FAILURE | ERROR | Failed to connect to the service API |

Times are in UTC

Die Verbindungsfehler werden auch in **SDWAN_DPI.log protokolliert**. Um das Protokoll anzuzeigen, navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Logging/Überwachung > Log-Optionen**. Wählen Sie die SDWAN_dpi.log aus der Dropdown-Liste aus und klicken Sie auf **Protokoll anzeigen**.

Sie können die Protokolldatei auch herunterladen. Um die Protokolldatei herunterzuladen, wählen Sie die erforderliche Protokolldatei aus der Dropdown-Liste unter dem Abschnitt **Protokolldatei herunterladen** aus und klicken Sie auf **Protokoll herunterladen**.



Citrix SD-WAN Orchestrator für die lokale Konfiguration auf der Citrix SD-WAN-Appliance

November 16, 2022

Citrix SD-WAN Orchestrator for On-Premises ist die lokale Softwareversion des Citrix SD-WAN Orchestrator Service Orchestrator-Dienstes. Citrix SD-WAN Orchestrator for On-Premises bietet Citrix Partnern eine Einscheiben-Glas-Management-Plattform, mit der sie mehrere Kunden zentral verwalten können, mit geeigneten rollenbasierten Zugriffskontrollen.

Sie können eine Verbindung zwischen Ihrer Citrix SD-WAN-Appliance und dem Citrix SD-WAN Orchestrator für lokale Standorte herstellen, indem Sie Orchestrator-Konnektivität aktivieren und den Citrix SD-WAN Orchestrator für lokale Identität angeben.

Hinweis

- Cloud Orchestrator Zero-Touch-Bereitstellung funktioniert nicht, wenn die **lokale SD-WAN Orchestrator-Konfiguration auf der SD-WAN-Appliance-Funktion** auf den SD-WAN-Appliances konfiguriert ist.
- Citrix SD-WAN Orchestrator für lokal auf der SD-WAN-Appliance geht verloren, wenn der Citrix SD-WAN Orchestrator für die lokale Konfiguration auf der SD-WAN-Appliance, die in Citrix SD-WAN Version 11.3.0 konfiguriert ist, auf Version 10.2.7 heruntergestuft wird. Ein Downgrade von Version 11.3.0 auf Version 10.2.7 wird nicht unterstützt. Die Problemlösung besteht darin, den Citrix SD-WAN Orchestrator für die lokale Identität nach dem Downgrade neu zu konfigurieren.
- Nach dem Downgrade der SD-WAN-Appliance von 11.3.0 auf 11.1.1/11.2.0/10.2.7 Softwareversion müssen Sie erneut Identitätseinstellungen auf der Benutzeroberfläche der Citrix SD-

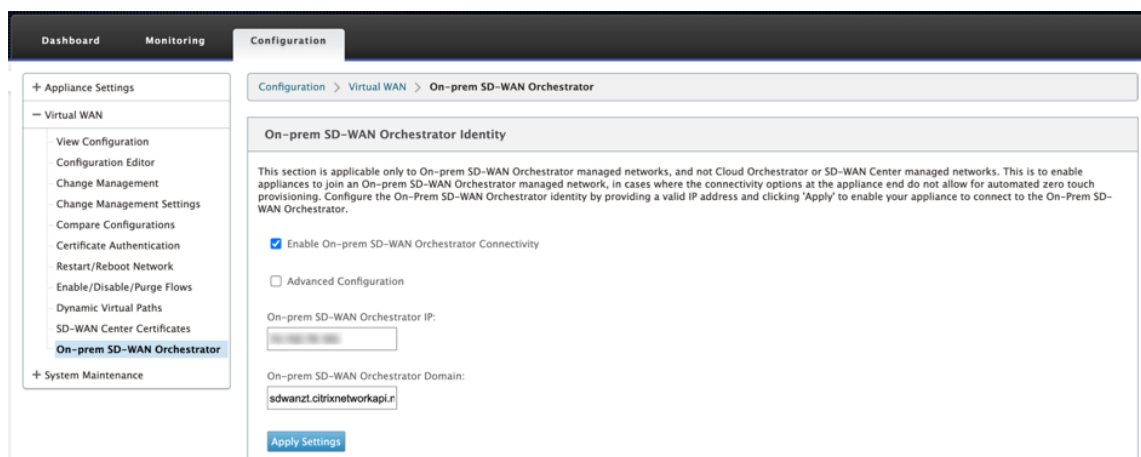
WAN Appliance anwenden. Wenn Probleme im Zusammenhang mit dem Citrix SD-WAN Orchestrator für die lokale Konfiguration oder die SD-WAN-Appliance-Konnektivität auftreten, deaktivieren Sie den Citrix SD-WAN Orchestrator für lokale Konnektivität und aktivieren Sie dann den Citrix SD-WAN Orchestrator erneut für lokale Konnektivität.

So aktivieren Sie Citrix SD-WAN Orchestrator für lokale Konnektivität ab Version Citrix SD-WAN 11.2.1:

1. Navigieren Sie in der Appliance-Benutzeroberfläche zu **Konfiguration > Virtual WAN > On-prem SD-WAN Orchestrator**.
2. **Aktivieren Sie das Kontrollkästchen On-Prem SD-WAN Orchestrator-Konnektivität** aktivieren.

Hinweis

Ab Version von Citrix SD-WAN 11.2.1 werden die Optionen **SD-WAN Appliance** und **On-prem SD-WAN Orchestrator-Zertifikate**, **On-prem SD-WAN Orchestrator-Domain**, **Authentication Type** und **Advanced Configuration** eingeführt.



3. Geben Sie entweder den Citrix SD-WAN Orchestrator für lokale IP-Adresse oder Domäne oder beides (IP-Adresse und Domäne) für die Konfiguration ein.

Wenn der Kunde nur Domäne konfiguriert, muss er sicherstellen, dass DNS-Eintrag in seinem lokalen DNS-Server hinzugefügt wird, und die DNS-Server-IP-Adresse auf SD-WAN-Appliances konfigurieren. Um zu konfigurieren, navigieren Sie zu **Konfiguration > Netzwerkadapter > IP-Adresse**.

Wenn beispielsweise der Citrix SD-WAN Orchestrator für die lokale Domäne als **citrix.com** konfiguriert ist. Dann müssen Sie im DNS-Server einen DNS-Eintrag für den folgenden FQDN und Citrix SD-WAN Orchestrator für die lokale IP-Adresse erstellen:

- download.citrix.com

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

In erweiterter Konfiguration:

Beispiel: Wenn der Citrix SD-WAN Orchestrator für die lokale Domäne als **citrix.com** konfiguriert ist, wird die Download-Verwaltungsdienstdomäne als **download.citrix.com** konfiguriert, und die Statistikverwaltungsdienstdomäne ist als **statistics.citrix.com** konfiguriert, dann müssen Sie eine DNS-Eintrag im DNS-Server für den folgenden FQDN und die entsprechende IP-Adresse:

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

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN Orchestrator interface. The left sidebar lists various configuration options, with 'On-prem SD-WAN Orchestrator' selected. The main content area is titled 'On-prem SD-WAN Orchestrator Identity' and contains the following fields and options:

- On-prem SD-WAN Orchestrator Identity**
 - ☒ Enable On-prem SD-WAN Orchestrator Connectivity
 - ☒ Advanced Configuration
 - On-prem SD-WAN Orchestrator IP: [Text Field]
 - Download Management Service IP: [Text Field]
 - Statistics Management Service IP: [Text Field]
 - On-prem SD-WAN Orchestrator Domain: sdwanzt.citrixnetworkapi.com
 - Download Management Service Domain: [Text Field]
 - Statistics Management Service Domain: [Text Field]
 - [Apply Settings](#)
- Authentication Type**
 - No Authentication**: No Authentication between On-prem SD-WAN Orchestrator and SD-WAN Appliance. Customer can use this option if they have already secure network. For eg: MPLS
 - One-way Authentication**: SD-WAN Appliance will authenticate On-prem SD-WAN Orchestrator. On-prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance.
 - Two-way Authentication**: On-prem SD-WAN Orchestrator and SD-WAN Appliance authenticates each other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.
 - Authentication Type: **No Authentication** (Dropdown)
 - [Apply](#)

Citrix SD-WAN Orchestrator für On-Premises unterstützt möglicherweise das Ausführen von Diensten wie Download, Statistiken auf einer unabhängigen Serverinstanz, um eine bessere Skalierbarkeit für große Netzwerke zu ermöglichen. Sie können die **erweiterte Konfiguration** auswählen und den **Download-Verwaltungsdienst** und den **Statistik-Verwaltungsdienst** konfigurieren.

Aktivieren Sie das Kontrollkästchen **Erweiterte Konfiguration** und geben Sie die folgenden Details an:

- **Download Management Service IP/Domain:** Geben Sie die IP-Adresse /domäne an, mit der Sie SD-WAN-Software und Konfigurationsdownloadaspekte auf eine unabhängige Serverinstanz auslagern können, um eine bessere Skalierbarkeit für große Netzwerke zu ermöglichen.

- **Statistic Management Service IP/Domäne:** Stellen Sie die IP-Adresse/Domäne bereit, die die Erfassung und Verwaltung von SD-WAN-Statistiken von Geräten auf eine unabhängige Serverinstanz auslagert, um eine bessere Skalierbarkeit für große Netzwerke zu ermöglichen.
4. Wählen Sie den **Authentifizierungstyp** Im Folgenden sind die Authentifizierungstypen aufgeführt, die zwischen der SD-WAN-Appliance und dem Citrix SD-WAN Orchestrator für lokale Konnektivität unterstützt werden:
- **Keine Authentifizierung** —Keine Authentifizierung zwischen dem Citrix SD-WAN Orchestrator für lokale und der SD-WAN-Appliance, und es ist nicht erforderlich, die **SD-WAN-Appliance** oder das **lokale SD-WAN Orchestrator-Zertifikat** zu verwenden. Sie können diese Option jedoch verwenden, wenn Sie über ein sicheres Netzwerk wie MPLS verfügen.
 - **Einweg-Authentifizierung** —Bei Auswahl des **Einweg-Authentifizierungstyps** müssen Sie den Citrix SD-WAN Orchestrator für das lokale Zertifikat hochladen. Laden Sie das Zertifikat vom Citrix SD-WAN Orchestrator für lokal herunter und klicken Sie auf **Hochladen**. Die SD-WAN-Appliance vertraut dem Citrix SD-WAN Orchestrator für die lokale Verwendung der hochgeladenen Zertifikate.
 - **Zwei-Wege-Authentifizierung** —Citrix SD-WAN Orchestrator für lokale und Appliance-Zertifikate müssen miteinander ausgetauscht werden. Für die **bidirektionale Authentifizierung** müssen Sie das SD-WAN-Appliance-Zertifikat auf dem Citrix SD-WAN Orchestrator für lokal neu generieren, herunterladen und hochladen. SD-WAN-Appliance und Citrix SD-WAN Orchestrator für On-Premises vertrauen einander mithilfe der ausgetauschten Zertifikate.

Hinweis

Es wird empfohlen, nur Unidirektionale Authentifizierung oder Zwei-Wege-Authentifizierung zu verwenden. Stellen Sie im Falle von No Authentication sicher, dass der DNS vor DNS-Angriffen geschützt ist.

Wenn der Citrix SD-WAN Orchestrator für den lokalen **Authentifizierungstyp** deaktiviert ist, kann die Appliance entweder über **Keine Authentifizierung** oder **Einweg-Authentifizierung** oder **Zweiwege-Authentifizierung** oder **Zweiwege-Authentifizierung**** eine Verbindung zum Citrix SD-WAN Orchestrator herstellen.

Wenn der Citrix SD-WAN Orchestrator für den lokalen **Authentifizierungstyp** aktiviert ist, kann die Appliance nur eine Verbindung zum Citrix SD-WAN Orchestrator für lokale **Authentifizierung** herstellen.

Beim Deaktivieren des **Authentifizierungstyps** in Citrix SD-WAN Orchestrator für On-Premises aus dem Aktivierungsstatus wechseln vorhandene Appliances im Einweg-Authentifizierungsmodus

in den Status “Getrennt”. Kunden müssen den Authentifizierungstyp der Appliance in Zwei-Wege-Authentifizierung ändern und das SD-WAN-Appliance-Zertifikat auf den Citrix SD-WAN Orchestrator hochladen, damit es verbunden wird.

Hinweis

- Generierte Zertifikate sind selbstsignierte X509-Zertifikate.
- Der Kunde muss die Zertifikate neu generieren, wenn das Zertifikat abgelaufen oder gefährdet ist.
- Die Gültigkeit des Zertifikats beträgt 10 Jahre.
- Sie können die Zertifikatdetails wie Fingerabdruck, Startdatum und Enddatum anzeigen
- Der Kunde muss sicherstellen, dass die Zertifikate neu generiert und zwischen Citrix SD-WAN Orchestrator für lokale und SD-WAN-Appliance ausgetauscht werden, um den Verlust der Appliance-Konnektivität mit Citrix SD-WAN Orchestrator für lokale Standorte zu vermeiden.

Authentication Type

No Authentication : No Authentication between On-prem SD-WAN Orchestrator and SD-WAN Appliance. Customer can use this option if they have already secure network. For eg: MPLS
One-way Authentication : SD-WAN Appliance will authenticate On-prem SD-WAN Orchestrator. On-prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance.
Two-way Authentication : On-prem SD-WAN Orchestrator and SD-WAN Appliance authenticates each other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.

Authentication Type **Two-way Authentication** ▼

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Filename: **Choose file** No file chosen **Upload**

Certificate Details

Certificate Fingerprint: 75:38:C2:32:AC:07:6E:26:6C:D9:C6:08:73:A2:73:8D:81:91:5A:4C
Start Date: Jul 22 11:26:32 2020 GMT
End Date: Jul 20 11:26:32 2030 GMT

SD-WAN Appliance Certificate

Certificate Details

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

Regenerate **Download**

5. Klicken Sie auf **Einstellungen anwenden**.

Um den Citrix SD-WAN Orchestrator für lokale Konnektivität zu deaktivieren, **deaktivieren Sie die Option On-Prem SD-WAN Orchestrator-Konnektivität** aktivieren und klicken Sie auf **Einstellungen anwenden**. Um Citrix SD-WAN Orchestrator für ein lokal verwaltetes Netzwerk entweder in Cloud Orchestrator oder MCN Managed Network zu konvertieren, müssen Sie Citrix SD-WAN Orchestrator

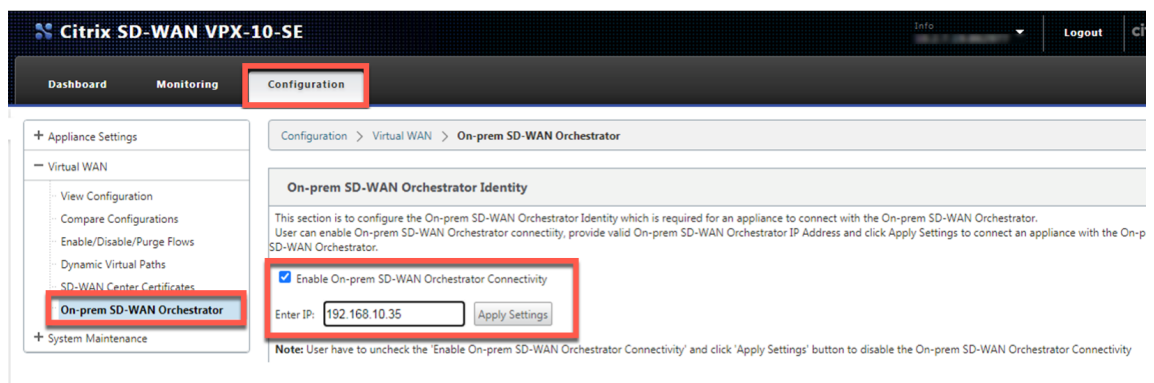
für lokale Konnektivität deaktivieren und das Zurücksetzen der Konfiguration durchführen. Um die Konfiguration zurückzusetzen, navigieren Sie zu **Konfiguration > Systemwartung > Configuration Reset**.

Bereitstellen von Citrix SD-WAN Appliances, die auf Softwareversionen 10.2.7, 11.1.1 oder 11.2.0 ausgeführt werden, mit Citrix SD-WAN Orchestrator für lokale Anwendungen

HINWEIS

Um Citrix SD-WAN Appliances mit den Softwareversionen 10.2.7, 11.1.1 oder 11.2.0 bereitzustellen, benötigen Sie Citrix SD-WAN Orchestrator für die lokale Version 11.1 oder höher.

1. Melden Sie sich für jede Citrix SD-WAN-Appliance mit Softwareversion 10.2.7, 11.1.1 oder 11.2.0 bei der Appliance-Weboberfläche an und führen Sie Folgendes aus:
 - a) Navigieren Sie zu **Konfiguration > Virtual WAN > On-Prem SD-WAN Orchestrator** und **aktivieren Sie das Kontrollkästchen On-Prem SD-WAN Orchestrator-Konnektivität** aktivieren.
 - b) Geben Sie die IP-Adresse von Citrix SD-WAN Orchestrator für lokal ein.
 - c) Klicken Sie auf **Einstellungen anwenden**.



2. Melden Sie sich bei Citrix SD-WAN Orchestrator für die lokale Benutzeroberfläche an. Erstellen Sie eine Site und erstellen Sie die Konfiguration. Geben Sie die Seriennummer jeder Citrix SD-WAN-Appliance in der jeweiligen Site-Konfiguration ein. Speichern Sie die Konfiguration.

Network Configuration: Home

Site Group: All

Software Version:

+ Add Site

Batch Add Sites

Deploy Config/Software

Back Up/Review Checkpoints

More Actions ...

Search

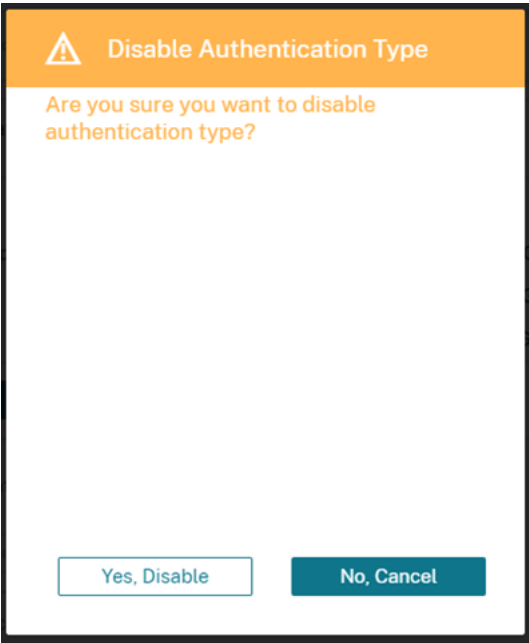
| Availability | Orchestrator Connectivity | Site Name | Site Role | Device Model | Serial No | Bandwidth Tier | Actions |
|--------------|---------------------------|-----------|-----------|--------------|-----------|----------------|-------------------------------------|
| | Offline | NYC | MCN | VPX-SE | | 50 | <div></div> <div></div> <div></div> |
| | Offline | LON | Branch | VPX-SE | | 50 | <div></div> <div></div> <div></div> |

Page Size: 50

Showing 1-2 of 2 items

Page 1 of 1

3. Navigieren Sie zu **Administration > Zertifikatauthentifizierung** und schalten Sie den Schalter **Authentifizierungstyp** auf **AUS**. Klicken Sie auf **Ja, Deaktivieren**, um das Pop-up “**Deaktivierter Authentifizierungstyp**“



Network Administration: Certificate Authentication

Disabled authentication type successfully.

Authentication Type

On-prem Orchestrator Certificate

Certificate Details:

Certificate Fingerprint:
Start Date:
End Date:

[REDACTED]

July 13 05:57:34 2021 GMT
July 11 05:57:34 2031 GMT

Regenerate

Download

Appliance Certificate

Select an appliance ▾

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

Upload

4. Auf der **Homepage Konfiguration > Netzwerkkonfiguration** werden SD-WAN-Appliances in der Spalte **Cloud-Konnektivität** als **Online** angezeigt. Dies ist auf die deaktivierte Zertifikatauthentifizierung auf Citrix SD-WAN Orchestrator für lokale und SD-WAN-Appliances zurückzuführen, die für Citrix SD-WAN Orchestrator für lokale Konnektivität mit der entsprechenden IP-Adresse aktiviert sind. Warten Sie ein paar Minuten, bis die Geräte als Online gemeldet werden.

Network Configuration: Home

Site Group: All

Software Version :

+ Add Site
Batch Add Sites
Deploy Config/Software
Back Up/Review Checkpoints
More Actions ...

Search

| Availability | Orchestrator Connectivity | Site Name | Site Role | Device Model | Serial No | Bandwidth Tier | Actions |
|--------------|---------------------------|-----------|-----------|--------------|--------------------------------------|----------------|---------|
| | Online | NYC | MCN | VPX-SE | XXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX | 50 | |
| | Online | LON | Branch | VPX-SE | XXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX | 50 | |

Page Size: 50
 Showing 1-2 of 2 items
 Page 1 of 1

5. Wählen Sie eine veröffentlichte Softwareversion (11.3.0 oder höher) aus und klicken Sie auf **Konfiguration/Software bereitstellen**. Weitere Einzelheiten zur Auswahl der veröffentlichten Softwareversion finden Sie unter [Software](#). **Stage** und **Activate** der Sites. Nach der Aktivierung zeigen die Geräte in der Spalte **Online** die Option **Nein** an.

Verify Config

Current Deployment

Deployment History

Change Management Settings

Site Details

Software Version : 11.3.2.25

Stage

✓

Activate

☐ Ignore Incomplete

2/2

Staged Appliances

0/2

Activated Appliances

| Total Appliances | Ready For Activation | Activated | Failed | Offline |
|------------------|----------------------|-----------|--------|---------|
| 2 | 2 | 0 | 0 | 0 |

Search

| Online | Site | Status | HA State | Software Version | Actions |
|--------|------|------------------------|----------|------------------|---------|
| No | NYC | Activation In Progress | Unknown | 10.2.719.862977 | |
| No | LON | Activation In Progress | Unknown | 10.2.719.862977 | |

Page Size: 50

Showing 1-2 of 2 items

Page 1 of 1

6. Navigieren Sie zu **Administration > ZTD-Einstellungen > Non-Cloud ZTD**. Klicken Sie auf **+Site** und fügen Sie eine Site hinzu. Geben Sie die Management-IP und die Anmeldeinformationen für jede Appliance ein. Klicken Sie auf **+**, um weitere Websites hinzuzufügen. Klicken Sie auf **Hinzufügen**.

Network Administration: ZTD Settings

[Non-Cloud ZTD](#) [Cloud Brokered ZTD \(Preview\)](#)



- Non-Cloud ZTD Settings helps to configure On-prem SD-WAN Orchestrator Information on SD-WAN Appliances running 11.3.0 and above releases.
- Multiple sites can also be added by importing a .csv file with all the site details. [Click here](#) to download a sample .csv file.

Add Sites

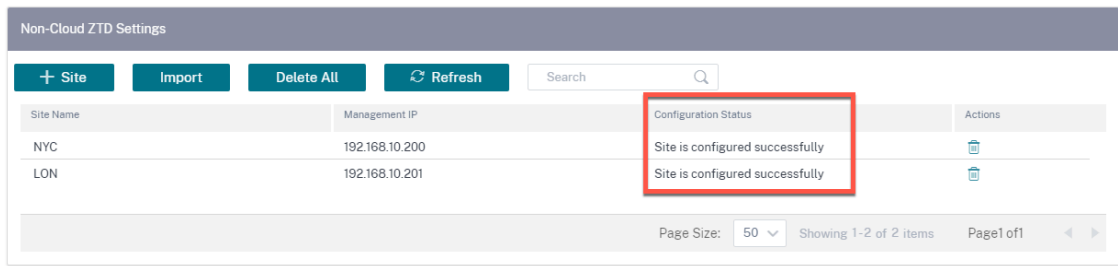
| Site Name | Management IP | Username | Freshly Provisioned | Password | New Password | |
|-----------|----------------|----------|--------------------------|----------|--------------|-------------------------------------|
| NYC | 192.168.10.200 | admin | <input type="checkbox"/> | ***** | | — |
| LON | 192.168.10.201 | admin | <input type="checkbox"/> | ***** | New password | <div><div>+</div><div>—</div></div> |

Add

Cancel

7. Klicken Sie auf **Aktualisieren**, um den Konfigurationsstatus zu überwachen. Wenn die Site erfolgreich konfiguriert wurde, wird in der Spalte **“Konfigurationsstatus”** angezeigt, dass Standort

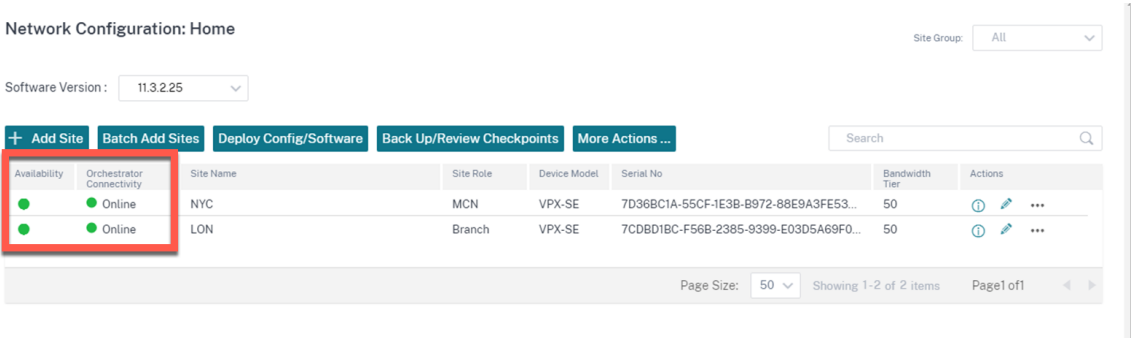
erfolgreich konfiguriert wurde.



The screenshot shows the 'Non-Cloud ZTD Settings' interface. It includes buttons for '+ Site', 'Import', 'Delete All', and 'Refresh', along with a search bar. A table lists two sites: NYC and LON, with their respective Management IPs (192.168.10.200 and 192.168.10.201). A red box highlights the 'Configuration Status' column, which shows 'Site is configured successfully' for both sites. The bottom of the interface shows 'Page Size: 50', 'Showing 1-2 of 2 items', and 'Page 1 of 1'.

| Site Name | Management IP | Configuration Status | Actions |
|-----------|----------------|---------------------------------|---------|
| NYC | 192.168.10.200 | Site is configured successfully | |
| LON | 192.168.10.201 | Site is configured successfully | |

8. Navigieren Sie zu **Homepage Configuration > Network Config**. Erfolgreich konfigurierte Sites werden in der Spalte **Orchestrator-Konnektivität** als **Online** angezeigt.



The screenshot shows the 'Network Configuration: Home' page. It includes a 'Software Version' dropdown set to '11.3.2.25' and a 'Site Group' dropdown set to 'All'. Below these are buttons for '+ Add Site', 'Batch Add Sites', 'Deploy Config/Software', 'Back Up/Review Checkpoints', and 'More Actions ...'. A table lists two sites: NYC and LON, with their respective Site Roles (MCN and Branch), Device Models (VPX-SE), Serial Numbers, and Bandwidths (50). A red box highlights the 'Availability' and 'Orchestrator Connectivity' columns, which show 'Online' for both sites. The bottom of the interface shows 'Page Size: 50', 'Showing 1-2 of 2 items', and 'Page 1 of 1'.

| Availability | Orchestrator Connectivity | Site Name | Site Role | Device Model | Serial No | Bandwidth Tier | Actions |
|--------------|---------------------------|-----------|-----------|--------------|---------------------------------------|----------------|---------|
| Online | Online | NYC | MCN | VPX-SE | 7D36BC1A-55CF-1E3B-B972-88E9A3FE53... | 50 | |
| Online | Online | LON | Branch | VPX-SE | 7CDBD1BC-F56B-2385-9399-E03D5A69F0... | 50 | |

9. Gehen Sie genauso vor, um zusätzliche Websites hinzuzufügen. Die Durchführung der vorangegangenen Schritte hat keine Auswirkungen auf bestehende Standortbereitstellungen.

PPPoE-Sitzungen

May 10, 2021

Point-to-Point-Protokoll über Ethernet (PPPoE) verbindet mehrere Computerbenutzer in einem lokalen Ethernet-Netzwerk mit einem Remote-Standort, z. B. Citrix SD-WAN. PPPoE ermöglicht Benutzern, eine gemeinsame DSL (Digital Subscriber Line), ein Kabelmodem oder eine drahtlose Verbindung zum Internet freizugeben. PPPoE kombiniert das Point-to-Point-Protokoll (PPP), das häufig in DFÜ-Verbindungen verwendet wird, mit dem Ethernet-Protokoll, das mehrere Benutzer in einem lokalen Netzwerk unterstützt. Die PPP-Protokollinformationen sind in einem Ethernet-Frame gekapselt.

Citrix SD-WAN-Appliances verwenden PPPoE zur Unterstützung von Internetdiensteanbietern (Internet Service Provider, ISP), um fortlaufende und kontinuierliche DSL- und Kabelmodemverbindungen im Gegensatz zu DFÜ-Verbindungen zu haben. PPPoE bietet jede Benutzer-Remote-Standortsitzung, um die Netzwerkadressen des anderen durch einen anfänglichen Austausch namens Discovery zu lernen. Nachdem eine Sitzung zwischen einem einzelnen Benutzer und dem Remote-Standort, z. B. einem

ISP-Provider, eingerichtet wurde, kann die Sitzung überwacht werden. Unternehmen nutzen gemeinsam genutzten Internetzugang über DSL-Leitungen über Ethernet und PPPoE.

Citrix SD-WAN fungiert als PPPoE-Client. Es authentifiziert sich beim PPPoE-Server und erhält dynamische IP-Adresse oder verwendet statische IP-Adresse, um PPPoE-Verbindungen herzustellen.

Zum Aufbau erfolgreicher PPPoE-Sitzungen ist Folgendes erforderlich:

- Konfigurieren Sie die virtuelle Netzwerkschnittstelle (VNI).
- Eindeutige Anmeldeinformationen zum Erstellen von PPPoE-Sitzungen.
- WAN-Link konfigurieren. Für jede VNI kann nur eine WAN-Verbindung konfiguriert werden.
- Konfigurieren Sie die virtuelle IP-Adresse. Jede Sitzung erhält eine eindeutige IP-Adresse, dynamisch oder statisch, basierend auf der bereitgestellten Konfiguration.
- Stellen Sie die Appliance im Bridge-Modus bereit, um PPPoE mit statischer IP-Adresse zu verwenden, und konfigurieren Sie die Schnittstelle als “vertrauenswürdig”.
- Statische IP wird bevorzugt, eine Konfiguration zu haben, um die vorgeschlagene IP-Adresse des Servers zu erzwingen; wenn sie sich von der konfigurierten statischen IP unterscheidet, kann andernfalls ein Fehler auftreten.
- Stellen Sie die Appliance als Edge-Gerät bereit, um PPPoE mit dynamischer IP zu verwenden, und konfigurieren Sie die Schnittstelle als “nicht vertrauenswürdig”.
- Unterstützte Authentifizierungsprotokolle sind PAP, CHAP, EAP-MD5, EAP-SRP.
- Die maximale Anzahl mehrerer Sitzungen hängt von der Anzahl der konfigurierten VNIs ab.
- Erstellen Sie mehrere VNIs zur Unterstützung mehrerer PPPoE-Sitzungen pro Schnittstellen-Gruppe.

Hinweis:

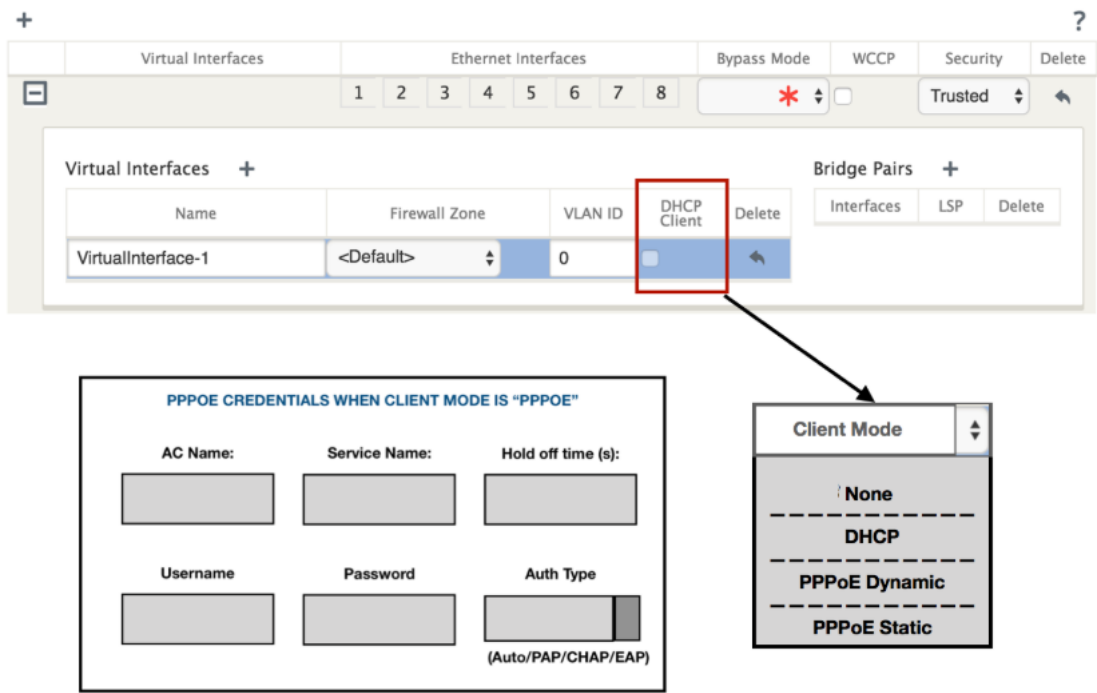
Mehrere VNIs können mit demselben 802.1Q-VLAN-Tag erstellt werden.

Einschränkungen für die PPPoE-Konfiguration:

- 802.1q VLAN-Tagging wird nicht unterstützt.
- Die EAP-TLS-Authentifizierung wird nicht unterstützt.
- Adresse/Kontrollieren Sie die Komprimierung.
- Deflate Kompression.
- Protokollfeldkomprimierung Verhandlung.
- Kompressionssteuerungsprotokoll.
- BSD Kompressionskompression.
- IPv6- und IPX-Protokolle.
- PPP Multi Link.

- Van Jacobson Stil TCP/IP Header Kompression.
- Verbindungs-ID-Komprimierungsoption in Van Jacobson-Stil TCP/IP-Header-Komprimierung.
- PPPoE wird auf LTE-Schnittstellen nicht unterstützt

Um die PPPoE-Konfiguration zu erleichtern, wird die **DHCP-Client-Option** durch eine neue Option namens **Clientmodus** in der SD-WAN-Webverwaltungsschnittstelle unter **Standortkonfiguration** ersetzt.



In der folgenden Tabelle werden die PPPoE-Konfigurationsoptionen für Clientmodus beschrieben, die auf einer MCN- bzw. Zweig-SD-WAN-Appliance verfügbar sind.

MCN

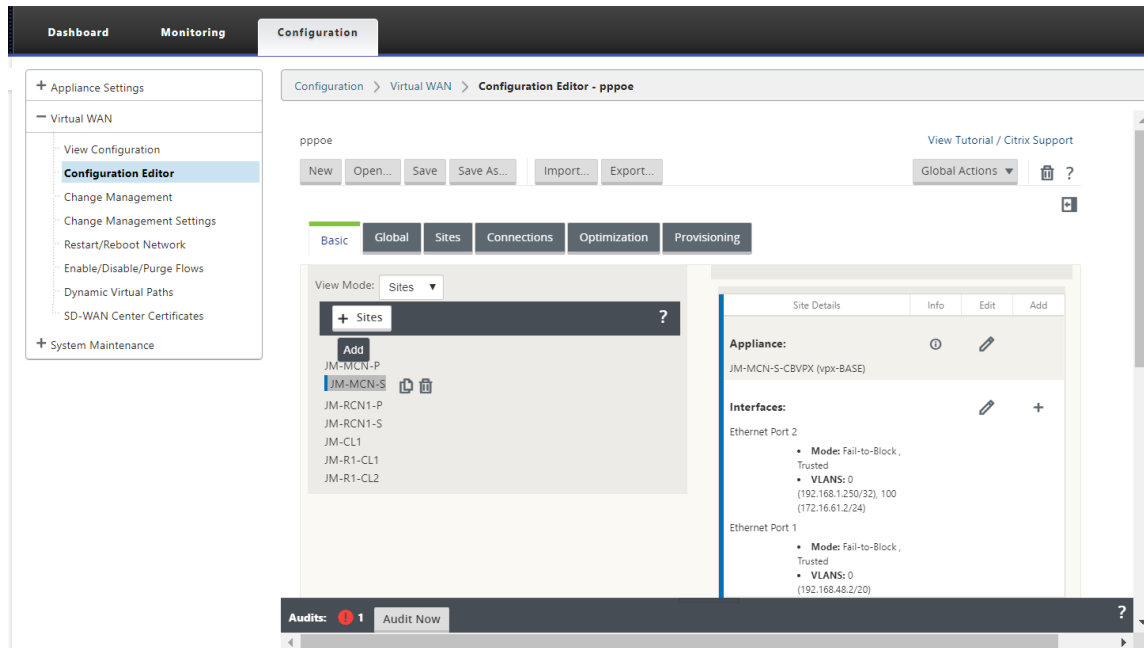
- Ohne
- PPPoE Static

Zweig

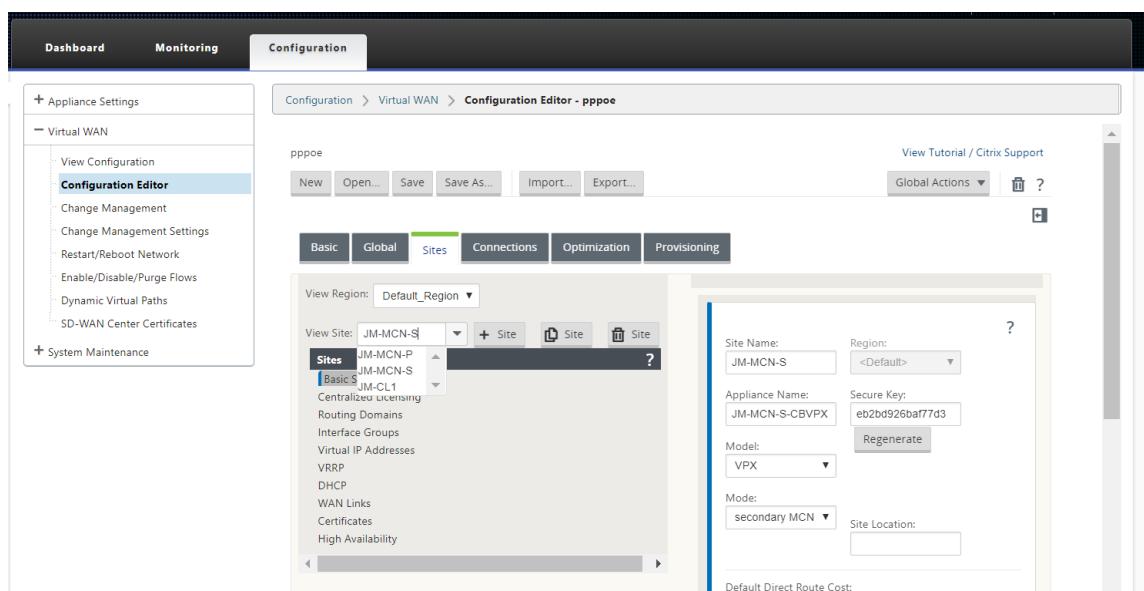
- Ohne
- PPPoE Static
- PPPoE Dynamisch
- DHCP

MCN-Appliance konfigurieren

1. Navigieren Sie in der Benutzeroberfläche der SD-WAN MCN-Appliance zu **Konfiguration** > **Virtuelles WAN** > **Konfigurations-Editor** . Fügen Sie die Website unter der Registerkarte **Basic** hinzu. Weitere Informationen finden Sie in der Konfiguration des Zweigknotens unter, [MCN konfigurieren](#).



2. Öffnen Sie nach dem Erstellen der neuen Website die Registerkarte **Sites** . Wählen Sie die neu erstellte Website aus der Dropdown-Liste **Site anzeigen** aus.

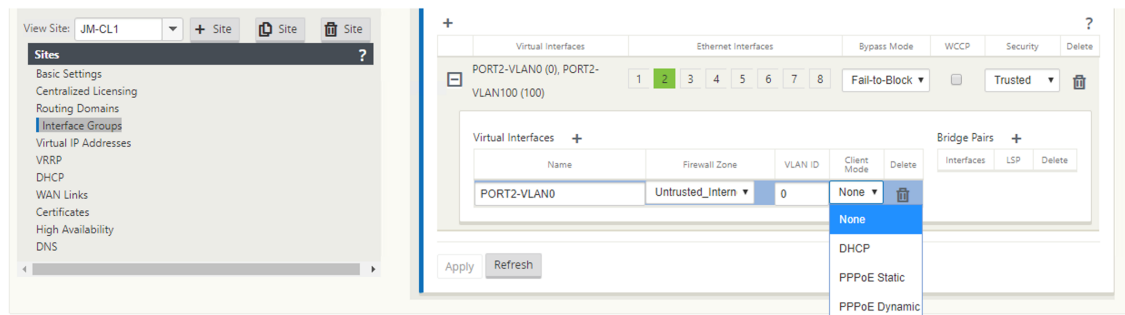


3. Wählen Sie **Schnittstellengruppen** für den MCN-Site aus. Gehen Sie wie folgt vor:

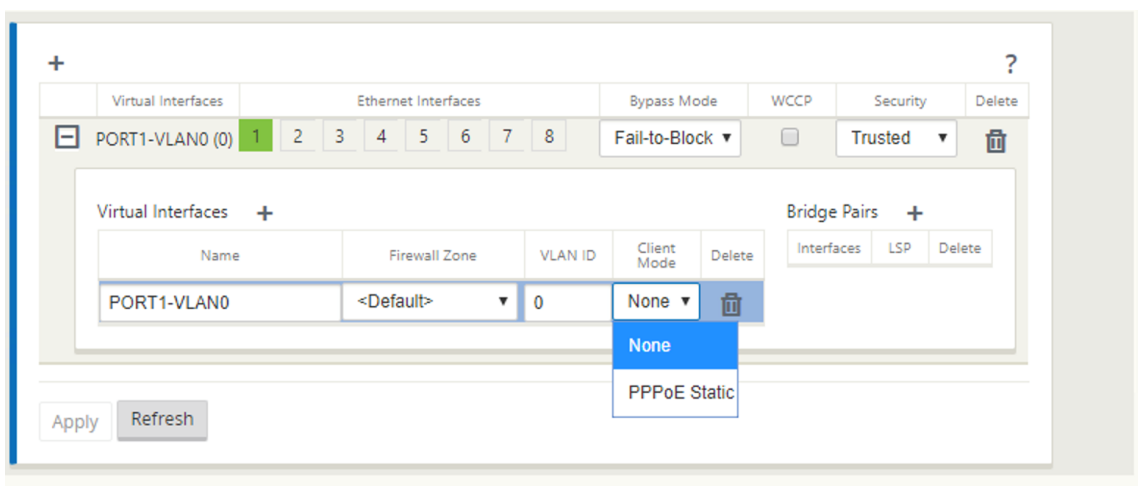
- Virtuelle Schnittstellen hinzufügen.
- Konfigurieren Sie Ethernet-Schnittstellen.
- Konfigurieren Sie den Umgehungsmodus.
- Wählen Sie ggf. **WCCP**.
- Wählen Sie Sicherheit —Vertrauens/Nicht vertrauenswürdig.

Für virtuelle Schnittstelle:

- Konfigurieren Sie den Namen, die Firewall-Zone, die VALN-ID und den Client-Modus.
- Ein mit mehreren Schnittstellen konfiguriertes VNI kann nur eine Schnittstelle für PPPoE-Konnektivität verwenden.
- Wenn ein VNI, das mit mehreren Schnittstellen und einer PPPoE-Konnektivität konfiguriert ist, auf einer anderen Schnittstelle geändert wird, kann die Monitorseite verwendet werden, um die vorhandene Sitzung zu stoppen und eine neue Sitzung zu starten, dann kann eine neue Sitzung über die neue Schnittstelle eingerichtet werden.



4. Wählen Sie **PPPoE Statisch oder Keine** basierend auf Ihrer Netzwerkkonfiguration für die Option Client-Modus auf der MCN-Appliance aus. Die folgenden weiteren Optionen werden angezeigt.

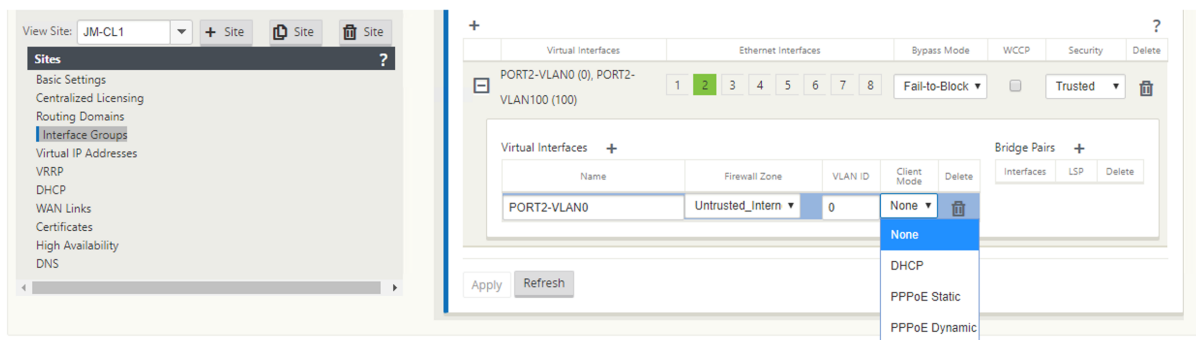


Konfigurieren Sie die folgenden PPPoE-Parameter, und klicken Sie auf **Übernehmen**.

- Access Concentrator (AC) Name (Feld).
- Service Name:
- Zurückhaltende Wiederverbindungszeit (Standardeinstellung ist die sofortige Wiederverbindung, '0')
- Authentifizierungstyp - (AUTO/PAP/CHAP/EAP).
 - Wenn die Option Auth auf Auto festgelegt ist, berücksichtigt die SD-WAN-Appliance die vom Server empfangene Anforderung des unterstützten Authentifizierungsprotokolls.
 - Wenn die Authentifizierungsoption auf PAP/CHAP/EAP festgelegt ist, werden nur bestimmte Authentifizierungsprotokolle berücksichtigt. Wenn PAP in der Konfiguration vorhanden ist und der Server eine Authentifizierungsanforderung mit CHAP sendet, wird die Verbindungsanforderung abgelehnt. Wenn der Server nicht mit PAP ausgehandelt wird, tritt ein Authentifizierungsfehler auf.
- CHAP umfasst CHAP, Microsoft CHAP und Microsoft CHAPv2.
- EAP unterstützt EAP-MD5.
- Benutzername und Kennwort.

The screenshot displays the configuration page for 'PORT2-VLAN0' under the 'Virtual Interfaces' tab. The interface includes a top navigation bar with tabs: Virtual Interfaces, Ethernet Interfaces, Bypass Mode, WCCP, and Security. Below the navigation bar, there are tabs for 'PORT2-VLAN0' and 'VLAN100 (100)'. The 'PORT2-VLAN0' tab is active, showing a configuration table with columns: Name, Firewall Zone, VLAN ID, Client Mode, and Delete. The table lists 'PORT2-VLAN0' with 'Untrusted_Intern' as the Firewall Zone, '0' as the VLAN ID, and 'PPPoE' as the Client Mode. Below the table, the 'PPPoE Credentials' section is expanded, showing fields for AC Name (isp), Service Name (testservice), Reconnect Hold Off (s) (10), Username (adc), Password (masked), and Auth (Auto). A note states: 'Note : Converting Virtual Interface to PPPoE will clear any Gateway IP Address and Virtual IP Address (in case of PPPoE Dynamic only) associate with it under access interfaces.' At the bottom, there is a summary bar for 'PORT2-VLAN0' with 'Untrusted_Intern' as the Firewall Zone, '100' as the VLAN ID, and 'Default' as the Client Mode. The bottom of the interface shows a navigation bar with tabs: PORT1-VLAN0 (0), 1, 2, 3, 4, 5, 6, 7, 8, Fail-to-Block, and Trusted.

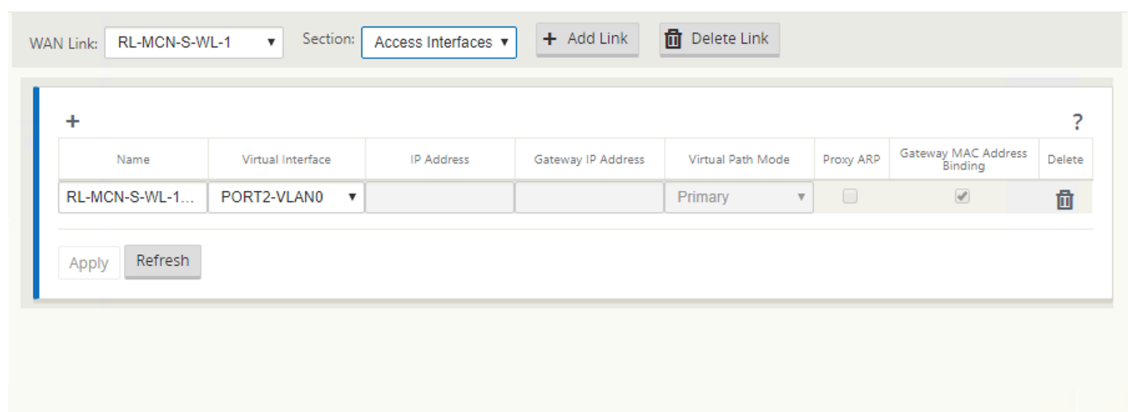
Die folgende Abbildung zeigt die PPPoE-Clientmodus-Optionen für eine Zweig-SD-WAN-Appliance. Wenn PPPoE Dynamic ausgewählt ist, muss der VNI "Nicht vertrauenswürdig" sein.



Konfigurieren von WAN-Verbindungen

1. Navigieren Sie in der SD-WAN-GUI zu **Sites > WAN-Links**. Pro PPPoE statischen oder dynamischen VNI ist nur eine WAN-Link-Erstellung zulässig. Die WAN-Verbindungskonfiguration hängt von der VNI-Auswahl des Client-Modus ab.
2. Wenn der VNI mit dem dynamischen PPPoE-Client-Modus konfiguriert ist:
 - IP-Adress- und Gateway-IP-Adressfelder werden inaktiv.
 - Der Modus "Virtueller Pfad" ist auf "Primär" eingestellt.
 - Proxy ARP kann nicht konfiguriert werden.

Standardmäßig ist Gateway MAC-Adressbindung ausgewählt.



3. Wenn der VNI mit dem statischen PPPoE-Clientmodus konfiguriert ist, konfigurieren Sie die IP-Adresse.

WAN Link: **RL-MCN-S-WL-1** Section: **Access Interfaces** **+ Add Link** **Delete Link**

| Name | Virtual Interface | IP Address | Gateway IP Address | Virtual Path Mode | Proxy ARP | Gateway MAC Address Binding | Delete |
|------------------|-------------------|---------------|--------------------|-------------------|--------------------------|-------------------------------------|--------|
| RL-MCN-S-WL-1... | PORT2-VLAN0 | 192.168.1.250 | | Primary | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

Apply **Refresh**

Hinweis:

Wenn der Server die konfigurierte statische IP-Adresse nicht berücksichtigt und eine andere IP-Adresse anbietet, tritt ein Fehler auf. Die PPPoE-Sitzung versucht, die Verbindung in regelmäßigen Abständen wiederherzustellen, bis der Server die konfigurierte IP-Adresse akzeptiert.

PPPoE-Sitzungen überwachen

Sie können PPPoE-Sitzungen überwachen, indem Sie in der SD-WAN-GUI zur Seite **Überwachung > PPPoE** navigieren.

Die Seite PPPoE enthält Statusinformationen der konfigurierten VNIs mit dem statischen oder dynamischen PPPoE-Client-Modus. Es ermöglicht Ihnen, die Sitzungen zur Fehlerbehebung manuell zu starten oder zu stoppen.

- Wenn der VNI bereit ist, **werden in den Spalten IP- und Gateway-IP** die aktuellen Werte in der Sitzung angezeigt. Es zeigt an, dass diese kürzlich empfangenen Werte sind.
- Wenn der VNI gestoppt wird oder sich im fehlerhaften Zustand befindet, werden die Werte zuletzt empfangenen Werte.
- Wenn Sie den Mauszeiger über die Gateway-IP-Spalte zeigen, wird die MAC-Adresse des PPPoE Access Concentrators angezeigt, von dem die Sitzung und die IP empfangen werden.
- Wenn Sie mit der Maus über den Wert “state” zeigen, wird eine Meldung angezeigt, die für einen “Failed”-Status nützlicher ist.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

Monitoring > PPPoE

PPPoE Monitoring

| Virtual Interface | IP Address | Gateway IP | Session ID | State | Action |
|-------------------|--------------|---------------|------------|---------|--------|
| PORT2-VLAN0 | 192.168.1.22 | 192.168.1.254 | 18 | Ready | Stop |
| abcd | 0.0.0.0 | 0.0.0.0 | 0 | Failed | Start |
| newVif | 0.0.0.0 | 0.0.0.0 | 0 | Stopped | Start |

In der Spalte **Status** wird der Status der PPPoE-Sitzung mit drei Farbcodes angezeigt: Grün, Rot, Gelb und Werte. In der folgenden Tabelle werden die Zustände und Beschreibungen beschrieben. Sie können den Mauszeiger über die Zustände bewegen, um Beschreibungen zu erhalten.

| PPPoE-Sitzungstyp | Farbe | Beschreibung |
|-------------------|-------|--|
| Konfiguriert | Gelb | Ein VNI ist mit PPPoE konfiguriert. Dies ist ein Anfangszustand. |
| Wählvorgang | Gelb | Nachdem ein VNI konfiguriert wurde, wechselt der PPPoE-Sitzungsstatus in den Wählstatus, indem er die PPPoE-Erkennung startet. Paketinformationen werden erfasst. |
| Sitzung | Gelb | VNI wird vom Ermittlungsstatus in den Sitzungsstatus verschoben. Warten auf IP, wenn dynamisch oder warten auf Bestätigung vom Server für die angekündigte IP, falls statisch. |
| Bereit | grün | IP-Pakete werden empfangen und VNI- und die zugehörige WAN-Verbindung können verwendet werden. |

| PPPoE-Sitzungstyp | Farbe | Beschreibung |
|-------------------|-------|---|
| Fehler | rot | PPP/PPPoE-Sitzung wird beendet. Der Grund für den Fehler kann auf ungültige Konfiguration oder schwerwiegenden Fehler zurückzuführen sein. Die Sitzung versucht, die Verbindung nach 30 Sekunden wieder herzustellen. |
| Beendet | gelb | PPP/PPPoE-Sitzung wird manuell beendet. |
| Beenden | gelb | Ein Zwischenzustand, der aus einem Grund beendet wird. Dieser Zustand beginnt automatisch nach einer bestimmten Dauer (5 Sekunden für normalen Fehler oder 30 Sekunden für einen schwerwiegenden Fehler). |
| Disabled | gelb | Der SD-WAN-Dienst ist deaktiviert. |

Problembehandlung bei PPPoE-Sitzungsfehlern

Wenn auf der Seite Überwachung ein Problem beim Einrichten einer PPPoE-Sitzung vorliegt:

- Wenn Sie mit der Maus über den Status Failed zeigen, wird der Grund für den letzten Fehler angezeigt.
- Um eine neue Sitzung einzurichten oder eine aktive PPPoE-Sitzung zu beheben, verwenden Sie die Seite Monitoring->PPPoE und starten Sie die Sitzung neu.
- Wenn eine PPPoE-Sitzung manuell beendet wird, kann sie erst gestartet werden, wenn sie manuell gestartet und eine Konfigurationsänderung aktiviert ist oder der Dienst neu gestartet wird.

Eine PPPoE-Sitzung kann aus folgenden Gründen fehlschlagen:

- Wenn SD-WAN sich aufgrund eines falschen Benutzernamens/Kennworts in der Konfiguration nicht beim Peer authentifiziert.

- PPP-Aushandlung schlägt fehl - die Verhandlung erreicht nicht den Punkt, an dem mindestens ein Netzwerkprotokoll ausgeführt wird.
- Systemspeicher- oder Systemressourcenproblem.
- Ungültig/fehlerhafte Konfiguration (falscher AC-Name oder Dienstname).
- Fehler beim Öffnen des seriellen Ports aufgrund eines Betriebssystemfehlers.
- Keine Antwort für die Echo-Pakete empfangen (Link ist fehlerhaft oder Server reagiert nicht).
- Es gab mehrere kontinuierliche erfolglose Wählsitzungen mit in einer Minute.

Nach 10 aufeinanderfolgenden Fehlern wird der Grund für den Fehler beobachtet.

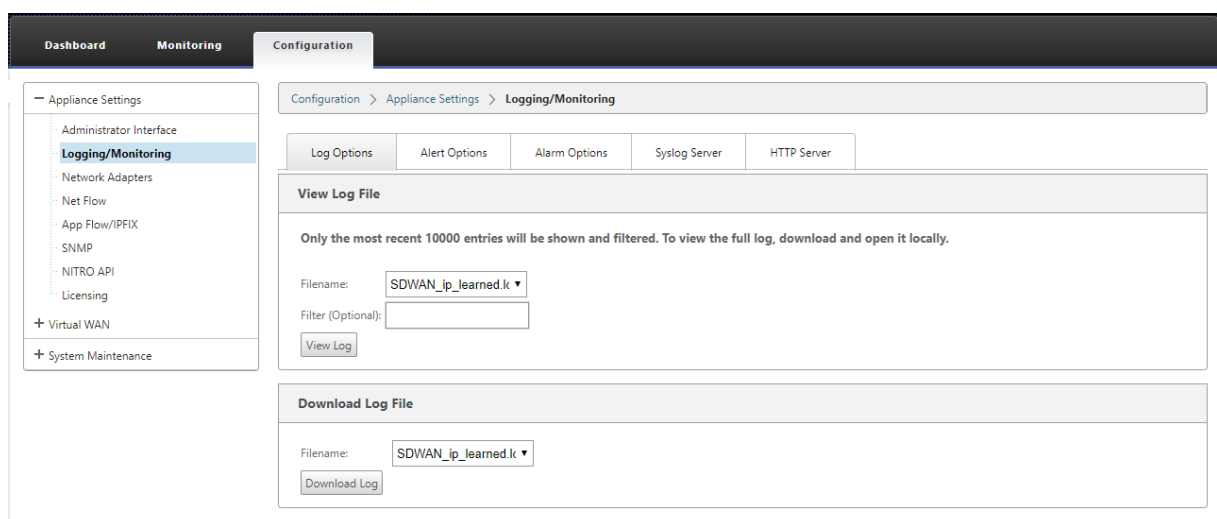
- Wenn der Fehler normal ist, wird er sofort neu gestartet.
- Wenn der Fehler ein Fehler ist, wird der Neustart für 10 Sekunden zurückgesetzt.
- Wenn der Fehler schwerwiegend ist, wird der Neustart 30 Sekunden lang vor dem Neustart zurückgesetzt.

LCP-Echo-Anforderungspakete werden alle 60 Sekunden aus SD-WAN generiert, und wenn 5 Echo-Antworten nicht empfangen werden, wird dies als Verbindungsfehler angesehen und die Sitzung wird wieder hergestellt.

PPPoE-Protokolldatei

Die Datei *SDWAN_IP_learned.log* enthält Protokolle, die sich auf PPPoE beziehen.

Um die Datei *SDWAN_IP_learned.log* von der SD-WAN-GUI anzuzeigen oder herunterzuladen, navigieren Sie zu **Appliance-Einstellungen > Logging/Monitoring > Log-Optionen**. Zeigen Sie die Datei *SDWAN_IP_Learned.log* an oder laden Sie sie herunter.



Qualität der Dienstleistung

May 10, 2021

Das Netzwerk zwischen Bürostandorten und dem Rechenzentrum oder der Cloud muss eine Vielzahl von Anwendungen und Daten transportieren, einschließlich qualitativ hochwertiger Video- oder Echtzeit-Stimmen. Bandbreitensensitive Anwendungen erweitern die Fähigkeiten und Ressourcen des Netzwerks. Citrix SD-WAN bietet garantierte, sichere, messbare und berechenbare Netzwerkdienste. Dies wird durch die Verwaltung der Verzögerung, Jitter, Bandbreite und Paketverlust im Netzwerk erreicht.

Die Citrix SD-WAN Lösung umfasst ein hochentwickeltes QoS-Modul (Application Quality of Service), das auf den Anwendungsdatenverkehr zugreift und kritische Anwendungen priorisiert. Es versteht auch die Anforderungen an die WAN-Netzwerkqualität und wählt einen Netzwerkpfad basierend auf den Qualitätsmerkmalen in Echtzeit aus.

In den Themen in den folgenden Abschnitten werden QoS-Klassen, IP-Regeln, Anwendungs-QoS-Regeln und andere Komponenten beschrieben, die zum Definieren von Anwendungs-QoS erforderlich sind.

Klassen

October 28, 2021

Die Citrix SD-WAN Konfiguration stellt einen standardmäßigen Satz von anwendungs- und IP/Port-basierten QoS-Richtlinien bereit, die auf den gesamten Datenverkehr angewendet werden, der über virtuelle Pfade übertragen wird. Diese Einstellungen können an die Bereitstellungsanforderungen angepasst werden.

Klassen sind nützlich, um den Datenverkehr zu priorisieren. Anwendungs- und IP/Port-basierte QoS-Richtlinien klassifizieren den Datenverkehr und fügen ihn in die entsprechenden Klassen ein, die in der Konfiguration angegeben sind.

Weitere Informationen zu Anwendungs-QoS und IP-Adresse-/Port-basierten QoS finden Sie unter [Regeln nach Anwendungsname](#) und [Regeln nach IP-Adresse bzw. Portnummer](#).

Das SD-WAN bietet 17 Klassen (IDs: 0—16). Es folgt die Standardkonfiguration aller 17 Klassen.

Virtual Path Default Set: New_Default_Set-1 Section: Classes + Add Default Set 🗑 Delete Default Set

| ID | Name | Type | Initial | | | | Sustained | | Reset |
|----|----------------------------|-------------|---------|------|--------|---------|-----------|---------|-------|
| | | | Period | Rate | %/Kbps | Share % | Rate | Share % | |
| 0 | HDX_priority_tag_0 | Realtime | 0 | 30 | % | 0 | 30 | 0 | 🔄 |
| 1 | HDX_priority_tag_1 | Interactive | 0 | 0 | % | 20 | 0 | 20 | 🔄 |
| 2 | HDX_priority_tag_2 | Interactive | 0 | 0 | % | 6 | 0 | 6 | 🔄 |
| 3 | HDX_priority_tag_3 | Interactive | 0 | 0 | % | 2 | 0 | 2 | 🔄 |
| 4 | class_4 | Bulk | | 0 | % | 0 | 0 | 0 | 🔄 |
| 5 | class_5 | Bulk | | 0 | % | 0 | 0 | 0 | 🔄 |
| 6 | class_6 | Bulk | | 0 | % | 0 | 0 | 0 | 🔄 |
| 7 | class_7 | Bulk | | 0 | % | 0 | 0 | 0 | 🔄 |
| 8 | class_8 | Bulk | | 0 | % | 0 | 0 | 0 | 🔄 |
| 9 | class_9 | Bulk | | 0 | % | 0 | 0 | 0 | 🔄 |
| 10 | realtime_class | Realtime | 0 | 30 | % | 0 | 30 | 0 | 🔄 |
| 11 | interactive_high_class | Interactive | 0 | 0 | % | 20 | 0 | 20 | 🔄 |
| 12 | interactive_medium_class | Interactive | 0 | 0 | % | 13 | 0 | 13 | 🔄 |
| 13 | interactive_low_class | Interactive | 0 | 0 | % | 6 | 0 | 6 | 🔄 |
| 14 | interactive_very_low_class | Interactive | 0 | 0 | % | 3 | 0 | 3 | 🔄 |
| 15 | bulk_background_class | Bulk | | 0 | % | 0 | 0 | 100 | 🔄 |
| 16 | bulk_unused_class | Bulk | | 0 | % | 0 | 0 | 0 | 🔄 |

Apply Revert

Im Folgenden sind die verschiedenen Arten von Klassen:

- **Echtzeit:** Wird für niedrige Latenz, niedrige Bandbreite und zeitkritischen Datenverkehr verwendet. Echtzeitanwendungen sind zeitempfindlich, benötigen aber keine wirklich hohe Bandbreite (zum Beispiel Voice over IP). Echtzeitanwendungen reagieren empfindlich auf Latenz und Jitter, können aber einige Verluste tolerieren.
- **Interaktiv:** Wird für interaktive Datenverkehr mit niedrigen bis mittleren Latenzanforderungen und niedrigen bis mittleren Bandbreitenanforderungen verwendet. Die Interaktion erfolgt in der Regel zwischen einem Client und einem Server. Die Kommunikation benötigt möglicherweise keine hohe Bandbreite, ist aber empfindlich gegenüber Verlust und Latenz.
- **Bulk:** Wird für Traffic mit hoher Bandbreite und Anwendungen verwendet, die hohe Latenz tolerieren können. Anwendungen, die Dateiübertragung verarbeiten und eine hohe Bandbreite benötigen, werden als Massenkategorie kategorisiert. Diese Anwendungen beinhalten wenig menschliche Eingriffe und werden meist von den Systemen selbst behandelt.

Bandbreitenfreigabe zwischen Klassen

Bandbreite wird wie folgt von Klassen gemeinsam genutzt:

- **Echtzeit:** Traffic, der Echtzeitklassen trifft, hat garantiert eine geringe Latenz und die Bandbreite ist bei konkurrierenden Datenverkehr auf den Klassenanteil begrenzt.
- **Interaktiv:** Traffic, der die interaktiven Klassen trifft, erhält nach der Bereitstellung von Echtzeit-Datenverkehr die verbleibende Bandbreite, und die verfügbare Bandbreite wird fair unter den interaktiven Klassen geteilt.
- **Bulk:** Masse ist beste Anstrengung. Die Bandbreite, die nach der Bereitstellung von Echtzeit- und interaktivem Datenverkehr übrig bleibt, wird Massenklassen auf fairer Basis gegeben. Massenverkehr kann verhungern, wenn Echtzeit- und interaktiver Datenverkehr die gesamte verfügbare Bandbreite nutzt.

Hinweis

Jede Klasse kann die gesamte verfügbare Bandbreite verwenden, wenn kein Konflikt besteht.

Im folgenden Beispiel wird die Bandbreitenverteilung basierend auf der Klassenkonfiguration erläutert:

Betrachten Sie, dass eine aggregierte Bandbreite von 10 Mbit/s über virtuellen Pfad vorhanden ist. Wenn die Klassenkonfiguration

- Echtzeit: 30%
- Interaktives Hoch: 40%
- Interaktives Medium: 20%
- Interaktiv niedrig: 10%
- Bulk: 100%

Das Ergebnis der Bandbreitenverteilung ist

- Der Echtzeitverkehr erhält je nach Bedarf 30% von 10 Mbit/s (3 Mbit/s). Wenn weniger als 10% benötigt werden, wird der Rest der Bandbreite den anderen Klassen zur Verfügung gestellt.
- Interaktive Klassen teilen sich die verbleibende Bandbreite auf Fair Share-Basis (4 Mbit/s: 2 Mbit/s: 1 Mbit/s).
- Alles, was übrig ist, wenn interaktiver Echtzeit-Verkehr seinen Anteil nicht vollständig nutzt, wird der Bulk-Klasse übergeben.

So passen Sie Klassen an:

1. Wenn Standardsätze für virtuelle Pfade verwendet werden, können Klassen unter **Global > Virtual Path Default Sets** geändert werden.

Hinweis:

Sie können Klassen auch auf der Ebene Virtueller Pfad ändern (**Verbindungen -> Virtuelle**

Pfade -> Klassen)

2. Klicken Sie auf **Standardsatz hinzufügen**, geben Sie einen Namen für den Standardsatz ein, und klicken Sie auf **Hinzufügen**. Wählen Sie im Feld **Abschnitt** die Option **Klassenaus**.
3. Geben Sie im Feld **Name** entweder den Standardnamen ein, oder geben Sie einen Namen Ihrer Wahl ein.
4. Wählen Sie im Feld **Typ** den Klassentyp (Echtzeit, Interaktiv oder Bulk) aus.
5. Für Echtzeitklassen können Sie die folgenden Attribute angeben:
 - **Anfangsperiode**: Der Zeitraum in Millisekunden, in dem eine Anfangsrate angewendet werden soll, bevor Sie zu einer nachhaltigen Rate wechseln.
 - **Anfangsrate**: Maximale Rate oder Prozentsatz, mit dem Pakete die Warteschlange während der Anfangsperiode verlassen.
 - **Nachhaltige Rate**: Maximale Rate oder Prozentsatz, mit dem die Pakete die Warteschlange nach der Anfangsperiode verlassen.
6. Für interaktive Klassen können Sie die folgenden Attribute angeben:
 - **Anfangszeitraum**: Der Zeitraum in Millisekunden, in dem der anfängliche Prozentsatz der verfügbaren Bandbreite angewendet wird, bevor auf den anhaltenden Prozentsatz gewechselt wird. Typischerweise 20 ms.
 - **Anfangsvorteilung%**: Der maximale Anteil der verbleibenden Bandbreite virtueller Pfade, nachdem während der ersten Periode in Echtzeit gedient wurde.
 - **Nachhaltige Freigabe%**: Der maximale Anteil der verbleibenden Bandbreite virtueller Pfade, nachdem der Echtzeitverkehr nach der ersten Periode gesorgt wurde.
7. Für Massenklassen können Sie nur die **Nachhaltige Freigabe** angeben, die die verbleibende Bandbreite des virtuellen Pfads bestimmt, die nach der Bereitstellung von Echtzeit- und interaktivem Datenverkehr für eine Bulk-Klasse verwendet werden soll.
8. Klicken Sie auf **Apply**.

Hinweis

Speichern Sie die Konfiguration, exportieren Sie sie in den Change Management-Posteingang und initiieren Sie den Änderungsmanagementprozess.

Regeln nach IP-Adresse und Portnummer

May 10, 2021

Regeln nach IP-Adresse und Portnummer Funktion hilft Ihnen, Regeln für Ihr Netzwerk zu erstellen und bestimmte Quality of Service (QoS) Entscheidungen basierend auf den Regeln zu treffen. Sie können benutzerdefinierte Regeln für Ihr Netzwerk erstellen. Sie können beispielsweise eine Regel erstellen als —Wenn die Quell-IP-Adresse 172.186.30.74 und die Ziel-IP-Adresse 172.186.10.89 lautet, legen Sie den **Übertragungsmodus** als Persistent Path und **LAN auf WAN-Klasse** als 10 (realtime_class) fest.

Mit dem Konfigurationseditor können Sie Regeln für den Verkehrsfluss erstellen und die Regeln mit Anwendungen und Klassen verknüpfen. Sie können Kriterien zum Filtern des Datenverkehrs für einen Flow angeben und allgemeine Verhaltensweisen, LAN-zu-WAN-Verhalten, WAN-zu-LAN-Verhalten und Paketprüfungsregeln anwenden.

Sie können Regeln lokal auf Standortebene oder auf globaler Ebene erstellen. Wenn mehr als eine Website dieselbe Regel erfordert, können Sie unter **Global > Virtual Path Default Sets > Rules eine Vorlage für Regeln** erstellen. Die Vorlage kann dann an die Sites angehängt werden, auf denen die Regeln angewendet werden müssen. Selbst wenn eine Site mit der global erstellten Regelvorlage verknüpft ist, können Sie standortspezifische Regeln erstellen. In solchen Fällen haben standortspezifische Regeln Vorrang und überschreiben die global erstellte Regelvorlage.

Erstellen von Regeln nach IP-Adresse und Portnummer

1. Navigieren Sie im SD-WAN-Konfigurations-Editor zu **Global > Virtual Path Default Sets**.

Hinweis

Sie können Regeln auf Site-Ebene erstellen, indem Sie zu **Sites > Verbindungen > Virtuelle Pfade > Regeln** navigieren.

2. Klicken Sie auf **Standardsatz hinzufügen**, geben Sie einen Namen für den Standardsatz ein, und klicken Sie auf **Hinzufügen**. Wählen Sie im Feld Abschnitt die Option **Regeln** aus, und klicken Sie auf **+**.

3. Geben Sie im Feld **Reihenfolge** den Auftragswert ein, der definiert werden soll, wann die Regel in Bezug auf andere Regeln angewendet wird.

4. Wählen Sie im Feld **Regelgruppenname** eine Regelgruppe aus. Die Statistiken für Regeln mit derselben Regelgruppe werden gruppiert und können zusammen angezeigt werden.

Um Regelgruppen anzuzeigen, navigieren Sie zu **Überwachung > Statistiken**, und wählen Sie im Feld **Anzeigen** die Option **Regelgruppen** aus.

Sie können auch benutzerdefinierte Anwendungen hinzufügen. Weitere Informationen finden Sie unter [Regelgruppen hinzufügen und MOS aktivieren](#).

5. Wählen Sie im Feld **Routingdomäne** eine der konfigurierten Routingdomänen aus.

6. Sie können Regeln Abgleichskriterien definieren, um Dienste basierend auf den aufgeführten Parametern zu filtern. Nach der Filterung werden die Regeleinstellungen auf die Dienste angewendet, die diesen Kriterien entsprechen.

- **Quell-IP-Adresse:** Quell-IP-Adresse und Subnetzmaske, die mit dem Datenverkehr übereinstimmen.
- **Ziel-IP-Adresse:** Ziel-IP-Adresse und Subnetzmaske, die mit dem Datenverkehr übereinstimmen.

Hinweis

Wenn das Kontrollkästchen **Dest=Src** aktiviert ist, wird die Quell-IP-Adresse auch für die Ziel-IP-Adresse verwendet.

- **Protokoll:** Protokoll, das mit dem Datenverkehr übereinstimmt.
- **Quellport:** Quellportnummer oder Portbereich, der mit dem Datenverkehr übereinstimmt.
- **Zielpport:** Zielpportnummer oder Portbereich, der mit dem Datenverkehr übereinstimmt.

Hinweis

Wenn das Kontrollkästchen **Dest=Src** aktiviert ist, wird der Quellport auch für den Zielpport verwendet.

- **DSCP:** Das **DSCP-Tag** im IP-Header, das mit dem Datenverkehr übereinstimmt.
 - **VLAN:** Die **VLAN-ID**, die mit dem Datenverkehr übereinstimmt.
7. Klicken Sie auf das Symbol Hinzufügen (+) neben der neuen Regel.
8. Klicken Sie auf **Eigenschaften mit Protokoll** initialisieren, um die Regeleigenschaften zu initialisieren, indem Sie die Regelstandardwerte und empfohlenen Einstellungen für das Protokoll anwenden. Dadurch werden die Standardregeleinstellungen aufgefüllt. Sie können die Einstellungen auch manuell anpassen, wie in den folgenden Schritten gezeigt.
9. Klicken Sie auf die Kachel **WAN Allgemein**, um die folgenden Eigenschaften zu konfigurieren.
- **Übertragungsmodus:** Wählen Sie einen der folgenden Übertragungsmodi aus.
 - **Lastenausgleichspfad:** Der Datenverkehr für den Fluss wird über mehrere Pfade für den Dienst ausgeglichen. Der Datenverkehr wird über den besten Pfad gesendet, bis dieser Pfad verwendet wird. Überbleibende Pakete werden über den nächstbesten Pfad gesendet.
 - **Persistenter Pfad:** Der Datenverkehr für den Flow bleibt auf demselben Pfad, bis der Pfad nicht mehr verfügbar ist.

- **Doppelter Pfad:** Der Datenverkehr für den Fluss wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht.
- **Dienst überschreiben:** Der Datenverkehr für den Flow überschreibt einen anderen Dienst. Wählen Sie im Feld Dienst überschreiben den Diensttyp aus, für den der Dienst außer Kraft setzt. Ein virtueller Pfaddienst kann beispielsweise zu einem Intranet-, Internet- oder Passthrough-Dienst überschreiben.
- **Verlorene Pakete erneut übertragen:** Senden Sie Datenverkehr, der dieser Regel entspricht, über einen zuverlässigen Dienst an die Remote-Appliance und senden Sie verlorene Pakete erneut.
- **TCP-Beendigung aktivieren:** Aktivieren Sie die TCP-Beendigung des Datenverkehrs für diesen Flow. Die Roundtrip-Zeit für die Bestätigung von Paketen wird reduziert und verbessert somit den Durchsatz.
- **Bevorzugter WAN-Link:** Der WAN-Link, den die Flows zuerst verwenden sollten.
- **Persistente Impedanz:** Die Mindestzeit in Millisekunden, für die der Datenverkehr im selben Pfad verbleiben würde, bis die Wartezeit beträgt, bei der der Pfad länger als der konfigurierte Wert ist.
- **Aktivieren Sie IP, TCP und UDP:** Komprimieren Sie Header in IP-, TCP- und UDP-Paketen.
- **GRE aktivieren:** Kopfzeilen in GRE-Paketen komprimieren.
- **Paketaggregation aktivieren:** Aggregieren Sie kleine Pakete zu größeren Paketen.
- **Performance verfolgen:** Zeichnet die Performance-Attribute dieser Regel in einer Sitzungsdatenbank auf (z. B. Verlust, Jitter, Latenz und Bandbreite).

WAN General

Transmit Mode:
 Load Balance Paths ☐ Retransmit Lost Packets

Override Service: Preferred WAN Link: Persistent Impedance(ms):

Traffic Optimization

TCP Termination
 Enable TCP Termination:

Header Compression
☐ Enable IP, TCP and UDP ☐ Enable GRE

☐ Enable Packet Aggregation

☐ Track Performance

10. Klicken Sie auf die Kachel **LAN-zu-WAN**, um das LAN-zu-WAN-Verhalten für diese Regel zu konfigurieren.

- **Klasse:** Wählen Sie eine Klasse aus, der diese Regel zugeordnet werden soll.

Hinweis

Sie können Klassen auch anpassen, bevor Sie Regeln anwenden. Weitere Informationen finden Sie unter [So passen Sie Klassen an](#).

- **Große Paketgröße:** Pakete, die kleiner oder gleich dieser Größe sind, werden die Werte für **Drop Limit** und **Drop Depth** zugewiesen, die in den Feldern rechts neben dem Feld **Klasse** angegeben sind.

Pakete, die größer als diese Größe sind, werden den Werten zugewiesen, die in den Standardfeldern **Drop Limit** und **Drop Depth** im Abschnitt **Große Pakete** des Bildschirms angegeben sind.

- **Drop-Limit:** Länge der Zeit, nach der Pakete, die im Klassenplaner warten, gelöscht werden. Nicht anwendbar für eine Massenkategorie.
- **Drop-Tiefe:** Schwellenwert für die Warteschlange, nach dem Pakete gelöscht werden.

- **RED aktivieren:** Random Early Detection (RED) sorgt für eine faire gemeinsame Nutzung von Klassenressourcen, indem Pakete verworfen werden, wenn Staus auftreten.
- **Größe neu zuweisen:** Paketlänge, die bei Überschreitung dazu führt, dass das Paket der Klasse neu zugewiesen wird, die im Feld Klasse neu zuweisen angegeben ist.
- **Klasseneu zuweisen: Klasse,** die verwendet wird, wenn die Paketlänge die im Feld Größe neu zuweisen angegebene Paketlänge überschreitet.
- **Deaktivieren Limit:** Zeit, für die Duplizierung deaktiviert werden kann, um zu verhindern, dass doppelte Pakete Bandbreite belegen.
- **Deaktivieren Tiefe:** Die Warteschlangentiefe des Klassenplaners, zu welchem Zeitpunkt die doppelten Pakete nicht generiert werden.
- **TCP-Standalone-ACK-Klasse:** Klasse mit hoher Priorität, der TCP-Standalone-Bestätigungen bei großen Dateiübertragungen zugeordnet werden.

The screenshot displays the 'LAN to WAN' configuration window, which is divided into three sections: General, Reassign, and TCP Standalone ACK. Each section contains various settings for packet handling, including class selection, drop limits, and packet sizes.

General Section:

- Class:** 3 (citrix_class_3)
- Drop Limit (ms):** 60
- Large Packet Size (bytes):** 0
- Enable RED:** ☒
- Large Packets:**
 - Drop Limit (ms):** 50
 - Drop Depth (bytes):** 128000
- Duplicate Packets:**
 - Disable Limit (ms):** 0
 - Disable Depth (bytes):** 128000

Reassign Section:

- Reassign Class:** 1 (citrix_class_1)
- Drop Limit (ms):** 50
- Reassign Size (bytes):** 2000
- Large Packet Size (bytes):** 0
- Enable RED:** ☒
- Large Packets:**
 - Drop Limit (ms):** 1
 - Drop Depth (bytes):** 0
- Duplicate Packets:**
 - Disable Limit (ms):** 0
 - Disable Depth (bytes):** 128000

TCP Standalone ACK Section:

- TCP Standalone ACK Class:** Disabled <Default>
- Drop Limit (ms):** 50
- Large Packet Size (bytes):** 0
- Enable RED:** ☒
- Large Packets:**
 - Drop Limit (ms):** 0
 - Drop Depth (bytes):** 0

11. Klicken Sie auf die **WAN-zu-LAN-Kachel**, um das WAN-zu-LAN-Verhalten für diese Regel zu konfigurieren.

- **Paketresequenzierung aktivieren:** Sequenziert die Pakete in der richtigen Reihenfolge am Ziel.

- **Haltezeit:** Zeitintervall, für das die Pakete für die Wiedersequenzierung gehalten werden, danach werden die Pakete an das LAN gesendet.
- **Späte Wiedersequenzierungspakete verwerfen:** Verwerfen Sie nicht bestellbare Pakete, die eingetroffen sind, nachdem die für die Wiedersequenzierung erforderlichen Pakete an das LAN gesendet wurden.
- **DSCP-Tag:** DSCP-Tag wird auf die Pakete angewendet, die dieser Regel entsprechen, bevor sie an das LAN gesendet werden.

WAN to LAN

Packet Resequencing

☒ Enable Packet Resequencing

☒ Discard Late Resequencing Packets

Hold Time (ms):

DSCP Tag: af12

12. Klicken Sie auf **Deep Packet Inspection** (Deep Packet Inspection), und wählen Sie **Passive FTP-Erkennung aktivieren** (Enable Passive FTP-Erkennung), damit die Regel den für die FTP-Datenübertragung verwendeten Port erkennt und die Regeleinstellungen automatisch auf
13. Klicken Sie auf **Übernehmen**.

Hinweis

Speichern Sie die Konfiguration, exportieren Sie sie in den Posteingang der Änderungsverwaltung und starten Sie den Änderungsverwaltungsprozess.

Regeln überprüfen

Navigieren Sie im Konfigurations-Editor zu **Monitoring > Flows**. Wählen Sie das Feld **Flow-Typ** im Abschnitt **Flows auswählen** oben auf der Seite **Flows** aus. Neben dem Feld **Flow-Typ** gibt es eine Reihe von Kontrollkästchen zum Auswählen der Flow-Informationen, die Sie anzeigen möchten. Überprüfen Sie, ob die Flussinformationen den konfigurierten Regeln entsprechen.

Beispiel:

Die Regel "Wenn die Quell-IP-Adresse 172.186.30.74 und die Ziel-IP-Adresse 172.186.10.89 ist, legen Sie den **Übertragungsmodus** als persistenter Pfad fest" zeigt die folgenden **Flow-Daten** an.

Select Flows

Flow Type:
☒ LAN to WAN
☒ WAN to LAN
☐ Internet Load Balancing Table
☐ TCP Termination Table
Max Flows to Display (Per Flow Type):
50
Filter (Optional):
Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

| Details | Source IP Address | Dest IP Address | Direction | Source Port | Dest Port | IPP | IP DSCP | HIT Count | Service Type | Service Name | LAN GW IP | Age (ms) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|---------|-------------------|-----------------|------------|-------------|-----------|-----|---------|-----------|--------------|--------------|-----------|----------|---------|-----------|----------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|------------------------|-----------------------------|-------------------|-------------|
| | 172.166.30.74 | 172.166.10.89 | LAN to WAN | 55502 | 5003 | TCP | default | 88311 | Virtual Path | DC-Client-1 | LOCAL | 0 | 88251 | 126639068 | 7558028 | 86763.328 | 3446.461 | 0.000 | 1 | N/A | 9 | BULK | DC-WL-1->Client-1-WL-1 | N/A | Persistent | iperf |
| | 172.166.10.89 | 172.166.30.74 | WAN to LAN | 5003 | 55502 | TCP | default | 45207 | Virtual Path | DC-Client-1 | LOCAL | 1 | 45207 | 2385488 | 3871.667 | 1634.405 | 1765.480 | 0.000 | 69 | N/A | N/A | N/A | N/A | N/A | Persistent | iperf |

Total LAN to WAN flows displayed: 1 out of 1
Total WAN to LAN flows displayed: 1 out of 1

Navigieren Sie im Konfigurations-Editor zu **Monitoring > Statistiken** und überprüfen Sie die konfigurierten Regeln.

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Statistics

Statistics

Show: Rules

Enable Auto Refresh

 5 seconds

Stop

Rule Statistics

Filter: in Any column

Apply

Show 100 entries Showing 1 to 100 of 275 entries

| Num | Site | Service | IP Address | | IP Proto | Port | | VLAN ID | IP DSCP | LAN to WAN | | WAN to LAN | | | | | | |
|-----|------|-------------|------------|-----|----------|-----------|-----------|---------|---------|------------|---------|------------|---------|-------------|--------------|------------------|------------------|------------------|
| | | | Src | Dst | | Src | Dst | | | Bytes | Packets | Bytes | Packets | Jitter (ms) | Packets Lost | Avg Latency (ms) | Min Latency (ms) | Max Latency (ms) |
| 0 | DC | DC-Client-1 | * | * | TCP | 5003 | * | * | * | 0 | 0 | 0 | 0 | | | | | |
| 1 | DC | DC-Client-1 | * | * | TCP | * | 5003 | * | * | 426121168 | 285604 | 0 | 0 | | | | | |
| 2 | DC | DC-Client-1 | * | * | TCP | 5060-5061 | * | * | ef | 0 | 0 | 0 | 0 | | | | | |
| 3 | DC | DC-Client-1 | * | * | TCP | * | 5060-5061 | * | ef | 0 | 0 | 0 | 0 | | | | | |
| 4 | DC | DC-Client-1 | * | * | UDP | 5060-5061 | * | * | ef | 0 | 0 | 0 | 0 | | | | | |
| 5 | DC | DC-Client-1 | * | * | UDP | * | 5060-5061 | * | ef | 0 | 0 | 0 | 0 | | | | | |

Regeln nach Anwendungsname

May 10, 2021

Die Anwendungsklassifizierungsfunktion ermöglicht es der Citrix SD-WAN Appliance, eingehenden Datenverkehr zu analysieren und sie als zu einer bestimmten Anwendung oder Anwendungsfamilie zu klassifizieren. Diese Klassifizierung ermöglicht es uns, die QoS einzelner Anwendungen oder Anwendungsfamilien zu verbessern, indem Anwendungsregeln erstellt und angewendet werden.

Sie können Datenverkehrsflüsse basierend auf Anwendungs-, Anwendungs- oder Anwendungsobjekt-Übereinstimmungstypen filtern und Anwendungsregeln darauf anwenden. Die Anwendungsregeln ähneln den IP-Regeln (Internet Protocol). Informationen zu IP-Regeln finden Sie unter Regeln nach IP-Adresse und Portnummer.

Für jede Anwendungsregel können Sie den Übertragungsmodus angeben. Die folgenden Übertragungsmodi sind verfügbar:

- **Load Balance-Pfad:** Der Anwendungsdatenverkehr für den Flow wird über mehrere Pfade ausgeglichen. Der Datenverkehr wird über den besten Pfad gesendet, bis dieser Pfad verwendet wird. Die verbleibenden Pakete werden über den nächstbesten Pfad gesendet.
- **Persistenter Pfad:** Der Anwendungsdatenverkehr verbleibt auf demselben Pfad, bis der Pfad nicht mehr verfügbar ist.
- **Doppelter Pfad:** Anwendungsdatenverkehr wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht.

Die Anwendungsregeln sind Klassen zugeordnet. Informationen zu Klassen finden Sie unter [Anpassen von Klassen](#).

Standardmäßig sind die folgenden fünf vordefinierten Anwendungsregeln für Citrix ICA-Anwendungen verfügbar:

| | | | Verlorene Pakete erneut übertragen | | Paketaktivieren | Paketaktivieren | Spätes Wiedersequenzieren von Paketen | Drop-Limit | Drop-Tiefe | RED aktivieren | Limit deaktivieren | Tiefe deaktivieren |
|-----------------------|------------|---------------|------------------------------------|--------|-----------------|-----------------|---------------------------------------|------------|------------|----------------|--------------------|--------------------|
| Regel | Klasse | Sendemodus | Wahr | Falsch | Wahr | Haltezeit(ms) | Interw. | (ms) | (Byte) | (ms) | (Byte) | (Byte) |
| HDX_Priority_0 | Priority_0 | Lastausgleich | Wahr | Falsch | Wahr | 250 | True | 350 | 30000 | True | 0 | 128000 |
| (HDX_priority_tag_0) | | | | | | | | | | | | |
| HDX_Priority_1 | Priority_1 | Lastausgleich | Wahr | Falsch | Wahr | 250 | True | 350 | 30000 | True | 0 | 128000 |
| (HDX_priority_tag_1) | | | | | | | | | | | | |
| HDX_Priority_2 | Priority_2 | Lastausgleich | Wahr | Falsch | Wahr | 250 | True | 350 | 30000 | True | 0 | 128000 |
| (HDX_priority_tag_2) | | | | | | | | | | | | |
| HDX_Priority_3 | Priority_3 | Lastausgleich | Wahr | Falsch | Wahr | 250 | True | 350 | 30000 | True | 0 | 128000 |
| (HDX_priority_tag_3) | | | | | | | | | | | | |
| HDX | 11 | Lastausgleich | Wahr | Falsch | Wahr | 250 | True | 350 | 30000 | True | 0 | 128000 |
| (inactive_high_class) | | | | | | | | | | | | |

Wie werden Anwendungsregeln angewendet?

Wenn die eingehenden Pakete im SD-WAN-Netzwerk die SD-WAN-Appliance erreichen, werden die anfänglichen Pakete keiner DPI-Klassifizierung unterzogen. Zu diesem Zeitpunkt werden die IP-Regelattribute wie Klasse, TCP-Beendigung auf die Pakete angewendet. Nach der DPI-Klassifizierung überschreiben die Anwendungsregelattribute wie Klasse, Übertragungsmodus die IP-Regelattribute.

Die IP-Regeln haben mehr Anzahl von Attributen im Vergleich zu den Anwendungsregeln. Die Anwendungsregel überschreibt nur wenige IP-Regelattribute, die restlichen IP-Regelattribute bleiben auf den Paketen verarbeitet.

Angenommen, Sie haben eine Anwendungsregel für eine Webmail-Anwendung wie Google Mail angegeben, die das SMTP-Protokoll verwendet. Der IP-Regelsatz für das SMTP-Protokoll wird zunächst vor der DPI-Klassifizierung angewendet. Nach dem Analysieren der Pakete und Klassifizieren als Zugehörigkeit zur Google Mail-Anwendung wird die für die Google Mail-Anwendung angegebene Anwendungsregel angewendet.

Anwendungsregeln erstellen

So erstellen Sie Anwendungsregeln:

1. Navigieren Sie im SD-WAN-Konfigurations-Editor zu **Global > Virtual Path Default Sets**.
2. Klicken Sie auf **Standardsatz hinzufügen**, geben Sie einen Namen für den Standardsatz ein, und klicken Sie auf **Hinzufügen**. Wählen Sie im Feld **Abschnitt** die Option **Application QoS** aus und klicken Sie auf **+**.

Hinweis

Sie können Anwendungsregeln auch erstellen, indem Sie zu **Verbindungen > Virtuelle Pfade > Anwendungs-QoS** oder **Global > Dynamischer virtueller Pfad Standardsatz > Anwendungs-QoS** navigieren.

? x

Add

Order: 100
Match Type: Application Object ▼
Application Objects: Any ▼
Rule Group Name: ALTHHTTP ▼

Source IP Address: 10.102.29.3/32
Destination IP Address: *
☐ Src = Dest

Source Port: *
Destination Port: *
☐ Src = Dest

WAN General
Transmit Mode: Load Balance Paths ▼
☐ Retransmit Lost Packets
Persistent Impedance(ms): 50

LAN to WAN
Class: 10 (realtime_class) ▼
Drop Limit (ms): 50
Drop Depth (bytes): 128000
☒ Enable RED

Duplicate Packets
Disable Limit (ms): 0
Disable Depth (bytes): 128000

WAN to LAN
☐ Enable Packet Resequencing
Resequencing Hold Time (ms):
☒ Discard Late Resequenced Packets
DSCP Tag: Any ▼

Add Cancel

3. Geben Sie im Feld **Reihenfolge** den Auftragswert ein, der definiert werden soll, wann die Regel in Bezug auf andere Regeln angewendet wird.
4. Wählen Sie im Feld **Abgleichart** eine der folgenden Übereinstimmungstypen aus:
 - **Anwendung** —Wenn dieser Übereinstimmungstyp ausgewählt ist, geben Sie die Anwendung an, die als Übereinstimmungskriterien für diesen Filter verwendet wird.
 - **Anwendungsfamilie** —Wenn dieser Übereinstimmungstyp ausgewählt ist, wählen Sie eine Anwendungsfamilie aus, die als Übereinstimmungskriterien für diesen Filter verwendet wird.
 - **Anwendungsobjekt** —Wenn dieser Übereinstimmungstyp ausgewählt ist, wählen Sie ein Anwendungsobjekt, das als Übereinstimmungskriterien für diesen Filter verwendet wird

Weitere Hinweise zu Anwendung, Anwendungsfamilie und Anwendungsobjekt finden Sie unter [Anwendungsklassifizierung](#).

5. Wählen Sie im Feld **Regelgruppenname** eine Regelgruppe aus. Die Statistiken für Regeln mit derselben Regelgruppe werden gruppiert und können zusammen angezeigt werden.

Um Regelgruppen anzuzeigen, navigieren Sie zu **Überwachung > Statistiken**, und wählen Sie im Feld **Anzeigen** die Option **Regelgruppen** aus.

Sie können auch benutzerdefinierte Regelgruppen hinzufügen. Weitere Informationen finden Sie unter [Hinzufügen benutzerdefinierter Anwendungen und Aktivieren von MOS](#).

6. Geben Sie die folgenden Kriterien für die Anwendungsregel an, um den Anwendungsdatenverkehr zu filtern. Nach der Filterung werden die Regeleinstellungen auf die Dienste angewendet, die diesen Kriterien entsprechen.
 - **Quell-IP-Adresse:** Quell-IP-Adresse und Subnetzmaske, die mit dem Datenverkehr übereinstimmen.
 - **Ziel-IP-Adresse:** Ziel-IP-Adresse und Subnetzmaske, die mit dem Datenverkehr übereinstimmen.
 - **Quellport:** Quellportnummer oder Portbereich, der mit dem Datenverkehr übereinstimmt.
 - **Zielport:** Zielportnummer oder Portbereich, der mit dem Datenverkehr übereinstimmt.

Hinweis

Wählen Sie **Src = Dest**, wenn die Quell- und Ziel-Internetprotokolladresse identisch sind.

7. Konfigurieren Sie die folgenden allgemeinen WAN-Einstellungen:
 - Wählen Sie im Feld **Übertragungsmodus** einen der folgenden Übertragungsmodi aus:
 - **Load Balance-Pfad:** Der Anwendungsdatenverkehr für den Flow wird über mehrere Pfade ausgeglichen. Der Verkehr wird über den besten Pfad gesendet, bis dieser Pfad vollständig verwendet wird. Die verbleibenden Pakete werden über den nächstbesten Pfad gesendet.
 - **Persistenter Pfad:** Der Anwendungsdatenverkehr verbleibt auf demselben Pfad, bis der Pfad nicht mehr verfügbar ist.

Geben Sie im Feld **Persistente Impedanz** die Mindestzeit in Millisekunden an, für die der Datenverkehr im selben Pfad verbleibt, bis die Wartezeit auf dem Pfad länger ist als der konfigurierte Wert.
 - **Doppelter Pfad:** Anwendungsdatenverkehr wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht.
 - Aktivieren Sie die Option **Verlorene Pakete erneut übertragen**, um Datenverkehr, der dieser Regel entspricht, über einen zuverlässigen Dienst an die Remote-Appliance zu senden und verlorene Pakete erneut zu übertragen.

8. Konfigurieren Sie die LAN-zu-WAN-Einstellungen:

- **Klasse:** Wählen Sie eine Klasse aus, der diese Regel zugeordnet werden soll.

Sie können Klassen auch anpassen, bevor Sie Regeln anwenden, weitere Informationen finden Sie unter [Klassen anpassen](#).

- **Drop-Limit:** Länge der Zeit, nach der Pakete, die im Klassenplaner warten, gelöscht werden. Nicht anwendbar für eine Massenkategorie.
- **Drop-Tiefe:** Schwellenwert für die Warteschlangentiefe, nach der Pakete verworfen werden.
- **RED aktivieren:** Random Early Detection (RED) sorgt für eine faire gemeinsame Nutzung von Klassenressourcen, indem Pakete verworfen werden, wenn Staus auftreten.
- **Limit deaktivieren:** Zeit, für die die Duplizierung deaktiviert werden kann, um zu verhindern, dass doppelte Pakete Bandbreite verbrauchen.
- **Deaktivieren Tiefe:** Die Warteschlangentiefe des Klassenplaners, zu welchem Zeitpunkt die doppelten Pakete nicht generiert werden.

9. Konfigurieren Sie das folgende WAN-zu-LAN-Verhalten für diese Regel:

- **Paketresequenzierung aktivieren:** Sequenziert die Pakete in der richtigen Reihenfolge am Ziel.
- **Resequenz-Haltezeit:** Zeitintervall, für das die Pakete für die Wiedersequenzierung gehalten werden, danach werden die Pakete an das LAN gesendet.
- **Späte Wiedersequenzierungspakete verwerfen:** Verwerfen Sie nicht bestellbare Pakete, die eingetroffen sind, nachdem die für die Wiedersequenzierung erforderlichen Pakete an das LAN gesendet wurden.

10. Klicken Sie auf **Übernehmen**.

Um zu bestätigen, ob Anwendungsregeln auf den Verkehrsfluss angewendet werden, navigieren Sie zu **Überwachung > Flows**.

Notieren Sie sich die App-Regelkennung und überprüfen Sie, ob der Klassentyp und der Übertragungsmodus gemäß Ihrer Regelkonfiguration sind.

| Source IP Address | Dest IP Address | Direction | Source Port | Dest Port | IP | IP DSCP | Htt Count | Service Type | Service Name | LAN GW IP | Age (ms) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type |
|-------------------|-----------------|------------|-------------|-----------|-----|---------|-----------|--------------|--------------|-----------|----------|---------|---------|---------|---------------|----------------------------|---------------------|---------|-------------|-------|-------------|------------------------|-----------------------------|-------------------|
| 172.16.30.74 | 172.16.10.89 | LAN to WAN | 35118 | 5001 | UDP | default | 4981 | Virtual Path | DC-Client-1 | LOCAL | 0 | 4959 | 7428582 | 292.687 | 3507.565 | 126.441 | 0.000 | 48 | 0 | 11 | INTERACTIVE | DC-WL-1->Client-1-WL-1 | N/A | Duplicate |

Total LAN to WAN flows displayed: 1 out of 1
Total WAN to LAN flows displayed: 0 out of 0

Sie können die Anwendung QoS überwachen, wie z. B. Anzahl der an jedem Standort hochgeladenen, heruntergeladenen oder gelöschten Pakete, indem Sie zu **Überwachung > Statistik > Anwendungs-QoS** navigieren.

Der Parameter **Num** gibt die App-Regelkennung an. Überprüfen Sie die App-Regelkennung, die aus dem Flow erhalten wurde.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

ICE/ISec

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

Monitoring > Statistics

Statistics

Show: Application QoS

Enable Auto Refresh

 5 seconds

Refresh

Application QoS Statistics

Filter:

Any column

Apply

Show: 100 entries Showing 1 to 12 of 12 entries

| Num | Site | Service | IP Address | | Port | | Application Object | Application | Family | LAN to WAN | | WAN to LAN | | Dropped | | Last Hit (DHHMM ago) |
|-----|----------|-------------|------------|-----|------|-----|--------------------|----------------|--------|------------|---------|------------|---------|---------|---------|----------------------|
| | | | Src | Dst | Src | Dst | | | | Bytes | Packets | Bytes | Packets | Bytes | Packets | |
| 0 | DC | DC-Client-1 | * | * | * | * | * | iperf | * | 26325792 | 32262 | 0 | 0 | 267616 | 192 | 0000 |
| 1 | DC | DC-Client-1 | * | * | * | * | * | ica_priority_0 | * | 0 | 0 | 0 | 0 | 0 | 0 | |
| 2 | DC | DC-Client-1 | * | * | * | * | * | ica_priority_1 | * | 0 | 0 | 0 | 0 | 0 | 0 | |
| 3 | DC | DC-Client-1 | * | * | * | * | * | ica_priority_2 | * | 0 | 0 | 0 | 0 | 0 | 0 | |
| 4 | DC | DC-Client-1 | * | * | * | * | * | ica_priority_3 | * | 0 | 0 | 0 | 0 | 0 | 0 | |
| 5 | DC | DC-Client-1 | * | * | * | * | * | ica | * | 0 | 0 | 0 | 0 | 0 | 0 | |
| 6 | Client-1 | DC-Client-1 | * | * | * | * | * | iperf | * | 0 | 0 | 4710 | 5 | 1484 | 1 | 0038 |

Showing 1 to 12 of 12 entries

First

Previous

1

Next

Last

Erstellen benutzerdefinierter Anwendungen

Sie können Anwendungsobjekte verwenden, um benutzerdefinierte Anwendungen basierend auf den folgenden Übereinstimmungstypen zu definieren:

- IP-Protokoll
- Anwendungsname
- Anwendungsfamilie

Der DPI-Klassifikator analysiert die eingehenden Pakete und klassifiziert sie als Anwendungen basierend auf den angegebenen Übereinstimmungskriterien. Sie können diese klassifizierten benutzerdefinierten Anwendungen in QoS, Firewall und Anwendungsrouting verwenden.

Tipp

Sie können einen oder mehrere Übereinstimmungstypen angeben.

Sie können die Berichte für die klassifizierten benutzerdefinierten Anwendungen im SD-WAN Center anzeigen. Weitere Informationen finden Sie unter [Anwendungsbericht](#).

So erstellen Sie benutzerdefinierte Anwendungen:

1. Navigieren Sie im Konfigurations-Editor zu **Global > Anwendungen > Benutzerdefinierte Anwendungen**, und klicken Sie auf **+**.

Add

Name: Priority: ☒ Enable Reporting

Application Match Criteria +

| Match Type | Application Family | Application | Protocol | Network IP Address 1 | Port 1 |
|---------------|--------------------|-------------|-----------|----------------------|--------|
| IP Protocol ▼ | | | TCP (6) ▼ | * | * |
| | | | | | |

Add **Cancel**

2. Legen Sie die folgenden Parameter fest:

- **Name:** Name für die benutzerdefinierte Anwendung
- **Berichterstellung aktivieren:** Ermöglicht das Anzeigen benutzerdefinierter Anwendungsberichte im SD-WAN Center. Weitere Informationen, siehe [Anwendungsbericht](#).
- **Priorität:** Die Priorität der benutzerdefinierten Anwendung. Wenn die eingehenden Pakete mit zwei oder mehr benutzerdefinierten Anwendungsdefinitionen übereinstimmen, wird die benutzerdefinierte Anwendungsdefinition mit der höchsten Priorität angewendet.

3. Klicken Sie im Abschnitt **Anwendungsübereinstimmungskriterien** auf +.

4. Wählen Sie einen der folgenden Übereinstimmungstypen:

- **IP-Protokoll:** Geben Sie das Protokoll, die Netzwerk-IP-Adresse, die Portnummer und das DSCP-Tag an.
- **Anwendung:** Geben Sie den Anwendungsnamen, die Netzwerk-IP-Adresse, die Portnummer und das DSCP-Tag an.
- **Anwendungsfamilie:** Wählen Sie eine Anwendungsfamilie aus, und geben Sie die Netzwerk-IP-Adresse, die Portnummer und das DSCP-Tag an.

5. Klicken Sie auf +, um weitere Anwendungsübereinstimmungskriterien hinzuzufügen.

6. Klicken Sie auf **Übernehmen**.

Regelgruppen hinzufügen und MOS aktivieren

May 10, 2021

Eine bestimmte Anwendung im Netzwerk kann durch die Gruppe von Regeln definiert werden, die darauf angewendet wird. Der SD-WAN-Konfigurationseditor bietet eine Standardliste von Regelgruppen. Sie können auch benutzerdefinierte Regelgruppen erstellen und einzelne IP-Regeln oder QoS-Regeln für Anwendungen kennzeichnen.

Weitere Informationen zu Regeln finden Sie unter [Regeln nach IP-Adresse und Portnummer](#) und [Regeln nach Anwendungsname](#).

Die Statistiken für Regeln mit derselben Regelgruppe werden zusammengefasst und können zusammen angezeigt werden.

Um Statistiken basierend auf Regelgruppen anzuzeigen, navigieren Sie zu **Überwachung > Statistiken**, und wählen Sie im **Feld Anzeigen** die Option **Regelgruppen** aus.

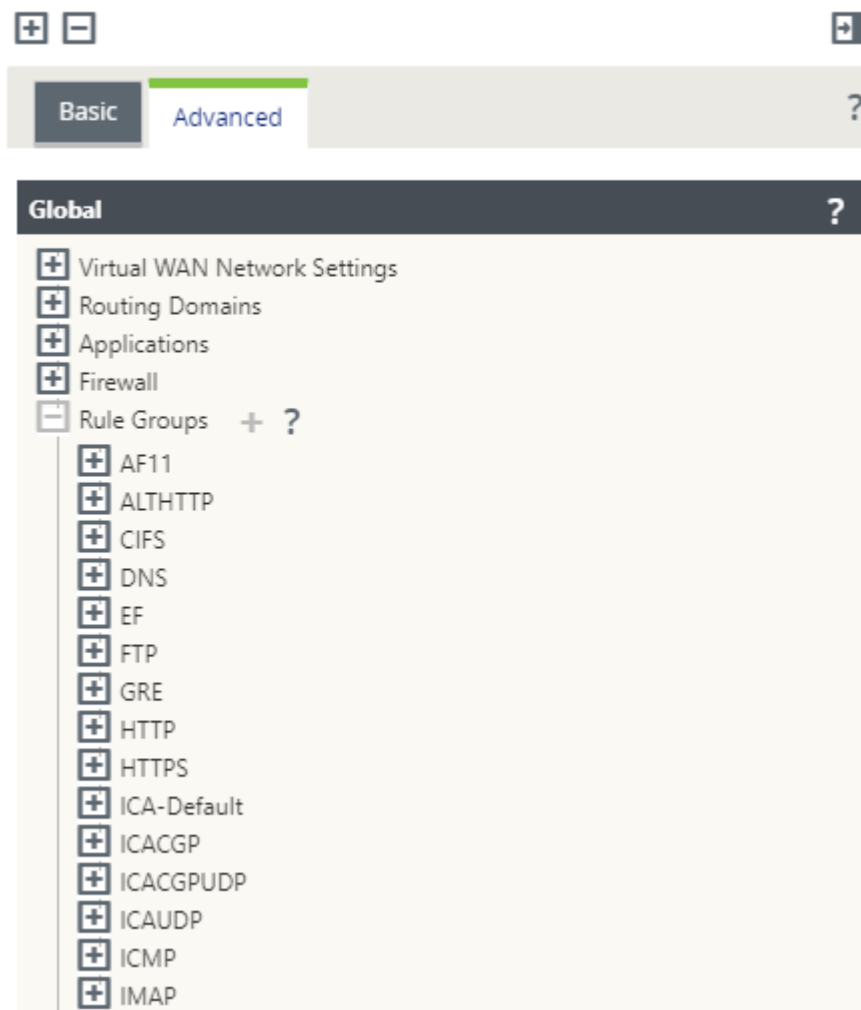
Der mittlere Meinungswert (MOS) ist ein numerisches Maß für die Qualität der Erfahrung, die eine Anwendung an Endbenutzer liefert. Es wird hauptsächlich für VoIP-Anwendungen verwendet. In SD-WAN wird MOS auch verwendet, um die Qualität von Nicht-VoIP-Anwendungen zu bewerten, indem der Datenverkehr so beurteilt wird, als ob es sich um einen VoIP-Anruf handelte.

Der durchschnittliche MoS-Wert wird mit einem Abtastintervall von 1 Minute berechnet. Die von anderen Tools von Drittanbietern berechnete MOS-Bewertung kann je nach verwendetem Stichprobenintervall variieren.

SD-WAN Center zeigt den MOS für vorhandenen Datenverkehr an, der den virtuellen Pfad durchläuft. Weitere Informationen zum Anzeigen von MOS in SD-WAN Center finden Sie unter [MOS für Anwendungen](#).

So fügen Sie eine benutzerdefinierte Regelgruppe hinzu:

1. Navigieren Sie im Konfigurations-Editor zu **Global > Regelgruppen..** Die Standardliste der Regelgruppen wird angezeigt.
2. Klicken Sie auf das Symbol Hinzufügen (+).
3. Geben Sie den Anwendungsnamen ein.
4. Klicken Sie auf das Bearbeitungssymbol und wählen Sie **MOS aktivieren** aus.



5. Klicken Sie auf **Übernehmen**.

Hinweis

- Sie können auch die MOS-Schätzung für die Standardanwendungen aktivieren, indem Sie **MOS aktivieren** auswählen.
- Aktivieren Sie unter Regeln die Option Leistung verfolgen, um MOS für Anwendungen zu schätzen und im SD-WAN Center anzuzeigen. Weitere Informationen finden Sie unter [MOS für Anwendungen](#).

Anwendungsklassifizierung

November 16, 2022

Die Citrix SD-WAN Appliances führen Deep Packet Inspection (DPI) durch, um Anwendungen anhand der folgenden Techniken zu identifizieren und zu klassifizieren:

- Klassifizierung der DPI-Bibliothek
- Citrix-proprietäre Independent Computing Architecture (ICA) Klassifizierung
- Anwendungshersteller-APIs (z. B. Microsoft REST-APIs für Office 365)
- Domännennamenbasierte Anwendungsklassifizierung

Klassifizierung der DPI-Bibliothek

Die Deep Packet Inspection (DPI) Bibliothek erkennt Tausende kommerzieller Anwendungen. Es ermöglicht die Echtzeiterkennung und Klassifizierung von Anwendungen. Mithilfe der DPI-Technologie analysiert die SD-WAN-Appliance die eingehenden Pakete und klassifiziert den Datenverkehr als zu einer bestimmten Anwendung oder Anwendungsfamilie. Die Anwendungsklassifizierung für jede Verbindung benötigt einige Pakete.

Um die DPI-Bibliotheksklassifizierung zu aktivieren, navigieren Sie im **Konfigurations-Editor** zu **Global > Anwendungen > DPI-Einstellungen** und **aktivieren Sie das Kontrollkästchen Deep Packet Inspection** aktivieren.

ICA-Klassifizierung

Citrix SD-WAN Appliances können Citrix HDX-Datenverkehr auch für virtuelle Apps und Desktops identifizieren und klassifizieren. Citrix SD-WAN erkennt die folgenden Varianten des ICA-Protokolls:

- ICA
- ICA-CGP
- Einzelstream-ICA (SSI)
- Multistream-ICA (MSI)
- ICA über TCP
- ICA über UDP/EDT
- ICA über nicht standardmäßige Ports (einschließlich Multi-Port ICA)
- Adaptiver HDX-Transport
- ICA über WebSocket (verwendet von HTML5 Receiver)

Hinweis

Die Klassifizierung des über SSL/TLS oder DTLS gelieferten ICA-Datenverkehrs wird in der SD-WAN Standard Edition nicht unterstützt, wird jedoch in der SD-WAN Premium Edition und der SD-WAN WANOP Edition unterstützt.

Die Klassifizierung des Netzwerkverkehrs erfolgt während der anfänglichen Verbindungen oder

der Flow-Einrichtung. Daher werden bereits vorhandene Verbindungen nicht als ICA klassifiziert. Die Klassifizierung von Verbindungen geht auch verloren, wenn die Verbindungstabelle manuell gelöscht wird.

Framehawk Datenverkehr und Audio-over-UDP/RTP werden nicht als HDX-Anwendungen klassifiziert. Sie werden entweder als UDP oder Unbekanntes Protokoll gemeldet.

Seit Release 10 Version 1 kann die SD-WAN-Appliance jeden ICA-Datenstrom in Multi-Stream-ICA sogar in einer Konfiguration mit einem Port unterscheiden. Jeder ICA-Stream wird als separate Anwendung mit einer eigenen Standard-QoS-Klasse zur Priorisierung klassifiziert.

- Damit die Multi-Stream-ICA-Funktionalität ordnungsgemäß funktioniert, müssen Sie über SD-WAN Standard Edition 10.1 oder höher oder SD-WAN Premium Edition verfügen.
- Damit HDX benutzerbasierte Berichte auf SDWAN-Center angezeigt werden können, müssen Sie SD-WAN Standard Edition oder Premium Edition 11.0 oder höher haben.

Minimale Softwareanforderungen für den virtuellen HDX-Informationskanal:

- Eine aktuelle Version von Citrix Virtual Apps and Desktops (früher XenApp und XenDesktop), da die erforderliche Funktionalität in XenApp und XenDesktop 7.17 eingeführt wurde und nicht in der Version 7.15 Langzeitdienst enthalten ist.
- Eine Version der Citrix Workspace App (oder deren Vorgänger Citrix Receiver), die Multi-Stream-ICA und den virtuellen HDX Insights-Informationskanal CTXNSAP unterstützt. Suchen Sie nach **HDX Insight mit NSAP VC** und Multiport/Multi-Stream ICA in der [Citrix Workspace-App –Featurematrix](#). Siehe die derzeit unterstützten Release-Versionen unter [HDX-Erkenntnisse](#).
- Ab Version 11.2 ist die Paketduplizierung jetzt standardmäßig für HDX-Echtzeitverkehr aktiviert, wenn Multistream-ICA verwendet wird.

Nach der Klassifizierung kann die ICA-Anwendung in Anwendungsregeln und zum Anzeigen von Anwendungsstatistiken ähnlich wie bei anderen klassifizierten Anwendungen verwendet werden.

Es gibt fünf Standardanwendungsregeln für ICA-Anwendungen jeweils eine für die folgenden Prioritäts-Tags:

- Unabhängige Datenverarbeitungsarchitektur (Citrix) (ICA)
- ICA Echtzeit (ica_priority_0)
- ICA Interaktiv (ica_priority_1)
- ICA Bulk-Transfer (ica_priority_2)
- ICA-Hintergrund (ica_priority_3)

Weitere Informationen finden Sie unter [Regeln nach Anwendungsname](#).

Wenn Sie eine Kombination von Software ausführen, die Multi-Stream-ICA nicht über einen einzigen

Port unterstützt, müssen Sie zum Ausführen von QoS mehrere Ports konfigurieren, einen für jeden ICA-Stream.

Um HDX auf nicht standardmäßigen Ports wie in der XA/XD-Serverrichtlinie konfiguriert zu klassifizieren, müssen Sie diese Ports in ICA-Portkonfigurationen hinzufügen. Um den Datenverkehr an diesen Ports mit gültigen IP-Regeln abzugleichen, müssen Sie außerdem die ICA-IP-Regeln aktualisieren.

In der ICA-IP- und Portliste können Sie nicht standardmäßige Ports angeben, die in der XA/XD-Richtlinie für die Verarbeitung der HDX-Klassifizierung verwendet werden. IP-Adresse wird verwendet, um die Ports weiter auf ein bestimmtes Ziel zu beschränken. Verwenden Sie '*' für Port, der zu einer beliebigen IP-Adresse bestimmt ist. IP-Adresse mit Kombination von SSL-Port wird auch verwendet, um anzuzeigen, dass der Datenverkehr wahrscheinlich ICA ist, obwohl der Datenverkehr nicht schließlich als ICA klassifiziert wird. Diese Angabe wird verwendet, um L4 AppFlow Datensätze zur Unterstützung von Multi-Hop-Berichten in Citrix Application Delivery Management zu senden.

Um die ICA-basierte Klassifizierung zu aktivieren, navigieren Sie im **Konfigurations-Editor** zu **Global > Applications > DPI-Einstellungen** und **aktivieren Sie das Kontrollkästchen Deep Packet Inspection für Citrix ICA-Anwendungen** aktivieren.

Anwendungshersteller-API-basierte Klassifizierung

Citrix SD-WAN unterstützt die folgende API-basierte Klassifikation des Anwendungsherstellers:

- Office 365. Weitere Informationen finden Sie unter [Office 365-Optimierung](#).
- Citrix Cloud und Citrix Gateway Service Weitere Informationen finden Sie unter [Optimierung des Gateway](#).

Domännennamenbasierte Anwendungsklassifizierung

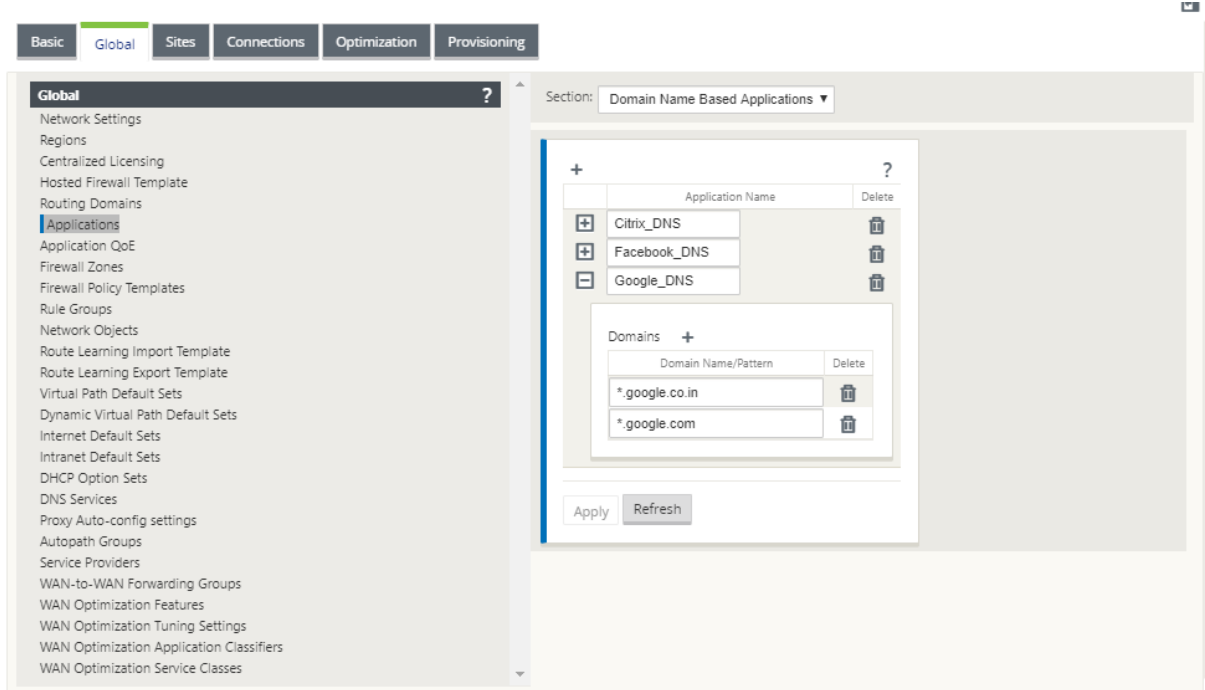
Die DPI-Klassifikations-Engine wurde erweitert, um Anwendungen basierend auf dem Domännennamen und -mustern zu klassifizieren. Nachdem die DNS-Weiterleitung die DNS-Anforderungen abgefangen und analysiert hat, verwendet das DPI-Modul den IP-Klassifikator, um die erste Paketklassifizierung durchzuführen. Weitere DPI-Bibliothek und ICA-Klassifizierung werden durchgeführt und die Domännennamen-basierte Anwendungs-ID wird angehängt.

Mit der Domännennamen-basierten Anwendungsfunktion können Sie mehrere Domännennamen gruppieren und als einzelne Anwendung behandeln. Erleichterung der Anwendung von Firewall, Anwendungssteuerung, QoS und anderen Regeln. Es können maximal 64 domännennamenbasierte Anwendungen konfiguriert werden.

Um domänenbasierte Anwendungen zu definieren, navigieren Sie im Konfigurations-Editor zu **Global > Anwendungen > Domännennamenbasierte Anwendungen** . Geben Sie einen Anwendungsnamen

ein, und fügen Sie die erforderlichen Domännennamen oder -muster hinzu. Sie können entweder den vollständigen Domainnamen eingeben oder am Anfang Wildcards verwenden. Folgende Domainnamenformate sind zulässig:

- beispiel.com
- *.beispiel.com



Die klassifizierten Domännennamen-basierten Anwendungen werden für die Konfiguration der folgenden verwendet:

- [DNS-Proxy](#)
- [Transparente DNS-Weiterleitung](#)
- Anwendungsobjekte
- [Anwendungsrouten](#)
- [Firewall-Richtlinie](#)
- [Anwendungs-QoS-Regeln](#)
- [Anwendung QoE](#)

Einschränkungen

- Wenn keine DNS-Anfrage/Antwort vorhanden ist, die einer domännennamenbasierten Anwendung entspricht, klassifiziert das DPI-Modul die domänenbasierte Anwendung nicht und wendet daher nicht die Anwendungsregeln an, die der domänenbasierten Anwendung entsprechen.

- Wenn ein Anwendungsobjekt so erstellt wird, dass der Portbereich Port 80 und/oder Port 443 mit einem bestimmten IP-Adressenübereinstimmungstyp enthält, der einer domänennamenbasierten Anwendung entspricht, klassifiziert das DPI-Modul die domänennamenbasierte Anwendung nicht.
- Wenn explizite Webproxys konfiguriert sind, müssen Sie der PAC-Datei alle Domänennamenmuster hinzufügen, um sicherzustellen, dass die DNS-Antwort nicht immer dieselbe IP-Adresse zurückgibt.
- Die domänennamenbasierten Anwendungsklassifizierungen werden beim Konfigurationsupdate zurückgesetzt. Die Reklassifizierung erfolgt basierend auf Klassifizierungstechniken vor 11.0.2, wie DPI-Bibliotheksklassifizierung, ICA-Klassifizierung und Anbieteranwendungs-APIs basierend auf Klassifizierung.
- Die erlernten Anwendungssignaturen (Ziel-IP-Adressen) nach der domänenbasierten Anwendungsklassifizierung werden bei der Konfigurationsupdate zurückgesetzt.
- Nur die standardmäßigen DNS-Abfragen und deren Antworten werden verarbeitet.
- AAAA-Einträge oder IPv6-Einträge werden nicht unterstützt.
- DNS-Antwortdatensätze, die auf mehrere Pakete aufgeteilt sind, werden nicht verarbeitet. Nur DNS-Antworten in einem einzigen Paket werden verarbeitet.
- DNS über TCP wird nicht unterstützt.
- Nur Domänen der obersten Ebene werden als Domänennamenmuster unterstützt.

Verschlüsselten Datenverkehr klassifizieren

Die Citrix SD-WAN Appliance erkennt verschlüsselten Datenverkehr im Rahmen der Anwendungsberichterstattung mit den folgenden beiden Methoden:

- Für HTTPS-Datenverkehr überprüft die DPI-Engine das SSL-Zertifikat, um den gemeinsamen Namen zu lesen, der den Namen des Dienstes trägt (z. B. Facebook, Twitter). Je nach Anwendungsarchitektur kann nur ein Zertifikat für mehrere Diensttypen verwendet werden (z. B. E-Mail, Nachrichten usw.). Wenn verschiedene Dienste unterschiedliche Zertifikate verwenden, kann die DPI-Engine zwischen Diensten unterscheiden.
- Bei Anwendungen, die ihr eigenes Verschlüsselungsprotokoll verwenden, sucht die DPI-Engine nach binären Mustern in den Flows, zum Beispiel im Falle von Skype sucht die DPI-Engine nach einem Binärmuster im Zertifikat und bestimmt die Anwendung.

So konfigurieren Sie Anwendungsklassifizierungseinstellungen:

1. Klicken Sie im **Konfigurations-Editor** auf **Global > Anwendungen > Einstellungen**.

Settings ?

☒ Enable Deep Packet Inspection

☒ Enable Deep Packet Inspection for Citrix ICA Applications

Citrix ICA Deep Packet Inspection Settings

☒ Enable HDX User Reporting

☒ Enable Multi-Stream ICA

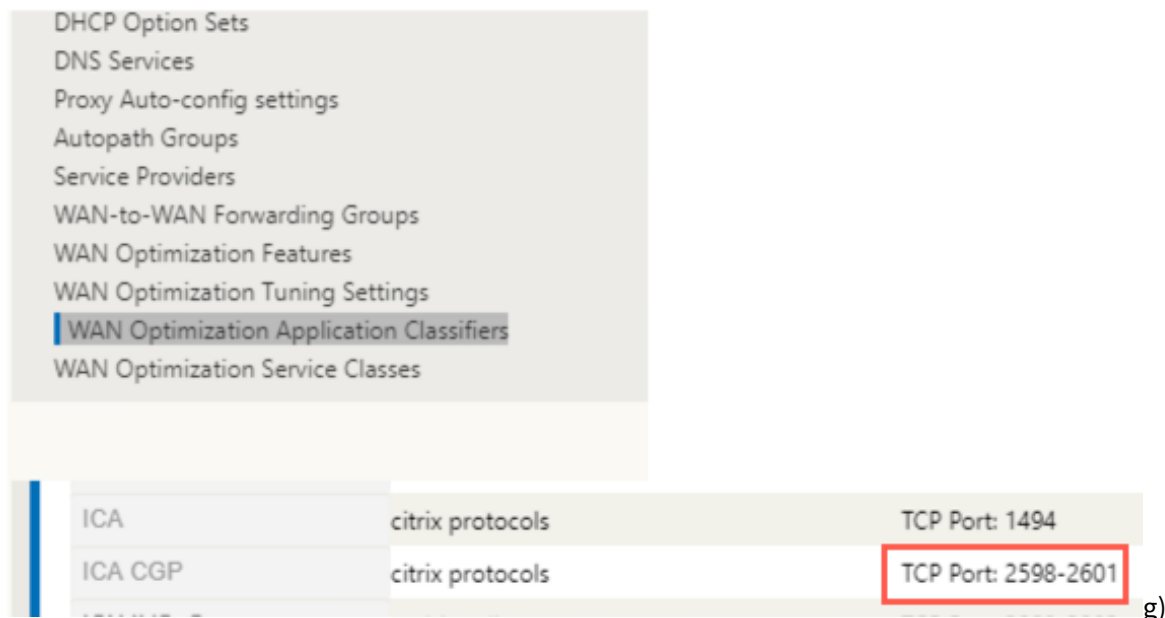
DPI ICA IP and Port List

| | |
|----------------------|-----------------------------------|
| DPI ICA IP-1: | DPI ICA Port-1: |
| <input type="text"/> | <input type="text" value="2599"/> |
| DPI ICA IP-2: | DPI ICA Port-2: |
| <input type="text"/> | <input type="text" value="2600"/> |
| DPI ICA IP-3: | DPI ICA Port-3: |
| <input type="text"/> | <input type="text" value="2601"/> |
| DPI ICA IP-4: | DPI ICA Port-4: |
| <input type="text"/> | <input type="text"/> |
| DPI ICA IP-5: | DPI ICA Port-5 : |
| <input type="text"/> | <input type="text"/> |

Hinweis

Wenn Sie zusätzlichen ICA-Port für die Bereitstellung mit mehreren Ports hinzufügen, müssen diese Ports in Anwendungsklassifizierern für die WAN-Optimierung hinzugefügt werden. Andernfalls wird der Datenverkehr auf den drei zusätzlichen Ports nicht an

WANOP weitergeleitet. Nur der standardmäßige 2598-Port wird weitergeleitet, wenn ICA für die Optimierung konfiguriert ist.



- Wählen Sie **Deep Packet Inspection aktivieren** aus. Dadurch wird die Anwendungsklassifizierung auf der Appliance aktiviert. Sie können Anwendungsstatistiken im SD-WAN Center anzeigen und überwachen. Weitere Informationen finden Sie unter [Anwendungsbericht](#).

Hinweis

Standardmäßig erfasst **Enable Deep Packet Inspection** Statistiken für klassifizierte Daten.

- Wählen Sie **Deep Packet Inspection für Citrix ICA-Anwendungen aktivieren**. Dies ermöglicht die Klassifizierung von Citrix ICA-Anwendungen und sammelt Statistiken für Benutzer, Sitzungen und Flusszählungen. Wenn diese Option aktiviert ist, wird möglicherweise ein Teil des HDX-Datenverkehrs noch klassifiziert und QoE berechnet, aber Statistiken zum SD-WAN-Center sind nicht verfügbar. Sie können ICA-Anwendungsstatistiken im SD-WAN Center anzeigen und überwachen. Diese Option ist standardmäßig aktiviert. Weitere Informationen finden Sie unter [HDX-Berichte](#).
- Wählen Sie **HDX User Reporting aktivieren** aus, um neu hinzugefügte benutzerbasierte Berichte (HDX Summary, HDX User Sessions und **HDX Apps**) zu generieren. Diese Berichte sind im SD-WAN Center verfügbar. Dies gilt nicht für den **HDX Site Stats** Bericht. Diese Option ist auf globaler Ebene und Standortebene verfügbar, ähnlich der DPI-Option. Um **HDX User Reporting auf Standortebene zu aktivieren**, klicken Sie im **Konfigurations-Editor** auf **Verbindungen > Anwendungen**.

Section: **DPI Settings**

☐ Use Global Application Settings

☒ Enable Deep Packet Inspection

☒ Enable Deep Packet Inspection for Citrix ICA Applications

Citrix ICA Deep Packet Inspection Settings

☐ Enable HDX User Reporting

☐ Enable Multi-Stream ICA

DPI ICA IP and Port List

| | |
|----------------------|----------------------|
| DPI ICA IP-1: | DPI ICA Port-1: |
| <input type="text"/> | <input type="text"/> |
| DPI ICA IP-2: | DPI ICA Port-2: |
| <input type="text"/> | <input type="text"/> |
| DPI ICA IP-3: | DPI ICA Port-3: |
| <input type="text"/> | <input type="text"/> |
| DPI ICA IP-4: | DPI ICA Port-4: |
| <input type="text"/> | <input type="text"/> |
| DPI ICA IP-5: | DPI ICA Port-5: |
| <input type="text"/> | <input type="text"/> |

Apply **Revert**

5. Geben Sie im **DPI-ICA-Port** nicht standardmäßige Ports an, die in der XA/XD-Richtlinie für die Verarbeitung der HDX-Klassifizierung verwendet werden. Geben Sie keine Standardportnummern 2598 oder 1494 in diese Liste ein, da diese bereits intern enthalten sind.
6. Geben Sie in **DPI ICA IP** die IP-Adresse an, die verwendet werden soll, um die Ports auf bestimmte Ziele weiter zu beschränken.

Hinweis

Verwenden Sie '*' für Port, der zu einer beliebigen IP-Adresse bestimmt ist.

7. Klicken Sie auf **Anwenden**

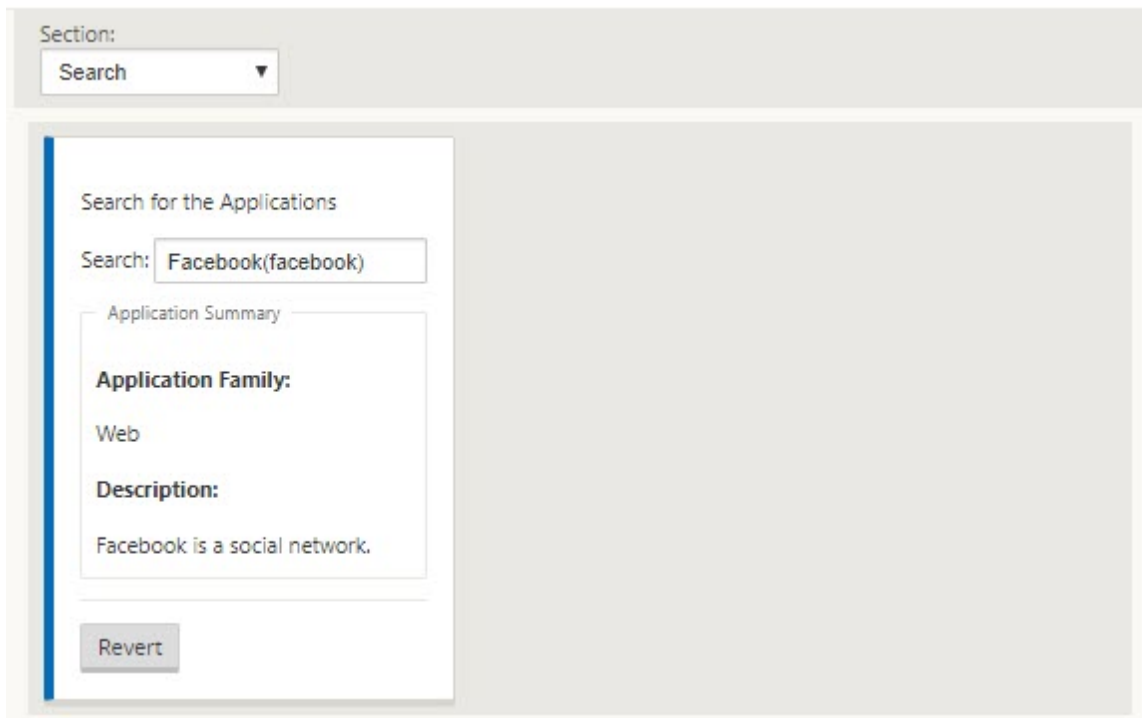
Sie können die Anwendungsklassifizierungseinstellungen an jedem Standort individuell konfigurieren. Klicken Sie auf **Verbindungen**, wählen Sie eine Site aus und klicken Sie auf **Anwendungseinstellungen**. Sie können auch die globalen Anwendungseinstellungen verwenden.

Anwendungen suchen

Sie können nach einer Anwendung suchen, um den Namen der Anwendungsfamilie zu bestimmen. Eine kurze Beschreibung des Antrags ist ebenfalls enthalten.

So suchen Sie nach einer Anwendung:

1. Klicken Sie im Konfigurations-Editor auf **Global > Anwendungen > Suchen**.
2. Geben Sie im Feld Suchen den Namen der Anwendung ein, und klicken Sie auf die Eingabetaste.
Eine kurze Beschreibung der Anwendung und des Namens der Anwendungsfamilie wird angezeigt.



Die folgenden Funktionen verwenden Anwendung als Übereinstimmungstyp:

- [Firewall-Richtlinie](#)
- [Anwendungs-QoS-Regeln](#)
- [Anwendung QoE](#)

Hinweis

Informationen zu Anwendungen, die die SD-WAN-Appliance mithilfe der Deep Packet Inspection identifizieren kann, finden Sie unter [Anwendungssignaturbibliothek](#).

Anwendungsobjekte

Anwendungsobjekte ermöglichen es Ihnen, verschiedene Typen von Übereinstimmungskriterien in einem einzigen Objekt zu gruppieren, das in Firewall-Richtlinien und Anwendungssteuerung verwen-

det werden kann. IP-Protokoll, Anwendung und Anwendungsfamilie sind die verfügbaren Übereinstimmungstypen.

Die folgenden Features verwenden Anwendungsobjekt als Übereinstimmungstyp:

- [Anwendungsrouten](#)
- [Firewall-Richtlinie](#)
- [Anwendungs-QoS-Regeln](#)
- [Anwendung QoE](#)

So erstellen Sie ein Anwendungsobjekt:

1. Klicken Sie im Konfigurations-Editor auf **Global > Anwendungen > Anwendungsobjekte**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie im Feld **Name** einen Namen für das Objekt ein.

Add ? x

Name: office-apps Priority: 500 ☒ Enable Reporting

Application Match Criteria +

| Match Type | Application Family | Application | Protocol | Network IP Address 1 | Port 1 |
|-------------|--------------------|-------------------------|----------|----------------------|--------|
| Application | | Salesforce(salesforce) | Any | 192.168.3.4/3 | * |
| Application | | Onjira.com (JIRA)(jira) | Any | 192.168.4.4/3 | * |

Add Cancel

3. Wählen Sie **Reporting aktivieren** aus, um die Anzeige benutzerdefinierter Anwendungsberichte in Citrix SD-WAN Center zu aktivieren. Weitere Informationen, siehe [Anwendungsbericht](#).
4. Geben Sie im Feld **Priorität** die Priorität des Anwendungsobjekts ein. Wenn die eingehenden Pakete mit zwei oder mehr Anwendungsobjektdefinitionen übereinstimmen, wird das Anwendungsobjekt mit der höchsten Priorität angewendet.
5. Klicken Sie im Abschnitt **Anwendungsübereinstimmungskriterien** auf +.
6. Wählen Sie einen der folgenden Übereinstimmungstypen:
 - **IP-Protokoll:** Geben Sie das Protokoll, die Netzwerk-IP-Adresse, die Portnummer und das DSCP-Tag an.
 - **Anwendung:** Geben Sie den Anwendungsnamen, die Netzwerk-IP-Adresse, die Portnummer und das DSCP-Tag an.
 - **Anwendungsfamilie:** Wählen Sie eine Anwendungsfamilie aus, und geben Sie die Netzwerk-IP-Adresse, die Portnummer und das DSCP-Tag an.

7. Klicken Sie auf **+**, um weitere Anwendungsübereinstimmungskriterien hinzuzufügen.
8. Klicken Sie auf **Hinzufügen**.

Verwenden der Anwendungsklassifizierung mit einer Firewall

Durch die Klassifizierung von Datenverkehr als Anwendungen, Anwendungsfamilien oder Domänennamen können Sie die Anwendung, Anwendungsfamilien und Anwendungsobjekte als Übereinstimmungstypen verwenden, um Datenverkehr zu filtern und Firewall-Richtlinien und -Regeln anzuwenden. Sie gilt für alle Vor-, Post- und lokalen Richtlinien. Weitere Hinweise zur Firewall finden Sie unter [Stateful Firewall](#) und [NAT-Unterstützung](#).

Edit Firewall Policy ? x

Priority: 100

From Zones

| Zone | Enable |
|-------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |
| Untrusted_Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|-------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |
| Untrusted_Internet_Zone | <input type="checkbox"/> |

Action: Allow Log Interval (s): 0 Log Start Log End Connection State Tracking: Use Site Setting

Match Type: IP Protocol (highlighted) Application Application Family Application Objects

Application Objects: Any Application: Application Family:

DSCP: Any Allow Fragments Reverse Also Match Established

Source Service Type: Any Source Service Name: Any Source IP: * Source Port: *

Dest Service Type: Any Dest Service Name: Any Dest IP: * Dest Port: *

Apply Cancel

Anwendungsklassifizierung anzeigen

Nachdem Sie die Anwendungsklassifizierung aktiviert haben, können Sie den Anwendungsnamen und die Anwendungsfamilie in den folgenden Berichten anzeigen:

- Firewall-Verbindungsstatistiken
- Informationen zu Flows

- Anwendungsstatistiken

Firewall-Verbindungsstatistiken

Navigieren Sie im **Konfigurations-Editor** zu **Monitoring > Firewall**. Im Abschnitt **Verbindungen** werden in den Spalten **Anwendung** und **Familie** die Anwendungen und die zugehörige Familie aufgeführt.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics:
Maximum entries to display: 50

Filtering:
Application: Any
IP Protocol: Any
Source Service Type: Any
Destination Service Type: Any
Refresh
Clear Connections
Help

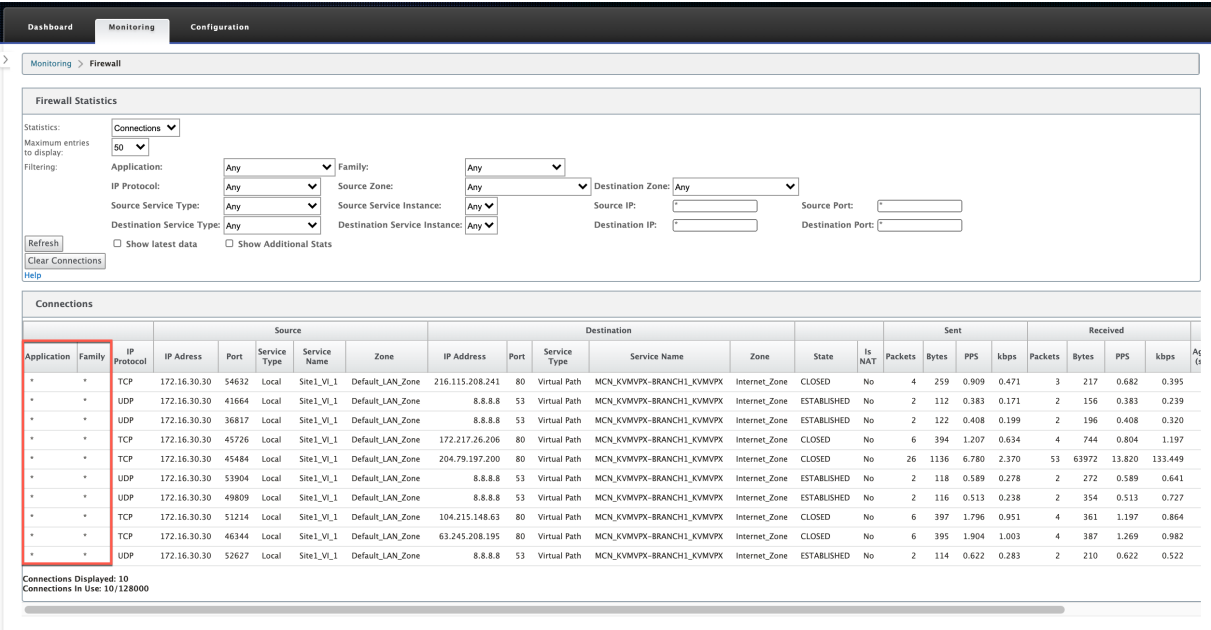
Family: Any
Source Zone: Any
Source Service Instance: Any
Destination Service Instance: Any
Destination Zone: Any
Source IP:
Destination IP:
Source Port:
Destination Port:
☐ Show latest data
☐ Show Additional Stats

Connections

| Application | Family | IP Protocol | Source | | | | Destination | | | | State | Is NAT | Sent | | | | | |
|---|--------------------|-------------|--------------|-------|--------------|--------------|------------------|-----------------|------|--------------|---------------------------|---------------|-------------|-------|-----|------|-------|-------|
| | | | IP Address | Port | Service Type | Service Name | Zone | IP Address | Port | Service Type | Service Name | Zone | Packets | Bytes | PPS | kbps | | |
| GoToMeeting Online Meeting(gotomeeting) | Audio/Video | TCP | 172.16.30.30 | 54612 | Local | Site1_VI_1 | Default_LAN_Zone | 216.115.208.241 | 80 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | CLOSED | No | 4 | 259 | 0.716 | 0.371 |
| Domain Name Service(dns) | Network Service | UDP | 172.16.30.30 | 47397 | Local | Site1_VI_1 | Default_LAN_Zone | 8.8.8.8 | 53 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | ESTABLISHED | No | 1 | 60 | 0.262 | 0.126 |
| Network Time Protocol(ntp) | Network Service | UDP | 172.16.30.30 | 48743 | Local | Site1_VI_1 | Default_LAN_Zone | 91.189.94.4 | 123 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | NEW | No | 1 | 76 | 0.264 | 0.160 |
| Domain Name Service(dns) | Network Service | UDP | 172.16.30.30 | 41348 | Local | Site1_VI_1 | Default_LAN_Zone | 8.8.8.8 | 53 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | ESTABLISHED | No | 2 | 118 | 0.476 | 0.225 |
| Domain Name Service(dns) | Network Service | UDP | 172.16.30.30 | 44961 | Local | Site1_VI_1 | Default_LAN_Zone | 8.8.8.8 | 53 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | ESTABLISHED | No | 2 | 114 | 0.513 | 0.234 |
| Domain Name Service(dns) | Network Service | UDP | 172.16.30.30 | 44119 | Local | Site1_VI_1 | Default_LAN_Zone | 8.8.8.8 | 53 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | ESTABLISHED | No | 1 | 60 | 0.263 | 0.126 |
| Google Generic(google_gen) | Web | TCP | 172.16.30.30 | 45706 | Local | Site1_VI_1 | Default_LAN_Zone | 172.217.26.206 | 80 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | CLOSED | No | 6 | 394 | 1.017 | 0.534 |
| BING | Custom Application | TCP | 172.16.30.30 | 45464 | Local | Site1_VI_1 | Default_LAN_Zone | 204.79.197.200 | 80 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | CLOSED | No | 31 | 1348 | 6.428 | 2.236 |
| Domain Name Service(dns) | Network Service | UDP | 172.16.30.30 | 59856 | Local | Site1_VI_1 | Default_LAN_Zone | 8.8.8.8 | 53 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | ESTABLISHED | No | 2 | 116 | 0.410 | 0.190 |
| Domain Name Service(dns) | Network Service | UDP | 172.16.30.30 | 49607 | Local | Site1_VI_1 | Default_LAN_Zone | 8.8.8.8 | 53 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | ESTABLISHED | No | 2 | 122 | 0.354 | 0.173 |
| Mozilla.com - Mozilla.org(mozilla) | Web | TCP | 172.16.30.30 | 46324 | Local | Site1_VI_1 | Default_LAN_Zone | 63.245.208.195 | 80 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | CLOSED | No | 6 | 395 | 1.551 | 0.817 |
| Domain Name Service(dns) | Network Service | UDP | 172.16.30.30 | 52889 | Local | Site1_VI_1 | Default_LAN_Zone | 8.8.8.8 | 53 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | ESTABLISHED | No | 2 | 112 | 0.332 | 0.149 |
| Microsoft(microsoft) | Web | TCP | 172.16.30.30 | 51194 | Local | Site1_VI_1 | Default_LAN_Zone | 104.215.148.63 | 80 | Virtual Path | MCN_KVMVPK-BRANCH1_KVMVPK | Internet_Zone | CLOSED | No | 6 | 397 | 1.433 | 0.758 |

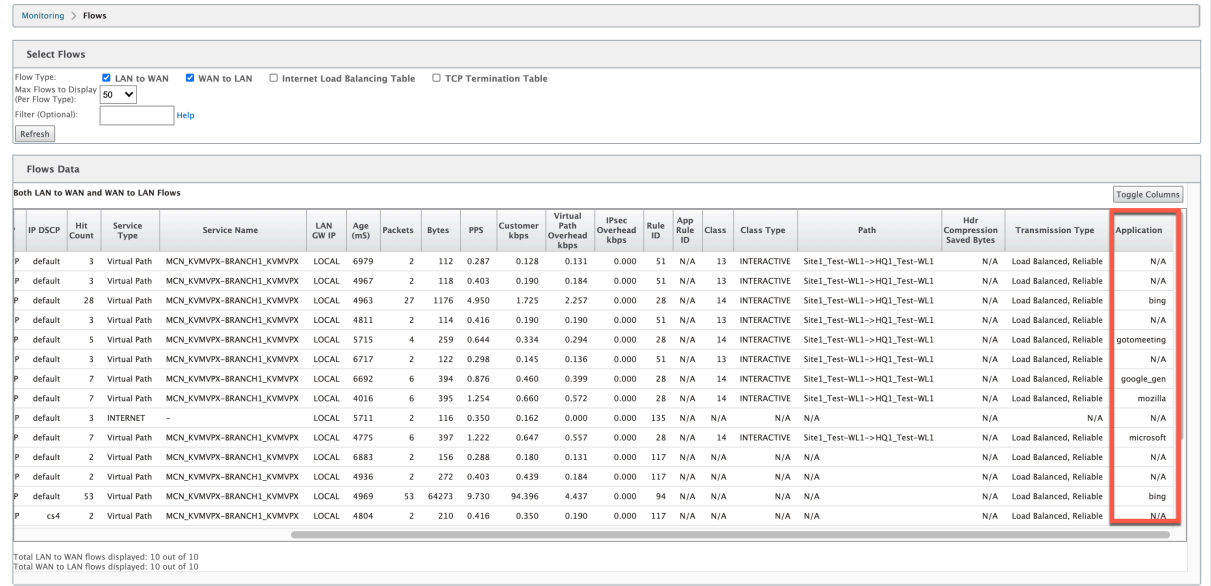
Connections Displayed: 19
Connections in Use: 13/128000

Wenn Sie die Anwendungsklassifizierung nicht aktivieren, zeigen die Spalten **Anwendung** und **Familie** keine Daten an.



Informationen zu Flows

Navigieren Sie im **Konfigurations-Editor** zu **Monitoring > Flows**. Im Abschnitt **“Flows Data”** werden in der Spalte **“Anwendung”** die Anwendungsdetails aufgeführt.



Anwendungsstatistiken

Navigieren Sie im **Konfigurations-Editor** zu **Monitoring > Statistiken**. Im Abschnitt **Anwendungsstatistiken** werden in der Spalte **Anwendung** die Anwendungsdetails aufgelistet.

| Application | Family | Bytes Received | Bytes Sent | Total Bytes |
|------------------------------------|--------|----------------|------------|-------------|
| Adobe | Web | 122923 | 41896 | 164819 |
| Akamai Technologies CDN | Web | 40935 | 87002 | 127937 |
| Amazon Ad System | Web | 25405 | 8439 | 33844 |
| Amazon Elastic Services | Web | 44130 | 13405 | 57535 |
| Amazon Web Services/Cloudfront CDN | Web | 12147 | 3804 | 20951 |
| Bing.com (formerly MSN Search) | Web | 914343 | 74913 | 989256 |
| BitChart Live Chat | Web | 224158 | 97936 | 322094 |
| Clicktale | Web | 323870 | 69287 | 393157 |

Problembehandlung

Nachdem Sie die Anwendungsklassifizierung aktiviert haben, können Sie die Berichte im Abschnitt **Überwachung** anzeigen und sicherstellen, dass sie Anwendungsdetails anzeigen. Weitere Informationen finden Sie unter [Anwendungsklassifizierung anzeigen](#).

Wenn ein unerwartetes Verhalten vorliegt, sammeln Sie das STS-Diagnosepaket, während das Problem beobachtet wird, und teilen Sie es mit dem Citrix Supportteam.

Das STS-Paket kann mit **Konfiguration > Systemwartung > Diagnose > Diagnoseinformationen** erstellt und heruntergeladen werden.

QoS Fairness (ROT)

May 10, 2021

Die QoS-Fairness-Funktion verbessert die Fairness mehrerer virtueller Pfadflüsse, indem QoS-Klassen und Random Early Detection (RED) verwendet werden. Ein virtueller Pfad kann einer von 16 verschiedenen Klassen zugewiesen werden. Eine Klasse kann einer von drei Grundtypen sein:

- Echtzeitklassen dienen Datenverkehrsflüssen, die einen Prompt-Dienst bis zu einer bestimmten Bandbreite benötigen. Niedrige Latenz wird gegenüber dem aggregierten Durchsatz bevorzugt.
- Interaktive Klassen haben eine geringere Priorität als in Echtzeit, haben jedoch absolute Priorität gegenüber Massenverkehr.
- Massenklassen erhalten, was von Echtzeit- und interaktiven Klassen übrig bleibt, da Latenz für Massenverkehr weniger wichtig ist.

Benutzer geben unterschiedliche Bandbreitenanforderungen für verschiedene Klassen an, wodurch der virtuelle Pfadplaner konkurrierende Bandbreitenanforderungen aus mehreren Klassen desselben Typs verlegen kann. Der Scheduler verwendet den Algorithmus Hierarchical Fair Service Curve (HFSC), um Fairness zwischen den Klassen zu erreichen.

HFSC Serviceklassen in FIFO-Reihenfolge (FIFO). Vor dem Planen von Paketen untersucht Citrix SD-WAN den für die Paketklasse ausstehenden Datenverkehr. Wenn übermäßiger Datenverkehr aussteht, werden die Pakete nicht in die Warteschlange gestellt (Tail Dropping).

Warum verursacht TCP Warteschlangen?

TCP kann nicht steuern, wie schnell das Netzwerk Daten übertragen kann. Zur Steuerung der Bandbreite implementiert TCP das Konzept eines Bandbreitenfensters, d. h. der Menge des nicht bestätigten Datenverkehrs, den es im Netzwerk zulässt. Es beginnt zunächst mit einem kleinen Fenster und verdoppelt die Größe dieses Fensters, wenn Bestätigungen empfangen werden. Dies wird als langsame Start- oder exponentielle Wachstumsphase bezeichnet.

TCP identifiziert Netzwerküberlastung durch Erkennung von verlorenen Paketen. Wenn der TCP-Stack einen Burst von Paketen sendet, die eine Verzögerung von 250 ms einführen, erkennt TCP keine Überlastung, wenn keines der Pakete verworfen wird, sodass die Größe des Fensters weiter vergrößert wird. Möglicherweise wird dies weiter getan, bis die Wartezeit 600—800 ms erreicht.

Wenn TCP sich nicht im langsamen Startmodus befindet, reduziert es die Bandbreite um die Hälfte, wenn Paketverlust erkannt wird, und erhöht die zulässige Bandbreite für jede empfangene Bestätigung um ein Paket. TCP wechselt daher zwischen dem Aufwärtsdruck auf die Bandbreite und dem Absetzen. Wenn die Wartezeit 800 ms durch den Zeitpaketverlust erkannt wird, verursacht die Bandbreitenreduzierung eine Übertragungsverzögerung.

Auswirkungen auf QoS-Fairness

Wenn TCP-Übertragungsverzögerung eintritt, ist die Bereitstellung jeglicher Art von Fairnessgarantie innerhalb einer virtuellen Pfadklasse schwierig. Der virtuelle Pfadplaner muss Tail-Drop-Verhalten anwenden, um zu vermeiden, dass enorme Datenmengen gehalten werden. Die Art von TCP-Verbindungen ist so, dass eine kleine Anzahl von Datenverkehr fließt, um den virtuellen Pfad zu füllen, was es für eine neue TCP-Verbindung schwierig macht, einen fairen Anteil der Bandbreite zu erreichen. Für die gemeinsame Nutzung der Bandbreite muss sichergestellt werden, dass die Bandbreite für neue Pakete verfügbar ist, die übertragen werden sollen.

Zufällige Früherkennung

Random Early Detection (RED) verhindert, dass Verkehrswarteschlangen gefüllt werden und dass Tail-Drop-Aktionen ausgelöst werden. Es verhindert unnötige Warteschlangen durch den virtuellen Pfadplaner, ohne den Durchsatz zu beeinträchtigen, den eine TCP-Verbindung erreichen kann.

Wie benutzt man RED?

1. Starten Sie eine TCP-Sitzung, um den virtuellen Pfad zu erstellen. Stellen Sie sicher, dass bei aktivierter RED die Wartezeit für diese Klasse bei etwa 50 ms im stationären Zustand bleibt.
2. Starten Sie eine zweite TCP-Sitzung, und stellen Sie sicher, dass beide TCP-Sitzungen die Bandbreite des virtuellen Pfades gleichmäßig teilen. Stellen Sie sicher, dass die Wartezeit in der Klasse im stationären Zustand bleibt.
3. Stellen Sie sicher, dass der Konfigurations-Editor zum Aktivieren und Deaktivieren von RED verwendet werden kann und dass der korrekte Wert für den Parameter angezeigt wird.
4. Stellen Sie sicher, dass auf der Seite Konfiguration anzeigen auf der Seite SD-WAN GUI angezeigt wird, ob RED für eine Regel aktiviert ist.

So aktivieren Sie RED

1. Navigieren Sie zu **Konfigurations-Editor > Verbindungen > Virtuelle Pfade > [Virtuellen Pfad]** auswählen > **Regeln** > Regel auswählen, zum Beispiel; **(VOIP)**.
2. Erweitern Sie den Bereich **LAN zu WAN**. Klicken Sie unter **LAN-zu-WAN-Abschnitt** auf das Kontrollkästchen **RED aktivieren**, um es für TCP-basierte Regeln zu aktivieren.

Virtual Path to Site: NSSDWANVPX_MCN-NSSDWAN1kBranch Section: Rules + Add Virtual Path Delete Virtual Path

| Order | Rule Group Name | IP Address | | | Protocol | Protocol # | Port | | | DSC |
|-------|-----------------|---------------|-------------------------------------|------|----------|------------|--------|-------------------------------------|------|-----|
| | | Source | Dest=Src | Dest | | | Source | Dest=Src | Dest | |
| 100 | IPERF | 10.102.29.3/5 | <input checked="" type="checkbox"/> | * | Any | 0 | * | <input checked="" type="checkbox"/> | * | Any |

Initialize Properties Using Protocol

WAN General

LAN to WAN

General

Class: <Default>

Drop Limit (ms): 50 Drop Depth: 128000

Large Packet Size (bytes): 0

☒ Enable RED

Large Packets

Drop Limit (ms): 0 Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0 Disable Depth (bytes): 128000

MPLS-Warteschlangen

May 10, 2021

Diese Funktion vereinfacht das Erstellen von SD-WAN-Konfigurationen beim Hinzufügen einer Multiprotocol Layer Switching (MPLS) WAN-Link. Zuvor musste für jede MPLS-Warteschlange ein WAN-Link erstellt werden. Jeder WAN-Link erforderte eine eindeutige virtuelle IP-Adresse (VIP), um die WAN-Link zu erstellen, und ein eindeutiges DSCP-Tag (Differentiated Services Code Point), das dem Warteschlangenschema des Anbieters entspricht. Nach dem Definieren einer WAN-Link für jede MPLS-Warteschlange wird der Intranetdienst definiert, der einer bestimmten Warteschlange zugeordnet werden soll.

Derzeit ist eine neue MPLS-spezifische WAN-Link-Definition (d. h. Zugriffstyp) verfügbar. Wenn ein neuer privater MPLS-Zugriffstyp ausgewählt ist, können Sie die MPLS-Warteschlangen definieren, die der WAN-Verbindung zugeordnet sind. Dies ermöglicht eine einzelne VIP mit mehreren DSCP-Tags, die der Warteschlangenimplementierung des Anbieters für den MPLS WAN-Link entsprechen. Dadurch wird der Intranetdienst mehreren MPLS-Warteschlangen auf einer einzelnen MPLS-WAN-Link zugeordnet.

Ermöglicht MPLS-Anbietern, Datenverkehr basierend auf DSCP-Markierungen zu identifizieren, sodass die Dienstklasse vom Anbieter angewendet werden kann.

Hinweis

Wenn Sie bereits MPLS-Konfigurationen haben und den privaten MPLS-Zugriffstyp implementieren möchten, wenden Sie sich an den Citrix Support, um Unterstützung zu erhalten.

Konfigurieren von privaten MPLS-WAN-Links

1. Definieren Sie den WAN-Link-Zugriffstyp als Privates MPLS.
2. Definieren Sie die MPLS-Warteschlangen, die den Service Provider MPLS-Warteschlangen entsprechen.
3. Aktivieren Sie den WAN-Link für den virtuellen Pfaddienst (standardmäßig aktiviert für Private MPLS-WAN-Links).
4. Weisen Sie im virtuellen Pfad einer WAN-Link eine Autopath-Gruppe zu.

Hinweis

Wenn die Autopath-Gruppe von der WAN-Link-Ebene zugewiesen wird, erstellt SD-WAN automatisch Pfade zwischen den MCN- und Client-MPLS-Warteschlangen basierend auf übereinstimmenden DSCP-Tags. Wenn die Autopath-Gruppe von der MPLS-

Warteschlangenebene zugewiesen wird, erstellt SD-WAN automatisch Pfade, unabhängig davon, ob die DSCP-Tags übereinstimmen.

5. Stellen Sie sicher, dass dieselbe Autopath-Gruppe am MCN und Client konfiguriert ist.
6. Stellen Sie sicher, dass die Pfade für die WAN-Link automatisch erstellt werden.
7. Weisen Sie den Intranetdienst bei Bedarf einer bestimmten Warteschlange zu.

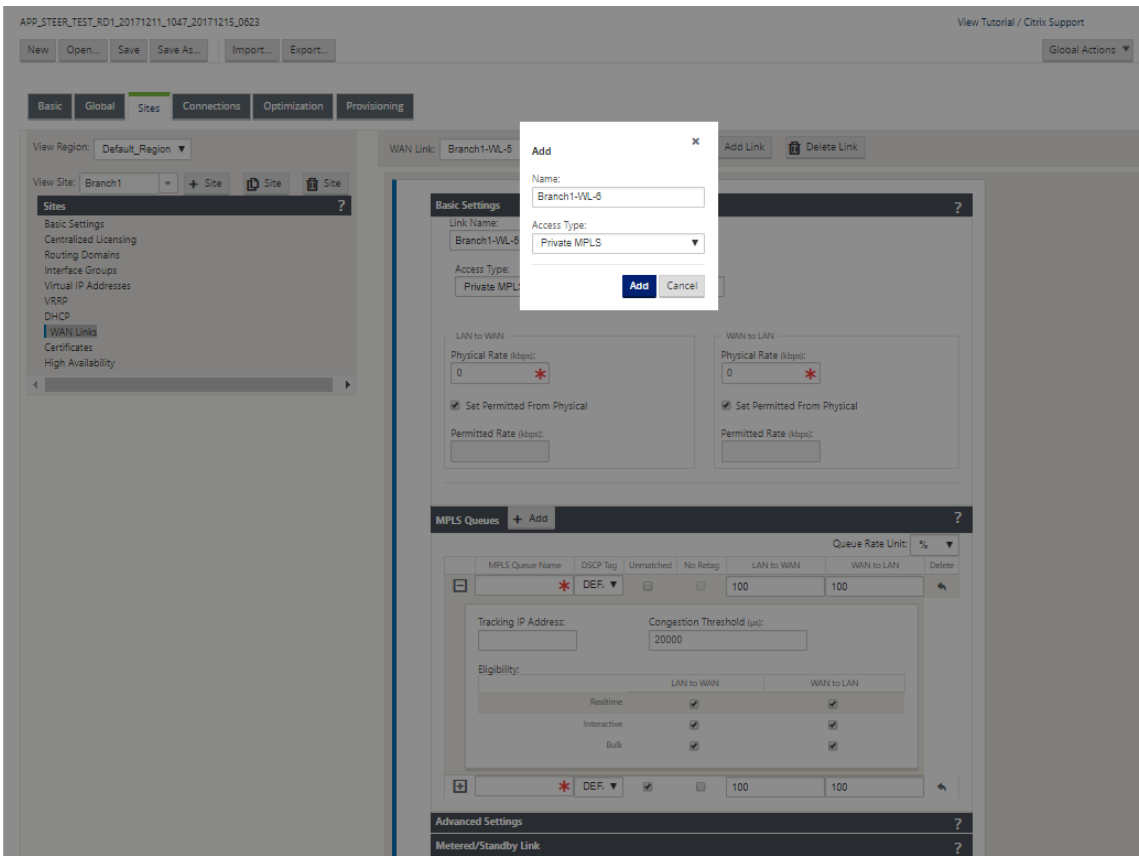
Hinweis

Die SD-WAN-Konfiguration verfügt möglicherweise nicht über eine Eins-zu-Eins-Zuordnung für anbieterbasierte Warteschlangen. Dies basiert auf bestimmten Bereitstellungsszenarien. Sie können keine Autopath-Gruppen zwischen verschiedenen privaten Zugriffstypen erstellen. Beispielsweise können Sie keine Autopath-Gruppen zwischen einem privaten Internetzugriffstyp und einem privaten MPLS-Zugriffstyp erstellen.

So fügen Sie privaten MPLS WAN LINK hinzu

So konfigurieren Sie einen neuen WAN-Link-Zugriffstyp für private MPLS:

1. Navigieren Sie im Konfigurations-Editor zu **Sites > [Site-Name] > WAN-Links**. Klicken Sie auf **Link hinzufügen**. Geben Sie den WAN-Link-Namen ein, und wählen Sie **Privates MPLS** als Zugriffstyp aus.



2. Unter den **Grundeinstellung** gibt es jetzt eine neue Registerkarte **MPLS-Warteschlangen**. Klicken Sie auf + Hinzufügen, um bestimmte MPLS-Warteschlangen hinzuzufügen. Diese sollten mit den vom Dienstanbieter definierten Warteschlangen übereinstimmen.

| Feld | Beschreibung |
|----------------------------------|--|
| MPLS-Warteschlangenname | Der Name der MPLS-Warteschlange |
| DSCP-Tag | Die DSCP-Tag-Einstellung des Dienstanbieters für die Warteschlange. |
| Unübertroffen | Wenn diese Option aktiviert ist, werden alle ankommenden Frames, die nicht mit den definierten Tags in der Konfigurationsdatei übereinstimmen, dieser Warteschlange zugeordnet und die Bandbreite für diese Warteschlange definiert. |
| LAN-zu-WAN-Zulässige Rate (kbps) | Die Bandbreite, die SD-WAN-Geräte für den Upload verwenden dürfen, die die definierte physische Upload-Rate des WAN-Link nicht überschreiten darf. |

| Feld | Beschreibung |
|----------------------------------|--|
| Zulässige WAN-zu-WAN-Rate (kbps) | Die Bandbreite, die SD-WAN-Geräte zum Herunterladen verwenden dürfen, die die definierte physische Downloadrate des WAN-Link nicht überschreiten darf. |

Erweitern Sie die MPLS-Queue-Definition (durch Klicken auf das +), und weitere Optionen werden angezeigt. Zu diesen Optionen gehören:

| Feld | Beschreibung |
|---------------------------|---|
| Verfolgung der IP-Adresse | WAN-Link-Tracking-Adresse |
| Überlastungsschwelle | Die definierte Zeitspanne für Staus (in Mikrosekunden), nach der die MPLS-Warteschlange die Paketübertragung drosselt, um mehr Staus zu vermeiden. Wenn die Überlastung den festgelegten Schwellenwert überschreitet, sichert SD-WAN die Senderate ab. |
| Berechtigung | Die Berechtigung der MPLS-Queue zur Verarbeitung bestimmter Verkehrsklassen. Wenn die Berechtigung für eine bestimmte Klasse von Datenverkehr deaktiviert ist, ist es unwahrscheinlich, dass diese Klasse von Datenverkehr durch die MPLS-Warteschlange weitergeleitet wird, es sei denn, die Netzwerkbedingungen erfordern dies. |

Konfigurieren Sie die MPLS-Warteschlangen, die den vorhandenen WAN-Link-Warteschlangendefinitionen für Service Provider entsprechen.

Hinweis

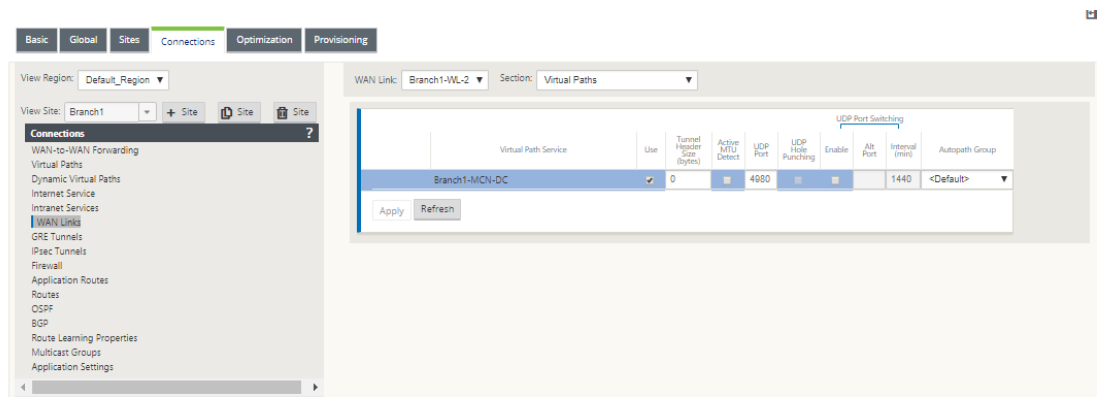
Vorhandene MPLS-WAN-Links, die vor SD-WAN 9.1 konfiguriert wurden, sind nicht betroffen.

Definieren von WAN-Link-Eigenschaften für private MPLS

Sobald die Private MPLS WAN-Link mit ihren MPLS-Warteschlangen definiert ist, sollten Sie eine Autopath-Gruppe für den WAN-Link unter einer bestimmten Definition des virtuellen Pfads zuweisen.

So weisen Sie Autopath-Gruppe zu:

1. Gehen Sie zu **Verbindungen** > **[Site-Name]** > **WAN-Links** > **[MPLS WAN-Verbindungsname]** > **Virtuelle Pfade** > **[Name des virtuellen Pfads]** > **[Lokale Website]** > **WAN-Links** und klicken Sie auf **Bearbeiten** ().
2. Klicken Sie auf das Dropdownmenü **Autopath Group** und wählen Sie eine der verfügbaren Gruppen aus. Standardmäßig erben MPLS-Warteschlangen die der MPLS-WAN-Link zugewiesene Autopath-Gruppe. Sie können die einzelnen MPLS-Queues so einstellen, dass die gewählte Autopath-Gruppe übernommen wird, oder eine Alternative aus dem Dropdownmenü Autopath-Gruppe für jede MPLS-Queue auswählen.



Hinweis

Wenn zwischen Warteschlangen am lokalen Standort und dem Remotestandort keine 1:1-Zuordnung basierend auf dem DSCP-Tag besteht, müssen Sie MPLS-Queues bestimmten Autopath-Gruppen zuordnen. Durch das Erben einer Autopath-Gruppe vom MPLS-WAN-Link werden automatisch Pfade zwischen Warteschlangen mit passenden DSCP-Tags generiert.

Zuweisen einer Autopath-Gruppe zu virtuellem Pfad-WAN-Link

Die definierte Autopath-Gruppe ist für die MCN und die Client-Appliance identisch. Dadurch kann das System die Pfade automatisch erstellen. Am MCN-Standort können Sie auch den mit dem virtuellen Pfad verknüpften WAN-Link erweitern.

Zulässige Rate und Überlastung für WAN-Verbindungen anzeigen

Mit der SD-WAN-Weboberfläche können Sie nun die zulässige Rate für WAN-Links und WAN-Link-Usages anzeigen und ob sich ein WAN-Link, ein Pfad oder ein virtueller Pfad im überlasteten Zustand befindet. In den vorherigen Versionen waren diese Informationen nur in SD-WAN-Protokolldateien

und über die CLI verfügbar. Diese Optionen sind jetzt in der Weboberfläche verfügbar, um bei der Fehlerbehebung zu helfen.

Zulässige Rate anzeigen

Zulässige Rate ist die Bandbreite, die ein bestimmter WAN-Link, virtueller Pfaddienst, Intranetdienst oder Internetdienst zu einem bestimmten Zeitpunkt verwenden darf. Die zulässige Rate für eine WAN-Link ist statisch und wird explizit in der SD-WAN-Konfiguration definiert. Die zulässige Rate für einen Virtual Path Service, Intranet Service oder Internetdienst schwankt im Laufe der Zeit, als Reaktion auf Überlastung, Benutzernachfrage und faire Freigaben, aber immer größer als oder gleich der minimalen reservierten Bandbreite für den Dienst.

WAN-Link überwachen

Gehen Sie zu **Monitor Statistiken** und wählen Sie **WAN-Link** aus der Dropdown-Liste **Anzeigen** aus.

Monitoring > Statistics

Statistics

Show: WAN Link ☒ Enable Auto Refresh 5 seconds ☒ Show latest data. Processing...

WAN Link Statistics

Filter: in Any column

Show 100 entries Showing 1 to 6 of 6 entries

First Previous 1 Next Last

| WAN Link | Access Interface | IP Address | Proxy Address | Proxy ARP State | MAC | Last ARP Reply Age (ms) |
|---------------|------------------|---------------|---------------|-----------------|-----|-------------------------|
| Client-1-WL-1 | N/A | 172.186.10.75 | N/A | N/A | N/A | N/A |
| Client-1-WL-2 | N/A | 172.186.20.75 | N/A | N/A | N/A | N/A |
| Client-2-WL-1 | N/A | 172.186.70.50 | N/A | N/A | N/A | N/A |
| Client-2-WL-2 | N/A | 172.186.80.50 | N/A | N/A | N/A | N/A |
| DC-WL-1 | DC-WL-1-AI-1 | 172.186.30.85 | N/A | DISABLED | N/A | N/A |
| DC-WL-2 | DC-WL-2-AI-1 | 172.186.40.85 | N/A | DISABLED | N/A | N/A |

Showing 1 to 6 of 6 entries

First Previous 1 Next Last

Virtual Path Service Data Rates

Filter: in Any column

Show 100 entries Showing 1 to 4 of 4 entries

First Previous 1 Next Last

| Name | Direction | Virtual Path Service Packets | Virtual Path Service kB | Delta Virtual Path Service Packets | Delta Virtual Path Service kB | Virtual Path Service kbps | IP,TCP,UDP Header Compression Bytes Saved |
|---------|-----------|------------------------------|-------------------------|------------------------------------|-------------------------------|---------------------------|---|
| DC-WL-1 | Recv | 2618687 | 195069.42 | 289 | 26.16 | 37.81 | 0 |

Gehen Sie zu **Monitor > Statistiken** und wählen Sie in der Dropdown-Liste **Anzeigen** die Option **WAN-Link-Nutzung** aus.

Statistics

Show

WAN Link Usage

Enable Auto Refresh

5

seconds

Stop

Show latest data

Processing...

WAN Link Usage Statistics

Local WAN Links

Filter

in

Any column

Apply

Show

100

entries

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

| WAN Link | Direction | Packets | Delta Packets | Delta KB | Kbps | Permitted Kbps | Congestion |
|----------|-----------|---------|---------------|----------|-------|----------------|------------|
| DC-WG-1 | Send | 2551622 | 238 | 17.69 | 28.24 | 100000 | N/A |
| DC-WG-1 | Recv | 2630429 | 240 | 21.87 | 35.38 | 80000 | NO |
| q1 | Send | 2358231 | 312 | 20.84 | 33.77 | 50000 | N/A |
| q1 | Recv | 2366461 | 308 | 18.26 | 29.74 | 49000 | NO |
| q2 | Send | 118164 | 306 | 16.32 | 26.77 | 50000 | N/A |
| q2 | Recv | 128766 | 321 | 19.88 | 32.21 | 49000 | NO |

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

Usage and Permitted Rates

Filter

in

Any column

Apply

Show

100

entries

Showing 1 to 14 of 14 entries

First

Previous

1

Next

Last

| WAN Link | Service | Direction | Packets | Packets KB | Delta Packets | Delta KB | Kbps | Permitted Kbps | Congestion |
|----------|-------------------|-----------|---------|------------|---------------|----------|-------|----------------|------------|
| DC-WG-1 | DC-Client-1 | Recv | 1473996 | 134889.42 | 118 | 10.8 | 16.99 | 14481.65 | NO |
| DC-WG-1 | DC-Client-2 | Recv | 958409 | 71407.76 | 138 | 12.12 | 19.07 | 14490 | NO |
| DC-WG-1 | DC-Client-1 | Send | 1623618 | 108311624 | 134 | 10.34 | 16.27 | 14990 | N/A |
| DC-WG-1 | DC-Client-2 | Send | 690096 | 64771056 | 132 | 9.47 | 14.9 | 14990 | N/A |
| DC-WG-1 | Internet-Intranet | Send | 0 | 0 | 0 | 0 | 0 | 50020 | N/A |
| DC-WG-1 | Internet-Intranet | Recv | 208 | 55.25 | 0 | 0 | 0 | 49020 | N/A |
| q1 | DC-Client-1 | Recv | 1337987 | 96716.01 | 208 | 11.12 | 17.31 | 14510 | NO |
| q1 | DC-Client-2 | Recv | 821873 | 52380.57 | 106 | 7.4 | 11.64 | 14990 | NO |
| q1 | DC-Client-1 | Send | 1314280 | 97359168 | 210 | 10.51 | 21.26 | 23010 | N/A |
| q1 | DC-Client-2 | Send | 847803 | 57291606 | 109 | 7.33 | 11.88 | 14990 | N/A |
| q2 | DC-Client-1 | Recv | 91058 | 6260.83 | 237 | 15.83 | 24.94 | 14510 | NO |
| q2 | DC-Client-2 | Recv | 40378 | 2232.83 | 104 | 5.56 | 8.75 | 14990 | NO |
| q2 | DC-Client-1 | Send | 81296 | 4710784 | 208 | 11.12 | 17.31 | 23010 | N/A |
| q2 | DC-Client-2 | Send | 40353 | 2271700 | 105 | 5.81 | 8.83 | 14990 | N/A |

Showing 1 to 14 of 14 entries

First

Previous

1

Next

Last

Remote WAN Links

Filter

in

Any column

Apply

Show

100

entries

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

| WAN Link | Service | Direction | Congestion |
|---------------|-------------|-----------|------------|
| Client-1-WG-1 | DC-Client-1 | Recv | NO |
| Client-2-WG-1 | DC-Client-2 | Recv | NO |
| q3 | DC-Client-1 | Recv | NO |
| q4 | DC-Client-1 | Recv | NO |
| q5 | DC-Client-2 | Recv | NO |
| q6 | DC-Client-2 | Recv | NO |

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

MPLS-Warteschlangen überwachen

Gehen Sie zu **Überwachen Statistiken** und wählen Sie in der Dropdown-Liste **Anzeigen** die Option **MPLS-Warteschlangen** aus.

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

588

Show: MPLS Queues

☒ Enable Auto Refresh

5 seconds

Stop

☒ Show latest data.

MPLS Queue Statistics

Filter: in Any column

Apply

Show 100 entries Showing 1 to 4 of 4 entries Processing...

Private MPLS

| Private MPLS | MPLS Queue | Access Interface | IP Address | Proxy Address | Proxy ARP State | MAC | Last ARP Reply Age (ms) |
|-----------------|---------------|----------------------|---------------|---------------|-----------------|-----|-------------------------|
| EE-Branch1-WL-2 | SAMPLE-Queue1 | EE-Branch1-WL-2-AI-1 | 172.184.19.19 | N/A | DISABLED | N/A | N/A |
| EE-Branch1-WL-2 | SAMPLE-Queue2 | EE-Branch1-WL-2-AI-1 | 172.184.19.19 | N/A | DISABLED | N/A | N/A |
| VPX-DC-WL-2 | DC-Queue01 | N/A | 172.184.3.19 | 172.184.3.19 | N/A | N/A | N/A |
| VPX-DC-WL-2 | DC-Queue2 | N/A | 172.184.3.19 | 172.184.3.19 | N/A | N/A | N/A |

Showing 1 to 4 of 4 entries

Virtual Path Service Data Rates

Filter: in Any column

Apply

Show 100 entries Showing 1 to 4 of 4 entries

| Name | Direction | Virtual Path Service Packets | Virtual Path Service kB | Delta Virtual Path Service Packets | Delta Virtual Path Service kB | Virtual Path Service kbps | Mismatched DSCP Packets | Mismatched DSCP kB | IP/TCP/UDP Header Compression Bytes Saved |
|---------------|-----------|------------------------------|-------------------------|------------------------------------|-------------------------------|---------------------------|-------------------------|--------------------|---|
| SAMPLE-Queue1 | Recv | 14279 | 1177.77 | 251 | 20.72 | 33.15 | 5932 | 407.36 | 0 |
| SAMPLE-Queue1 | Send | 13400 | 919.09 | 217 | 14.47 | 23.15 | N/A | N/A | 0 |
| SAMPLE-Queue2 | Recv | 12806 | 705.61 | 216 | 11.84 | 18.95 | 5803 | 250.8 | 0 |
| SAMPLE-Queue2 | Send | 13953 | 915.39 | 241 | 16.73 | 26.77 | N/A | N/A | 0 |

Showing 1 to 4 of 4 entries

Problembehandlung bei MPLS-Warteschlangen

Um den Status von MPLS-Warteschlangen zu überprüfen, navigieren Sie zu **Überwachen > Statistiken** und wählen Sie in der Dropdown-Liste **Anzeigen** die Option **Pfade (Zusammenfassung)** aus. Im folgenden Beispiel befindet sich der Pfad von der MPLS-Warteschlange “q1”zu “q3”im Zustand DEAD und wird rot angezeigt. Der Pfad von der MPLS-Warteschlange “q1”zu “q5”befindet sich im Zustand GOOD und wird grün angezeigt.

Statistics

Show: Paths (Summary)

☒ Enable Auto Refresh

5 seconds

Stop

☒ Show latest data. Processing...

Path Statistics Summary

Filter:

in Any column

Apply

Show 100 entries

| Num | From Link | To Link | Path State | Virtual Path Service State | Virtual Path Service Type | BOWT | Jitter (mS) | Loss % | kbps | Congestion |
|-----|---------------|---------------|------------|----------------------------|---------------------------|------|-------------|--------|-------|------------|
| 1 | DC-WL-1 | Client-1-WL-1 | GOOD | GOOD | Static | 5 | 2 | 0.00 | 15.30 | NO |
| 2 | q1 | q3 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 12.53 | UNKNOWN |
| 3 | q1 | q4 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 8.92 | UNKNOWN |
| 4 | q2 | q3 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 8.92 | UNKNOWN |
| 5 | q2 | q4 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 8.92 | UNKNOWN |
| 6 | Client-1-WL-1 | DC-WL-1 | GOOD | GOOD | Static | 4 | 2 | 0.00 | 19.96 | NO |
| 7 | q3 | q1 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 8 | q3 | q2 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 9 | q4 | q1 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 10 | q4 | q2 | DEAD | GOOD | Static | 9999 | 0 | 0.00 | 0.00 | UNKNOWN |
| 11 | DC-WL-1 | Client-2-WL-1 | GOOD | GOOD | Static | 2 | 2 | 0.00 | 15.12 | NO |
| 12 | q1 | q5 | GOOD | GOOD | Static | 2 | 2 | 0.00 | 11.53 | NO |
| 13 | q2 | q6 | GOOD | GOOD | Static | 2 | 2 | 0.00 | 8.51 | NO |
| 14 | Client-2-WL-1 | DC-WL-1 | GOOD | GOOD | Static | 2 | 2 | 0.00 | 20.09 | NO |
| 15 | q5 | q1 | GOOD | GOOD | Static | 2 | 2 | 0.00 | 11.69 | NO |
| 16 | q6 | q2 | GOOD | GOOD | Static | 2 | 2 | 0.00 | 8.82 | NO |

Um detaillierte Informationen zu Pfaden zu erhalten, wählen Sie **Pfade (Detailliert)** aus der Dropdown-Liste **Anzeigen** aus. Die Informationen zu Pfaden wie Grund für den Zustand, Dauer, Quellport, Zielport, MTU sind

Im folgenden Beispiel befindet sich der Pfad von der MPLS-Warteschlange “q1”zu “q3”im Zustand DEAD und der Grund ist PEER. Der Pfad von der MPLS-Warteschlange “q3”zu “q1”ist tot und der Grund ist SILENCE. Die folgende Tabelle enthält die Liste der verfügbaren Gründe und deren Beschreibungen.

| Grund | Beschreibung |
|---------|--|
| GATEWAY | Der Pfad ist DEAD, da die Appliance das Gateway nicht erreichen oder erkennen kann |
| SILENCE | Der Pfad ist BAD oder DEAD, da die Appliance keine Pakete von der Peer-Site erhalten hat |
| LOSS | Der Pfad ist BAD aufgrund von Paketverlust |
| PEER | Die Peer-Site meldet, dass der Pfad BAD ist |

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 |

Um die mit den MPLS-Warteschlangen verknüpfte Zugriffsschnittstelle und IP-Adresse zu überprüfen, wählen Sie in der Dropdown-Liste **Anzeigen** die Option **Access Interfaces** aus.

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

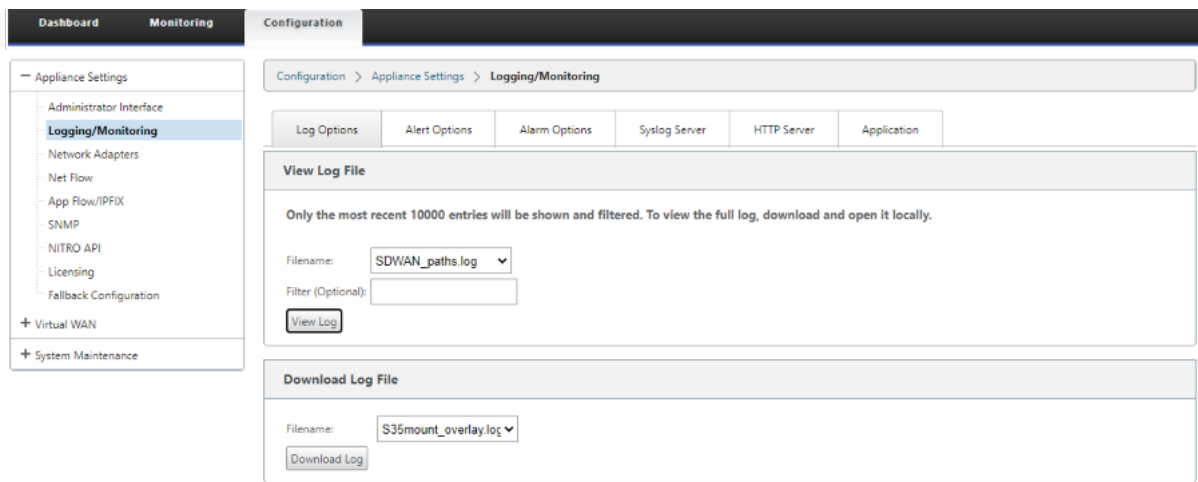
| WAN Link | Access Interface | Service Name | Direction | Virtual Path Service Packets | Virtual Path Service kB | Delta Virtual Path Service Packets | Delta Virtual Path Service kB | Virtual Path Service kbps | IP/TCP/UDP Header Compression Bytes Saved |
|----------|------------------|--------------|-----------|------------------------------|-------------------------|------------------------------------|-------------------------------|---------------------------|---|
| 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 |

Sie können die Protokolldateien zur weiteren Fehlerbehebung herunterladen. Navigieren Sie zu **Kon-**

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

591

figuration > Logging/Monitoring und wählen Sie auf der Registerkarte **Log-Optionen** die Option **SDWAN_paths.log** oder **SDWAN_common.log** aus.



Berichterstellung

May 10, 2021

[Anwendung QoE](#)

[Mehrere Net Flow Kollektoren](#)

Anwendung QoE

May 10, 2021

Application QoE ist ein Maß für die Qualität der Erfahrung von Anwendungen im SD-WAN-Netzwerk. Es misst die Qualität von Anwendungen, die durch die virtuellen Pfade zwischen zwei SD-WAN-Appliances fließen. Der **Anwendungs-QoE-Wert** ist ein Wert zwischen 0 und 10. Der Wertungsbereich, in den er fällt, bestimmt die Qualität einer Anwendung.

| Qualität | Bereich |
|----------|---------|
| Gut | 8–10 |
| Fair | 4–8 |
| Schlecht | 0–4 |

QualitätBereich

Anwendungs-QoE-Wert kann verwendet werden, um die Qualität von Anwendungen zu messen und problematische Trends zu identifizieren.

Sie können die Qualitätsschwellenwerte für Echtzeit- und interaktive Appliances mithilfe von QoE-Profilen definieren und diese Profile Anwendungen oder Anwendungsobjekten zuordnen.

Hinweis:

Um Application QoE zu überwachen, ist es wichtig, Deep Packet Inspection zu aktivieren. Weitere Informationen finden Sie unter [Anwendungsklassifizierung](#).

Echtzeit-Anwendung QoE

Die Applikations-QoE-Berechnung für Echtzeitanwendungen verwendet eine innovative Citrix Technik, die aus der MOS-Score abgeleitet wird.

Die Standardschwellenwerte sind:

- Latenzschwelle: 160 ms
- Jitter-Schwellenwert: 30 ms
- Paketverlustschwelle: 2%

Ein Fluss einer Echtzeitanwendung, der die Schwellenwerte für Latenz, Verlust und Jitter erfüllt, wird als von guter Qualität angesehen.

QoE für Echtzeitanwendungen wird anhand des Prozentsatzes der Flüsse ermittelt, die den Schwellenwert erreichen, dividiert durch die Gesamtzahl der Flussstichproben.

QoE für Echtzeit = (Anzahl von Flussproben, die den Schwellenwert erreichen/Gesamtzahl der Flussproben) * 100

Es wird als QoE-Score im Bereich von 0 bis 10.

Sie können QoE-Profile mit benutzerdefinierten Schwellenwerten erstellen und auf Anwendungen oder Anwendungsobjekte anwenden.

Hinweis:

Der QoE-Wert kann Null sein, wenn die Netzwerkbedingungen außerhalb der konfigurierten Schwellenwerte für den Echtzeitverkehr liegen.

Interaktive Anwendung QoE

Die Application QoE für interaktive Anwendungen verwendet eine innovative Citrix Technik, die auf Schwellenwerten für Paketverluste und Burstrate basiert.

Interaktive Anwendungen reagieren empfindlich auf Paketverlust und Durchsatz. Daher messen wir den Prozentsatz der Paketverluste und die Burstrate des Ein- und Auslaufverkehrs in einem Flow.

Die konfigurierbaren Schwellenwerte sind:

- Prozentsatz der Paketverluste.
- Prozentsatz der erwarteten Egress-Burstrate im Vergleich zur Ingress-Burstrate.

Die Standardschwellenwerte sind:

- Schwellenwert für Paketverlust: 1%
- Burstrate: 60%

Ein Fluss ist von guter Qualität, wenn folgende Bedingungen erfüllt sind:

- Der prozentuale Verlust für einen Flow ist geringer als der konfigurierte Schwellenwert.
- Die ausgehende Burstrate entspricht mindestens dem konfigurierten Prozentsatz der eingehenden Burstrate.

Konfigurieren der Anwendung QoE

Ordnen Sie Anwendungs- oder Anwendungsobjekte Standard- oder benutzerdefinierten QoE-Profilen zu.

Sie können benutzerdefinierte QoE-Profile für Echtzeit- und interaktiven Datenverkehr erstellen.

So erstellen Sie benutzerdefinierte QoE-Profile:

1. Navigieren Sie im Konfigurations-Editor zu **Global > Application QoE > QoE Profile**, und klicken Sie auf **+**.
2. Geben Sie den Wert für die folgenden Parameter ein:
 - **Profilname:** Ein Name zur Identifizierung des Profils, das Schwellenwerte für Echtzeit- und interaktive Datenverkehr festlegt.
 - **Echtzeit:** Konfigurieren Sie Schwellenwerte für Datenverkehrsflüsse, die die QoS-Richtlinie in Echtzeit treffen. Ein Fluss einer Echtzeitanwendung, der die Schwellenwerte für Latenz, Verlust und Jitter erfüllt, wird als von guter Qualität angesehen.
 - **Einwege-Latenz:** Der Latenzschwellenwert in Millisekunden. Der Standard-QoE-Profilwert ist 160 ms.

- **Jitter:** Die Jitterschwelle in Millisekunden. Der Standard-QoE-Profilwert ist 30 ms.
- **Paketverlust:** Der Prozentsatz des Paketverlustes. Der Standard-QoE-Profilwert beträgt 2%.
- **Interaktiv:** Konfigurieren Sie Schwellenwerte für Datenverkehrsflüsse, die die interaktive QoS-Richtlinie treffen. Ein Fluss einer interaktiven Anwendung, die den Schwellenwert für Burst-Verhältnis und Paketverlust erfüllt, wird als von guter Qualität angesehen.
 - **Erwartete Burstrate:** Der Prozentsatz der erwarteten Burstrate. Die ausgehende Burstrate sollte mindestens der konfigurierte Prozentsatz der eingehenden Burstrate sein. Der Standard-QoE-Profilwert ist 60%.
 - **Paketverlust pro Fluss:** Der Prozentsatz des Paketverlustes. Der Standard-QoE-Profilwert ist 1%.

Section: QoE Profiles ▼

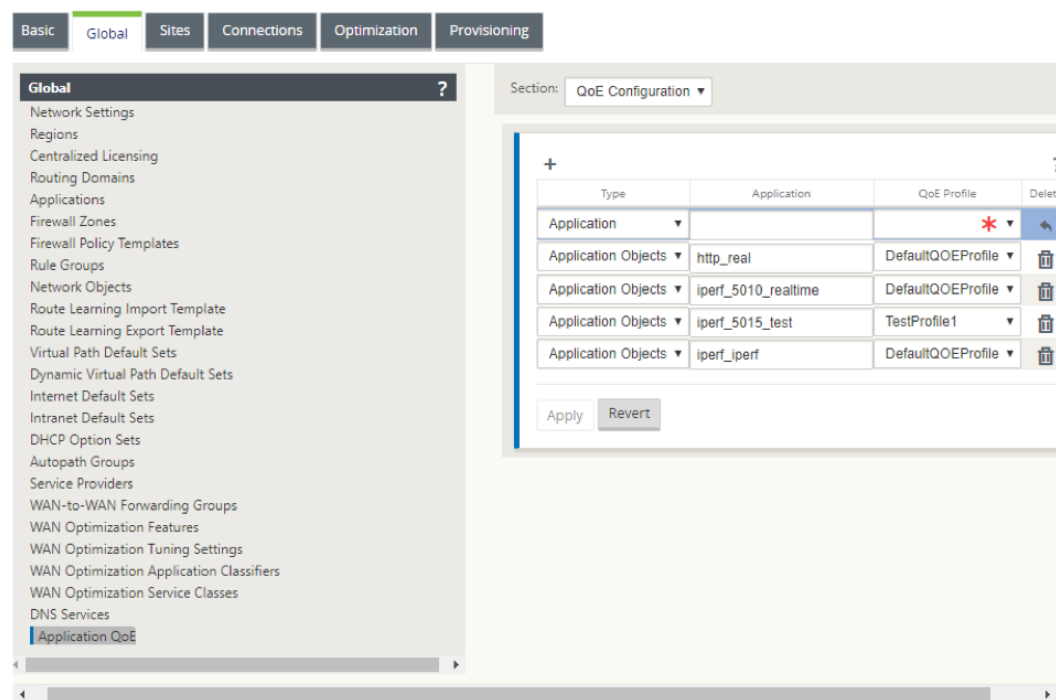
| Profile Name | Realtime | | | Interactive | | Delete |
|-------------------|----------------------|-------------|-----------------|-------------------------|--------------------------|--------|
| | One Way Latency (ms) | Jitter (ms) | Packet Loss (%) | Expected Burst Rate (%) | Packet loss per flow (%) | |
| TestProfile2 | 190 | 30 | 3.0 | 60.0 | 1.0 | |
| DefaultQOEProfile | 160 | 30 | 2.0 | 60.0 | 1.0 | |
| TestProfile1 | 170 | 30 | 2.0 | 60.0 | 2.0 | |

Apply **Revert**

3. Klicken Sie auf **Übernehmen**.

So ordnen Sie Anwendungen oder Anwendungsobjekte mit QoE-Profilen zu:

1. Navigieren Sie im Konfigurations-Editor zu **Global > Application QoE > QoE Configuration**, und klicken Sie auf **+**.
2. Wählen Sie Werte für die folgenden Parameter:
 - **Typ:** Eine DPI-Anwendung oder ein Anwendungsobjekt.
 - **Anwendung:** Suchen Sie ein Anwendungs- oder Anwendungsobjekt basierend auf dem ausgewählten Typ und wählen Sie es aus.
 - **QoE-Profil:** Wählen Sie ein QoE-Profil aus, das dem Anwendungs- oder Anwendungsobjekt zugeordnet werden soll.



3. Klicken Sie auf **Übernehmen**.

Sie können bis zu 10 Anwendungen oder Anwendungsobjekte mit QoE-Profilen zuordnen. Sie können die Application QoE-Berichte im SD-WAN Center anzeigen. Weitere Informationen finden Sie im [Anwendungs-QoE-Bericht](#) Bericht.

HDX QoE

May 10, 2021

Netzwerkparameter wie Latenz, Jitter und Paketabfall beeinflussen die Benutzererfahrung von HDX-Benutzern. Quality of Experience (QoE) wird eingeführt, um den Benutzern zu helfen, ihre ICA-Erfahrung zu verstehen und zu überprüfen. QoE ist ein berechneter Index, der die ICA-Verkehrsleistung angibt. Die Benutzer können die Regeln und Richtlinien optimieren, um die QoE zu verbessern.

Der QoE ist ein numerischer Wert zwischen 0 und 100, je höher der Wert, desto besser die Benutzererfahrung. QoE ist standardmäßig für alle ICA/HDX-Anwendungen aktiviert.

Die Parameter, die zur Berechnung der QoE verwendet werden, werden zwischen den beiden SD-WAN-Appliances auf Client- und Serverseite gemessen und nicht zwischen dem Client oder den Server-Appliances selbst gemessen. Latenz, Jitter und Paketabfall werden auf der Flusstufe

gemessen und kann sich von den Statistiken auf der Linkebene unterscheiden. Die Endhostanwendung (Client oder Server) weiß möglicherweise nie, dass ein Paketverlust im WAN vorliegt. Wenn die erneute Übertragung erfolgreich ist, ist die Paketverlustrate des Flusspegels niedriger als der Verlust der Verbindungsebene. Infolgedessen kann es die Latenz und den Jitter etwas erhöhen.

Die Standardkonfiguration für HDX-Datenverkehr ermöglicht SD-WAN die erneute Übertragung von Paketen. Dadurch wird der QoE-Indexwert verbessert, der aufgrund von Paketverlust im Netzwerk verloren gegangen ist.

Im Dashboard des SD-WAN Centers können Sie eine grafische Darstellung der Gesamtqualität von HDX-Anwendungen anzeigen. Die HDX-Anwendungen werden in die folgenden drei Qualitätskategorien eingeteilt:

| Qualität | QoE-Reihe |
|----------|-----------|
| Gut | 80–100 |
| Fair | 50–80 |
| Schlecht | 0–50 |

Eine Liste der fünf unteren Standorte mit der geringsten QoE wird ebenfalls im Citrix SD-WAN Center-Dashboard angezeigt.

Eine grafische Darstellung des QoE für unterschiedliche Zeitintervalle ermöglicht es Ihnen, die Leistung von HDX-Anwendungen an jedem Standort zu überwachen.

Weitere Informationen finden Sie unter [SD-WAN Center Dashboard](#).

Sie können auch die detaillierten HDX-Berichte der einzelnen Standorte im Citrix SD-WAN Center anzeigen. Weitere Informationen, siehe [HDX-Berichte](#).

Hinweis

- *Erwarten Sie nicht, dass die WAN-Latenz, der Jitter und das Paketablegen immer mit der Anwendungslatenz, dem Jitter und dem Paketabfall übereinstimmen. Der WAN-Link-Verlust korreliert mit dem tatsächlichen WAN-Paketverlust, während der Anwendungsverlust nach der erneuten Übertragung liegt, was niedriger ist als der Verlust von WAN-Verbindungen.*
- *Die WAN-Latenz, die in der GUI angezeigt wird, ist BOWT (Best One Way Time). Es sind die besten Metriken des Links als Mittel, um die Gesundheit der Verbindung zu messen. Die Anwendung QoE verfolgt und berechnet die Gesamt- und durchschnittliche Latenz aller Pakete für diese Anwendung. Dies stimmt oft nicht mit dem Link BOWT überein.*
- *Wenn eine MSI-Sitzung während des ICA-Handshake gestartet wird, wird die Sitzung möglicherweise vorübergehend als 4 SSI statt 1 MSI gezählt. Nachdem der Handshake abgeschlossen ist, wird er zu 1 MSI konvergieren. Wenn die Konvertierung erfolgt, bevor*

die SQL-Tabelle aktualisiert wird, wird sie möglicherweise für diese Minute in ICA_Summary angezeigt.

- Bei der erneuten Verbindung der Sitzung, da die anfänglichen Protokollinformationen nicht ausgetauscht werden, ist SD-WAN nicht in der Lage, MSI zu identifizieren, daher wird jede Verbindung als SSI-Informationen gezählt.*
- Bei UDP-Verbindungen kann es nach dem Schließen der Verbindung bis zu 5 Minuten dauern, bis die Verbindung in ICA_Summary als geschlossen und aktualisiert angezeigt wird. Bei TCP-Verbindungen kann es nach dem Schließen der Verbindung bis zu 2 Minuten dauern, bis die Anzeige in ICA_Summary als geschlossen angezeigt wird.*
- QoE von TCP-Sitzungen und UDP-Sitzungen sind möglicherweise nicht auf demselben Pfad identisch, da sich zwischen TCP und UDP unterscheiden.*
- Wenn ein Benutzer zwei virtuelle Desktops startet, wird die Anzahl der Benutzer als zwei gezählt.*

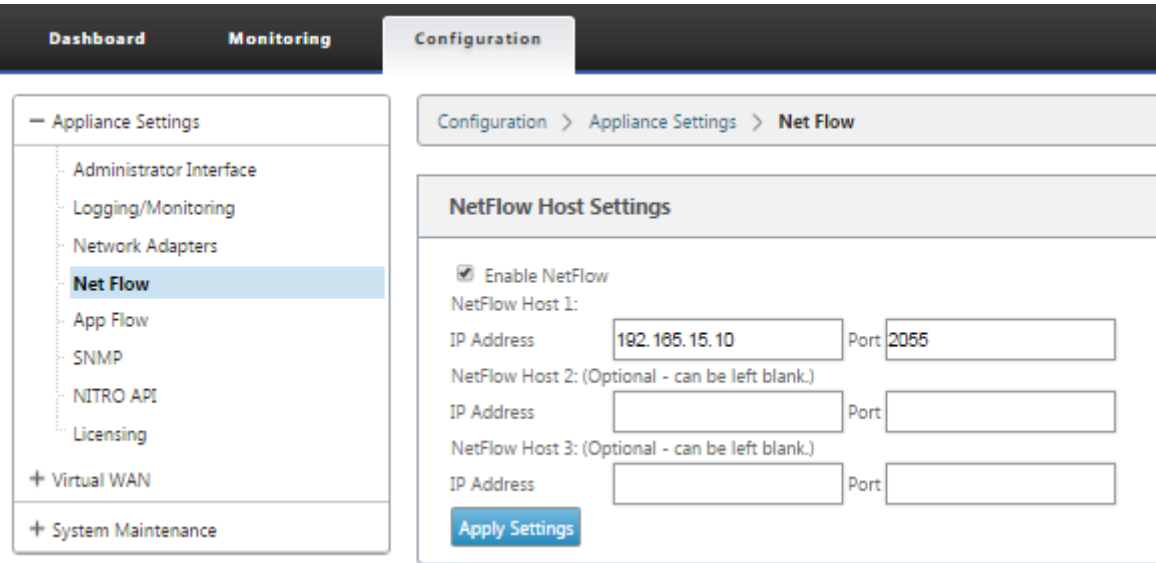
Mehrere Net Flow Kollektoren

October 28, 2021

Net Flow Collectors erfassen IP-Netzwerkverkehr, wenn er in eine SD-WAN-Schnittstelle eintritt oder diese verlässt. Durch die Analyse der von Net Flow bereitgestellten Daten können Sie die Quelle und das Ziel des Datenverkehrs, die Serviceklasse und die Ursachen für Verkehrsstaus ermitteln. Citrix SD-WAN-Geräte können so konfiguriert werden, dass sie grundlegende statistische Daten der Net Flow-Version 5 an den konfigurierten Net Flow-Collector senden. Citrix SD-WAN bietet Net Flow-Unterstützung für Verkehrsflüsse, die durch das transportzuverlässige Protokoll verdeckt werden. Geräte am WAN-Rand der Lösung verlieren die Fähigkeit, Net Flow-Datensätze zu sammeln, da nur die mit SD-WAN gekapselten UDP-Pakete angezeigt werden. Net Flow wird auf den Citrix SD-WAN Standard und Premium (Enterprise) Edition-Appliances unterstützt.

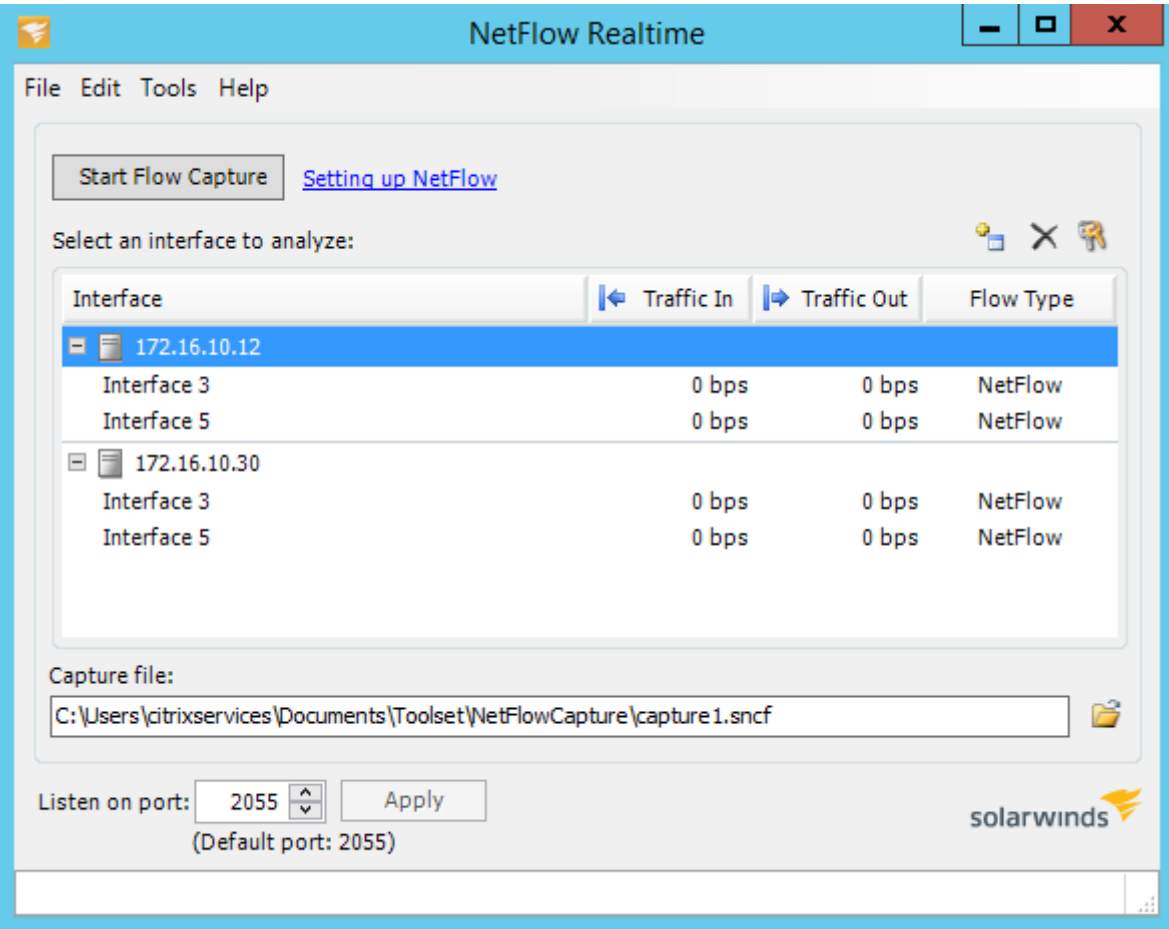
So konfigurieren Sie Net Flow-Hosts:

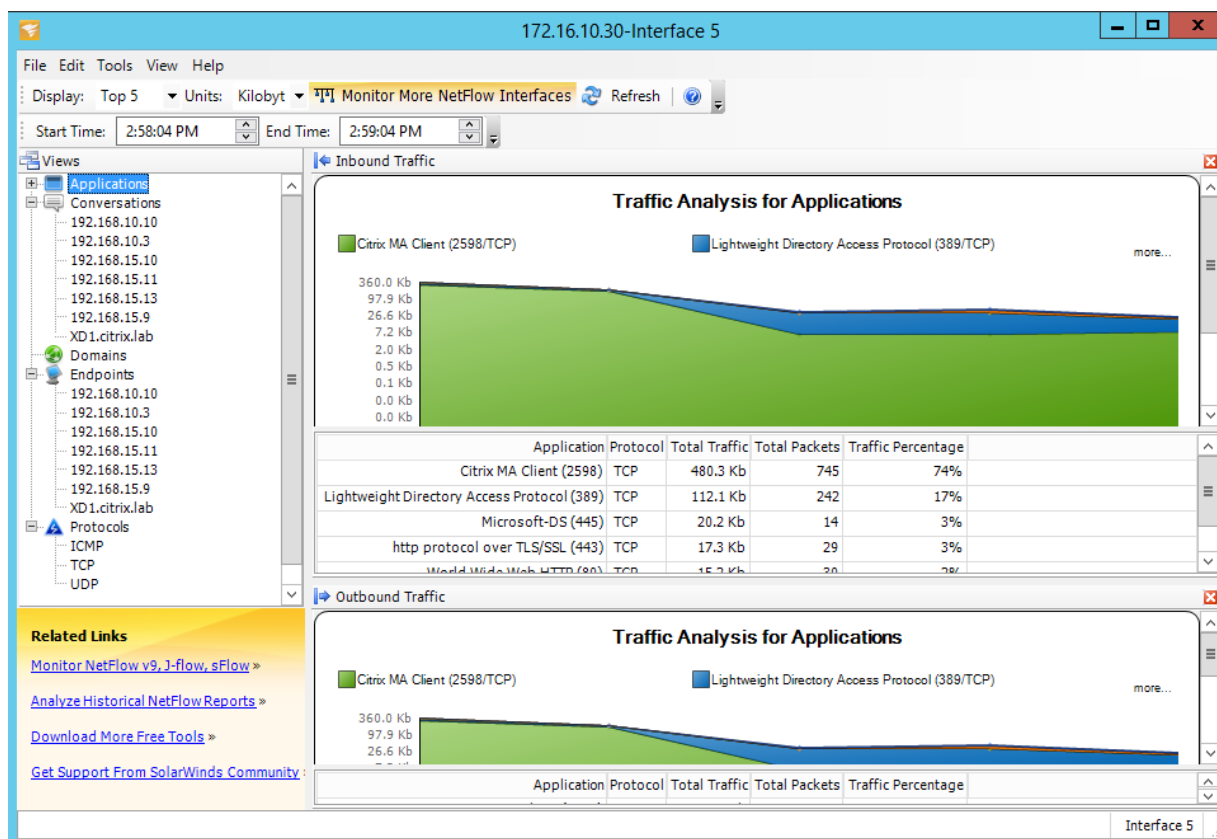
Navigieren Sie zur Seite **Konfiguration > Appliance-Einstellungen > Net Flow Netflow-Host-Einstellungen**. Klicken Sie auf das **KontrollkästchenNetFlow aktivieren**, geben Sie die **IP-Adresse** und die **Portnummern** für bis zu drei Net Flow-Hosts ein und klicken Sie dann auf **Einstellungen anwenden, um die Änderungen zu speichern**.



NetFlow-Export

Net Flow-Daten werden vom Management-Port des SD-WAN-Geräts exportiert. In Ihrem Net Flow Collector-Tool werden die SD-WAN-Geräte als konfigurierte Management-IP-Adresse aufgeführt, wenn SNMP nicht konfiguriert ist. Die Schnittstellen werden als eine für eingehende und eine zweite für ausgehende (Virtual Path Traffic) aufgeführt.





NetFlow-Einschränkungen

- Wenn Netflow auf SD-WAN Standard- und Premium Edition-Appliances aktiviert ist, werden Virtual Path-Daten zu den ausgewiesenen Netflow-Collectors gestreamt. Eine Einschränkung besteht darin, dass man nicht unterscheiden kann, welche physische WAN-Verbindung von SD-WAN verwendet wird, da die Lösung aggregierte Virtual Path Informationen meldet (Ein virtueller Pfad kann aus mehreren unterschiedlichen WAN-Pfaden bestehen), gibt es keine Möglichkeit, die Netflow-Datensätze nach den unterschiedlichen WAN-Pfaden zu filtern.
- TCP-Steuerungsbits melden sich als N/A, was darauf hinweist, dass SD-WAN nicht dem Internetstandard für Netflow-Exporte folgt, der auf [RFC 7011](#) basiert und die Element-ID 6 für TcpControl-Bits ([IANA](#)) hat. Ohne TCP-Flags ist die Berechnung der Roundtrip-Zeit (RTT), Latenz, Jitter und anderer Leistungsmetriken in den Flussdaten nicht möglich. Auf der Sicherheitsseite kann der Net Flow-Collector ohne TCP-Flags nicht feststellen, ob FIN, ACK/RST oder SYN-Scans auftreten.

Routenstatistik

May 10, 2021

Um die Routenstatistiken Ihrer SD-WAN-Appliances anzuzeigen, navigieren Sie in der SD-WAN-GUI zu **Überwachung > Statistiken > Routen**.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IPsec

IGMP

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRP

PPPoE

DNS

Monitoring > Statistics

Statistics

Show Routes ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh [Purge dynamic routes](#)

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 10 of 10 entries

| Details | Num | Network Addr | Gateway IP Address | Service | Firewall Zone | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----------------------------------|-----------------|--------------|----------------------|------------------|---------------|-----------|-----------------|---------|-------------|----------|-----------------|-------|-----------|----------|------------------|-------------------|
| 0 | 172.186.30.0/24 | * | Local | Default_LAN_Zone | YES | * | DC | Static | - | - | - | 5 | 55365 | YES | N/A | N/A |
| 1 | 172.186.40.0/24 | * | Local | Default_LAN_Zone | YES | * | DC | Static | - | - | - | 5 | 0 | YES | N/A | N/A |
| 2 | 172.186.50.0/24 | * | New_Intranet_Service | Default_LAN_Zone | YES | * | DC | Static | - | - | - | 5 | 11 | YES | N/A | N/A |
| 3 | 172.186.10.0/24 | * | DC-Client-1 | Default_LAN_Zone | YES | * | Client-1 | Dynamic | Virtual WAN | YES | YES | 10 | 27912 | YES | N/A | N/A |
| Site Path: Client-1 | | | | | | | | | | | | | | | | |
| Optimal Route: NO | | | | | | | | | | | | | | | | |
| Summarized / Summary Route: NO/NO | | | | | | | | | | | | | | | | |
| 4 | 172.186.20.0/24 | * | DC-Client-1 | Default_LAN_Zone | YES | * | Client-1 | Dynamic | Virtual WAN | YES | YES | 10 | 0 | YES | N/A | N/A |
| 5 | 172.186.10.0/24 | * | New_Intranet_Service | Default_LAN_Zone | YES | * | DC | Static | - | - | - | 15 | 0 | YES | N/A | N/A |
| 6 | 172.186.20.0/24 | * | New_Intranet_Service | Default_LAN_Zone | YES | * | DC | Static | - | - | - | 15 | 0 | YES | N/A | N/A |
| 7 | 0.0.0.0/0 | * | Internet | Internet_Zone | YES | * | DC | Static | - | - | - | 5 | 20 | YES | N/A | N/A |
| 8 | 0.0.0.0/0 | * | Passthrough | Any | YES | * | * | Static | - | - | - | 65535 | 238 | YES | N/A | N/A |
| 9 | 0.0.0.0/0 | * | Discard | Any | YES | * | * | Static | - | - | - | 65535 | 0 | YES | N/A | N/A |

Showing 1 to 10 of 10 entries

First Previous 1 Next Last

Sie können die folgenden Parameter anzeigen:

- **Netzwerkadresse:** Die Netzwerkadresse und die Subnetzmaske der Route.
- **Details:** Klicken Sie auf +, um die folgenden Informationen anzuzeigen.
 - **Standortpfad:** Standortpfad ist eine Quelle der Wahrheitsmetrik für das empfangene Präfix. Es wird in Situationen verwendet, in denen die WAN-zu-WAN-Weiterleitung auf mehreren Geräten und in der Netzbereitstellung aktiviert ist. Mehrere solche Präfixe werden empfangen, und die Administratoren können die Präfixattribute beurteilen, indem sie den Standortpfad anzeigen.

Betrachten Sie beispielsweise eine einfache Topologie von Branch1, Branch2 und MCN zusammen mit einem Geo-MCN. Branch1 hat ein Präfix 172.16.1.0/24 und muss zu Branch2 gelangen. Geo MCN und MCN haben WAN-zu-WAN-Weiterleitung aktiviert.

Das Präfix 172.16.1.0/24 kann über Branch1-MCN-Branch2, Branch1-Geo-Branch2 und Branch1-MCN-Geo-Branch2 zu Branch2 gelangen. Für jedes dieser eindeutigen Präfixe wird die Routingtabelle mit ihrer Standortpfadmetrik aktualisiert. Die Standortpfadmetrik gibt den Ursprung des Routenpräfixes und die Kosten an, die für den Abflug zu Branch2 entstehen.
 - **Optimale Route:** Optimale Route gibt an, ob die Route im Vergleich zu allen anderen Routen die optimale Route ist, um dieses Subnetz zu erreichen. Diese optimale Route wird auf andere Standorte exportiert.

- **Zusammenfassungroute:** Eine Sammelroute ist eine Route, die explizit von einem Administrator konfiguriert wurde, um mehrere Präfixe zusammenzufassen, die in das Supernetz fallen. Zusammengefasste Routen sind die Präfixe, die unter die Sammelroute fallen.

Angenommen, wir haben eine Zusammenfassung Route 172.16.0.0/16. Dies ist nur eine zusammenfassende Route und keine zusammengefasste Route. Eine Sammelroute hat Zusammenfassung 'YES' und Zusammenfassung 'NO'. Wenn es nur wenige andere Subnetze wie 172.16.1.0/24, 172.16.2.0/24 und 172.16.3.0/24 gibt, fallen diese drei Routen unter die Summary Route oder das Supernet und werden daher als zusammengefasste Routen bezeichnet. Eine zusammengefasste Route hat zusammengefasste 'YES' und Zusammenfassung 'NO'.

- **Gateway IP-Adresse:** Die IP-Adresse des Gateways/der Route, die verwendet wurde, um diese Route zu erreichen.
- **Dienst:** Der Typ des Citrix SD-WAN Dienstes.
- **Firewall-Zone:** Die Firewall-Zone, die von der Route verwendet wird.
- **Erreichbar:** Ist die Route erreichbar oder nicht.
- **IP-Adresse des Standorts:** Die IP-Adresse der Site.
- **Site:** Der Name der Site.
- **Typ:** Die Art einer Route hängt von der Quelle des Routenlernens ab. Bei den Routen auf der LAN-Seite und bei der Konfiguration manuell eingegebene Routen handelt es sich um statische Routen. Routen, die aus dem SD-WAN oder dynamischen Routing-Peers gelernt wurden, sind dynamische Routen.
- **Protokoll:** Das Protokoll der Präfixe.
 - **Lokal:** Lokale virtuelle IP-Adressen der Appliance.
 - **Virtuelles WAN:** Präfixe, die von Peer SD-WAN-Appliances gelernt wurden.
 - **OSPF:** Präfixe, die von OSPF Dynamic Routing-Peer gelernt wurden.
 - **BGP:** Präfixe, die von BGP Dynamic Routing-Peer gelernt wurden.
- **Neighbor Direct:** Gibt an, ob das Subnetz mit dem Zweig verbunden ist, von dem die Route zur Appliance kam.
- **Kosten:** Die Kosten, die verwendet werden, um den besten Pfad zu einem Zielnetzwerk zu ermitteln.
- **Trefferanzahl:** Gibt an, wie oft eine Route getroffen wurde, um ein Paket an dieses Subnetz weiterzuleiten.
- **Berechtigt:** Gibt an, dass die Route berechtigt ist und für die Weiterleitung oder Weiterleitung der Pakete an das Präfix verwendet wird, das während der Datenverarbeitung getroffen wurde.

- **Berechtigungsart:** Die folgenden beiden Berechtigungsarten sind verfügbar.
 - **Gateway-Berechtigung:** Bestimmt, ob das Gateway erreichbar ist oder nicht.
 - **Pfadberechtigung:** Bestimmt, ob der Pfad DEAD oder NOT DEAD ist.
- **Berechtigungswert:** Der Wert, der für das Gateway oder den Pfad in der Konfiguration ausgewählt wurde, während die Route im System erstellt wird. Zum Beispiel kann eine Route als berechtigt bezeichnet werden, basierend auf einem Pfad MCN-WL-1->BR1-WL-2. Der Berechtigungswert für diese Route im Streckenabschnitt ist also der Wert MCN-WL-1->BR1-WL-2.

Routing

May 10, 2021

Dynamisches Routing

Citrix SD-WAN führt Unterstützung für bekannte Routing-Protokolle unter der Funktion **Dynamic Routing** ein. Diese Funktion erleichtert die Erkennung von LAN-Subnetzen, Ankündigung für virtuelle Pfadrouten, die mit den Protokollen BGP und OSPF nahtlos in Netzwerken funktionieren, sodass SD-WAN nahtlos in einer vorhandenen Umgebung bereitgestellt werden kann, ohne dass statische Routenkonfigurationen und ein ordnungsgemäßes Router-Failover erforderlich sind.

Routenfilterung

Für Netzwerke mit aktiviertem Routenlernen bietet Citrix SD-WAN mehr Kontrolle darüber, welche SD-WAN-Routen an Routing Nachbarn angekündigt werden und welche Routen von Routing Nachbarn empfangen werden, anstatt alle oder keine Routen zu akzeptieren.

- Exportfilter werden verwendet, um Routen für Werbung mit OSPF- und BGP-Protokollen basierend auf bestimmten Übereinstimmungen ein- oder auszuschließen Kriterien.
- Importfilter werden verwendet, um Routen zu akzeptieren oder nicht zu akzeptieren, die mithilfe von OSPF- und BGP-Nachbarn empfangen werden, basierend auf bestimmten Übereinstimmungskriterien.

Die Routenfilterung wird auf LAN-Routen und virtuellen Pfadrouten in einem SD-WAN-Netzwerk (Data Center/Branch) implementiert und über BGP und OSPF an ein Nicht-SD-WAN-Netzwerk angekündigt.

Routenzusammenfassung

Routenzusammenfassung reduziert die Anzahl der Routen, die ein Router verwalten muss. Eine Sammelroute ist eine einzelne Route, die verwendet wird, um mehrere Routen darzustellen. Es spart Bandbreite, indem eine einzelne Routenankündigung gesendet wird, wodurch die Anzahl der Verbindungen zwischen Routern reduziert wird. Es spart Speicher, da nur eine Routenadresse gepflegt wird. Die CPU-Ressourcen werden effizienter genutzt, indem rekursive Lookups vermieden werden.

VRRP

Virtual Router Redundancy Protocol (VRRP) ist ein weit verbreitetes Protokoll, das Device Redundanz bereitstellt, um den Single Point of Failure in der statischen Standardumgebung zu eliminieren. VRRP ermöglicht es Ihnen, zwei oder mehr Router zu konfigurieren, um eine Gruppe zu bilden. Diese Gruppe wird als einzelnes Standard-Gateway mit einer virtuellen IP-Adresse und einer virtuellen MAC-Adresse angezeigt.

Citrix SD-WAN (Version 10.0 und höher) unterstützt VRRP Version 2 und Version 3 für die Zusammenarbeit mit Routern von Drittanbietern. Die SD-WAN-Appliance fungiert als Master-Router und leitet den Datenverkehr an, den Virtual Path Service zwischen Standorten zu verwenden. Sie können die SD-WAN-Appliance als VRRP-Master konfigurieren, indem Sie die Virtual Interface IP als VRRP-IP konfigurieren und die Priorität manuell auf einen höheren Wert als die Peer-Router festlegen. Sie können das Ankündigungsintervall und die Präempt-Option konfigurieren.

Verwenden von CLI für den Zugriff auf Routing-Funktionen

Sie können zusätzliche Informationen zum dynamischen Routing und zum Protokollstatus anzeigen. Geben Sie den folgenden Befehl und die folgende Syntax ein, um auf den Routing-Daemon zuzugreifen und die Liste der Befehle anzuzeigen.

```
'  
dynamic_routing?  
'
```

SD-WAN-Überlagerungsrouting

May 10, 2021

Citrix SD-WAN bietet robuste und robuste Konnektivität zwischen Remote-Standorten, Rechenzentren und Cloud-Netzwerken. Die SD-WAN-Lösung kann dies erreichen, indem Tunnel zwischen SD-WAN-Appliances im Netzwerk eingerichtet werden, um die Konnektivität zwischen Standorten zu ermöglichen, indem Routentabellen angewendet werden, die das vorhandene Unterlagennetz über-

lagern. SD-WAN-Routingtabellen können die vorhandene Routinginfrastruktur vollständig ersetzen oder mit ihr koexistieren.

Citrix SD-WAN Appliances messen die unidirektional verfügbaren Pfade in Bezug auf Verfügbarkeit, Verlust, Latenz, Jitter und Überlastung und wählen den besten Pfad pro Paket aus. Das bedeutet, dass der von Standort A nach Standort B gewählte Pfad nicht notwendigerweise der Pfad von Standort B zu Standort A sein muss. Der beste Pfad zu einem bestimmten Zeitpunkt wird unabhängig in jede Richtung ausgewählt. Citrix SD-WAN bietet paketbasierte Pfadauswahl zur schnellen Anpassung an alle Netzwerkänderungen. SD-WAN-Appliances können Pfadausfälle nach nur zwei oder drei fehlenden Paketen erkennen, was ein nahtloses Failover des Anwendungsdatenverkehrs in einer Subsekundenzeit zum nächstbesten WAN-Pfad ermöglicht. SD-WAN-Appliances berechnen jeden WAN-Verbindungsstatus in etwa 50 ms neu. Der folgende Artikel enthält eine detaillierte Routingkonfiguration im Citrix SD-WAN Netzwerk.

Citrix SD-WAN Routentabelle

Die SD-WAN-Konfiguration ermöglicht statische Routeneinträge für bestimmte Standorte und Routeneinträge, die aus dem Unterlagennetzwerk über unterstützte Routingprotokolle wie OSPF, eBGP und iBGP gelernt wurden. Routen werden nicht nur durch ihren nächsten Hop, sondern durch ihren Service-Typ definiert. Dies bestimmt, wie die Route weitergeleitet wird. Im Folgenden werden die wichtigsten verwendeten Service-Typen aufgeführt:

- **Lokaler Dienst:** Gibt jede Route oder Subnetz an, die zur SD-WAN-Appliance lokal sind. Dazu gehören die Subnetze der virtuellen Schnittstelle (erstellt automatisch lokale Routen) und alle in der Routentabelle definierten lokalen Routen (mit einem lokalen nächsten Hop). Die Route wird an andere SD-WAN-Appliances angekündigt, die über einen virtuellen Pfad zu diesem lokalen Standort verfügen, an dem diese Route konfiguriert wird, wenn sie als Partner vertrauenswürdig ist.

Hinweis

Seien Sie vorsichtig, wenn Sie Standardrouten und Sammelrouten als lokale Routen hinzufügen, da diese zu virtuellen Pfadrouten an anderen Standorten führen können. Überprüfen Sie immer die Routingtabellen, um sicherzustellen, dass das korrekte Routing wirksam ist.

- **Virtueller Pfad** —Bezeichnet jede lokale Route, die von einem Remote-SD-WAN-Site gelernt wurde, der über die virtuellen Pfade erreichbar ist. Diese Routen sind normalerweise automatisch, aber eine virtuelle Pfadroute kann manuell an einem Standort hinzugefügt werden. Jeder Datenverkehr für diese Route wird an den definierten virtuellen Pfad für diese Zielroute (Subnetz) weitergeleitet.
- **Intranet** —Bezeichnet Routen, die über eine private WAN-Verbindung (MPLS, P2P, VPN usw.) erreichbar sind. Ein Remote-Zweig, der sich im MPLS-Netzwerk befindet, aber keine

SD-WAN-Appliance hat. Es wird davon ausgegangen, dass diese Routen an einen bestimmten WAN-Router weitergeleitet werden müssen. Der Intranetdienst ist standardmäßig nicht aktiviert. Jeder Datenverkehr, der dieser Route (Subnetz) entspricht, wird als Intranet für diese Appliance klassifiziert, um an einen Standort zuzustellen, der über keine SD-WAN-Lösung verfügt.

Hinweis

Beachten Sie, dass beim Hinzufügen einer Intranetroute kein nächster Hop vorhanden ist, sondern ein Weiterleiten an einen Intranetdienst. Der Dienst ist einem bestimmten WAN-Link zugeordnet.

- **Internet** —Dies ähnelt dem Intranet, wird jedoch verwendet, um Datenverkehr zu öffentlichen Internet-WAN-Verbindungen und nicht zu privaten WAN-Verbindungen zu definieren. Ein eindeutiger Unterschied besteht darin, dass der Internetdienst mehreren WAN-Verbindungen zugeordnet und auf Lastausgleich (pro Flow) oder aktiv/Backup eingestellt werden kann. Eine Standard-Internetroute wird erstellt, wenn der Internetdienst aktiviert ist (standardmäßig deaktiviert). Jeder Datenverkehr, der dieser Route (Subnetz) entspricht, wird für diese Appliance als Internet klassifiziert, um sie an öffentliche Internetressourcen zu liefern.

Hinweis

Internet-Service-Routen können an die anderen SD-WAN-Appliances angekündigt oder daran gehindert werden, je nachdem, ob Sie den Internetzugang über die virtuellen Pfade backhauling.

- **Passthrough** —Dieser Dienst fungiert als letzter Ausweg oder Override-Dienst, wenn sich eine Appliance im In-Line-Modus befindet. Wenn eine Ziel-IP-Adresse nicht mit einer anderen Route übereinstimmt, leitet die SD-WAN-Appliance sie einfach an den nächsten Hop WAN-Link weiter. Eine Standardroute: 0.0.0.0/0 Kosten von 16 Pass-Through-Route werden automatisch erstellt. Passthrough funktioniert nicht, wenn die SD-WAN-Appliance außerhalb des Pfades oder im Edge/Gateway-Modus bereitgestellt wird. Jeder Datenverkehr, der dieser Route (Subnetz) entspricht, wird als Passthrough für diese Appliance klassifiziert. Es wird empfohlen, dass der Passthrough-Verkehr so weit wie möglich begrenzt ist.

Hinweis

Passthrough kann nützlich sein, wenn Sie einen POC durchführen, um zu vermeiden, dass zahlreiche Routings konfiguriert werden müssen. Seien Sie jedoch vorsichtig in der Produktion, da SD-WAN die WAN-Link-Auslastung für Datenverkehr, der an Passthrough gesendet wird, nicht berücksichtigt. Es ist auch hilfreich, wenn Sie Probleme beheben und einen bestimmten IP-Fluss über den virtuellen Pfad aus der Zustellung herausnehmen möchten.

- **Verwerfen** - Dies ist kein Dienst, sondern eine letzte Ausweg, die die Pakete fallen lassen, wenn sie übereinstimmen. Normalerweise tritt dies nicht auf, wenn die SD-WAN-Appliance außer-

halb des Pfades bereitgestellt wird. Sie müssen einen Intranetdienst oder eine lokale Route als Catch all Route haben, andernfalls wird der Datenverkehr verworfen, da kein Passthrough-Dienst vorhanden ist (obwohl eine Passthrough-Standardroute vorhanden ist).

Der SD-WAN-Konfigurationseditor ermöglicht die Anpassung der Routentabellen für jeden verfügbaren Standort:

The screenshot shows the Citrix SD-WAN Configuration Editor interface. The 'Connections' tab is selected, and the 'Routes' section is highlighted in the left sidebar. The main area displays a table of routes with the following data:

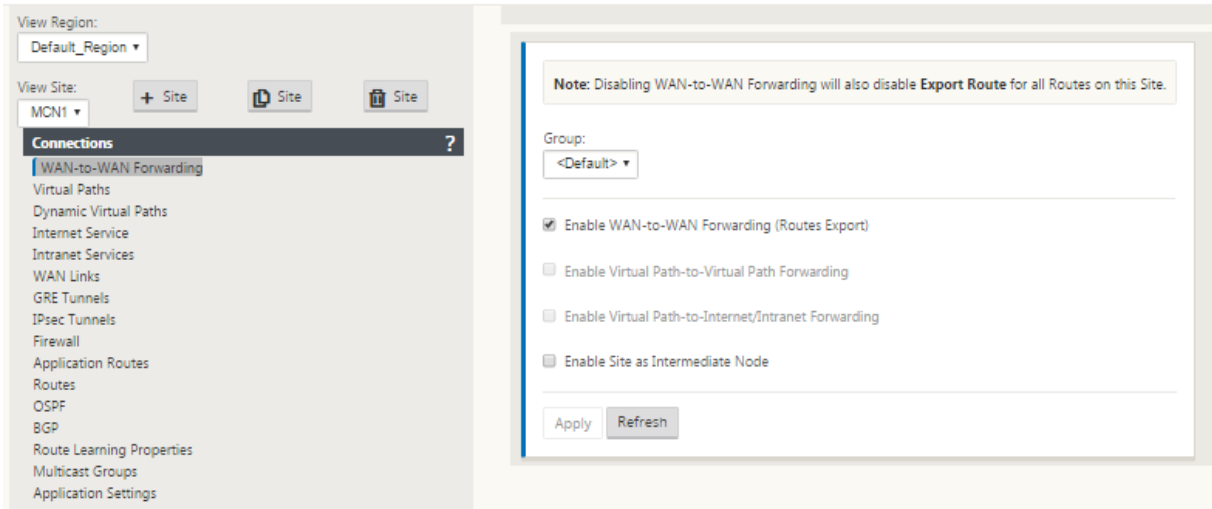
| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|-------|--------------|--------------|--------------------|------|------|--------|
| 1 | 172.120.21.100/32 | 5 | Passthrough | | | | | |
| 2 | 172.120.21.64/32 | 4 | Internet | | | | | |
| 3 | 172.120.21.65/32 | 4 | Passthrough | | | | | |
| 4 | 172.120.24.64/32 | 4 | Internet | | | | | |
| 5 | 10.101.0.0/22 | 5 | Virtual Path | BR1 | | | | |
| 6 | 224.225.1.1/32 | 5 | Multicast | | | | | |
| 7 | 224.225.1.2/32 | 5 | Multicast | | | | | |
| 8 | 224.225.1.3/32 | 5 | Multicast | | | | | |
| 9 | 172.120.24.7/24 | 5 | Local | | | | | |
| 10 | 182.120.24.7/24 | 5 | Local | | | | | |
| 11 | 0.0.0.0/0 | 5 | Internet | | | | | |
| 12 | 0.0.0.0/0 | 65535 | Passthrough | | | | | |

Routentableneinträge werden aus verschiedenen Eingaben aufgefüllt:

- Konfigurierte virtuelle IP-Adresse (VIP) wird automatisch als Service Type Local route aufgefüllt. Der Konfigurationseditor verhindert dieselbe VIP-Zuweisung zu verschiedenen Standortknoten.
- Internetdienste, die an einem lokalen Standort aktiviert sind, füllen automatisch eine Standardroute (0.0.0.0/0) lokal für direkte Internetausbrüche aus.
- Admin definierte statische Routen pro Standort, die auch als Service Type Local Route definiert werden.
- Ein Standardwert (0.0.0.0/0) fängt alle Routen ab, wobei Kosten 16 als Passthrough definiert sind.

Administratoren können eine der oben genannten Routen konfigurieren, aber zusätzlich zu den Routenkosten auch einen Diensttyp, nächsten Hop oder Gateway einschließen. Zu jedem Routentyp werden automatisch Standardkosten hinzugefügt (Standardkosten für Routen finden Sie in der folgenden Tabelle). Außerdem werden nur vertrauenswürdige Routen an andere SD-WAN-Appliances angekündigt. Nicht vertrauenswürdige Routen werden nur von der lokalen Appliance verwendet.

Client-Knotenrouten werden nur an den MCN-Knoten angekündigt und keine anderen Client-Knoten standardmäßig. Damit Clientknotenrouten für andere Clientknoten sichtbar sind, muss WAN zu WAN-Weiterleitung am MCN-Knoten aktiviert sein.



Wenn WAN-zu-WAN-Weiterleitung (Routenexport Template) unter den globalen Einstellungen aktiviert ist, teilt die MCN-Site die angekündigten Routen für alle Clients, die am SD-WAN-Overlay teilnehmen. Durch Aktivieren dieser Funktion wird die IP-Konnektivität zwischen Hosts an verschiedenen Clientknotenstandorten aktiviert, wobei die Kommunikation über den MCN erfolgt. Die Routing-Tabelle für den lokalen Client-Knoten kann auf der Seite **Überwachung > Statistiken** überwacht werden, wobei Routen für die Dropdown-Liste **Anzeigen** ausgewählt sind.

Statistics

Flows

Routing Protocols

Firewall

IKE/Sec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP Protocol

Monitoring > Statistics

Statistics

Show: Routes

☐ Enable Auto Refresh

5 seconds

Refresh

☒ Clear Counters on Refresh

Purge dynamic routes

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter:

in Any column

Apply

Show 100 entries

Showing 1 to 54 of 54 entries

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 | 172.120.21.64/32 | * | Internet | Internet_Zone | YES | * | MCN1 | Static | - | - | 4 | 0 | YES | N/A | N/A |
| 1 | 172.120.24.64/32 | * | Internet | Internet_Zone | YES | * | MCN1 | Static | - | - | 4 | 0 | YES | N/A | N/A |
| 2 | 172.120.21.65/32 | * | Passthrough | Any | YES | * | * | Static | - | - | 4 | 0 | YES | N/A | N/A |
| 3 | 224.225.1.1/32 | * | Multicast | Any | YES | * | MCN1 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 4 | 224.225.1.2/32 | * | Multicast | Any | YES | * | MCN1 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 5 | 224.225.1.3/32 | * | Multicast | Any | YES | * | MCN1 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 6 | 172.120.21.100/32 | * | Passthrough | Any | YES | * | * | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 7 | 172.120.24.64/32 | * | MCN1-BR1 | Default_LAN_Zone | YES | * | BR1 | Dynamic | Virtual WAN | YES | 9 | 0 | YES | N/A | N/A |
| 8 | 172.120.24.0/24 | * | Local | Default_LAN_Zone | YES | * | MCN1 | Static | - | - | 5 | 3458 | YES | N/A | N/A |
| 9 | 182.120.24.0/24 | * | Local | Default_LAN_Zone | YES | * | MCN1 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 10 | 172.120.10.0/24 | * | MCN1-APAC_RCN | Default_LAN_Zone | YES | * | APAC_RCN | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A | N/A |
| 11 | 172.120.21.0/24 | * | MCN1-BR1 | Default_LAN_Zone | YES | * | BR1 | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A | N/A |
| 12 | 182.120.10.0/24 | * | MCN1-APAC_RCN | Default_LAN_Zone | YES | * | APAC_RCN | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A | N/A |
| 13 | 192.168.255.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | RCN01-2000 | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A | N/A |
| 14 | 192.172.0.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx01 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 15 | 192.172.1.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx02 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 16 | 192.172.2.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx03 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 17 | 192.172.3.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx04 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 18 | 192.172.4.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx05 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 19 | 192.172.5.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx06 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 20 | 192.172.6.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx07 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 21 | 192.172.7.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx08 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 22 | 192.172.12.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx13 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 23 | 192.172.13.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx14 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 24 | 192.172.14.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx15 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 25 | 192.172.15.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx16 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 26 | 192.172.16.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx17 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 27 | 192.172.17.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx18 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 28 | 192.172.18.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx19 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 29 | 192.172.19.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx20 | Dynamic | Virtual WAN | NO | 10 | 0 | YES | N/A | N/A |
| 30 | 192.120.10.0/24 | * | MCN1-APAC_RCN | Default_LAN_Zone | YES | * | APAC_RCN | Dynamic | Virtual WAN | YES | 11 | 0 | YES | N/A | N/A |
| 31 | 172.108.0.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx01 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 32 | 172.108.1.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx02 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 33 | 172.108.2.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx03 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 34 | 172.108.3.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx04 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 35 | 172.108.4.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx05 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 36 | 172.108.5.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx06 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 37 | 172.108.6.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx07 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 38 | 172.108.7.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx08 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 39 | 172.108.12.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx13 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 40 | 172.108.13.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx14 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 41 | 172.108.14.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx15 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 42 | 172.108.15.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx16 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 43 | 172.108.16.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx17 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 44 | 172.108.17.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx18 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 45 | 172.108.18.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx19 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 46 | 172.108.19.0/24 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | AMEA_r1_vpx20 | Dynamic | Virtual WAN | NO | 15 | 0 | YES | N/A | N/A |
| 47 | 10.101.0.0/22 | * | MCN1-BR1 | Any | YES | * | BR1 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 48 | 10.101.0.0/22 | * | MCN1-BR1 | Default_LAN_Zone | YES | * | BR1 | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A | N/A |
| 49 | 172.105.96.0/20 | * | MCN1-RCN01-2000 | Default_LAN_Zone | YES | * | RCN01-2000 | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A | N/A |
| 50 | 0.0.0.0/0 | * | Internet | Internet_Zone | YES | * | MCN1 | Static | - | - | 5 | 401109 | YES | N/A | N/A |
| 51 | 0.0.0.0/0 | * | MCN1-BR1 | Default_LAN_Zone | YES | * | BR1 | Dynamic | Virtual WAN | YES | 10 | 88 | YES | N/A | N/A |
| 52 | 0.0.0.0/0 | * | Passthrough | Any | YES | * | * | Static | - | - | 65535 | 40031944 | YES | N/A | N/A |
| 53 | 0.0.0.0/0 | * | Discard | Any | YES | * | * | Static | - | - | 65535 | 0 | YES | N/A | N/A |

Showing 1 to 54 of 54 entries

First

Previous

1

Next

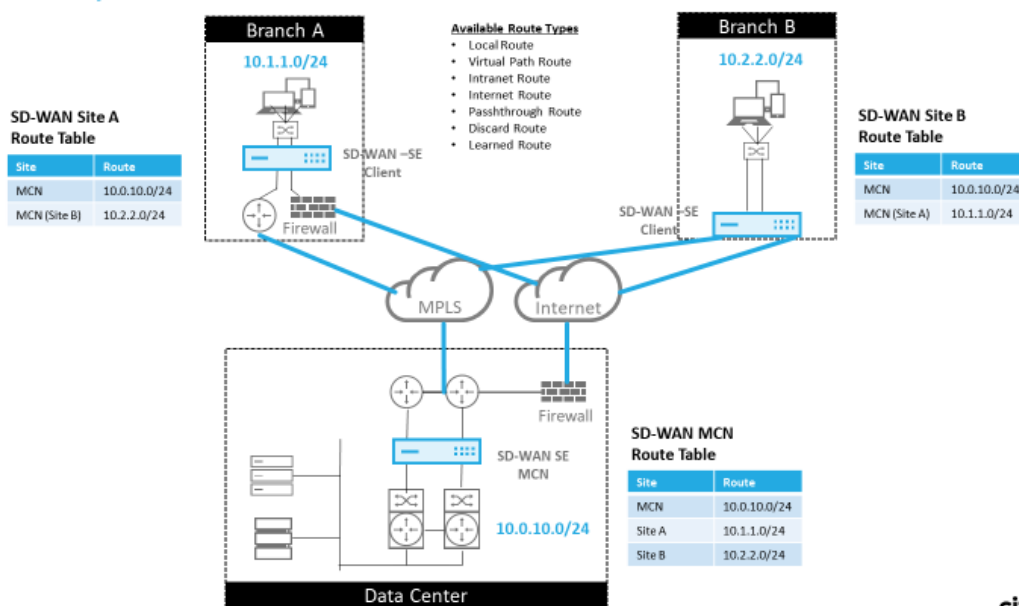
Last

Jede Route für Subnetze von Remote-Zweigstellen wird über den virtuellen Pfad, der über den MCN verbunden ist, als Dienst beworben, wobei die Spalte **Site** mit dem Client-Knoten gefüllt ist, in dem sich das Ziel als lokales Subnetz befindet.

Im folgenden Beispiel hat Zweig A bei aktivierter **WAN-to-WAN-Weiterleitung** (Routes Export) einen

Routingtabelleneintrag für das Branch B-Subnetz (10.2.2.0/24) durch den MCN als nächsten Hop.

SD-WAN Overlay Route Tables



Übereinstimmung mit dem Citrix SD-WAN Datenverkehr auf definierten Routen

Der Abgleichsprozess für definierte Routen auf Citrix SD-WAN basiert auf der längsten Präfixübereinstimmung für das Zielsubnetz (ähnlich wie bei einem Routervorgang). Je spezifischer die Route ist, desto höher ist die Änderung. Die Sortierung erfolgt in der folgenden Reihenfolge:

1. Längste Präfix-Übereinstimmungen
2. Kosten
3. Service

Daher geht eine /32 Route immer vor einer /31 Route. Bei zwei /32 Routen geht eine Cost-4-Route immer vor einer Cost-5-Route. Für zwei /32 Kosten 5 Routen werden Routen basierend auf dem bestellten IP-Host ausgewählt. Serviceauftrag ist wie folgt: Lokal, Virtueller Pfad, Intranet, Internet, Passthrough, Verwerfen.

Betrachten Sie als Beispiel die folgenden beiden Routen wie folgt:

- 192.168.1.0/24 Kosten 5
- 192.168.1.64/26 Kosten 10

Ein Paket, das für den Host 192.168.1.65 bestimmt ist, würde die letztere Route verwenden, obwohl die Kosten höher sind. Auf dieser Grundlage ist es üblich, dass die Konfiguration nur für die Routen vorhanden ist, die über das Virtual Path Overlay bereitgestellt werden sollen, wobei anderer Datenverkehr alle Routen abfangen, z. B. eine Standardroute zum Passthrough-Service.

Routen können in einer Standortknoten-Tabelle konfiguriert werden, die das gleiche Präfix haben. Der Unterbrechung geht dann zu den Routenkosten, dem Diensttyp (Virtueller Pfad, Intranet, Internet usw.) und der nächsten Hop-IP.

Citrix SD-WAN Routingpaketfluss

- LAN-zu-WAN (Virtual Path) Traffic-Routenübereinstimmung:
 1. Der eingehende Datenverkehr wird von der LAN-Schnittstelle empfangen und verarbeitet.
 2. Der empfangene Frame wird mit der Routentabelle für die längste Präfixübereinstimmung verglichen.
 3. Wenn eine Übereinstimmung gefunden wird, wird der Frame von der Regelengine verarbeitet und ein Flow in der Flow-Datenbank erstellt.
- WAN zu LAN (Virtual Path) Traffic Routenübereinstimmung:
 1. Der virtuelle Pfadverkehr wird vom SD-WAN aus dem Tunnel empfangen und verarbeitet.
 2. Die Appliance vergleicht die Quell-IP-Adresse, um festzustellen, ob die Quelle lokal ist.
 - Wenn ja —dann WAN-qualifiziert und IP-Ziel mit Routingtabelle/Virtual Path übereinstimmen.
 - Wenn nein —dann Überprüfung der WAN-zu-WAN-Weiterleitung aktiviert.
 3. (WAN-zu-WAN-Weiterleitung deaktiviert) Weiterleiten an LAN basierend auf lokalen Routen.
 4. (WAN-zu-WAN-Weiterleitung aktiviert) Weiterleiten an virtuellen Pfad basierend auf der Routingtabelle.
- Nicht-virtueller Pfadverkehr:
 1. Eingehender Datenverkehr wird über die LAN-Schnittstelle empfangen und verarbeitet.
 2. Der empfangene Frame wird mit der Routentabelle für die längste Präfixübereinstimmung verglichen.
 3. Wenn eine Übereinstimmung gefunden wird, wird der Frame von der Regelengine verarbeitet und ein Flow in der Flow-Datenbank erstellt.

Unterstützung des Citrix SD-WAN Routingprotokolls

Citrix SD-WAN Version 9.1 führte OSPF- und BGP-Routingprotokolle in die Konfiguration ein. Die Einführung von Routingprotokollen in SD-WAN ermöglichte eine einfachere Integration von SD-WAN

in komplexere Unterlagennetzwerke, in denen Routingprotokolle aktiv eingesetzt werden. Mit den gleichen Routing-Protokollen, die auf SD-WAN aktiviert sind, wurde die Konfiguration von Subnetzen vereinfacht, die für die Verwendung des SD-WAN-Overlays bezeichnet werden. Darüber hinaus ermöglichen die Routingprotokolle die Kommunikation zwischen SD-WAN- und Nicht-SD-WAN-Standorten mit direkter Kommunikation zu bestehenden Kunden-Edge-Routern über das gemeinsame Routing-Protokoll. Citrix SD-WAN, die an Routingprotokollen im Unterlagennetzwerk teilnehmen, kann unabhängig vom Bereitstellungsmodus von SD-WAN (Inline-Modus, Virtual Inline-Modus oder Edge/Gateway-Modus) durchgeführt werden. Außerdem kann SD-WAN im “Nur lernen”-Modus bereitgestellt werden, in dem SD-WAN Routen empfangen, aber keine Routen zur Unterlage ankündigen kann. Dies ist nützlich, wenn die SD-WAN-Lösung in ein Netzwerk eingeführt wird, in dem die Routinginfrastruktur komplex oder unsicher ist.

Wichtig

Es ist einfach, den unerwünschten Weg zu lecken, wenn Sie nicht vorsichtig sind.

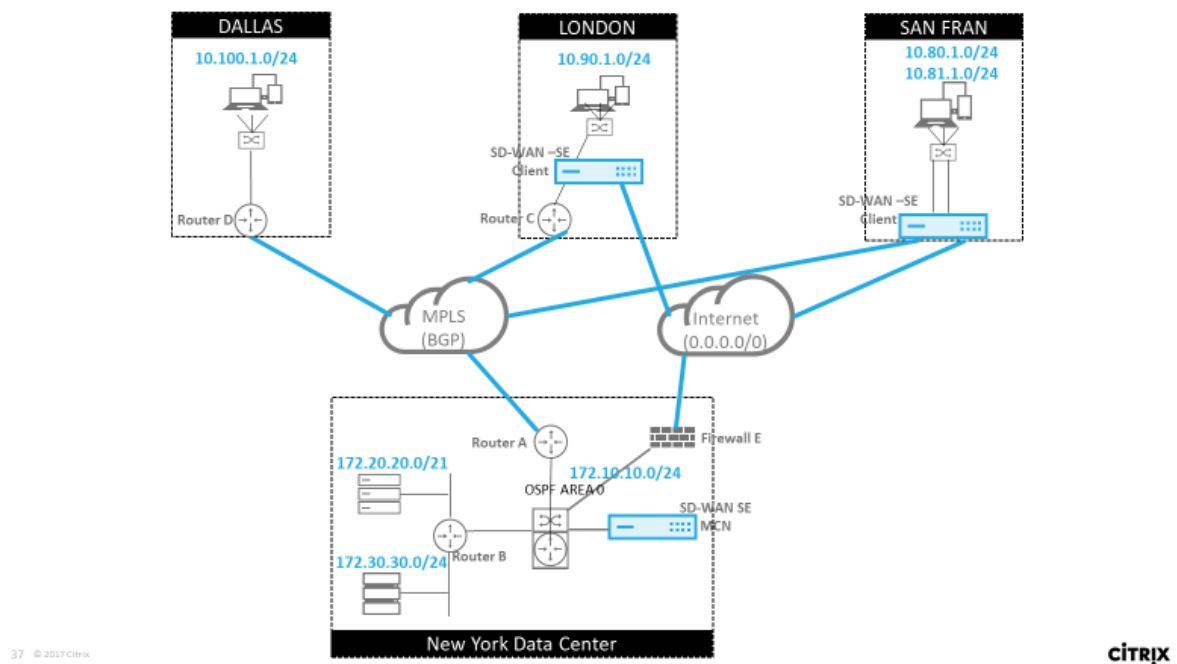
Die SD-WAN Virtual Path Routen-Tabelle funktioniert wie ein External Gateway Protocol (EGP), ähnlich wie BGP (Think Site-to-Site). Wenn SD-WAN beispielsweise Routen von der SD-WAN-Appliance zu OSPF anmeldet, werden sie normalerweise als extern für Standort und Protokoll betrachtet.

Hinweis

Beachten Sie Umgebungen mit IGP über die gesamte Infrastruktur (über das WAN), da dies die Verwendung von SD-WAN-angekündigten Routen erschwert. EIGRP wird in großem Umfang auf dem Markt verwendet, und SD-WAN arbeitet nicht mit diesem Protokoll zusammen.

Eine Herausforderung bei der Einführung von Routingprotokollen in eine SD-WAN-Bereitstellung besteht darin, dass die Routingtabelle erst verfügbar ist, wenn der SD-WAN-Dienst aktiviert und im Netzwerk ausgeführt wird. Daher wird es nicht empfohlen, zuerst Ankündigungsroueten von der SD-WAN-Appliance zu aktivieren. Verwenden Sie die Import- und Exportfilter für eine schrittweise Einführung von Routingprotokollen auf SD-WAN.

Lassen Sie uns einen genaueren Blick, indem Sie das folgende Beispiel überprüfen:



In diesem Beispiel untersuchen wir einen Anwendungsfall des Routingprotokolls. Das vorhergehende Netzwerk hat vier Standorte: New York, Dallas, London und San Francisco. Wir stellen SD-WAN-Appliances an drei dieser Standorte bereit und verwenden SD-WAN, um ein hybrides WAN-Netzwerk zu erstellen, in dem MPLS- und Internet-WAN-Links verwendet werden, um ein virtualisiertes WAN bereitzustellen. Da Dallas kein SD-WAN-Gerät haben wird, müssen wir überlegen, wie Sie am besten in bestehende Routenprotokolle zu diesem Standort integrieren können, um eine vollständige Konnektivität zwischen Unterlagen- und SD-WAN-Overlay-Netzwerken zu gewährleisten.

Im Beispielnetzwerk wird eBGP zwischen allen vier Standorten im MPLS-Netzwerk verwendet. Jeder Standort hat seine eigene Autonomous System Number (ASN).

Im New Yorker Rechenzentrum wird OSPF ausgeführt, um die Kernsubnetze des Rechenzentrums an die Remote-Standorte anzukündigen und außerdem eine Standardroute von der New York Firewall (E) anzukündigen. In diesem Beispiel wird der gesamte Internetverkehr in das Rechenzentrum zurückgeführt, obwohl die Niederlassungen in London und San Francisco über einen Pfad zum Internet verfügen.

Der Standort San Francisco muss ebenfalls darauf hingewiesen werden, dass er keinen Router hat. SD-WAN wird im Edge/Gateway-Modus bereitgestellt, wobei diese Appliance das Standard-Gateway für das San Francisco-Subnetz ist und auch an eBGP zum MPLS beteiligt ist.

- Beachten Sie beim New York Data Center, dass das SD-WAN im Virtual Inline-Modus bereitgestellt wird. Die Absicht besteht darin, am vorhandenen OSPF-Routingprotokoll teilzunehmen, um Datenverkehr als bevorzugtes Gateway an die Appliance weiterzuleiten.

- Die Londoner Site wird im traditionellen Inline-Modus bereitgestellt. Der Upstream-WAN-Router (C) ist weiterhin das Standard-Gateway für das London-Subnetz.
- Der San Francisco-Standort ist ein neu eingeführter Standort in diesem Netzwerk, und das SD-WAN soll im Edge/Gateway-Modus bereitgestellt werden und als Standard-Gateway für das neue San Francisco-Subnetz fungieren.

Überprüfen Sie einige der vorhandenen Unterlagen-Routentabellen, bevor Sie SD-WAN implementieren.

New York Core Router B:

```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:08:56
O>* 10.90.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h00m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

Die lokalen New Yorker Subnetze (172.x.x.x) sind auf Router B als direkt verbunden verfügbar, und aus der Routingtabelle erkennen wir, dass die Standardroute 172.10.10.3 (Firewall E) ist. Außerdem können wir sehen, dass Dallas (10.90.1.0/24) und London (10.100.1.0/24) Subnetze über 172.10.10.1 (MPLS Router A) verfügbar sind. Die Routenkosten deuten darauf hin, dass sie von eBGP gelernt wurden.

Hinweis

Im angegebenen Beispiel wird San Francisco nicht als Route aufgeführt, da wir die Site noch nicht mit SD-WAN im Edge/Gateway-Modus für dieses Netzwerk bereitgestellt haben.

```
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
```

Für den New York WAN Router (A) sind OSPF erlernte Routen und Routen aufgelistet, die über das MPLS durch eBGP gelernt wurden. Beachten Sie die Routenkosten. BGP ist niedriger administrative Domäne und Kosten standardmäßig 20/1 im Vergleich zu OSPF 110/10.

Dallas Router D:

Für den Dallas WAN Router (D) werden alle Routen über das MPLS erlernt.

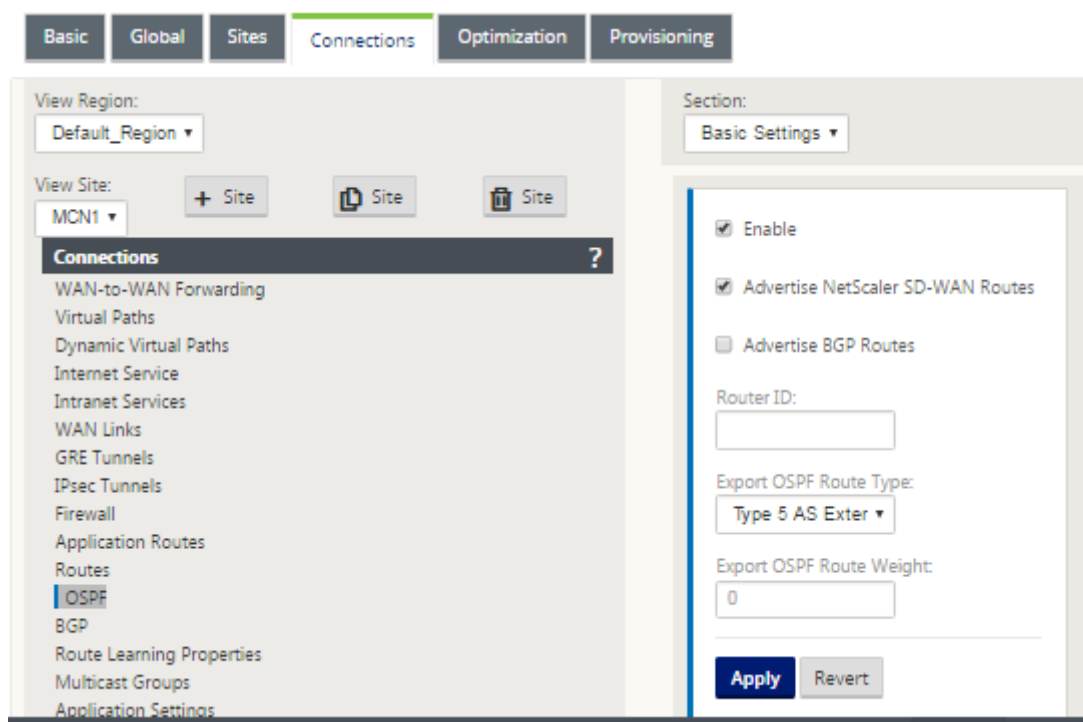
```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

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
```

Hinweis

In diesem Beispiel können Sie das Subnetz 192.168.65.0/24 ignorieren. Dies ist ein Management-Netzwerk und nicht relevant für das Beispiel. Alle Router sind mit dem Management-Subnetz verbunden, werden jedoch in keinem Routingprotokoll angekündigt.

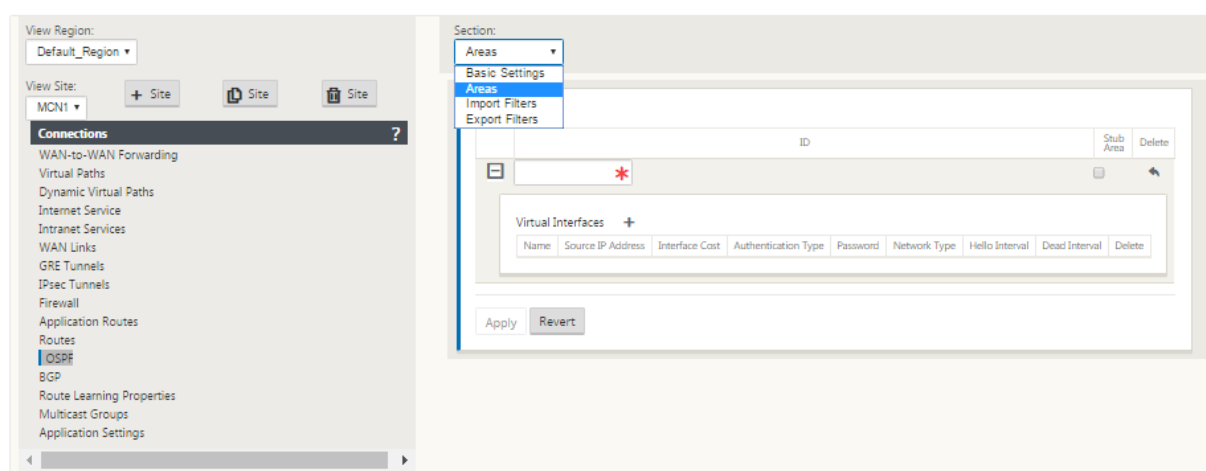
In Citrix SD-WAN können Sie das SD-WAN-Overlay hinzufügen, indem Sie OSPF auf dem SD-WAN auf der New Yorker Website unter **Verbindungen > Site anzeigen > OSPF > Grundeinstellungen aktivieren**:



Hinweis

Der **OSPF-Routentyp exportieren** ist standardmäßig Typ 5 Extern. Dies liegt daran, dass die SD-WAN-Routing-Tabelle außerhalb des OSPF-Protokolls betrachtet wird und OSPF daher eine interne Route (intern) bevorzugt, weshalb die von SD-WAN angekündigten Routen möglicherweise keinen Vorrang haben.

Wenn OSPF über das WAN (also MPLS-Netzwerke) verwendet wird, kann dies in Typ 1 innerhalb des Bereichs geändert werden. OSPF-Bereiche können wie unten dargestellt konfiguriert werden.



Bereich 0 hinzugefügt mit dem lokalen Netzwerk abgeleitet von der virtuellen Schnittstelle (172.10.10.0), alle anderen Einstellungen wurden standardmäßig belassen.

Für den neuen Standort in San Francisco müssen wir eBGP aktivieren, da es direkt mit dem MPLS-Netzwerk verbunden ist und als Customer Edge-Route für den Standort fungiert. BGP kann unter **Verbindungen > Site anzeigen > BGP > Grundeinstellungen aktiviert werden**.

Beachten Sie die Nummer des autonomen Systems 13.

Section: Basic Properties

☒ Enable

☒ Advertise NetScaler SD-WAN Routes

☐ Advertise OSPF Routes

Router ID:
192.168.10.4

Local Autonomous System:
13

Apply Revert

Section: Neighbors

| Virtual Interface | Source IP | Neighbor IP | Neighbor AS | Hold Time(s) | Local Preference | IGP Metric | Multi Hop | Password | Delete |
|-------------------|--------------|--------------|-------------|--------------|------------------|------------|-------------------------------------|----------|--------|
| V1 | 192.168.10.4 | 192.168.10.1 | 65011 | 3600 | 100 | | <input checked="" type="checkbox"/> | | |

Policies +

| Order | Network Address | BGP Community(AASN) | AS Path | BGP Policy | Direction | Delete |
|--------|-----------------|---------------------|---------|------------|-----------|--------|
| (auto) | <Manual> | <Manual> | * | <Accept> | | |

| | | | | | | | | | | |
|---|----|--------------|--------------|-------|------|-----|-------------------------------------|-------------------------------------|--|--|
| + | V1 | 192.168.10.4 | 192.168.10.2 | 65012 | 3600 | 100 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |
|---|----|--------------|--------------|-------|------|-----|-------------------------------------|-------------------------------------|--|--|

Apply Refresh

Der eBGP-Peers untereinander. Jede ASN ist anders.

Es ist wichtig zu verstehen, wie die Routen zwischen der Routingtabelle des virtuellen Pfades und den verwendeten dynamischen Routenprotokollen übergeben werden. Es ist einfach, Routingschleifen zu erstellen oder Routen in einer ungünstigen Weise zu werben. Der Filtermechanismus gibt uns die Möglichkeit zu steuern, was in und aus der Routingtabelle gelangt. Wir betrachten jeden Standort der Reihe nach.

- Der Standort San Francisco verfügt über zwei lokale Subnetze **10.80.1.0/24** und **10.81.1.0/24**. Wir wollen sie über eBGP bewerben, damit Standorte wie Dallas noch über das Unterlay-Netzwerk den Standort San Francisco erreichen können und auch Standorte wie London und New York über das Virtual Path Overlay-Netzwerk weiterhin San Francisco erreichen können. Wir möchten auch von der Erreichbarkeit von eBGP auf alle Standorte lernen, falls das SD-WAN

Virtual Path Overlay ausfällt und die Umgebung auf die Verwendung von MPLS zurückgreifen muss. Wir wollen auch nichts lesen, was SD-WAN von eBGP bis zu den SD-WAN-Routern lernt. Um dies zu erreichen, müssen die Filter wie folgt konfiguriert werden:

- Importieren Sie alle Routen aus eBGP. Routen nicht in SD-WAN-Appliances lesen/exportieren.

| Order | Source Router | Destination | Prefix | Next Hop | Protocol | Route Tag | Cost | AS Path Length | Include | Enabled | Delete | Clone |
|---|---------------|-------------|--------|----------|----------|-----------|------|----------------|-------------------------------------|-------------------------------------|--------|-------|
| 100 | * | <Manual> | eq * | * | Any | * | eq * | eq * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| <div><div><input type="checkbox"/> Export Route to Citrix Appliances</div><div><input type="checkbox"/> Eligibility Based On Gateway</div><div><div>Citrix SD-WAN Cost: 6</div><div>Service Type: Local</div><div>Service Name: <Any></div></div><div><input type="checkbox"/> Eligibility Based On Path</div><div>Path: <None></div></div> | | | | | | | | | | | | |
| 200 | * | <Manual> | eq * | * | Any | * | eq * | eq * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| 200 | * | <Manual> | eq * | * | Any | * | eq * | eq * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |

Apply Revert

- Lokale Routen nach eBGP exportieren

Die Standardregel für den Export besteht darin, alles zu exportieren. Regel 200 wird verwendet, um die Fehlerregel außer Kraft zu setzen, um die Routen nicht zu lesen. Jede Route, die mit einem Präfix SD-WAN übereinstimmt, hat über die virtuellen Pfade gelernt.

| | Order | Network Address | Prefix | NetScaler SD-WAN Cost | Service Type | Site/Service Name | Gateway IP Address | Include | Enabled | Delete | Clone |
|---|--------|--------------------|--------|-----------------------|--------------|-------------------|--------------------|-------------------------------------|-------------------------------------|--------|-------|
| + | 100 | <Manual> * | eq 24 | eq * | Local | <Any> | * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| + | 200 | <Manual> 0.0.0.0/0 | eq * | eq * | Any | <Any> | * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| | (auto) | <Manual> * | eq * | eq * | Any | <Any> | * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |

Nachdem die Citrix SD-WAN Appliances bereitgestellt wurden, können wir einen aktualisierten Blick auf die Routentabellen für den BGP-Router am Standort Dallas werfen. Wir sehen, dass 10.80.1.0/24 und 10.81.1.0/24 Subnetze korrekt über eBGP aus dem San Francisco SD-WAN gesehen werden.

Dallas Router D:

```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

Darüber hinaus kann die Citrix SD-WAN Routentabelle auf der Seite **Überwachung > Statistiken > Routen anzeigen** angezeigt werden.

San Francisco Citrix SD-WAN:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 16 of 16 entries

| Num | Network Addr | Gateway IP Address | Service | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|-----------------|--------------------|-------------|-----------|-----------------|------|---------|-------------|-----------------|------|-----------|----------|------------------|-------------------|
| 0 | 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

Citrix SD-WAN zeigt alle erlernten Routen an, einschließlich Routen, die über das virtuelle Pfad-Overlay verfügbar sind.

Betrachten wir 172.10.10.0/24, die sich im New York Data Center befindet. Diese Route wird auf zwei Arten erlernt:

- Als Virtual Path Route (Nummer 3), Service = NYC-SFO mit einem Preis von 5 und Typ statisch. Dies ist ein lokales Subnetz, das von der SD-WAN-Appliance in New York angekündigt wird. Es ist

statisch, da es entweder direkt mit der Appliance verbunden ist oder es sich um eine manuelle statische Route handelt, die in die Konfiguration eingegeben wurde. Es ist erreichbar, da sich der virtuelle Pfad zwischen den Sites in einem funktionieren/aufbereitenden Zustand befindet.

- Als beworbene Route durch BGP (Nummer 6), mit einem Preis von 6. Dies gilt jetzt als Fallback-Route.

Da das Präfix gleich ist und die Kosten unterschiedlich sind, verwendet SD-WAN die virtuelle Pfadrouten, es sei denn, sie wird nicht verfügbar. In diesem Fall wird die Fallback-Route über BGP erlernt.

Betrachten wir nun die Route 172.20.20.0/24.

- Dies wird als Virtual Path Route (Nummer 9) erlernt, hat aber eine Art von Dynamik und einen Preis von 6. Dies bedeutet, dass die Remote-SD-WAN-Appliance diese Route über ein Routingprotokoll, in diesem Fall OSPF, gelernt hat. Standardmäßig sind die Routenkosten höher.
- SD-WAN lernt diese Route auch über BGP mit den gleichen Kosten, so dass in diesem Fall diese Route möglicherweise gegenüber der Virtual Path Route bevorzugt wird.

Um ein korrektes Routing zu gewährleisten, müssen wir die BGP-Routenkosten erhöhen, um sicherzustellen, ob wir eine Virtual Path Route haben und es ist die bevorzugte Route. Dies kann getan werden, indem Sie das Gewicht der Import-Filter-Route so anpassen, dass es höher ist als der Standardwert 6 ist.

Order: 100, Source Router: *, Destination: <Manual>, Prefix: eq, Next Hop: *, Protocol: Any, Cost: eq, Include: [checked], Enabled: [checked], Delete: [trash icon], Clone: [clone icon]

☐ Export Route to Citrix Appliances

NetScaler SD-WAN Cost: 10, Service Type: Local, Service Name: [dropdown]

☐ Eligibility Based On Gateway

☐ Eligibility Based On Path

Path: <None>

(auto), *, <Manual>, eq, *, Any, eq, [checkbox]

Apply Revert

Nach der Anpassung können wir die SD-WAN-Routentabelle auf der San Francisco-Appliance aktualisieren, um die angepassten Routenkosten anzuzeigen. Verwenden Sie die Filteroption, um die angezeigte Liste zu fokussieren.

Routes for routing domain : Default_RoutingDomain

Filter: 172.20.20.0/24 in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries (filtered from 16 total entries)

| Num | Network Addr | Gateway IP Address | Service | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|----------------|--------------------|---------|-----------|-----------------|------|---------|-------------|-----------------|------|-----------|----------|------------------|-------------------|
| 5 | 172.20.20.0/24 | * | NYC-SFO | YES | * | NYC | Dynamic | Virtual WAN | YES | 6 | 0 | YES | N/A | N/A |
| 8 | 172.20.20.0/24 | 192.168.10.1 | Local | YES | * | SFO | Dynamic | BGP | - | 10 | 0 | YES | N/A | N/A |

Showing 1 to 2 of 2 entries (filtered from 16 total entries)

Lassen Sie uns schließlich die erlernte Standardroute auf dem San Francisco SD-WAN betrachten. Wir wollen den gesamten Internetverkehr nach New York zurückholen. Wir können sehen, dass wir es mit dem virtuellen Pfad senden, wenn es oben ist, oder durch das MPLS-Netzwerk als Fallback.

Routes for routing domain : Default_RoutingDomain

Filter: 0.0.0.0/0 in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 16 total entries)

| Num | Network Addr | Gateway IP Address | Service | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|--------------|--------------------|-------------|-----------|-----------------|------|---------|-------------|-----------------|------|-----------|----------|------------------|-------------------|
| 12 | 0.0.0.0/0 | * | NYC-SFO | YES | * | NYC | Dynamic | Virtual WAN | YES | 6 | 0 | YES | N/A | N/A |
| 13 | 0.0.0.0/0 | 192.168.10.1 | Local | YES | * | SFO | Dynamic | BGP | - | 10 | 0 | YES | N/A | N/A |
| 14 | 0.0.0.0/0 | * | Passthrough | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |
| 15 | 0.0.0.0/0 | * | Discard | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |

Showing 1 to 4 of 4 entries (filtered from 16 total entries)

Wir sehen auch eine Passthrough und verwerfen Route mit Kosten 16. Dies sind automatische Routen, die nicht entfernt werden können. Wenn das Gerät inline ist, wird die Passthrough-Route als letztes Mittel verwendet. Wenn ein Paket nicht mit einer spezifischeren Route abgeglichen werden kann, wird SD-WAN diese an den nächsten Hop der Schnittstellengruppe weiterleiten. Wenn sich das SD-WAN außerhalb des Pfades befindet oder im Kante/Gateway-Modus, gibt es keinen Passthrough-Dienst. In diesem Fall wird das Paket mit der Standardverwerfungsrouten entfernt. Die Trefferanzahl gibt die Anzahl der Pakete an, die jede Route treffen, was bei der Fehlerbehebung hilfreich sein kann.

Wenn wir uns jetzt auf die New Yorker Website konzentrieren, möchten wir den Datenverkehr für entfernte Standorte (London und San Francisco) an die SD-WAN-Appliance weiterleiten, wenn der virtuelle Pfad aktiv ist.

Auf der New Yorker Website sind mehrere Subnetze verfügbar:

- 172.10.10.0/24 (direkt verbunden)
- 172.20.20.0/24 (über OSPF vom Core-Router B beworben)
- 172.30.30.0/24 (über OSPF vom Core-Router B beworben)

Wir sind auch verpflichtet, den Verkehrsfluss nach Dallas (10.100.1.0/24) über MPLS bereitzustellen.

Schließlich wollen wir alle Internet-gebundenen Verkehrswege zur Firewall E über 172.10.10.3 als nächsten Hop. SD-WAN lernt diese Standardroute über OSPF und über den virtuellen Pfad hinweg zu werben. Die Filter für die New Yorker Site sind:

| | Order | Source Router | Destination | Prefix | Next Hop | Protocol | Cost | Include | Enabled | Delete | Clone |
|---|--------|---------------|--------------------------|--------|----------|----------|------|-------------------------------------|-------------------------------------|--------|-------|
| | 100 | * | <Manual> 192.168.65.0/24 | eq * | * | Any | eq * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| <div><div><input type="checkbox"/> Export Route to Citrix Appliances</div><div><input type="checkbox"/> Eligibility Based On Gateway</div><div>NetScaler SD-WAN Cost: 6</div><div>Service Type: Local</div><div>Service Name:</div><div><input type="checkbox"/> Eligibility Based On Path</div><div>Path: <None></div></div> | | | | | | | | | | | |
| + | 200 | * | <Manual> 192.168.10.0/24 | eq * | * | Any | eq * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| + | 300 | * | <Manual> * | eq * | * | Any | eq * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| | (auto) | * | <Manual> * | eq * | * | Any | eq * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |

Der New York SD-WAN-Standort importiert alle Routen für das Management-Netzwerk. Dies kann ignoriert werden. Wir können uns auf Filter 200 konzentrieren.

| | | | | | | | | | | | |
|---|-----|---|--------------------------|------|---|-----|------|-------------------------------------|-------------------------------------|--|--|
| | 200 | * | <Manual> 192.168.10.0/24 | eq * | * | Any | eq * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| <div><div><input type="checkbox"/> Export Route to Citrix Appliances</div><div><input type="checkbox"/> Eligibility Based On Gateway</div><div>NetScaler SD-WAN Cost: 6</div><div>Service Type: Local</div><div>Service Name:</div><div><input type="checkbox"/> Eligibility Based On Path</div><div>Path: <None></div></div> | | | | | | | | | | | |

Filter 200 wird verwendet, um 192.168.10.0/24 (unser MPLS-Kern) für Erreichbarkeit zu importieren, aber nicht um ihn in den virtuellen Pfad zu exportieren. Aktivieren Sie das Kontrollkästchen **Einschließen**, und stellen Sie sicher, dass das Kontrollkästchen **Route zu Citrix Appliances exportieren** deaktiviert ist. Alle anderen Routen sind dann eingeschlossen.

Für die Exportfilter können wir die Route für 192.168.10.0/24 ausschließen. Dies liegt daran, dass wir als direkt verbundenes Subnetz am Standort San Francisco diese Route nicht an der Quelle herausfiltern können, so dass sie an diesem Ende unterdrückt wird.

| | Order | Network Address | Prefix | NetScaler SD-WAN Cost | Service Type | Site/Service Name | Gateway IP Address | Include | Enabled | Delete | Clone |
|---|--------|--------------------------|--------|-----------------------|--------------|-------------------|--------------------|-------------------------------------|-------------------------------------|--------|-------|
| + | 100 | <Manual> 192.168.10.0/24 | eq * | eq * | Any | <Any> | * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| | (auto) | <Manual> * | eq * | eq * | Any | <Any> | * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |

Lassen Sie uns nun die aktualisierte Routen-Tabelle überprüfen, die an der Kernroute in New York beginnt.

New York Router 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
```

Die Subnetze für San Francisco (10.80.1.0 & 10.81.1.0) und London (10.90.1.0) werden nun über die New York SD-WAN Appliance (172.10.10.10) beworben. Die Route 10.100.1.0/24 wird noch durch die Unterlage MPLS Router A beworben. Lassen Sie uns die New Yorker Site SD-WAN Routentabelle überprüfen.

New Yorker Standort SD-WAN Routentabelle:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 11 of 11 entries

| Num | Network Addr | Gateway IP Address | Service | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|-----------------|--------------------|-------------|-----------|-----------------|------|---------|----------|-----------------|------|-----------|----------|------------------|-------------------|
| 0 | 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 |

Wir können die richtigen Routen für die lokalen Subnetze sehen, die über OSPF gelernt wurden, eine Route zum Standort Dallas, die vom MPLS Router A gelernt wurde, und die Remote-Subnetze für die Standorte San Francisco und London. Schauen wir uns den MPLS Router A an. Dieser Router beteiligt sich an OSPF und 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
```

Aus der Routentabelle lernt dieser Router A die entfernten Subnetze über BGP und OSPF mit der administrativen Entfernung und Kosten der BGP-Route (20/5) niedriger als OSPF (110/10) und daher bevorzugt. In diesem Beispiel kann das Netzwerk, in dem nur eine Kernroute vorhanden ist, keine Bedenken verursachen. Der hier ankommende Datenverkehr würde jedoch über das MPLS-Netzwerk zugestellt und nicht an die SD-WAN-Appliance gesendet werden (172.10.10.10). Wenn wir eine vollständige Routing-Symmetrie beibehalten möchten, benötigen wir eine Routenkarte, um die AD/Metrik-Kosten so anzupassen, dass es Routenpräferenz von der Route kommt aus 172.10.10.10 statt der Route, die über eBGP gelernt wurde.

Alternativ kann eine Backdoor -Route so konfiguriert werden, dass der Router die OSPF-Route gegenüber der BGP-Route bevorzugt. Beachten Sie die statische Route für die virtuelle SD-WAN-IP-Adresse zur SD-WAN-Appliance des Londoner Standorts.

```
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
```

Dies ist erforderlich, um sicherzustellen, dass der virtuelle Pfad wieder an die SD-WAN-Appliance des New Yorker Standortes weitergeleitet wird, wenn der MPLS-Pfad ausfällt. Da gibt es eine Route für den 10.90.1.0/24 wird über 172.10.10.10 (New York SD-WAN) beworben. Es wird auch empfohlen, eine Überschreibungs-Service-Regel zu erstellen, um alle UDP 4.980 Pakete an der SD-WAN-Appliance zu löschen, um zu verhindern, dass der virtuelle Pfad zu sich selbst zurückkehrt.

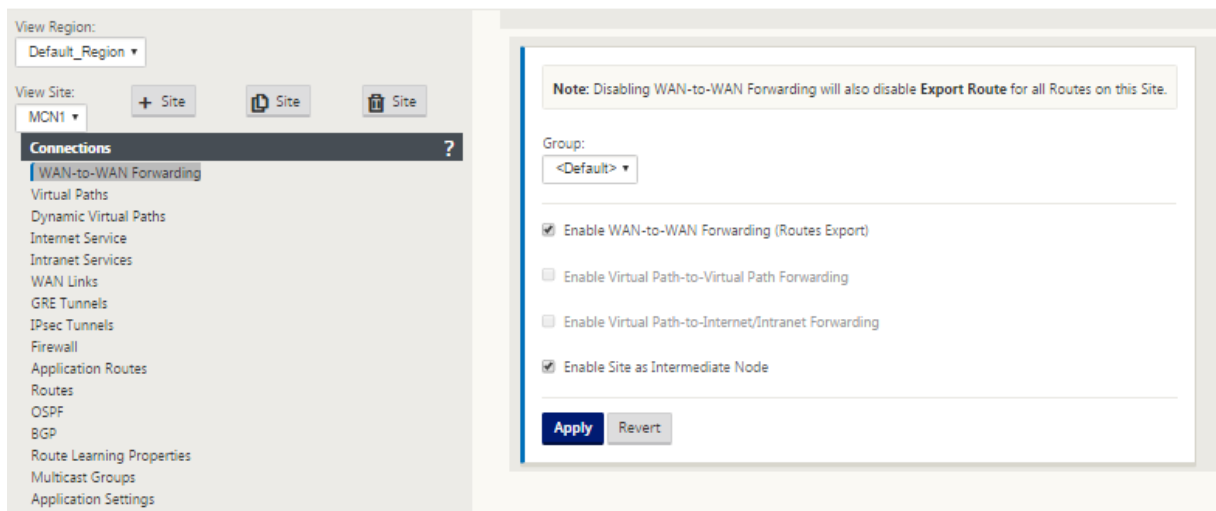
Dynamische virtuelle Pfade

Dynamische virtuelle Pfade können zwischen zwei Clientknoten erlaubt werden, virtuelle Pfade auf Anforderung für die direkte Kommunikation zwischen den beiden Standorten zu erstellen. Der Vorteil eines dynamischen virtuellen Pfads besteht darin, dass der Datenverkehr direkt von einem Clientknoten zum zweiten fließen kann, ohne das MCN oder zwei virtuelle Pfade durchlaufen zu müssen, wodurch der Verkehrsfluss Latenz ermöglicht wird. Dynamische virtuelle Pfade werden basierend auf benutzerdefinierten Datenverkehrsschwellenwerten dynamisch erstellt und entfernt. Diese Schwellenwerte sind entweder Pakete pro Sekunde (pps) oder Bandbreite (kbps) definiert. Diese Funktionalität ermöglicht eine dynamische SD-WAN-Overlay-Topologie mit vollem Netz.

Sobald die Schwellenwerte für dynamische virtuelle Pfade erfüllt sind, erstellen die Clientknoten dynamisch ihren virtualisierten Pfad zueinander unter Verwendung aller verfügbaren WAN-Pfade zwischen den Standorten und nutzen ihn folgendermaßen vollständig:

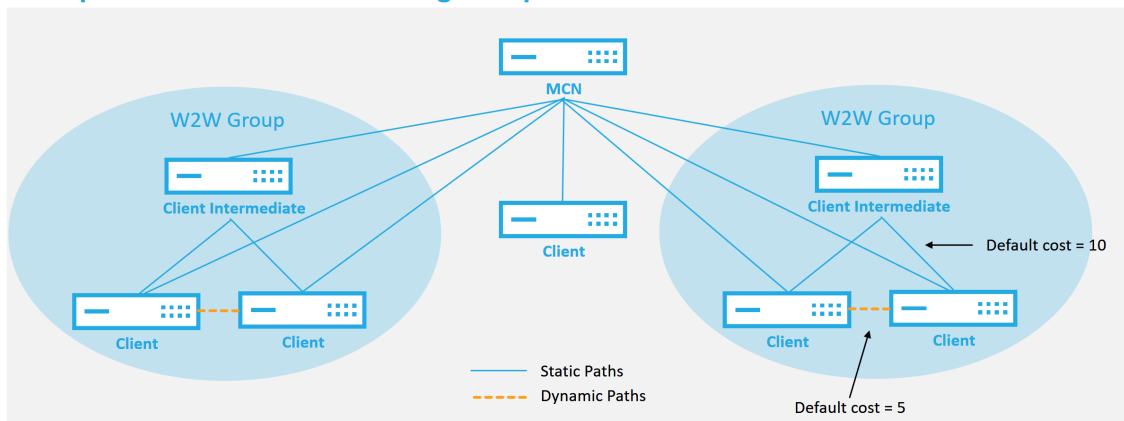
- Senden Sie Massendaten, falls vorhanden, und überprüfen Sie keinen Verlust, dann
- Senden Sie interaktive Daten und überprüfen Sie keinen Verlust, dann
- Senden von Echtzeitdaten, nachdem die Massen- und Interaktive Daten als stabil angesehen werden (kein Verlust oder akzeptable Werte)
- Wenn keine Massen- oder interaktive Daten vorhanden sind, senden Sie Echtzeitdaten, nachdem der dynamische virtuelle Pfad für einen Zeitraum stabil war
- Wenn die Benutzerdaten für einen benutzerdefinierten Zeitraum unter die konfigurierten Schwellenwerte fallen, wird der dynamische virtuelle Pfad abgerissen

Dynamische virtuelle Pfade haben das Konzept einer Zwischen-Site. Der Zwischenstandort kann ein MCN-Standort oder ein anderer Standort im Netzwerk sein, für den der statische virtuelle Pfad konfiguriert und mit zwei oder mehr anderen Clientknoten verbunden ist. Eine weitere Anforderung zur Entwurfsüberlegung besteht darin, dass die WAN-zu-WAN-Weiterleitung aktiviert ist, sodass alle Routen von allen Standorten an die Clientknoten angekündigt werden können, auf denen der dynamische virtuelle Pfad gewünscht wird. **Standort als Zwischenknoten aktivieren** muss zusätzlich zur **WAN-zu-WAN-Weiterleitung** aktiviert werden, damit dieser Zwischenstandort die Kommunikation von Client-Knoten überwachen und bestimmen kann, wann der dynamische Pfad eingerichtet und abgerissen werden muss.



In der SD-WAN-Konfiguration können mehrere WAN-zu-WAN-Weiterleitungsgruppen zulässig sein, wodurch die vollständige Kontrolle über die Pfadeinrichtung zwischen bestimmten Clientknoten und nicht anderen ermöglicht wird.

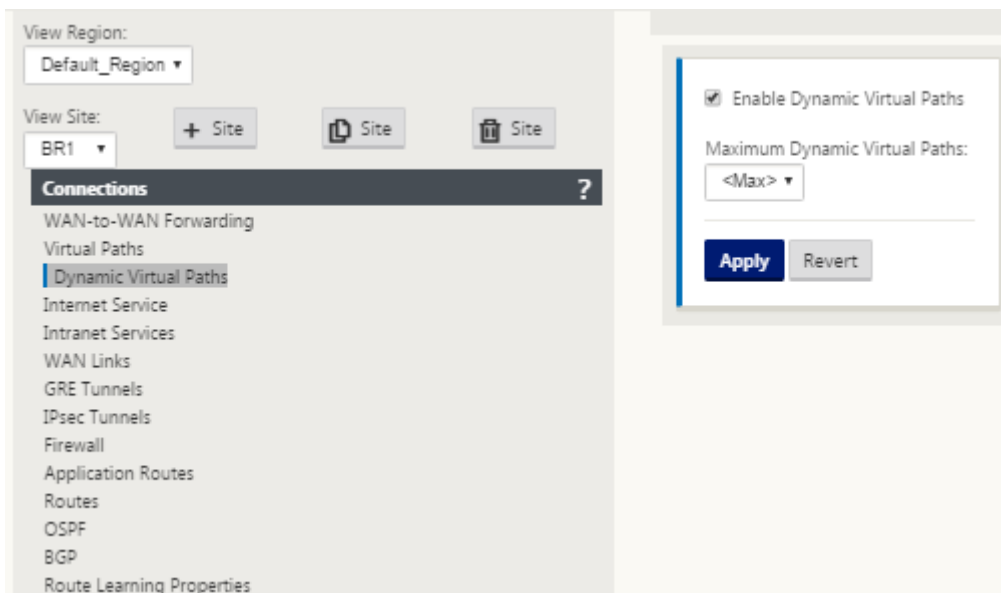
Multiple WAN to WAN Forwarding Groups



WAN to WAN Forwarding Group:

- A network can have multiple WAN to WAN Forwarding Groups
- Direct dynamic path will have a lower cost than through the intermediate node

Damit Clientknoten als Zwischenstandorte arbeiten können, muss zwischen ihm und den Clients, die dieser **WAN-zu-WAN-Weiterleitungsgruppe** zugeordnet sind, ein statischer virtueller Pfad konfiguriert werden. Darüber hinaus müssen Clientknoten die Option **Dynamischen virtuellen Pfad aktivieren** für jeden Clientknoten aktiviert.



Jedes SD-WAN-Gerät verfügt über eine eigene eindeutige Routentabelle mit den folgenden Details für jede Route:

- Zahl —Reihenfolge der Route dieser Appliance basierend auf dem Vergleichsprozess (niedrigste Zahl, die zuerst verarbeitet wurde)
- Netzwerkadresse —Subnetz oder Hostadresse
- Gateway bei Bedarf
- Service —welcher Dienst für diese Route angewendet wird
- Firewall-Zone —die Firewall-Zonenklassifizierung der Route
- Erreichbar —Gibt an, ob der Status Virtueller Pfad für diese Site aktiv ist
- Standort —Der Name des Standorts, an dem die Route erwartet wird
- Typ —Identifizierung des Streckentyps (statisch oder dynamisch)
- Neighbor Direct
- Kosten - Kosten der jeweiligen Strecke
- Trefferanzahl —wie oft die Route pro Paket verwendet wurde. Dies würde verwendet, um zu überprüfen, ob eine Route richtig getroffen wird.
- Berechtigte
- Berechtigungsart
- Berechtigungswert

Der folgende Code ist ein Beispiel für eine SD-WAN-Standortroute:

Routes for routing domain : Default_RoutingDomain

Filter: in

Show entries Showing 1 to 13 of 13 entries

| Num | Network Addr | Gateway IP Address | Service | Firewall Zone | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|------------------|--------------------|-------------|------------------------|-----------|-----------------|--------|--------|----------|-----------------|------|-----------|----------|------------------|-------------------|
| 0 | 172.16.10.0/24 | 192.168.15.1 | DC-AWS | Default_LAN_Zone | YES | * | DC | Static | - | - | 4 | 0 | YES | N/A | N/A |
| 1 | 192.168.100.0/24 | * | Local | Default_LAN_Zone | YES | * | AWS | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 2 | 192.168.15.0/24 | * | DC-AWS | Default_LAN_Zone | YES | * | DC | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 3 | 172.16.250.0/24 | * | DC-AWS | Default_LAN_Zone | YES | * | DC | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 4 | 172.16.150.0/24 | * | DC-AWS | Default_LAN_Zone | YES | * | DC | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 5 | 192.168.200.0/24 | * | DC-AWS | Default_LAN_Zone | NO | * | Azure | Static | - | - | 15 | 0 | YES | N/A | N/A |
| 6 | 192.168.10.0/24 | * | DC-AWS | Default_LAN_Zone | YES | * | Branch | Static | - | - | 15 | 0 | YES | N/A | N/A |
| 7 | 172.16.200.0/24 | * | DC-AWS | Default_LAN_Zone | YES | * | Branch | Static | - | - | 15 | 0 | YES | N/A | N/A |
| 8 | 172.16.100.0/24 | * | DC-AWS | Default_LAN_Zone | YES | * | Branch | Static | - | - | 15 | 0 | YES | N/A | N/A |
| 9 | 172.16.30.0/24 | * | DC-AWS | Default_LAN_Zone | YES | * | Branch | Static | - | - | 15 | 0 | YES | N/A | N/A |
| 10 | 0.0.0.0/0 | * | Internet | Untrusted_Internet_Zon | YES | * | * | Static | - | - | 5 | 1 | YES | N/A | N/A |
| 11 | 0.0.0.0/0 | * | Passthrough | Any | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |
| 12 | 0.0.0.0/0 | * | Discard | Any | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |

Showing 1 to 13 of 13 entries

Beachten Sie aus der vorangegangenen SD-WAN-Routentabelle, dass in herkömmlichen Routern normalerweise mehr Elemente nicht verfügbar sind. Am bemerkenswertesten ist die Spalte Erreichbar, die die Route je nach WAN-Pfadstatus entweder aktiv oder inaktiv (ja/nein) macht. Die hier aufgelisteten Routen werden basierend auf verschiedenen Zuständen des Dienstes unterdrückt (der virtuelle Pfad ist als Beispiel heruntergefahren). Andere Ereignisse, die erzwingen können, dass eine Route nicht berechtigt ist, sind Pfad-Down-Status, nächster Hop nicht erreichbar oder WAN-Link down.

Aus der obigen Tabelle können wir 14 definierte Routen sehen. Eine Beschreibung der Routen oder Streckengruppen wird wie folgt beschrieben:

- Route 0 —Auf dem MCN handelt es sich um eine Host-Subnetzroute, die sich am DC-Standort befindet. 172.16.10.0/24 befindet sich im DC-LAN und 192.168.15.1 ist das Gateway im LAN, das der nächste Hop ist, der zu diesem Subnetz gelangen wird.
- Route 1 - Dies ist eine lokale Route zu diesem SD-WAN-Gerät, das die Routentabelle anzeigt.
- Route 2—4 —Dies sind die Subnetze, die Teil der virtuellen Schnittstellen sind, die für den DC-Standort SD-WAN konfiguriert sind. Diese Subnetze werden von den definierten vertrauenswürdigen virtuellen Schnittstellen abgeleitet.
- Route 5 —Dies ist eine freigegebene Route zu einem anderen Clientknoten, der vom MCN gemeinsam genutzt wird, mit dem Erreichbarkeitsstatus Nein aufgrund des virtuellen Pfads zwischen diesem Standort und dem MCN.
- Route 6—9 —Diese Routen existieren an einem anderen Clientstandort. Für diese Route wird eine virtuelle Pfadroute für den passenden WAN-Datenverkehr erstellt, der für die Remote-Site auf dem virtuellen Pfad bestimmt ist.
- Route 10 —Wenn der Internetdienst definiert ist, fügt das System eine Catch All Route für direkte Internetausbrüche für diese lokale Site hinzu.
- Route 11 —Passthrough ist die Standardroute, die das System immer hinzufügt, damit Pakete durchfließen können, falls es keine Übereinstimmung auf vorhandenen Routen

gibt. Der Passthrough wird nicht gepflegt, normalerweise werden lokale Broadcasts und ARP-Datenverkehr diesem Dienst zugeordnet.

- Route 12 —Verwerfen ist die Standardroute, die das System immer hinzufügt, um etwas undefiniertes zu löschen.

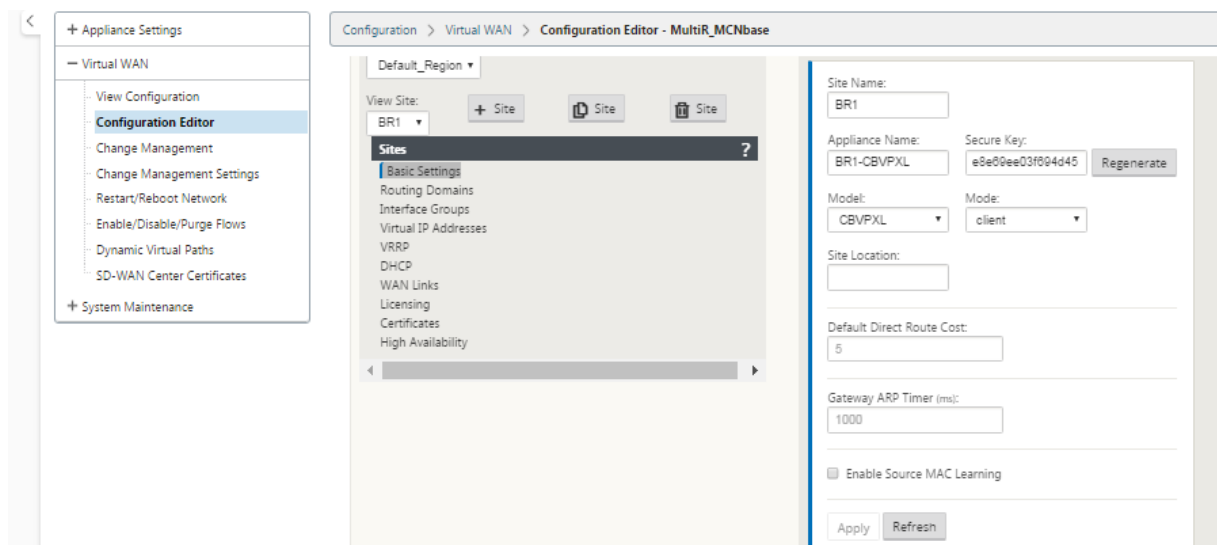
Die Standardwerte für die Routenkosten:

- WAN-zu-WAN-Weiterleitung —10
- Standardkosten für direkte Route —5
- Automatisch generierte Routen —5
- Virtueller Pfad —5
- Lokal —5
- Intranet —5
- Internet —5
- Durchgang —5
- Optional —Route ist 0.0.0.0/0 definiert als Service-Level

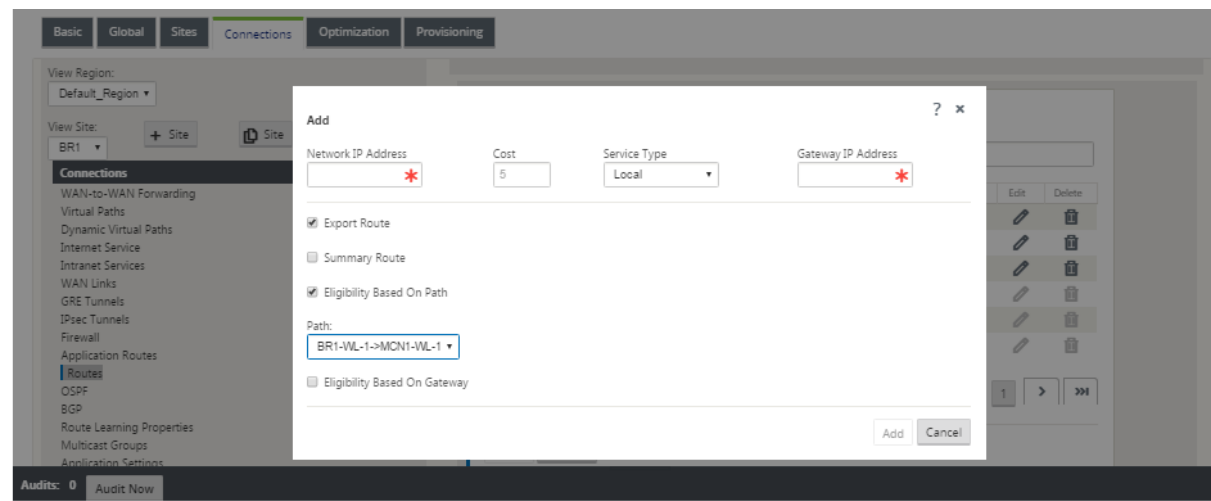
Nach der Definition dieser Routen ist es wichtig zu verstehen, wie der Verkehr über die definierten Routen fließt. Diese Verkehrsflüsse sind in folgende Flüsse unterteilt:

- LAN zu WAN (Virtual Path) —Datenverkehr in den SD-WAN-Overlay-Tunnel
- WAN zu LAN (Virtual Path) —Datenverkehr im SD-WAN-Overlay-Tunnel
- Nicht-Virtual Path Traffic —Datenverkehr an das Unterlagennetz weitergeleitet

Die standardmäßigen Routenkosten können pro Standort geändert werden. Die Konfiguration finden Sie unter **View Site > Basic Settings** :



Statische Routen können pro Standort unter dem Knoten **Verbindungen > Standort > Routes** definiert werden:



Sie stellen fest, dass Routen an den virtuellen Pfad oder die Gateway-IP-Verfügbarkeit gebunden werden können. Internetrouten können in das virtuelle Pfad-Overlay exportiert werden oder nicht je nach gewünschtem Verhalten. Sie können auch statische Virtual Path Routen erstellen, um den Datenverkehr zu einem virtuellen Pfad zu erzwingen, obwohl wir nicht das Präfix für SD-WAN angekündigt bekommen (dh eine kostengünstigere Route der letzten Instanz). SD-WAN kann auch lokale Subnetze unterdrücken, indem die Virtual IP Address (VIP) privat gemacht wird.

| IP Address / Prefix | Virtual Interface | Firewall Zone | Identity | Private | Security | Delete |
|---------------------|-------------------|------------------|-------------------------------------|-------------------------------------|----------|--------|
| 172.10.10.10/24 | E1Vlan0 | Default_LAN_Zone | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Trusted | |
| 172.10.10.11/24 | E1Vlan0 | Default_LAN_Zone | <input type="checkbox"/> | <input type="checkbox"/> | Trusted | |

Apply

Revert

Hinweis

Die Konfiguration erfordert mindestens einen nicht-privaten VIP in jeder Routendomäne.

Intranet- und Internetrouten

Für Intranet- und Internetdiensttypen muss der Benutzer eine SD-WAN-Verbindung definiert haben, um diese Arten von Diensten zu unterstützen. Es ist eine Voraussetzung für alle definierten Routen für einen dieser Dienste. Wenn die WAN-Link nicht zur Unterstützung des Intranetdienstes definiert ist, wird sie als lokale Route betrachtet. Die Intranet-, Internet- und Passthrough-Routen sind nur für die Standort/Appliance relevant, für die sie konfiguriert sind.

Bei der Definition von Intranet-, Internet- oder Passthrough-Routen gelten folgende Entwurfsüberlegungen:

- Dienst muss auf der WAN-Verbindung definiert sein (Intranet/Internet —erforderlich)
- Intranet/Internet muss Gateway für die WAN-Verbindung definiert haben
- Relevant für lokales SD-WAN-Gerät
- Intranet-Routen können über den virtuellen Pfad erlernt werden, werden jedoch zu höheren Kosten durchgeführt.
- Mit Internet Service wird automatisch eine Standard-Route erstellt (0.0.0.0/0) fangen alle Route mit einem maximalen Preis
- Gehen Sie nicht davon aus, dass Passthrough funktioniert, es muss getestet/verifiziert werden, auch testen Sie mit Virtual Path herunter/deaktiviert, um das gewünschte Verhalten zu überprüfen
- Routentabellen sind statisch, es sei denn, die Routenlernfunktion ist aktiviert

Der maximal unterstützte Grenzwert für mehrere Routingparameter lautet wie folgt:

- Maximale Routingdomänen: 255
- Maximale Zugriffsschnittstellen pro WAN-Link: 64
- Maximale BGP-Nachbarn pro Standort: 255
- Maximale OSPF-Fläche pro Standort: 255
- Maximale virtuelle Schnittstellen pro OSPF-Bereich: 255
- Maximale Route Learning Importfilter pro Site: 512
- Maximale Routenlern-Exportfilter pro Site: 512
- Maximale BGP-Routing-Richtlinien: 255
- Maximale BGP-Community-String-Objekte: 255

Routingdomäne

May 10, 2021

Citrix SD-WAN ermöglicht das Segmentieren von Netzwerken für mehr Sicherheit und Verwaltbarkeit mithilfe der Routingdomäne. Sie können beispielsweise Gastnetzwerkverkehr vom Mitarbeiterdatenverkehr trennen, eigene Routingdomänen erstellen, um große Unternehmensnetzwerke zu segmentieren, und den Datenverkehr segmentieren, um mehrere Kundennetzwerke zu unterstützen. Jede

Routingdomäne verfügt über eine eigene Routingtabelle und ermöglicht die Unterstützung überlappender IP-Subnetze.

Citrix SD-WAN Appliances implementieren OSPF- und BGP-Routingprotokolle für die Routingdomänen, um den Netzwerkverkehr zu steuern und zu segmentieren.

Ein virtueller Pfad kann unabhängig von der Definition des Zugriffspunkts über alle Routingdomänen kommunizieren. Dies ist möglich, da die SD-WAN-Kapselung die Routingdomäneninformationen für das Paket enthält. Daher wissen beide Endnetzwerke, wohin das Paket gehört. Es ist nicht notwendig, für jede Routingdomäne einen WAN-Link oder eine Access Interface zu erstellen.

Im Folgenden finden Sie eine Liste der Punkte, die bei der Konfiguration der Routingdomänenfunktionalität berücksichtigt werden sollten:

- Standardmäßig sind Routingdomänen auf einem MCN aktiviert.
- Routingdomänen sind auf den Zweigstandorten aktiviert.
- Jeder aktivierten Routingdomäne muss eine virtuelle Schnittstelle und eine virtuelle IP zugeordnet sein.
- Die Routing Auswahl ist Teil aller folgenden Konfigurationen:
 - Schnittstellengruppe
 - Virtuelle IP
 - GRE
 - WAN-Link -> Zugriffsoberfläche
 - IPsec-Tunnel
 - Routen
 - Regeln
- Routingdomänen werden in der Webschnittstellenkonfiguration nur verfügbar gemacht, wenn mehrere Domänen erstellt werden.
- Für eine öffentliche Internetverbindung kann nur eine primäre und sekundäre Zugriffsschnittstelle erstellt werden.
- Für einen privaten Intranet/MPLS-Link kann pro Routingdomäne eine primäre und sekundäre Zugriffsoberfläche erstellt werden.

Routingdomäne konfigurieren

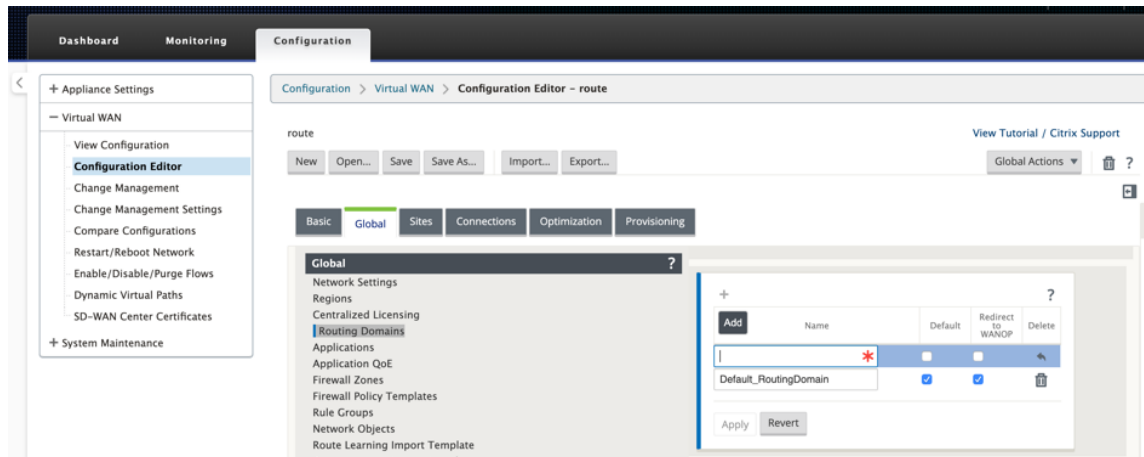
May 10, 2021

Citrix SD-WAN Appliances ermöglichen die Konfiguration von Routingprotokollen, die einen zentralen Verwaltungspunkt für die Verwaltung eines Unternehmensnetzwerks, eines Zweigstellennetzwerks

oder eines Rechenzentrumsnetzwerks bereitstellen. Sie können bis zu 254 Routingdomänen konfigurieren.

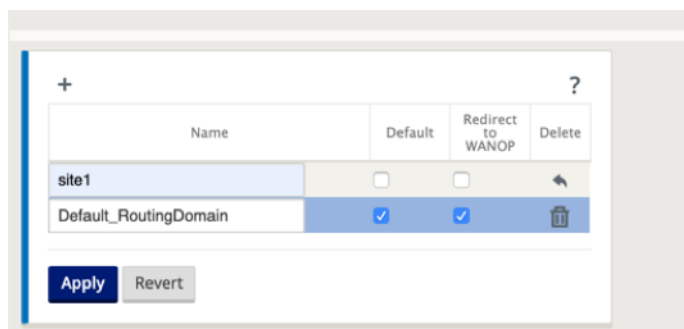
So konfigurieren Sie die Routingdomäne:

1. Navigieren Sie in der SD-WAN-Weboberfläche zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor**. Navigieren Sie im **Konfigurations-Editor** zu **Global > Routingdomänen**, klicken Sie auf **Hinzufügen (+)**, und geben Sie einen Namen für die neue Routingdomäne ein.

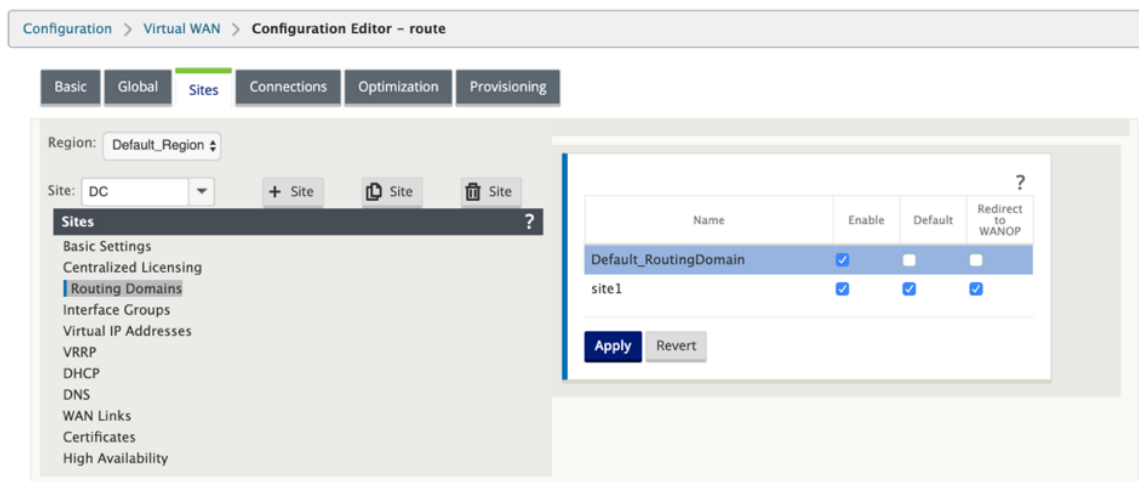


2. Wenn Sie diese Routingdomäne standardmäßig verwenden möchten, aktivieren Sie das Kontrollkästchen **Standard**. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern. Wenn Sie eine einzelne Routingdomäne implementieren möchten, ist keine explizite Konfiguration erforderlich.

Alle neuen Konfigurationen werden automatisch mit einer Standard-Routingdomäne gefüllt.



3. Navigieren Sie zu **Sites > [Client-Sitenname] > Routingdomänen**. Aktivieren Sie das Kontrollkästchen **Aktivieren**, um eine konfigurierte Routingdomäne für den Standort zu aktivieren.
4. Aktivieren Sie das Kontrollkästchen **Standard**, um diese Routingdomäne als Standard für den Standort festzulegen. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.



Hinweis

Wenn Sie die Option Für eine Routingdomäne **aktivieren** deaktivieren, ist sie nicht für die Verwendung am Standort verfügbar.

Ab Version 11.0.2 sind **Routing-Domänen ohne routable Virtual IPs (VIPs)** mit den folgenden Funktionen zulässig:

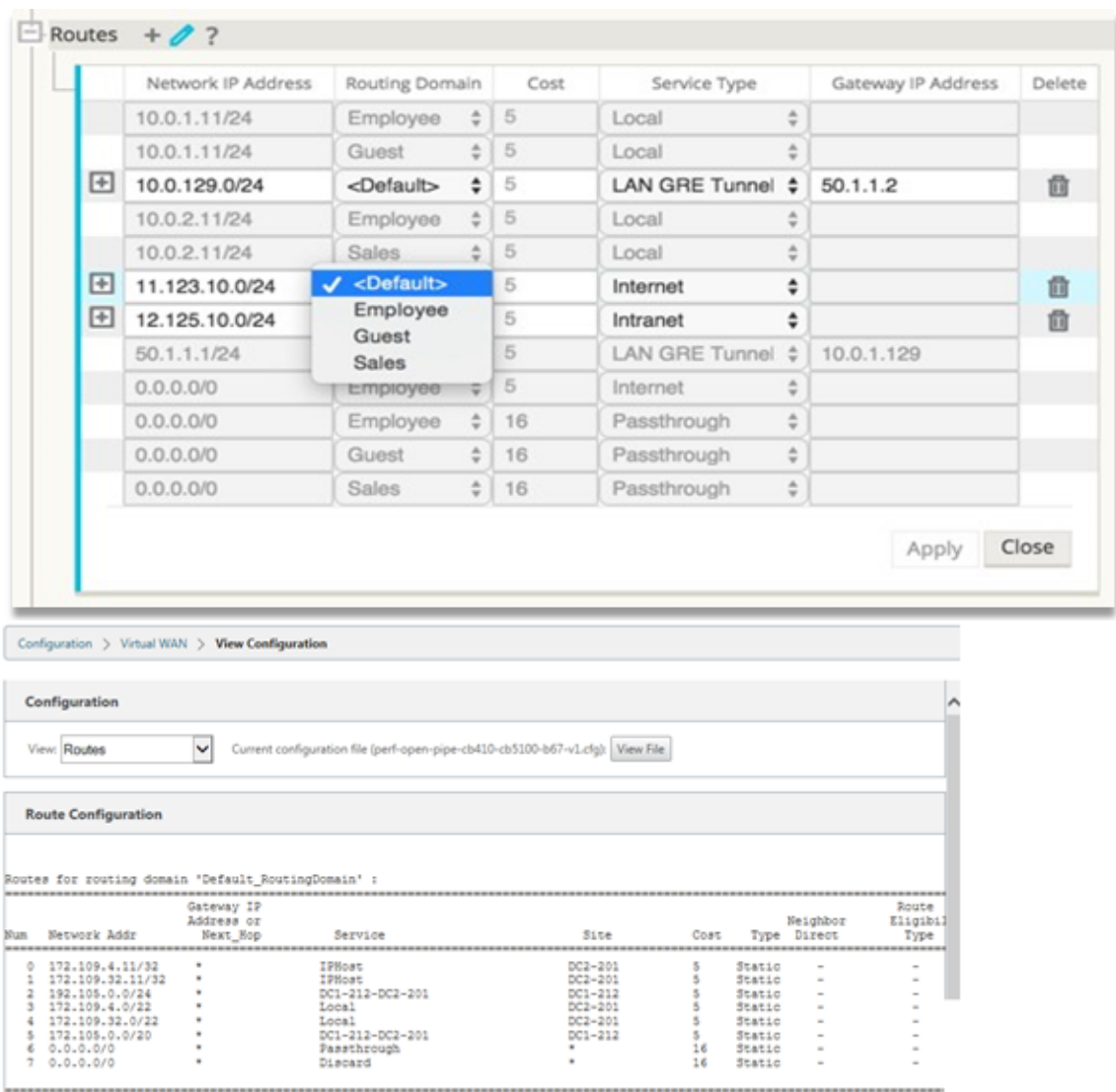
- Erlauben Sie einem Gerät, eine Routingdomäne für nicht vertrauenswürdige oder keine Schnittstellen zu haben.
- Zweige können untereinander über eine Routingdomäne kommunizieren, die keine physische Präsenz an einem Zwischenstandort hat.

Routen konfigurieren

May 10, 2021

So konfigurieren Sie Routen:

1. Navigieren Sie im **Konfigurations-Editor** zu **Verbindungen** > **[Standortname]** > **Routen**.
2. Wählen Sie eine **Routingdomäne** aus dem Dropdownmenü. Neue Routen werden automatisch der Standard-Routingdomäne zugeordnet. Ausführliche Anweisungen finden Sie unter [Konfigurieren von Routen](#).



Nachdem Sie Routen konfiguriert haben, überprüfen Sie die Routingtabellen für die konfigurierte Routingdomäne, indem Sie zu **Konfiguration > Virtuelles WAN > Ansicht > Routen** navigieren.

Verwenden von CLI für den Zugriff auf Routing

May 10, 2021

In Citrix SD-WAN Version 10.0 können Sie zusätzliche Informationen zum dynamischen Routing und zum Protokollstatus anzeigen. Geben Sie den folgenden Befehl und die folgende Syntax ein, um auf den Routing-Daemon zuzugreifen und die Liste der Befehle anzuzeigen.

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

Dynamisches Routing

May 10, 2021

Die folgenden zwei dynamischen Routingprotokolle werden von Citrix SD-WAN unterstützt:

- Öffnen Sie zuerst den kürzesten Pfad (OSPF)
- Border Gateway Protocol (BGP)

OSPF

OSPF ist ein Routing-Protokoll, das von der Interior Gateway Protocol (IGP) -Gruppe der Internet Engineering Task Force (IETF) für IP-Netzwerke entwickelt wurde. Es enthält die frühe Version des Intermediate System to Intermediate System (IS-IS) Routingprotokolls von OSI.

Das OSPF-Protokoll ist offen, was bedeutet, dass sich seine Spezifikation in der gemeinfreien Domäne befindet (RFC 1247). OSPF basiert auf dem Shortest Path First (SPF) Algorithmus namens Dijkstra. Es ist ein Link-State-Routing-Protokoll, das das Senden von Link-State-Advertisements (LSAs) an alle anderen Router innerhalb desselben hierarchischen Bereichs fordert. Informationen zu angehängten Schnittstellen, verwendeten Metriken und anderen Variablen sind in OSPF-LSAs enthalten. OSPF-Router sammeln Link-State-Informationen an, die vom SPF-Algorithmus verwendet werden, um den kürzesten Pfad zu jedem Knoten zu berechnen.

Sie können jetzt Citrix SD-WAN Appliances (Standard und Premium (Enterprise) Editions) konfigurieren, um Routen zu lernen und Routen mit OSPF anzukündigen.

Hinweis

- Citrix SD-WAN Appliances sind nicht als Designated Router (DR) und BDR (Backup Designated Router) in jedem Multi-Access-Netzwerk beteiligt, da die Standard-DR-Priorität auf "0" festgelegt ist.
- Die Citrix SD-WAN Appliance unterstützt keine Zusammenfassung als Area Border Router (ABR).

Konfigurieren von OSPF

So konfigurieren Sie OSPF:

1. Navigieren Sie im **Konfigurations-Editor** zu **Verbindungen > Region > Standort > OSPF > Grundeinstellungen**.

2. Klicken Sie auf **Aktivieren**, wählen Sie Werte für die folgenden Parameter aus, oder geben Sie Werte ein, und klicken Sie auf **Übernehmen**.

- **Werbung für Citrix SD-WAN Routen:** Erlauben Sie, dass Citrix SD-WAN Routen über OSPF angekündigt werden. Sie können auch ein Tag für die OSPF-Umverteilung angeben.
- **Werbung für BGP-Routen:** Erlauben Sie, dass Routen, die von BGP-Peers gelernt wurden, über OSPF beworben werden. Sie können auch ein Tag für die OSPF-Umverteilung angeben.
- **Router-ID:** Die eindeutige Router-ID, der Router wird für OSPF-Anzeigen verwendet. Wenn die Router-ID nicht angegeben ist, wird sie automatisch als niedrigste virtuelle IP ausgewählt, die im SD-WAN-Netzwerk gehostet wird.
- **OSPF-Routentyp exportieren:** Geben Sie die Citrix SD-WAN-Routen an OSPF-Peers als innerbereichsinterne oder externe Routen an.
- **OSPF-Routengewicht exportieren:** Wenn Sie Citrix SD-WAN Routen nach OSPF exportieren, fügen Sie dieses Gewicht zu den Citrix SD-WAN-Kosten jeder Route hinzu.
- **Protokolleinstellung:** Wenn Präfixe über mehrere Routingprotokolle gelernt werden, bestimmt der Wert der Protokolleinstellung die Auswahl des Routingprotokolls. Weitere Informationen finden Sie unter [Protokollpräferenz](#).

The screenshot displays the Citrix SD-WAN configuration interface. At the top, there are tabs: Basic, Global, Sites, **Connections** (selected), Optimization, and Provisioning. Below the tabs, the 'Region' is set to 'Default_Region'. On the left, a 'Connections' sidebar lists various options: WAN-to-WAN Forwarding, Virtual Paths, Dynamic Virtual Paths, Internet Service, Intranet Services, WAN Links, GRE Tunnels, IPsec Tunnels, Firewall, Application Routes, Routes, **OSPF** (highlighted), BGP, Route Learning Properties, Multicast Groups, and Applications. The main panel shows the 'Basic Settings' for OSPF. It includes checkboxes for 'Enable', 'Advertise Citrix SD-WAN Routes' (with a 'Tag Value' of 10), and 'Advertise BGP Routes' (with a 'Tag Value' of 20). The 'Router ID' is set to '5.5.5.5'. The 'Export OSPF Route Type' is set to 'Type 5 AS Extern'. The 'Export OSPF Route Weight' is set to '4'. The 'Protocol Preference' is set to '150'. At the bottom, there are 'Apply' and 'Revert' buttons.

3. Erweitern Sie **OSPF > Bereich**, und klicken Sie auf **Bearbeiten**.

Section: Areas

ID

Stub Area Delete

Virtual Interfaces

| Name | Source IP Address | Interface Cost | Authentication Type | Password | Network Type | Hello Interval | Dead Interval | Delete |
|------------------|-------------------|----------------|---------------------|----------|--------------|----------------|---------------|--------|
| VirtualInterface | 172.111.64.5 | 10 | None | | Auto | 10 | 40 | |

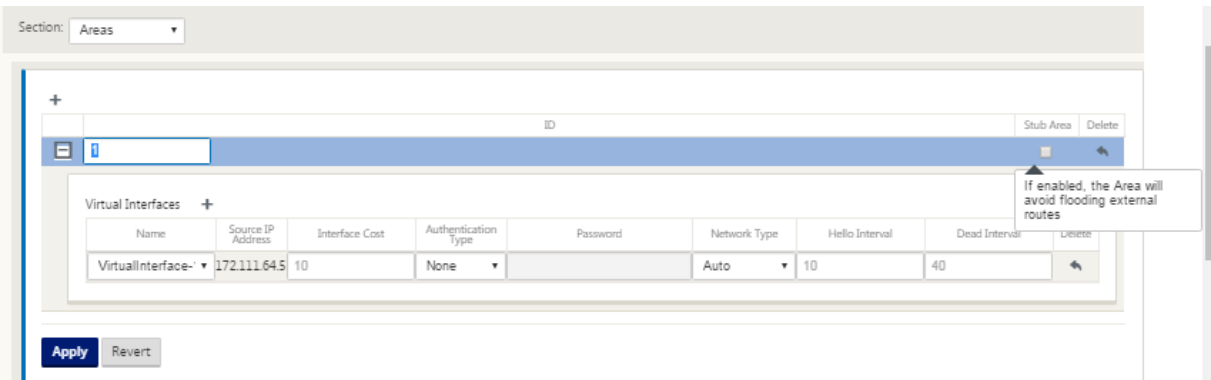
Apply Revert

4. Geben Sie eine **Bereichs-ID** ein, um Routen zu lernen und anzukündigen.
5. Wenn Identity nicht für eine bestimmte virtuelle IP-Adresse geprüft wird, ist die zugeordnete virtuelle Schnittstelle für IP-Dienste nicht verfügbar.
6. Wählen Sie eine der verfügbaren virtuellen Schnittstellen aus dem Menü **Name**. Das virtuelle Interface bestimmt die **Quell-IP-Adresse**.
7. Geben Sie die **Schnittstellenkosten** ein (10 ist der Standardwert).
8. Wählen Sie im Menü einen **Authentifizierungstyp** aus.
9. Wenn Sie in Schritt 8 **Kennwort** oder **MD5** gewählt haben, geben Sie das zugehörige Textfeld Kennwort ein.
10. Geben Sie im Feld **Hallo Intervall** die Zeit ein, die zwischen dem Senden von Hello Protokollpaketen an direkt verbundene Nachbarn gewartet werden soll (10 Sekunden sind die Standardeinstellung).
11. Geben Sie im Feld **Dead Intervall** das zu wartende Intervall ein, bevor Sie einen Router als tot markieren. Das standardmäßige Deadintervall beträgt 40 Sekunden.
12. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Stub Bereich

Stub-Bereiche sind von externen Routen abgeschirmt und erhalten Informationen über Netzwerke, die zu anderen Bereichen derselben OSPF-Domäne gehören.

Aktivieren Sie das Kontrollkästchen **Stub Area**.



OSPF-Umverteilung-Tags

Sie können OSPF-Tags verwenden, um Routingschleifen während der gegenseitigen Umverteilung zwischen OSPF und anderen Protokollen zu verhindern. Wenn in der OSPF-Domäne SD-WAN- und BGP-Learned Routen zu demselben Subnetz vorhanden sind, identifiziert der OSPF-Schleifenpräventionsmechanismus ihn als Schleife und ignoriert die Routen. Durch die Angabe verschiedener Tags für SD-WAN- und BGP-Learned Routen können diese Routen in der OSPF-Routingtabelle installiert werden.

Sie können die OSPF-Umverteilung-Tags für Routen konfigurieren, die über SD-WAN und BGP gelernt wurden, im Abschnitt OSPF, **Grundeinstellungen**.

Section: Basic Settings ▾

☑ Enable

☑ Advertise Citrix SD-WAN Routes Tag Value: 10

☑ Advertise BGP Routes Tag Value: 20

Router ID:
5.5.5.5

Export OSPF Route Type:
Type 5 AS Exterr ▾

Export OSPF Route Weight:
4

Protocol Preference:
150

Apply Revert

BGP

BGP ist ein interautonomes System Routing-Protokoll. Ein autonomes Netzwerk oder eine Gruppe von Netzwerken wird unter einer gemeinsamen Verwaltung und mit gemeinsamen Routing-Richtlinien verwaltet. BGP wird verwendet, um Routing-Informationen für das Internet auszutauschen und ist das zwischen ISPs verwendete Protokoll. Kundennetzwerke stellen Interior Gateway Protokolle wie RIP oder OSPF für den Austausch von Routinginformationen in ihren Netzwerken bereit. Kunden stellen eine Verbindung zu ISPs her, und ISPs verwenden BGP, um Kunden- und ISP-Routen auszutauschen. Wenn BGP zwischen autonomen Systemen (AS) verwendet wird, heißt das Protokoll External BGP (EBGP). Wenn ein Dienstanbieter BGP verwendet, um Routen innerhalb

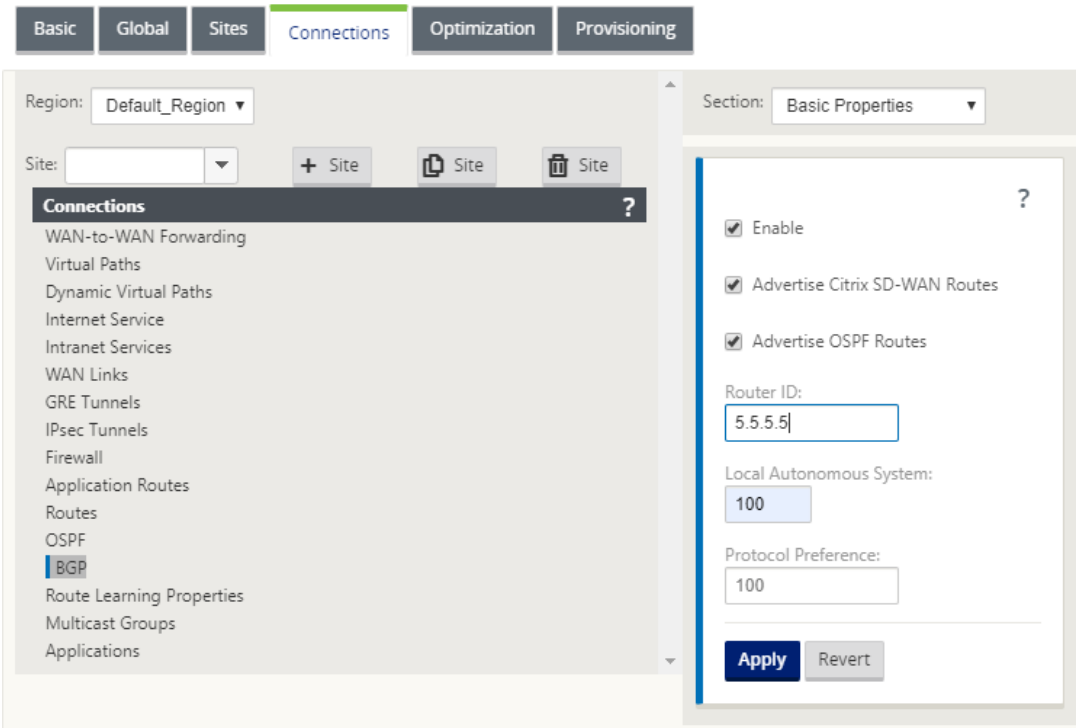
eines AS auszutauschen, wird das Protokoll Interior BGP (IBGP) genannt.

BGP ist ein robustes und skalierbares Routing-Protokoll, das im Internet bereitgestellt wird. Um Skalierbarkeit zu erreichen, verwendet BGP viele Routenparameter, die als Attribute bezeichnet werden, um Routingrichtlinien zu definieren und eine stabile Routingumgebung zu erhalten. BGP-Nachbarn tauschen vollständige Routinginformationen aus, wenn die TCP-Verbindung zwischen Nachbarn zum ersten Mal hergestellt wird. Wenn Änderungen an der Routing-Tabelle erkannt werden, senden die BGP-Router nur die Routen, die sich geändert haben. BGP-Router senden keine regelmäßigen Routing-Updates und geben nur den optimalen Pfad zu einem Zielnetzwerk an. Sie können Citrix SD-WAN Appliances konfigurieren, um Routen zu lernen und Routen mit BGP anzukündigen.

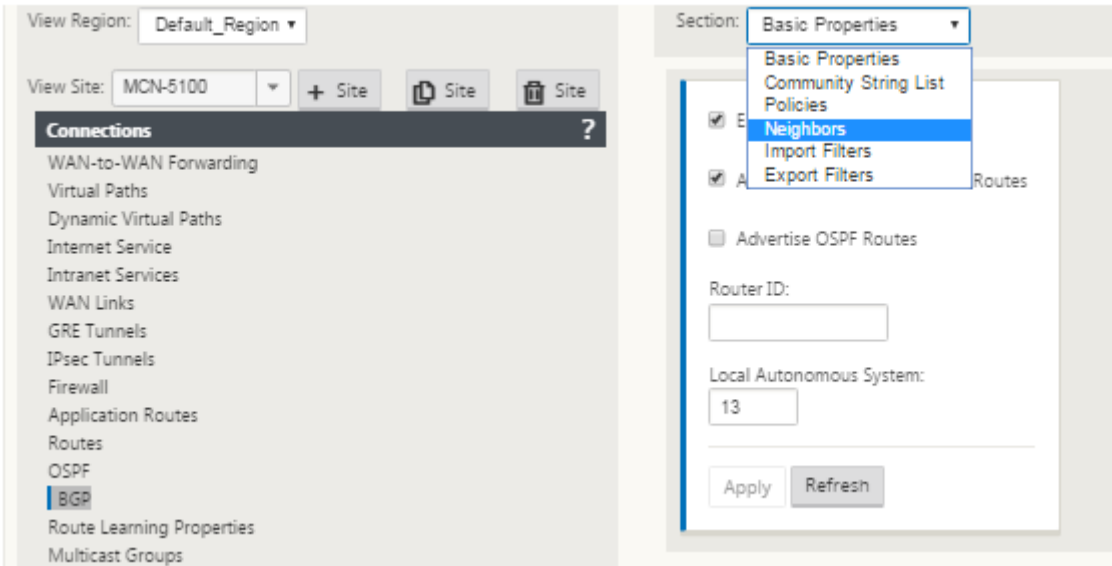
BGP konfigurieren

So konfigurieren Sie BGP:

1. Navigieren Sie im **Konfigurations-Editor** zu **Verbindungen > Region > Standort > BGP > Grundeinstellungen**.
2. Klicken Sie auf **Aktivieren**, wählen Sie Werte für die folgenden Parameter aus, oder geben Sie Werte ein, und klicken Sie auf **Übernehmen**.
 - **Werbung für Citrix SD-WAN Routen:** Erlauben Sie, dass Citrix SD-WAN Routen über BGP angekündigt werden.
 - **Werbung für OSPF-Routen:** Erlauben Sie, dass Routen, die von OSPF-Kollegen gelernt wurden, über BGP beworben werden.
 - **Router-ID:** Die eindeutige Router-ID, der Router wird für OSPF-Anzeigen verwendet. Wenn die Router-ID nicht angegeben ist, wird sie automatisch als niedrigste virtuelle IP ausgewählt, die im SD-WAN-Netzwerk gehostet wird.
 - **Lokales autonomes System:** Die lokale autonome Systemnummer, von der die Routen gelernt und beworben werden. Die autonome Systemnummer muss mit einer auf den benachbarten Routern übereinstimmen.
 - **Protokolleinstellung:** Wenn Präfixe über mehrere Routingprotokolle gelernt werden, bestimmt der Wert der Protokolleinstellung die Auswahl des Routingprotokolls. Weitere Informationen finden Sie unter [Protokollpräferenz](#).



3. Erweitern Sie **Grundeinstellungen > Nachbarn** und klicken Sie auf das Symbol **Hinzufügen (+)**



Section: Neighbors

| | Virtual Interface | Source IP | Neighbor IP | Neighbor AS | Hold Time(s) | Local Preference | BGP Metric | Multi Hop | Password | Delete |
|--|-------------------|--------------|-------------|-------------|--------------|------------------|-------------------------------------|-------------------------------------|----------|--------------------------|
| | VirtualInterface- | 172.111.64.5 | * | 13 | 180 | 100 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |

Policies +

| | Order | Network Address | BGP Community(AA:NN) | AS Path | BGP Policy | Direction | Delete |
|--|-------|-----------------|----------------------|---------|------------|-----------|--------|
| | | | | | | | |

Apply Revert

Wählen Sie für Sites mit mehreren Routingdomänen eine Routingdomäne aus. Routingdomäne bestimmt, welche virtuellen Schnittstellen verfügbar sind.

- Wählen Sie eine **virtuelle Schnittstelle** aus dem Menü. Die virtuelle Schnittstelle bestimmt die Quell-IP-Adresse.
- Geben Sie die **IP-Adresse** des IBGP-Neighbor-Routers in das Feld Nachbar IP und die Nummer des **lokalen autonomen Systems** in das Feld Nachbar AS ein.
- Geben Sie im Feld **Haltezeit** die Haltezeit in Sekunden ein, um zu warten, bevor Sie einen Nachbarn deklarieren (der Standardwert ist 180).
- Geben Sie im Feld **Lokale Einstellungen** den Wert Lokale Voreinstellungen in Sekunden ein, der für die Auswahl aus mehreren BGP-Routen verwendet wird (der Standardwert ist 100).
- Aktivieren Sie das Kontrollkästchen **IGP-Metrik**, um den Vergleich der internen Entfernungen zu aktivieren, um die beste Route zu berechnen.
- Aktivieren Sie das Kontrollkästchen **Multi-Hop**, um mehrere Hops für die Route zu aktivieren.
- Geben Sie im Feld **Kennwort** ein Kennwort für die MD5-Authentifizierung von BGP-Sitzungen ein (Authentifizierung ist nicht erforderlich).

Hinweis

Das Konfigurieren von Routenreflektoren und Konföderationen für iBGP wird im SD-WAN-Netzwerk nicht unterstützt.

Exterieur BGP (eBGP)

Citrix SD-WAN Appliances verbinden sich mit einem Switch auf der LAN-Seite und einem Router auf der WAN-Seite. Da die SD-WAN-Technologie zunehmend integraler für Enterprise-Netzwerkbereitstellungen wird, ersetzen SD-WAN-Appliances die Router. SD-WAN implementiert dynamisches Routing-Protokoll eBGP, um als dedizierte Routinggerät zu fungieren.

Die SD-WAN-Appliance baut eine Nachbarschaft mit Peer-Routern mit eBGP zur WAN-Seite auf und ist in der Lage, Routen von und zu Peers zu lernen, zu werben. Sie können das Importieren und Exportieren von eBGP erlernten Routen auf Peergeräten auswählen. Außerdem können SD-WAN statische, virtuelle Pfadlernrouten konfiguriert werden, um eBGP-Peers zu werben.

Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

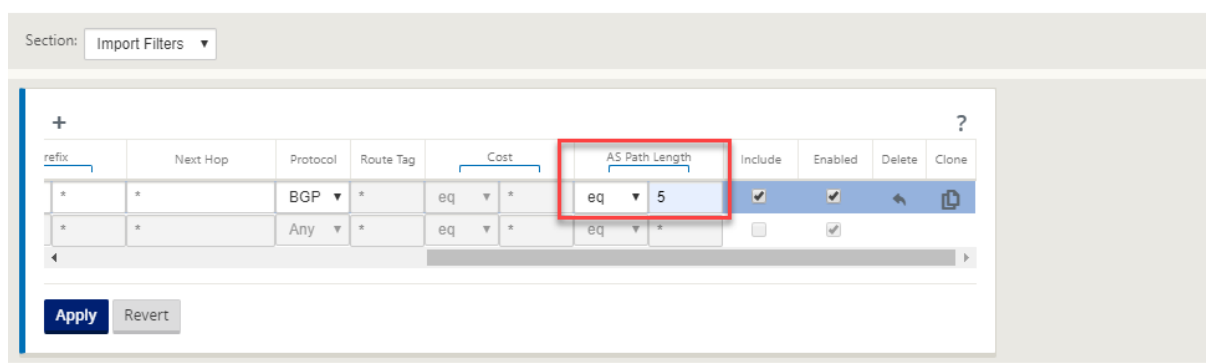
- [SD-WAN-Site Kommunikation mit Nicht-SD-WAN-Site über eBGP](#)
- [Kommunikation zwischen SD-WAN-Sites mit Virtual Path und eBGP](#)
- [Implementierung von OSPF in der Einarm-Topologie](#)
- [OSPF-Typ5-zu-Typ1-Bereitstellung im MPLS-Netzwerk](#)
- [SD-WAN- und Nicht-SD-WAN \(Drittanbieter-Appliance\) OSPF-Bereitstellung](#)
- [Implementierung von OSPF mit SD-WAN-Netzwerk mit Hochverfügbarkeits-Setup](#)

AS-Pfadlänge

Das BGP-Protokoll verwendet das **AS-Pfadlängenattribut**, um die beste Route zu bestimmen. Die AS-Pfadlänge gibt die Anzahl der autonomen Systeme in einer Route an. Citrix SD-WAN verwendet das Attribut **BGP AS Pfadlänge** zum Filtern und Importieren von Routen.

Nicht-SD-WAN-Appliances können den Datenverkehr an primäre DC- oder sekundäre DC-SD-WAN-Appliances weiterleiten, indem Routen basierend auf ihrer AS-Pfadlänge importiert werden. Sie können den Datenverkehr auch dynamisch von einem Router zu einem sekundären DC steuern, indem Sie einfach die AS-Pfadlänge der primären DC-Einheit auf dem Router erhöhen, wodurch sie nicht bevorzugt wird. Vermeidet die Notwendigkeit, die Routenkosten zu ändern und eine Konfigurationsupdate durchzuführen.

Um die AS-Pfadlänge in Importfiltern zu konfigurieren, wählen Sie BGP als Protokoll, wählen Sie ein Prädikat aus und geben Sie die **AS-Pfadlänge** ein. Weitere Informationen finden Sie unter [Routenfilterung](#).



Routenstatistiken überwachen

Navigieren Sie zu **Überwachen> Statistiken**. Wählen Sie im Dropdownmenü **Anzeigen** die Option **Routen** aus.

Alle Funktionen für die entsprechenden Routen werden im Citrix SD-WAN Netzwerk unterstützt, unabhängig davon, ob eine Route dynamisch oder statisch ist.

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

Show 100 entries Showing 1 to 28 of 28 entries

| Num | Network Addr | Gateway IP Address | Service | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|-----------------|--------------------|-----------------|-----------|-----------------|---------|---------|-------------|-----------------|------|-----------|----------|------------------|-------------------|
| 0 | 115.1.1.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 1 | 115.168.0.16/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 2 | 115.168.0.12/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 3 | 115.168.0.8/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 4 | 115.168.0.4/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 5 | 115.168.0.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 6 | 115.14.14.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 7 | 115.13.13.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 8 | 115.12.12.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 9 | 115.10.10.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 10 | 115.9.9.16/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 11 | 115.8.8.12/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 12 | 115.7.7.8/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 13 | 115.6.6.4/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 14 | 115.5.5.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 15 | 115.4.4.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 16 | 115.3.3.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 17 | 115.2.2.0/30 | 182.120.1.1 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 0 | YES | N/A | N/A |
| 18 | 182.120.1.0/24 | * | Local | YES | * | pod2_DC | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 19 | 172.120.1.0/24 | * | Local | YES | * | pod2_DC | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 20 | 182.120.2.0/24 | * | pod2_DC-pod3_Br | YES | * | pod3_Br | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 21 | 172.120.2.0/24 | * | pod2_DC-pod3_Br | YES | * | pod3_Br | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 22 | 182.120.0.0/24 | * | pod2_DC-pod1_Br | YES | * | pod1_Br | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 23 | 172.120.0.0/24 | * | pod2_DC-pod1_Br | YES | * | pod1_Br | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 24 | 192.120.1.0/24 | 172.120.1.2 | Local | YES | * | pod2_DC | Dynamic | OSPF | - | 6 | 75612 | YES | N/A | N/A |
| 25 | 192.120.0.0/24 | * | pod2_DC-pod1_Br | YES | * | pod1_Br | Dynamic | Virtual WAN | YES | 6 | 75612 | YES | N/A | N/A |
| 26 | 0.0.0.0/0 | * | Passthrough | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |
| 27 | 0.0.0.0/0 | * | Discard | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |

Showing 1 to 28 of 28 entries

OSPF

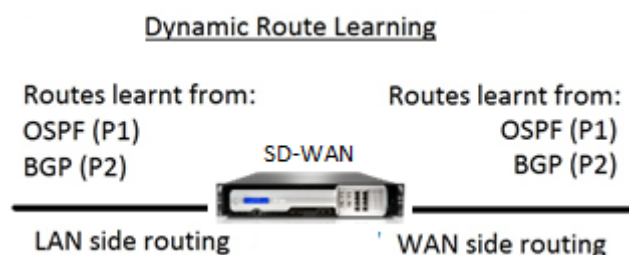
May 10, 2021

LAN-Seite: Dynamisches Routenlernen

OSPF wird auf dem LAN-Port der Citrix SD-WAN Appliance ausgeführt, die im Gateway-Modus bereitgestellt wird:

Citrix SD-WAN Appliances führen Routenermittlung von Layer-3-Routingankündigungen innerhalb eines lokalen Kundennetzwerks (Zweigstelle und Rechenzentrum) für jedes der gewünschten Routingprotokolle (OSPF und BGP) durch. Die erlernten Routen werden dynamisch erfasst und angezeigt.

Auf diese Weise müssen SD-WAN-Administratoren die LAN-seitige Netzwerkumgebung für jede Appliance, die Teil des SD-WAN-Netzwerks ist, statisch definieren.



WAN-Seite: Dynamische Routenfreigabe

Citrix SD-WAN Appliance, deren AREA als STUB-Bereich definiert ist, indem das Lernen von Typ 5 AS-External LSA eingeschränkt wird.

Citrix SD-WAN Appliances können die lokal erlernten dynamischen Routen mit dem MCN werben. Der MCN kann diese Routen dann an andere SD-WAN-Appliances im Netzwerk weiterleiten. Dieser Informationsaustausch ermöglicht dynamisch die Aufrechterhaltung der Konnektivität zwischen Standorten im sich ändernden Netzwerk.

OSPF-Bereitstellungsmodi

In früheren Versionen wurden die von der OSPF-Instanz erlernten Routen aus SD-WAN als externe Routen mit Typ 5 LSA behandelt. Diese Routen wurden ihren Nachbarroutern in Type 5 External LSA angekündigt. Dies führte dazu, dass SD-WAN-Routen nach dem OSPF-Pfadauswahlalgorithmus weniger bevorzugte Routen sind.

Mit der neuesten Version kann SD-WAN nun Routen als Intra-Area Routes (LSA Type 1) ankündigen, um anhand des OSPF-Pfadauswahlalgorithmus die Präferenz gemäß den Routenkosten zu erhalten. Die Routenkosten können konfiguriert und dem Nachbarrouter angekündigt werden. Dies ermöglicht die Bereitstellung der SD-WAN-Appliance in einem einarmigen Modus, wie unten beschrieben.

Implementierung von OSPF in der Einarm-Topologie

Bei einer Einarm-Konfiguration benötigt der Router eine komplizierte PBR- oder WCCP-Konfiguration in OSPF-Bereitstellungen. Durch die Änderung des Standard-Export-Routentyps von Typ 5 auf Typ 1 können wir diese Bereitstellung vereinfachen. Wenn SD-WAN-Routen als gebietsinterne Routen mit geringeren Kosten angekündigt werden und die SD-WAN-Appliance aktiv wird, wählt der Nachbarrouter SD-WAN-Routen aus und beginnt automatisch mit der Weiterleitung des Datenverkehrs über das SD-WAN-Netzwerk. Zusätzliche PBR- oder WCCP-Konfiguration ist nicht mehr erforderlich.

Voraussetzungen:

- SD-WAN-Appliances an den DC- und Zweigstandorten müssen die neueste Release-Version ausgeführt werden.
- End-to-End-IP-Konnektivität muss konfiguriert werden und funktioniert einwandfrei.
- OSPF ist auf allen Sites aktiviert.

So konfigurieren Sie OSPF Typ 1:

1. Konfigurieren Sie **virtuelle Schnittstellen** und **WAN-Verbindungen** sowohl auf den DC- als auch auf Branch-Sites, damit Sie den virtuellen Pfad zwischen ihnen erstellen können.
2. Under **Connections** > [MCN] > **Route Learning** > **OSPF->Basic Settings**, select **Export OSPF Route Type** to be **Type 1 Intra Area**.
3. Speichern Sie die Konfiguration, stellen Sie die Konfiguration ein und aktivieren Sie die Konfiguration.

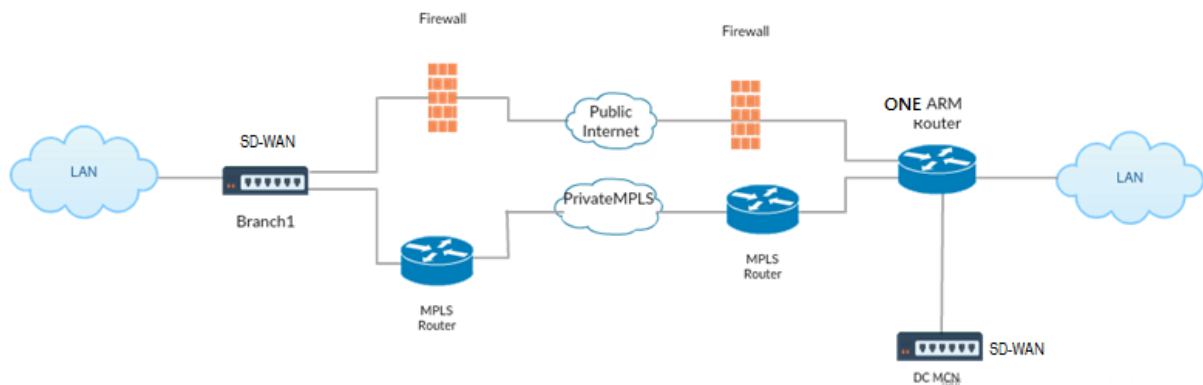
Sie müssen die folgenden Routentypen unter

Export-OSPF-Routentyp sehen können

- Typ 5 AS extern
- Typ 1 Intra-Bereich

Sie müssen in der Lage sein, die **externe Route vom Typ 5 AS** zu konfigurieren.

Nach der Aktivierung der geänderten Konfiguration müssen die Änderungen des Routentyps unter **Konfiguration** > **Virtuelles WAN** > **Konfiguration anzeigen** > **Dynamic Routing** angezeigt werden.

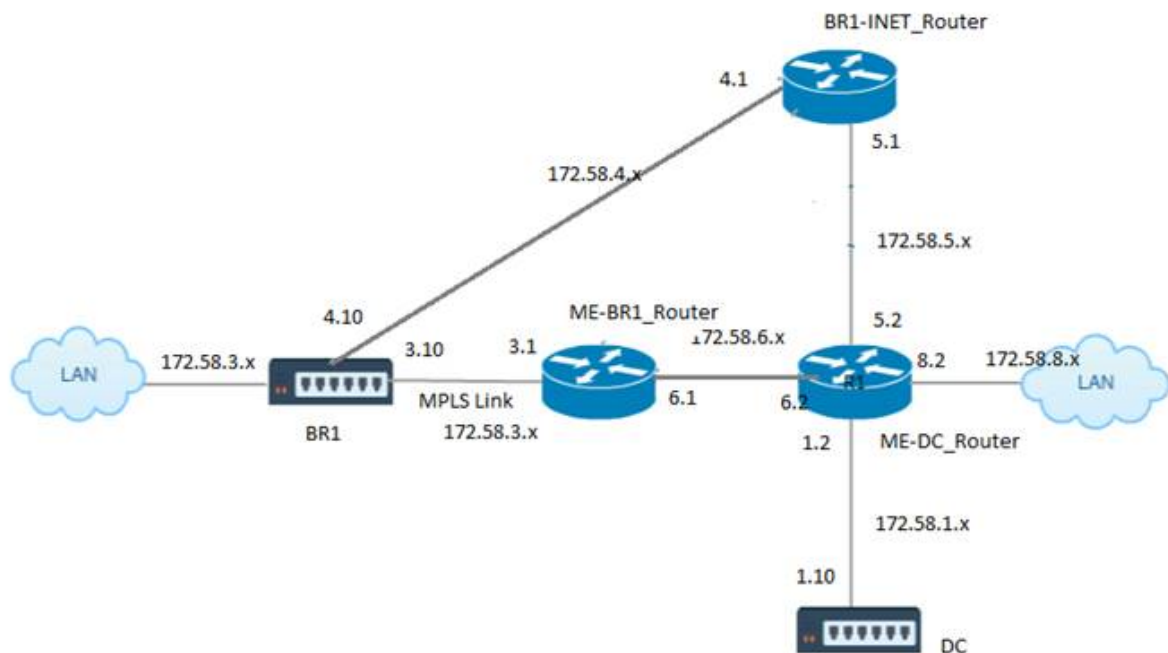


Wie in der Abbildung oben gezeigt, wird DC MCN in der Einarm-Topologie eingesetzt. Wenn der DC-Standort hochgefahren ist, leitet der einarmige Router den gesamten Datenverkehr vom lokalen LAN an andere Standorte weiter, z. B. das lokale LAN der Zweigstelle, dessen Ziel-IP-Adresse sich innerhalb desselben Subnetzes befindet, zuerst an das SD-WAN. Anschließend wickelt die SD-WAN-Appliance alle Pakete ein und sendet sie mit allen Paketziel-IP an den Router -Adresse in der virtuellen Branch-IP-Adresse. Der Router leitet diese Pakete dann an WAN weiter.

Wenn der DC-Standort ausfällt, leitet der Router den gesamten Datenverkehr vom lokalen LAN an andere Standorte (lokales LAN des Zweigstandorts, Ziel-IP befindet sich innerhalb des Subnetzes) direkt an WAN und nicht an die SD-WAN-Appliance weiter.

OSPF-Typ5-zu-Typ1-Bereitstellung im MPLS-Netzwerk

Der folgende Bereitstellungsmodus wird zur Vermeidung von Schleifenbildung in einem MPLS-Netzwerk bereitgestellt, das mit SD-WAN-Appliances konfiguriert wurde. Die folgende Abbildung beschreibt die standardmäßige MPLS-Netzwerkimplementierung.



In der obigen Abbildung:

- OSPF ist zwischen *ME-BR1_Router* und *ME-DC_Router* im Bereich 0 konfiguriert.
- OSPF ist zwischen *ME-DC_Router* und *DC* im Bereich 0 konfiguriert.

Empfohlene Konfiguration:

- DC VW und *ME-DC_Router* auf Bereich0
- *ME-BR1_Router* und *ME-DC_Router* auf Bereich0
- BR1 VW und *ME-BR1_Router* auf Bereich0

Auf dem *ME-DC_Router*:

1. Hinzufügen, statische Route für 172.58.3.10/32 (Virtuelle IP von BR1 für MPLS Link) bis 172.58.6.1
2. Hinzufügen, statische Route für 172.58.4.10/32 (Virtuelle IP von BR1 für INET) bis 172.58.5.1

Durch das Hinzufügen statischer Routen wird die Schleifenbildung zwischen dem *ME-DC_Router* und der DC-SD-WAN-Einheit verhindert. Wenn Sie keine statischen Routen hinzufügen, leitet der MCN den Datenverkehr an den *ME-DC_Router* weiter und zurück vom Router zum MCN, wodurch kontinuierlich eine Schleife entsteht.

Die statischen Routen, bei denen es sich nicht um PBR-Routen handelt, sondern um die Ziel-Host-IP-basierte Routen gehen in Richtung der richtigen Verbindung, die von der DC-Seite ausgewählt werden soll, basierend auf dem gewählten Pfad und der danach durchgeführten Kapselung. Daher würden

bei konfigurierten statischen Routen die gekapselten Pakete mit einer beliebigen virtuellen Ziel-IP der BR1 SD-WAN-Appliance diese Links gemäß dem besten Pfad verwenden, der vom DC MCN ausgewählt wurde.

Fügen Sie ACL hinzu, um Schleifenbildung zu vermeiden, wenn IPHOST-Routen installiert sind (wenn keine statischen virtuellen IPs konfiguriert sind):

- Wenn die von der BR1 SD-WAN-Appliance beworbenen IPHOST-Routen vom MCN-Router *ME-DC_Router* installiert und nicht wie oben erwähnt als statische Routen hinzugefügt werden, besteht die Möglichkeit der Schleifenbildung, wenn die teilnehmende OSPF-Schnittstelle (172.58.6.x) zwischen *ME-br1_Router* und *ME-dc_Router* ausfällt. Dies liegt daran, dass mit dieser Schnittstelle die IPHOST-Routen aus der Routingtabelle von *ME-DC_Router* geleert werden.
- In diesem Fall leitet MCN das gekapselte Paket, das für einen der BR1-VIPs bestimmt ist, an den *ME-DC-Router* weiter und zurück vom Router zum MCN und schleifen kontinuierlich.

Auf dem *ME-BR1_Router*:

Beantragen Sie das 172.58.3.x-Netzwerk bei *ME-DC_Router* mit höheren Kosten als die Kosten, die für dasselbe Netzwerk von DC angegeben werden, wenn dieselbe AREA-ID zwischen **Me-BR1_Router <-> ME-dc_Router** und **ME-dc_Router <-> DC (SD-WAN)** verwendet wird.

- Basierend auf der Kostenmetrik-Berechnung von OSPF $10^8/BW$ und den Kosten für Routenpräfixe basieren auf dem Schnittstellentyp. SD-WAN-Appliances geben die virtuellen Pfad- und virtuellen WAN-spezifischen statischen Routen zu den externen oder Peer-Routern mit den standardmäßigen SD-WAN-Kosten von 5.
- Wenn der *ME-BR1_Router* neben DC (SD-WAN) auch 172.58.3.0/24 als interne OSPF-Typ-1-Route ankündigt, die auch das gleiche Präfix wie eine interne OSPF Typ 1-Route ankündigt, dann wird laut Kostenberechnung standardmäßig die Route des *ME-BR1_Routers* konfiguriert, da die Kosten geringer sind als die SD-WANs Standardkosten von 5. Um dies zu vermeiden und die SD-WAN-Appliance zunächst als bevorzugte Route zu wählen, müssen die Schnittstellenkosten von (172.58.3.1) so manipuliert werden, dass sie auf dem *ME-BR1_Router* höher ist, sodass die DC-SD-WAN-Route in der Routingtabelle des *ME-DC_Routers* konfiguriert wird.

Dadurch wird auch sichergestellt, dass bei einem Ausfall der DC SD-WAN-Appliance die alternative Route zur Verwendung des *ME-BR1_Routers* als nächstes bevorzugtes Gateway einen unterbrechungs-freien Datenfluss gewährleistet.

Verwenden Sie *ME-DC_Router* als Quelle für die Werbung des 172.58.8.0/24-Netzwerks sowohl für DC-SD-WAN als auch für den *ME-BR1_Router*:

Mit dieser Route kann das DC SD-WAN Pakete an den Upstream-Router senden, der sich nach der Enkapselung des LAN-Subnetzes bewusst ist. Wenn DC SD-WAN ausfällt, würde die Legacy-Routing-

Infrastruktur ME-BR1_Router dabei helfen, den ME-DC_Router als nächsten Hop zu verwenden, um das 172.58.8.x-Netzwerk zu erreichen.

So konfigurieren Sie exportierte OSPF-Routen als Typ1 unter **Grundlegende OSPF-Einstellungen**:

1. Konfigurieren Sie **Virtual Interfaces** und **WAN-Links** auf DC- und Branch-Standorten, um den virtuellen Pfad zwischen ihnen zu erstellen.
2. Wählen Sie unter **Verbindungen**->**[MCN]**>**Routenlernen**->**OSPF**->**Grundeinstellungen** die Option **OSPF Routentyp exportieren**, um **Typ 1 Intra-Bereich** zu sein.
3. Speichern Sie die Konfiguration, stellen Sie sie ein und aktivieren Sie sie. Unter **Export-OSPF-Routentyp** müssen Sie die folgenden beiden Routentypen sehen können:
 - Typ 5 AS extern
 - Typ 1 Intra-Bereich

Nach der Aktivierung der geänderten Konfiguration sehen Sie die Routentypänderungen unter **Konfiguration > Virtuelles WAN > Konfiguration anzeigen > Dynamisches Routing**.

Routen müssen von der SD-WAN-Appliance als External AS vom Typ 5 angekündigt werden. Routen, die über SD-WAN gelernt wurden, müssen in den benachbarten Routern als Typ5 AS Externe Routen angezeigt werden.

So konfigurieren Sie das OSPF-Gewicht für exportierte Routen unter **Grundlegende OSPF-Einstellungen**:

1. Konfigurieren Sie virtuelle Schnittstellen und WAN-Verbindungen auf DC- und Zweigstandorten, um den virtuellen Pfad zwischen ihnen zu erstellen.
2. Konfigurieren Sie unter **Verbindungen**MCN**[MCN] > > Routenlernen > OSPF > Grundeinstellungen** die Option **OSPF-Routengewicht exportieren**.
3. Speichern Sie die Konfiguration, stellen Sie sie ein und aktivieren Sie sie.
4. Konfigurieren Sie nun den Export OSPF-Routengewicht auf einen beliebigen numerischen Wert zwischen **1** und **65529**.
5. Nach der Aktivierung der geänderten Konfiguration sehen Sie die Routengewichtung unter **Konfiguration > Virtuelles WAN > Konfiguration anzeigen > Dynamisches Routing**. Die exportierte Standard-Routenstärke muss 0 sein. Die tatsächlichen Kosten der Route dürfen nur die Kosten für SD-WAN sein.

So konfigurieren Sie exportierte OSPF-Routen als Typ1 unter Exportfiltereinstellungen:

1. Konfigurieren Sie **virtuelle Schnittstellen** und **WAN-Verbindungen** sowohl auf DC als auch auf Branch, damit wir den virtuellen Pfad zwischen ihnen erstellen können. Konfigurieren Sie unter **Verbindungen > [MCN] > Route Learning > OSPF > Exportfilter** einen Exportfilter.

2. Erweitern Sie den Filter. Konfigurieren Sie den **OSPF-Routentyp exportieren** auf **Typ 1 Intra Area** Route.
3. Speichern Sie die Konfiguration, stellen Sie sie ein und aktivieren Sie sie. Sie müssen die folgenden beiden Routentypen unter **Export-OSPF-Routentyp** sehen können
 - Typ 5 AS extern
 - Typ 1 Intra-Bereich

Nach der Aktivierung der geänderten Konfiguration muss ein Benutzer die Änderungen des Routentyps unter **Konfiguration > Virtuelles WAN > Konfiguration anzeigen** können. Der Routentyp muss als Typ 5 AS Extern angezeigt werden.

So konfigurieren Sie die exportierte OSPF-Routengewichtung unter den Einstellungen des Exportfilters:

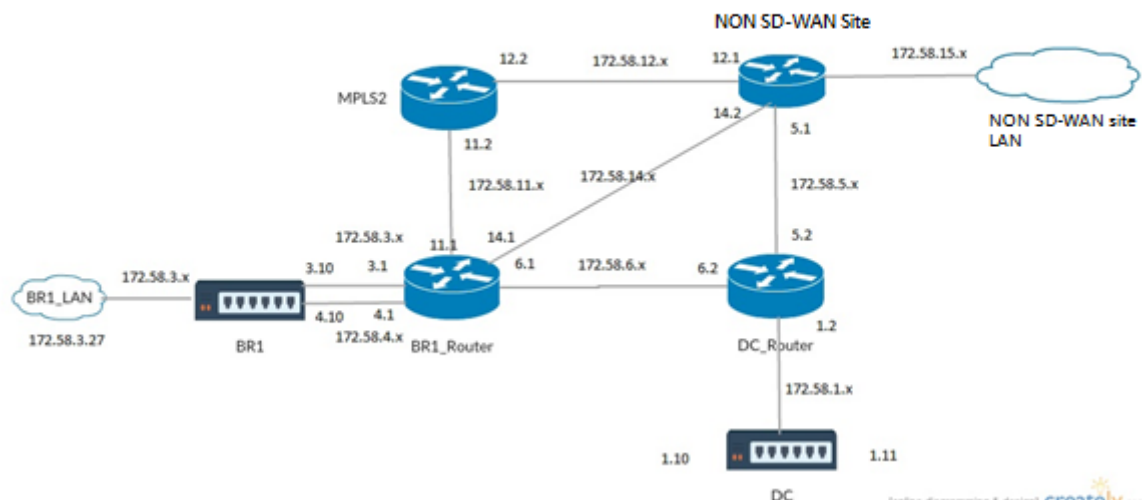
1. Konfigurieren Sie virtuelle Schnittstellen und WAN-Verbindungen auf DC und Branch, so dass wir den virtuellen Pfad zwischen ihnen erstellen können.
2. Konfigurieren Sie unter **Verbindungen > [MCN] -> Routenlernen > OSPF > Exportfilter** einen Exportfilter.
3. Erweitern Sie den Filter. Konfigurieren Sie Export OSPF Routengewicht auf einen beliebigen numerischen Wert zwischen **1** und **65529**.
4. Speichern Sie die Konfiguration, stellen Sie sie ein und aktivieren Sie sie.

Nach der Aktivierung der geänderten Konfiguration muss ein Benutzer die Änderungen des Routentyps unter **Konfiguration > Virtuelles WAN > Konfiguration anzeigen** können.

Die unter Exportfilter konfigurierte Streckengewichtung muss das unter **Grundlegende OSPF-Einstellungen** konfigurierte Gewicht überschreiben.

Bereitstellung von SD-WAN- und Drittanbieter-Appliances (Nicht-SD-WAN)

Wie in der Abbildung unten gezeigt, kann die Appliance-Site eines Drittanbieters zum LAN von Standort B gelangen, indem Datenverkehr direkt an Standort B gesendet wird. Wenn der Datenverkehr nicht direkt gesendet werden kann, geht die Fallbackroute an Standort A und verwendet dann den virtuellen Pfad zwischen DC zu Zweigstellen, um zur Zweigstelle zu gelangen. Wenn dies fehlschlägt, verwendet es MPLS2, um zur Branch-Site zu gelangen.



Konfigurationsschritte:

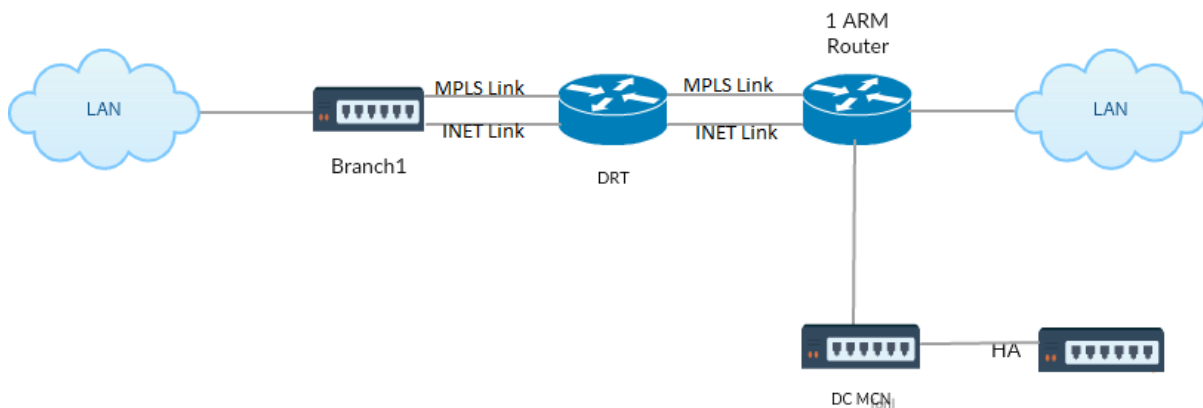
1. Konfigurieren Sie **virtuelle Schnittstellen** und **WAN-Links** auf Domänencontroller und Zweig, so dass zwischen den Standorten ein virtueller Pfad erstellt wird.
2. Konfigurieren Sie den **Routentyp exportieren** als **Typ1**, und weisen Sie die Kosten auf der SD-WAN-Appliance als **195** zu.
3. Speichern, Staging und Aktivieren der Konfiguration.
4. Senden Sie Datenverkehr zwischen den Endhosts auf DC- und Zweigstandorten.
5. Fahren Sie die Verbindung zwischen R1 und R2 herunter.
6. Senden Sie Datenverkehr zwischen den Endhosts auf DC- und Zweigstandorten.
7. Heben Sie die Verbindung zwischen R1 und R2 auf.
8. Senden Sie Datenverkehr zwischen den Endhosts auf DC- und Zweigstandorten.
9. Deaktivieren Sie den virtuellen WAN-Dienst auf dem DC-Standort, damit virtuelle Pfade ausgefallen werden.
10. Senden Sie den Datenverkehr zwischen den Endhosts auf DC- und Zweigstandorten.

Konfiguration wird überprüft:

1. Zunächst wird in Schritt 4 der gesamte Datenverkehr durch die SD-WAN-Appliance geleitet.
2. Wenn in Schritt 6 die Verbindung zwischen R1 und R2 unterbrochen ist, wird der Datenverkehr über R3 in Richtung SD-WAN weitergeleitet.
3. In Schritt 8 fließt der Datenverkehr durch die SD-WAN-Appliance mit R2 als nächsten Hop für den LAN-Router R1.
4. In Schritt 10 gehen Virtual WAN-Pfade zwischen DC und BR1-Appliance herunter, und der Datenverkehr muss wie vor der Konfiguration des SD-WAN-Netzwerks normal fließen.

Der Verkehrsfluss kann in der SD-WAN GUI unter **Überwachung > Flows** beobachtet werden.

Implementieren von OSPF mit SD-WAN-Netzwerk in Hochverfügbarkeit-Setup



OSPF Typ5 zu Typ1 mit Hochverfügbarkeitsstandorten während des Failovers auf Standby-Appliance und Bereitstellung in Hochverfügbarkeits-Setup:

So konfigurieren Sie OSPF in der HA-Bereitstellung:

1. Konfigurieren Sie **Virtual Interfaces** und **WAN-Verbindungen** sowohl auf DC als auch auf Branch, um den virtuellen Pfad zwischen ihnen zu erstellen.
2. Richten Sie die Hochverfügbarkeit ein.
3. **Routentyp** exportieren, der als **Typ 1** und **Routengewicht50** konfiguriert ist.
4. Speichern Sie die Konfiguration, stellen Sie sie ein und aktivieren Sie sie.
5. Verkehrsfluss starten.
6. Beachten Sie, dass unter **Monitor > Statistik > Routen** die Trefferanzahl für OSPF-Routen mit geringsten Kosten erhöht wird.
7. Bringen Sie den Active MCN herunter und beobachten Sie das Verhalten.
8. Bringen Sie das Original Active MCN wieder nach oben.
9. Das **Dashboard > Hochverfügbarkeitsstatus** wird für lokale HA-Appliance und Peer-Appliance für Aktiv und Standby korrekt angezeigt.
10. Unter **Konfiguration > Konfiguration anzeigen > Dynamisches Routing** ist OSPF aktiviert und **export_ospf_route_type** zeigt **Typ1** und **export_ospf_route_weight** als **50**.
11. Auch nach einem Failover zeigt der Hochverfügbarkeitsstatus die korrekte OSPF-Konfiguration für die lokale und Peer-Appliance an.
12. Ansicht **Monitor > Statistik > Routen** . Die Trefferanzahl steigt bei OSPF-Routen mit geringsten Kosten.
13. Nach dem Failback zeigt der Hochverfügbarkeitsstatus die korrekte OSPF-Konfiguration für lokale und Peer-Appliance an.
14. Stellen Sie unter der Ansicht **Überwachen > Statistiken > Routen** sicher, dass die Trefferzahl für **OSPF-Routen** mit geringen Kosten zunimmt.

Problembehandlung

Sie können die OSPF-Parameter unter **Monitoring > Routing Protocols** anzeigen.

DashboardMonitoringConfiguration

StatisticsFlowsRouting ProtocolsFirewallIKE/IPsecIGMPPerformance ReportsQos ReportsUsage ReportsAvailability ReportsAppliance ReportsDHCP Server/RelayVRRP

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: OSPF Interface Routing Domain: Default_RoutingDomain Refresh

OSPF Interface

ospf_rdomain_0:
Interface vni-0 (172.58.1.0/24)
Type: broadcast
Area: 0.0.0.0 (0)
State: DROther
Priority: 0
Cost: 10
Hello timer: 10
Wait timer: 40
Dead timer: 40
Retransmit timer: 5
Designated router (ID): 105.105.105.105
Designated router (IP): 172.58.1.28
Backup designated router (ID): 0.0.0.0
Backup designated router (IP): 0.0.0.0

DashboardMonitoringConfiguration

StatisticsFlowsRouting ProtocolsFirewallIKE/IPsecIGMPPerformance ReportsQos Reports

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: OSPF Neighbors Routing Domain: Default_RoutingDomain Refresh

OSPF Neighbors

ospf_rdomain_0:

| Router ID | Pri | State | DTime | Interface | Router IP |
|-----------------|-----|---------|-------|-----------|-------------|
| 105.105.105.105 | 1 | Full/DR | 00:39 | vni-0 | 172.58.1.28 |

Sie können auch die dynamischen Routingprotokolle beobachten, um festzustellen, ob ein Problem mit der OSPF-Konvergenz vorliegt.

Diagnose

Debug Logging: ☒ On ☐ Off

Filename: ▼

BGP

May 10, 2021

Mit der SD-WAN BGP-Routing-Funktionalität können Sie:

- Konfigurieren Sie die Nummer des autonomen Systems (AS) eines Nachbarn oder eines anderen Peer-Routers (iBGP oder eBGP).
- Erstellen Sie BGP-Richtlinien, die selektiv auf eine Gruppe von Netzwerken pro Nachbarn angewendet werden, in beide Richtungen (Import oder Export). Eine SD-WAN-Appliance unterstützt acht Richtlinien pro Site, wobei bis zu acht Netzwerkobjekte (oder acht Netzwerke) mit einer Richtlinie verknüpft sind.
- Für jede Richtlinie können Benutzer mehrere Community-Strings konfigurieren, AS-PATH-PREPEND, MED-Attribut. Benutzer können bis zu 10 Attribute für jede Richtlinie konfigurieren.

Hinweis

Nur lokale Präferenz und die IGP-Metrik für die Pfadauswahl und -manipulation sind zulässig.

Konfigurieren von Richtlinien

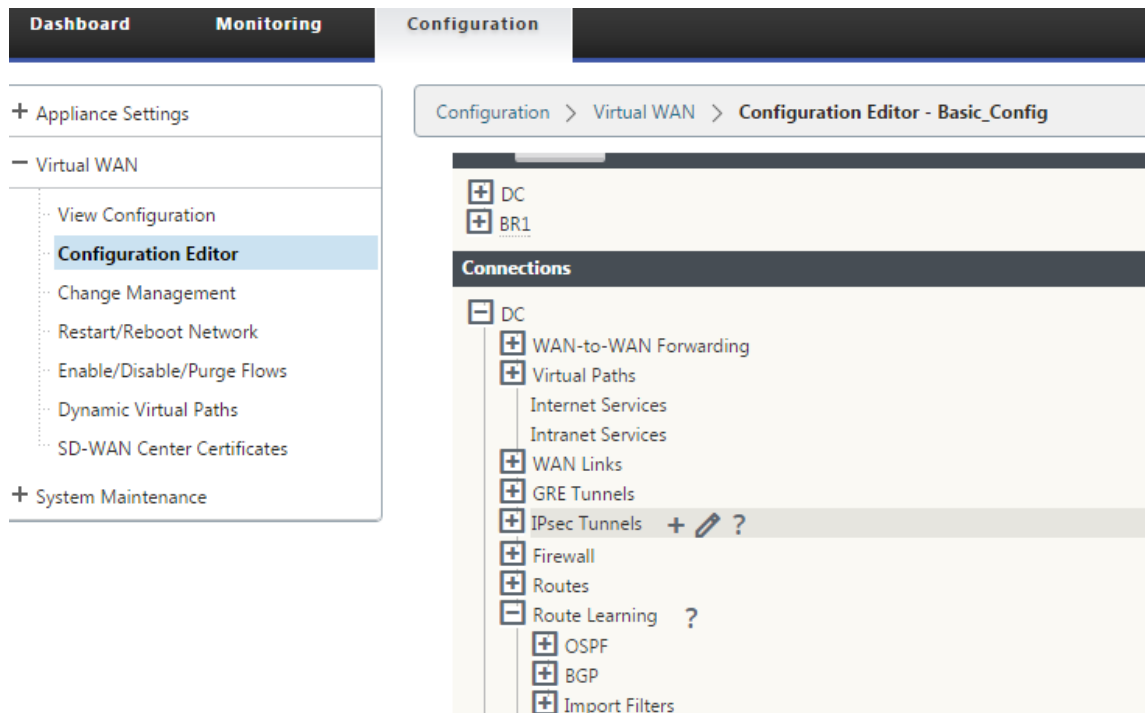
In der SD-WAN-Webverwaltungsschnittstelle verfügt der Konfigurationseditor über einen neuen Abschnitt, BGP-Richtlinie, unter **Route Learning > BGP**. In diesem Abschnitt können Benutzer BGP-Attribute hinzufügen, die eine Richtlinie darstellen. Das Hinzufügen von Community-Strings, das Voranstellen von AS-Pfaden und das Konfigurieren von MED werden unterstützt.

Sie können jede Community-Zeichenfolge manuell konfigurieren oder keine Werbung oder keine Exportgemeinschaftszeichenfolge aus einem Dropdownmenü auswählen. Zur manuellen Konfiguration können Sie eine AS-Nummer und eine Community eingeben. Sie können **Einfügen/Entfernen** auswählen, um die Routen zu markieren oder die Community von den Routen zu entfernen.

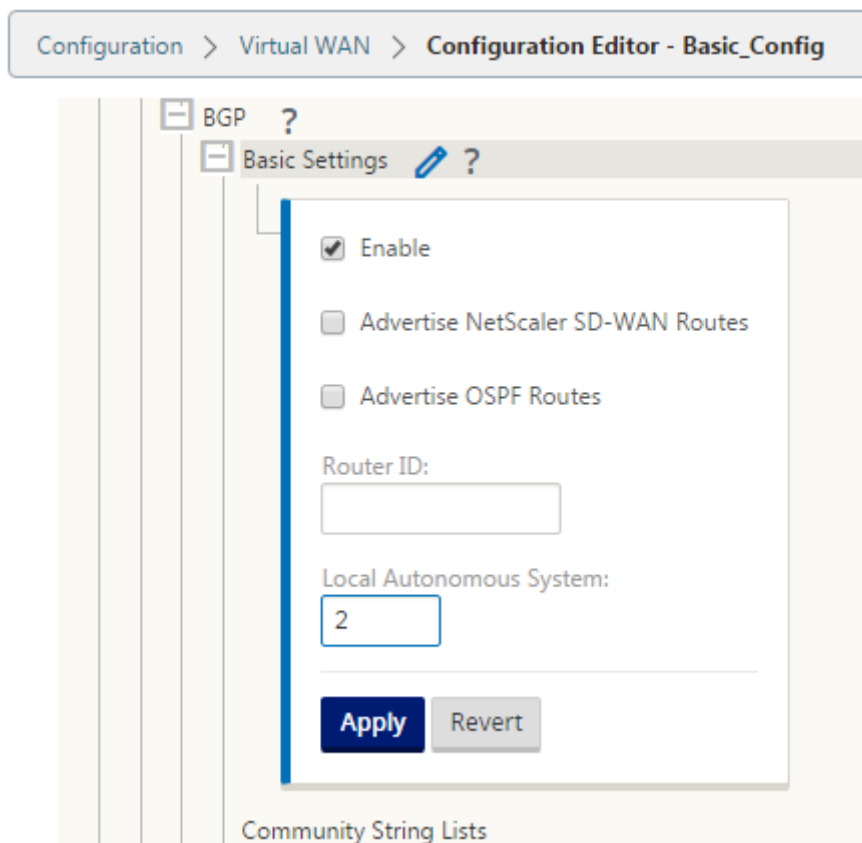
Sie können konfigurieren, wie oft Sie das lokale AS dem AS-Pfad voranstellen möchten, bevor Sie außerhalb des lokalen Netzwerks Werbung machen. Sie können MED für passende Routen konfigurieren.

So konfigurieren Sie die BGP-Richtlinie:

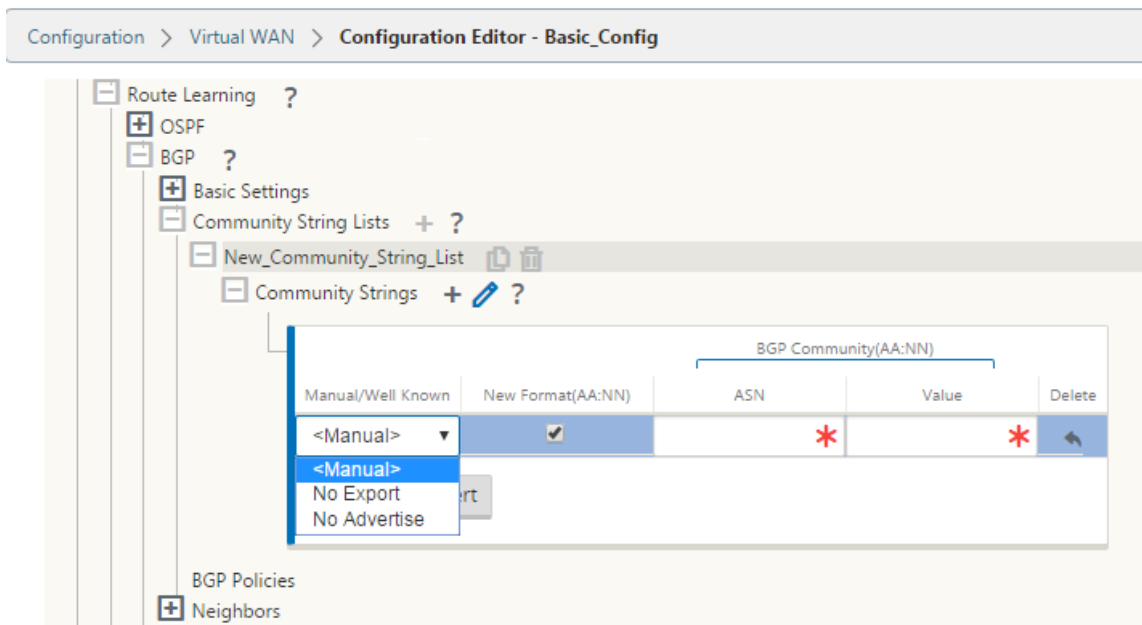
1. Wechseln Sie in der NetScaler SD-WAN-Webverwaltungsschnittstelle zu **Konfiguration** > **Virtuelles WAN** > **Konfigurations-Editor** . Öffnen Sie ein vorhandenes Konfigurationspaket. Wechseln Sie zu **Sites** > **DC-** oder **Zweigeinstellungen** .



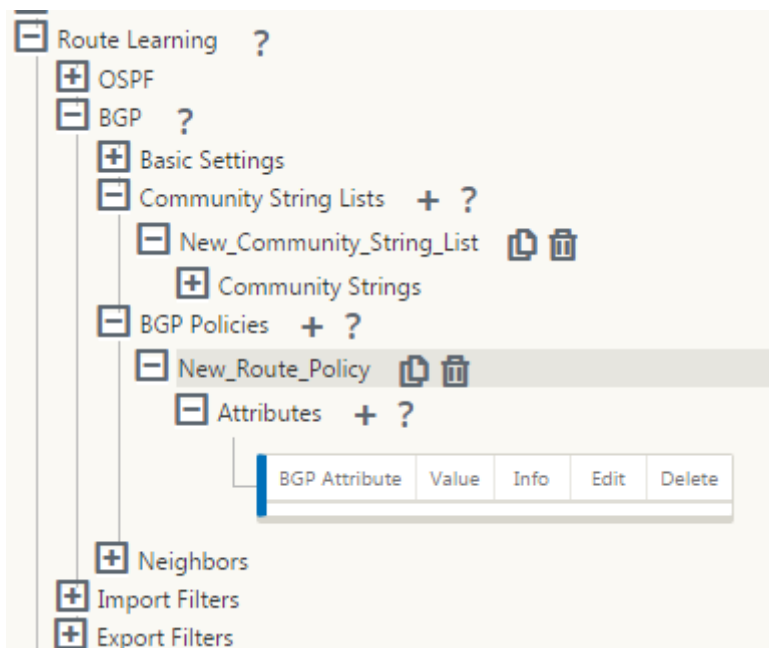
2. Erweitern Sie **BGP** und klicken Sie unter **Grundeinstellungen** auf **Aktivieren** . Geben Sie **Router-ID** und Wert **des lokalen autonomen Systems ein**, und klicken Sie auf **Übernehmen** .



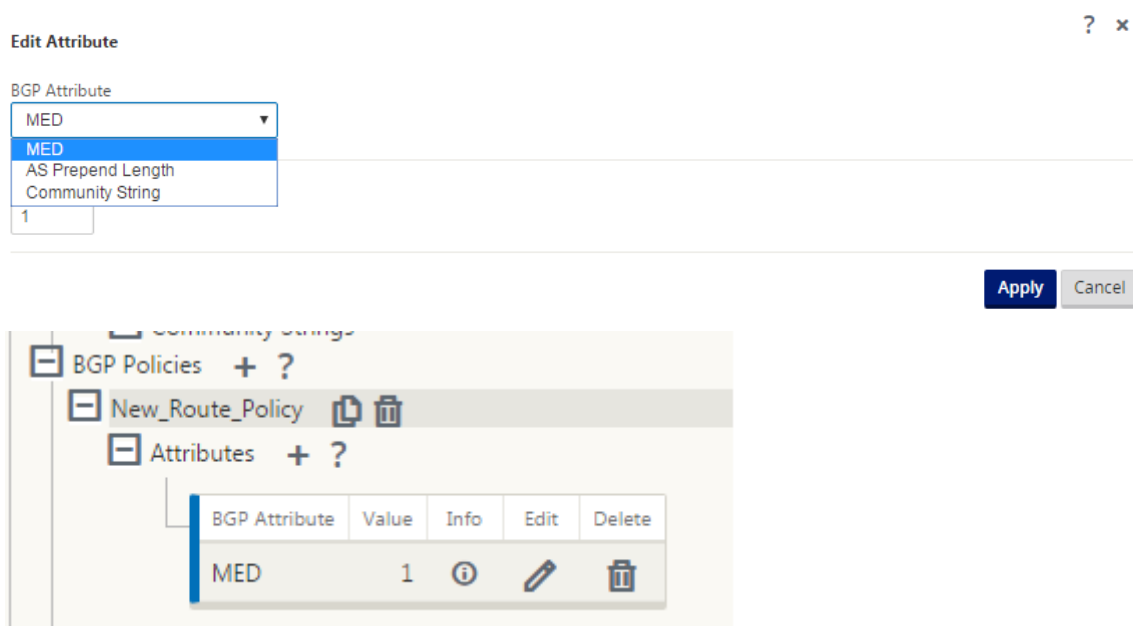
3. Klicken Sie neben den **Community-Zeichenfolgenlisten** auf + Zeichen. Konfigurieren Sie jede Community-Zeichenfolge manuell oder indem Sie keine Ankündigungs- oder keine Exportgemeinschaftszeichenfolge aus dem Dropdownmenü auswählen. Zur manuellen Konfiguration können Sie eine AS-Nummer und eine Community eingeben. Sie können die Routen mit der Community-Zeichenfolge **einfügen/entfernen** auswählen oder die Community-Zeichenfolge von den Routen entfernen, die von den Peers empfangen wurden.



4. Konfigurieren Sie die BGP-Richtlinie, indem Sie **BGP-Richtlinien erweitern**. Fügen Sie der **neuen Routenrichtlinie** BGP-Attribute hinzu.



5. Klicken Sie auf das + Zeichen neben **Attribute**, um BGP-Attribute zu bearbeiten. Das Fenster **Attribute bearbeiten** wird angezeigt. Wählen Sie im Dropdownmenü das gewünschte BGP-Attribut aus. Geben Sie gemäß Ihrer Auswahl den gewünschten Wert für **MED**, **AS Prepend Length** oder **Community String** ein. Klicken Sie auf **Übernehmen**.



Hinweis

Jede Richtlinie kann nur ein Vorkommen eines Attributs aufweisen und kann nicht mehrere Vorkommen desselben Attributs annehmen. Sie können nicht 2 MED oder 2 AS Path Prepend haben. Es kann entweder MED/AS-PATH Prepend/Community String oder eine Kombination haben.

Nachbarn konfigurieren

Um eBGP zu konfigurieren, wird eine zusätzliche Spalte zum bestehenden BGP-Nachbarabschnitt hinzugefügt, um die AS-Nummer des Nachbarn zu konfigurieren. Die vorhandenen Konfigurationen werden in dieses Feld mit der lokalen AS-Nummer ausgefüllt, wenn Sie die vorherige Konfiguration mit dem Konfigurationseditor SD-WAN 9.2 importieren.

Die Nachbarkonfiguration verfügt auch über einen optionalen erweiterten Abschnitt (erweiterbare Zeile), in dem Sie Richtlinien für jeden Nachbarn hinzufügen können.

Erweiterte Nachbarn konfigurieren

Mit dieser Option können Sie Netzwerkobjekte hinzufügen und eine konfigurierte BGP-Richtlinie für dieses Netzwerkobjekt hinzufügen. Dies ähnelt dem Erstellen einer Routenkarte und einer ACL, die bestimmten Routen entspricht, und dem Konfigurieren von BGP-Attributen für diesen Nachbarn. Sie können die Richtung angeben, um anzugeben, ob diese Richtlinie für eingehende oder ausgehende Routen angewendet wird.

Die Standardrichtlinie gilt für <accept> alle Routen. Richtlinien für Akzeptanz und Ablehnung sind Standardwerte und können nicht geändert werden.

Sie haben die Möglichkeit, Routen basierend auf Netzwerkadresse (Zieladresse), AS-Pfad, Community-Zeichenfolge abzugleichen und eine Richtlinie zuzuweisen und die Richtung für die anzuwendende Richtlinie auszuwählen.

So konfigurieren Sie Nachbarn:

1. Konfigurieren Sie Nachbarn, indem Sie auf **Hinzufügen** klicken, wie unten gezeigt.

The screenshot shows the 'Neighbors' configuration page. At the top, there is a table with columns: Virtual Interface, Source IP, Neighbor IP, Neighbor AS, Hold Time(s), Local Preference, IGP Metric, Multi Hop, Password, and Delete. An 'Add' button is visible next to the 'Virtual Interface' column header.

2. Klicken Sie auf das + Zeichen. Wählen Sie eine **virtuelle Schnittstelle** aus. Geben Sie die **Nachbar-IP-Adresse** ein.

The screenshot shows the 'Neighbors' configuration page with a neighbor added. The table has the following data:

| Virtual Interface | Source IP | Neighbor IP | Neighbor AS | Hold Time(s) | Local Preference | IGP Metric | Multi Hop | Password | Delete |
|--------------------|-------------|-------------|-------------|--------------|------------------|-------------------------------------|-------------------------------------|----------|--------|
| VirtualInterface-1 | 172.58.1.20 | * | 2 | 180 | 100 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | |

Below the table, there is a 'Policies' section with an 'Add' button. The 'Policies' table has columns: Order, Network Address, BGP Community(AA:NN), AS Path, BGP Policy, Direction, and Delete.

3. Richtlinien hinzufügen. Wählen Sie wie gewünscht **Netzwerkadresse**, **BGP-Community** und **AS-Pfaddetails** aus. Klicken Sie auf **Übernehmen**.

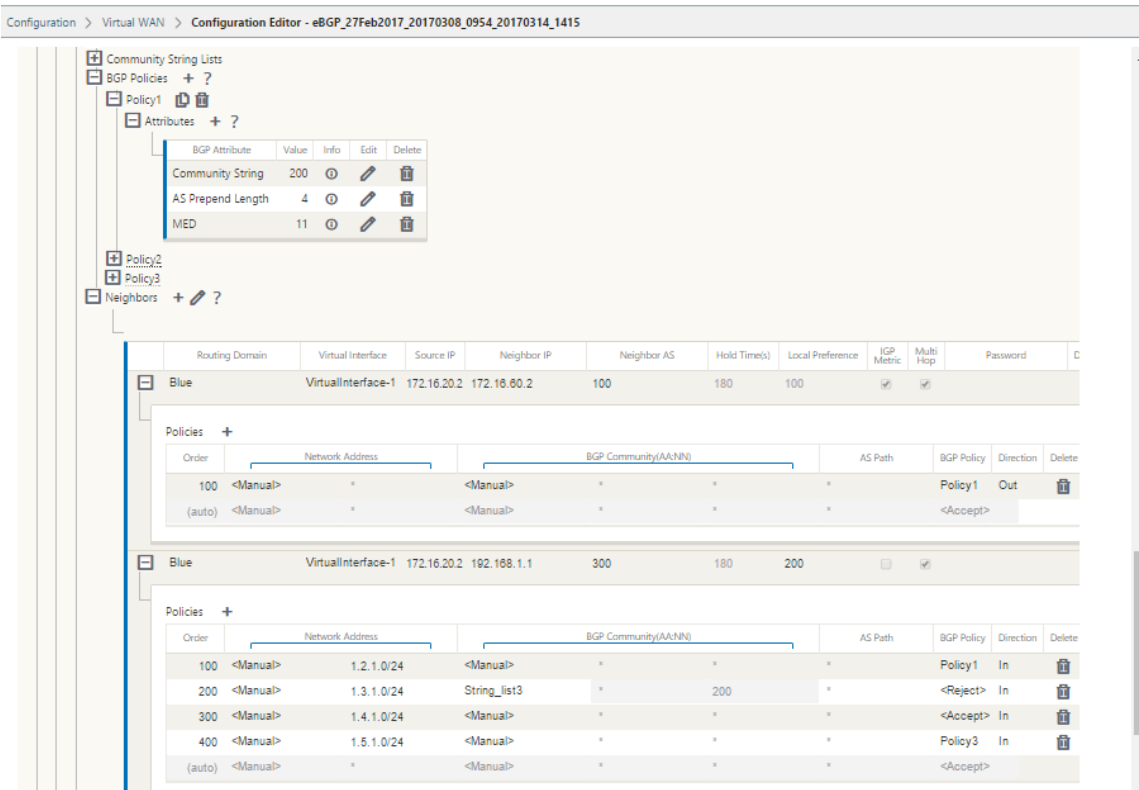
The screenshot shows the 'Neighbors' configuration page with a policy added. The table has the following data:

| Virtual Interface | Source IP | Neighbor IP | Neighbor AS | Hold Time(s) | Local Preference |
|--------------------|-------------|-------------|-------------|--------------|------------------|
| VirtualInterface-1 | 172.58.1.20 | * | 2 | 180 | 100 |

Below the table, there is a 'Policies' section with an 'Add' button. The 'Policies' table has columns: Order, Network Address, BGP Community(AA:NN), and AS Path.

| Order | Network Address | BGP Community(AA:NN) | AS Path |
|-------|-----------------|----------------------|---------|
| 100 | <Manual> * | <Manual> * | * |

The 'BGP Community(AA:NN)' dropdown menu is open, showing options: <Manual> and New_Community_String_List.



4. Gehen Sie zu **Überwachung > Routing-Protokolle > Dynamische Routing-Protokolle**, um die konfigurierten BGP-Richtlinien und Nachbarn für die DC- oder Zweigstand-Appliance zu überwachen.

Sie können die Debug-Protokollierung aktivieren und Protokolldateien für das Routing auf der Seite **Monitor > Routing-Protokoll** anzeigen. Die Protokolle für den Routing-Daemon werden in separate Protokolldateien aufgeteilt. Die Standard-Routinginformationen werden in *dynamic_routing.log* gespeichert, während dynamische Routingprobleme in *dynamic_routing_diagnostics.log* erfasst werden, die aus der Überwachung von Routingprotokollen angezeigt werden können.

BGP Sanfte Neukonfiguration

Routingrichtlinien für BGP-Peer umfassen Konfigurationen wie Routenzuordnung, Verteilerliste, Präfixliste und Filterliste, die sich auf eingehende oder ausgehende Routingtabellenaktualisierungen auswirken können. Wenn sich die Routingrichtlinie geändert hat, muss die BGP-Sitzung gelöscht oder zurückgesetzt werden, damit die neue Richtlinie wirksam wird.

Das Löschen einer BGP-Sitzung mit einem Hard Reset macht den Cache ungültig und führt zu negativen Auswirkungen auf den Betrieb der Netzwerke, da die Informationen im Cache nicht verfügbar werden.

Die BGP Soft Reset Enhancement Funktion bietet automatische Unterstützung für dynamisches Soft-

Reset eingehender BGP-Routing-Tabellenaktualisierungen, die nicht von Aktualisierungsinformationen für gespeicherte Routingtabellen abhängig sind.

Problembehandlung

Um die BGP-Parameter anzuzeigen, navigieren Sie zu **Überwachung > Routingprotokolle** > wählen Sie im Feld **AnsichtBGP-Status** aus.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: BGP State Routing Domain: Default_RoutingDomain BGP Session: <ALL>

Reset Session

Refresh

BGP State

| name | proto | table | state | since | Info |
|----------------|-------|-------|-------|---------------------|-------------|
| bgp1_rdomain_0 | BGP | T0 | up | 2020-08-27 10:46:44 | Established |

Preference: 100
Input filter: neighbour_0_in
Output filter: neighbour_0_out
Routes: 8 imported, 4 exported, 1 preferred
Route change stats:

| | received | rejected | filtered | ignored | accepted |
|-------------------|----------|----------|----------|---------|----------|
| Import updates: | 16 | 0 | 0 | 8 | 8 |
| Import withdraws: | 0 | 0 | --- | 0 | 0 |
| Export updates: | 43 | 19 | 18 | --- | 6 |
| Export withdraws: | 2 | --- | --- | --- | 2 |

BGP state: Established
Neighbor address: 172.58.1.28
Neighbor AS: 10
Citrix SD-WAN Interface: vni-0
Neighbor ID: 105.105.105.105
Neighbor caps: refresh AS4
Session: internal multihop AS4
Source address: 172.58.1.10
Hold timer: 130/180
Keepalive timer: 46/60

Sie können die Dynamische Routingprotokolle beobachten, um festzustellen, ob ein Problem mit der BGP-Konvergenz vorliegt.

Diagnose

Debug Logging: ☒ On ☐ Off

Filename:

dynamic_routing_diagnostics.log

View Log

iBGP

May 10, 2021

Citrix SD-WAN Appliance mit iBGP auf der LAN-Seite und eBGP auf der WAN-Seite:

Citrix SD-WAN Appliances werben mit NEXT HOP SELF alle erlernten eBGP-Routen, wenn sie mit iBGP auf der LAN-Seite und eBGP auf der WAN-Seite bereitgestellt werden.

Mehrere iBGP-LAN-Router in einer linearen Netzwerktopologie mit Direct Peering und vernetzt mit Citrix SD-WAN.

Einschränkungen:

- AS-Path Prepend-, Med und Community-Attribute werden nicht unterstützt.
- Routenfilterung zwischen OSPF und BGP während der Neuverteilung wird nicht unterstützt. Entweder werden alle (oder) keine der von OSPF erlernten Routen an BGP-Peers beworben und umgekehrt.
- Routenaggregation wird nicht unterstützt.
- Es können nur maximal 16 BGP-Peers (einschließlich iBGP und eBGP) konfiguriert werden.

eBGP

May 10, 2021

SD-WAN-Site kommuniziert mit nicht SD-WAN-Site über eBGP:

Wenn ein Standort ohne SD-WAN-Appliance mit einem anderen Standort mit SD-WAN-Appliance (Site-A) über einen einzelnen WAN-Pfad kommuniziert (nur Internet verfügbar) und wenn der Standort mit SD-WAN-Appliance (Site-A) die Internetverbindung verliert, kann der Standort ohne SD-WAN mit Site-A über ein anderes SD-WAN kommunizieren. -Appliance-Standort (Standort-B). Site-B leitet den Datenverkehr von der Site ohne SD-WAN-Appliance an die Site-A weiter.

Kommunikation zwischen SD-WAN-Sites mit Virtual Path und eBGP:

Bietet Unterlay Route Learning zur Kommunikation mit lokalen Subnetzen von Remotestandorten, wenn sich der virtuelle Pfad zwischen zwei Standorten befindet, während die Virtual WAN-Appliance noch aktiv ist.

Anwendungsrouten

May 10, 2021

In einem typischen Unternehmensnetzwerk greifen die Zweigstellen auf Anwendungen im lokalen Rechenzentrum, im Cloud-Rechenzentrum oder in den SaaS-Anwendungen zu. Die Anwendungs-Routing-Funktion ermöglicht es Ihnen, die Anwendungen einfach und kosteneffizient durch Ihr Netzwerk zu steuern. Wenn beispielsweise ein Benutzer am Zweigstandort versucht, auf eine SaaS-Anwendung zuzugreifen, kann der Datenverkehr so weitergeleitet werden, dass die Zweigstellen direkt auf die SaaS-Anwendungen im Internet zugreifen können, ohne vorher das Rechenzentrum durchlaufen zu müssen.

Mit Citrix SD-WAN können Sie die Anwendungsrouten für die folgenden Dienste definieren:

- **Virtueller Pfad:** Dieser Dienst verwaltet den Datenverkehr über die virtuellen Pfade. Ein virtueller Pfad ist eine logische Verbindung zwischen zwei WAN-Verbindungen. Es umfasst eine Sammlung von WAN-Pfaden, die kombiniert werden, um eine hohe Service-Level-Kommunikation zwischen zwei SD-WAN-Knoten zu ermöglichen. Die SD-WAN-Appliance misst das Netzwerk pro Pfad und passt sich an veränderte Anwendungsanforderungen und WAN-Bedingungen an. Ein virtueller Pfad kann statisch (immer vorhanden) oder dynamisch sein (nur vorhanden, wenn der Datenverkehr zwischen zwei SD-WAN-Appliances einen konfigurierten Schwellenwert erreicht).
- **Internet:** Dieser Dienst verwaltet den Datenverkehr zwischen einem Enterprise-Standort und Websites im öffentlichen Internet. Der Internetverkehr ist nicht gekapselt. Wenn eine Überlastung auftritt, verwaltet das SD-WAN aktiv die Bandbreite, indem es den Internetverkehr relativ zum virtuellen Pfad und dem Intranetdatenverkehr einschränkt.
- **Intranet:** Dieser Dienst verwaltet Enterprise-Intranet-Datenverkehr, der nicht für die Übertragung über einen virtuellen Pfad definiert wurde. Der Intranetdatenverkehr ist nicht gekapselt. Das SD-WAN verwaltet die Bandbreite, indem dieser Datenverkehr im Verhältnis zu anderen Diensttypen während der Staus begrenzt wird. Unter bestimmten Bedingungen und wenn Intranet-Fallback auf dem virtuellen Pfad konfiguriert ist, kann Datenverkehr, der normalerweise durch den virtuellen Pfad fließt, stattdessen als Intranet-Datenverkehr behandelt werden.
- **Lokal:** Dieser Dienst verwaltet den lokalen Datenverkehr auf der Website, der keinem anderen Dienst entspricht. SD-WAN ignoriert Datenverkehr, der für eine lokale Route bestimmt ist.
- **GRE-Tunnel:** Dieser Dienst verwaltet IP-Datenverkehr, der für einen GRE-Tunnel bestimmt ist, und entspricht dem am Standort konfigurierten LAN-GRE-Tunnel. Mit der Funktion GRE Tunnel können Sie SD-WAN-Appliances so konfigurieren, dass GRE Tunnel im LAN beendet werden. Bei

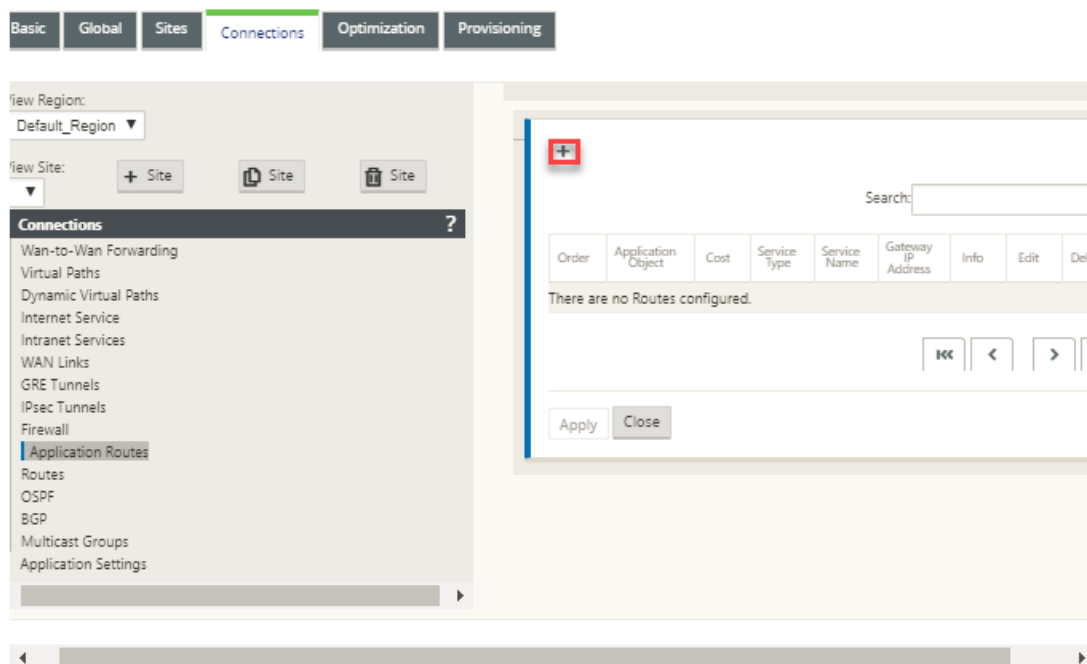
einer Route mit Servicetyp GRE Tunnel muss sich das Gateway in einem der Tunnelsubnetze des lokalen GRE Tunnels befinden.

- **LAN IPsec-Tunnel:** Dieser Dienst verwaltet IP-Datenverkehr, der für einen LAN-IPsec-Tunnel bestimmt ist, und entspricht dem am Standort konfigurierten LAN-IPsec-Tunnel. Mit der LAN-IPsec-Tunnelfunktion können Sie SD-WAN-Appliances so konfigurieren, dass IPsec-Tunnel auf der LAN- oder WAN-Seite beendet werden.

Um Service Steering für Anwendungen durchzuführen, ist es wichtig, eine Anwendung auf dem ersten Paket selbst zu identifizieren. Zunächst fließen die Pakete durch die IP-Route, sobald der Datenverkehr klassifiziert und die Anwendung bekannt ist, wird die entsprechende Anwendungsroute verwendet. Die erste Paketklassifizierung wird durch Erlernen der IP-Subnetze und Ports erreicht, die mit Anwendungsobjekten verknüpft sind. Diese werden mit historischen Klassifizierungsergebnissen des DPI-Klassifikators und vom Benutzer konfigurierten IP-Port-Typen abgerufen.

So konfigurieren Sie das Anwendungsrouting:

1. Navigieren Sie im Konfigurations-Editor zu **Connections > Application Routes** und klicken Sie auf **+**.



2. Legen Sie auf der Seite **Hinzufügen** die folgenden Parameter fest:
 - **Application Object:** Das Anwendungsobjekt, das Sie steuern möchten. Die von Ihnen erstellten Anwendungsobjekte werden hier aufgelistet. Weitere Informationen finden Sie im Abschnitt **Anwendungsobjekte** im [Anwendungsklassifizierung](#) Thema.

Add

Application Object: CUSTOM

Routing Domain: <Default>

Cost: 5

Service Type: Virtual Path

Gateway IP Address:

Next Hop Site: <None>

☒ Eligibility Based On Path

Path: Branch1-WL-1->MCN-DC-WL-3

Add **Cancel**

- **Routingdomäne:** Die Routingdomäne, die von der Anwendungsroute verwendet werden soll. Wählen Sie eine der konfigurierten Routingdomänen aus.
- **Kosten:** Eine Gewichtung, die die Routenpriorität für diese Route bestimmt. Lower-Cost-Routen haben Vorrang vor höheren Kosten Routen. Der Bereich beträgt 1—65534. Der Standardwert ist 5.
- **Servicetyp:** Wählen Sie einen der folgenden Dienste aus. Dadurch wird die Anwendung einem Dienst zugeordnet.
- **Virtueller Pfad:** Identifiziert Anwendungsdatenverkehr als virtueller Pfadverkehr und entspricht einem virtuellen Pfad basierend auf Regeln für virtuelle Pfade. Geben Sie im Feld **Next Hop Site** die Next-Hop-Remote-Site ein, an die Virtual Path Pakete weitergeleitet werden.

Hinweis

Jeder Flow, der auf die Virtual Path Application Routes trifft, geht nicht über dynamischen virtuellen Pfad.

- **Internet:** Identifiziert Anwendungsdatenverkehr als Internetverkehr und entspricht dem Internetdienst.
- **Intranet:** Identifiziert Anwendungsdatenverkehr als Intranetdatenverkehr und entspricht einem Intranetdienst basierend auf den Intranetregeln. Wählen Sie im Feld **Intranetdienst** einen Intranetdienst aus, der für die Route verwendet werden soll.
- **Lokal:** Identifiziert den Anwendungsdatenverkehr als lokal zur Site und entspricht keinem Dienst. Datenverkehr, der für eine lokale Route bestimmt ist, wird ignoriert.

Hinweis

Für den lokalen Diensttyp treffen die konfigurierten IP-Routen nach Abschluss der DPI-Klassifizierung die Routing-Entscheidung.

- **GRE-Tunnel:** Identifiziert den Anwendungsdatenverkehr als für einen GRE-Tunnel bestimmt und entspricht dem am Standort konfigurierten LAN-GRE-Tunnel. Geben Sie im Feld **Gateway IP-Adresse** die Gateway-IP-Adresse ein, die sich im Subnetz des LAN GRE Tunnels befinden muss. Wählen Sie **Berechtigung basierend auf Gateway** aus, damit die Route keinen Datenverkehr empfängt, wenn das Gateway nicht erreichbar ist.
- **LAN IPsec-Tunnel:** Identifiziert den Anwendungsdatenverkehr als für einen LAN-IPsec-Tunnel bestimmt und entspricht dem am Standort konfigurierten LAN-IPsec-Tunnel. Wählen Sie im Feld **IPsec-Tunnel** einen der konfigurierten IPsec-Tunnel aus. Wählen Sie **Berechtigung basierend auf Tunnel** aus, damit die Route keinen Datenverkehr empfängt, wenn der Tunnel nicht erreichbar ist.

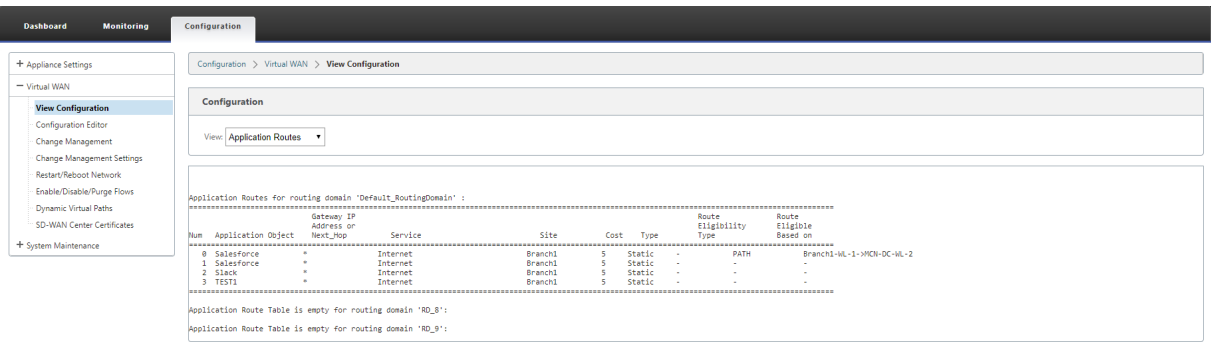
Hinweis

Wenn Sie einen Dienst für eine benutzerdefinierte Anwendung ausgewählt haben, ändern Sie ihn nicht.

- **Berechtigung basierend auf Pfad:** Wählen Sie diese Option aus, damit die Route keinen Datenverkehr empfängt, wenn der angegebene Pfad ausgefallen ist. Geben Sie im Feld **Pfad** den Pfad an, der zum Bestimmen der Routenberechtigung verwendet werden soll.

3. Klicken Sie auf **Übernehmen**.

So zeigen Sie die auf Ihrer SD-WAN-Appliance konfigurierten Anwendungsrouten an. Navigieren Sie in der SD-WAN-GUI zu **Konfiguration > Virtuelles WAN > Konfiguration anzeigen** . Wählen Sie im Dropdownmenü **Ansicht** die Option **Anwendungsrouten** aus.



So zeigen Sie Statistikdaten für die Anwendungsrouten an:

1. Navigieren Sie in der SD-WAN-GUI zu **Überwachung > Statistik** .

2. Wählen Sie in der Dropdown-Liste **Anzeigen** die Option **Anwendungsrouten** aus.

Monitoring > Statistics

Statistics

Show: Application Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain: Default_RoutingDomain

Filter: Any column Apply

Show: 100 entries Showing 1 to 4 of 4 entries

| Num | Application Object | Gateway IP Address | Service | Firewall Zone | Reachable | Site | Type | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|--------------------|--------------------|----------|---------------|-----------|---------|--------|------|-----------|----------|------------------|---------------------------|
| 0 | TEST1 | * | Internet | Internet_Zone | YES | Branch1 | Static | 5 | 0 | YES | N/A | N/A |
| 1 | Stack | * | Internet | Internet_Zone | YES | Branch1 | Static | 5 | 0 | YES | N/A | N/A |
| 2 | Salesforce | * | Internet | Internet_Zone | YES | Branch1 | Static | 5 | 173 | YES | Path | Branch1-WL-1->MCN-DC-WL-2 |
| 3 | Salesforce | * | Internet | Internet_Zone | YES | Branch1 | Static | 5 | 0 | YES | N/A | N/A |

Showing 1 to 4 of 4 entries

Sie können die folgenden Statistiken anzeigen:

- **Application Object:** Name des Anwendungsobjekts.
- **Gateway IP-Adresse:** Die Gateway-IP-Adresse, die von Anwendungsobjekten mit dem GRE-Tunneldiensttyp verwendet wird.
- **Dienst:** Der Dienstyp, der dem Anwendungsobjekt zugeordnet ist.
- **Firewall-Zone:** Die Firewall-Zone, in die diese Route fällt.
- **Erreichbar:** Der Status der Anwendungsroute.
- **Site:** Name der Website.
- **Typ:** Gibt an, ob die Route statisch oder dynamisch ist.
- **Kosten:** Die Priorität der Route.
- **Trefferanzahl:** Gibt an, wie oft die Anwendungsroute verwendet wird, um den Datenverkehr zu steuern.
- **Berechtigt:** Ist die Anwendungsroute berechtigt, den Datenverkehr zu senden.
- **Berechtigungsart:** Die Art der Berechtigungsbedingung für die Route, die auf diese Route angewendet wird. Der Berechtigungstyp kann Pfad, Gateway oder Tunnel sein.
- **Berechtigungswert:** Der Wert, der für die Berechtigungsbedingung für die Route angegeben wurde.

Hinweis

In der aktuellen Version können Anwendungen, die zur Anwendungsfamilie gehören, mit dem im Anwendungsobjekt definierten Typ übereinstimmen, nicht gesteuert werden.

Problembehandlung

Nachdem Sie die Anwendungsroute erstellt haben, können Sie mithilfe des Abschnitts **Überwachung** bestätigen, dass die Anwendung korrekt an den vorgesehenen Dienst weitergeleitet wurde.

Navigieren Sie zu den folgenden Seiten, um anzuzeigen, ob die Anwendung korrekt an den beabsichtigten Dienst weitergeleitet wurde:

- **Überwachung > Statistik > Anwendungsrouten**
- **Überwachung > Flows**
- **Überwachung > Firewall**

Wenn ein unerwartetes Routingverhalten auftritt, sammeln Sie das STS-Diagnosepaket, während das Problem beobachtet wird, und teilen Sie es mit dem Citrix Support-Team.

Das STS-Paket kann mit **Konfiguration > Systemwartung > Diagnose > Diagnoseinformationen** erstellt und heruntergeladen werden.

Routenfilterung

May 10, 2021

Für Netzwerke mit aktiviertem Routenlernen bietet Citrix SD-WAN mehr Kontrolle darüber, welche SD-WAN-Routen an Routing Nachbarn angekündigt werden und welche Routen von Routing Nachbarn empfangen werden, anstatt alle oder keine Routen zu akzeptieren.

- Exportfilter werden verwendet, um Routen für Werbung mit OSPF- und BGP-Protokollen basierend auf bestimmten Übereinstimmungen ein- oder auszuschließen Kriterien. Exportfilterregeln sind die Regeln, die erfüllt sein müssen, wenn SD-WAN-Routen über dynamische Routingprotokolle Werbung gemacht werden. Alle Routen werden standardmäßig an Peers angekündigt.
- Importfilter werden verwendet, um Routen zu akzeptieren oder nicht zu akzeptieren, die mithilfe von OSPF- und BGP-Nachbarn empfangen werden, basierend auf bestimmten Übereinstimmungskriterien. Importfilterregeln sind die Regeln, die erfüllt werden müssen, bevor dynamische Routen in die SD-WAN-Routendatenbank importiert werden. Standardmäßig werden keine Routen importiert.

Die Routenfilterung wird auf LAN-Routen und virtuellen Pfadrouten in einem SD-WAN-Netzwerk (Data Center/Branch) implementiert und über BGP und OSPF an ein Nicht-SD-WAN-Netzwerk angekündigt.

Sie können bis zu 512 Exportfilter und 512 Importfilter konfigurieren. Dies ist das Gesamtlimit, nicht pro Routingdomänenlimit.

Exportfilter konfigurieren

Navigieren Sie im **Konfigurations-Editor** zu **Verbindungen > Regionen > Standort > OSPF** oder **BGP > Filter exportieren**.

Section: Export Filters

100

<Manual>

10.102.29.220/16

eq

12

eq

10

Virtual Path

Client-1

*

☒

☒

Export OSPF Route Type:
Type 5 AS External

Export OSPF Route Weight:
4

100

<Manual>

*

eq

*

eq

*

Any

<Any>

*

☒

☒

Apply

Revert

Verwenden Sie die folgenden Kriterien, um jeden Exportfilter zu erstellen, den Sie erstellen möchten.

| Feldkriterien | Beschreibung | Wert |
|----------------------|---|--|
| Reihenfolge | Die Reihenfolge, in der Filter priorisiert werden. Der erste Filter, dem eine Route entspricht, wird auf diese Route angewendet | 100, 200, 300, 400, 500, 600 |
| Netzwerkadresse | Geben Sie die IP-Adresse und die Subnetzmaske des konfigurierten Netzwerkobjekts ein, das das Netzwerk der Route beschreibt | <ul style="list-style-type: none">IP-Adresse |
| Präfix | Um Routen nach Präfix abzugleichen, wählen Sie ein Übereinstimmungsprädikat aus dem Menü und geben Sie ein Routenpräfix in das angrenzende Feld ein | <ul style="list-style-type: none">eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to |
| Citrix SD-WAN Kosten | Die Methode (Prädikat) und die SD-WAN Routenkosten, die verwendet werden, um die Auswahl der exportierten Routen zu beschränken | Numerischer Wert |
| Servicetyp | Wählen Sie die Diensttypen aus, die übereinstimmenden Routen aus einer Liste der Citrix SD-WAN Dienste zugewiesen sind. | Beliebig, Lokal, Virtueller Pfad, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel |

| Feldkriterien | Beschreibung | Wert |
|---------------------|---|------------------|
| Standort/Dienstname | Geben Sie für Intranet, LAN GRE Tunnel und LAN IPsec-Tunnel den Namen des konfigurierten Diensttyps an, der verwendet werden soll. | Textzeichenfolge |
| Gateway-IP-Adresse | Wenn Sie LAN GRE Tunnel als Service Type wählen, geben Sie die Gateway IP für den Tunnel ein | IP-Adresse |
| Einschließen | Aktivieren Sie das Kontrollkästchen Routen einschließen, die mit diesem Filter übereinstimmen. Ansonsten werden passende Routen ignoriert | Ohne |
| Aktiviert | Aktivieren Sie das Kontrollkästchen Diesen Filter aktivieren. Andernfalls wird der Filter ignoriert | Ohne |
| Löschen | Wählen Sie das Löschsymbol, um diesen Filter zu löschen. | Ohne |
| Klonen | Klicken Sie auf das Klonsymbol, um eine Kopie eines vorhandenen Filters zu erstellen | Ohne |

Import-Filter konfigurieren

Navigieren Sie im **Konfigurations-Editor** zu **Verbindungen > Regionen > Standort > OSPF** oder **BGP > Filter importieren**.

Section: Import Filters

| | Order | Source Router | Destination | Prefix | Next Hop | Protocol | Route Tag | Cost | AS Path Length | Include | Enabled | | | | |
|---|-------|---------------|-------------|----------------|----------|----------|-------------|-------|----------------|---------|---------|------|---|-------------------------------------|-------------------------------------|
| + | 100 | 10.130.240.5 | <Manual> ▼ | 10.102.10.9/24 | eq ▼ | 6 | 10.102.45.9 | BGP ▼ | * | eq ▼ | * | le ▼ | 5 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 100 | * | <Manual> ▼ | * | eq ▼ | * | * | Any ▼ | * | eq ▼ | * | eq ▼ | * | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Apply Revert

Verwenden Sie die folgenden Kriterien, um jeden Exportfilter zu erstellen, den Sie erstellen möchten.

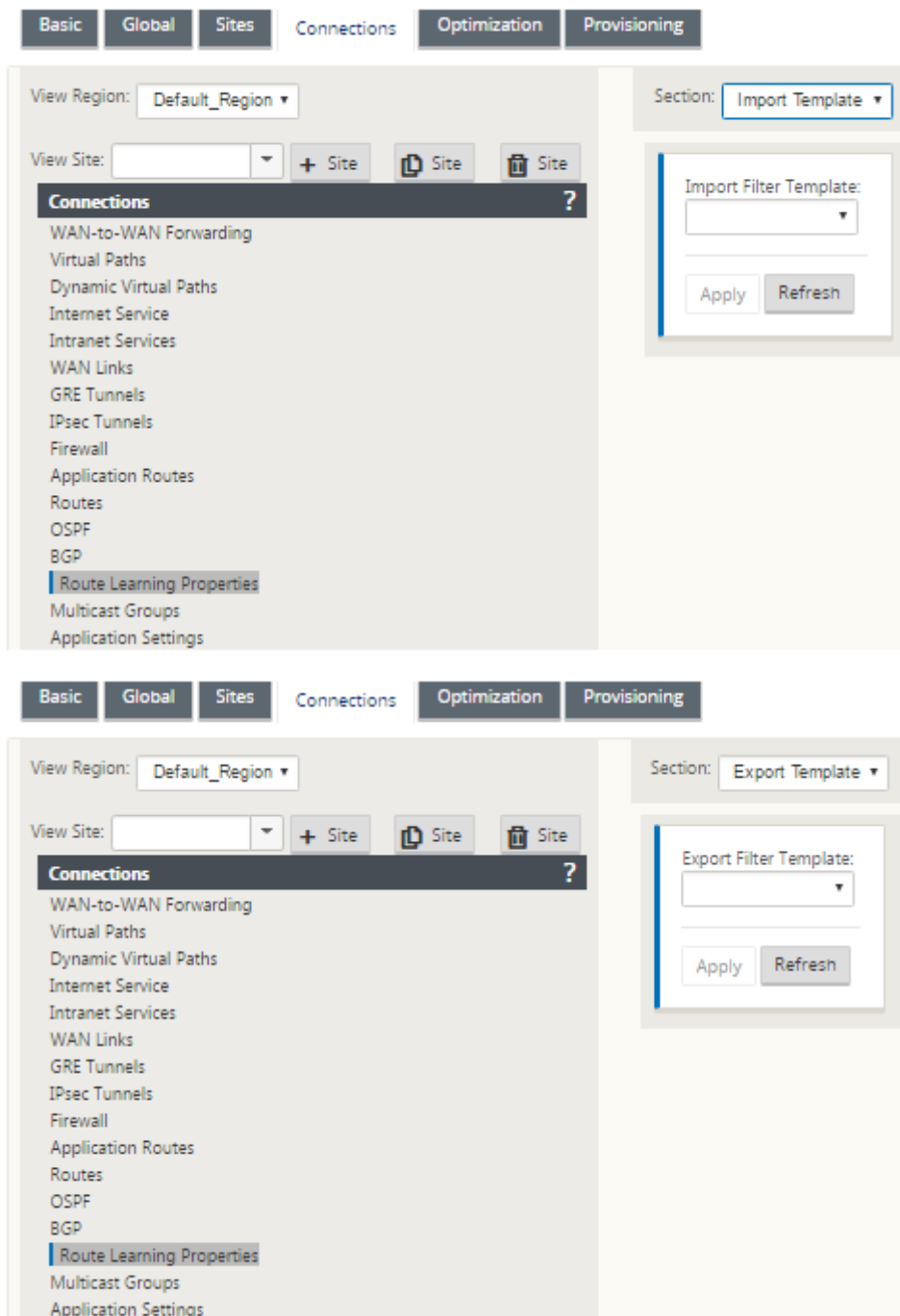
| Feldkriterien | Beschreibung | Wert |
|---------------|--|--|
| Reihenfolge | Die Reihenfolge, in der Filter priorisiert werden. Der erste Filter, dem eine Route entspricht, wird auf diese Route angewendet | 100, 200, 300, 400, 500, 600 |
| Quellrouter | Die IP-Adresse des Quellrouters, es gilt nur für iBGP | • IP-Adresse |
| Ziel | IP-Adresse und Subnetzmaske des Ziels einer Route | • IP-Adresse |
| Präfix | Um Routen nach Präfix abzugleichen, wählen Sie ein Übereinstimmungsprädikat aus dem Menü und geben Sie ein Routenpräfix in das angrenzende Feld ein | • eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to |
| Nächster Hop | Die IP-Adresse des nächsten Hop | • IP-Adresse |
| Protokoll | Das Routingprotokoll, mit dem eine Route erlernt wird | OSPF oder BGP |
| Route Tag | Das OSPF-Routen-Tag, das der Filter übereinstimmt. OSPF-Routen-Tags verhindern Routingschleifen während der gegenseitigen Umverteilung zwischen OSPF und anderen Protokollen | Numerischer Wert |
| Kosten | Die Routenkosten, die zum Abgleich von OSPF-Routen für den Import verwendet werden | Numerischer Wert |
| AS-Pfadlänge | Die AS-Pfadlänge, die zum Importieren von BGP-Routen verwendet wird | Numerischer Wert |

| Feldkriterien | Beschreibung | Wert |
|---------------|---|------|
| Einschließen | Aktivieren Sie das Kontrollkästchen Routen einschließen, die mit diesem Filter übereinstimmen. Ansonsten werden passende Routen ignoriert | Ohne |
| Aktiviert | Aktivieren Sie das Kontrollkästchen Diesen Filter aktivieren. Andernfalls wird der Filter ignoriert | Ohne |
| Löschen | Klicken Sie auf das Löschesymbol, um diesen Filter zu löschen. | Ohne |
| Klonen | Klicken Sie auf das Klonsymbol, um eine Kopie eines vorhandenen Filters zu erstellen | Ohne |

Konfigurieren von Routenrichtlinienfiltervorlagen

Sie können mehrere Import- oder Exportfiltervorlagen mit verschiedenen Filterregeln erstellen und die Vorlage an jedem Standort zuordnen.

Die vom Benutzer erstellten Import/Exportfilterregeln auf Websiteebene haben mehr Vorrang. Die Vorlagenregeln folgen den vom Benutzer erstellten Regeln, wenn sie der Website im Abschnitt **Routenlernen** von Connections zugeordnet sind.



Routenzusammenfassung

May 10, 2021

Mit der Zunahme der Größe der Unternehmensnetzwerke müssen die Router die große Anzahl von

Routen in ihrer Routingtabelle beibehalten. Die Router benötigen erhöhte CPU-, Arbeitsspeicher- und Bandbreitenressourcen, um die großen Routingtabellen nachzuschauen und einzelne Routen zu verwalten. Sie können eine zusammenfassende Route mit Dienstypen Lokal und Verwerfen konfigurieren. Diese zusammenfassende Route wird an die Next-Hop-Geräte angekündigt.

So konfigurieren Sie eine Zusammenfassungsroute für ein lokales Subnetz:

1. Navigieren Sie im Konfigurations-Editor zu **Verbindungen > Routen**, und klicken Sie auf das **+**, um eine Route hinzuzufügen.
2. Legen Sie auf der Seite **Route hinzufügen** die folgenden Parameter fest, und klicken Sie dann auf **Hinzufügen**.
 - **Netzwerk-IP-Adresse:** Die berechnete IP-Adresse der zusammenfassenden Route.
 - **Kosten:** Eine Gewichtung, die die Routenpriorität für diese Route bestimmt. Lower-Cost-Routen haben Vorrang vor höheren Kosten Routen. Der Bereich beträgt 1—15. Der Standardwert ist 5.
 - **Routingdomäne:** Routing-Protokolle, die den zentralen Verwaltungspunkt für die Verwaltung eines Unternehmensnetzwerks, eines Zweigstellennetzwerks oder eines Rechenzentrumsnetzwerks bereitstellen.
 - **Dienststart:** Wählen Sie Lokaler Dienstyp aus.

Hinweis

Sie können nur Service-Typen **Lokal** und **Verwerfen** für Sammelrouten auswählen.

- **Gateway-IP-Adresse:** Gateway-IP-Adresse für diese Route.
- **Route exportieren:** Exportiert die Route in andere verbundene Standorte.
- **Summary Route:** Werbt die Route als einzelne Sammelroute zu den anderen verbundenen Geräten anstelle aller anderen übereinstimmenden Subnetze an.

Add ? x

| Network IP Address | Routing Domain | Cost | Service Type | Gateway IP Address |
|--------------------|-----------------|------|--------------|--------------------|
| 172.16.0.0/22 | Default_Routing | 5 | Local | |

☒ Export Route
☒ Summary Route
☐ Eligibility Based On Path
 Path: <None>
☐ Eligibility Based On Gateway

Add **Cancel**

Problembehandlung

Die zusammengefassten Routen, die auf dem MCN konfiguriert sind, werden über den virtuellen Pfad an die Niederlassung gesendet. Falls Sie die Details des virtuellen Pfads nicht in der Routing-Tabelle des Branch sehen, überprüfen Sie das Zweigstellen-Dashboard. Das Dashboard zeigt den Status des virtuellen Pfads zwischen dem MCN und Branch an.

Dashboard **Monitoring** **Configuration**

System Status

| | |
|-------------------------|--------------------------------------|
| Name: | BR1_VPX |
| Model: | VPX |
| Sub-Model: | BASE |
| Appliance Mode: | Client |
| Serial Number: | 5f4519dd-e39a-d3f6-24a6-6ba0e6578d2c |
| Management IP Address: | 10.105.172.7 |
| Appliance Uptime: | 6 days, 56 minutes, 1.4 seconds |
| Service Uptime: | 6 days, 50 minutes, 39.0 seconds |
| Routing Domain Enabled: | Default_RoutingDomain |

Local Versions

| | |
|---------------------------|-------------------------|
| Configuration Created On: | Wed Sep 2 11:15:54 2020 |
| Software Version: | 11.2.1.53.864510 |
| Built On: | Aug 25 2020 at 19:02:21 |
| Hardware Version: | VPX |
| OS Partition Version: | 5.1 |

Virtual Path Service Status

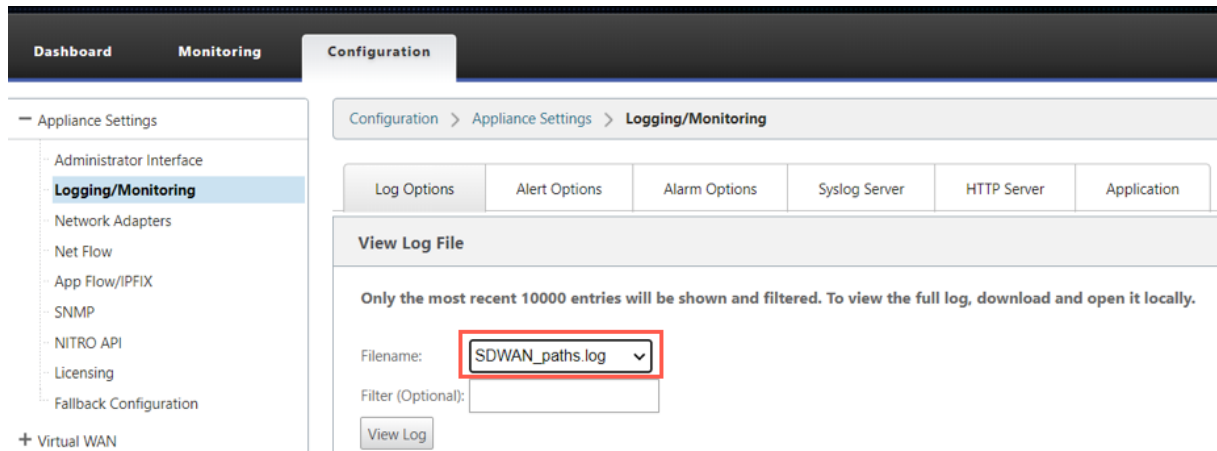
| | |
|------------------------------|---|
| Virtual Path MCN_VPX-BR1_VPX | Uptime: 6 days, 50 minutes, 19.0 seconds. |
|------------------------------|---|

Wenn der virtuelle Pfad ausgefallen ist, überprüfen Sie den Grund dafür unter **Konfiguration > Logging/Monitoring**.

Wählen Sie eine der folgenden Dateien aus der Dropdown-Liste **Dateiname** aus, um dies zu überprüfen:

- SDWAN_paths.log

- SDWAN_common.log



Protokollpräferenz

May 10, 2021

Die Protokolleinstellung ist eine Citrix SD-WAN spezifische Funktion, die der Administratorentfernung des Routers ähnelt.

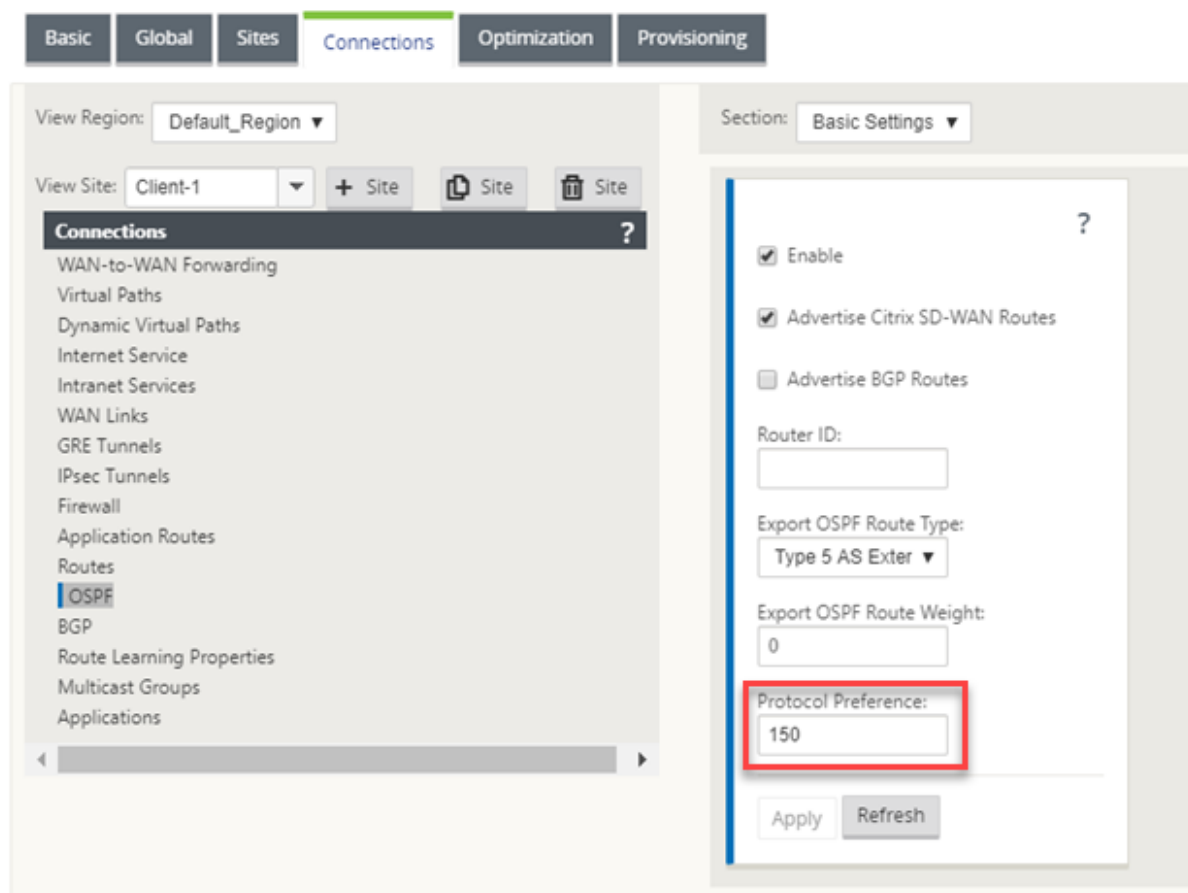
Wenn Citrix SD-WAN ein Routenpräfix über virtuelle Pfade, OSPF-Protokoll oder BGP-Protokoll erlernt, folgt es der folgenden Standardeinstellungsreihenfolge.

- OSPF -150
- BGP - 100
- SD-WAN - 250

Das Protokoll mit der höchsten Präferenzreihenfolge ist am meisten bevorzugt. Die Route unter Verwendung des Protokolls mit dem höchsten Protokollpräferenzwert

Sie können das BGP-Protokoll auch über das OSPF-Protokoll verwenden, indem Sie den Protokolleinstellungswert festlegen, während Sie das BGP- oder OSPF-Protokoll konfigurieren. Sie können eine Voreinstellung im Bereich von 100 bis 200 angeben.

Die Protokollprioritätsinformationen sind lokal für die Citrix SD-WAN Appliance und werden nicht an Peer-Netzwerkelemente angekündigt.



Multicast-Routing

May 10, 2021

Multicast-Routing ermöglicht eine effiziente Verteilung des 1:n-Datenverkehrs. Eine Multicastquelle sendet Multicast-Datenverkehr in einem einzelnen Stream an eine Multicast-Gruppe. Die Multicastgruppe enthält Empfänger wie Hosts und angrenzende Router, die das IGMP-Protokoll für die Multicastkommunikation verwenden. Voice over IP, Video on Demand, IP-TV und Videokonferenzen sind einige der gängigen Technologien, die Multicast-Routing verwenden. Wenn Sie Multicastroouting auf der Citrix SD-WAN Appliance aktivieren, fungiert die Appliance als Multicastrouter.

Quellspezifischer Multicast

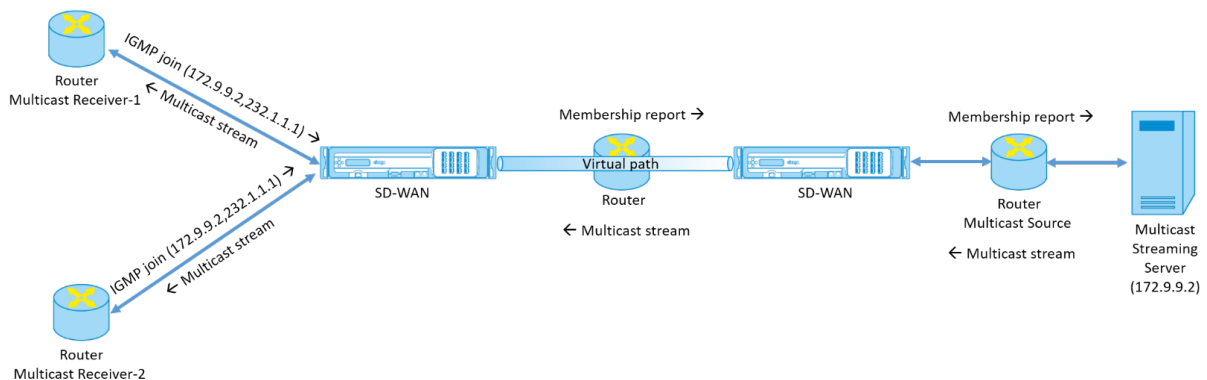
Multicast-Protokolle ermöglichen Multicastempfänger in der Regel den Empfang von Multicast-Datenverkehr von jeder Quelle. Mit quellspezifischem Multicast (SSM) können Sie die Quelle angeben, von der die Empfänger den Multicastverkehr empfangen. Es stellt sicher, dass die

Empfänger nicht offene Listener für jede Quelle sind, die Multicast-Streams sendet, sondern vielmehr eine bestimmte Multicastquelle hören. SSM reduziert die Kosten für Ressourcen, die für den Verbrauch von Datenverkehr aus jeder möglichen Quelle verwendet werden, und bietet außerdem eine Sicherheitsstufe, indem sichergestellt wird, dass die Empfänger Datenverkehr von einem bekannten Absender empfangen.

Die folgende Topologie zeigt zwei Multicastempfänger an einem Zweigstandort und einen Multicastserver (172.9.9.2) im Rechenzentrum. Der Multicast-Server streamt Datenverkehr über eine bestimmte Gruppe (232.1.1.1), wobei die Empfänger der Gruppe beitreten. Jeder Datenverkehr, der in der Multicastgruppe gestreamt wird, wird an alle Empfänger weitergeleitet, die der Gruppe beigetreten sind.

Hinweis

Damit SSM funktioniert, muss die IP der Multicastgruppe im Bereich 232.0.0.0/8 liegen.



1. Die Multicastempfänger senden eine IP-IGMP-Join-Anforderung, die angibt, dass die Empfänger der Multicastgruppe beitreten und den Multicast-Stream von der Quelle empfangen möchten. Der IGMP-Join enthält 2 Attribute die Multicastquelle und -gruppe (S, G). IGMP Version 3 wird für SSM auf der Multicastquelle und der Empfänger verwendet, um einige INCLUDE-spezifische Quelladressen weiterzuleiten. SSM ermöglicht es den Empfängern, Streams von bestimmten Multicast-Servern explizit zu empfangen, deren Quelladresse explizit von den Empfängern als Teil der JOIN-Anfrage bereitgestellt wird. In diesem Beispiel wird eine IGMP v3-Join-Anforderung mit einer expliziten Include-Quellliste ausgelöst, die die Quelle 172.9.9.2 enthält, um die Adresse zu sein, die den Multicast-Stream über die Gruppe 232.1.1.1 sendet.
2. Das Citrix SD-WAN in der Zweigstelle hört alle IGMP-Anforderungen von diesen Empfängern ab und konvertiert sie in einen Mitgliedschaftsbericht und sendet ihn über den virtuellen Pfad an die SD-WAN-Appliance im Rechenzentrum.
3. Die Citrix SD-WAN Appliance im Rechenzentrum empfängt den Mitgliedschaftsbericht über den virtuellen Pfad und leitet ihn an die Multicastquelle weiter, um einen Kontrollkanal zu erstellen.

4. Die Multicastquelle überträgt den Multicast-Stream über den virtuellen Pfad an die Multicastempfänger.

Der Datenverkehr des Kontrollkanals und der Multicast-Stream fließen durch den etablierten virtuellen Pfad zwischen der Zweigstelle und dem Rechenzentrum. Der Citrix SD-WAN Overlay-Pfad sichert und isoliert Multicast-Datenverkehr vor WAN-Verschlechterung oder Link-Brownouts.

Konfigurieren von Multicast

Um Multicast zu konfigurieren, führen Sie die folgenden Schritte auf der SD-WAN-Appliance sowohl an der Quelle als auch am Ziel aus.

1. Multicastgruppe erstellen - Geben Sie einen Namen und eine IP-Adresse für die Multicastgruppe an. Die IP der Multicastgruppe muss im Bereich 232.0.0.0/8 für quellspezifisches Multicast liegen.
2. IGMP-Proxy aktivieren —Sie können die Citrix SD-WAN Appliance als IGMP-Proxy konfigurieren, um die IGMP-Kontrollkanalinformationen für Multicast-Routing zu übertragen. IGMP V3 ist für Single-Source-Multicast erforderlich.
3. Definieren der Upstream- und Downstream-Dienste - Eine Upstream-Schnittstelle ermöglicht es dem IGMP PROXY, eine Verbindung mit der SD-WAN-Appliance herzustellen, die näher an der eigentlichen Multicastquelle liegt, die den Datenverkehr streamt. Eine Downstream-Schnittstelle ermöglicht es dem IGMP-Proxy, eine Verbindung zu den Hosts herzustellen, die weiter von der eigentlichen Multicastquelle entfernt sind, die den Datenverkehr streamt. Die Upstream- und Downstream-Dienste unterscheiden sich für die Appliance an der Quelle und die Appliance am Zielort

Um Multicast auf der Citrix SD-WAN SD-WAN-Appliance zu konfigurieren, navigieren Sie zu **Verbindungen > Multicastgruppen**. Erstellen Sie eine Multicast-Gruppe, indem Sie einen Namen und eine IP-Adresse für die Multicast-Gruppe angeben. Klicken Sie auf **IGMP-Proxy aktivieren**.

Multicast Groups: Grp2 Section: Basic Settings

+ Group

Group

?

Group Name:
Grp2

Multicast Group IP:
232.1.1.1

☒ Enable IGMP Proxy

Apply

Revert

Konfigurieren Sie die Upstream- und Downstream-Pfade für die Zweigstellen- und Rechenzentrumsgeräte.

Für die Appliance, die näher am Multicast-Empfänger (Branch) ist, empfängt die Appliance den Multicast-Verkehr auf dem Virtual Path Interface und sendet den Datenverkehr auf der lokalen Schnittstelle an den Empfänger.

Multicast Groups: Grp2 Section: Service

+ Group

Group

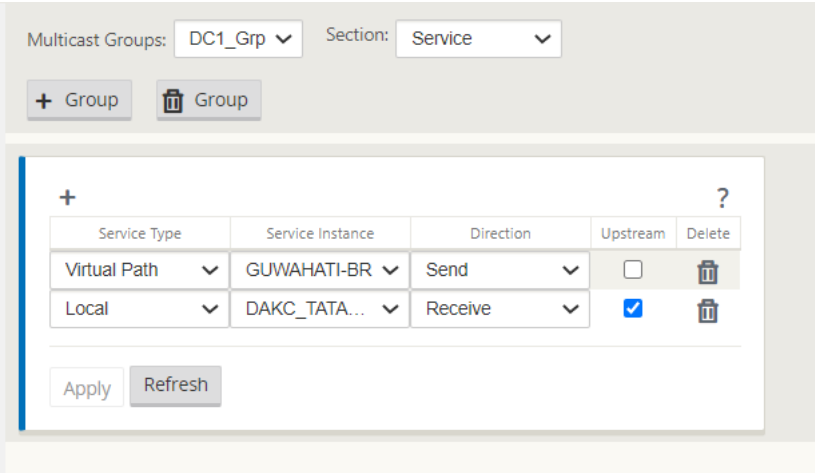
+ ?

| Service Type | Service Instance | Direction | Upstream | Delete |
|--------------|------------------|-----------|-------------------------------------|-------------|
| Virtual Path | BANGALOR... | Receive | <input checked="" type="checkbox"/> | <div></div> |
| Local | DAKC_Airtel... | Send | <input type="checkbox"/> | <div></div> |

Apply

Refresh

Für die Appliance, die näher an der Multicast-Quelle (Rechenzentrum) liegt, empfängt die Appliance den Multicast-Verkehr auf der lokalen Schnittstelle und sendet den Datenverkehr auf der virtuellen Pfadschnittstelle.



Überwachen

IGMP-Statistik

Wenn die Multicast-Empfänger eine Join-Gruppenanforderung initiieren, können Sie die Details des Empfängers unter **Überwachung > IGMP** auf der Appliance anzeigen. Sie können diese Informationen auf den Appliances sowohl an der Quelle als auch am Ziel sehen.

Die folgende Abbildung zeigt, dass ein IGMP Version 3-Join initiiert wird und der Filtertyp INCLUDE verwendet wird, um bestimmte Quelladressen einzuschließen. Sie können auch die IGMP-Mitgliederstatistiken sehen.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > IGMP

Filter/Purge

Refresh

Purge IGMP Group

Purge IGMP Stats

IGMP PROXY Groups

Max Groups to Display: 50

Service Type to Display:

Refresh

| Type | Name | Group | Filter | Version | Packets Sent | Bytes Sent |
|------|----------------|-----------|---------|---------|--------------|------------|
| HOST | VIF-1-Bridge-1 | 232.1.1.1 | INCLUDE | IGMPv3 | 4285 | 6418930 |

Total Groups Displayed: 1 out of 1

IGMP Stats

Max IGMP Stats to Display: 50

Stats Type to Display: MEMBER

Refresh

| Type | Description | Value |
|--------|----------------|-------|
| MEMBER | Add Member | 1 |
| MEMBER | Remove Member | 0 |
| MEMBER | Current Member | 1 |

Total IGMP Stats Displayed: 3 out of 70

Routenkosten für virtuelle Pfade konfigurieren

May 10, 2021

Citrix SD-WAN unterstützt die folgenden Routingverbesserungen im Zusammenhang mit der Verwaltung von Rechenzentren.

Betrachten Sie beispielsweise das SD-WAN-Netzwerk mit zwei Rechenzentren: eines in Nordamerika und eines in Europa. Sie möchten, dass alle Standorte in Nordamerika Datenverkehr durch das Rechenzentrum in Nordamerika weiterleiten und alle Standorte in Europa das europäische Rechenzentrum nutzen. Bisher wurde in SD-WAN 9.3 und früheren Versionen diese Funktionalität der Verwaltung des Rechenzentrums nicht unterstützt. Dies wird mit der Einführung der virtuellen Pfadroute Kosten implementiert.

- Kosten für virtuelle Pfadroute: Sie können die Kosten für virtuelle Pfade für einzelne virtuelle

Pfade konfigurieren, die zu den Routenkosten hinzugefügt werden, wenn eine Route von einem Remotestandort erlernt wird.

Mit dieser Funktion werden die Kosten für die WAN-zu-WAN-Weiterleitung ungültigen oder gelöscht.

- OSPF-Routenkosten: Sie können jetzt OSPF-Routenkosten (Typ-1-Metrik) importieren, indem **Sie OSPF-Routenkosten kopieren** in den Importfiltern aktivieren. OSPF Routenkosten werden bei der Routenauswahl anstelle der SD-WAN-Kosten berücksichtigt. Kosten bis zu 65534 statt 15 werden unterstützt. Es ist jedoch ratsam, eine geeignete virtuelle Pfadroute Kosten zu berücksichtigen, die hinzugefügt werden, wenn die Route von einem entfernten Standort gelernt wird.
- BGP - VP-Kosten nach MED: Sie können nun die Kosten für virtuelle Pfade für SD-WAN-Routen in BGP-MED-Werte kopieren, wenn Sie SD-WAN-Routen in BGP-Peers exportieren (umverteilen). Dies kann für einzelne Nachbarn festgelegt werden, indem eine BGP-Richtlinie erstellt und sie in der Richtung "OUT" für jeden Nachbarn angewendet wird.
- Jeder Standort kann mehrere virtuelle Pfade zu anderen Sites haben. Wenn es einen Zweig gibt, zu dem Verbindungen zu Diensten über mehr virtuelle Pfade besteht, kann es manchmal zwei virtuelle Pfade vom Zweigstandort geben. Ein virtueller Pfad über DC1 und der andere über DC2. DC1 kann ein MCN sein und DC2 kann ein Geo-MCN sein und kann als ein anderer Standort mit statischem virtuellem Pfad konfiguriert werden.
- Fügen Sie Standardkosten für jeden VP als 1 hinzu. Die Kosten für virtuelle Pfadroute helfen dabei, jedem virtuellen Pfad eines Standorts Kosten zuzuordnen. Dies hilft, Routenaustausch/Aktualisierungen über einen bestimmten virtuellen Pfad anstelle der Standardstandortkosten zu manipulieren. Damit können wir manipulieren, welches Rechenzentrum für den Versand des Datenverkehrs bevorzugt wird.
- Erlauben Sie die Konfiguration der Kosten innerhalb eines kleinen Wertebereichs (z. B. 1—10) für jeden VP.
- Kosten für virtuelle Pfade müssen jeder Route hinzugefügt werden, die mit Nachbarstandorten gemeinsam genutzt werden, um die Routing-Voreinstellung anzugeben, einschließlich Routen, die über dynamisches Routing gelernt wurden
- Kein statischer virtueller Pfad darf geringere Kosten aufweisen als ein dynamischer virtueller Pfad.

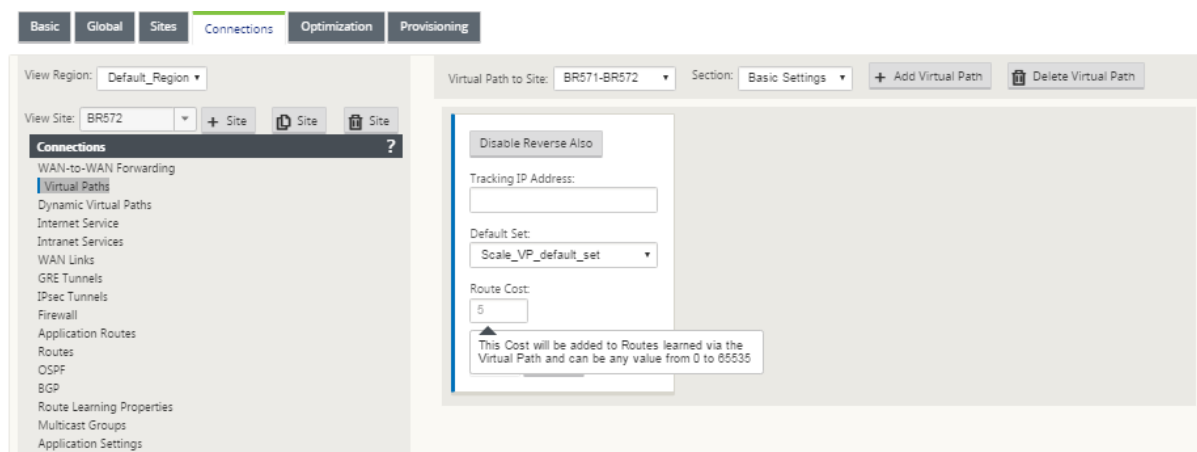
Hinweis

VP Routenkosten veraltet die WAN-zu-WAN-Weiterleitungskosten, die in Releaseversionen vor Version 10.0 existierten. Die Routing-Entscheidungen, die auf WAN-zu-WAN-Weiterleitungskosten basieren, müssen erneut beeinflusst werden, indem VP-Routenkosten verwendet werden, da die WAN-zu-WAN-Weiterleitungskosten bei der Migration auf Version 10.0

keine Bedeutung haben.

Konfigurieren von Routenkosten für virtuelle Pfade

Sie können Virtual Path Route in der SD-WAN GUI unter **Verbindungen** > **Region anzeigen** > **Site anzeigen** > **Virtuelle Pfade** > **Grundeinstellungen** konfigurieren. Alle Routen werden mit grundlegenden Citrix SD-WAN Kosten und VP-Routenkosten installiert, um die Routenkosten über mehrere virtuelle Pfade hinweg zu beeinflussen.



Anwendungsfall:

Beispielsweise gibt es Subnetze 172.16.2.0/24 und 172.16.3.0/24. Angenommen, es gibt zwei Rechenzentren DC1 und DC2, die beide diese Subnetze verwenden, um Datenverkehr an SD-WAN zu übertragen. Bei den Standardkosten für virtuelle Pfade können Sie das Routing nicht beeinflussen, da es davon abhängt, welche Route zuerst installiert wurde, es kann entweder zuerst DC2 oder die nächste DC1 sein.

Mit virtuellem Pfad können Sie speziell den virtuellen DC2-Pfad beeinflussen, um höhere Kosten für virtuelle Pfade zu haben (z. B. 10), während DC1 die standardmäßigen VP-Routenkosten von 5 aufweist. Diese Manipulation hilft, Routen mit DC1 zuerst und DC2 weiter für beide zu installieren.

Sie können vier Routen haben, zwei Routen bis 172.16.2.0/24; eine über DC1 mit niedrigeren Kosten und dann über DC2 mit höheren Kosten und 2 weitere für 172.16.3.0/24.

Überwachung und Fehlerbehebung

In der Routingtabelle wird angezeigt, wie dieselben Subnetze, die von zwei Standorten angekündigt werden, die über den virtuellen Pfad mit einem Zweigstandort verbunden sind, mit dem Kostenanteil virtueller Pfadrouten installiert werden.

Um die Routenkosten und die in der Routing-Tabelle verwendeten Routen zu überprüfen, navigieren Sie zu **Überwachung > Statistiken**. Wählen Sie unter dem Feld **Anzeigen** die Option **Routen** aus. Routenkosten und Trefferzählungen können auf derselben Seite überprüft werden.

Die folgende Abbildung zeigt die Routing-Tabelle mit zwei unterschiedlichen Kosten für dieselbe Route, die 172.16.6.0/24 mit Kosten 10 und 11 für die Dienste **DC-Branch01** bzw. **GEOMCN-Branch01** beträgt.

Monitoring > Statistics

Statistics

Show: **Routes** ☐ Enable Auto Refresh **5** seconds **Refresh** ☒ Clear Counters on Refresh

Routing Domain: **<ALL>** **Purge dynamic routes**

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain: Default_RoutingDomain

Filter: in **Any column** **Apply**

Show **100** entries Showing 1 to 18 of 18 entries **First** **Previous** **1**

| Details | Num | Network Addr | Gateway IP Address | Service | Firewall Zone | Reachable | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type |
|--------------------------|-----|----------------|--------------------|-----------------|------------------|-----------|----------|---------|-------------|-----------------|------|-----------|----------|------------------|
| <input type="checkbox"/> | 0 | 172.16.60.0/24 | * | Local | Default_LAN_Zone | YES | Branch01 | Static | - | - | 5 | 0 | YES | N/A |
| <input type="checkbox"/> | 1 | 172.16.61.0/24 | * | Local | Default_LAN_Zone | YES | Branch01 | Static | - | - | 5 | 0 | YES | N/A |
| <input type="checkbox"/> | 2 | 172.16.41.0/24 | * | DC-Branch01 | Default_LAN_Zone | YES | DC | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A |
| <input type="checkbox"/> | 3 | 172.16.40.0/24 | * | DC-Branch01 | Default_LAN_Zone | YES | DC | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A |
| <input type="checkbox"/> | 4 | 172.16.6.0/24 | * | DC-Branch01 | Default_LAN_Zone | YES | DC | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A |
| <input type="checkbox"/> | 5 | 172.16.4.0/24 | * | DC-Branch01 | Default_LAN_Zone | YES | DC | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A |
| <input type="checkbox"/> | 6 | 172.16.3.0/24 | * | DC-Branch01 | Default_LAN_Zone | YES | DC | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A |
| <input type="checkbox"/> | 7 | 172.16.2.0/24 | * | DC-Branch01 | Default_LAN_Zone | YES | DC | Dynamic | Virtual WAN | YES | 10 | 0 | YES | N/A |
| <input type="checkbox"/> | 8 | 172.16.51.0/24 | * | GeoMCN-Branch01 | Default_LAN_Zone | YES | GeoMCN | Dynamic | Virtual WAN | YES | 11 | 0 | YES | N/A |
| <input type="checkbox"/> | 9 | 172.16.50.0/24 | * | GeoMCN-Branch01 | Default_LAN_Zone | YES | GeoMCN | Dynamic | Virtual WAN | YES | 11 | 0 | YES | N/A |
| <input type="checkbox"/> | 10 | 172.16.6.0/24 | * | GeoMCN-Branch01 | Default_LAN_Zone | YES | GeoMCN | Dynamic | Virtual WAN | YES | 11 | 0 | YES | N/A |
| <input type="checkbox"/> | 11 | 172.16.4.0/24 | * | GeoMCN-Branch01 | Default_LAN_Zone | YES | GeoMCN | Dynamic | Virtual WAN | YES | 11 | 0 | YES | N/A |

Konfigurieren des Virtual Router-Redundanzprotokolls

May 10, 2021

Virtual Router Redundancy Protocol (VRRP) ist ein weit verbreitetes Protokoll, das Device Redundanz bereitstellt, um den Single Point of Failure in der statischen Standardumgebung zu eliminieren. VRRP ermöglicht es Ihnen, zwei oder mehr Router zu konfigurieren, um eine Gruppe zu bilden. Diese Gruppe wird als einzelnes Standard-Gateway mit einer virtuellen IP-Adresse und einer virtuellen MAC-Adresse angezeigt.

Ein Backup-Router übernimmt automatisch, wenn der primäre /Master-Router ausfällt. In einer VRRP-Einrichtung sendet der Master-Router ein VRRP-Paket, das als Ankündigung bezeichnet wird,

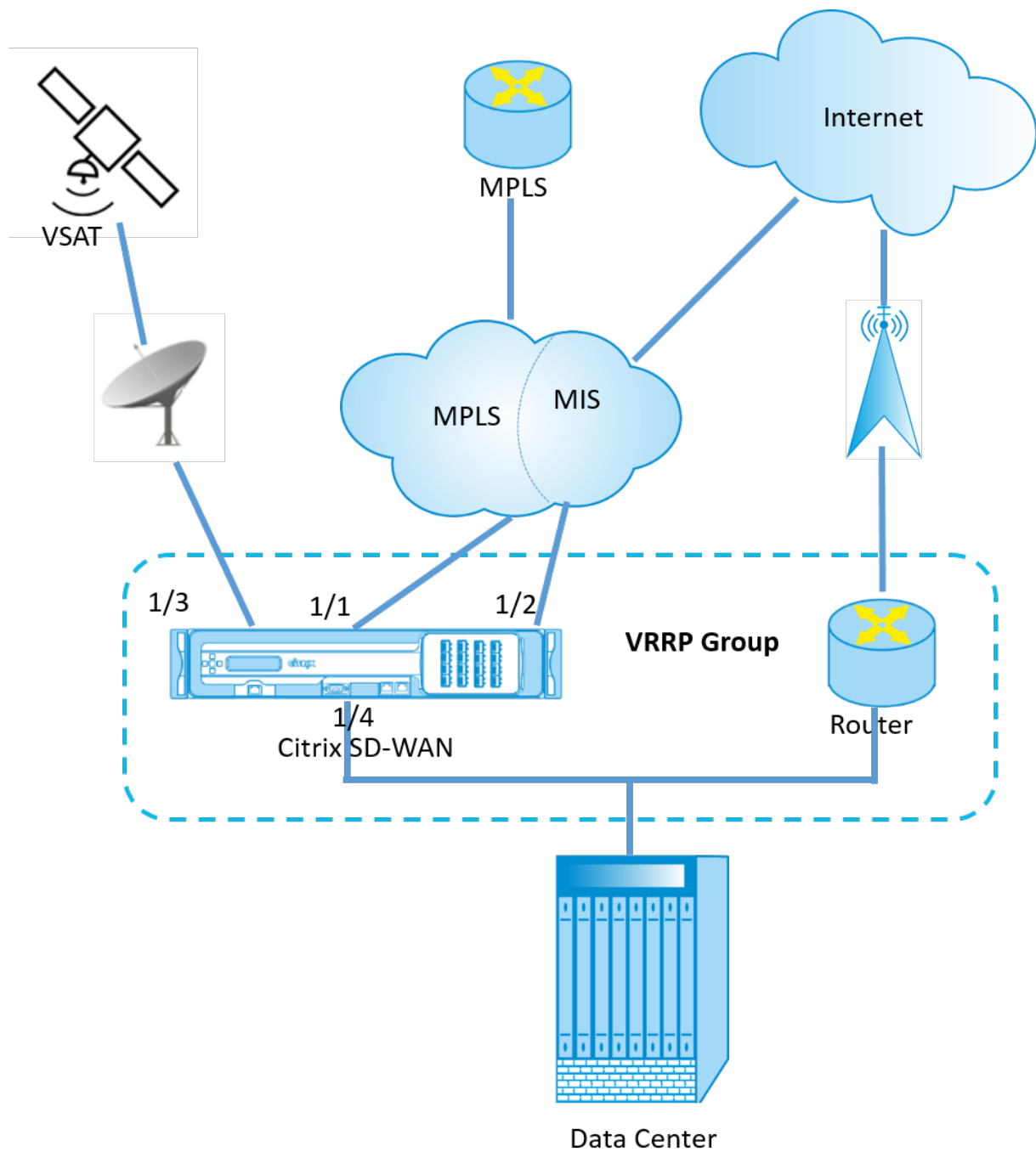
an die Backup-Router. Wenn der Master-Router die Ankündigung nicht mehr sendet, setzt der Backup-Router den Intervall-Timer ein. Wenn innerhalb dieses Haltezeitraums keine Ankündigung empfangen wird, initiiert der Backup-Router die Failover-Routine.

VRRP gibt einen Wahlprozess an, bei dem der Router mit der höchsten Priorität zum Master wird. Wenn die Priorität unter den Routern gleich ist, wird der Router mit der höchsten IP-Adresse zum Master. Die anderen Router befinden sich im Backup-Zustand. Der Wahlprozess wird erneut gestartet, wenn der Master fehlschlägt, ein neuer Router der Gruppe beitrifft oder ein vorhandener Router die Gruppe verlässt.

VRRP stellt einen Standardpfad für hohe Verfügbarkeit sicher, ohne dynamische Routing- oder Router-erkennungsprotokolle auf jedem Endhost zu konfigurieren.

Citrix SD-WAN Version 10.1 unterstützt VRRP Version 2 und Version 3, um mit Routern von Drittanbietern zu arbeiten. Die SD-WAN-Appliance fungiert als Master-Router und leitet den Datenverkehr an, den Virtual Path Service zwischen Standorten zu verwenden. Sie können die SD-WAN-Appliance als VRRP-Master konfigurieren, indem Sie die Virtual Interface IP als VRRP-IP konfigurieren und die Priorität manuell auf einen höheren Wert als die Peer-Router festlegen. Sie können das Ankündigungsintervall und die Präempt-Option konfigurieren.

Das folgende Netzwerkdiagramm zeigt eine Citrix SD-WAN Appliance und einen Router, der als VRRP-Gruppe konfiguriert ist. Die SD-WAN-Appliance ist als Master konfiguriert. Wenn die SD-WAN-Appliance ausfällt, übernimmt der Backup-Router innerhalb von Millisekunden und stellt sicher, dass keine Ausfallzeiten vorliegen.



So konfigurieren Sie die VRRP-Instanz:

1. Navigieren Sie im Konfigurations-Editor zu **Sites > Site-Name > VRRP**, und klicken Sie auf **+**.

| + | VRRP Group ID | Version | Priority | Advertisement Interval | Authentication type | Authentication text | Reclaim | Use Check |
|-------------------------|---------------|---------|----------|------------------------|---------------------|---------------------|-------------------------------------|-------------------------------------|
| + | 245 | V3 | 255 | 1000 | * | None | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <div>Apply Revert</div> | | | | | | | | |

1. Konfigurieren Sie eine VRRP-Instanz. Geben Sie die Werte für die folgenden Felder ein:

- **VRRP-Gruppen-ID:** Die VRRP-Gruppen-ID. Die Gruppen-ID muss ein Wertebereich von 1—255 sein. Die gleiche Gruppen-ID muss auch auf den Backup-Routern konfiguriert werden.

Hinweis

Derzeit können Sie nur bis zu vier Gruppen konfigurieren.

- **Version:** Die Version des VRRP-Protokolls. Sie können zwischen VRRP-Protokoll V2 und V3 wählen.
- **Priorität:** Die Priorität der Citrix SD-WAN Appliance für die VRRP-Gruppe. Der Prioritätsbereich beträgt 1 —254. Setzen Sie diesen Wert auf maximal (254), damit die SD-WAN-Appliance zum Master wird.

Hinweis

Wenn der Router Eigentümer der VRRP-IP-Adresse ist, ist die Priorität standardmäßig auf 255 festgelegt.

- **Anzeige Interval:** Die Häufigkeit in Millisekunden, mit der die VRRP-Anzeigen gesendet werden, wenn die SD-WAN-Appliance der Master ist. Das standardmäßige Anzeigenintervall beträgt eine Sekunde.
- **Authentifizierungstyp:** Sie können **Nur-Text** wählen, um eine Authentifizierungszeichenfolge einzugeben. Die Authentifizierungszeichenfolge wird als Klartext ohne Verschlüsselung in den VRRP-Anzeigen gesendet. Wählen Sie **Keine**, wenn Sie die Authentifizierung nicht einrichten möchten.
- **Authentifizierungstext:** Die Authentifizierungszeichenfolge, die in der VRRP-Ankündigung gesendet werden soll. Diese Option ist aktiviert, wenn der **Authentifizierungstyp Nur-Text** ist.

Hinweis

Die Authentifizierung wird nur in VRRPv2 unterstützt.

- **Rückgewinnung:** ermöglicht die Präemption, wenn die Priorität der SD-WAN-Appliance in der VRRP-Gruppe am höchsten ist. Dies wird im VRRP-Wahlprozess verwendet.
- **V2-Prüfsumme verwenden:** Aktiviert die Kompatibilität mit Netzwerkgeräten von Drittanbietern für VRRPv3. Standardmäßig verwendet VRRPv3 die Prüfsummenberechnungsmethode v3. Bestimmte Geräte von Drittanbietern unterstützen möglicherweise nur die VRRPv2-Prüfsummenberechnung. Aktivieren Sie in solchen Fällen diese Option.

Konfigurieren Sie die VRRP-IP-Adresse. Geben Sie Werte für die folgenden Felder ein, und klicken Sie auf **Anwenden**.

- **Virtuelle Schnittstelle:** Die virtuelle Schnittstelle, die für VRRP verwendet werden soll. Wählen Sie eine der konfigurierten virtuellen Schnittstellen aus.
- **Virtuelle IP-Adresse:** Die virtuelle IP-Adresse, die der virtuellen Schnittstelle zugewiesen wurde. Wählen Sie eine der konfigurierten virtuellen IP-Adressen für die virtuelle Schnittstelle aus.
- **VRRP Router IP:** Die IP-Adresse des virtuellen Routers für die VRRP-Gruppe. Standardmäßig wird die virtuelle IP-Adresse der SD-WAN-Appliance als virtuelle Router-IP-Adresse zugewiesen.

| VRRP Group ID | Version | Priority | Advertisement Interval | Authentication type | Authentication text | Reclaim | Use V2 Checksum |
|---------------|---------|----------|------------------------|---------------------|---------------------|-------------------------------------|-------------------------------------|
| 245 | V3 | 255 | 1000 | None | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

| Virtual Interface | Virtual IP Address | VRRP Router IP | Delete |
|--------------------|--------------------|----------------|--------|
| VirtualInterface-1 | 172.16.2.100/24 | 172.16.2.100 | |

Apply Revert

VRRP-Statistik

Sie können die VRRP-Statistiken unter **Überwachung > VRRP-Protokoll** anzeigen.

| VRRP ID | Version | Interface(s) | State | Priority | Virtual Router IP | Advertisement Interval | Enable | Disable |
|---------|---------|--------------|--------|----------|-------------------|------------------------|---------------------------------------|--|
| 20 | 2 | LAN-7 | Master | 250 | 172.58.7.100 | 2000 | <input type="button" value="Enable"/> | <input type="button" value="Disable"/> |
| 245 | 3 | LAN | Master | 200 | 172.58.5.20 | 1000 | <input type="button" value="Enable"/> | <input type="button" value="Disable"/> |

Sie können die folgenden Statistikdaten anzeigen:

- **VRRP-ID:** Die VRRP-Gruppen-ID
- **Version:** Die VRRP-Protokollversion.
- **Schnittstelle:** Die virtuelle Schnittstelle, die für VRRP verwendet wird.
- **Status:** Der VRRP-Status der SD-WAN-Einheit. Es gibt an, ob es sich bei der Appliance um einen Master oder eine Sicherung handelt.
- **Priorität:** Die Priorität der SD-WAN-Appliance für eine VRRP-Gruppe
- **Virtueller Router IP:** Die IP-Adresse des virtuellen Routers für die VRRP-Gruppe.
- **Anzeigenintervall:** Die Häufigkeit von VRRP-Anzeigen.

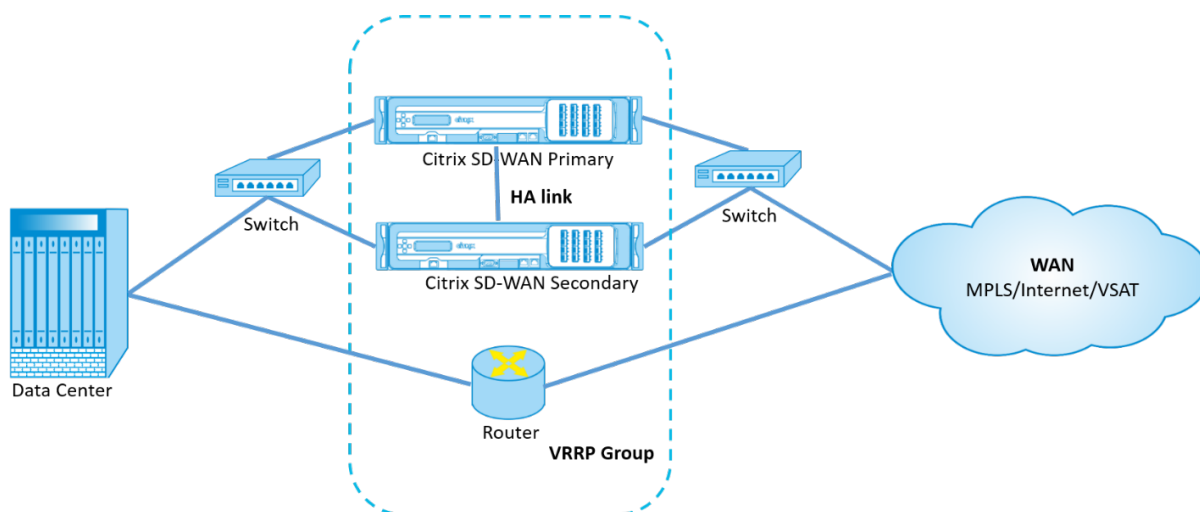
- **Aktivieren:** Wählen Sie diese Option, um die VRRP-Instanz auf der SD-WAN-Appliance zu aktivieren.
- **Deaktivieren:** Wählen Sie diese Option, um die VRRP-Instanz auf der SD-WAN-Appliance zu deaktivieren.

Einschränkungen

- VRRP wird nur in der Gatewaymodus-Bereitstellung unterstützt.
- Sie können bis zu vier VRRP-IDs (VRID) konfigurieren.
- Bis zu 16 virtuelle Netzwerkschnittstellen können an VRID teilnehmen.

Hochverfügbarkeit und VRRP

Sie können Netzwerkausfallzeiten und Verkehrsunterbrechungen erheblich reduzieren, indem Sie sowohl die Hochverfügbarkeits- als auch VRRP-Funktionen in Ihrem SD-WAN-Netzwerk nutzen. Stellen Sie ein Paar Citrix SD-WAN Appliance in Aktiv/Standby-Rollen zusammen mit einem Standby-Router zur VRRP-Gruppe bereit. Diese Gruppe wird als einzelnes Standard-Gateway mit einer virtuellen IP-Adresse und einer virtuellen MAC-Adresse angezeigt.



Im Folgenden sind 2 Fälle mit der obigen Bereitstellung aufgeführt:

1. Fall: Hochverfügbarkeits-Failover-Timer auf SD-WAN entspricht dem VRRP-Failover-Timer.

Das erwartete Verhalten ist ein Switchover mit hoher Verfügbarkeit, der vor dem VRRP-Switchover stattfindet, d. h. der Datenverkehr fließt weiter durch die neue Active SD-WAN-Appliance. In diesem Fall setzt SD-WAN mit der VRRP-Master-Rolle fort.

2. Fall: Hochverfügbarkeits-Failover-Timer auf SD-WAN größer als der VRRP-Failover-Timer.

Das erwartete Verhalten ist die VRRP-Umstellung auf den Router geschieht, das heißt, der Router wird VRRP-Master und Datenverkehr möglicherweise vorübergehend durch den Router fließen, unter Umgehung der SD-WAN-Appliance.

Aber sobald der Hochverfügbarkeits-Switchover passiert, wird SD-WAN wieder zu VRRP Master, d. h. der Datenverkehr fließt jetzt durch die neue aktive SD-WAN-Appliance.

Weitere Informationen zu Bereitstellungsmodi für Hochverfügbarkeit finden Sie unter [Hohe Verfügbarkeit](#).

Konfigurieren von Netzwerkobjekten

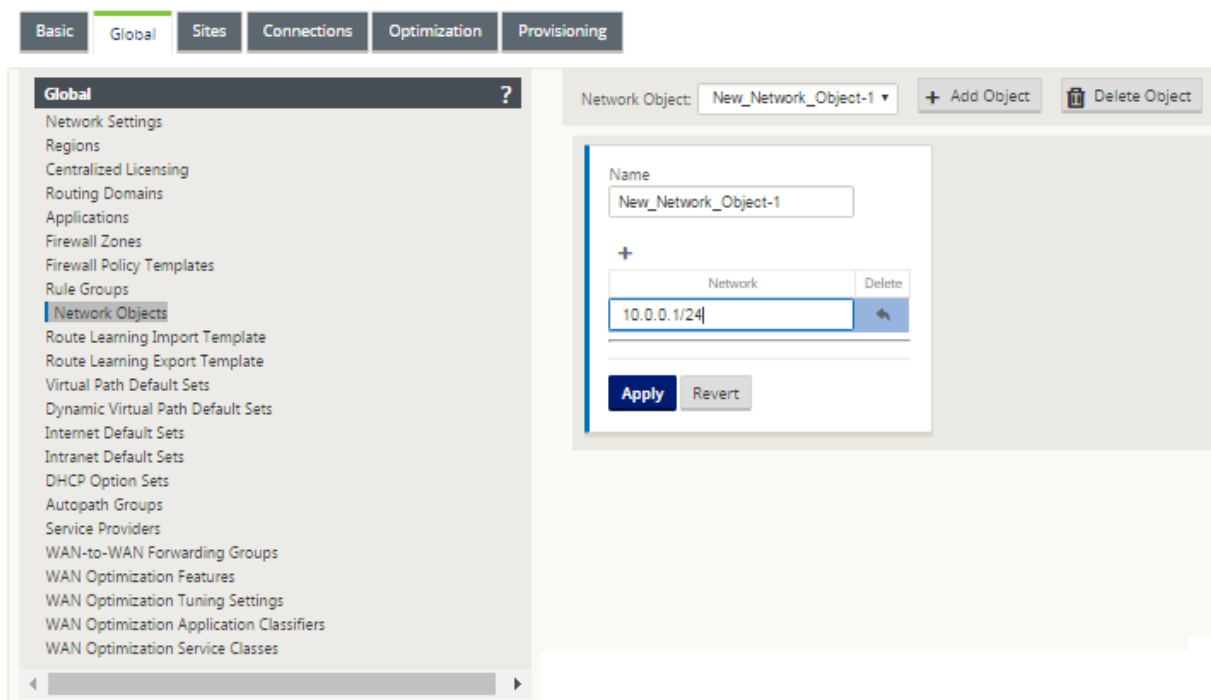
May 10, 2021

Citrix SD-WAN führt die Option ein, Netzwerkobjekte im Bereich **Global** im Konfigurationseditor hinzuzufügen. Sie können mehrere Subnetze zusammenfassen und auf ein einzelnes Netzwerkobjekt verweisen, wenn Sie einen Routenfilter definieren, anstatt für jedes Subnetz einen Filter zu erstellen.

So konfigurieren Sie Netzwerkobjekte:

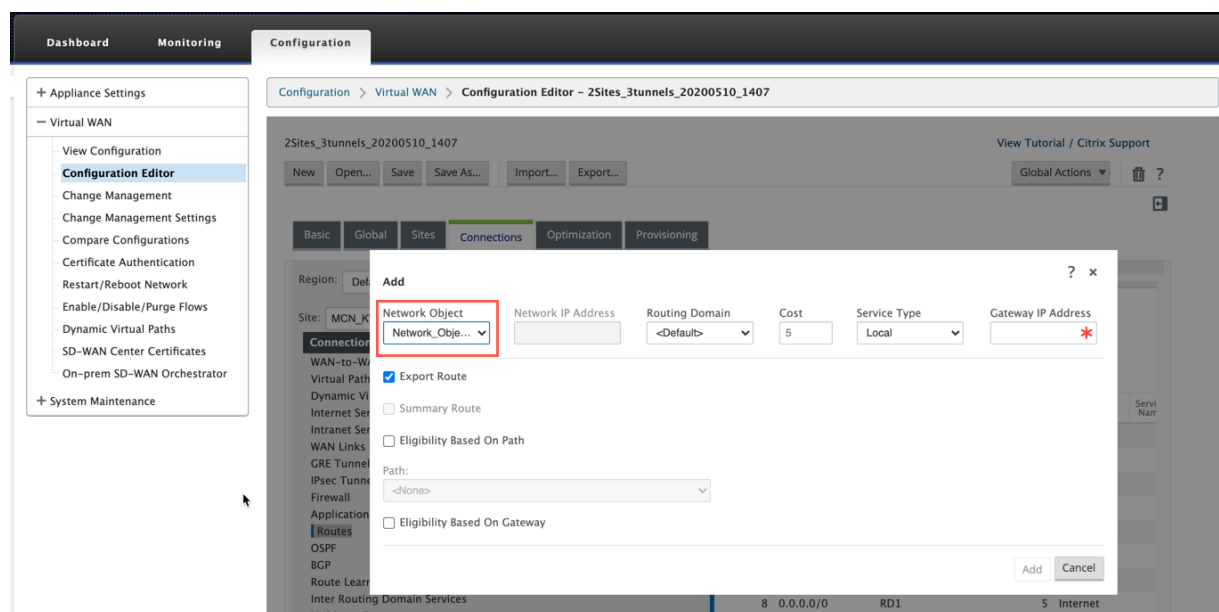
1. Navigieren Sie im **Konfigurations-Editor** zu **Global** > **Netzwerkobjekte**, klicken Sie auf **Hinzufügen (+)**.
2. Klicken Sie unter Netzwerke auf **Hinzufügen (+)**.
3. Geben Sie die **IP-Adresse** und das **Subnetz** des neuen Netzwerkobjekts ein.
4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Um den Namen des Netzwerkobjekts zu bearbeiten, klicken Sie auf den Namen des Netzwerkobjekts und geben einen neuen Namen ein.

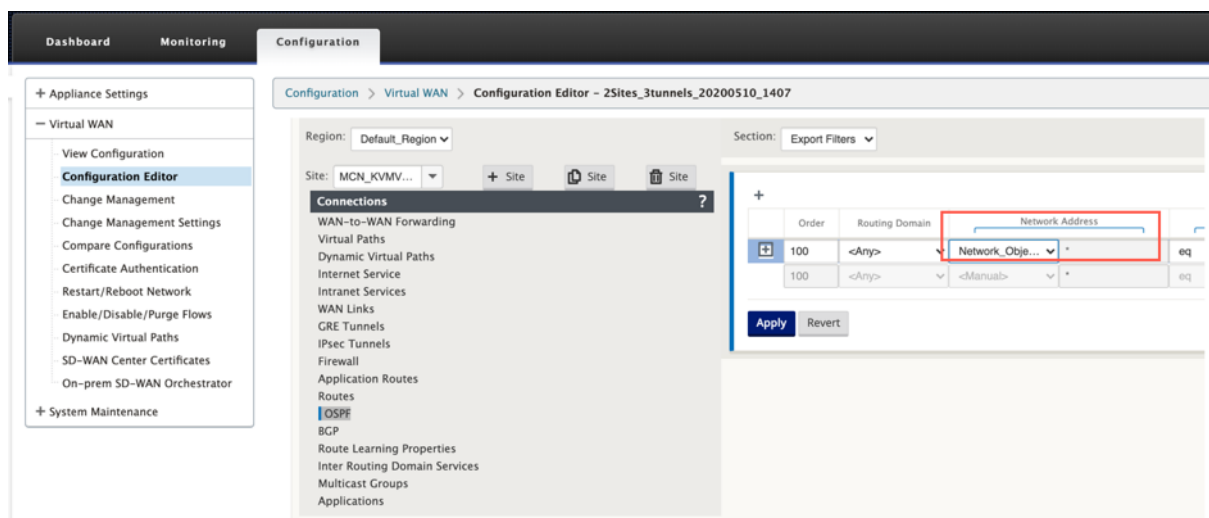


Folgende Funktionen nutzen die Netzwerkobjekte:

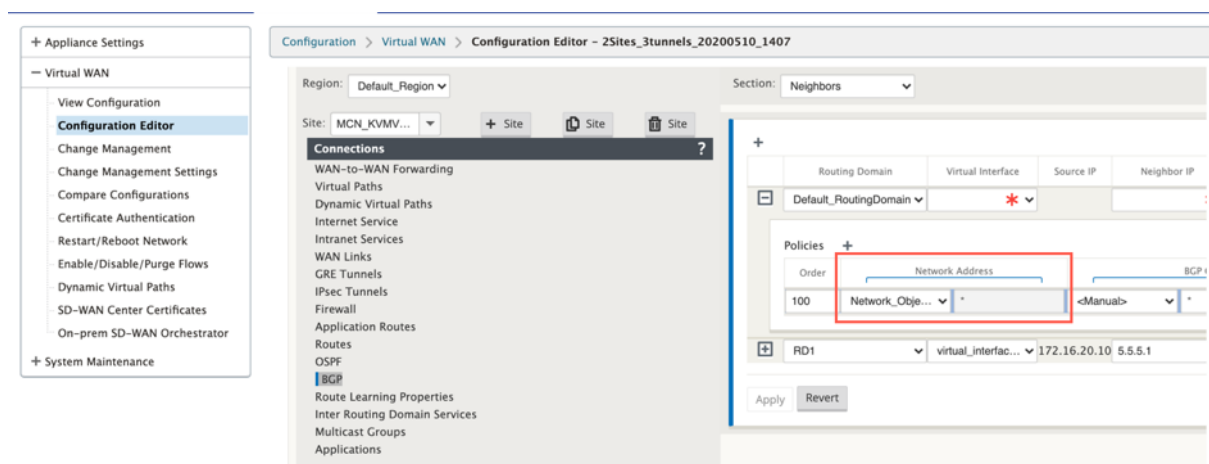
- Routen (**Konfigurations-Editor > Verbindungen > Routen > Klick+**Netzwerkobjekt****)



- BGP- und OSPF-Import- und Exportfilter (**Konfigurations-Editor > Verbindungen > BGP/OSPF > Filter exportieren/importieren click + > Netzwerkadresse**)



- BGP-Nachbar-Richtlinien (**Konfigurations-Editor > Verbindungen > BGP > Nachbarn > Richtlinien** click + > **Netzwerkadresse**)



Routing-Unterstützung für die LAN-Segmentierung

May 10, 2021

Die SD-WAN Standard und Premium (Enterprise) Edition-Appliances implementieren die LAN-Segmentierung an verschiedenen Standorten, an denen eine Appliance bereitgestellt wird. Die Appliances erkennen und pflegen eine Aufzeichnung der verfügbaren LAN-seitigen VLANs und konfigurieren Regeln, mit denen andere LAN-Segmente (VLANs) an einem Remote-Standort mit einer anderen SD-WAN Standard- oder Premium (Enterprise) Edition-Appliance verbunden werden können.

Die obige Funktion wird mithilfe einer VRF-Tabelle (Virtual Routing and Forwarding) implementiert,

die in der SD-WAN Standard oder Premium (Enterprise) Edition-Appliance verwaltet wird. Die Überwachung der Remote-IP-Adressbereiche, auf die ein lokales LAN-Segment zugreifen kann. Dieser VLAN-zu-VLAN-Datenverkehr würde weiterhin das WAN durch denselben vordefinierten virtuellen Pfad zwischen den beiden Appliances durchlaufen (es müssen keine neuen Pfade erstellt werden).

Ein Beispiel für diese Funktionalität ist, dass ein WAN-Administrator möglicherweise in der Lage ist, lokale Zweignetzwerkumgebung über ein VLAN zu segmentieren und einige dieser Segmente (VLANs) Zugriff auf DC-seitige LAN-Segmente bereitzustellen, die Zugriff auf das Internet haben, während andere diesen Zugriff möglicherweise nicht erhalten. Die Konfiguration der VLAN-zu-VLAN-Zuordnungen erfolgt über den Konfigurations-Editor des MCN in der SD-WAN-Management-Weboberfläche.

Domänenendienst für den übergreifenden Routing

May 10, 2021

Mit Citrix SD-WAN können Sie das Netzwerk mithilfe von Routingdomänen segmentieren, was eine hohe Sicherheit und eine einfache Verwaltung gewährleistet. Mit der Routingdomäne wird der Datenverkehr im Overlay-Netzwerk voneinander isoliert. Jede Routingdomäne verwaltet ihre eigene Routingtabelle. Weitere Informationen zur Routingdomäne finden Sie unter [Routingdomäne](#).

Manchmal müssen wir jedoch den Datenverkehr zwischen den Routing-Domänen weiterleiten. Beispielsweise wenn freigegebene Dienste wie Drucker, Scanner und Mailserver als separate Routingdomäne bereitgestellt werden. Inter-Routingdomäne ist erforderlich, damit Benutzer aus verschiedenen Routingdomänen auf die gemeinsam genutzten Dienste zugreifen können.

Citrix SD-WAN bietet Static Inter-Routing-Domänenendienst, der das Routenlecken zwischen Routingdomänen innerhalb eines Standorts oder zwischen verschiedenen Standorten ermöglicht. Dadurch entfällt die Notwendigkeit, dass ein Edgerouter Routeleaking verarbeitet. Der Domänendienst "Inter-Routings" kann außerdem zum Einrichten von Routen, Firewall-Richtlinien und NAT-Regeln verwendet werden.

Eine neue Firewall-Zone, **Inter_Routing_Domain_Zone**, wird standardmäßig erstellt und dient als Firewall-Zone für die Inter-Routing Domain Services für Routing und Filterung.

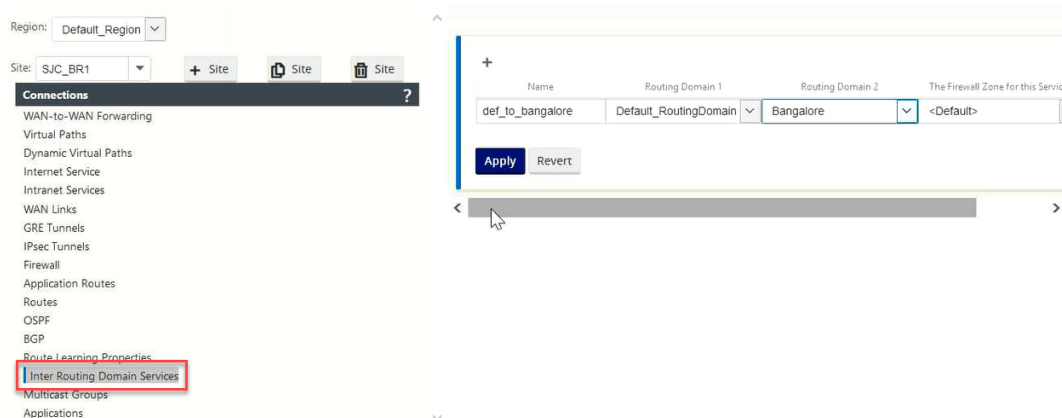
Hinweis

Citrix SD-WAN PE-Appliances führen keine WAN-Optimierungsfunktionen für Inter-Routing-Domänenpakete durch.

So konfigurieren Sie den Domänendienst zwischen zwei Routingdomänen.

Betrachten Sie ein SD-WAN-Netzwerk mit einem MCN und zwei oder mehr Zweigstellen, bei denen mindestens zwei Routing Domains global konfiguriert sind. Standardmäßig sind alle Routingdomänen im MCN aktiviert. Aktivieren Sie selektiv die erforderlichen Routingdomänen auf den anderen Sites. Informationen zur Konfiguration der Routingdomäne finden Sie unter [Routingdomäne konfigurieren](#).

1. Navigieren Sie im SD-WAN-Konfigurationseditor zu **Verbindungen** > Standort auswählen > **Domänendienst zwischen Routing**.
2. Klicken Sie auf **+** und geben Sie Werte für die folgenden Parameter ein:
 - **Name:** Der Name des Inter-Routing Domain-Dienstes.
 - **Routingdomäne 1:** Die erste Routingdomäne des Paares.
 - **Routingdomäne 2:** Die zweite Routingdomäne des Paares.
 - **Firewall-Zone:** Die Firewall-Zone des Dienstes.
 - Default: Die Firewallzone Inter_Routing_Domain_Zone ist zugewiesen.
 - Keine: Es wurde keine Zone ausgewählt und die ursprüngliche Zone des Pakets wird beibehalten.
 - Möglicherweise sind alle im Netzwerk konfigurierten Zonen ausgewählt.



1. Klicken Sie auf **Anwenden**, um den Domänendienst zwischen Routing zu erstellen. Der erstellte Dienst kann zum Erstellen von Routen, Firewall-Richtlinien und NAT-Richtlinien verwendet werden.

Hinweis:

Sie können einen Domänendienst zwischen Routing nicht konfigurieren, der Routingdomänen verwendet, die auf einer Site nicht aktiviert sind.

Um Routen mit dem Domänendienst zwischen Routing zu erstellen, erstellen Sie eine Route mit dem

Diensttyp als **Inter-Routing Domain Service** und wählen Sie den Inter-Routing-Domänendienst aus. Weitere Informationen zum Konfigurieren von Routen finden Sie unter [So konfigurieren Sie Routen](#).

Add

Network Object: <Manual> Network IP Address: 172.58.135.0/24 Routing Domain: Bangalore Cost: 5 Service Type: Inter Routing ... Gateway IP Address:

☒ Export Route

Inter Routing Domain Service: def_to_bang...

Add **Cancel**

Fügen Sie außerdem eine Route aus dem anderen Routingdomänenpaar hinzu, um eine Verbindung zwischen den beiden Routingdomänen herzustellen.

Sie können Firewall-Richtlinien auch konfigurieren, um den Datenverkehr zwischen Routingdomänen zu steuern. Wählen Sie in den Firewall-Richtlinien die Option Inter-Routing-Domänendienst für die Quell- und Zieldienste aus, und wählen Sie die erforderliche Firewall-Aktion aus. Informationen zum Konfigurieren von Firewall-Richtlinien finden Sie unter [Richtlinien](#).

Default_LAN_Zone Internet_Zone Untrusted_Internet_Zone

Routing Domain: Any

Traffic Match Type: IP Protocol Any DSCP: Any Match Established

Application: Application Family: Application Objects: Any

Source Service Type: Inter Routing Domain Source Service Name: def_to_bangalore Source IP: * Source Port: *

Dest Service Type: Inter Routing Domain Dest Service Name: def_to_bangalore Dest IP: * Dest Port: *

Actions

Action: Allow Drop Reject Count and Continue

☒ Allow Fragments

Connection State Tracking: Use Site Setting

☐ Log Start ☐ Log End ☐ Add Reverse Policy

Sie können auch den Intranetdiensttyp auswählen, um statische und dynamische NAT-Richtlinien zu

konfigurieren. Weitere Informationen zum Konfigurieren von NAT-Richtlinien finden Sie unter [Netzwerkadressübersetzung](#).

?

x

Add

Priority:

100

Routing Domain:

Direction:

Outbound

Type:

Port Restricted

Service Type:

Inter Routing ...

Service Name:

def_to_bang...

Inside Zone:

Any

Inside IP Address:

*

Outside IP Address:

☐ Allow Related

☐ IPsec Passthrough

☐ GRE/PPTP Passthrough

☐ Port Parity

☐ Bind Responder Route

Port Forwarding Rules +

Routing Domain

Protocol

Outside Port

Inside IP Address

Inside Port

Fragments

Log Interval (s)

Log Start

Log End

Connection State Tracking

Delete

Add

Cancel

Überwachen

Unter **Überwachung > Firewall-Statistiken > Verbindungen** können Sie Überwachungsstatistiken für Verbindungen anzeigen, die Interrouting-Domain-Dienste verwenden.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics

Connections

Maximum entries to display:

50

Filtering:

Routing Domain:

Any

Applications:

Any

Family:

Any

IP Protocol:

Any

Source Zones:

Any

Destination Zones:

Any

Source Service Types:

Any

Source Service Instances:

Any

Destination Service Types:

Any

Destination Service Instances:

Any

Source IP:

*

Source Ports:

*

Destination IP:

*

Destination Ports:

*

Refresh

Clear Connections

Help

Connections

| | | | | Source | | | | Destination | | | | Sent | | | |
|-----------------------|---|-----------------|-------------|---------------|-------|----------------------|-----------------|---------------------------|-------------|-------|----------------------|-----------------|---------------------------|-------------|--------|
| Routing Domain | Application | Family | IP Protocol | IP Address | Port | Service Type | Service Name | Zone | IP Address | Port | Service Type | Service Name | Zone | State | Is NAT |
| Default_RoutingDomain | Internet Control Message Protocol(ICMP) | Network Service | ICMP | 172.16.25.10 | 19973 | Local | VIF-2-LAN-1 | Default_LAN_Zone | 172.16.1.10 | 19973 | Inter-Routing-Domain | Default_to_MPLS | Inter_Routing_Domain_Zone | ESTABLISHED | Yes |
| RD_MPLS | Internet Control Message Protocol(ICMP) | Network Service | ICMP | 172.16.15.100 | 19973 | Inter-Routing-Domain | Default_to_MPLS | Inter_Routing_Domain_Zone | 172.16.1.10 | 19973 | Virtual Path | DC_MCN-BR3 | Default_LAN_Zone | ESTABLISHED | No |

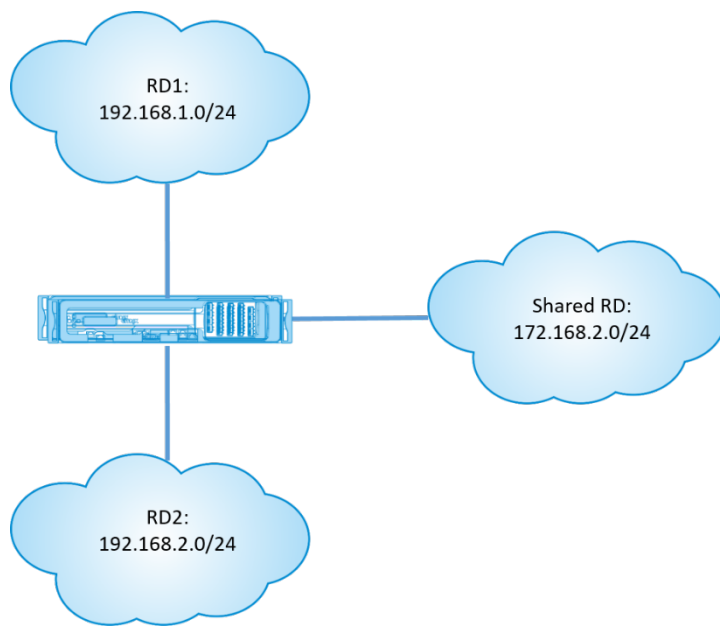
Connections Displayed: 2
Connections In Use: 2/128000

Anwendungsfall: Teilen von Ressourcen über Routingdomänen hinweg

Betrachten wir ein Szenario, in dem Benutzer in verschiedenen Routing-Domänen müssen gemeinsame Assets zugreifen, wie ein Drucker oder Netzwerkspeicher. Es gibt 3 Routingdomänen in einem Zweig RD1, RD2 und gemeinsam genutzte RD, wie in der Abbildung dargestellt.

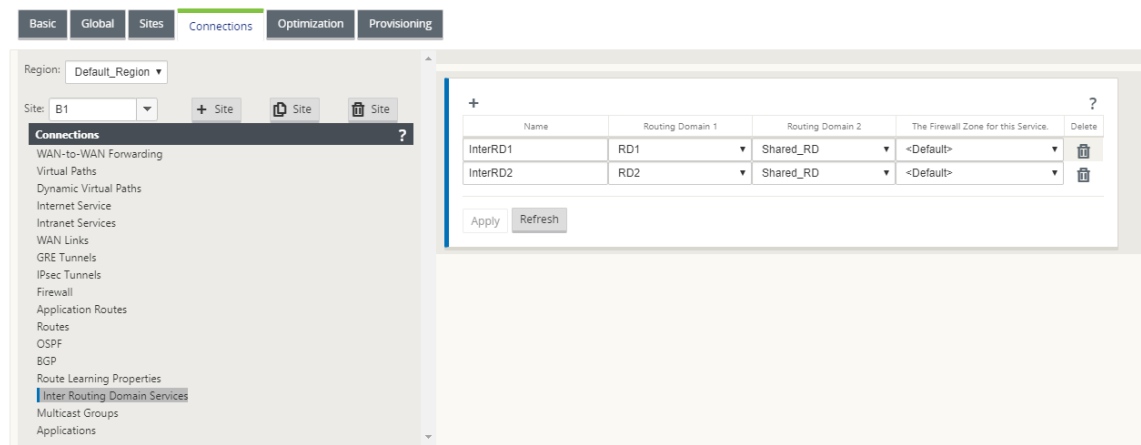
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

700



So ermöglichen Sie Benutzern in RD1 und RD2 den Zugriff auf Ressourcen in freigegebener RD:

1. Erstellen Sie einen Inter-Routing Domain-Dienst zwischen RD1 und Shared RD, zum Beispiel **Inter RD1**.
2. Erstellen Sie einen Inter-Routing Domain-Dienst zwischen RD2 und Shared RD, zum Beispiel **Inter RD2**.



3. Konfigurieren Sie eine statische Route zu freigegebener RD von RD1 und RD2. Fügen Sie in RD1 eine Route 172.168.2.0/24 zu InterRD1 hinzu.

Add ? x

Network Object: <Manual> Network IP Address: 172.168.2.0/24 Routing Domain: RD1 Cost: 5 Service Type: Inter Routing Dor Gateway IP Address:

☒ Export Route

Inter Routing Domain Service: InterRD1

Add Cancel

4. Fügen Sie in RD2 eine Route 172.168.2.0/24 zu InterRD2 hinzu.

Add ? x

Network Object: <Manual> Network IP Address: 172.168.2.0/24 Routing Domain: RD2 Cost: 5 Service Type: Inter Routing Dor Gateway IP Address:

☒ Export Route

Inter Routing Domain Service: InterRD2

Add Cancel

5. Fügen Sie InterRD1 eine dynamische NAT-Regel mithilfe einer VIP in freigegebenem Remotedesktop-RD hinzu. Aktivieren Sie “**Responder Route binden**“, um sicherzustellen, dass die umgekehrte Route denselben Dienstyp verwendet.

Add ? x

Priority: 100 Routing Domain: Shared_RD

Direction: Outbound Type: Port Restricted Service Type: Inter Routing Dor Service Name: InterRD1

Inside Zone: Any Inside IP Address: 0.0.0.0/0 Outside IP Address: 172.168.2.0

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☒ Bind Responder Route

Port Forwarding Rules +

| Routing Domain | Protocol | Outside Port | Inside IP Address | Inside Port | Fragments | Log Interval (s) | Log Start | Log End | Connection State Tracking | Delete |
|----------------|----------|--------------|-------------------|-------------|-----------|------------------|-----------|---------|---------------------------|--------|
|----------------|----------|--------------|-------------------|-------------|-----------|------------------|-----------|---------|---------------------------|--------|

Add Cancel

6. Fügen Sie eine dynamische NAT-Regel zu InterRD2 hinzu, indem Sie eine VIP in freigegebener RD verwenden, z. B. 10.0.0.11. Aktivieren Sie “Binden Responderoute”, um sicherzustellen, dass die umgekehrte Route denselben Dienstyp verwendet.

? x

Add

Priority: Routing Domain:

Direction: Type: Service Type: Service Name:

Inside Zone: Inside IP Address: Outside IP Address:

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☒ Bind Responder Route

Port Forwarding Rules +

| Routing Domain | Protocol | Outside Port | Inside IP Address | Inside Port | Fragments | Log Interval (s) | Log Start | Log End | Connection State Tracking | Delete |
|----------------|----------|--------------|-------------------|-------------|-----------|------------------|-----------|---------|---------------------------|--------|
|----------------|----------|--------------|-------------------|-------------|-----------|------------------|-----------|---------|---------------------------|--------|

Add Cancel

7. Verwenden Sie Filter, um zu begrenzen, auf welche Ressourcen in freigegebener RD von Benutzern in RD1/RD2 zugegriffen werden darf.

Sicheres Peering

May 10, 2021

Die Premium (Enterprise) Edition-Appliance kann im Rechenzentrum installiert werden und kann ein automatisches oder manuelles sicheres Peering initiieren, SSL-Profil erstellen und Serviceklasse verknüpfen und die Appliance mit einem Windows-Domänencontroller verbinden, sodass Benutzer/Administrator erweiterte Funktionen von eigenständigen WANOP verwenden können. -Appliance.

Im Folgenden werden die für Auto Secure Peering und manuelles Secure Peering unterstützten Bereitstellungsmodi aufgeführt:

Auto Secure Peering-Bereitstellungen:

[So führen Sie automatisch sicheres Peering an eine PE-Appliance von einem eigenständigen WANOP/SDWAN SE/WANOP auf dem DC-Standort aus.](#)

Schritte zum Initiieren dieser Bereitstellung:

- Die WANOP DC-Einheit befindet sich im LISTEN ON-Modus (2312/Beliebiger nicht standardmäßiger Port) und Branch PE ist im CONNECT-TO Modus.
- WANOP DC initiiert das automatische Secure Peering zu einer PE-Appliance, die die Private CA Certs und CERT KEY Pairs installiert und CONNECT-TO auf der PE-Appliance mit WANOPs LISTEN-ON IP konfiguriert.

So führen Sie automatisch sicheres Peering durch, das von der PE-Appliance am DC-Standort und der PE-Appliance für Zweigstandorte.

Schritte zum Initiieren dieser Bereitstellung:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443). Branch PE befindet sich im CONNECT-TO-Modus.
- Die PE-DC-Einheit initiiert ein automatisches sicheres Peering an eine PE-Zweig-Appliance, die die Private CA-Certs und CERT-KEY-Paare installiert und CONNECT-TO auf der PE-Zweig-Appliance mit der LISTEN-ON IP von DC PE konfiguriert.
- LISTEN-ON IP for PE befindet sich in der Schnittstellen-IP, die der Routingdomäne zugeordnet ist, für die "Redirect to WANOP" aktiviert ist.

Auto Secure Peering wurde von PE Appliance am DC-Standort und Zweig mit WANOP/SDWAN SE Appliance initiiert.

Schritte zum Initiieren dieser Bereitstellung:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443). Zweig WANOP/SD-WAN SE befindet sich im CONNECT-TO Modus.
- Die PE-DC-Appliance initiiert ein automatisches sicheres Peering zu Branch WANOP/SD-WAN SE Appliance, das die Private CA Certs und CERT KEY Pairs installiert und CONNECT-TO auf der PE-Appliance mit der LISTEN-ON IP von DC PE konfiguriert.

Manuelle Secure Peering-Bereitstellungen:

Manuelles Secure Peering von der PE-Appliance am DC-Standort zur Branch PE-Appliance initiiert.

Schritte zum Initiieren dieser Bereitstellung:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443). Branch PE befindet sich im CONNECT-TO-Modus.
- LISTEN-ON IP for PE befindet sich in der Schnittstellen-IP, die der Routingdomäne zugeordnet ist, für die "Redirect to WANOP" aktiviert ist.
- Laden Sie CA- und Cert Key-Paare Zertifikate manuell hoch, die von authentischer Quelle der Zertifizierungsstelle erhalten wurden.

Manuelles Secure Peering wurde von der PE-Appliance am DC-Standort zur Branch WANOP/SDWAN-SE Appliance initiiert.

Schritte zum Initiieren dieser Bereitstellung:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443). Zweig WANOP/SD-WAN SE befindet sich im CONNECT-TO Modus.
- LISTEN-ON IP for PE befindet sich in der Schnittstellen-IP, die der Routingdomäne zugeordnet ist, für die "Redirect to WANOP" aktiviert ist.

- Laden Sie CA- und Cert Key-Paare Zertifikate manuell hoch, die von authentischer Quelle der Zertifizierungsstelle erhalten wurden.

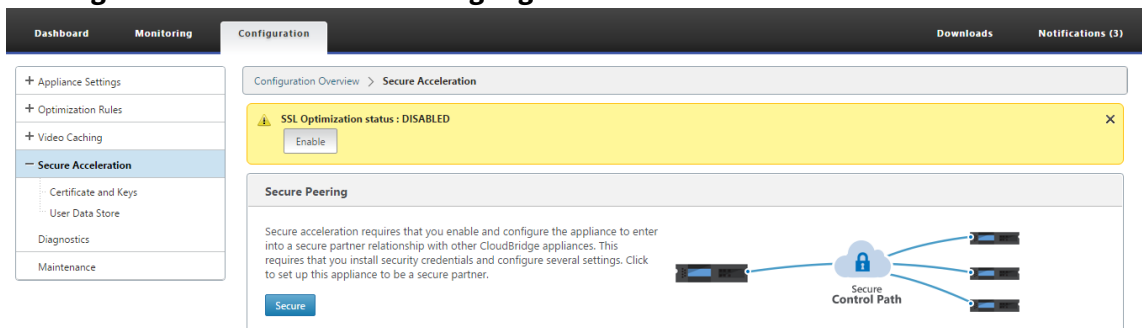
Auto Secure Peering an eine PE-Appliance von einer eigenständigen SD-WAN SE und WANOP Appliance am DC-Standort

May 10, 2021

So führen Sie automatisch sicheres Peering auf einer PE-Appliance von einer eigenständigen SD-WAN SE und WANOP-Appliance auf der DC-Seite aus:

- Die WANOP DC-Einheit befindet sich im LISTEN ON-Modus (2312/Beliebiger nicht standardmäßiger Port).
- Die Zweig-PE-Appliance befindet sich im CONNECT-TO-Modus.
- WANOP DC initiiert das automatische Secure Peering zu einer PE-Appliance, die die Private CA Certs und CERT KEY Pairs installiert und CONNECT-TO auf der PE-Appliance mit WANOPs LISTEN-ON IP konfiguriert.

1. Klicken Sie auf einer eigenständigen WANOP-Appliance im Rechenzentrum im Bereich **Secure Peering** der Seite **Sichere Beschleunigung** auf **Sichern**.



2. Konfigurieren Sie die Keystore-Einstellungen, indem Sie das **Keystore-Kennwort angeben** oder den Keystore deaktivieren.

Dashboard Monitoring **Configuration**

← Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Password*

Confirm Keystore Password*

☐ Disable Keystore Password

Save Cancel

3. Aktivieren Sie **Secure Peering**, indem Sie **Private CA** auswählen, um AUTOMATIC SECURE PEERING durchzuführen.

Dashboard Monitoring **Configuration** Downloads Notif

← Back

Secure Peering

Keystore Settings

Keystore Status
Opened

Secure Peering Certificate and Keys

Secure communications with the CloudBridge partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☒ Private CA ☐ CA Certificate

Save Cancel

4. Das CA-Zertifikat auf Appliance-Ebene und das private Zertifikat und der Schlüssel werden auf dem lokalen WANOP generiert und eine Tabelle zum Hinzufügen eines sicheren REMOTE PEER TO Perform AUTO Peering with wird angezeigt.
5. Klicken Sie auf das +-Symbol und ein Popupfenster, um IP-Adresse mit Benutzername und Kennwort hinzuzufügen, wird angezeigt. Nach erfolgreicher Authentifizierung mit der Remote-IP mit bereitgestellten Anmeldeinformationen wird eine Anforderung an den Remotecomputer gesendet, der das Zertifizierungsstellenzertifikat sowie das private Zertifikat und den Schlüssel für sich selbst (auf dem Remotecomputer) installiert.

DashboardMonitoringConfigurationDownloadsNotifications (3)

Back

Secure Peering

Keystore Settings

Keystore StatusOpened

Secure Peering Certificate and Keys

| | | | |
|-----------------------|--|--|---|
| Secure PeeringEnabled | Certificate/Key Pair Nameprivate_10_105_184_74 | CA Certificate Store NamePrivateRootCA | Cipher Specification!ADH:!AECDH:!MD5:HIG@STRENGTH |
|-----------------------|--|--|---|

Connected Peers

Hinweis

- IP-Adresse —IP-Adresse remote PREMIUM (ENTERPRISE) EDITION APPLIANCE MANAGEMENT IP
- Benutzername —Benutzername remote PREMIUM (ENTERPRISE) EDITION APPLIANCE
- Kennwort —Kennwort remote PREMIUM (ENTERPRISE) EDITION APPLIANCE

DashboardMonitoringConfigurationDownloadsNotifications (3)

Back

Secure Peering

Keystore Settings

Keystore StatusOpened

Secure Peering Certificate and Keys

| | | | |
|-----------------------|--|--|---|
| Secure PeeringEnabled | Certificate/Key Pair Nameprivate_10_105_184_74 | CA Certificate Store NamePrivateRootCA | Cipher Specification!ADH:!AECDH:!MD5:HIG@STRENGTH |
|-----------------------|--|--|---|

Connected Peers

Connect Peer

IP Address10.1.1.1UsernamePROVIDE_VW_APPLIANCE_UNAMEPassword

ConnectClose

Nach erfolgreicher Authentifizierung sehen Sie Secure Peering als TRUE und die Partner-IP-Adresse als eine der virtuellen IP-Adressen der Remote Premium (Enterprise) Edition Appliance.

DashboardMonitoringConfigurationDownloadsNotifications (3)

Back

Secure Peering

Keystore Settings

Keystore StatusOpened

Secure Peering Certificate and Keys

| | | | |
|-----------------------|--|--|---|
| Secure PeeringEnabled | Certificate/Key Pair Nameprivate_10_105_184_74 | CA Certificate Store NamePrivateRootCA | Cipher Specification!ADH:!AECDH:!MD5:HIG@STRENGTH |
|-----------------------|--|--|---|

Connected Peers

| Peer Name | IP Address | Secure | Connection Status | Time Connected ↑ | Time Since Last Contacted |
|--------------|--------------|--------|---------------------|------------------|---------------------------|
| CloudBridge1 | 172.184.1.19 | True | Connected Available | 7m 44s | 0m 5s |

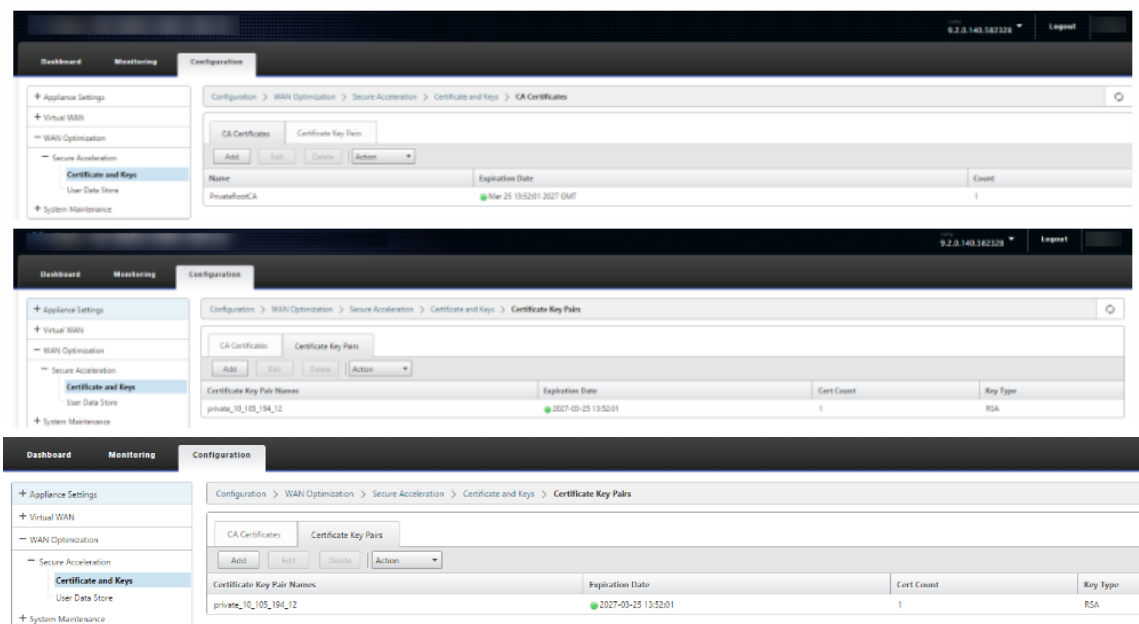


VIP of Remote EE App

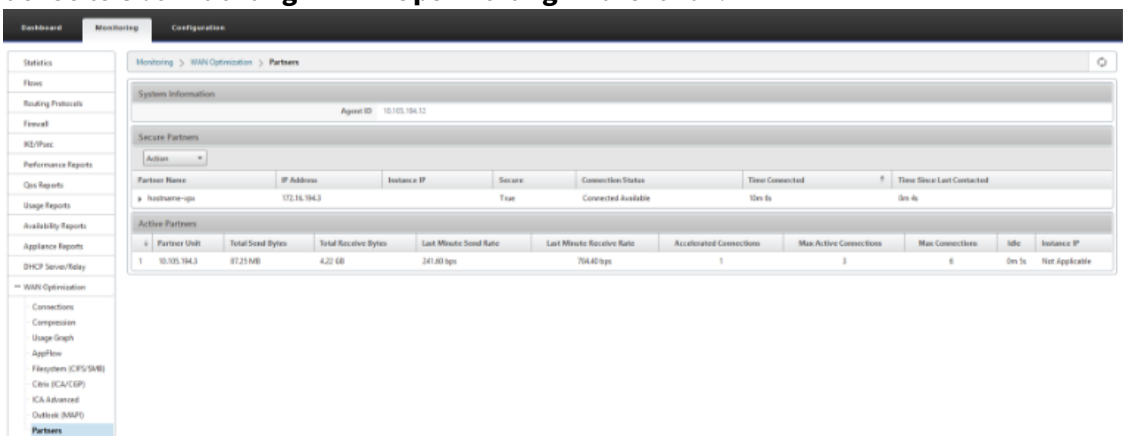
Überwachen

Sichere Partnerinformationen auf der Premium (Enterprise) Edition-Appliance unter **WANOPTIMIZATION > Partner** auf der Seite **Überwachung** anzeigen.

1. Die Data Store-Verschlüsselung kann auf der Premium (Enterprise) Edition-Appliance über die Funktionsaktivierung des MCN unter Optimierungsknoten für eine Premium (Enterprise) Edition-Appliance durchgeführt werden.
2. Für eine Premium (Enterprise) Edition-Appliance ist Secure Peering immer aktiviert.
3. Überprüfen Sie die folgenden Informationen, um zu überprüfen, ob das Paar **Private CA** und **Private Certificate Key** erfolgreich generiert wurden:



4. Zeigen Sie **Secure Partner Information** auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung > WAN-Optimierung > Partner** an.



5. Auf der Partner-Appliance die **Secure Partnerinformationen der Premium (Enterprise)**

Edition-Appliance auf der Seite Überwachung>Partner & Plug-ins>Secure Partner anzeigen.

The screenshot shows the Citrix SD-WAN 11.2 interface. The top navigation bar includes Dashboard, Monitoring, Configuration, Downloads, and Notifications (1). The left sidebar has a tree view with categories like Optimization, Appliance Performance, and Partners & Plug-ins. Under Partners & Plug-ins, the 'Secure Partners' option is selected. The main content area displays the 'Secure Partners' page with a breadcrumb trail: Monitoring > Partners & Plug-ins > Secure Partners. A table lists the details for a partner named 'MCN2K'.

| Partner Name | IP Address | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|---------------|--------|---------------------|----------------|---------------------------|
| MCN2K | 172.20.194.11 | True | Connected Available | 15m 45s | 0m 6s |

Below the table, detailed information for the selected partner is shown:

- Software Version: 9.2.0.105.575120 (Production)
- Connection Initiator: false
- SSL Cipher: ECDH-IE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_12
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 78.3M
- Bytes Sent: 3.8G
- Number Of Connections: 2

Problembehandlung

1. Zeigen Sie **Secure Partner Success/Failure Information** auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung>WAN-Optimierung>Partner>Secure Partners** an.

The screenshot shows the Citrix SD-WAN 11.2 interface. The top navigation bar includes Dashboard, Monitoring, and Configuration. The left sidebar has a tree view with categories like Statistics, Flows, Routing Protocols, Firewall, and WAN Optimization. Under WAN Optimization, the 'Partners' option is selected. The main content area displays the 'Secure Partners' page with a breadcrumb trail: Monitoring > WAN Optimization > Partners. A table lists the details for a partner named 'Isotname-ups'.

| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|--------------|-------------|--------|---------------------|----------------|---------------------------|
| Isotname-ups | 172.16.194.3 | | True | Connected Available | 10m 5s | 0m 4s |

Below the table, detailed information for the selected partner is shown:

- Software Version: 9.2.0.105.575120 (Production)
- Connection Initiator: true
- SSL Cipher: ECDH-IE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_3
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 4.2G
- Bytes Sent: 87.2M
- Number Of Connections: 1

At the bottom, an 'Active Partners' table provides summary statistics:

| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accumulated Connections | Max Active Connections | Max Connections | Idle | Instance IP | |
|--------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|------|-------------|----------------|
| 1 | 10.105.194.3 | 87.25 MB | 4.22 GB | 247.80 kbps | 704.80 kbps | 1 | 3 | 6 | 0m 5s | Not Applicable |

2. Zeigen Sie auf der Partner-Appliance Secure Partner Information auf der Premium (Enterprise) Edition-Appliance auf der Seite **Monitoring > Partners & Plug-ins > Secure Partners** an.

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

+ Appliance Performance

- Partners & Plug-ins

NetScaler SD-WAN WANOP Clients

NetScaler SD-WAN WO Partners

Secure Partners

Monitoring > Partners & Plug-ins > Secure Partners

Action

| Partner Name | IP Address | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|---|---------------|--------|---------------------|----------------|---------------------------|
| MCH2K | 172.20.194.11 | True | Connected Available | 15m 45s | 0m 6s |
| Software Version 9.2.0.105.373120 (Production) | | | | | |
| Connection Initiator false | | | | | |
| SSL Cipher ECCDHE-RSA-AES256-SHA 256 bit | | | | | |
| Last Common Name private_10_100_194_12 | | | | | |
| Last SSL Connection Error --No Last SSL Error-- | | | | | |
| Last Connection Error --No Last Error-- | | | | | |
| Bytes Received 78.3M | | | | | |
| Bytes Sent 3.85 | | | | | |
| Number Of Connections 2 | | | | | |

3. Zeigen Sie auf der Partner-Appliance Secure Partner Information auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung > Appliance-Performance > Logging** an.

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

- Appliance Performance

Compression Engine

WCCP

AppFlow

Load Statistics

+ Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Action

Search

| Record | Date/Time | Details |
|--------|-----------------------|--|
| 5356 | Mar 01, 2017 05:50:20 | syslog:Mar 1 05:50:20 hostname=vps-NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5355 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname=vps-NITRO[6762]: RESPONSE -Status: Success |
| 5354 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname=vps-NITRO[6762]: PAYLOAD: [{"params":{"system_info":{" |
| 5353 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname=vps-NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5352 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname=vps-NITRO[6762]: RESPONSE -Status: Success |
| 5351 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname=vps-NITRO[6762]: PAYLOAD: [{"params":{"system_info":{" |
| 5350 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname=vps-NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5349 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname=vps-NITRO[6762]: RESPONSE -Status: Success |
| 5348 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname=vps-NITRO[6762]: PAYLOAD: [{"params":{"system_info":{" |
| 5347 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname=vps-NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5346 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname=vps-NITRO[6762]: RESPONSE -Status: Success |
| 5345 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname=vps-NITRO[6762]: PAYLOAD: [{"params":{"system_info":{" |
| 5344 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname=vps-NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5343 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname=vps-NITRO[6762]: RESPONSE -Status: Success |
| 5342 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname=vps-NITRO[6762]: PAYLOAD: [{"params":{"system_info":{" |
| 5341 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname=vps-NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5340 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname=vps-NITRO[6762]: RESPONSE -Status: Success |
| 5339 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname=vps-NITRO[6762]: PAYLOAD: [{"params":{"system_info":{" |

Auto Secure Peering wurde von der PE-Appliance am DC-Standort und der PE-Appliance des Zweigstellenstandorts initiiert

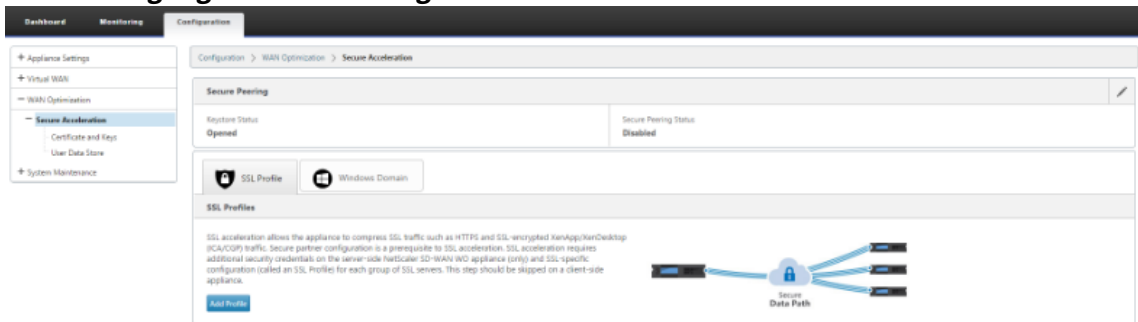
May 10, 2021

Konfiguration

So konfigurieren Sie das automatische Peering auf einer neuen Premium (Enterprise) Edition-Appliance unter DC:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443). Die Zweig-PE-Appliance befindet sich im CONNECT-TO-Modus.
- Die PE-DC-Appliance initiiert ein automatisches sicheres Peering zu einer PE-Zweig-Appliance, die die Private CA-Certs und CERT-KEY-Paare installiert und CONNECT-TO auf der PE-Zweig-Appliance mit der LISTEN-ON IP von DC EE konfiguriert.
- LISTEN-ON IP für PE-Appliance befindet sich in der Schnittstellen-IP, die der Routingdomäne zugeordnet ist, für die “Redirect to WANOP” aktiviert ist.

1. Navigieren Sie in der SD-WAN-Web-GUI zu **Konfiguration > WAN-Optimierung > Sichere Beschleunigung > Secure Peering**.



2. Konfigurieren Sie den Keystore, indem Sie das Keystore-Kennwort angeben oder den Keystore deaktivieren.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*
Open

☐ Change Keystore Password
☐ Disable Keystore Password
☐ Reset Keystore

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

3. Aktivieren Sie **Secure Peering**, indem Sie **Private CA** auswählen, um AUTOMATIC SECURE PEERING durchzuführen.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN VWO partner appliance requires that you generate OpenSSL credentials, including a CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☒ Private CA ☐ CA Certificate

Save Cancel

| Secure Peering Certificate and Keys | | | |
|-------------------------------------|---------------------------|---------------------------|---------------------------------|
| Secure Peering | Certificate/Key Pair Name | CA Certificate Store Name | Cipher Specification |
| Enabled | private_10_105_194_12 | PrivateRootCA | IADH:IAECDH:IMD5:HIGH:@STRENGTH |

| Secure Peering Certificate and Keys | | | |
|-------------------------------------|---------------------------|---------------------------|---------------------------------|
| Secure Peering | Certificate/Key Pair Name | CA Certificate Store Name | Cipher Specification |
| Enabled | private_10_105_194_12 | PrivateRootCA | IADH:IAECDH:IMD5:HIGH:@STRENGTH |

4. Klicken Sie auf das '+'-Symbol und fügen Sie IP mit Benutzernamen und Kennwort hinzu. Nach erfolgreicher Authentifizierung mit der angegebenen Remote-IP und den angegebenen Anmeldeinformationen wird eine Anforderung an den Remotecomputer gesendet, der das Zertifizierungsstellenzertifikat und den privaten Schlüssel für sich selbst lokal auf dem Remotecomputer installiert.

Hinweis

IP-Adresse — IP-Adresse der Remote-EE-Appliance-MANAGEMENT IP

Benutzername — Benutzername der entfernten EE-Appliance

Kennwort — Kennwort der Remote-EE-Appliance

Dashboard Monitoring Configuration

Secure Peering

Keystore Settings

Keystore Status

Opened

Secure Peering Certificate and Keys

Secure Peering

Enabled

Certificate/Key Pair Name

private_10_105_194_12

Connect Peer

Connect Peer

IP Address

10 . 105 . 194 . 3

Username

admin

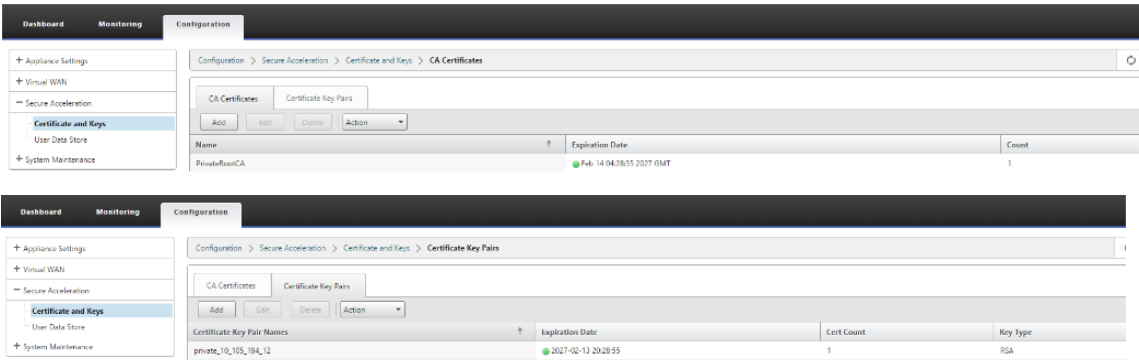
Password

.....

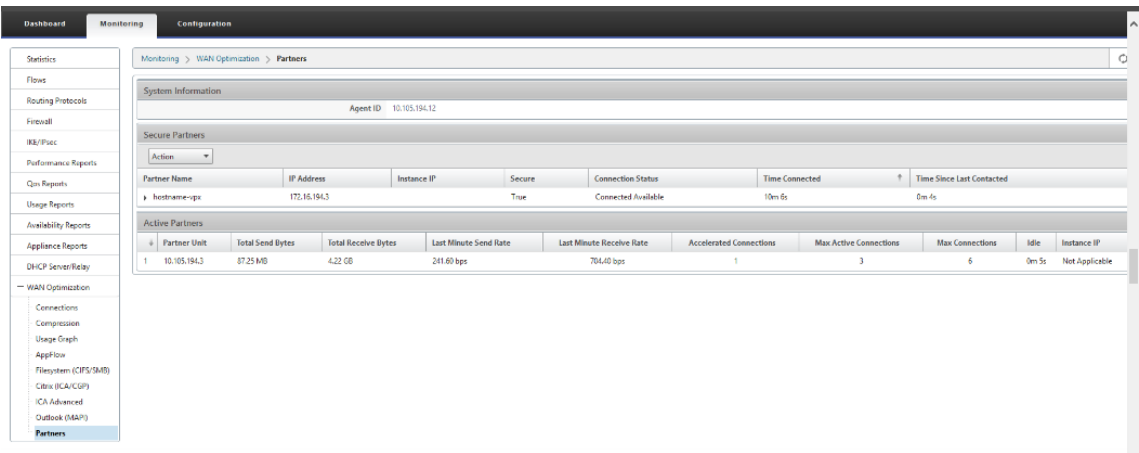
Connect Close

Überwachen

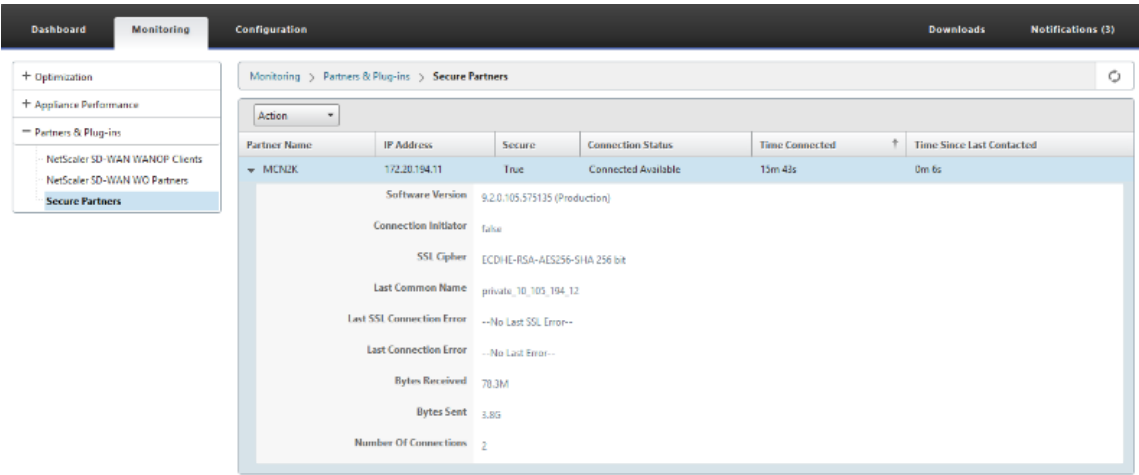
1. Überprüfen Sie die unten angezeigten Informationen, um zu überprüfen, ob das Paar Private CA und Private Certificate Key erfolgreich generiert wurden.



2. Zeigen Sie **Secure Partner Information** auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung > WAN-Optimierung > Partner** an.



3. Zeigen Sie auf der Partner-Appliance Secure Partner Information auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Partner & Plug-ins > Sichere Partner** an.



Problembehandlung

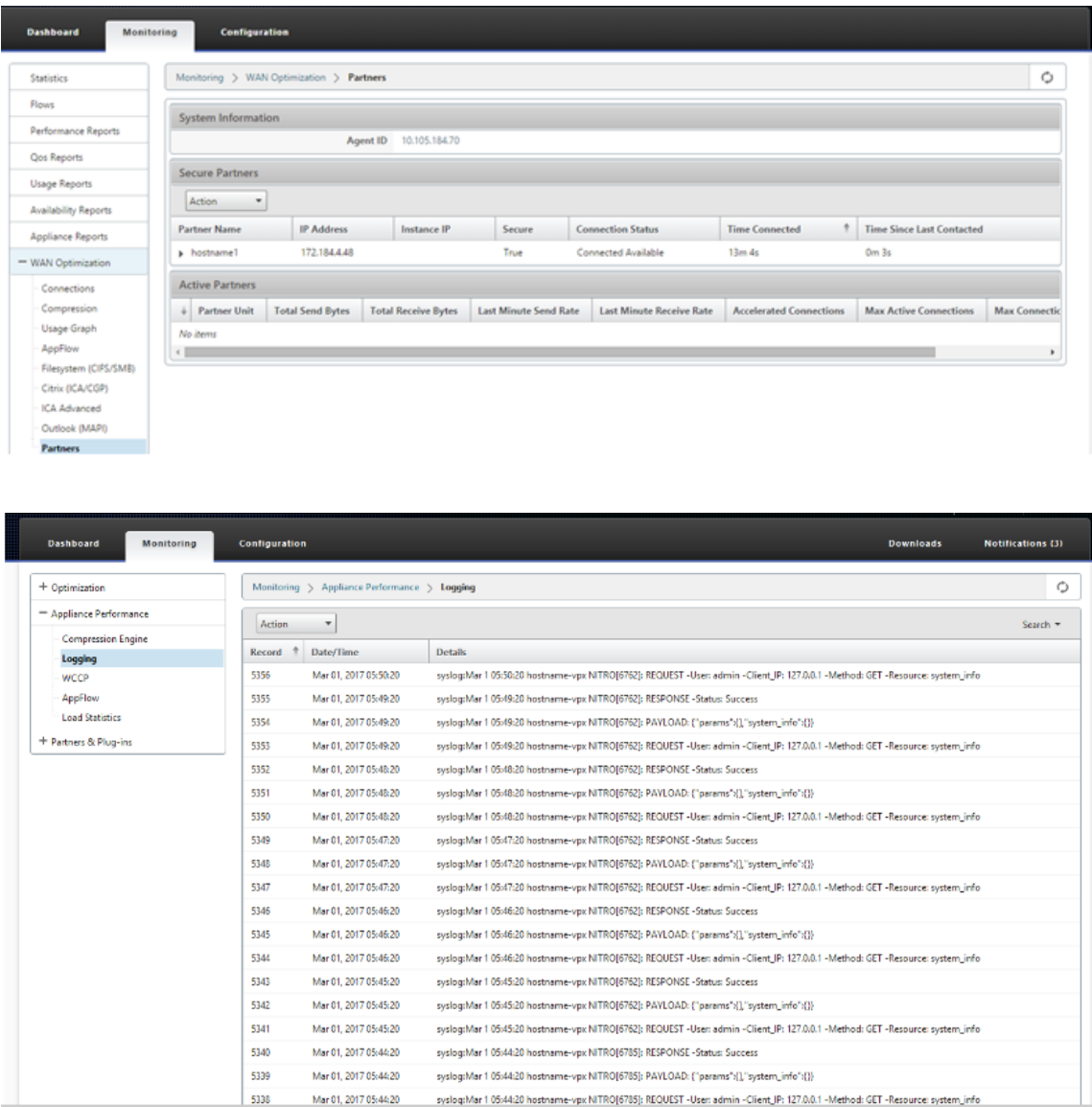
1. Sehen Sie sich die Erfolgs-/Fehlerinformationen für sichere Partner auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung > WAN-Optimierung > Partner > Secure Partners** an.

The screenshot shows the 'Secure Partners' page in the Citrix SD-WAN 11.2 interface. The left sidebar contains a navigation menu with options like Statistics, Flows, Routing Protocols, Firewall, NG/IPSec, Performance Reports, QoS Reports, Usage Reports, Availability Reports, Appliance Reports, DHCP Server/Proxy, WAN Optimization, Connections, Compression, Usage Graph, AppFlow, Filesystem (CIFS/SMB), Citrix (ICA/CGP), ICA Advanced, Outlook (MAP), and Partners. The main content area is titled 'Monitoring > WAN Optimization > Partners'. It displays system information for Agent ID 10.105.194.12. Below this, there is a table for 'Secure Partners' with columns: Partner Name, IP Address, Instance IP, Secure, Connection Status, Time Connected, and Time Since Last Contacted. The table shows one entry for 'localhost-ops' with IP 172.16.194.3, which is connected and available for 10m 4s. Below the table, there is a section for 'Active Partners' with a table showing details for the 'localhost-ops' partner, including total send/receive bytes, last minute send/receive rates, accelerated connections, and max active connections.

2. Zeigen Sie auf der Partner-Appliance Secure Partner Information auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Partner & Plug-ins > Sichere Partner** an.

The screenshot shows the 'Secure Partners' page in the Citrix SD-WAN 11.2 interface, accessed via 'Monitoring > Partners & Plug-ins'. The left sidebar shows a navigation menu with options like Optimization, Appliance Performance, Partners & Plug-ins, NetScaler SD-WAN WANOP Clients, NetScaler SD-WAN WO Partners, and Secure Partners. The main content area is titled 'Monitoring > Partners & Plug-ins > Secure Partners'. It displays a table for 'Secure Partners' with columns: Partner Name, IP Address, Secure, Connection Status, Time Connected, and Time Since Last Contacted. The table shows one entry for 'MCN2K' with IP 172.20.194.11, which is connected and available for 15m 42s. Below the table, there is a section for 'Active Partners' with a table showing details for the 'MCN2K' partner, including total send/receive bytes, last minute send/receive rates, accelerated connections, and max active connections.

3. Zeigen Sie auf der Partner-Appliance Secure Partner Information auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Appliance-Leistung > Protokollierung** an.



Auto Secure Peering initiiert von PE-Appliance am DC-Standort und Zweigstelle mit eigenständiger SD-WAN SE und WANOP Appliance

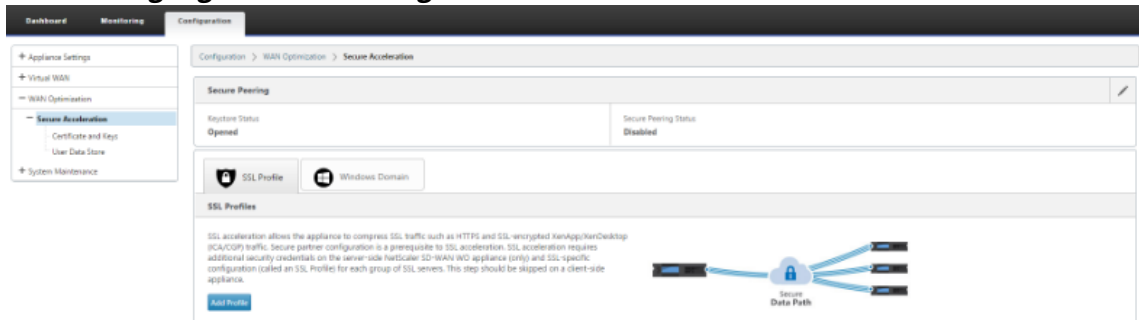
May 10, 2021

Konfiguration

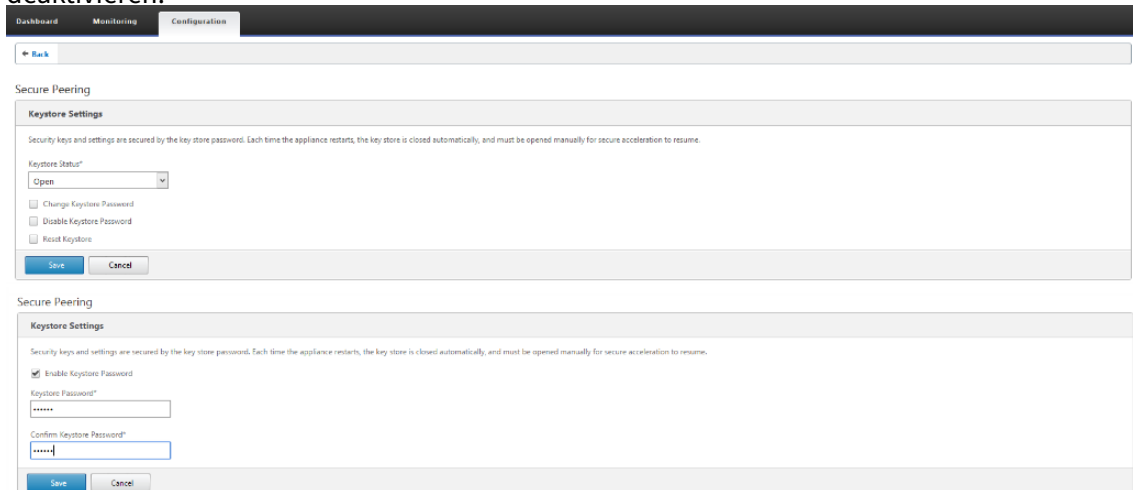
So konfigurieren Sie eine neue Premium (Enterprise) Edition-Appliance mit automatischem Secure Peering am DC-Standort und Zweig mit Standalone SD-WAN und WANOP-Appliance:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443).
- Branch Standalone SD-WAN SE und WANOP befindet sich im CONNECT-TO Modus.
- Die PE-DC-Appliance initiiert ein automatisches sicheres Peering zu Branch Standalone SD-WAN SE und WANOP Appliance, das die Private CA Certs und CERT KEY Pairs installiert und CONNECT-TO auf der PE-Appliance mit der LISTEN-ON IP von DC EE konfiguriert.

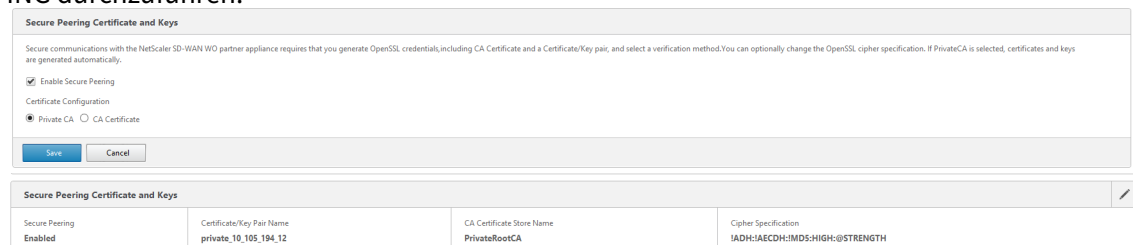
1. Navigieren Sie in der SD-WAN-Web-GUI zu **Konfiguration > WAN-Optimierung > Sichere Beschleunigung > Secure Peering**.



2. Konfigurieren Sie den Keystore, indem Sie das Keystore-Kennwort angeben oder den Keystore deaktivieren.



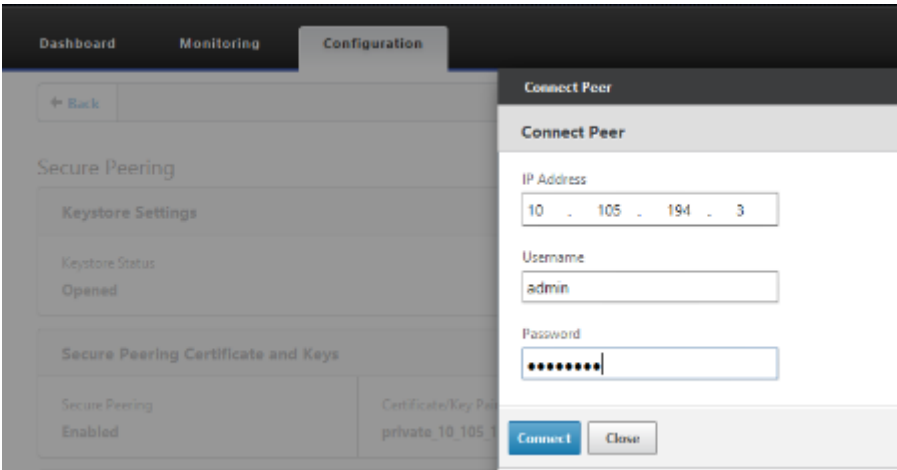
3. Aktivieren Sie **Secure Peering**, indem Sie **Private CA** auswählen, um AUTOMATIC SECURE PEERING durchzuführen.



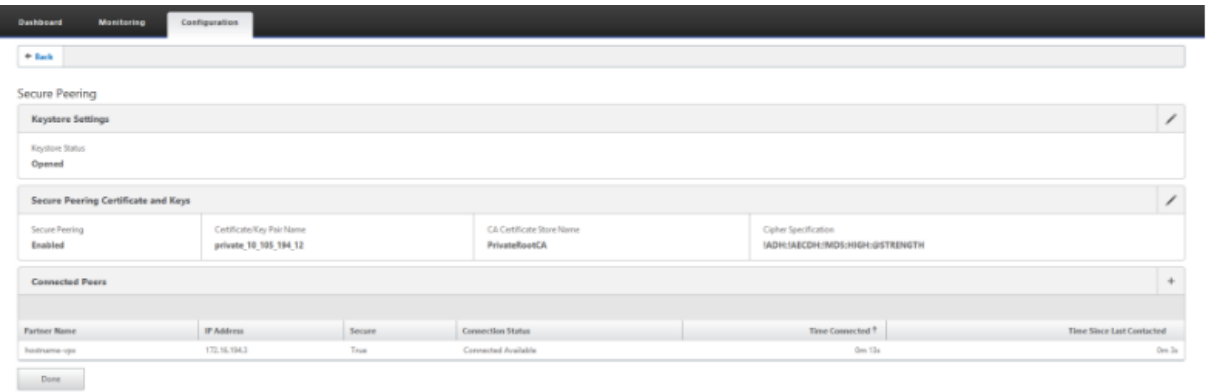
4. Klicken Sie auf das '+'-Symbol und fügen Sie IP mit Benutzernamen und Kennwort hinzu. Nach erfolgreicher Authentifizierung mit der angegebenen Remote-IP und den angegebenen

nen Anmeldeinformationen wird eine Anforderung an den Remotecomputer gesendet, der das Zertifizierungsstellenzertifikat und den privaten Schlüssel für sich selbst lokal auf dem Remotecomputer installiert.

- IP-Adresse —IP-Adresse der Remote-WANOP Standalone oder Standard Edition Appliance MANAGEMENT IP.
- Benutzername —Benutzername der entfernten WANOP Standalone oder Standard Edition Appliance.
- Kennwort —Kennwort der Remote-WANOP Standalone oder Standard Edition Appliance.

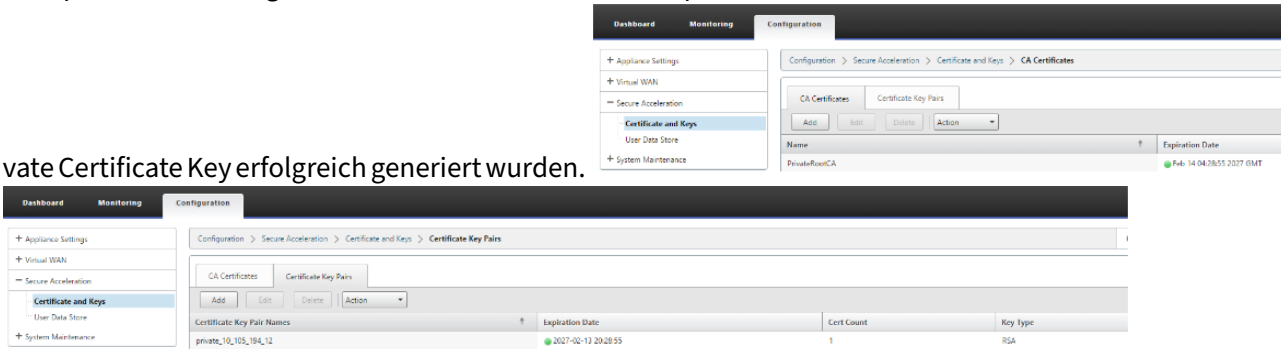


Nach erfolgreicher Authentifizierung können Sie Secure Peering als TRUE und die Partner-IP als eine der virtuellen IP der eigenständigen WANOP Remote-Appliance anzeigen.

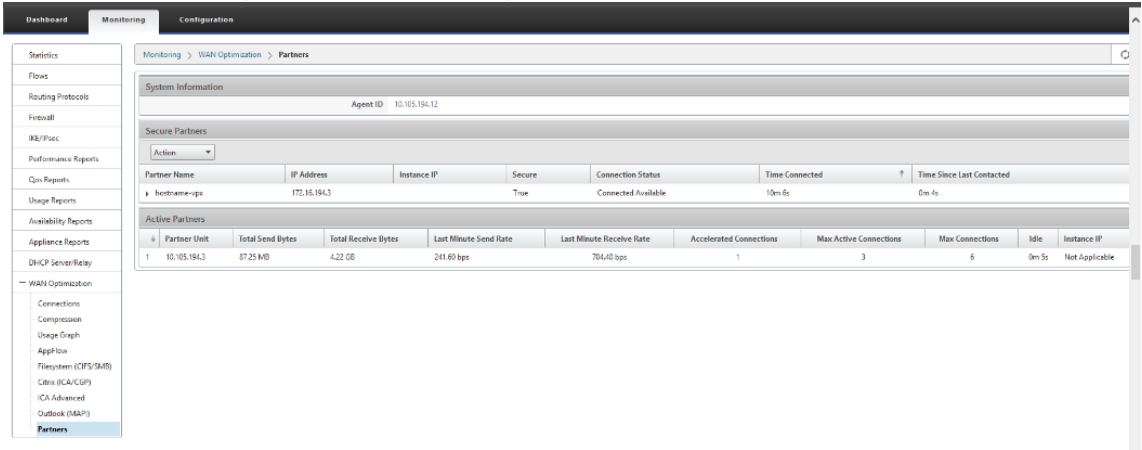


Überwachen

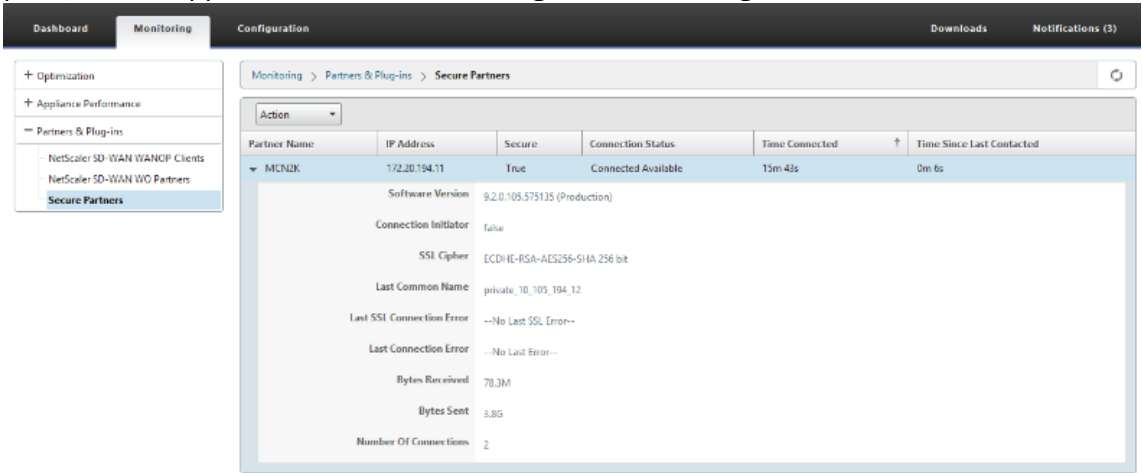
1. Überprüfen Sie die folgenden Informationen, um zu überprüfen, ob das Paar Private CA und Pri-



2. Zeigen Sie Informationen zu sicheren Partnern auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > WAN-Optimierung > Partner** an.



3. Zeigen Sie auf der Partner-Appliance Secure Partner Informationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Partner & Plug-ins > Secure Partners** Seite an.



Problembehandlung

1. Anzeigen von Erfolgs- und Fehlerinformationen für sichere Partner auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > WAN-Optimierung > Partner > Sichere Partner**.

The screenshot shows the 'Secure Partners' page in the Citrix SD-WAN 11.2 interface. The breadcrumb navigation is 'Monitoring > WAN Optimization > Partners'. The page displays system information for the appliance (Agent ID: 10.105.194.12) and a table of secure partners. The table has columns: Partner Name, IP Address, Instance IP, Secure, Connection Status, Time Connected, and Time Since Last Contacted. One partner is listed: 'localhost-194.3' with IP 172.16.194.3, Instance IP 172.16.194.3, Secure status 'True', Connection Status 'Connected Available', Time Connected '10m 4s', and Time Since Last Contacted '0m 4s'. Below the table, there is a section for 'Active Partners' with a table showing metrics for the partner unit.

| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|-----------------|--------------|--------------|--------|---------------------|----------------|---------------------------|
| localhost-194.3 | 172.16.194.3 | 172.16.194.3 | True | Connected Available | 10m 4s | 0m 4s |

| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accelerated Connections | Max Active Connections | Max Connections | Idle | Instance IP |
|----------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|-------|----------------|
| 1 10.105.194.3 | 87.25 MB | 4.22 GB | 241.60 bps | 704.40 bps | 1 | 2 | 6 | 0m 5s | Not Applicable |

2. Zeigen Sie auf der Partner-Appliance **Secure Partner Information** auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Partner & Plug-Ins > Sichere Partner an**.

The screenshot shows the 'Secure Partners' page on a partner appliance in the Citrix SD-WAN 11.2 interface. The breadcrumb navigation is 'Monitoring > Partners & Plug-Ins > Secure Partners'. The page displays system information for the partner unit (MCN2K) and a table of secure partners. The table has columns: Partner Name, IP Address, Instance IP, Secure, Connection Status, Time Connected, and Time Since Last Contacted. One partner is listed: 'localhost-194.3' with IP 172.20.194.11, Instance IP 172.20.194.11, Secure status 'True', Connection Status 'Connected Available', Time Connected '15m 42s', and Time Since Last Contacted '0m 6s'. Below the table, there is a section for 'Active Partners' with a table showing metrics for the partner unit.

| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|-----------------|---------------|---------------|--------|---------------------|----------------|---------------------------|
| localhost-194.3 | 172.20.194.11 | 172.20.194.11 | True | Connected Available | 15m 42s | 0m 6s |

| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accelerated Connections | Max Active Connections | Max Connections | Idle | Instance IP |
|----------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|-------|----------------|
| 1 10.105.194.3 | 87.25 MB | 4.22 GB | 241.60 bps | 704.40 bps | 1 | 2 | 6 | 0m 5s | Not Applicable |

3. Zeigen Sie auf der Partner-Appliance **Secure Partner Information** auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Appliance-Leistung > Protokollierung** an.

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

- Appliance Performance

Compression Engine

Logging

WCCP

AppFlow

Load Statistics

+ Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Action

Search

| Record | Date/Time | Details |
|--------|-----------------------|--|
| 5356 | Mar 01, 2017 05:50:20 | syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5355 | Mar 01, 2017 05:49:20 | syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5354 | Mar 01, 2017 05:49:20 | syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{" |
| 5353 | Mar 01, 2017 05:49:20 | syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5352 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5351 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{" |
| 5350 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5349 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5348 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{" |
| 5347 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5346 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5345 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{" |
| 5344 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5343 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5342 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{" |
| 5341 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5340 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5339 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{" |
| 5338 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info |

Manuelles Secure Peering von der PE-Appliance am DC-Standort und Branch PE-Appliance initiiert

May 10, 2021

Diese Bereitstellung konfiguriert die DC-Standort-PE-Appliance im LISTEN ON Modus und Zweigstand-PE-Appliance im CONNECT TO Modus.

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443).
- Die Zweig-PE-Appliance befindet sich im CONNECT-TO-Modus.
- LISTEN-ON IP for PE befindet sich in der Schnittstellen-IP, die der Routingdomäne zugeordnet ist, für die “Redirect to WANOP” aktiviert ist.
- Laden Sie CA- und Cert Key-Paare Zertifikate manuell hoch, die von authentischer Quelle der Zertifizierungsstelle erhalten wurden.

Konfiguration

So konfigurieren Sie automatisch Secure Peering, das von einer PE-Appliance am DC-Standort und einer PE-Appliance am Zweigstandort initiiert wurde:

1. Laden Sie **CA-Zertifikat** und **CA-Schlüsselzertifikat** aus authentischem Zertifikat und stellen Sie SD-WAN wie unten dargestellt hoch.

Configuration > Secure Acceleration > Certificate and Keys > CA Certificates

CA Certificates

Certificate Key Pairs

Add

Edit

Delete

Action

| Name | Expiration Date | Count |
|------|-------------------------------------|-------|
| CA | <div>Feb 25 01:39:42 2032 GMT</div> | 1 |

Configuration > Secure Acceleration > Certificate and Keys > Certificate Key Pairs

CA Certificates

Certificate Key Pairs

Add

Edit

Delete

Action

| Certificate Key Pair Names | Expiration Date | Cert Count | Key Type |
|----------------------------|--------------------------------|------------|----------|
| CAKeyPair | <div>2033-07-18 20:01:18</div> | 1 | RSA |

2. Wechseln Sie auf einer neuen PE-Appliance am DC-Standort in der SD-WAN-Web-GUI zu **Konfiguration > Sichere Beschleunigung > Secure Peering**.

DashboardMonitoringConfiguration

Appliance Settings

Virtual WAN

WAN Optimization

Secure Acceleration

Certificate and Keys

User Data Store

System Maintenance

Configuration > WAN Optimization > Secure Acceleration

Secure Peering

Keystore Status

Opened

Secure Peering Status

Disabled


SSL Profile

Windows Domain

SSL Profiles

SSL acceleration allows the appliance to compress SSL traffic such as HTTPS and SSL-encrypted RADIUS/NetFlow/ICMP/IGMP traffic. Secure peer configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server-side hardware SD-WAN WFO appliance (only) and SSL-specific configuration (called an SSL Profile) for each group of SSL servers. This step should be skipped on a client-side appliance.

Add Profile



3. Konfigurieren Sie den Keystore, indem Sie das Keystore-Kennwort angeben oder den Keystore deaktivieren.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Save

Cancel

DashboardMonitoringConfiguration

Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*

Open

Change Keystore Password

Disable Keystore Password

Reset Keystore

Save

Cancel

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

Save

Cancel

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

721

4. Aktivieren Sie sicheres Peering, indem Sie das Optionsfeld **CA-Zertifikat** auswählen und hochgeladene CA- und CA-Schlüsselpaarzertifikate entsprechend bereitstellen, wie unten dargestellt.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☐ Private CA ☒ CA Certificate

Certificate/Key Pair Name
CAKeyPair

CA Certificate Store Name
CA

Certificate Verification*
Signature/Expiration

SSL Cipher Specification
[ADH:!AECDH:!MD5:HIGH:@STRENGTH]

☐ Edit Cipher Specification

Save **Cancel**

5. Bereitstellen der virtuellen IP des Remote-Computers zusammen mit Port 443, wie unten gezeigt.

Listen On and Connect To

Auto Discovery is typically enabled, when enabled, any authenticated peers can connect via the Listen On addresses. If disabled, secure communications are allowed only with peers on the Connect To list.

☒ Enable Auto-Discovery

Listen On
169.254.1.20 : 443
169.254.1.20 : 2312

☒ Publish NAT addresses to peers

NAT Addresses
172.16.120.131 : 443

Connect To
172.16.220.140 : 443

Save **Cancel**

Überwachen

1. Um zu überprüfen, ob das Paar **Private CA** und **Private Certificate Key** erfolgreich generiert wurde, überprüfen Sie die folgenden Informationen.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IPsec/Psec

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

WAN Optimization

- Connections
- Compression
- Usage Graph
- AppFlow
- Filesystem (CIFS/SMB)
- Citrix (ICA/ICUP)
- CA Advanced
- Outlook (MAP)
- Partners

Monitoring > WAN Optimization > Partners

System Information

Agent ID 10.105.194.12

Secure Partners

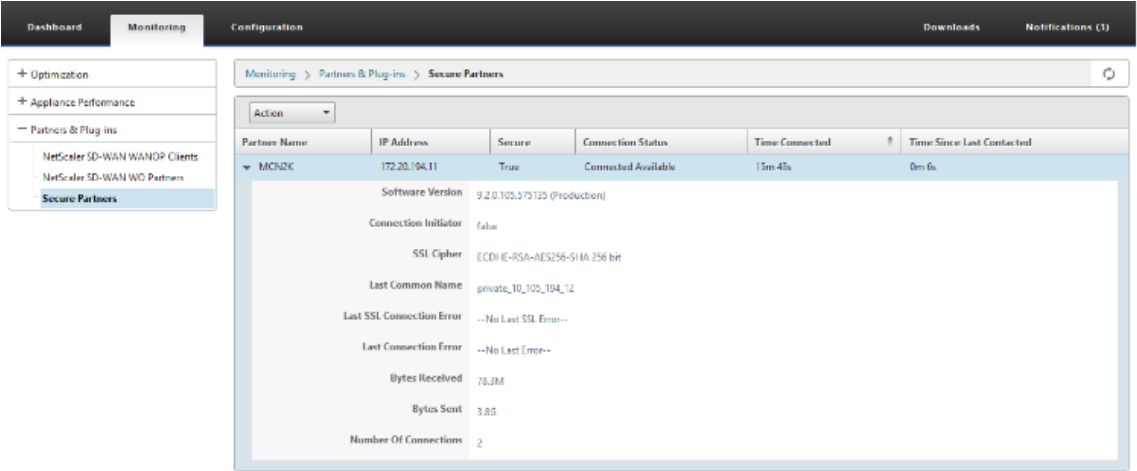
Action

| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|--------------|-------------|--------|---------------------|----------------|---------------------------|
| Hostname-gps | 172.16.194.3 | | True | Connected Available | 10m 5s | 0m 4s |

Active Partners

| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accelerated Connections | Max Active Connections | Max Connections | Idle | Instance IP | |
|--------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|------|-------------|----------------|
| 1 | 10.105.194.3 | 87.25 MB | 4.22 GB | 241.60 bps | 704.60 bps | 1 | 3 | 6 | 0m 5s | Not Applicable |

2. Auf der Partner-Appliance die **Secure Partnerinformationen auf der Premium (Enterprise) Edition-Appliance auf der SeiteMonitoring>Partners>Secure Partnersanzeigen.**

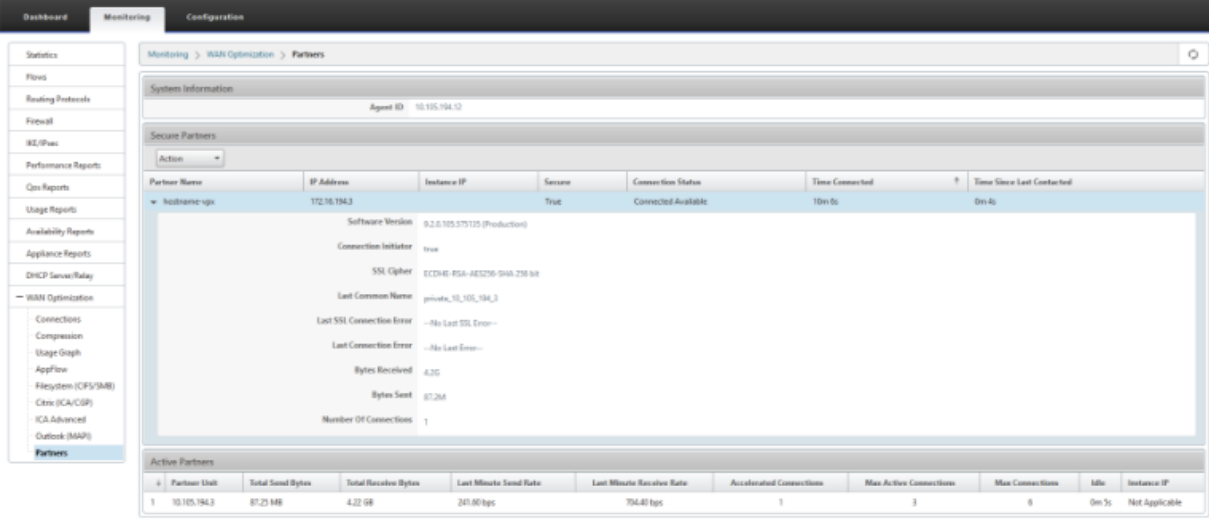


| Partner Name | IP Address | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|---------------|--------|---------------------|----------------|---------------------------|
| MCH2K | 172.20.194.11 | True | Connected Available | 15m 45s | 0m 6s |

| | |
|---------------------------|-------------------------------|
| Software Version | 9.2.0.105.379120 (Production) |
| Connection Initiator | false |
| SSL Cipher | ECDHE-RSA-AES256-SHA 256 bit |
| Last Common Name | private_10_105_194_12 |
| Last SSL Connection Error | --No Last SSL Error-- |
| Last Connection Error | --No Last Error-- |
| Bytes Received | 78.3M |
| Bytes Sent | 3.85 |
| Number Of Connections | 2 |

Problembehandlung

Sehen Sie sich die **Erfolgs-/Fehlerinformationen für sichere Partner** auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung > WAN-Optimierung > Partner > Secure Partners** an.



| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|--------------|---------------|--------|---------------------|----------------|---------------------------|
| NoName-vgx | 172.16.194.3 | 10.105.194.12 | True | Connected Available | 10m 5s | 0m 4s |

| | |
|---------------------------|-------------------------------|
| Software Version | 9.2.0.105.379120 (Production) |
| Connection Initiator | true |
| SSL Cipher | ECDHE-RSA-AES256-SHA 256 bit |
| Last Common Name | private_10_105_194_3 |
| Last SSL Connection Error | --No Last SSL Error-- |
| Last Connection Error | --No Last Error-- |
| Bytes Received | 4.35 |
| Bytes Sent | 67.2M |
| Number Of Connections | 1 |

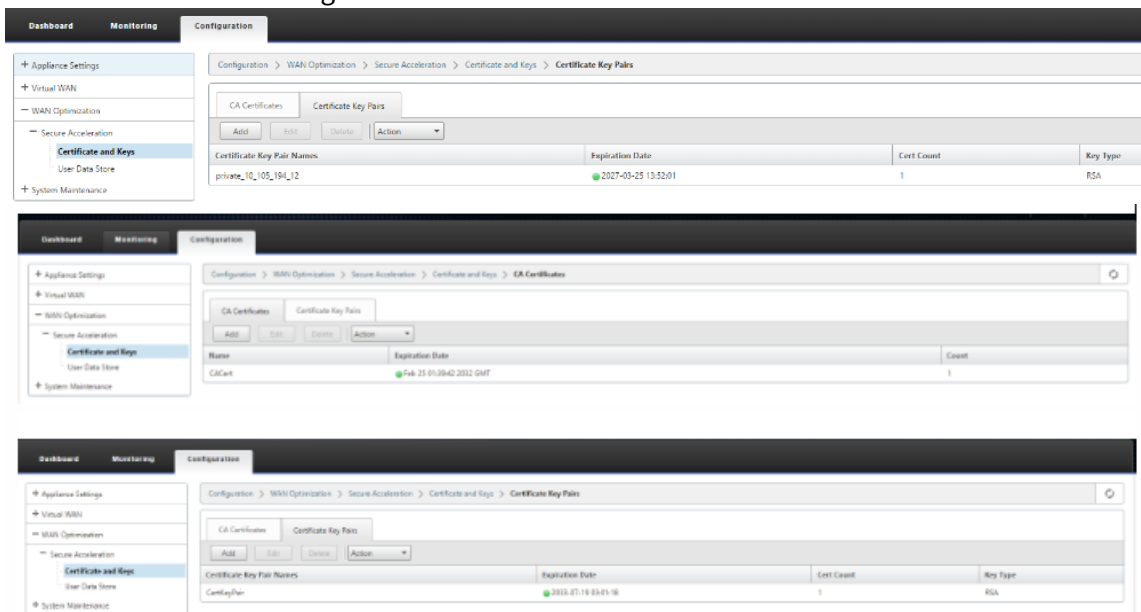
| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accelerated Connections | Max Active Connections | Max Connections | Idle | Instance IP |
|----------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|-------|----------------|
| 1 10.105.194.3 | 87.21 MB | 4.22 GB | 241.00 tps | 704.40 tps | 1 | 3 | 6 | 0m 3s | Not Applicable |

Manuelles Secure Peering von der PE-Appliance am DC-Standort in Zweigstelle Standalone SD-WAN SE und WANOP Appliance initiiert

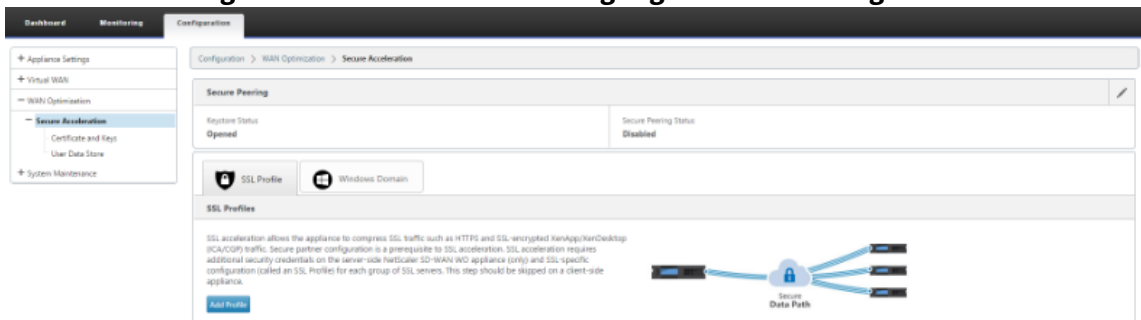
May 10, 2021

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443).
- Die Zweig-PE-Appliance befindet sich im CONNECT-TO-Modus.
- LISTEN-ON IP for PE befindet sich in der Schnittstellen-IP, die der Routingdomäne zugeordnet ist, für die “Redirect to WANOP” aktiviert ist.
- Laden Sie CA- und Cert Key-Paare Zertifikate manuell hoch, die von authentischer Quelle der Zertifizierungsstelle erhalten wurden.

1. Laden Sie **CA-Zertifikat** und **CA-Schlüsselzertifikat** aus authentischem Zertifikat und stellen Sie SD-WAN wie unten dargestellt hoch.



2. Wechseln Sie auf einer neuen PE (Premium Edition) -Appliance am DC-Standort in der SD-WAN-Web-GUI zu **Konfiguration > Sichere Beschleunigung > Secure Peering**.



3. Aktivieren Sie den Keystore, indem Sie das **Keystore-Kennwort angeben** oder den Keystore deaktivieren.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password

DashboardMonitoringConfiguration

Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*
Open

☐ Change Keystore Password
☐ Disable Keystore Password
☐ Reset Keystore

SaveCancel

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

SaveCancel

4. Aktivieren Sie sicheres Peering, indem Sie das Optionsfeld **CA-Zertifikat** auswählen und hochgeladene CA- und CA-Schlüsselpaarzertifikate entsprechend bereitstellen, wie unten dargestellt.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☐ Private CA ☒ CA Certificate

Certificate/Key Pair Name
CAKeyPair

CA Certificate Store Name
CA

Certificate Verification*
Signature/Expiration

SSL Cipher Specification
IADH:!AECDH:!MD5:HIGH:@STRENGTH

☐ Edit Cipher Specification

SaveCancel

5. Bereitstellen der virtuellen IP des Remote-Computers zusammen mit Port 443, wie unten gezeigt.

Listen On and Connect To

Connect To
172.16.194.3:443

SaveCancel

Done

Listen On and Connect To

| | | | |
|-------------------------|---------------------------|-----------------------------------|----------------------------------|
| NAT IP published Yes | Auto Discovery Enabled | Listening On 172.20.194.11:443 | Connected to 172.16.194.3:443 |
|-------------------------|---------------------------|-----------------------------------|----------------------------------|

Done

Überwachen

1. Zeigen Sie Informationen zu sicheren Partnern auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > WAN-Optimierung > Partner** an.

Monitoring > WAN Optimization > Partners

System Information

Agent ID: 10.105.194.12

Secure Partners

| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|--------------|--------------|--------|---------------------|----------------|---------------------------|
| hostname-vpn | 172.16.194.3 | 10.105.194.3 | True | Connected Available | 10m 5s | 0m 5s |

Active Partners

| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accelerated Connections | Max Active Connections | Max Connections | Idle | Instance IP |
|--------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|-------|----------------|
| 1 | 87.25 MB | 4.22 GB | 241.60 bps | 704.60 bps | 1 | 3 | 6 | 0m 5s | Not Applicable |

2. Zeigen Sie auf der Partner-Appliance Secure Partner Informationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Partner > Sichere Partner** an.

Monitoring > WAN Optimization > Partners

System Information

Agent ID: 10.105.194.12

Secure Partners

| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|--------------|--------------|--------|---------------------|----------------|---------------------------|
| hostname-vpn | 172.16.194.3 | 10.105.194.3 | True | Connected Available | 2m 0s | 0m 13s |

Active Partners

| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accelerated Connections | Max Active Connections | Max Connections | Idle | Instance IP |
|--------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|-------|----------------|
| 1 | 87.25 MB | 4.22 GB | 241.60 bps | 704.60 bps | 1 | 3 | 6 | 0m 5s | Not Applicable |

Problembehandlung

1. Anzeigen von **Erfolgs- und Fehlerinformationen für sichere Partner** auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > WAN-Optimierung > Partner > Sichere Partner**.

System Information
Agent ID: 10.105.194.12

Secure Partners

| Partner Name | IP Address | Instance IP | Secure | Connection Status | Time Connected | Time Since Last Contacted |
|--------------|--------------|-------------|--------|---------------------|----------------|---------------------------|
| hostname-vpx | 172.16.194.3 | | True | Connected Available | 10m 4s | 0m 4s |

Software Version: 6.2.0.101.571315 (Production)
Connection Initiator: true
SSL Cipher: ECDHE-RSA-AES128-GCM-SHA-256 (a)
Last Common Name: private_10_105_194_3
Last SSL Connection Error: --No Last SSL Error--
Last Connection Error: --No Last Error--
Bytes Received: 420
Bytes Sent: 67284
Number Of Connections: 1

Active Partners

| Partner Unit | Total Send Bytes | Total Receive Bytes | Last Minute Send Rate | Last Minute Receive Rate | Accelerated Connections | Max Active Connections | Max Connections | Idle | Instance IP |
|----------------|------------------|---------------------|-----------------------|--------------------------|-------------------------|------------------------|-----------------|-------|----------------|
| 1 10.105.194.3 | 87.25 MB | 4.22 GB | 247.60 bps | 704.40 bps | 1 | 3 | 6 | 0m 5s | Not Applicable |

2. Zeigen Sie auf der Partner-Appliance **Secure Partner Information** auf der Premium (Enterprise) Edition-Appliance unter **Überwachung > Appliance-Leistung > Protokollierung** an.

Monitoring > Appliance Performance > Logging

| Record | Date/Time | Details |
|--------|-----------------------|--|
| 5356 | Mar 01, 2017 05:50:20 | syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client:IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5355 | Mar 01, 2017 05:49:20 | syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5354 | Mar 01, 2017 05:49:20 | syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"id":10.105.194.3}}} |
| 5353 | Mar 01, 2017 05:49:20 | syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client:IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5352 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5351 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"id":10.105.194.3}}} |
| 5350 | Mar 01, 2017 05:48:20 | syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client:IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5349 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5348 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"id":10.105.194.3}}} |
| 5347 | Mar 01, 2017 05:47:20 | syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client:IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5346 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5345 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"id":10.105.194.3}}} |
| 5344 | Mar 01, 2017 05:46:20 | syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client:IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5343 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5342 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"id":10.105.194.3}}} |
| 5341 | Mar 01, 2017 05:45:20 | syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client:IP: 127.0.0.1 -Method: GET -Resource: system_info |
| 5340 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success |
| 5339 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: PAVLOAD: {"params":{"system_info":{"id":10.105.194.3}}} |
| 5338 | Mar 01, 2017 05:44:20 | syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client:IP: 127.0.0.1 -Method: GET -Resource: system_info |

Domänenbeitritt und Delegieren der Benutzererstellung

May 10, 2021

So konfigurieren Sie die neue Premium (Enterprise) Edition (PE) -Appliance auf der Domänencontroller zu Windows-Domäne:

1. Wechseln Sie zu Windows-Domäne in der SD-WAN-Web-GUI, navigieren Sie zu **Konfiguration >**

Sichere Beschleunigung > und klicken Sie auf **Windows-Domäne beitreten.**

Configuration > Secure Acceleration

SSL Optimization status: ACTIVE
Disable

Secure Peering

Keystore Status: Opened
Secure Peering Status: Enabled

SSL Profile | Windows Domain

Windows Domain Join

When the appliance joins the Windows domain, and the Windows domain controller accepts the appliance as a delegate user, the appliance becomes a trusted member of the domain for certain functions. This allows the appliance to be declared a member of the domain's security infrastructure, which in turn allows the acceleration of authenticated and encrypted data streams using Windows protocols such as CIFS and MAPI. For the purposes of accelerating CIFS and MAPI, security delegation can be limited to the relevant services as part of the standard Windows delegation mechanism. This constrained delegation became available with Windows Server 2003.

Join Windows Domain

Branch Office | WAN | Datacenter

Windows Domain

Join the server-side NetScaler SD-WAN appliance to a domain that the Windows file server and Exchange server are a part of. Joining the domain makes the appliance a trusted member of the Windows security system.

Domain Name*
Check Domain Join

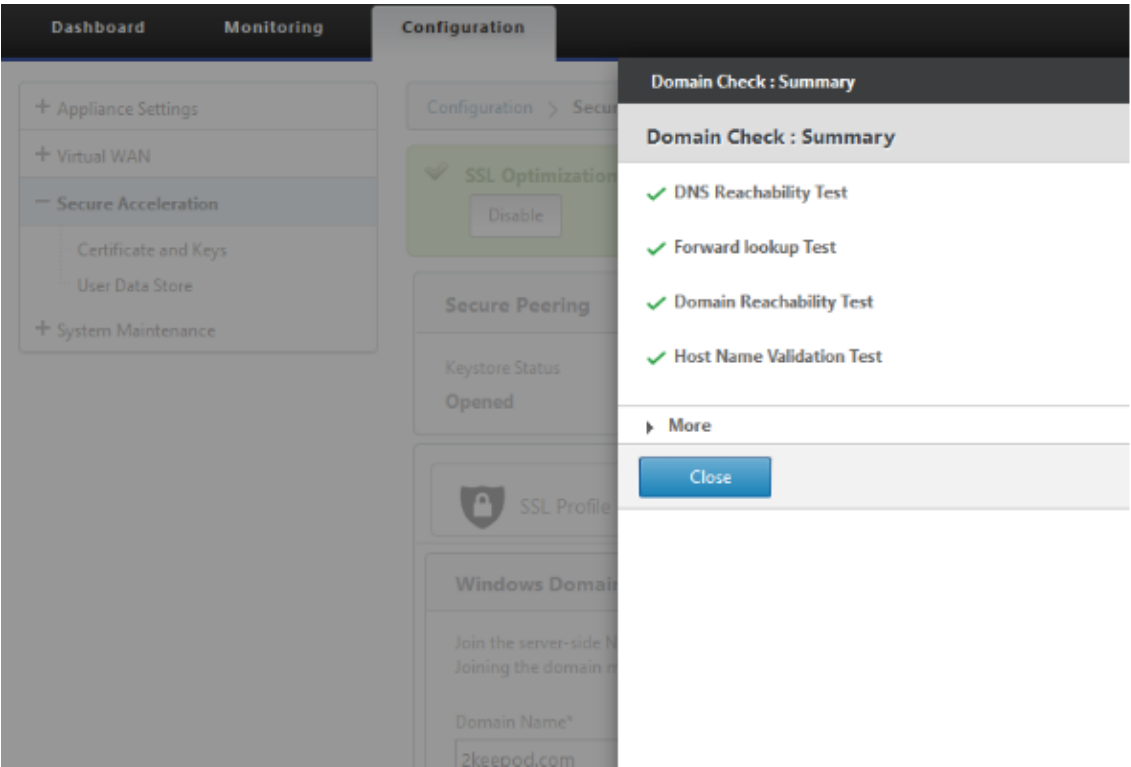
User Name*
Password*

☐ Leave Domain

DNS Servers*
10.105.194.17

OK Cancel

2. Geben Sie **Windows-Domännennamen** an und führen Sie Vorüberprüfungen für **Domänenbeitritte** durch.



3. Nachdem die Zusammenfassung der Überprüfung als erfolgreich angezeigt wird, geben Sie die Anmeldeinformationen des Domänencontrollers ein.

SSL Profile Windows Domain

Windows Domain

Join the server-side NetScaler SD-WAN appliance to a domain that the Windows file server and Exchange server are a part of. Joining the domain makes the appliance a trusted member of the Windows security system.

Domain Name*
2keepod.com [Check Domain Join](#)

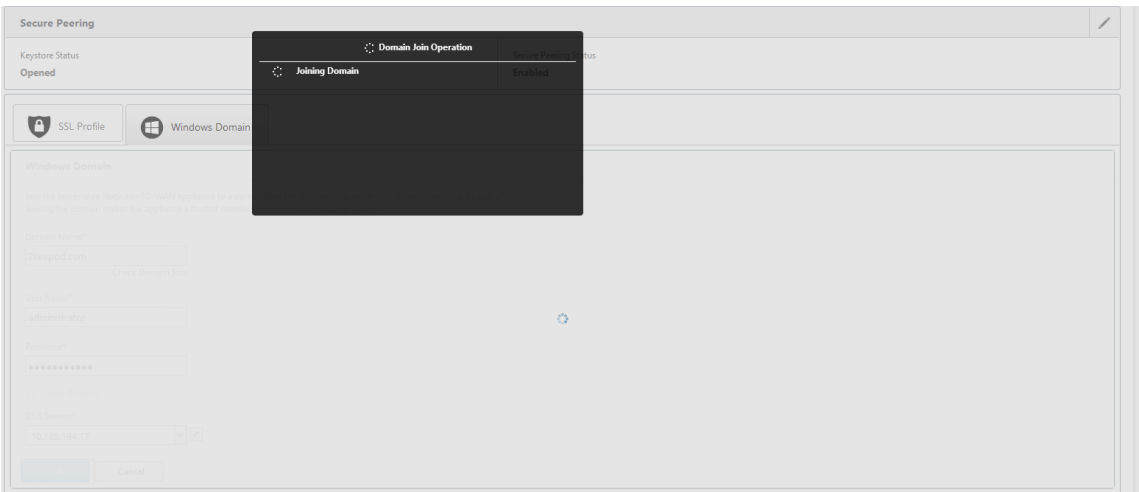
User Name*
administrator

Password*
•••••••• ⓘ

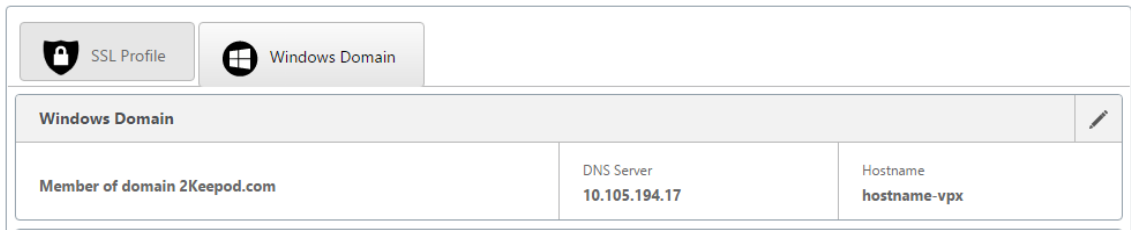
☐ Leave Domain

DNS Servers*
10.105.194.17 ✓

OK Cancel

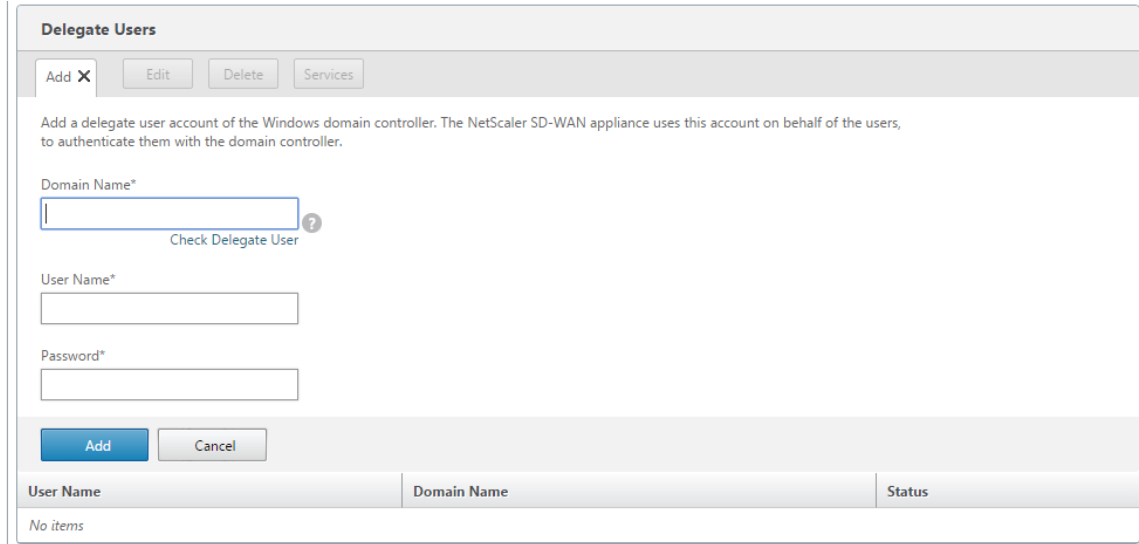


4. Bei erfolgreichem Domänenbeitritt erhalten Sie die folgende Ausgabe.



Benutzer delegieren

1. Fügen Sie delegierte Benutzer hinzu, um die Dienste zu delegieren, wie unten gezeigt.



2. Geben Sie den korrekten Domännennamen an und führen Sie die Vorprüfung des Delegatbenutzers durch.

Delegate Users

Add X Edit

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name*
2keepod.com

Check Delegate User

User Name*
userdel

Password*

Add Cancel

Delegate User Domain Check

Trying to validate Delegate User Domain ...

Delegate User Check : Summary

Delegate User Check : Summary

- ✓ DNS Reachability Test
- ✓ Forward lookup Test
- ✓ Domain Reachability Test
- ⚠ Host Name Validation Test
- ✓ Kerberos config file check
- ⚠ Reverse lookup zone
- ✓ Time Skew Check
- ✓ Kerberos Port Check
- ✓ NTP Port Check
- ✓ Server record for kerberos
- ✓ Server record for ldap

► More

Close

3. Nachdem die Vorüberprüfungen des delegierten Benutzers erfolgreich sind, geben Sie gültige

Anmeldeinformationen des delegierten Benutzers an.

Delegate Users

Add X
Edit
Delete
Services

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name*

Check Delegate User

User Name*

Password*

Add
Cancel

4. Nachdem delegierte Benutzer erfolgreich SD-WAN hinzugefügt wurde, sehen Sie eine Erfolgsmeldung.

| Delegate Users | | |
|---|-------------|---------|
| <div> Add ▼ Edit Delete Services </div> | | |
| User Name | Domain Name | Status |
| userdel | 2KEEPOD.COM | Success |

5. Um zu überprüfen, welche Dienste vom delegierten Benutzer delegiert werden, zeigen Sie auf den Benutzer, und wählen Sie Dienste aus.

Delegate User Details

Delegate User Details

Services

cifs/WIN-KJ8BEBRNRUD.2KEEPOD.COM/2KEEPOD.com
exchangeMDB/WIN-KJ8BEBRNRUD.2KEEPOD.COM

Close

Sicherheit

May 10, 2021

Die Themen in diesem Abschnitt enthalten allgemeine Sicherheitshinweise für Citrix SD-WAN Bereitstellungen.

Citrix SD-WAN Bereitstellungsrichtlinien

Um die Sicherheit während des Bereitstellungslebenszyklus aufrechtzuerhalten, empfiehlt Citrix folgende Sicherheitsüberlegungen:

- Physische Sicherheit
- Appliance-Sicherheit
- Netzwerksicherheit
- Verwaltung und Verwaltung

Die in den folgenden Links beschriebenen Themen enthalten weitere Informationen zum Konfigurieren der Sicherheit für SD-WAN-Netzwerke mit:

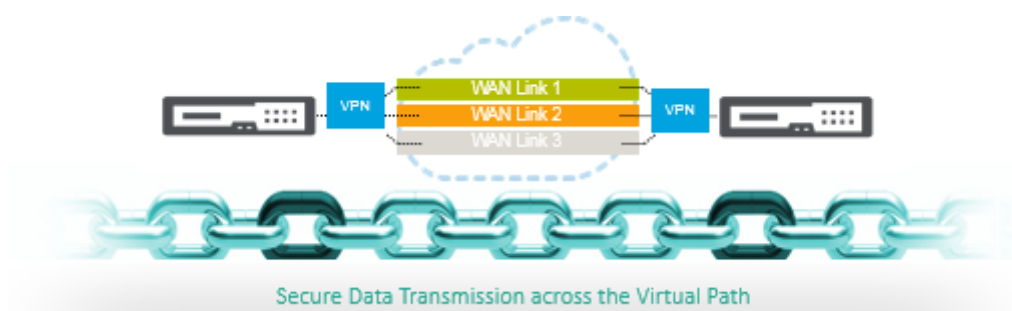
- [IPsec-Tunnel](#)
- [Firewall](#)

IPsec-Tunnelterminierung

May 10, 2021

Citrix SD-WAN unterstützt virtuelle IPsec-Pfade, sodass Geräte von Drittanbietern IPsec-VPN-Tunnel auf der LAN- oder WAN-Seite einer Citrix SD-WAN Appliance beenden können. Sie können Standort-zu-Site-IPsec-Tunnel sichern, die auf einer SD-WAN-Appliance beendet werden, indem Sie eine 140-2 Level 1 FIPS-zertifizierte IPsec-Kryptographikbinärdatei verwenden.

Citrix SD-WAN unterstützt auch das robuste IPsec-Tunneling mithilfe eines differenzierten virtuellen Pfadtunneling-Mechanismus.



Citrix SD-WAN Integration mit AWS Transit Gateway

May 10, 2021

Amazon Web Service (AWS) Transit Gateway Service ermöglicht es Kunden, ihre Amazon Virtual Private Clouds (VPCs) und ihre on-premises Netzwerke mit einem einzigen Gateway zu verbinden. Wenn die Anzahl der Workloads, die auf AWS ausgeführt werden, wächst, können Sie Ihre Netzwerke über mehrere Konten und Amazon VPCs hinweg skalieren, um mit dem Wachstum Schritt zu halten.

Sie können nun mit Peering Paare von Amazon VPCs verbinden. Die Verwaltung von Punkt-zu-Punkt-Konnektivität über viele Amazon VPCs hinweg, ohne die Möglichkeit, die Konnektivitätsrichtlinien zentral zu verwalten, kann jedoch kostspielig und umständlich sein. Für die lokale Konnektivität müssen Sie Ihr AWS-VPN an jede einzelne Amazon VPC anhängen. Diese Lösung kann zeitaufwändig zu erstellen und schwer zu verwalten sein, wenn die Anzahl der VPCs auf Hunderte ansteigt.

Mit **AWS Transit Gateway** müssen Sie nur eine einzige Verbindung vom zentralen Gateway zu jeder Amazon VPC, jedem on-premises Rechenzentrum oder jedem Remote-Büro in Ihrem Netzwerk erstellen und verwalten. Das Transit Gateway fungiert als Hub, der steuert, wie der Datenverkehr zwischen allen angeschlossenen Netzwerken geleitet wird, die sich wie Speichen verhalten. Dieses Hub- und Spoke-Modell vereinfacht die Verwaltung erheblich und senkt die Betriebskosten, da jedes Netzwerk nur eine Verbindung zum Transit Gateway und nicht zu jedem anderen Netzwerk herstellen muss. Jede neue VPC ist mit dem Transit Gateway verbunden und steht automatisch jedem anderen Netzwerk zur Verfügung, das mit dem Transit Gateway verbunden ist. Diese einfache Konnektivität erleichtert die Skalierung Ihres Netzwerks während des Wachstums.

Wenn Unternehmen eine wachsende Anzahl von Anwendungen, Services und Infrastrukturen in die Cloud migrieren, stellen sie schnell SD-WAN bereit, um die Vorteile der Breitbandkonnektivität zu nutzen und Benutzer von Zweigstellen direkt mit Cloud-Ressourcen zu verbinden. Es gibt viele Herausforderungen in Bezug auf die Komplexität des Aufbaus und Managements globaler privater Netzwerke mit Internet-Transportdiensten, um geografisch verteilte Standorte und Benutzer mit nahebasierenden Cloud-Ressourcen zu verbinden. Der **AWS Transit Gateway Network Manager** ändert dieses Paradigma. Citrix SD-WAN-Kunden, die AWS verwenden, können jetzt Citrix SD-WAN mit AWS Transit Gateway verwenden, indem sie die Citrix SD-WAN-Zweigstellen-Appliance AWS Transit Gateway integrieren, um Benutzern mit der Möglichkeit, alle mit dem Transit Gateway verbundenen VPCs zu erreichen.

Im Folgenden werden die Schritte beschrieben, um Citrix SD-WAN mit AWS Transit Gateway zu integrieren:

1. Erstellen Sie das AWS Transit Gateway.
2. Verbinden Sie ein VPN mit dem Transit Gateway (entweder vorhandenes oder ein neues VPN).
3. Verbinden Sie VPN mit dem konfigurierten Transit Gateway, an dem sich das VPN mit dem SD-WAN-Site befindet, der sich On-Prem oder in einer beliebigen Cloud befindet (AWS, Azure oder GCP).
4. Stellen Sie das Border Gateway Protocol (BGP) Peering über den IPsec-Tunnel mit dem AWS Transit Gateway von Citrix SD-WAN ein, um die mit Transit Gateway verbundenen Netzwerke

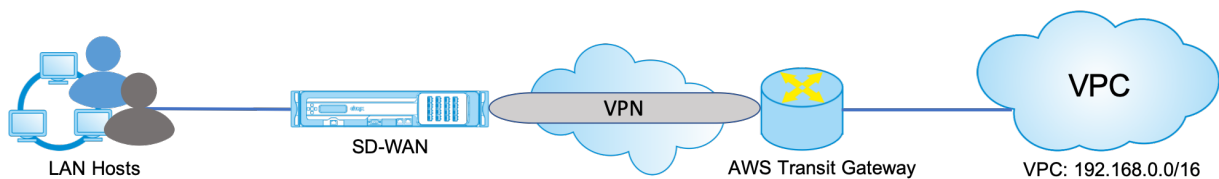
(VPCs) zu lernen.

Anwendungsfall

Der Anwendungsfall besteht darin, Ressourcen, die in AWS (in jeder VPC) bereitgestellt werden, aus der Zweigstellenumgebung zu erreichen. Mit AWS Transit Gateway kann der Datenverkehr zu allen VPCs gelangen, die mit dem Transit Gateway verbunden sind, ohne BGP-Routen zu behandeln. Um dies zu erreichen, führen Sie die folgenden Methoden aus:

- Richten Sie die IPsec to AWS Transit Gateway über die Zweigstelle Citrix SD-WAN Appliance ein. Bei dieser Bereitstellungsmethode erhalten Sie keine vollständigen SD-WAN-Vorteile, da der Datenverkehr über IPsec geht.
- Stellen Sie eine Citrix SD-WAN Appliance in AWS bereit, und verbinden Sie sie über einen virtuellen Pfad mit Ihrer lokalen Citrix SD-WAN Appliance.

Unabhängig davon, welche Methode gewählt wird, erreicht der Datenverkehr zu den VPCs, die mit dem Transit Gateway verbunden sind, ohne das Routing innerhalb von AWS infra manuell zu verwalten.

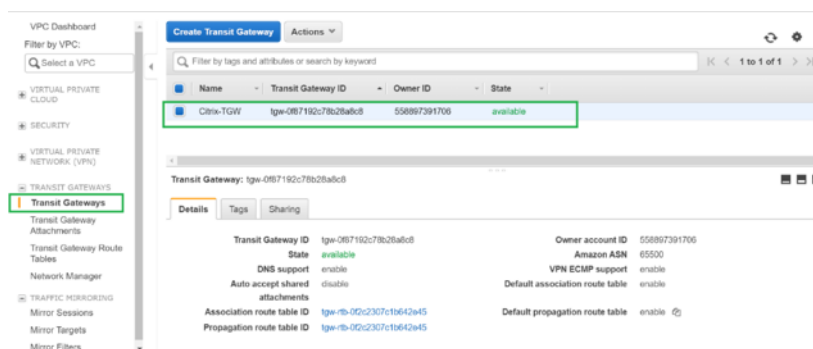


Konfiguration von AWS Transit Gateway

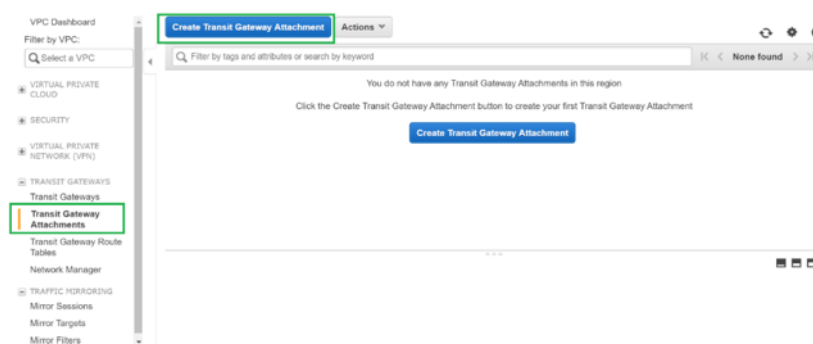
Um das **AWS Transit Gateway** zu erstellen, navigieren Sie zum VPC-Dashboard und wechseln Sie zum Abschnitt **Transit Gateway**.

1. Geben Sie den Transit Gateway-Namen, die Beschreibung und die Amazon-ASN-Nummer wie im folgenden Screenshot hervorgehoben an, und klicken Sie auf **Transit Gateway erstellen**.

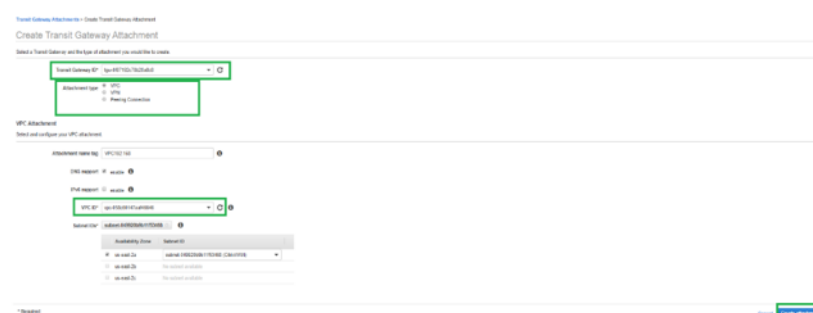
Sobald die Transit Gateway-Erstellung abgeschlossen ist, können Sie den Status als **Verfügbar** sehen.



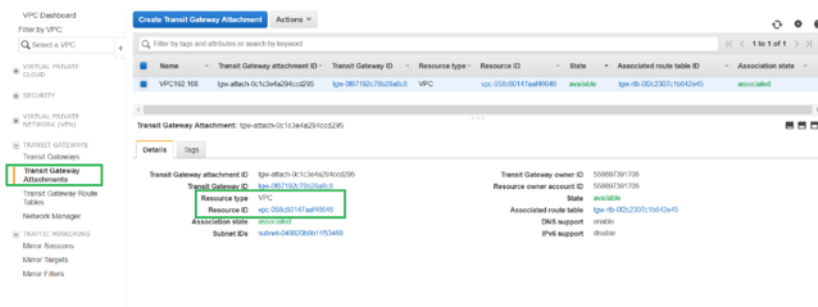
- Um die **Transit Gateway-Anhänge** zu erstellen, navigieren Sie zu **Transit Gateways > Transit Gateway Attachments** und klicken Sie auf **Transit-Gateway-Anlage erstellen**



- Wählen Sie das Transit Gateway aus der Dropdown-Liste aus und wählen Sie Anhangstyp als **VPC** aus. Geben Sie das Namens-Tag für die Anlage an, und wählen Sie die VPC-ID aus, die Sie an das erstellte Transit Gateway anhängen möchten. Eines der Subnetze der ausgewählten VPC wird automatisch ausgewählt. Klicken Sie auf **Anlage erstellen**, um VPC an das Transit-Gateway anzuhängen.

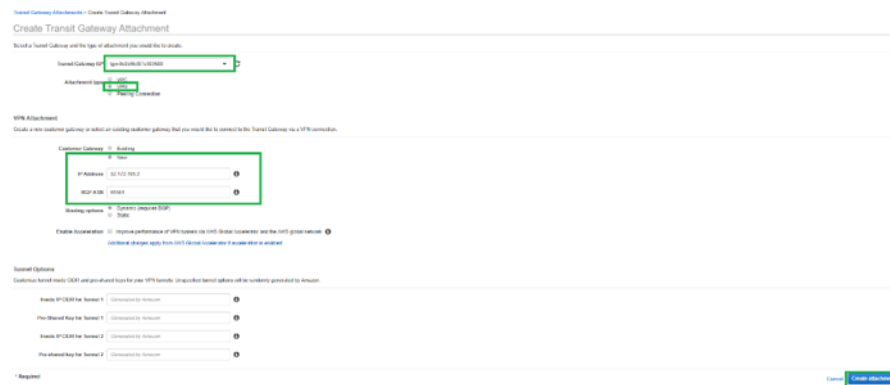


- Nachdem Sie die VPC an das Transit-Gateway angeschlossen haben, können Sie sehen, dass die **VPC des Ressourcentyps** mit dem Transit-Gateway verknüpft wurde.

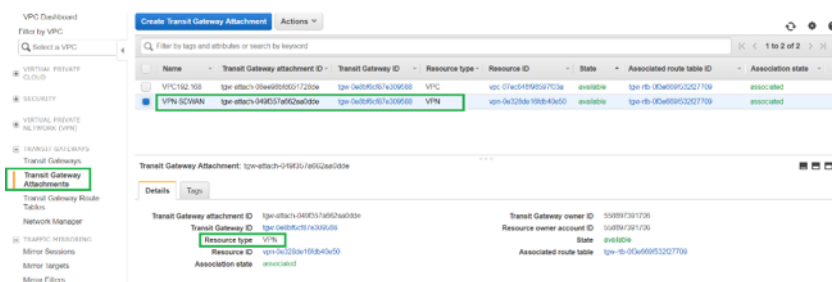


5. Um SD-WAN über VPN an das Transit Gateway anzuschließen, wählen Sie die **Transit Gateway-ID** aus der Dropdown-Liste aus und wählen Sie **Anhangstyp** als **VPN** aus. Stellen Sie sicher, dass Sie die richtige Transit Gateway ID auswählen.

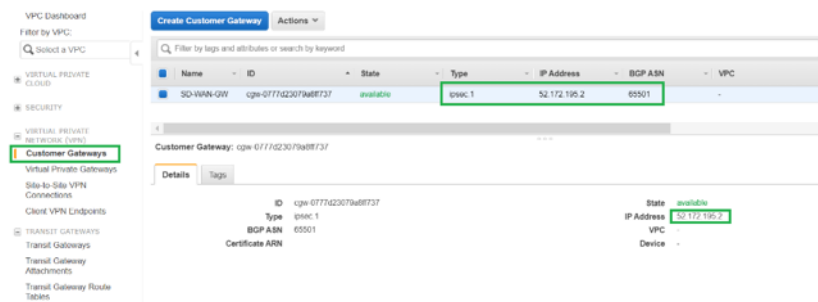
Fügen Sie ein neues VPN Customer Gateway hinzu, indem Sie die öffentliche IP-Adresse des SD-WAN-Links und die BGP-ASN-Nummer angeben. Klicken Sie auf **Anlage erstellen**, um VPN mit Transit Gateway zu verbinden.



6. Sobald das VPN an das Transit Gateway angeschlossen ist, können Sie die Details sehen, wie im folgenden Screenshot gezeigt:

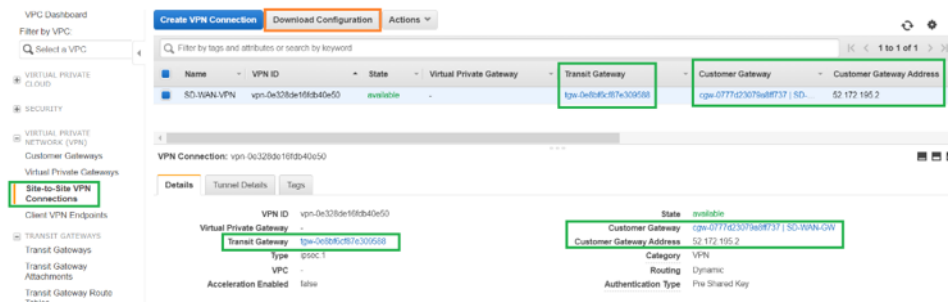


7. Unter **Customer Gateways** werden SD-WAN Customer Gateway und Site-to-Site VPN Connection als Teil von VPN Attachment to Transit Gateway erstellt. Sie sehen, dass das SD-WAN Customer Gateway zusammen mit der IP-Adresse dieses Customer Gateways erstellt wird, das die öffentliche WAN-Link-IP-Adresse von SD-WAN darstellt.

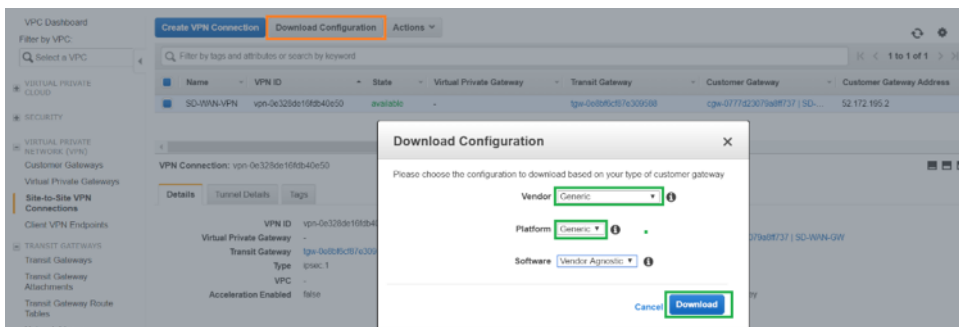


8. Navigieren Sie zu **Site-to-Site VPN Connections**, um die **VPN-Konfiguration des SD-WAN-Kunden-Gateways**. Diese Konfigurationsdatei enthält zwei IPsec-Tunneldetails zusammen mit den BGP-Peer-Informationen. Zwei Tunnel werden aus SD-WAN zu Transit Gateway für Redundanz erstellt.

Sie können sehen, dass die öffentliche IP-Adresse des SD-WAN WAN-Links als Kundengateway-Adresse konfiguriert wurde.



9. Klicken Sie auf **Konfiguration herunterladen** und laden Sie die VPN-Konfigurationsdatei herunter. Wählen Sie den **Anbieter**, die **Plattform** als **Generic** und **Software** as **Vendor Agnostic**.



Die heruntergeladene Konfigurationsdatei enthält die folgenden Informationen:

- IKE-Konfiguration
- IPsec-Konfiguration für AWS Transit Gateway
- Konfiguration der Tunnelschnittstelle
- BGP-Konfiguration

Diese Informationen stehen für zwei IPsec-Tunnel für hohe Verfügbarkeit (HA) zur Verfügung. Stellen Sie sicher, dass Sie beide Tunnelendpunkte konfigurieren, während Sie dies in SD-WAN konfigurieren. Siehe den folgenden Screenshot als Referenz:

#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is associated with the IPsec tunnel. All traffic transmitted to the tunnel interface is encrypted and transmitted to the Virtual Private Gateway.

The Customer Gateway and Virtual Private Gateway each have two addresses that relate to this IPsec tunnel. Each contains an outside address, upon which encrypted traffic is exchanged. Each also contain an inside address associated with the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway was created. Changing the IP address requires the creation of a new Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel interface.

Outside IP Addresses:

- Customer Gateway : 52.172.195.2
- Virtual Private Gateway : 3.133.37.22

Inside IP Addresses:

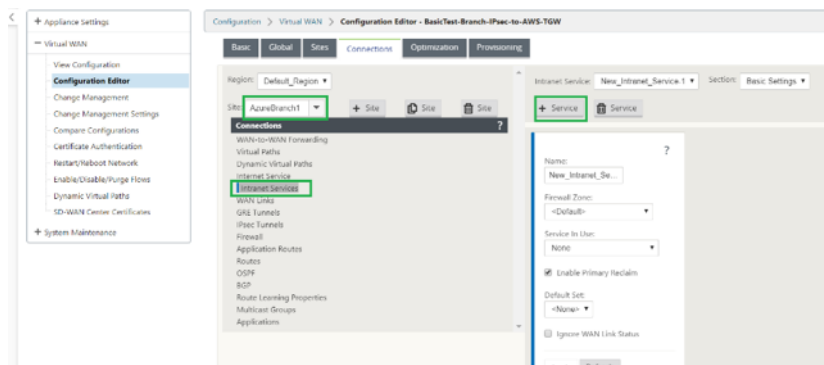
- Customer Gateway : 169.254.216.178/30
- Virtual Private Gateway : 169.254.216.177/30

Configure your tunnel to fragment at the optimal size:

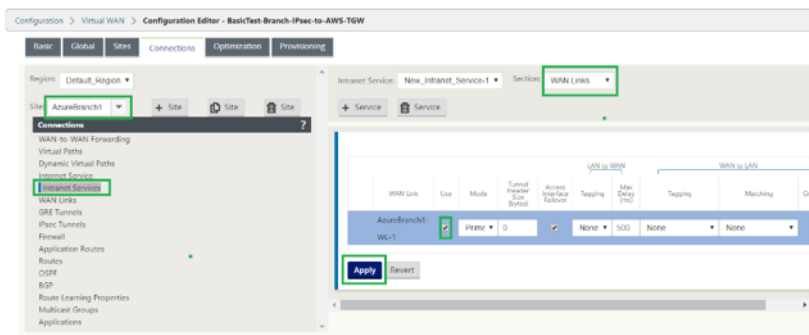
- Tunnel interface MTU : 1436 bytes

Konfigurieren des Intranetdienstes auf SD-WAN

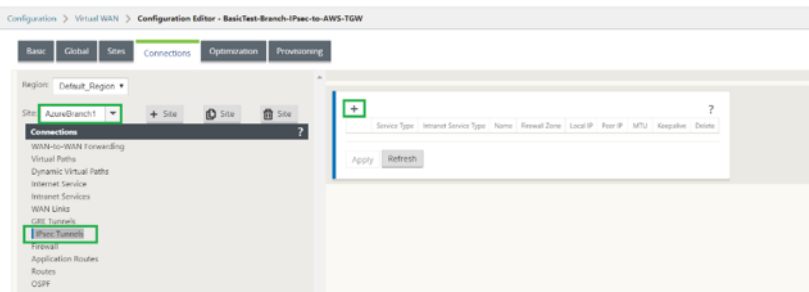
- Um den Intranetdienst zu konfigurieren, der in der IPsec-Tunnelkonfiguration auf SD-WAN verwendet wird, navigieren Sie zu **Konfigurations-Editor > Verbindungen**, wählen Sie die Site aus der Dropdown-Liste aus und wählen Sie **Intranetdienst** aus. Klicken Sie auf **+ Service**, um einen neuen Intranetdienst hinzuzufügen.



- Wählen Sie nach dem Hinzufügen des Intranetdienstes die WAN-Verbindung (mit der Sie den Tunnel zum Transit-Gateway einrichten möchten) aus, die für diesen Dienst verwendet wird.

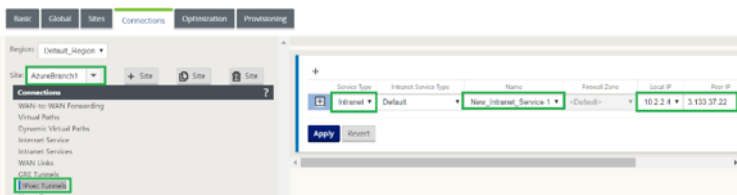


3. Um den IPsec-Tunnel in Richtung AWS Transit Gateway zu konfigurieren, navigieren Sie zu **Configuration Editor > Verbindungen** wählen Sie die Site aus der Dropdown-Liste aus und klicken Sie auf **IPsec-Tunnels**. Klicken Sie auf **+**, um IPsec-Tunnel hinzuzufügen.



4. Wählen Sie den **Diensttyp** als **Intranet** aus und wählen Sie den **Namen des Intranetdienstes** aus, den Sie hinzugefügt haben. Wählen Sie die **lokale IP-Adresse** als WAN-Link-IP-Adresse und **Peer-Adresse** als Transit Gateway Virtual Private Gateway IP-Adresse aus.

Klicken Sie auf das Kontrollkästchen **Keepalive**, damit der Tunnel sofort nach der Aktivierung der Konfiguration von SD-WAN initiiert wird.



5. Konfigurieren Sie IKE-Parameter basierend auf der VPN-Konfigurationsdatei, die Sie von AWS heruntergeladen haben.

| Service Type | Intranet Service Type | Name | Firewall Zone | Local IP | Peer IP |
|--------------|-----------------------|------------------------|---------------|----------|-------------|
| Intranet | Default | New_Intranet_Service-1 | <Default> | 10.2.2.4 | 3.133.37.22 |

IKE Settings

Version: IKEv1
Mode: Main
Identity: Auto
Authentication: Pre-Shared Key
Pre-Shared Key: ••••••••••••••••
☒ Validate Peer Identity
Peer Identity: Auto
DH Group: Group 2 (MODP1024)
Hash Algorithm: SHA1
Encryption Mode: AES 128-Bit
Lifetime (s): 3600
Lifetime (s) Max: 86400
DPD Timeout (s): 300

6. Konfigurieren Sie IPsec-Parameter basierend auf der VPN-Konfigurationsdatei, die Sie von AWS heruntergeladen haben. Konfigurieren Sie **IPsec-geschützte Netzwerke** auch basierend auf dem Netzwerk, das Sie durch den Tunnel senden möchten. Sie können sehen, dass es so konfiguriert ist, dass jeder Datenverkehr über den IPsec-Tunnel zugelassen wird.

IPsec Settings

Tunnel Type: ESP+Auth
PFS Group: Group 2 (MODP1024)
Encryption Mode: AES 128-Bit
Hash Algorithm: SHA1
Lifetime (s): 28800
Lifetime (s) Max: 86400
Lifetime (KB): 0
Lifetime (KB) Max: 0
Network Mismatch Behavior: Drop

IPsec Protected Networks + Add

| Source IP/Prefix | Destination IP/Prefix |
|------------------|-----------------------|
| 0.0.0.0/0 | 0.0.0.0/0 |

Apply Revert

7. Konfigurieren Sie die **IP-Adresse des Customer Gateway** als eine der virtuellen IP-Adressen auf SD-WAN. Suchen Sie in der heruntergeladenen VPN-Konfigurationsdatei das Kundengateway innerhalb der IP-Adresse, die sich auf Tunnel-1 bezieht. Konfigurieren Sie dieses Kundengateway innerhalb der IP-Adresse als eine der virtuellen IP-Adressen auf SD-WAN und aktivieren Sie das Kontrollkästchen **Identität**.

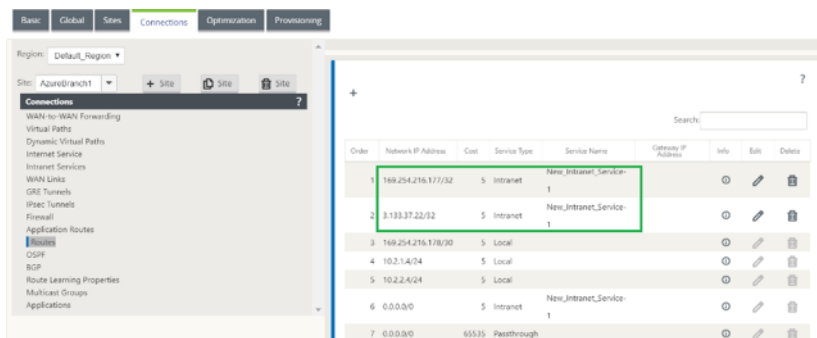
Basic Global Sites Connections Optimization Provisioning

Region: Default_Region
Site: AzureBranch1
Virtual IP Addresses

| IP Address / Prefix | Virtual Interface | Firewall Zone | Identity | Related VPN | Private | Security | Delete |
|---------------------|-------------------|------------------|-------------------------------------|--------------------------|--------------------------|----------|--------|
| 10.2.1.4/24 | LAN | Default_LAN_Zone | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Trusted | |
| 10.2.2.4/24 | WAN | Default_LAN_Zone | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Trusted | |
| 10.2.3.1/24 | LAN | Default_LAN_Zone | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Trusted | |

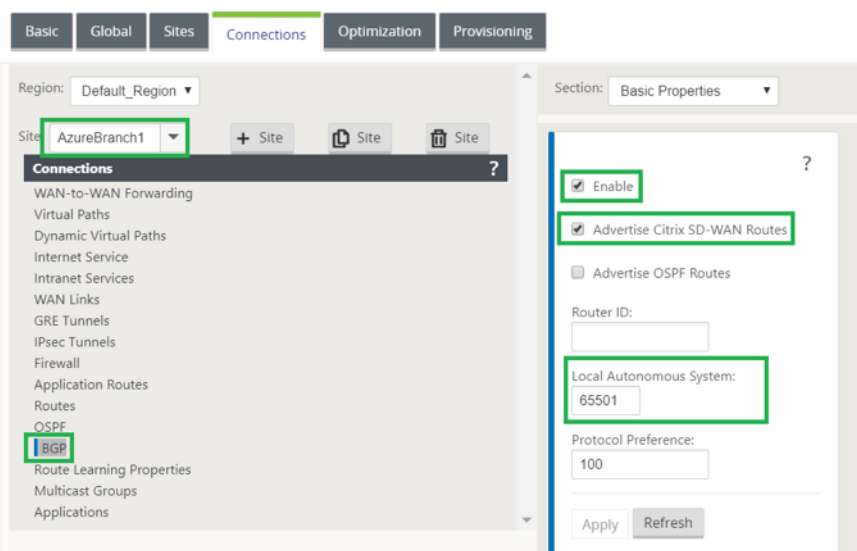
Backup Management Network: <None>
Apply Refresh

8. Fügen Sie **Routen** auf SD-WAN hinzu, um **Virtual Private Gateway** von Transit Gateway zu erreichen. Suchen Sie in der heruntergeladenen VPN-Konfigurationsdatei innerhalb und außerhalb der IP-Adresse von Virtual Private Gateway im Zusammenhang mit Tunnel-1. Fügen Sie Routen zur inneren und äußeren IP-Adresse von Virtual Private Gateway mit **Service Type** als **Intranet** hinzu und wählen Sie den in den obigen Schritten erstellten Intranetdienst aus.



9. Konfigurieren Sie **BGP** auf SD-WAN. Aktivieren Sie BGP mit der entsprechenden ASN-Nummer. Suchen Sie in der heruntergeladenen VPN-Konfigurationsdatei die BGP-Konfigurationsoptionen im Zusammenhang mit Tunnel-1. Verwenden Sie diese Details, um BGP Neighbor auf SD-WAN hinzuzufügen.

Um BGP auf SD-WAN zu aktivieren, navigieren Sie zu **Verbindungen** wählen Sie die Site aus der Dropdown-Liste und wählen Sie dann **BGP** aus. Klicken Sie auf **Aktivieren**, um BGP zu aktivieren. Aktivieren Sie das Kontrollkästchen **Citrix SD-WAN Routes** ankündigen, um SD-WAN Routen in Richtung Transit Gateway zu machen. Verwenden Sie die **Customer Gateway-ASN** aus den BGP-Konfigurationsoptionen und konfigurieren Sie diese als **Lokales autonomes System**.



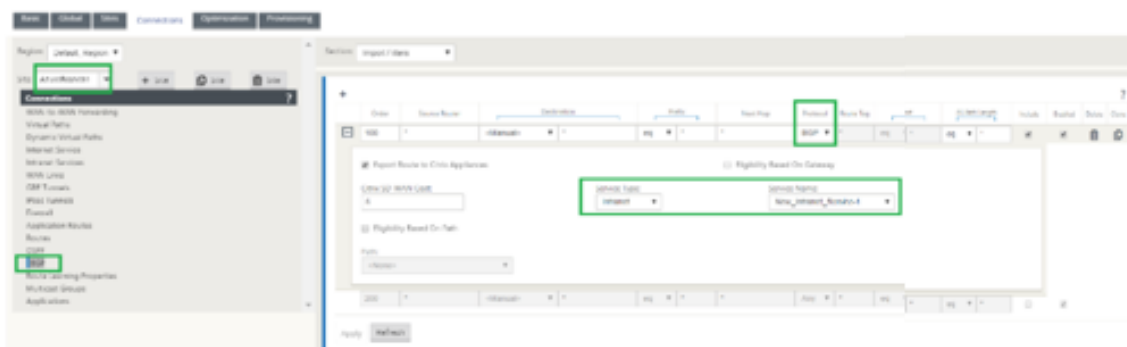
10. Um **BGP-Nachbarn** auf SD-WAN hinzuzufügen, navigieren Sie zu **Verbindungen** wählen Sie die Site aus der Dropdown-Liste aus und wählen Sie dann **BGP** aus. Klicken Sie auf den Abschnitt

Nachbarn und klicken Sie auf **+** Option.

Verwenden Sie **Neighbor IP Address** und **Virtual Private Gateway ASN** aus den BGP-Konfigurationsoptionen, während Sie Nachbarn hinzufügen. Die **Quell-IP** muss mit der IP-Adresse des **Kunden-Gateways** (Konfiguriert als virtuelle IP-Adresse auf SD-WAN) aus der heruntergeladenen Konfigurationsdatei von AWS übereinstimmen. Fügen Sie BGP Neighbor mit aktiviertem **Multi-Hop** für SD-WAN hinzu.



- Um **Importfilter** zum Importieren von BGP-Routen in SD-WAN hinzuzufügen, navigieren Sie zu **Verbindungen**, wählen Sie die Site aus der Dropdown-Liste aus, wählen Sie dann **BGP** aus und klicken Sie auf **Filter importieren**. Klicken Sie auf **+**, um einen Importfilter hinzuzufügen. Wählen Sie das **Protokoll** als **BGP** aus und passen Sie es an, um alle BGP-Routen zu importieren. Wählen Sie den **Diensttyp** als **Intranet** aus und wählen Sie den erstellten Intranetdienst aus. Dies ist, um BGP-Routen mit Service-Typ als Intranet zu importieren.



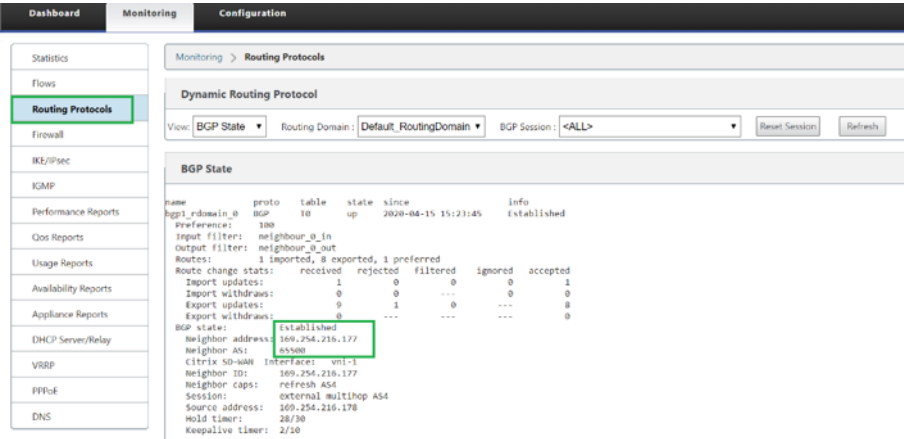
Überwachung und Fehlerbehebung auf SD-WAN

- Um den Status der IPsec-Tunneleinrichtung auf SD-WAN zu überprüfen, navigieren Sie zu **Monitoring > Statistics > IPsec-Tunnel**. Im folgenden Screenshot können Sie sehen, dass der IPsec-Tunnel von SD-WAN in Richtung AWS Transit Gateway eingerichtet wird und der Status **GOOD** ist. Außerdem können Sie die Menge des über diesen IPsec-Tunnel gesendeten und empfangenen Datenverkehrs überwachen.

! [Überwachung und Fehlerbehebung auf SD-WAN] (/en-us/citrix-sd-wan/11-2/media/monitoring-and-troubleshooting-on-sdwan.png)

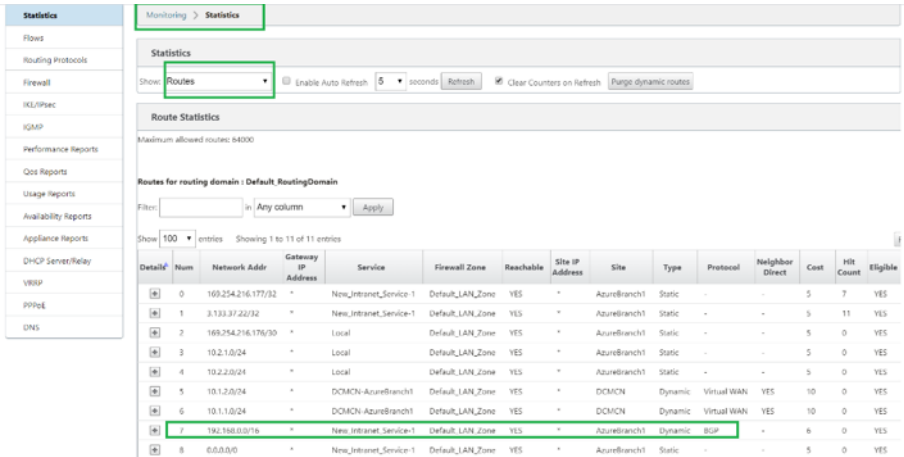
- Um den **BGP Peering-Status** auf SD-WAN zu überprüfen, navigieren Sie zu **Monitoring > Routing Protocols** und wählen Sie **BGP State** aus. Sie können sehen, dass der BGP-Status

als **Etabliert** gemeldet wurde und die **Nachbar-IP-Adresse** und die **Nachbar-ASN** den AWS BGP-Nachbardetails entsprechen. Damit können Sie sicherstellen, dass das BGP Peering von SD-WAN zu AWS Transit Gateway über IPsec-Tunnel etabliert wurde.



Eine VPC (192.168.0.0) ist mit AWS Transit Gateway verbunden. SD-WAN hat dieses VPC-Netzwerk (192.168.0.0) von AWS Transit Gateway über BGP gelernt. Und diese Route wurde auf SD-WAN mit Servicetyp als Intranet gemäß dem in den obigen Schritten erstellten Importfilter installiert.

- Um die BGP-Routeninstallation auf SD-WAN zu überprüfen, navigieren Sie zu **Monitoring > Statistics > Routes** und suchen Sie nach dem Netzwerk 192.168.0.0/16, das als BGP-Route mit Servicetyp als Intranet installiert wurde. Dies bedeutet, dass Sie die Netzwerke lernen können, die mit AWS Transit Gateway verbunden sind, und können mit diesen Netzwerken über IPsec-Tunnel kommunizieren.



Überwachung und Fehlerbehebung in AWS

- Um den Status der IPsec-Tuneleinrichtung auf AWS zu überprüfen, navigieren Sie zu **VIRTUAL PRIVATE NETWORK (VPN) > Site-to-Site VPN-Verbindungen**. Im folgenden Screenshot kön-

nen Sie beobachten, dass die Customer Gateway-Adresse SD-WAN Link öffentliche IP-Adresse darstellt, mit der Sie Tunnel eingerichtet haben.

Der Tunnelstatus wird als **UP** angezeigt. Es ist auch zu beobachten, dass AWS **8 BGP ROUTES** von SD-WAN gelernt hat. Dies bedeutet, dass SD-WAN in der Lage ist, Tunnel mit AWS Transit Gateway zu etablieren und auch Routen über BGP austauschen zu können.

The screenshot shows the AWS VPC console. On the left, the 'Site-to-Site VPN Connections' link is highlighted. The main panel shows a list of VPN connections. The 'SD-WAN VPN' connection is selected, and its 'Tunnel Details' tab is active. Below the tab, the 'Tunnel State' section displays a table with two tunnels.

| Tunnel Number | Outside IP Address | Inside IP CIDR | Status | Status Last Changed | Details | Certificate ARN |
|---------------|--------------------|--------------------|--------|---------------------------------------|---------------|-----------------|
| Tunnel 1 | 3.133.37.22 | 199.254.215.176/30 | UP | April 15, 2020 at 8:54:05 PM UTC+5:30 | 8 BGP ROUTES | |
| Tunnel 2 | 13.58.06.194 | 199.254.133.240/30 | DOWN | April 15, 2020 at 12:03:49 PM UTC+ | IPSEC IS DOWN | |

2. Konfigurieren Sie IPsec- und BGP-Details im Zusammenhang mit dem zweiten Tunnel basierend auf der heruntergeladenen Konfigurationsdatei auf SD-WAN.

Der Status, der sich auf beide Tunnel bezieht, kann auf SD-WAN wie folgt überwacht werden:

The screenshot shows the SD-WAN Monitoring page. The 'Statistics' tab is selected. Under 'IPsec Tunnel Statistics', a table displays the status of two tunnels.

| Name | Status | Service Type | Packets Received | Kbps Received | Packets Sent | Kbps Sent | Packets Dropped | Bytes Dropped | MTU |
|------------------------|--------|--------------|------------------|---------------|--------------|-----------|-----------------|---------------|------|
| New_Intranet_Service-1 | GOOD | Intranet | 1 | 0.27 | 1 | 0.24 | 0 | 0 | 1434 |
| New_Intranet_Service-2 | GOOD | Intranet | 1 | 0.27 | 1 | 0.24 | 0 | 0 | 1434 |

3. Der Status, der sich auf beide Tunnel bezieht, kann in AWS wie folgt überwacht werden:

The screenshot shows the AWS VPC console, similar to the first screenshot. The 'SD-WAN VPN' connection is selected, and its 'Tunnel Details' tab is active. The 'Tunnel State' section displays a table with two tunnels.

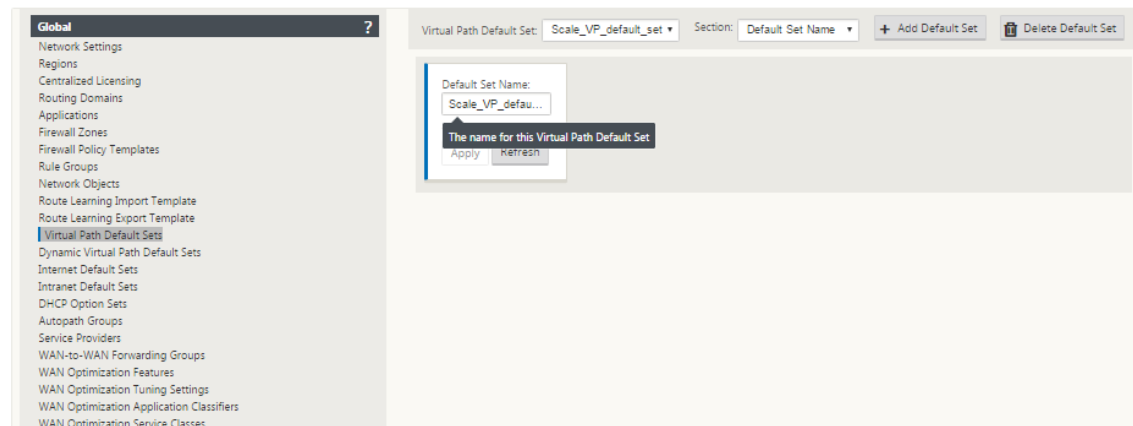
| Tunnel Number | Outside IP Address | Inside IP CIDR | Status | Status Last Changed | Details | Certificate ARN |
|---------------|--------------------|--------------------|--------|-----------------------------------|---------------|-----------------|
| Tunnel 1 | 3.133.37.22 | 199.254.215.176/30 | UP | Apr 16, 2020 at 11:58:30 AM UTC+5 | 11 BGP ROUTES | |
| Tunnel 2 | 13.58.06.194 | 199.254.133.240/30 | UP | Apr 16, 2020 at 11:57:30 AM UTC+5 | 11 BGP ROUTES | |

Konfigurieren von IPsec-Tunneln für virtuelle und dynamische Pfade

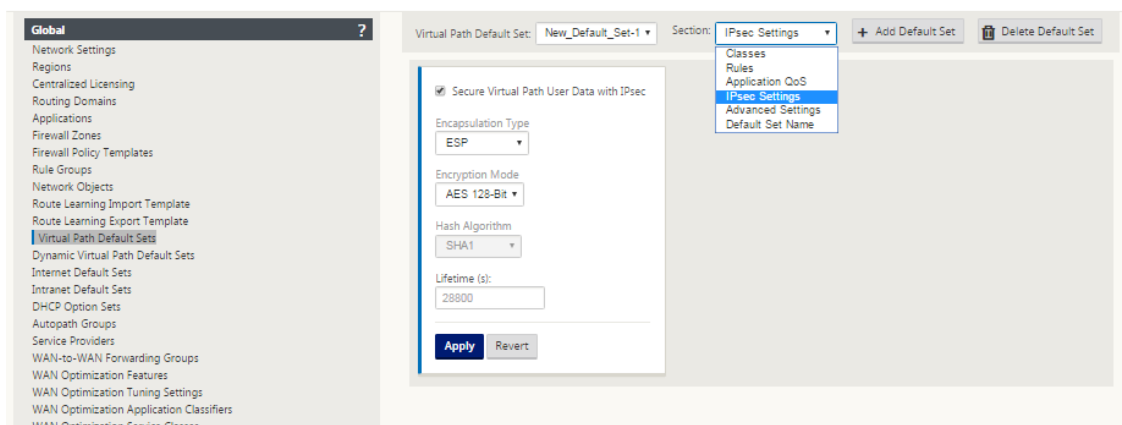
May 10, 2021

So konfigurieren Sie IPsec-Tunnel für virtuelle und dynamische virtuelle Pfade zwischen Citrix SD-WAN SD-WAN-Zweigstellen:

1. Navigieren Sie zu **Global > Virtual Path Default Sets** oder **Dynamic Virtual Path Default Sets**



2. Erstellen Sie einen neuen Standardsatz (virtueller oder dynamischer virtueller Pfad), und aktivieren Sie **Benutzerdaten für den sicheren virtuellen Pfad mit IPsec**.
3. Wählen Sie eine der verfügbaren Optionen für die IPsec-Verschlüsselung:
 - Verkapselungsarten: ESP, AH oder ESP+AH
 - Verschlüsselungsmodi: AES-CBC, AES 128 oder 256 Bit
 - Hash-Algorithmus: SHA1 oder SHA-256
4. Wenden Sie den erstellten Virtual Path Default Set auf den MCN-Knoten an. Dies wendet automatisch denselben Standardsatz auf alle Clientknoten an, die über einen virtuellen Pfad zum MCN verfügen.

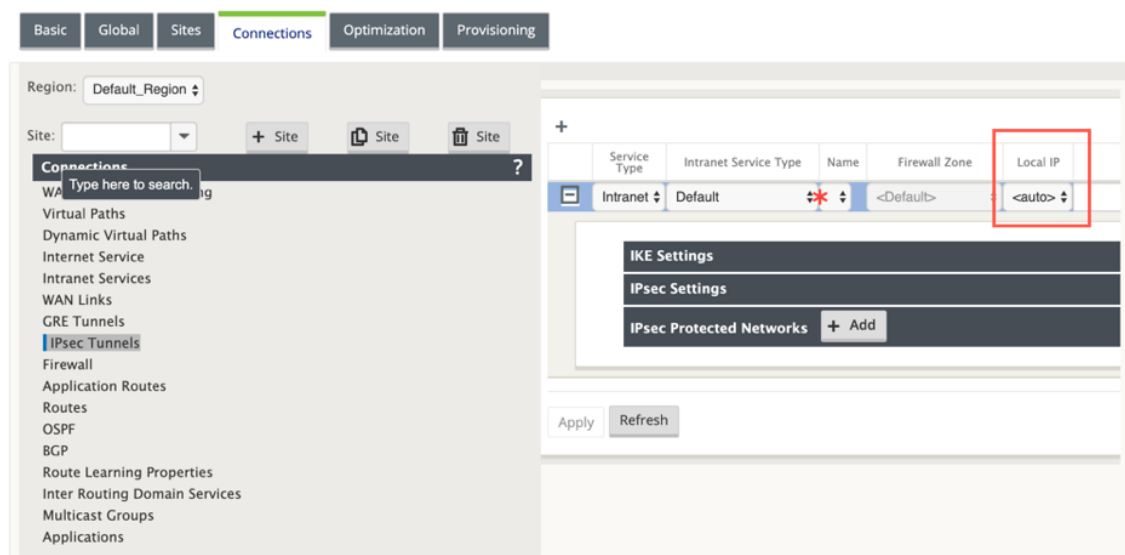


Konfigurieren des IPsec-Tunnels zwischen SD-WAN und Drittanbieter-Geräten

May 10, 2021

So konfigurieren Sie den IPsec-Tunnel für Intranet- oder LAN-Dienst:

1. Navigieren Sie im **Konfigurations-Editor** zu **Verbindungen** > **Site anzeigen** > **[Standortname]** > **IPsec-Tunnel**. Wählen Sie einen **Diensttyp** (LAN oder Intranet).
2. Geben Sie einen **Namen** für die Servicetyp ein. Für den Intranetdiensttyp bestimmt der konfigurierte Intranetserver, welche lokalen IP-Adressen verfügbar sind.



Citrix SD-WAN kann nun IPsec-Tunnel einrichten, wenn eine WAN-Verbindung direkt auf der Appliance beendet wird und der WAN-Verbindung eine dynamische IP zugewiesen wird.

Ab Version 11.1.0 müssen Intranet-IPsec-Tunnel konfigurierbar sein, wenn die lokale Tunnel-IP-Adresse nicht oder nicht bekannt ist. Dies hilft beim Erstellen von IPsec-Tunneln auf den Schnittstellen, deren Adresse über DHCP zugewiesen wird.

Bei der Konfiguration der Schnittstelle für den IPsec-Tunnel muss eine lokale Tunnel-IP erwähnt werden. Diese Schnittstelle wurde geändert, um die Auswahl einer leeren IP zu ermöglichen, wenn der Tunneltyp **Intranet** ist.

Außerdem wird das Label für eine nicht festgelegte Adresse in **Auto** geändert, wenn der Tunneltyp **Intranet** ist.

Wenn die lokale IP auf **Auto** festgelegt ist, kann sie die IP-Adresse übernehmen, die für die Zugriffsschnittstelle auf dieser WAN-Verbindung integriert ist. Diese WAN-Link-Zugriffsschnittstelle erhält möglicherweise die IP entweder statisch oder von DHCP. Der IPsec-Tunnel wird standardmäßig mit der primären WAN-Link-Zugriffs-Schnittstelle eingerichtet.

Früher können Sie IPsec-Tunnel über eine einzelne WAN-Verbindung einrichten. Dies macht die Zweigumgebung während Perioden von Verbindungsfehlern und wenn der Paketverlust auf einer Verbindung versehentlich hoch ist, um eine zuverlässige Konnektivität zu ermöglichen.

Ab Version 11.1.0 können Sie zwei WAN-Verbindungen verwenden, um IPsec-Tunnel einzurichten, um Zweigumgebungen vor Zeiten von Service-Unterbrechungen zu schützen. Wenn die primäre Verbindung heruntergeht, schaltet sich die sekundäre Verbindung innerhalb von Millisekunden aktiv/nach oben.

Hinweis

Wenn die Option **<Auto>** ausgewählt ist, wird der IPsec-Tunnel über die primäre WAN-Link-Zugriffsschnittstelle eingerichtet. Wenn die primäre WAN-Verbindung geht, wird IPsec-Tunnel mit der sekundären WAN-Link-Zugriffs-Schnittstelle eingerichtet.

The screenshot shows the Citrix SD-WAN configuration interface. The top navigation bar includes tabs for Basic, Global, Sites, Connections (selected), Optimization, and Provisioning. Below the navigation bar, the 'Connections' section is active, showing a list of connection types on the left and a configuration table on the right.

Connections List:

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services** (selected)
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups
- Applications

WAN Links Configuration Table:

| WAN Link | Use | Mode | Tunnel Header Size (bytes) | Access Interface Fallback | Tagging | Max Delay (ms) |
|---------------------------|-------------------------------------|--------|----------------------------|-------------------------------------|---------|----------------|
| BRANCH1_KVMVPX-Public-WL1 | <input checked="" type="checkbox"/> | Primar | 0 | <input checked="" type="checkbox"/> | None | 500 |
| BRANCH1_KVMVPX-Public-WL2 | <input checked="" type="checkbox"/> | Secund | 0 | <input checked="" type="checkbox"/> | None | 500 |

Buttons: Apply, Refresh

3. Wählen Sie die verfügbare **lokale IP-Adresse** aus und geben Sie die **Peer-IP-Adresse** des IPsec-Tunnels ein.

The first screenshot shows the 'Connections' menu on the left with 'IPsec Tunnels' selected. The main panel displays a table for configuring an IPsec tunnel. The 'Service Type' is set to 'Intranet'. The 'Local IP' and 'Peer IP' fields are marked with red asterisks, indicating they are required. Below the table, there are sections for 'IKE Settings', 'IPsec Settings', and 'IPsec Protected Networks'.

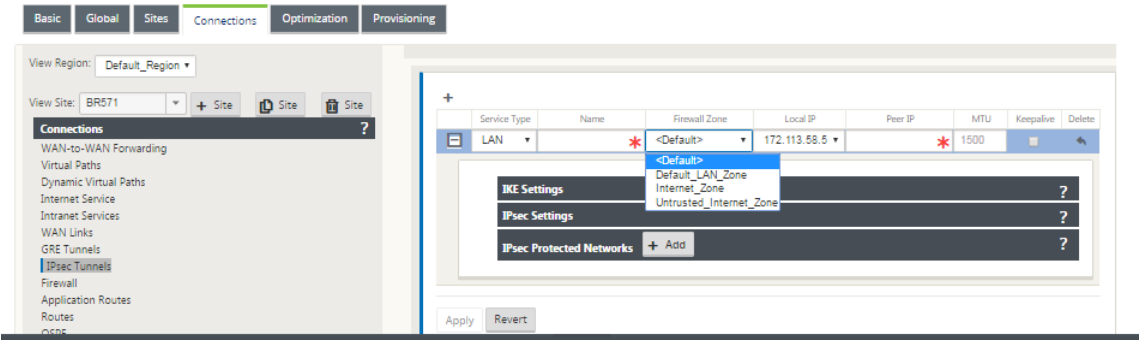
The second screenshot shows the 'Intranet' dropdown menu expanded, displaying a list of available services: 'Default', 'Azure', 'Citrix SaaS Gateway', and 'ZScaler'. The 'Default' option is currently selected.

The third screenshot shows the 'Connections' tab selected in the top navigation bar. The 'View Region' is set to 'Default_Region' and the 'View Site' is 'vpxmcn'. The 'IPsec Tunnels' section is expanded, showing a table with three configured tunnels:

| Service Type | Intranet Service Type | Name | Firewall Zone |
|--------------|-----------------------|------------------------|---------------|
| Intranet | Azure | | <Default> |
| LAN | Default | LAN-Service-1 | <Default> |
| Intranet | Default | New_Intranet_Service-1 | <Default> |

Hinweis

Wenn der Diensttyp Intranet ist, wird die IP-Adresse vom gewählten Intranetdienst vorab festgelegt.



4. Konfigurieren Sie IPsec-Einstellungen, indem Sie die in den folgenden Tabellen beschriebenen Kriterien anwenden. Wenn Sie fertig sind, klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern.

| Feld | Beschreibung | Wert |
|-------------------|---|---|
| Servicetyp | Wählen Sie einen Servicetyp aus dem Dropdownmenü | Intranet, LAN |
| Name | Wenn der Diensttyp Intranet ist, wählen Sie aus der Liste der konfigurierten Intranetdienste im Dropdownmenü aus. Wenn der Diensttyp LAN ist, geben Sie einen eindeutigen Namen ein | Textzeichenfolge |
| Lokale IP | Wählen Sie die lokale IP-Adresse des IPsec-Tunnels aus dem Dropdownmenü der verfügbaren virtuellen IP-Adressen, die an diesem Standort konfiguriert sind. | IP-Adresse |
| Peer-IP | Geben Sie die Peer-IP-Adresse des IPsec-Tunnels ein | IP-Adresse |
| MTU | Geben Sie die MTU zum Fragmentieren von IKE- und IPsec-Fragmenten ein | Standard: 1500 |
| IKE-Einstellungen | Version: Wählen Sie eine IKE-Version aus dem Dropdownmenü | IKEv1 IKEv2 |
| Modus | Wählen Sie einen Modus aus dem Dropdownmenü | FIPS-konform: Main, nicht FIPS-konform: Aggressiv |

| Feld | Beschreibung | Wert |
|-------------------------------|--|--|
| Identität | Wählen Sie eine Identität aus dem Dropdownmenü | Automatische IP-Adresse Manuelle IP-Adresse Benutzer-FQDN |
| Authentifizierung | Wählen Sie den Authentifizierungstyp aus dem Dropdownmenü | Pre-Shared Key: Wenn Sie einen vorinstallierten Schlüssel verwenden, kopieren Sie ihn und fügen Sie ihn in dieses Feld ein. Klicken Sie auf das Symbol Eyeball (), um den vorinstallierten Schlüssel anzuzeigen. Zertifikat: Wenn Sie ein Identitätszertifikat verwenden, wählen Sie es aus dem Dropdownmenü aus. |
| Validieren der Peer-Identität | Aktivieren Sie dieses Kontrollkästchen, um den Peer des IKE zu überprüfen. Wenn der ID-Typ des Peers nicht unterstützt wird, aktivieren Sie diese Funktion nicht | Ohne |
| DH-Gruppe | Wählen Sie die Diffie-Hellman-Gruppe für die IKE-Schlüsselgenerierung aus dem Dropdown-Menü | FIPS-konform: Gruppe 1, FIPS-konform: Gruppe 2 Gruppe 5 Gruppe 14 Gruppe 15 Gruppe 16 Gruppe 19 Gruppe 20 Gruppe 21 |
| Hash-Algorithmus | Wählen Sie einen Algorithmus aus dem Dropdownmenü, um IKE-Nachrichten zu authentifizieren | Nicht FIPS-konform: MD5 FIPS-konform: SHA1 SHA-256 |
| Verschlüsselungsmodus | Wählen Sie den Verschlüsselungsmodus für IKE-Nachrichten aus dem Dropdown-Menü | AES 128-Bit AES 192-bit AES 256-Bit |
| Lebensdauer (e) | Geben Sie die bevorzugte Dauer in Sekunden ein, für die eine IKE-Sicherheitszuordnung vorhanden sein soll. | 3600 Sekunden (Standard) |

| Feld | Beschreibung | Wert |
|-------------------------------|--|---|
| Lebensdauer (en) Max. | Geben Sie die maximal bevorzugte Dauer in Sekunden ein, um eine IKE-Sicherheitszuordnung zu ermöglichen. | 86400 Sekunden (Standard) |
| DPD-Zeitüberschreitung (en) | Geben Sie das Dead Peer Detection-Timeout für VPN-Verbindungen in Sekunden ein | 300 Sekunden (Standard) |
| IKEv2 | Peer-Authentifizierung: Wählen Sie Peer-Authentifizierung aus dem Dropdown-Menü | Gespiegeltes, vorgeteiltes Schlüsselzertifikat |
| IKE2 - Vorgeteilter Schlüssel | Peer Pre-Shared Key: Fügen Sie den IKEv2 Peer Pre-Shared Key zur Authentifizierung in dieses Feld ein. Klicken Sie auf das eyeball () -Symbol, um den Pre-Shared Key anzuzeigen. | Textzeichenfolge |
| Integritätsalgorithmus | Wählen Sie im Dropdownmenü einen Algorithmus als Hashing-Algorithmus aus, der für die HMAC-Verifizierung verwendet werden soll. | Nicht FIPS-konform: MD5 FIPS-konform: SHA1 SHA-256 |

Hinweis:

Wenn der abschließende IPsec-Router Hash-basierten Message Authentication Code (HMAC) in der Konfiguration enthält, ändern Sie den IPsec-Modus in **Exp+Auth** mit einem Hashing-Algorithmus als **SHA1**.

IKE Settings?

Version:
IKEv1

Mode:
Aggressive

Identity:
Auto

Authentication:
Pre-Shared Key

Pre-Shared Key:

☒ Validate Peer Identity

Peer Identity:
Auto

DH Group:
Group 1 (MODP768)

Hash Algorithm:
MD5

Encryption Mode:
AES 128-Bit

Lifetime (s):
3600

Lifetime (s) Max:
86400

DPD Timeout (s):
300

IPsec Settings?

IPsec Protected Networks + Add?

IKE Settings?

Version:
IKEv2

Identity:
Auto

Authentication:
Pre-Shared Key

Pre-Shared Key:

Peer Authentication:
Mirrored

☒ Validate Peer Identity

Peer Identity:
Auto

DH Group:
Group 1 (MODP768)

Hash Algorithm:
MD5

Integrity Algorithm:
MD5

Encryption Mode:
AES 128-Bit

Lifetime (s):
3600

Lifetime (s) Max:
86400

DPD Timeout (s):
300

IPsec Settings?

IPsec Protected Networks + Add?

IPsec- und IPsec-geschützte Netzwerkeinstellungen:

| Feld | Beschreibung | Wert (e) |
|------------|---|--|
| Tunneltyp | Wählen Sie den Tunneltyp aus dem Drop-down-Menü | ESP ESP+Auth ESP+NULL AH |
| PFS Gruppe | Wählen Sie die Diffie-Hellman-Gruppe für die perfekte Vorwärtsgeheimnis aus dem Dropdown-Menü | Keine Gruppe 1 Gruppe 2 Gruppe 5 Gruppe 14 Gruppe 15 Gruppe 16 Gruppe 19 Gruppe 20 Gruppe 21 |

| Feld | Beschreibung | Wert (e) |
|--|---|--|
| Verschlüsselungsmodus | Wählen Sie den Verschlüsselungsmodus für IPsec-Nachrichten aus dem Dropdown-Menü | Wenn Sie ESP oder ESP+ Auth gewählt haben, wählen Sie eine der folgenden Optionen: AES 128-Bit, AES 192-Bit, AES 256-Bit, AES 128-Bit GCM 64-Bit, AES 192-Bit GCM 64-Bit, AES 256-Bit GCM 64-Bit, AES 128-Bit GCM 96-Bit, AES 192-Bit GCM 96-Bit, AES 256-Bit GCM 96-Bit, AES 128-Bit GCM 128-Bit, AES 192-Bit GCM 128-Bit, AES 256-Bit GCM 128-Bit. AES 128/192/256-Bit werden CBC unterstützt. |
| Lebensdauer (e) | Geben Sie die Zeit in Sekunden ein, um eine IPsec-Sicherheitszuordnung zu ermöglichen. | 28800 Sekunden (Standard) |
| Max. Lebensdauer (n) | Geben Sie die maximale Zeit in Sekunden ein, um eine IPsec-Sicherheitszuordnung zu ermöglichen. | 86400 Sekunden (Standard) |
| Lebensdauer (KB) | Geben Sie die Datenmenge in Kilobyte ein, für die eine IPsec-Sicherheitszuordnung vorhanden sein soll. | Kilobyte |
| Lebensdauer (KB) Max. | Geben Sie die maximale Datenmenge in Kilobyte ein, um eine IPsec-Sicherheitszuordnung zu ermöglichen. | Kilobyte |
| Verhalten bei Nichtübereinstimmungen im Netzwerk | Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn ein Paket nicht mit den geschützten Netzwerken des IPsec-Tunnels übereinstimmt. | Löschen, unverschlüsselt senden, Nicht-IPsec-Route verwenden |

| Feld | Beschreibung | Wert (e) |
|----------------------------|--|------------|
| IPsec-geschützte Netzwerke | Quell-IP/Präfix: Nachdem Sie auf die Schaltfläche Hinzufügen (+ Hinzufügen) geklickt haben, geben Sie die Quell-IP und das Präfix des Netzwerkverkehrs ein, den der IPsec-Tunnel schützt | IP-Adresse |
| IPsec-geschützte Netzwerke | Ziel-IP/Präfix: Geben Sie die Ziel-IP und das Präfix des Netzwerkverkehrs ein, den der IPsec-Tunnel schützen wird | IP-Adresse |

IPsec Settings?

Tunnel Type:

ESP

PFS Group:

<None>

Encryption Mode:

AES 128-Bit

Lifetime (s):

28800

Lifetime (s) Max:

88400

Lifetime (KB):

0

Lifetime (KB) Max:

0

Network Mismatch Behavior:

Drop

IPsec Protected Networks

+ Add

?

Apply

Revert

Überwachung von IPsec-Tunneln

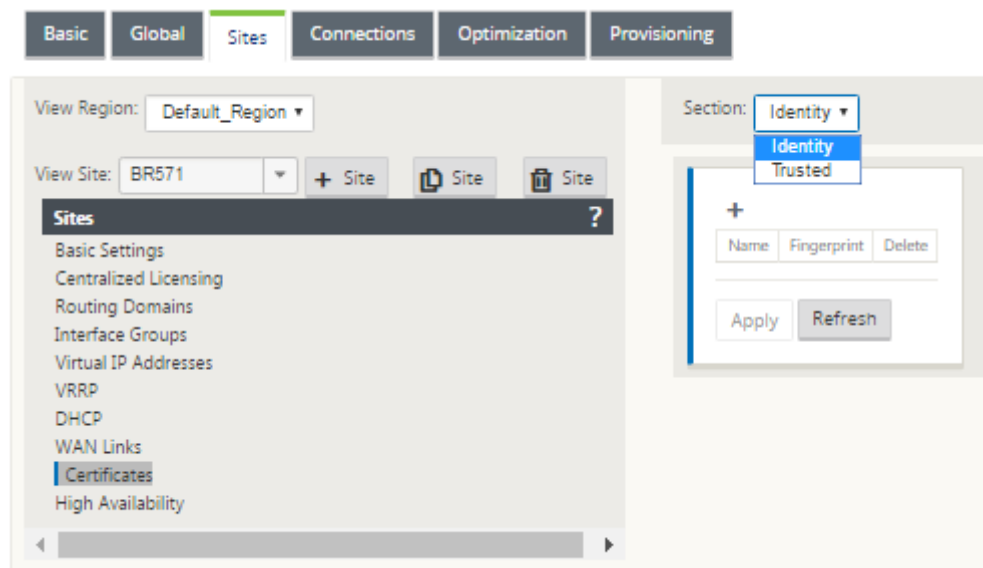
Navigieren Sie zu **Monitoring>IKE/IPsec** in der Benutzeroberfläche der SD-WAN-Appliance, um die IPsec-Tunnelkonfiguration anzuzeigen und zu überwachen.

Hinzufügen von IKE-Zertifikaten

May 10, 2021

So implementieren Sie Zertifikate für IKE-Aushandlung:

1. Navigieren Sie zu **Websites > Zertifikate**, und fügen Sie alle erforderlichen Zertifikate hinzu.



So zeigen Sie die IPsec-Tunnelkonfiguration an

May 10, 2021

So zeigen Sie die IPsec-Tunnelkonfiguration an:

1. Navigieren Sie zu **Konfiguration > Virtuelles WAN > Konfiguration anzeigen**.
2. Wählen Sie **Virtual Path Service** aus dem Dropdownmenü. Die IPsec-Einstellungen werden nur angezeigt, wenn IPsec im Konfigurations-Editor aktiviert ist.

DashboardMonitoringConfiguration

Configuration > Virtual WAN > View Configuration

Configuration

View: Virtual Path Service

Virtual Path Service Configuration

Virtual Path 515 = HCN-5100-88572

Local site(HCN-5100)

Remote site(88572)

Local send rate:20000 kbps

Remote send rate:20000 kbps

On-demand standby link trigger threshold: %

IPsec settings: IPsec

Routing Domain: Enabled

Default Routing Domain

PATHS:

| Path ID | From Link | To Link | Primary Src IP Address | Primary Dst IP Address | Secondary Src IP Address | Secondary Dst IP Address | Alternate Src Port | Alternate Dst Port | Alternate Src Port | Alternate Dst Port | IPsec | Encrypt | Loss | Percent |
|---------|---------------|---------------|------------------------|------------------------|--------------------------|--------------------------|--------------------|--------------------|--------------------|--------------------|-------|---------|------|---------|
| 0 | HCN-5100-HL-1 | 88572-HL-1 | 172.111.64.5 | 172.113.59.5 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |
| 3 | HCN-5100-HL-2 | 88572-HL-2 | 172.111.65.5 | 192.113.59.6 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |
| 1 | HCN-5100-HL-1 | 88572-HL-2 | 172.111.64.5 | 192.113.59.6 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |
| 2 | HCN-5100-HL-2 | 88572-HL-1 | 172.111.65.5 | 172.113.59.5 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |
| 0 | 88572-HL-1 | HCN-5100-HL-1 | 172.113.59.5 | 172.111.64.5 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |
| 3 | 88572-HL-2 | HCN-5100-HL-2 | 192.113.59.6 | 172.111.65.5 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |
| 1 | 88572-HL-1 | HCN-5100-HL-2 | 172.113.59.5 | 172.111.65.5 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |
| 2 | 88572-HL-2 | HCN-5100-HL-1 | 192.113.59.6 | 172.111.64.5 | - | - | 4800 | 4800 | - | - | - | aes128 | YES | - |

| From Link | To Link | Realtime Eligible | Interactive Eligible | Bulk Eligible | Path Group | Standby Heartbeat Interval(ms) | Active Heartbeat Interval(ms) |
|---------------|---------------|-------------------|----------------------|---------------|------------|--------------------------------|-------------------------------|
| HCN-5100-HL-1 | 88572-HL-1 | YES | YES | YES | 0 | n/a | n/a |
| HCN-5100-HL-2 | 88572-HL-2 | YES | YES | YES | 0 | n/a | n/a |
| HCN-5100-HL-1 | 88572-HL-2 | YES | YES | YES | 0 | n/a | n/a |
| HCN-5100-HL-2 | 88572-HL-1 | YES | YES | YES | 0 | n/a | n/a |
| 88572-HL-1 | HCN-5100-HL-1 | YES | YES | YES | 0 | n/a | n/a |
| 88572-HL-2 | HCN-5100-HL-2 | YES | YES | YES | 0 | n/a | n/a |
| 88572-HL-1 | HCN-5100-HL-2 | YES | YES | YES | 0 | n/a | n/a |
| 88572-HL-2 | HCN-5100-HL-1 | YES | YES | YES | 0 | n/a | n/a |

CLASSES:

Classes on virtual path "HCN-5100-88572":

| # | Type | Traffic Rate (kbps) | Initial Period (ms) | Initial Rate (kbps) | Sustain Rate (kbps) |
|----|-------------|---------------------|---------------------|---------------------|---------------------|
| 0 | REALTIME | 0 | 0 | 6000 | |
| 1 | INTERACTIVE | 0 | 0 | 2000 | |
| 2 | INTERACTIVE | 0 | 0 | 800 | |
| 3 | INTERACTIVE | 0 | 0 | 200 | |
| 4 | BULK | 0 | 0 | 1 | |
| 5 | BULK | 0 | 0 | 1 | |
| 6 | BULK | 0 | 0 | 1 | |
| 7 | BULK | 0 | 0 | 1 | |
| 8 | BULK | 0 | 0 | 1 | |
| 9 | BULK | 0 | 0 | 1 | |
| 10 | REALTIME | 0 | 0 | 6000 | |
| 11 | INTERACTIVE | 0 | 0 | 4000 | |
| 12 | INTERACTIVE | 0 | 0 | 3000 | |
| 13 | INTERACTIVE | 0 | 0 | 1400 | |
| 14 | INTERACTIVE | 0 | 0 | 600 | |
| 15 | BULK | 0 | 0 | 6000 | |
| 16 | BULK | 0 | 0 | 1 | |

3. Wählen Sie **IPsec-Tunnel** aus dem Dropdownmenü, um die IPsec-Tunnelkonfiguration anzuzeigen.

Configuration

View: IPsec Tunnels

IPsec Tunnel Configuration

Name: VPN-ASA-1

ipsec_service_type=transport

ike_local_ip_addr=10.0.0.6

ike_remote_ip_addr=10.101.0.100

network_mtu=1500

ike_version=2

ike_auth=psk

ike_identity=auto

ike_peer_auth=cert

ike_validate_peer_identity=1

ike_hash_algorithm=sha256

ike_integ_algorithm=sha256

ike_encryption_mode=aes256

ike_dhgroup=group2

ike_lifetime_s=300

ike_lifetime_s_max=86400

ike_dpd_s=300

ipsec_tunnel_mode=tunnel

ipsec_tunnel_type=esp_auth

ipsec_encryption_mode=aes128

ipsec_hash_algorithm=sha

ipsec_pfcgroup=none

ipsec_lifetime_s=28800

ipsec_lifetime_s_max=86400

ipsec_lifetime_kb=0

ipsec_lifetime_kb_max=0

ipsec_mismatch_behavior=drop

Protected Networks:

[1] 10.0.0.0/16 -> 10.101.0.0/16

[2] 10.4.0.0/16 -> 10.101.0.0/16

[3] 10.3.0.0/16 -> 10.101.0.0/16

[4] 10.2.0.0/16 -> 10.101.0.0/16

[5] 10.1.0.0/16 -> 10.101.0.0/16

4. Jeder virtuelle Pfad zeigt seinen eigenen IPsec-Tunnelstatus, wie unten gezeigt.

DashboardMonitoringConfiguration

System Status

Name:MCN-5100

Model:5100

Appliance Mode:MCN

Serial Number:4H30GCNPD0

Management IP Address:10.199.107.201

Appliance Uptime:1 weeks, 3 days, 2 hours, 7 minutes, 28.6 seconds

Service Uptime:6 hours, 21 minutes, 54.0 seconds

Routing Domain Enabled:Default_RoutingDomain

Local Versions

Software Version:10.0.0.193.659091

Built On:Feb 17 2018 at 17:32:45

Hardware Version:5100

OS Partition Version:4.6

Virtual Path Service Status

Virtual Path MCN-5100-BR572:

Uptime: 5 hours, 59 minutes, 34.0 secondsIPsec state: GOOD.

Virtual Path MCN-5100-BR573:

Uptime: 5 hours, 45 minutes, 0.0 seconds.IPsec state: GOOD.

Virtual Path MCN-5100-BR574:

Uptime: 4 hours, 56 minutes, 48.0 seconds.

Virtual Path 'MCN-5100-BR575' is currently dead.

Virtual Path MCN-5100-RCN1-5100:

Uptime: 2 hours, 7 minutes, 3.0 seconds.

Virtual Path 'MCN-5100-RCN3-2100' is currently dead (Configuration version mismatch)

Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.

Virtual Path 'MCN-5100-RCN4-ESxil' is currently dead.

IPsec-Überwachung und -Protokollierung

May 10, 2021

So überwachen Sie die IPsec-Tunnelstatistiken:

1. Navigieren Sie zu **Monitor > Statistik**. Wählen Sie **IPsec-Tunnel** aus dem Dropdownmenü **Anzeigen**, wie unten dargestellt:

Statistics

Show: IPsec Tunnel Enable Auto Refresh 5 seconds Show latest data.

IPsec Tunnel Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 8 of 8 entries

| Name | State | Service Type | Packets Received | Kbps Received | Packets Sent | Kbps Sent | Packets Dropped | Bytes Dropped | MTU |
|----------------------|-------|--------------|------------------|---------------|--------------|-----------|-----------------|---------------|------|
| AS-TB-NCN-AS-TB-CL-1 | GOOD | Conduit | 0 | 0 | 0 | 0 | 0 | 0 | 1359 |
| AS-TB-NCN-AS-TB-CL-2 | GOOD | Conduit | 0 | 0 | 0 | 0 | 0 | 0 | 1359 |
| AS-TB-NCN-AS-TB-CL-3 | GOOD | Conduit | 0 | 0 | 0 | 0 | 0 | 0 | 1359 |
| AS-TB-NCN-AS-TB-CL-4 | GOOD | Conduit | 0 | 0 | 0 | 0 | 0 | 0 | 1359 |
| VPN-ASA-1 | GOOD | Intranet | 0 | 0 | 0 | 0 | 0 | 0 | 1427 |
| VPN-ASA-2 | GOOD | LAN | 0 | 0 | 0 | 0 | 0 | 0 | 1377 |
| VPN-PaloAlto | GOOD | Intranet | 0 | 0 | 0 | 0 | 0 | 0 | 1439 |
| VPN-SonicWall | GOOD | Intranet | 0 | 0 | 0 | 0 | 0 | 0 | 1456 |

Showing 1 to 8 of 8 entries

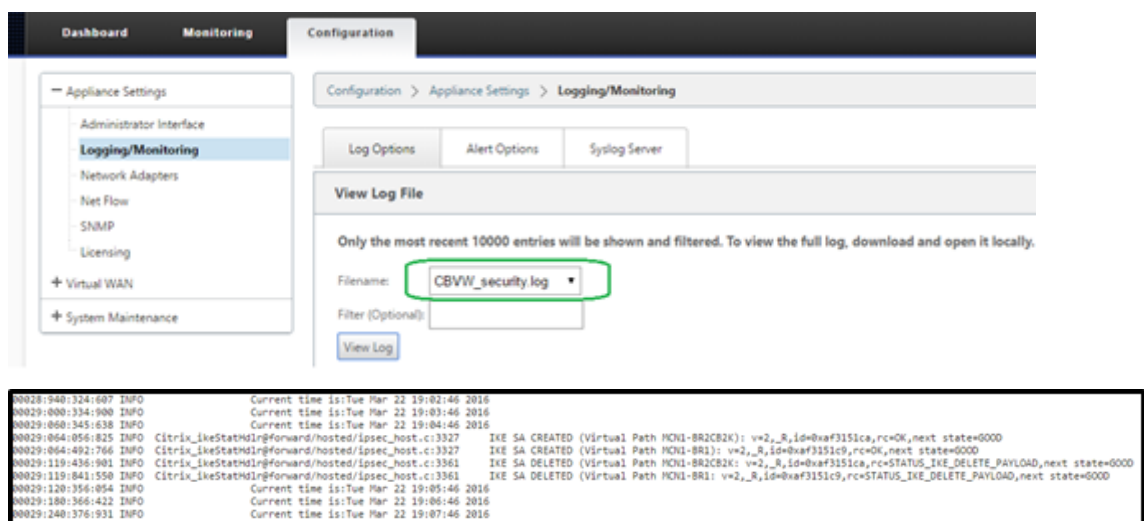
2. Navigieren Sie zu **Monitor > IKE/IPsec** . Beachten Sie die konfigurierten IPsec-Tunnel, die IKE-

und IPsec-Dienstzuordnungen zwischen zwei oder Modus-VPN-Endpunkten, die im SD-WAN-Netzwerk konfiguriert sind.

So überwachen Sie ipsec Protokolle

1. Navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Logging/Überwachung** . Wählen Sie im Dropdownmenü die Option **Dateiname** aus und klicken Sie auf **Protokoll anzeigen** . Sie können die folgenden Protokolldetails für den IPsec-Tunnel anzeigen:

- Erstellung und Löschung des IPsec-Tunnels
- Statusänderung des IPsec-Tunnels



So zeigen Sie IPsec-Tunnelwarnungen an

1. Navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Logging/Überwachung > Warnungsoptionen** .
2. Erstellen Sie E-Mail- und Syslog-Warnungen für IPsec-Tunnelzustandsberichte.
 - Unterstützt IPSEC_TUNNEL als einer der Ereignistypen, mit denen Sie E-Mail- und Syslog-Schweregradfilter konfigurieren können.

← Appliance Settings

Administrator Interface

Logging/Monitoring

Network Adapters

Net Flow

App Flow

SNMP

NETRO API

Licensing

+ Virtual WAN

+ System Maintenance

Configuration > Appliance Settings > Logging/Monitoring

Log OptionsAlert OptionsAlarm OptionsSyslog Server

Email Alerts

☐ Enable Email Alerts

Send Test Email

Destination Email Address(es):

SMTP Server Hostname or IP Address:

SMTP Server Port:

25

Source Email Address:

You may enter multiple destination email addresses separated with semicolons (;)

☐ Enable SMTP Authentication

SMTP User Name:

SMTP Password:

Verify SMTP Password:

General Event Configuration

| Event Type | Alert if State Persists | Email | Email Severity Filter | Syslog | Syslog Severity Filter | SNMP | SNMP Severity Filter |
|---------------------------|-------------------------|--------------------------|-----------------------|--------------------------|------------------------|--------------------------|----------------------|
| SERVICE | 0 | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| VIRTUAL_PATH | 0 | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| WAN_LINK | 0 | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| PATH | 0 | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| DYNAMIC_VIRTUAL_PATH | 0 | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| WAN_LINK_CONGESTION | 0 | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| USAGE_CONGESTION | 0 | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| HARD_DISK | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| APPLIANCE | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| USER_EVENT | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| CONFIG_UPDATE | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| SOFTWARE_UPDATE | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| PROXY_ARP | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| ETHERNET | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| WATCHDOG | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| APPLIANCE_SETTINGS_UPDATE | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| DISCOVERED_MTU | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| GRE_TUNNEL | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| IPSEC_TUNNEL | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| VIRTUAL_INTERFACE | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |
| LICENSE_EVENT | | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ | <input type="checkbox"/> | Warning ▼ |

Apply Settings

So überwachen Sie ipsec-Tunnelereignisse

1. Navigieren Sie zu **Konfiguration > Systemwartung > Diagnose > Ereignisse** .

2. Fügen Sie Ereignisse basierend auf dem **IPSEC_TUNNEL-Objekttyp** hinzu. Erstellen Sie Filter für alle IPsec-bezogenen Ereignisse.

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

760

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

System Maintenance

System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics**
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Insert Event

Object Type:USER EVENT

Event type:UNDEFINED

Severity:DEBUG

Add Event

Download Events

There are currently 487678 in the Events database, spanning from event 183612 at 2018-01-18 18:24:55 to event 671289 at 2018-02-17 18:14:15. You can download some or all of them in CSV format. You may wish to limit the amount to download because some common spreadsheet programs limit you to 65,536 rows.

Download events starting from2018January18182456Download487678 events

Alert Count

| Alert Type | Alerts Sent |
|------------------|-------------|
| Emails: | 0 |
| syslog Messages: | 0 |
| SNMP Traps: | 0 |

View Events

Quantity:25

Filter: Object Type = AnyEvent type = AnySeverity = Any

Reload Events Table

| ID | Object ID | Object Name | Object Type | Time | Event Type | Severity | Description |
|--------|-----------|---------------------------|-------------|---------------------|------------|----------|---|
| 671289 | 0 | MCN-5100-WL-1->BR572-WL-1 | PATH | 2018-02-17 18:14:15 | GOOD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from BAD to GOOD because notified by peer. |
| 671288 | 1 | MCN-5100-WL-1->BR572-WL-2 | PATH | 2018-02-17 18:14:15 | GOOD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671287 | 0 | MCN-5100-WL-1->BR574-WL-1 | PATH | 2018-02-17 18:14:15 | GOOD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer. |
| 671286 | 2 | MCN-5100-WL-2->BR572-WL-1 | PATH | 2018-02-17 18:14:14 | GOOD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from BAD to GOOD because notified by peer. |
| 671285 | 1 | MCN-5100-WL-1->BR572-WL-2 | PATH | 2018-02-17 18:14:04 | BAD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer. |
| 671284 | 0 | MCN-5100-WL-1->BR572-WL-1 | PATH | 2018-02-17 18:14:04 | BAD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from GOOD to BAD because notified by peer. |
| 671283 | 0 | MCN-5100-WL-1->BR574-WL-1 | PATH | 2018-02-17 18:14:04 | BAD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer. |
| 671282 | 2 | MCN-5100-WL-2->BR572-WL-1 | PATH | 2018-02-17 18:14:04 | BAD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from GOOD to BAD because notified by peer. |
| 671281 | 3 | MCN-5100-WL-2->BR573-WL-2 | PATH | 2018-02-17 18:13:17 | GOOD | NOTICE | Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671280 | 1 | MCN-5100-WL-1->BR572-WL-2 | PATH | 2018-02-17 18:13:17 | GOOD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671279 | 1 | MCN-5100-WL-1->BR574-WL-2 | PATH | 2018-02-17 18:13:17 | GOOD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671278 | 2 | MCN-5100-WL-2->BR574-WL-1 | PATH | 2018-02-17 18:13:17 | GOOD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from BAD to GOOD because notified by peer. |
| 671277 | 2 | MCN-5100-WL-2->BR574-WL-1 | PATH | 2018-02-17 18:13:06 | BAD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from GOOD to BAD because notified by peer. |
| 671276 | 1 | MCN-5100-WL-1->BR572-WL-2 | PATH | 2018-02-17 18:13:06 | BAD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer. |
| 671275 | 3 | MCN-5100-WL-2->BR573-WL-2 | PATH | 2018-02-17 18:13:06 | BAD | NOTICE | Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from GOOD to BAD because notified by peer. |
| 671274 | 1 | MCN-5100-WL-1->BR574-WL-2 | PATH | 2018-02-17 18:13:06 | BAD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-2 state has changed from GOOD to BAD because notified by peer. |
| 671273 | 3 | MCN-5100-WL-2->BR574-WL-2 | PATH | 2018-02-17 18:06:09 | GOOD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671272 | 0 | MCN-5100-WL-1->BR574-WL-1 | PATH | 2018-02-17 18:06:09 | GOOD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer. |
| 671271 | 1 | MCN-5100-WL-1->BR572-WL-2 | PATH | 2018-02-17 18:06:08 | GOOD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671270 | 1 | MCN-5100-WL-1->BR572-WL-2 | PATH | 2018-02-17 18:05:58 | BAD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer. |
| 671269 | 0 | MCN-5100-WL-1->BR574-WL-1 | PATH | 2018-02-17 18:05:58 | BAD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer. |
| 671268 | 3 | MCN-5100-WL-2->BR574-WL-2 | PATH | 2018-02-17 18:05:57 | BAD | NOTICE | Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from GOOD to BAD because notified by peer. |
| 671267 | 1 | MCN-5100-WL-1->BR573-WL-2 | PATH | 2018-02-17 18:05:09 | GOOD | NOTICE | Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671266 | 3 | MCN-5100-WL-2->BR572-WL-2 | PATH | 2018-02-17 18:05:09 | GOOD | NOTICE | Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-2 state has changed from BAD to GOOD because notified by peer. |
| 671265 | 1 | MCN-5100-WL-1->BR573-WL-2 | PATH | 2018-02-17 18:04:58 | BAD | NOTICE | Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from GOOD to BAD because notified by peer. |

Berechtigung für nicht-virtuelle IPsec-Pfadroutes

May 10, 2021

In früheren Versionen verbleiben ipsec-Tunnelrouten in der Routentabelle, selbst wenn der Tunnel nicht verfügbar wäre.

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

761

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries

| Num | Network Addr | Gateway IP Address | Service | Firewall Zone | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|------------------|--------------------|------------------------|------------------|-----------|-----------------|---------|---------|----------|-----------------|------|-----------|----------|------------------|-------------------|
| 0 | 172.186.120.0/24 | 172.186.40.1 | Local | Default_LAN_Zone | YES | * | DC | Static | - | - | 5 | 11369 | YES | N/A | N/A |
| 1 | 172.186.50.0/24 | * | Local | Default_LAN_Zone | YES | * | DC | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 2 | 172.186.40.0/24 | * | Local | Default_LAN_Zone | YES | * | DC | Static | - | - | 5 | 11389 | YES | N/A | N/A |
| 3 | 172.186.75.0/24 | * | DC-BRANCH2 | Default_LAN_Zone | YES | * | BRANCH2 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 4 | 172.186.30.0/24 | * | DC-BRANCH1 | Default_LAN_Zone | YES | * | BRANCH1 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 5 | 172.186.20.0/24 | * | DC-BRANCH1 | Default_LAN_Zone | YES | * | BRANCH1 | Static | - | - | 5 | 0 | YES | N/A | N/A |
| 6 | 172.186.160.0/24 | 172.186.40.1 | Local | Default_LAN_Zone | YES | * | DC | Dynamic | BGP | - | 6 | 0 | YES | N/A | N/A |
| 7 | 155.155.155.0/24 | 172.186.40.1 | Local | Default_LAN_Zone | YES | * | DC | Dynamic | BGP | - | 6 | 0 | YES | N/A | N/A |
| 8 | 172.186.30.0/24 | * | New_Intranet_Service-1 | Default_LAN_Zone | YES | * | DC | Static | - | - | 15 | 0 | YES | N/A | N/A |
| 9 | 172.186.20.0/24 | * | New_Intranet_Service-1 | Default_LAN_Zone | YES | * | DC | Static | - | - | 15 | 0 | YES | N/A | N/A |
| 10 | 16.16.0.0/16 | 172.186.40.1 | Local | Default_LAN_Zone | YES | * | DC | Dynamic | BGP | - | 6 | 0 | YES | N/A | N/A |
| 11 | 0.0.0.0/0 | * | Passthrough | Any | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |
| 12 | 0.0.0.0/0 | * | Discard | Any | YES | * | * | Static | - | - | 16 | 0 | YES | N/A | N/A |

Durch die Verwendung der Option Keepalive unter **Verbindungen** > [Sitenamen] > **IPsec-Tunnel** wird dieses Verhalten verbessert, sodass die nicht virtuellen IPsec-Pfadrouten nun als nicht zulässig angesehen werden, wenn der IPsec-Tunnel nicht mehr verfügbar ist. Wenn die Option Keepalive aktiviert ist, werden die SAs automatisch erstellt, ohne dass Datenverkehr durch den Tunnel gesendet wird.

Basic Global Sites **Connections** Optimization Provisioning

View Region: Default_Region

View Site: BR573 + Site Site Site

Connections ?

WAN-to-WAN Forwarding

Virtual Paths

Dynamic Virtual Paths

Internet Service

Intranet Services

WAN Links

Tunnels

IPsec Tunnels

Firewall

Application Routes

Routes

OSPF

BGP

Route Learning Properties

Multicast Groups

Application Settings

Audits: 0 Audit Now

+ Service Type Name Firewall Zone Local IP Peer IP MTU Keepalive Delete

Intranet * <Default> * * 1500 ☒

IKE Settings ?

IPsec Settings ?

IPsec Protected Networks + Add ?

Apply Revert

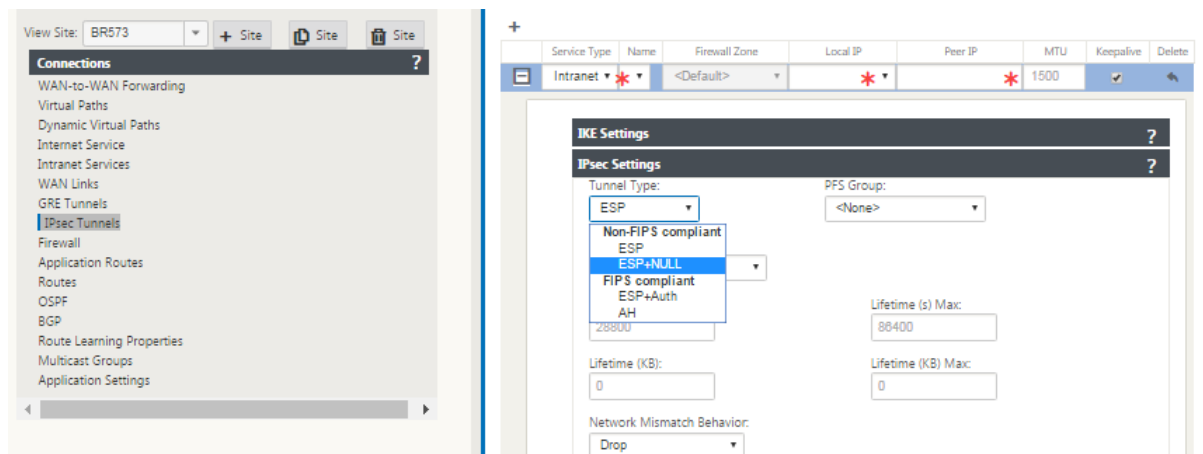
IPsec-Null-Verschlüsselung

May 10, 2021

In früheren Versionen wurde der Tunneltyp ESP+NULL eingeführt. Bei Verwendung des IPsec-ESP-Protokolls wird der Datenverkehr in der Regel verschlüsselt und authentifiziert. Sie können jedoch

festlegen, dass keine Verschlüsselung verwendet wird, indem Sie die Null-Verschlüsselung verwenden. Im Tunneltyp ESP + NULL werden die Pakete authentifiziert, aber nicht verschlüsselt.

Sie können den IPsec-Tunnel mit ESP+NULL Tunneltyp im Konfigurationseditor unter **IPsec-Einstellungen** konfigurieren.



FIPS-Konformität

May 10, 2021

In Citrix SD-WAN erzwingt der FIPS-Modus Benutzer, FIPS-konforme Einstellungen für ihre IPsec-Tunnel und IPsec-Einstellungen für virtuelle Pfade zu konfigurieren.

- Zeigt den FIPS-konformen IKE-Modus an.
- Zeigt eine FIPS-konforme IKE DH-Gruppe an, aus der Benutzer die erforderlichen Parameter für die Konfiguration der Appliance im FIPS-konformen Modus auswählen können (2,5,14 —21).
- Zeigt den FIPS-kompatiblen IPsec-Tunneltyp in IPsec-Einstellungen für virtuelle Pfade an
- IKE-Hash- und (IKEv2) Integritätsmodus, IPsec-Authentifizierungsmodus.
- Führt Überwachungsfehler für FIPS-basierte Lebensdauereinstellungen aus

So aktivieren Sie die FIPS-Konformität mithilfe der Citrix SD-WAN GUI:

1. Gehen Sie zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor > Global** und wählen Sie **FIPS-Modus aktivieren**.

Die Aktivierung des FIPS-Modus erzwingt Prüfungen während der Konfiguration, um sicherzustellen, dass alle IPsec-bezogenen Konfigurationsparameter den FIPS-Standards entsprechen. Sie werden durch Überwachungsfehler und Warnungen aufgefordert, IPsec zu konfigurieren.

So konfigurieren Sie IPsec-Einstellungen für virtuelle Pfade:

- Aktivieren Sie Virtual Path IPsec-Tunnel für alle virtuellen Pfade, bei denen FIPS-Konformität erforderlich ist. IPsec-Einstellungen für virtuelle Pfade werden über Standardsätze gesteuert.
- Konfigurieren Sie die Nachrichtenauthentifizierung, indem Sie den IPsec-Modus in AH oder ESP+Auth ändern und eine FIPS-zugelassene Hashing-Funktion verwenden. SHA1 wird von FIPS akzeptiert, aber SHA256 wird dringend empfohlen.
- Die IPsec-Lebensdauer sollte nicht länger als 8 Stunden (28.800 Sekunden) konfiguriert werden.

Das virtuelle WAN verwendet IKE Version 2 mit vorinstallierten Schlüsseln, um IPsec-Tunnel über den virtuellen Pfad mit den folgenden Einstellungen auszuhandeln:

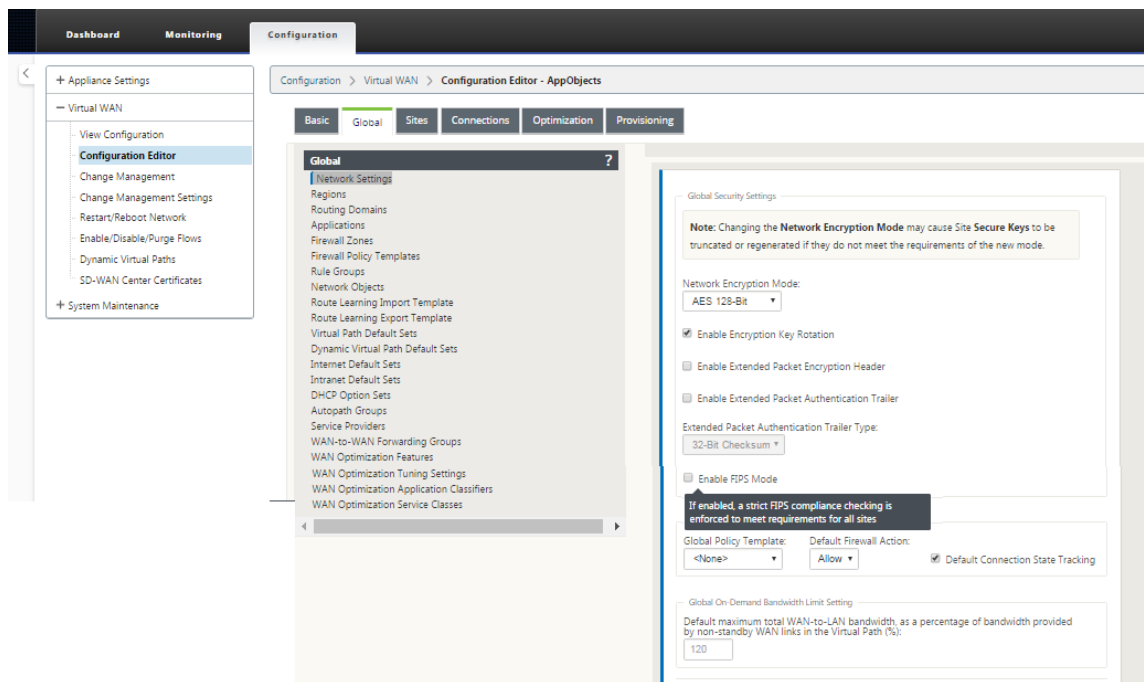
- DH Group 19: ECP256 (256-Bit-Elliptische Kurve) für Schlüsselerhandlungen
- 256-Bit-AES-CBC-Verschlüsselung
- SHA256-Hashing für die Nachrichtenauthentifizierung
- SHA256-Hashing für Nachrichtenintegrität
- DH Group 2: MODP-1024 für Perfect Forward Secrecy

Verwenden Sie die folgenden Einstellungen, um IPsec-Tunnel für einen Drittanbieter zu konfigurieren:

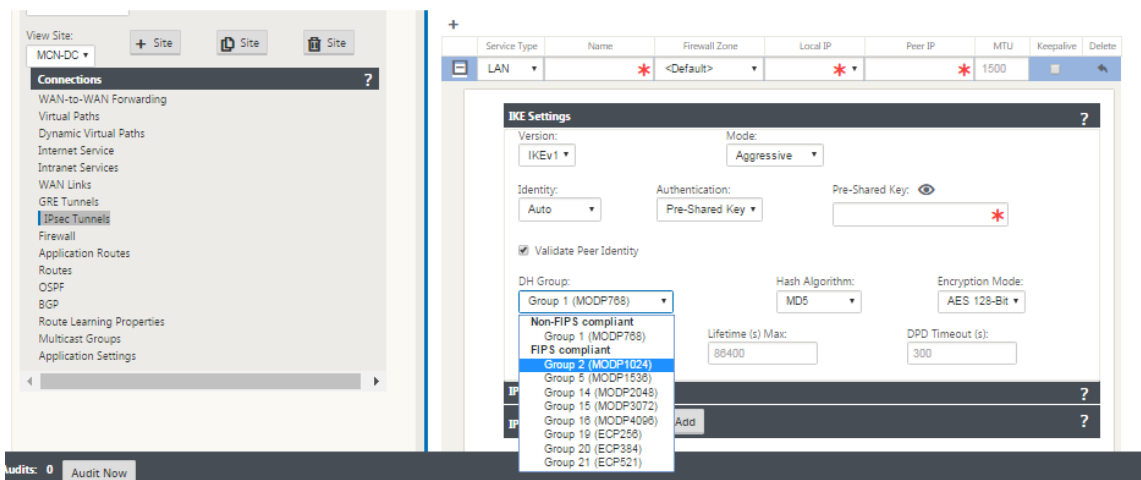
1. Konfigurieren Sie die FIPS-zugelassene DH-Gruppe. Gruppen 2 und 5 sind unter FIPS zulässig, aber Gruppen 14 und höher werden dringend empfohlen.
2. Konfigurieren Sie die FIPS-zugelassene Hash-Funktion. SHA1 wird von FIPS akzeptiert, jedoch wird SHA256 dringend empfohlen.
3. Wenn Sie IKEv2 verwenden, konfigurieren Sie eine von FIPS genehmigte Integritätsfunktion. SHA1 wird von FIPS akzeptiert, jedoch wird SHA256 dringend empfohlen.
4. Konfigurieren Sie eine IKE-Lebensdauer und maximale Lebensdauer von nicht mehr als 24 Stunden (86.400 Sekunden).
5. Konfigurieren Sie die IPsec-Nachrichtenauthentifizierung, indem Sie den IPsec-Modus in AH oder ESP+Auth ändern und eine FIPS-zugelassene Hashing-Funktion verwenden. SHA1 wird von FIPS akzeptiert, aber SHA256 wird dringend empfohlen.
6. Konfigurieren Sie eine IPsec-Lebensdauer und maximale Lebensdauer von höchstens acht Stunden (28.800 Sekunden).

So konfigurieren Sie IPsec-Tunnel:

1. Wechseln Sie auf der MCN-Appliance zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor**. Öffnen Sie ein vorhandenes Konfigurationspaket. Gehen Sie zu **Verbindungen > IPsec-Tunnel**.



2. Gehen Sie zu **Verbindungen > IPsec-Tunnel**. Wenn **LAN** oder **Intranettunnel** ausgewählt ist, unterscheidet der Bildschirm die FIPS-konformen Gruppen in den IKE-Einstellungen von denen, die nicht konform sind, sodass Sie die FIPS-Konformität problemlos konfigurieren können.



Der Bildschirm zeigt auch an, ob der Hash-Algorithmus FIPS-konform ist, wie in der folgenden Abbildung dargestellt.

+

| | Service Type | Name | Firewall Zone | Local IP | Peer IP | MTU | Keepalive | Delete |
|--|--------------|------|---------------|----------|---------|------|-----------|--------|
| | LAN | * | <Default> | * | * | 1500 | | |

IKE Settings

Version:

IKEv1

Mode:

Aggressive

Identity:

Auto

Authentication:

Pre-Shared Key

Pre-Shared Key:

☒ Validate Peer Identity

DH Group:

Group 1 (MODP768)

Hash Algorithm:

MD5

Encryption Mode:

AES 128-Bit

Lifetime (s):

3600

Lifetime (s) Max:

86400

DPD Timeout (s):

300

IPsec Settings

IPsec Protected Networks

+ Add

FIPS-Konformitätsoptionen für IPsec-Einstellungen:

+

| | Service Type | Name | Firewall Zone | Local IP | Peer IP | MTU | Keepalive | Delete |
|--|--------------|------|---------------|----------|---------|------|-----------|--------|
| | LAN | * | <Default> | * | * | 1500 | | |

IPsec Settings

Tunnel Type:

ESP

PFS Group:

<None>

Lifetime (s) Max:

86400

Lifetime (KB):

0

Lifetime (KB) Max:

0

Network Mismatch Behavior:

Drop

IPsec Protected Networks

+ Add

Wenn die IPsec-Konfiguration bei Aktivierung nicht den FIPS-Standards entspricht, kann ein Überwachungsfehler ausgelöst werden. Im Folgenden sind die Art der Überwachungsfehler, die in der GUI angezeigt werden.

- Wenn der FIPS-Modus aktiviert ist und nicht FIPS-kompatible Option ausgewählt ist.

- Wenn der FIPS-Modus aktiviert ist und ein falscher Lebensdauerwert eingegeben wird.
- Wenn der FIPS-Modus aktiviert ist und die IPsec-Einstellungen für den virtuellen Pfad ebenfalls aktiviert sind und der falsche Tunnelmodus ausgewählt ist (ESP vs ESP_Auth/AH).
- Wenn der FIPS-Modus aktiviert ist, werden auch IPsec-Einstellungen für den virtuellen Pfad aktiviert und ein falscher Lebensdauerwert eingegeben.

Secure Web Gateway für Citrix SD-WAN

May 10, 2021

Um Datenverkehr zu sichern und Richtlinien durchzusetzen, verwenden Unternehmen häufig MPLS-Links, um Zweigdatenverkehr in das Unternehmens-Rechenzentrum zurückzuleiten. Das Rechenzentrum wendet Sicherheitsrichtlinien an, filtert den Datenverkehr über Sicherheits-Appliances, um Malware zu erkennen, und leitet den Datenverkehr über einen ISP weiter. Ein solches Backhauling über private MPLS-Links ist teuer. Dies führt auch zu einer erheblichen Latenz, was zu einer schlechten Benutzererfahrung am Zweigstandort führt. Es besteht auch die Gefahr, dass Benutzer Ihre Sicherheitskontrollen umgehen.

Eine Alternative zum Backhauling ist das Hinzufügen von Sicherheits-Appliances in der Filiale. Die Kosten und Komplexität steigen jedoch, wenn Sie mehrere Appliances installieren, um konsistente Richtlinien auf den Websites aufrechtzuerhalten. Und wenn Sie viele Zweigstellen haben, wird das Kostenmanagement unpraktisch.

Zscaler:

Die ideale Lösung, um die Sicherheit ohne zusätzliche Kosten, Komplexität oder Latenz durchzusetzen, besteht darin, den gesamten Internetverkehr von der Citrix SD-WAN-Appliance an die Zscaler Cloud Security Platform weiterzuleiten. Anschließend können Sie eine zentrale Zscaler-Konsole verwenden, um detaillierte Sicherheitsrichtlinien für Ihre Benutzer zu erstellen. Die Richtlinien werden konsistent angewendet, unabhängig davon, ob sich der Benutzer im Rechenzentrum oder an einem Zweigstandort befindet. Da die Zscaler-Sicherheitslösung cloubasiert ist, müssen Sie dem Netzwerk keine weiteren Sicherheits-Appliances hinzufügen.

FIPS-Konformität:

Das National Institute for Standards and Technology (NIST) entwickelt Federal Information Processing Standards (FIPS) in Bereichen, für die keine freiwilligen Standards existieren. FIPS behebt die folgenden Probleme:

- Kompatibilität zwischen verschiedenen Systemen.
- Daten- und Software-Portabilität.
- Kostengünstige Computersicherheit und Datenschutz sensibler Informationen.

FIPS gibt die Sicherheitsanforderungen für ein kryptografisches Modul an, das in Sicherheitssystemen verwendet wird. Um diese Sicherheitsstandards auf die Verarbeitung einer Citrix SD-WAN Appliance anzuwenden, konfigurieren Sie den FIPS-Modus.

Kraftpunkt:

Mit Citrix SD-WAN können Sie die Funktion Firewallumleitung (transparenter Proxy nach Ziel-NAT) verwenden, um den Internetverkehr (HTTP und HTTPS) von einer SD-WAN-Appliance am Unternehmensrand zum Cloud-gehosteten Sicherheitsmodul von Forcepoint umzuleiten. Sie können HTTP-Datenverkehr von Port 80 zu Port 8081 und HTTPS-Datenverkehr von Port 443 zu Port 8443 des nächsten Forcepoint-Cloud-Proxy-Servers umleiten.

Zscaler Integration mit GRE-Tunneln und IPsec-Tunneln

October 28, 2021

Die Zscaler Cloud Security Platform fungiert als eine Reihe von Sicherheitskontrollen in mehr als 100 Rechenzentren auf der ganzen Welt. Indem Sie Ihren Internetverkehr einfach an Zscaler umleiten, können Sie Ihre Geschäfte, Filialen und Remotestandorte sofort sichern. Zscaler verbindet Benutzer und das Internet und überprüft jedes Byte des Datenverkehrs, auch wenn er verschlüsselt oder komprimiert ist.

Citrix SD-WAN-Appliances können über GRE-Tunnel am Standort des Kunden eine Verbindung zu einem Zscaler-Cloud-Netzwerk herstellen. Eine Zscaler-Bereitstellung mit SD-WAN-Appliances unterstützt die folgenden Funktionen:

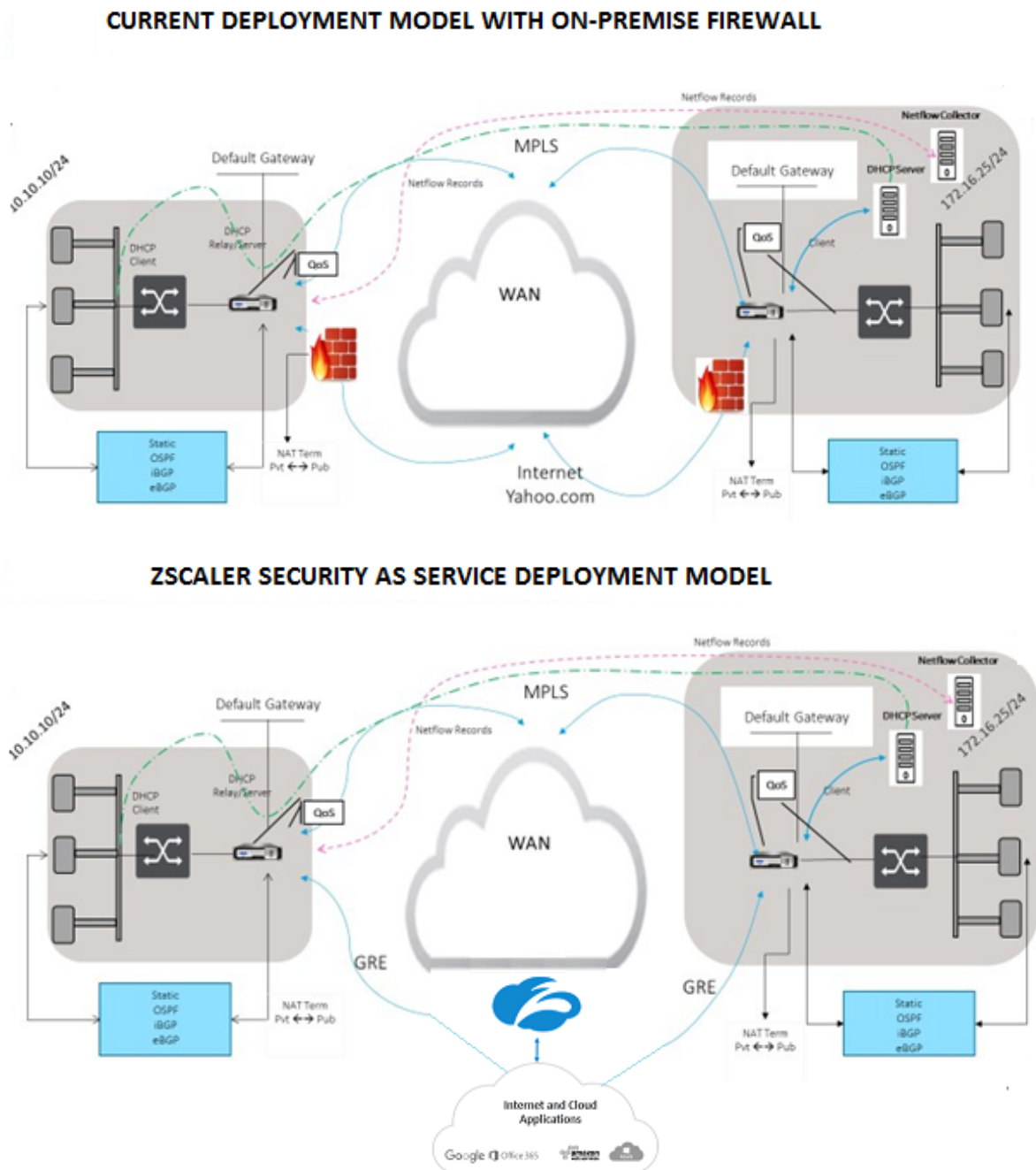
- Weiterleiten des gesamten GRE-Datenverkehrs an Zscaler, wodurch ein direktes Internetbreak-out möglich ist.
- Direkter Internetzugang (DIA) mit Zscaler pro Kundenstandort.
 - Auf einigen Websites möchten Sie DIA möglicherweise on-premises Sicherheitsausrüstung zur Verfügung stellen und Zscaler nicht verwenden.
 - Auf einigen Websites können Sie den Traffic auf einer anderen Kundenseite für den Internetzugang zurückholen.
- Virtuelle Routing- und Weiterleitungsbereitstellungen.
- Ein WAN-Link als Teil von Internetdiensten.

Zscaler ist ein Cloud-Dienst. Sie müssen es als Service einrichten und die zugrunde liegenden WAN-Links definieren:

- Konfigurieren Sie einen Internetdienst im Rechenzentrum und verzweigen Sie über GRE.

- Konfigurieren Sie eine vertrauenswürdige öffentliche Internetverbindung im Rechenzentrum und an den Zweigstellen.

Topologie



So verwenden Sie den GRE Tunnel oder den IPsec-Tunnel Traffic-Weiterleitung:

1. Melden Sie sich unter: im Zscaler-Hilfeportal an: <https://help.zscaler.com/submit-ticket>.

2. Erhöhen Sie ein Ticket und geben Sie die statische öffentliche IP-Adresse an, die als GRE-Tunnel oder IPsec-Tunnelquelladresse verwendet wird.

Zscaler verwendet die Quell-IP-Adresse, um die IP-Adresse des Kunden zu identifizieren. Die Quell-IP muss eine statische öffentliche IP sein. Zscaler antwortet mit zwei ZEN-IP-Adressen (Primär und Sekundär), um Datenverkehr zu übertragen. GRE-Keep-Alive-Nachrichten können verwendet werden, um den Zustand der Tunnel zu bestimmen.

Zscaler verwendet den Wert der Quell-IP-Adresse, um die Kunden-IP-Adresse zu identifizieren. Dieser Wert muss eine statische öffentliche IP-Adresse sein. Zscaler antwortet mit zwei ZEN-IP-Adressen [DR1], an die der Datenverkehr umgeleitet werden soll. GRE Keep-Alive-Nachrichten können verwendet werden, um den Zustand der Tunnel zu bestimmen.

Beispiel für IP-Adressen

Primary

Interne Router-IP-Adresse: 172.17.6.241/30

Interne ZEN-IP-Adresse: 172.17.6.242/30

Secondary

Interne Router-IP-Adresse: 172.17.6.245/30

Interne ZEN-IP-Adresse: 172.17.6.246/30

Konfigurieren eines Internetdienstes

So konfigurieren Sie einen Internetdienst:

1. Navigieren Sie zu **Verbindungen- Internetdienste**. Konfigurieren Sie den Internetdienst.
2. Wählen Sie **+ Service** und aktivieren Sie die Einstellungen (Grundeinstellungen, WAN-Links und Regeln) nach Bedarf.
3. Wählen Sie **Übernehmen**.

Weitere Informationen zum Aktivieren des Internetdienstes für eine Site finden Sie unter [Direct Internet Breakout in der Zweigstelle mit integrierter Firewall](#).

Sie können die folgenden Einstellungen für einen Internetdienst konfigurieren:

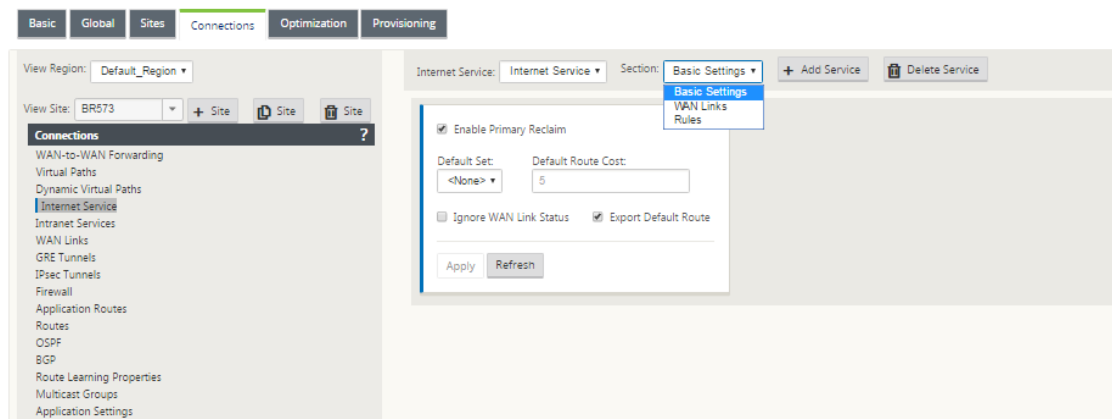
- [Grundeinstellungen](#)
- [WAN-Links](#)
- [Regeln](#)

Grundeinstellungen

Eine Firewall-Zoneneinstellung ist für einen Internetdienst nicht konfigurierbar. Wenn dem Internetdienst vertraut wird, wird er **Internet_Zone** zugewiesen. Wenn der Internetdienst nicht vertrauenswürdig ist, wird er **Untrusted_Internet_Zone** zugewiesen.

Die grundlegenden Einstellungen, die konfigurierbar sind, werden nachstehend beschrieben:

- **Primäre Rückforderung aktivieren:** Wenn diese Option aktiviert ist, wird die (use = primäre) Nutzung, die mit diesem Dienst auf einem WAN-Link verbunden ist, den Status als aktiver Dienst auf dieser WAN-Verbindung gewaltsam zurückerobert.
- **Standardsatz:** Name des Internet-Standardsatzes, der Regeln für den Internetdienst auf der Site ausfüllt.
- **Standardroutenkosten:** Routenkosten, die mit der standardmäßigen Internetroute (0.0.0.0/0) verknüpft sind.
- **WAN-Link-Status ignorieren:** Wenn diese Option aktiviert ist, wählen Pakete, die für diesen Dienst bestimmt sind, diesen Dienst immer noch aus, auch wenn alle WAN-Verbindungen für diesen Dienst nicht verfügbar sind.
- **Standardroute exportieren:** Wenn diese Option aktiviert ist, wird die Standardroute für den Internetdienst, 0.0.0.0/0, auf andere Sites exportiert, wenn die WAN-zu-WAN-Weiterleitung aktiviert ist.



WAN-Links

Die konfigurierbaren WAN-Link-Einstellungen werden nachstehend beschrieben:

- **Benutzen:** Erlauben Sie dem Dienst, diesen WAN-Link zu verwenden. Wenn Verwenden deaktiviert ist, sind alle anderen Optionen nicht verfügbar.
- **Modus:** Der Modus des Dienstes —Primär, Sekundär oder Balance, für Verkehrsredundanz oder Lastausgleich.

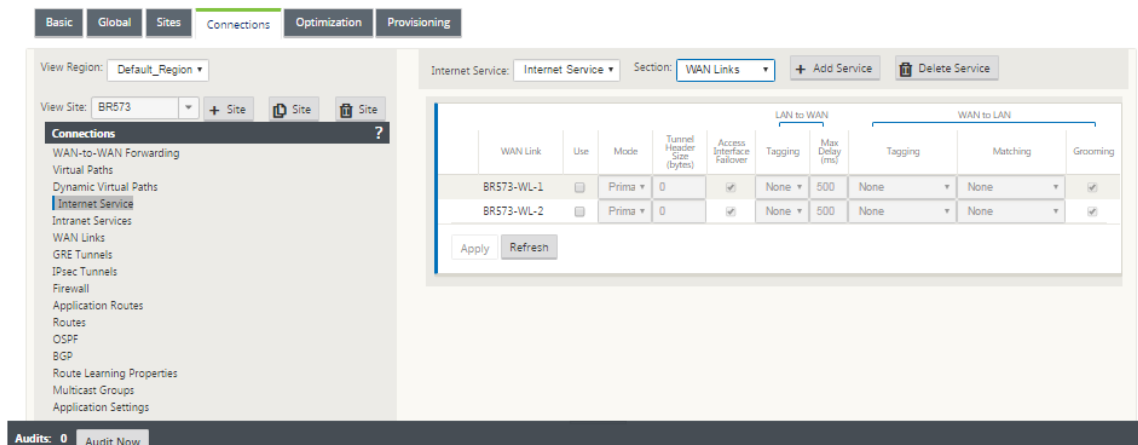
- **Tunnelkopfgröße (Byte):** Die Größe des Tunnelkopfs, falls zutreffend, in Byte.
- **Access Interface Failover:** Wenn diese Option aktiviert ist, können Internet- oder Intranet-Pakete mit nicht übereinstimmenden VLANs den Dienst weiterhin verwenden.

LAN zu WAN

- **Tagging:** Das DSCP-Tag, das auf LAN auf WAN-Pakete im Dienst angewendet werden soll.
- **Max Delay (ms):** Die maximale Zeit in Millisekunden, um Pakete zu puffern, wenn die WAN-Link-Bandbreite überschritten wird.

WAN zu LAN

- **Tagging:** Das DSCP-Tag, das auf WAN auf LAN-Pakete im Dienst angewendet werden soll.
- **Passend:** Internet-WAN zu LAN-Pakete, die diesem Tag entsprechen, werden dem Dienst zugewiesen.
- **Grooming:** Wenn diese Option aktiviert ist, werden Pakete nach dem Zufallsprinzip verworfen, um zu verhindern, dass der WAN-zu-LAN-Datenverkehr die bereitgestellte Bandbreite des Dienstes überschreitet.



Regeln

Der Internetverkehr wird anhand der definierten Regeln identifiziert. Eine Regeldefinition wird verwendet, um einen bestimmten Verkehrsfluss abzugleichen. Nach dem Abgleich müssen Sie die Aktion definieren, um den Verkehrsfluss zu beantragen.

Die Liste der verfügbaren Regeln wird nachstehend beschrieben:

- **Reihenfolge:** Die Reihenfolge, in der Regeln angewendet und automatisch neu verteilt werden.

- **Regelgruppenname:** Name einer Regel, die es ermöglicht, Regelstatistiken in Gruppen zu summieren, wenn sie angezeigt werden. Alle Statistiken für Regeln mit demselben Regelgruppennamen können zusammen angezeigt werden.
- **Quelle:** Die Quell-IP-Adresse und Subnetzmaske, die mit der Regel übereinstimmen.
- **Dest-Src:** Wenn aktiviert, wird die Quell-IP-Adresse auch als Ziel-IP-Adresse verwendet.
- **Ziel:** Die Ziel-IP-Adresse und Subnetzmaske, die mit der Regel übereinstimmen.
- **Protokoll:** Der Protokollname, der mit dem Filter übereinstimmt.
- **Protokoll #:** Die Protokollnummer, die mit dem Filter übereinstimmt.
- **DSCP:** Das DSCP-Tag im IP-Header, das mit der Regel übereinstimmt.

Die Liste der verfügbaren Aktionen wird nachstehend beschrieben:

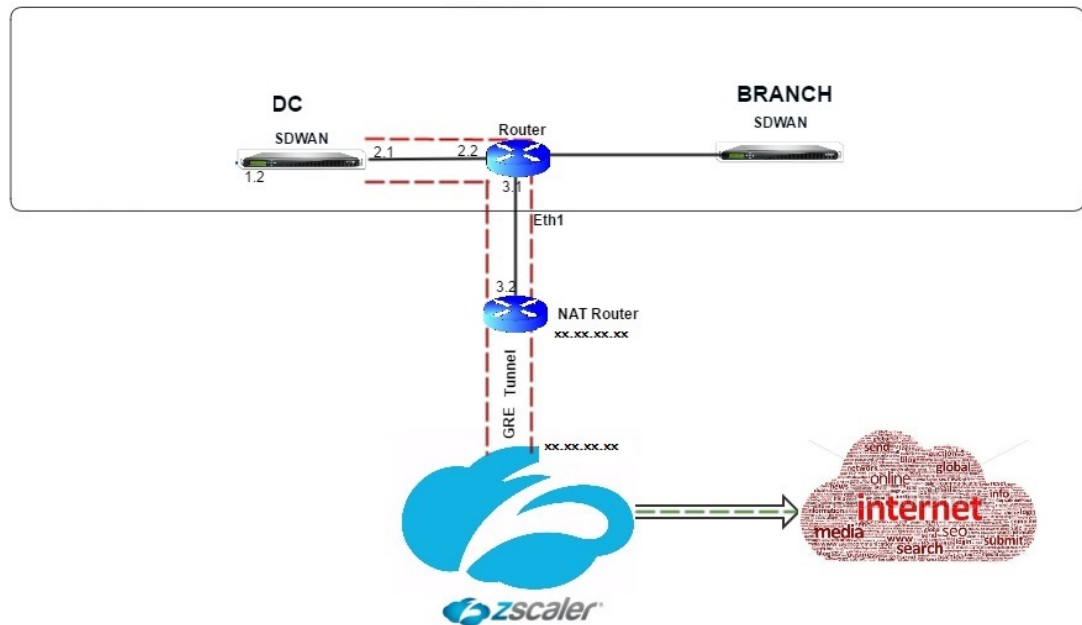
- **WAN-Verbindung:** Die WAN-Verbindung, die von Flows verwendet wird, die der Regel entsprechen, wenn der Internet-Lastausgleich aktiviert ist.
- **Dienst überschreiben:** Der Zieldienst für Flows, die der Regel entsprechen.
 - **Verwerfen:** Lass den Verkehr fallen.
 - **Passthrough:** Ordnen Sie den Fluss dem Passthrough zu und lassen Sie den Datenverkehr unverändert durch die Appliance fließen.

The screenshot shows the 'Rules' configuration page in the Citrix SD-WAN management console. At the top, there are tabs for 'Internet Service' and 'Rules', along with '+ Add Service' and 'Delete Service' buttons. Below this is a table with the following columns: Order, Rule Group Name, Source, Dest-Src, Dest, Protocol, Protocol #, Source, Dest-Src, Dest, DSCP, VLAN, and a set of action buttons (Rebind Flow on Change, Delete, Clone). The first row in the table has the value '100' in the Order column and '<None>' in the Rule Group Name column. Below the table, there is a configuration panel with the following options: Mode (set to 'WAN Link'), WAN Link (set to '<N/A>'), Override Service (set to '<N/A>'), and a checkbox for 'Enable Passive FTP Detection'. At the bottom of the panel are 'Apply' and 'Revert' buttons.

Konfigurieren von GRE-Tunnel

1. Die Quell-IP-Adresse ist die IP-Adresse von Tunnel Source. Wenn für die Tunnelquellen-IP-Adresse NAT verwendet wird, ist die Public Source IP-Adresse die öffentliche Tunnelquellen-IP-Adresse, auch wenn sie auf einem anderen Zwischengerät NAT verwendet.
2. Die Ziel-IP-Adresse ist die ZEN-IP-Adresse, die Zscaler bereitstellt.
3. Die Quell-IP-Adresse und die Ziel-IP-Adresse sind die GRE-Header des Routers, wenn die ursprüngliche Nutzlast gekapselt ist.

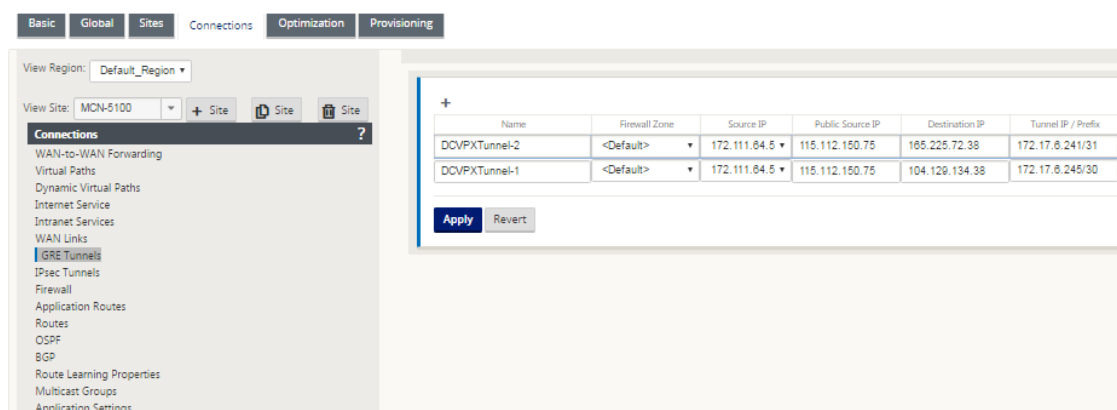
4. Tunnel-IP-Adresse und Präfix sind die IP-Adressierung im GRE-Tunnel selbst. Dies ist nützlich, um den Verkehr über den GRE-Tunnel zu leiten. Der Verkehr benötigt diese IP-Adresse als Gateway-Adresse.



So konfigurieren Sie GRE-Tunnel:

1. Navigieren Sie im Konfigurationseditor zu **Verbindungen > Standort > GRE-Tunnel** und konfigurieren Sie Routen, um Internet-Präfixdienste an die Zscaler GRE-Tunnel weiterzuleiten.

Die Quell-IP-Adresse kann nur auf vertrauenswürdigen Links aus der virtuellen Netzwerkschnittstelle ausgewählt werden. Siehe, [So konfigurieren Sie den GRE-Tunnel](#).



Konfigurieren von Routen für GRE-Tunnel

Konfigurieren Sie Routen, um Internet-Präfix-Dienste an die Zscaler GRE-Tunnel weiterzuleiten.

- Die ZEN-IP-Adresse (Tunnelziel-IP, in der obigen Abbildung als 104.129.194.38 dargestellt) muss auf Internet vom Typ Dienst eingestellt sein. Dies ist erforderlich, damit der für Zscaler bestimmte Datenverkehr vom Internetdienst abgerechnet wird.
- Der gesamte Verkehr, der nach Zscaler bestimmt ist, muss mit der Standardroute 0/0 übereinstimmen und über den GRE-Tunnel übertragen werden. Stellen Sie sicher, dass die für [DR1] den GRE-Tunnel verwendete 0/0-Route niedrigere Kosten verursacht als Passthrough oder ein anderer Servicetyp.
- Ebenso muss der Backup GRE Tunnel zu Zscaler höhere Kosten haben als die des primären GRE Tunnels.
- Stellen Sie sicher, dass nicht rekursive Routen für die ZEN-IP-Adresse existieren.

So konfigurieren Sie Routen für den GRE Tunnel:

1. Navigieren Sie zu **Verbindungen > Standort > Routen**, und befolgen Sie die unter [Konfigurieren von Routen](#) beschriebenen Verfahren, um Anweisungen zum Erstellen von Routen zu erhalten.

The screenshot shows the 'Routes' configuration page in the Citrix SD-WAN interface. The left sidebar contains a navigation menu with the following items: WAN-to-WAN Forwarding, Virtual Paths, Dynamic Virtual Paths, Internet Service, Intranet Services, WAN Links, GRE Tunnels, IPsec Tunnels, Firewall, Application Routes, **Routes**, OSPF, BGP, Route Learning Properties, Multicast Groups, and Application Settings. The main area displays a table of configured routes.

| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|------|--------------|--------------|--------------------|------|------|--------|
| 1 | 104.129.194.38/32 | 5 | Internet | | | ⓘ | ✎ | 🗑️ |
| 2 | 165.225.72.38/32 | 5 | Internet | | | ⓘ | ✎ | 🗑️ |
| 3 | 172.17.6.241/30 | 5 | GRE Tunnel | | 165.225.72.38 | ⓘ | | |
| 4 | 172.17.6.245/30 | 5 | GRE Tunnel | | 104.129.194.38 | ⓘ | | |
| 5 | 172.16.1.2/24 | 5 | Local | | | ⓘ | | |
| 6 | 172.16.4.0/24 | 5 | Local | | 172.16.1.1 | ⓘ | ✎ | 🗑️ |
| 7 | 0.0.0.0/0 | 3 | GRE Tunnel | | 172.17.6.242 | ⓘ | ✎ | 🗑️ |
| 8 | 0.0.0.0/0 | 4 | GRE Tunnel | | 172.17.6.246 | ⓘ | ✎ | 🗑️ |
| 9 | 0.0.0.0/0 | 5 | Internet | | | ⓘ | | |
| 10 | 0.0.0.0/0 | 16 | Passthrough | | | ⓘ | | |

At the bottom of the table, there are navigation buttons: «, <, 1, >, ».

Hinweis

Wenn Sie keine spezifischen Routen für die Zscaler-IP-Adresse haben, konfigurieren Sie das Routenpräfix 0.0.0.0/0 so, dass es mit der ZEN-IP-Adresse übereinstimmt, und leiten Sie es durch eine GRE-Tunnelkapselungsschleife. Diese Konfiguration verwendet die Tunnel in einem Aktiv-Backupmodus. Mit den in der obigen Abbildung dargestellten Werten wechselt der Datenverkehr automatisch in den Tunnel mit Gateway-IP-Adresse 172.17.6.242. Konfigurieren Sie bei Bedarf eine virtuelle Backhaul-Pfadroute. Andernfalls setzen Sie das Keep-Alive-Intervall des Backup-Tunnels auf Null. Dies ermöglicht einen sicheren Internet-

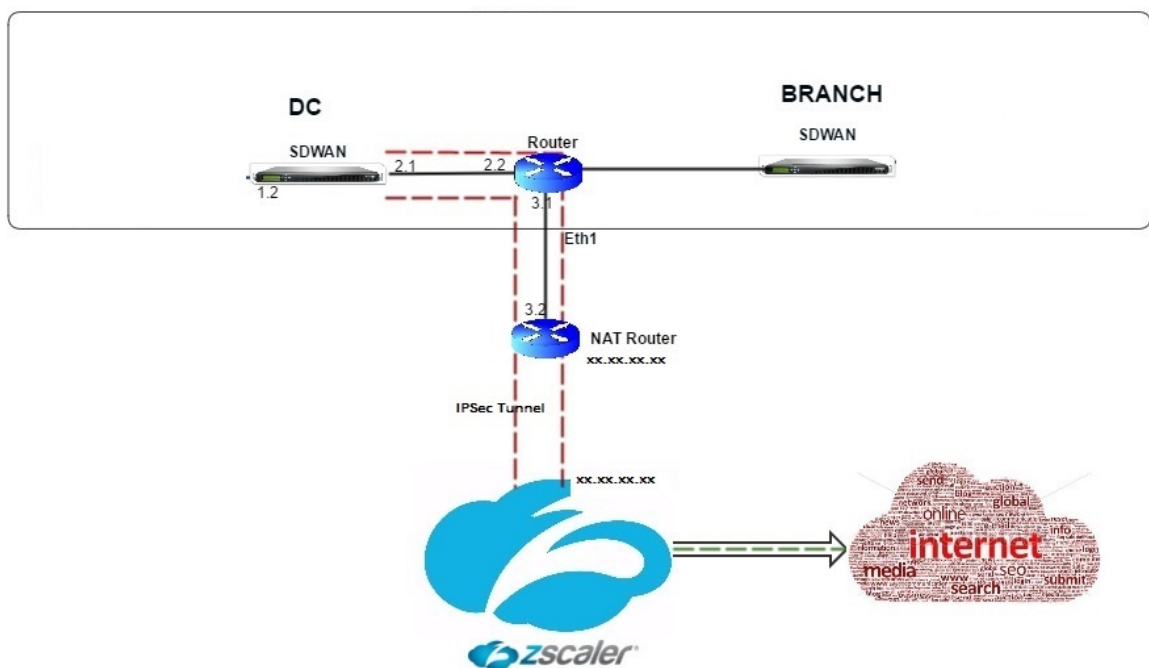
zugriff auf eine Site, auch wenn beide Tunnel zu Zscaler ausfallen.

GRE-Keep-Alive-Nachrichten werden unterstützt. Ein neues Feld mit der Bezeichnung **Public Source IP**, das die NAT-Adresse der GRE-Quelladresse bereitstellt, wird der Citrix SD-WAN GUI-Schnittstelle hinzugefügt (wenn die SD-WAN-Appliance Tunnel Source NAT von einem Zwischengerät verwendet). Die Citrix SD-WAN GUI enthält ein Feld mit der Bezeichnung Public Source IP, das die NAT-Adresse der GRE-Quelladresse bereitstellt, wenn die Tunnelquelle der Citrix SD-WAN Appliance NAT von einem Zwischengerät verwendet.

Einschränkungen

- Mehrere VRF-Bereitstellungen werden nicht unterstützt.
- Primäre Backup-GRE-Tunnel werden nur für einen Entwurfsmodus mit hoher Verfügbarkeit unterstützt.

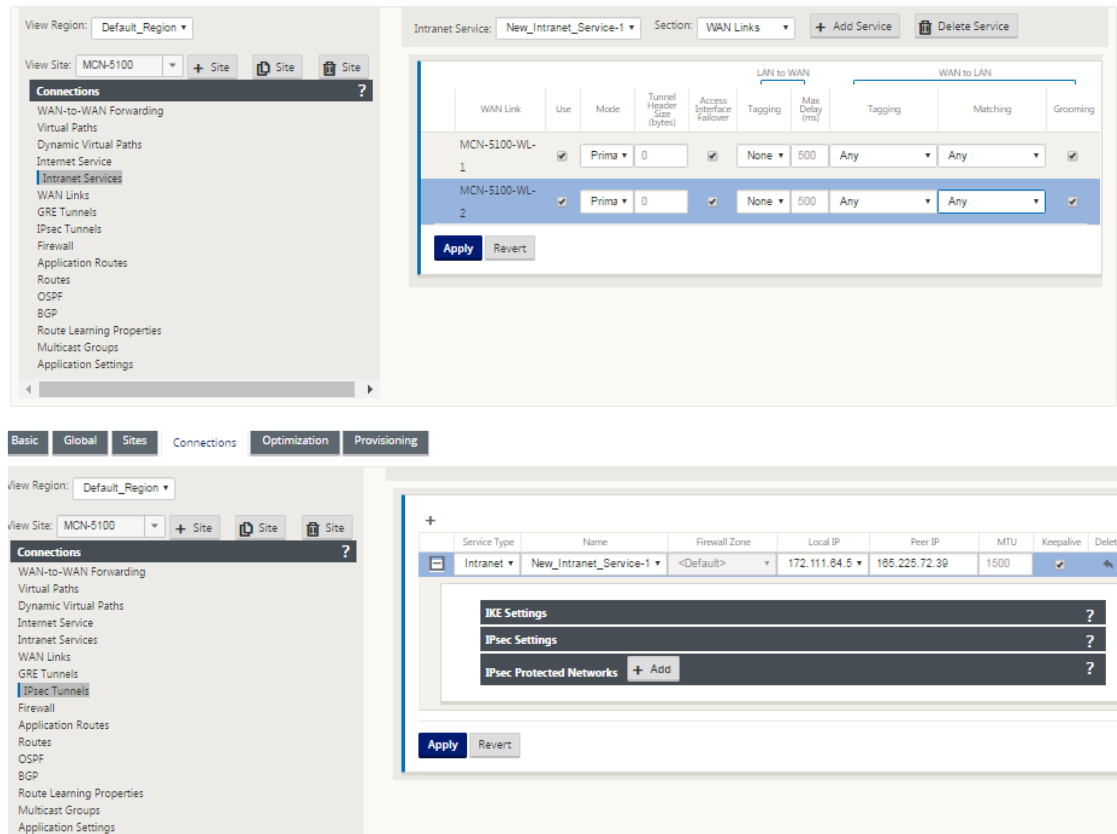
Konfigurieren von IPsec-Tunnels



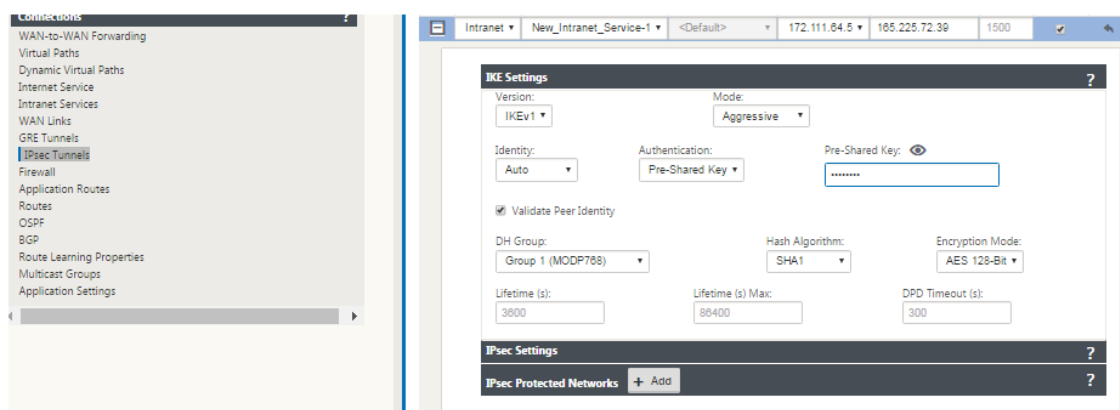
So konfigurieren Sie IPsec-Tunnel für Intranet- oder LAN-Dienste in der Benutzeroberfläche der Citrix SD-WAN Appliance:

1. Navigieren Sie im Konfigurationseditor zu **Verbindungen** > **<SiteName>** > **IPsec-Tunnel** und wählen Sie einen Dienstyp (LAN oder Intranet).

2. Geben Sie einen Namen für die Servicetyp ein. Für den Intranetdiensttyp bestimmt der konfigurierte Intranetserver, welche lokalen IP-Adressen verfügbar sind.
3. Wählen Sie die verfügbare lokale IP-Adresse aus und geben Sie die Peer-IP-Adresse für den virtuellen Pfad zum Remote-Peer ein.



4. Wählen Sie **IKEv1** für **IKE-Einstellungen**. Zscaler unterstützt nur IKEv1.



5. Wählen Sie unter IPsec-Einstellungen **ESP-NUL** für **Tunnel** aus, um den Datenverkehr über den IPsec-Tunnel nach Zscaler umzuleiten. Der IPsec-Tunnel verschlüsselt den Datenverkehr nicht.

IKE Settings?

IPsec Settings?

Tunnel Type:

ESP+NULL

PFS Group:

<None>

Hash Algorithm:

SHA1

Lifetime (s):

28800

Lifetime (s) Max:

86400

Lifetime (KB):

0

Lifetime (KB) Max:

0

Network Mismatch Behavior:

Drop

IPsec Protected Networks

+ Add

?

6. Da der Internetverkehr umgeleitet wird, kann die Ziel-IP/das Präfix eine beliebige IP-Adresse sein.

IKE Settings?

Version:

IKEv1

Mode:

Aggressive

Identity:

Auto

Authentication:

Pre-Shared Key

Pre-Shared Key:

.....

☒ Validate Peer Identity

DH Group:

Group 1 (MODP768)

Hash Algorithm:

SHA1

Encryption Mode:

AES 128-Bit

Lifetime (s):

3600

Lifetime (s) Max:

86400

DPD Timeout (s):

300

IPsec Settings

?

IPsec Protected Networks

+ Add

?

| Source IP/Prefix | Destination IP/Prefix | Delete |
|------------------|-----------------------|--------|
| 172.16.4.0/24 | 0.0.0.0/0 | |

Apply

Revert

Weitere Informationen zum Konfigurieren von IPSec-Tunneln mit der Citrix SD-WAN-Weboberfläche

finden Sie unter [IPsec-Tunnel](#).

Konfigurieren von Routen für IPsec-Tunnel

So konfigurieren Sie IPsec-Routen:

1. Navigieren Sie zu **Verbindungen > DC > Routen**, und befolgen Sie die unter [Konfigurieren von Routen](#) beschriebenen Verfahren, um Anweisungen zum Erstellen von Routen zu erhalten.

| Order | Network IP Address | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|------|--------------|----------------------|--------------------|------|------|--------|
| 1 | 165.225.72.39/32 | 5 | Intranet | New_Intranet_Service | | ⓘ | ✎ | 🗑️ |
| 2 | 172.16.1.2/24 | 5 | Local | | | ⓘ | | |
| 3 | 172.16.4.0/24 | 5 | Local | | 172.16.1.1 | ⓘ | ✎ | 🗑️ |
| 4 | 0.0.0.0/0 | 5 | Intranet | New_Intranet_Service | | ⓘ | | |
| 5 | 0.0.0.0/0 | 5 | Internet | | | ⓘ | | |
| 6 | 0.0.0.0/0 | 16 | Passthrough | | | ⓘ | | |

So überwachen Sie GRE- und IPsec-Tunnelstatistiken:

Navigieren Sie im SD-WAN-Webinterface zu **IPsec-Tunnel**.

Überwachung > Statistiken > [GRE-Tunnel

Weitere Informationen finden Sie unter [Überwachung von IPsec-Tunneln](#) und [GRE-Tunneln](#).

Unterstützung der Firewall-Verkehrsumleitung mithilfe von Forcepoint in Citrix SD-WAN

May 10, 2021

Forcepoint unterstützt die folgenden Funktionen, obwohl SD-WAN nur die Firewallumleitungsfunktion unterstützt:

- IPsec mit PKI
- IPsec mit PSK

- Proxy-Verkettung mit PAC-Dateikonfiguration
- Proxy-Verkettung mit Standard-Headern
- Proxy-Verkettung mit proprietären Headern entfällt die Notwendigkeit, den IP-Bereich des Clients zu konfigurieren - Partnerschaft/Entwicklung
- Firewall-Umleitung (transparenter Proxy nach Ziel-NAT)

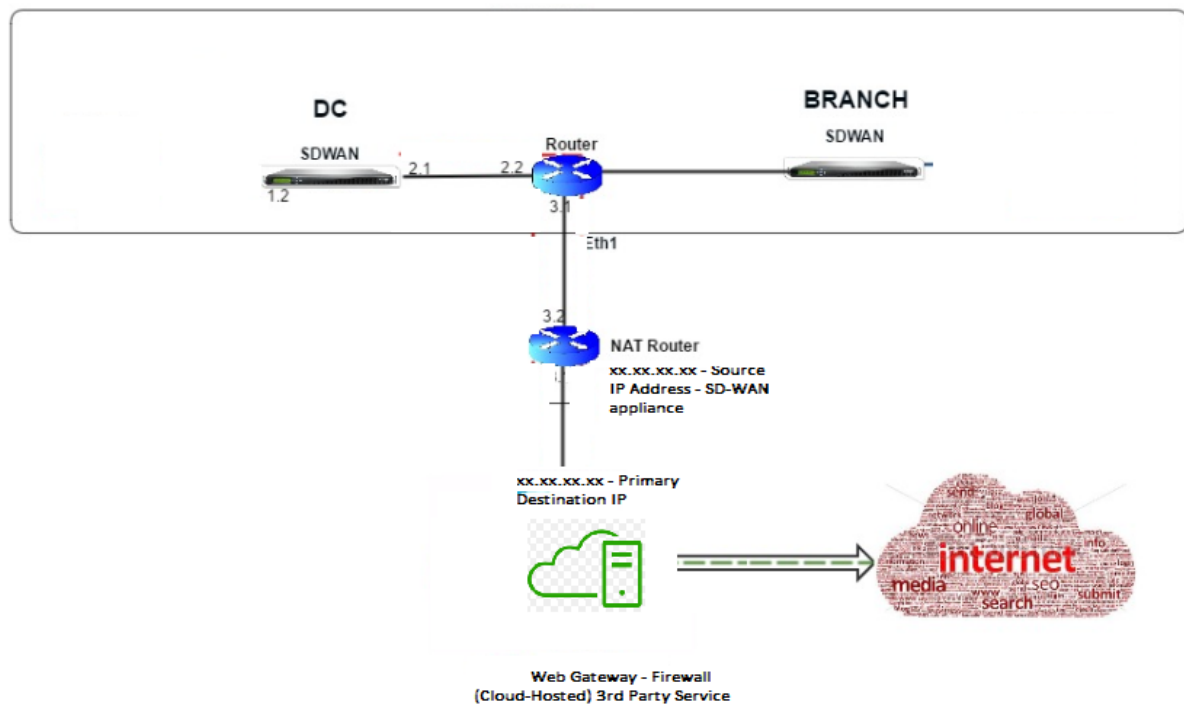
Mit der Ziel-NAT-Richtlinie können Unternehmen den Internetverkehr über den cloudgehosteten Sicherheitsdienst mithilfe von ForcePoint weiterleiten.

Lesen Sie den folgenden Anwendungsfall, um zu verstehen, wie Sie Destination NAT in SD-WAN-Appliances konfigurieren und Internetverkehr über einen sicheren cloudbasierten Firewalldienst umleiten.

Voraussetzungen:

1. Melden Sie sich bei der [anForcepoint Portalwebsite](#). Erstellen Sie eine Richtlinie, indem Sie die öffentliche Enterprise-IP-Adresse angeben, über die der Internetverkehr an Forcepoint umgeleitet werden muss. Rufen Sie die primären und sekundären IP-Adressen ab, an die der Internetverkehr umgeleitet werden soll.
2. Konfigurieren Sie in der SD-WAN-GUI auf einer SD-WAN-Appliance am DC-Standort den Internetdienst, der WAN-Verbindungen zugeordnet ist.
3. Ziel NAT wird unter Verwendung der Ziel-IP-Adresse des Internetverkehrs durchgeführt. Diese Zieladresse wird in die öffentliche Forcepoint-IP-Adresse geändert.
4. Konfigurieren Sie die Ziel-NAT-Richtlinie, indem Sie die Quell-IP-Adresse und die primäre IP-Adresse angeben. Die Quell-IP ist die Internet-IP-Adresse der SD-WAN-Appliance innerhalb der Ports 80 (http) und 443 (https), die in die primäre Ziel-IP-Adresse des cloudbasierten Firewall-Gateway mit externen Ports 8081 (http) bzw. 8443 (https) umgeleitet bzw. übersetzt wird.
5. Stellen Sie nach der Konfiguration der DNAT-Richtlinie sicher, dass für die auf dem Domänencontroller konfigurierten Routen der Internetdiensttyp für die IP-Adresse des SD-WAN-Netzwerks ausgewählt ist.

Weitere Informationen zur NAT-Unterstützung in Citrix SD-WAN finden Sie im folgenden Thema [NAT konfigurieren](#)



Konfigurieren von Ziel-NAT (DNAT)

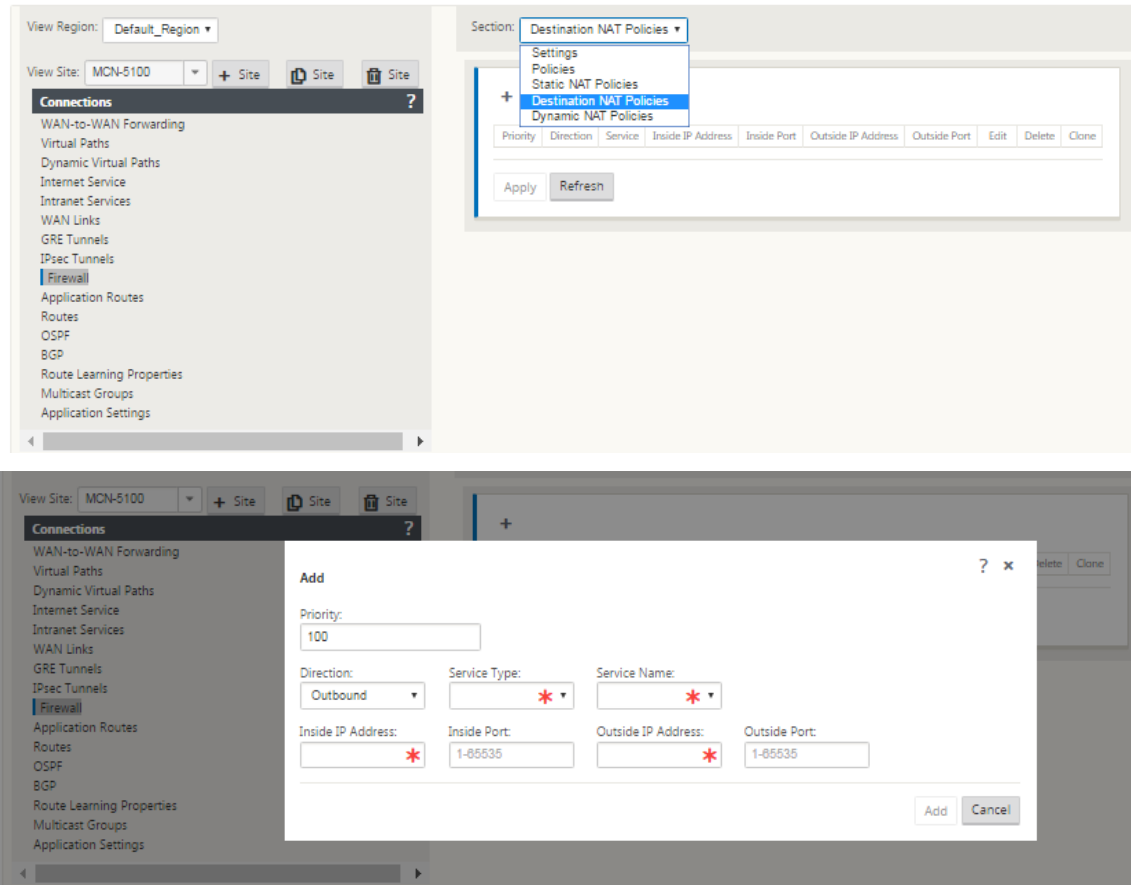
Verwenden Sie die Citrix SD-WAN GUI, um Destination NAT (DNAT) zu konfigurieren. Fügen Sie in der Konfiguration eine oder mehrere DNAT Richtlinien hinzu, die den Datenverkehr umleiten, der einer bestimmten Ziel-IP-Adresse und -port entspricht.

So konfigurieren Sie Ziel-NAT:

Gehen Sie in der SD-WAN SE/VPX GUI zu **Konfiguration** -> **Virtuelles WAN** -> Konfigurations-Editor. Klicken Sie auf **Öffnen**, um ein vorhandenes Paket zu öffnen. Wählen Sie ein gespeichertes Konfigurationspaket aus. Sie können auch DNAT Regeln erstellen, während Sie die Netzwerkkonfiguration erstellen.

1. Konfigurieren Sie Internetdienst am Domänencontroller (MCN). Gehen Sie zu **Verbindungen** -> **Firewall**.
2. Klicken Sie auf **+ Hinzufügen**, um eine DNAT Richtlinie hinzuzufügen.
3. **Geben Sie im Dialogfeld Ziel-NAT-Richtlinie hinzufügen** die folgenden Informationen ein:
 - Priorität
 - Richtung
 - Servicetyp
 - Servicename
 - Interne IP-Adresse

- Interner Port
- Externe IP-Adresse
- Externer Port



4. Bereitstellen von Ziel-NAT-Regeln für die Firewallverkehrsumleitung, ähnlich wie statische NAT-Regeln.
5. Geben Sie die übereinstimmenden Kriterien und die Ziel-IP/Port ein, für die NAT angewendet werden soll.
6. Führen Sie die Verbindungsabstimmung der DNAT Regel mit Statistiken durch.
7. Entfernen oder Aktualisieren von DNAT Regeln während der Konfigurationsupdates.

Überwachen einer Ziel-NAT-Richtlinie (Firewall)

Sie können auch die Citrix SD-WAN GUI verwenden, um die aktuelle DNAT-Richtlinienkonfiguration zu überwachen.

So überwachen Sie die aktuelle Ziel-NAT Richtlinienkonfiguration:

1. Navigieren Sie in der Citrix SD-WAN GUI zu **Überwachung > Firewall > NAT-Richtlinien**.

2. Wählen Sie die Registerkarte mit den Statistiken aus, die Sie überwachen möchten.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any

Service Type: Any Service Name: Any

Inside IP: * Inside Port: * Outside IP: * Outside Port: *

Refresh

Show latest data.

Help

NAT Policies

| ID | Rule Type | Rule Parent | Direction | IP Protocol | Service Type | Service Name | Inside IP Address | Port | Outside IP Address | Port | Allow Related | Allow IPsec Passthrough | Allow GRE Passthrough | Packets Sent | Bytes Sent | Packets Received | Bytes Received | Connections | Related Objects |
|----|------------|-------------|-----------|-------------|--------------|--------------|-------------------|------|--------------------|---------|---------------|-------------------------|-----------------------|--------------|------------|------------------|----------------|-------------|-----------------|
| 1 | Dynamic PR | - | Outbound | * | Internet | - | * | * | 172.16.2.101/32 | 0-65535 | No | No | No | 253825 | 26477410 | 452674 | 614179776 | 3 | [Connections] |

NAT Policies Displayed: 1
NAT Policies In Use: 1/100
Port Restricted Dynamic NAT Policies In Use: 1/100
Destination NAT Policies In Use: 0/100

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

Monitoring > Firewall

Firewall Statistics

Statistics: Connections

Maximum entries to display: 1

Filtering: NAT Policies

IP Protocol: Any Family: Any

Source Service Type: Any Source Zone: Any

Destination Service Type: Any Destination Zone: Any

Source Service Instance: Any Source IP: *

Destination Service Instance: Any Destination IP: *

Source Port: *

Destination Port: *

Refresh

Show latest data

Show Drops

Clear Connections

Help

Connections

| Application | Family | IP Protocol | IP Address | Port | Service Type | Service Name | Zone | IP Address | Port | Service Type | Service Name | Zone | State |
|--------------------------|-----------------|-------------|-------------|-------|--------------|-------------------|------------------|-------------|------|--------------|-----------------|---------------|-------------|
| Domain Name Service(dns) | Network Service | UDP | 172.16.6.10 | 36080 | Virtual Path | DC-MCN-BR1-CB2000 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | DC-MCN-Internet | Internet_Zone | ESTABLISHED |
| Domain Name Service(dns) | Network Service | UDP | 172.16.16.1 | 56451 | Virtual Path | DC-MCN-BR1-CB2000 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | DC-MCN-Internet | Internet_Zone | ESTABLISHED |

Palo Alto Integration mit IPsec-Tunneln

May 10, 2021

Palo Alto Netzwerke bieten cloudbasierte Sicherheitsinfrastruktur zum Schutz von Remote-Netzwerken. Es bietet Sicherheit, da Organisationen regionale, cloudbasierte Firewalls einrichten können, die die SD-WAN-Fabric schützen.

Mit dem Prisma Access Service für Remote-Netzwerke können Sie Remote-Netzwerkstandorte einbinden und den Benutzern Sicherheit bieten. Es beseitigt die Komplexität bei der Konfiguration und Verwaltung von Geräten an jedem Remote-Standort. Der Service bietet eine effiziente Möglichkeit, neue Remote-Netzwerkstandorte einfach hinzuzufügen und die betrieblichen Herausforderungen zu minimieren, indem sichergestellt wird, dass die Benutzer an diesen Standorten immer verbunden und sicher sind, und ermöglicht es Ihnen, Richtlinien zentral über Panorama zu verwalten, um eine konsistente und optimierte Sicherheit für Ihr Remote-Netzwerk zu gewährleisten. Netzwerkstandorte.

Um Ihre Remote-Netzwerkstandorte mit dem Prisma Access-Dienst zu verbinden, können Sie die Palo Alto Networks Firewall der nächsten Generation oder ein IPsec-kompatibles Gerät eines Drittanbieters einschließlich

SD-WAN verwenden, das einen IPsec-Tunnel für den Dienst einrichten kann.

- Planen des Prisma Access Service für Remote-Netzwerke
- Konfigurieren des Prisma Access Service für Remote-Netzwerke
- Onboard-Remote-Netzwerke mit Konfigurationsimport

Die Citrix SD-WAN Lösung bot bereits die Möglichkeit, den Internetverkehr von der Zweigstelle zu trennen. Dies ist entscheidend, um eine zuverlässigere Benutzererfahrung mit geringer Latenz zu ermöglichen und gleichzeitig die Einführung eines teuren Sicherheits-Stacks in jedem Zweig zu vermeiden. Citrix SD-WAN und Palo Alto Networks bieten nun verteilten Unternehmen eine zuverlässigere und sicherere Möglichkeit, Benutzer in Zweigstellen mit Anwendungen in der Cloud zu verbinden.

Citrix SD-WAN Appliances können über IPsec-Tunnel von SD-WAN-Appliances Standorten mit minimaler Konfiguration mit dem Palo Alto Cloud-Dienst-Netzwerk (Prisma Access Service) verbunden werden. Sie können das Palo Alto Netzwerk in Citrix SD-WAN Center konfigurieren.

Bevor Sie mit der Konfiguration des Prisma Access Service für Remote Networks beginnen, stellen Sie sicher, dass Sie die folgende Konfiguration bereit haben, um sicherzustellen, dass Sie den Dienst erfolgreich aktivieren und Richtlinien für Benutzer in Ihren Remote-Netzwerkstandorten erzwingen können:

1. **Dienstverbindung**—Wenn Ihre Remote-Netzwerkstandorte Zugriff auf die Infrastruktur in Ihrer Unternehmenszentrale benötigen, um Benutzer zu authentifizieren oder den Zugriff auf wichtige Netzwerkressourcen zu ermöglichen, müssen Sie den Zugriff auf Ihr Unternehmensnetzwerk so einrichten, dass die Zentrale und die Remote-Netzwerkstandorte verbunden.

Wenn der Remote-Netzwerkstandort autonom ist und an anderen Standorten nicht auf die Infrastruktur zugreifen muss, müssen Sie die Dienstverbindung nicht einrichten (es sei denn, Ihre mobilen Benutzer benötigen Zugriff).

1. **Vorlage**—Der Prisma Access-Dienst erstellt automatisch einen Vorlagenstapel (Remote_Network_Template) und eine oberste Vorlage (Remote_Network_Template) für den Prisma Access-Dienst für Remote-Netzwerke. Um den Prisma Access Service für Remote Networks zu konfigurieren, konfigurieren Sie die oberste Vorlage von Grund auf neu oder nutzen Ihre vorhandene Konfiguration, wenn Sie bereits eine Palo Alto Networks Firewall vor Ort ausführen.

Die Vorlage erfordert die Einstellungen zum Einrichten der IPsec-Tunnel- und IKE-Konfiguration (Internet Key Exchange) für die Protokollaushandlung zwischen Ihrem Remote-Netzwerkstandort und dem Prisma Access-Dienst für Remote-Netzwerke, Zonen, die Sie in der Sicherheitsrichtlinie referenzieren können, und ein Protokollweiterleitungsprofil, damit Sie kann

Protokolle vom Prisma Access-Dienst für Remote-Netzwerke an den Protokollierungsdienst weiterleiten.

2. **Übergeordnete Gerätegruppe**—Der Prisma Access-Dienst für Remote-Netzwerke erfordert, dass Sie eine übergeordnete Gerätegruppe angeben, die Ihre Sicherheitsrichtlinie, Sicherheitsprofile und andere Richtlinienobjekte (wie Anwendungsgruppen und Objekte und Adressgruppen) sowie Authentifizierungsrichtlinie enthält, damit Der Prisma Access-Dienst für Remote-Netzwerke kann Richtlinien für Datenverkehr durchsetzen, der durch den IPsec-Tunnel an den Prisma Access-Dienst für Remote-Netzwerke weitergeleitet wird. Sie müssen entweder Richtlinienregeln und -objekte in Panorama definieren oder eine vorhandene Gerätegruppe verwenden, um Benutzer am Remote-Netzwerkstandort zu schützen.

Hinweis:

Wenn Sie eine vorhandene Gerätegruppe verwenden, die auf Zonen verweist, müssen Sie die entsprechende Vorlage, die die Zonen definiert, dem Remote_Network_Template_Stack hinzufügen.

Auf diese Weise können Sie die Zonenzuordnung abschließen, wenn Sie den Prisma Access Service für Remote Networks konfigurieren.

3. **IP-Subnetze**—Damit der Prisma Access-Dienst Datenverkehr an Ihre Remote-Netzwerke weiterleitet, müssen Sie Routinginformationen für die Teilnetze bereitstellen, die Sie mit dem Prisma Access-Dienst sichern möchten. Sie können entweder eine statische Route zu jedem Teilnetz am Remote-Netzwerkstandort definieren oder BGP zwischen den Dienstverbindungsstandorten und dem Prisma Access-Dienst konfigurieren oder eine Kombination beider Methoden verwenden.

Wenn Sie beide statischen Routen konfigurieren und BGP aktivieren, haben die statischen Routen Vorrang. Zwar ist es praktisch, statische Routen zu verwenden, wenn Sie nur wenige Teilnetze an Ihren Remote-Netzwerkstandorten haben, in einer großen Bereitstellung mit vielen Remote-Netzwerken mit überlappenden Subnetzen, ermöglicht BGP Ihnen eine einfachere Skalierung.

Netzwerk Palo Alto in SD-WAN Center

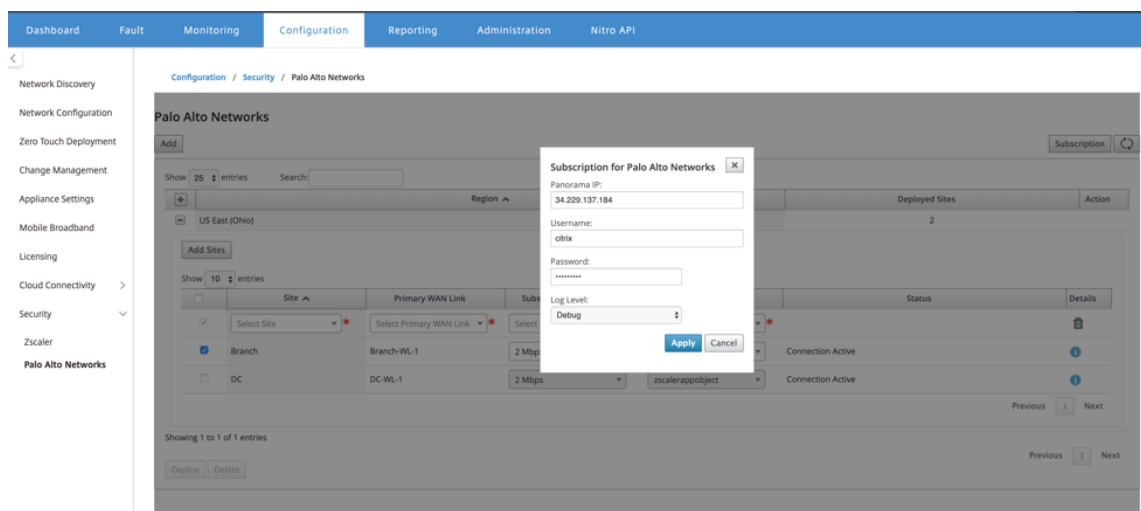
Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Rufen Sie die Panorama-IP-Adresse vom PRISMA ACCESS-Service ab.
- Rufen Sie Benutzernamen und Kennwortbenutzer im PRISMA ACCESS-Service ab.
- Konfigurieren Sie IPsec-Tunnel in der Benutzeroberfläche der SD-WAN-Appliance.

- Stellen Sie sicher, dass die Site nicht in eine Region integriert ist, in der bereits eine andere Site mit anderen ike/ipsec-Profilen als Citrix-ike-crypto-default/Citrix-IPsec-crypto-default konfiguriert ist.
- Stellen Sie sicher, dass die Prisma Access-Konfiguration nicht manuell geändert wird, wenn die Konfiguration vom SD-WAN Center aktualisiert wird.

Geben Sie in der Benutzeroberfläche des Citrix SD-WAN Centers Palo Alto Abonnementinformationen an.

- Konfigurieren Sie die Panorama-IP-Adresse. Diese IP-Adresse erhalten Sie von Palo Alto (PRISMA ACCESS Dienst).
- Konfigurieren Sie den Benutzernamen und das Kennwort, die im PRISMA ACCESS-Dienst verwendet werden.



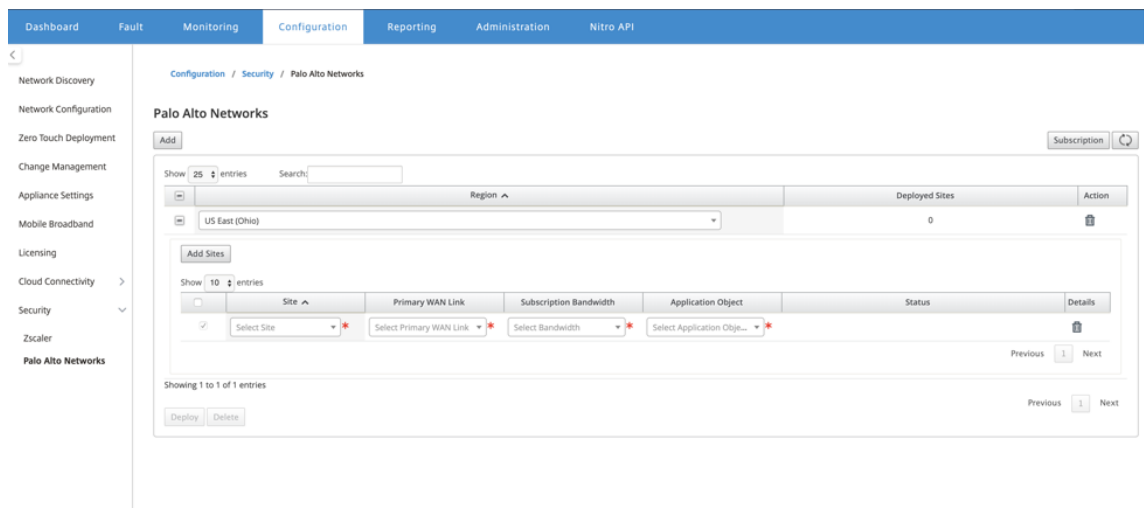
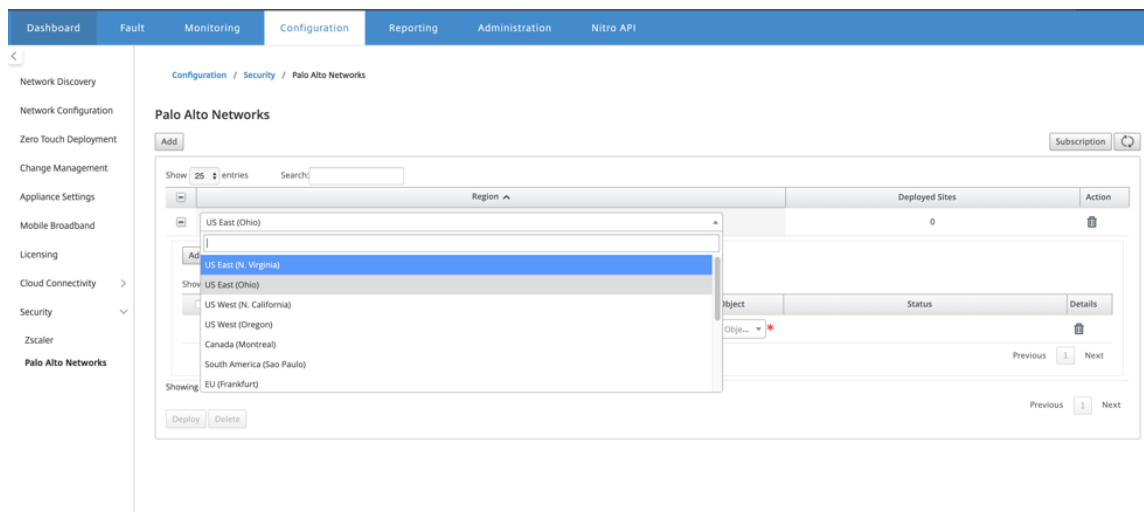
Hinzufügen und Bereitstellen von Websites

1. Um die Sites bereitzustellen, wählen Sie die PRISMA ACCESS-Netzwerkregion und die SD-WAN-Site aus, die für die Prisma Access-Region konfiguriert werden soll, und wählen Sie dann die Standort-WAN-Link, die Bandbreite und das Anwendungsobjekt für die Datenverkehrsauswahl aus.

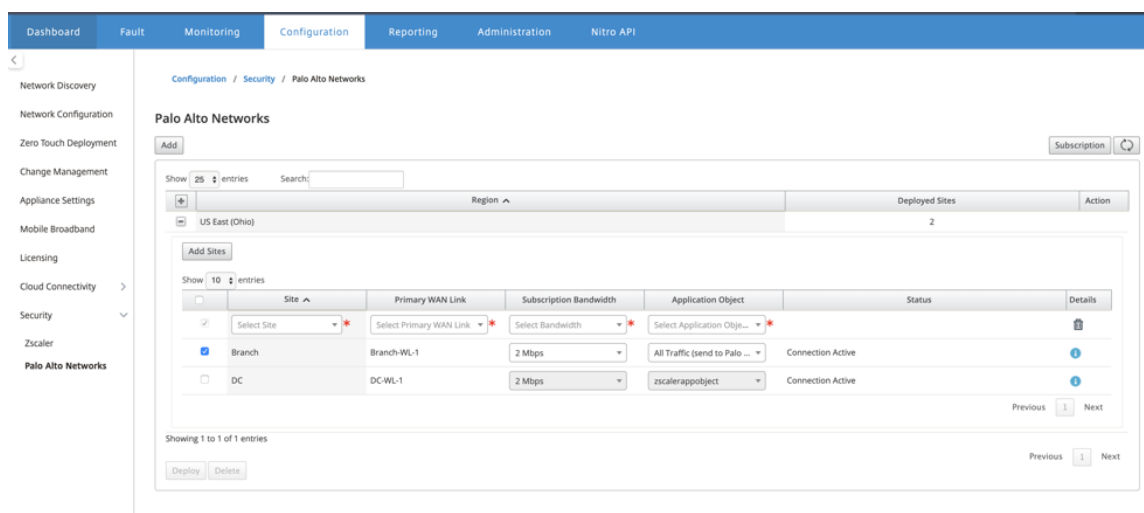
Hinweis:

Der Datenfluss wird beeinträchtigt, wenn die ausgewählte Bandbreite den verfügbaren Bandbreitenbereich überschreitet.

Sie können den gesamten internetgebundenen Datenverkehr an den PRISMA ACCESS-Service umleiten, indem Sie unter der Objektauswahl Anwendung die Option **Alle Datenverkehr** auswählen.

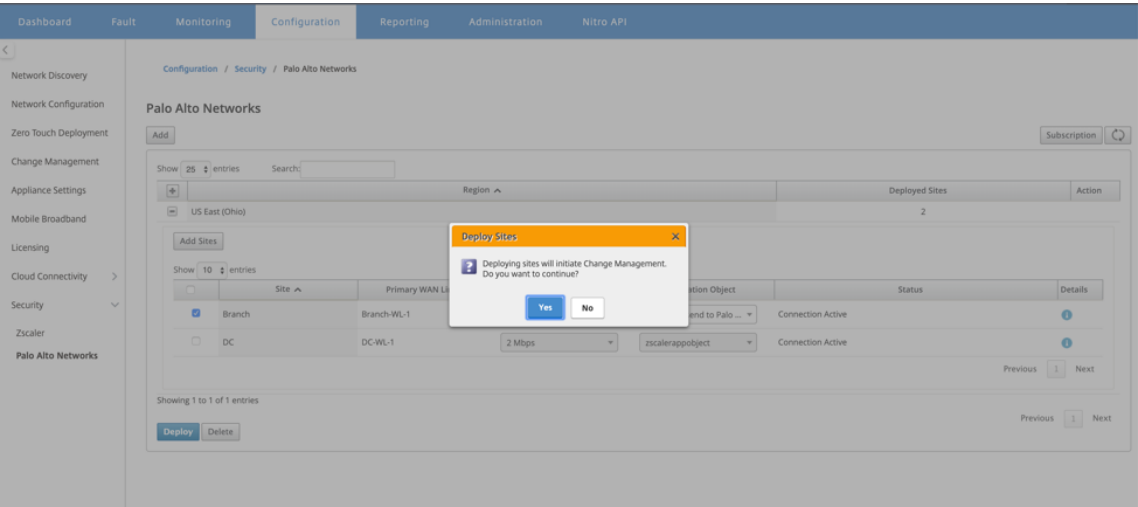


2. Sie können nach Bedarf weitere SD-WAN-Zweigstellen hinzufügen.

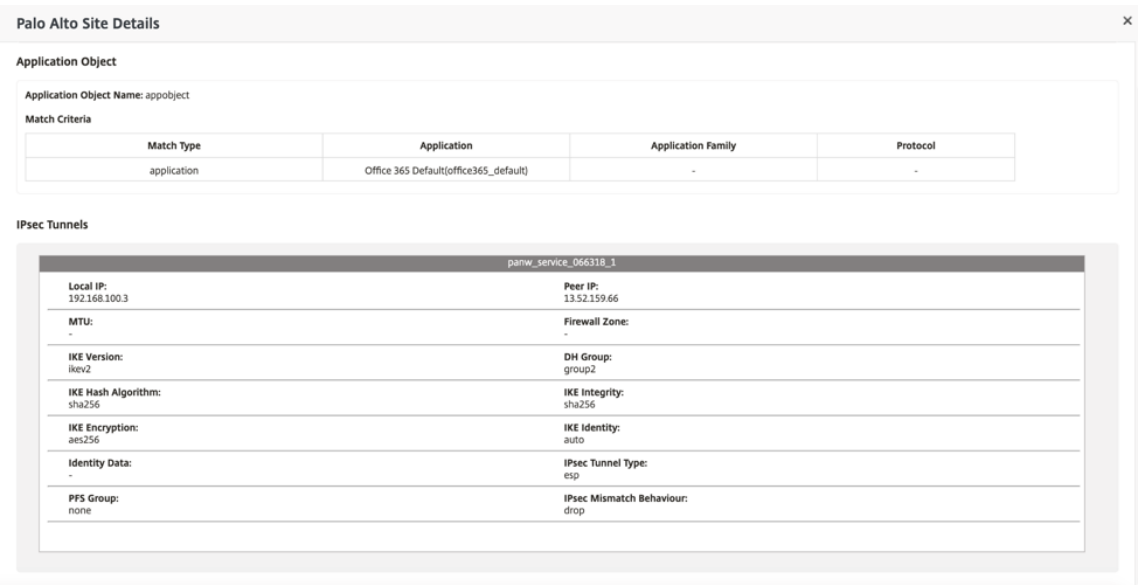


3. Klicken Sie auf **Bereitstellen**. Der Änderungsmanagement-Prozess wird initiiert. Klicken Sie

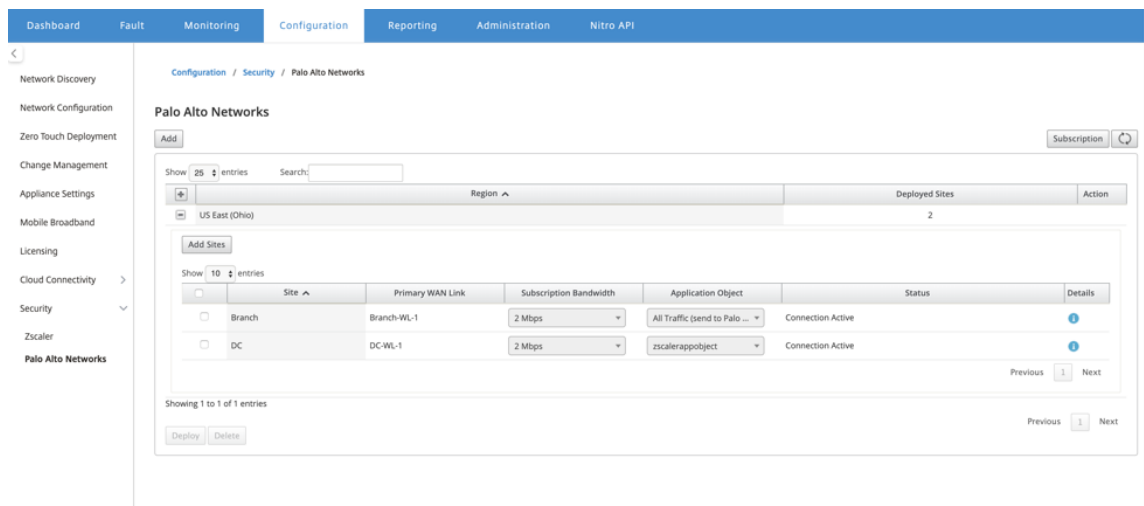
auf **Ja**, um fortzufahren.



Nach der Bereitstellung ist die IPsec-Tunnelkonfiguration, die zum Einrichten der Tunnel verwendet wird, wie folgt.



Die Zielseite zeigt die Liste aller Sites an, die unter verschiedenen SD-WAN-Regionen konfiguriert und gruppiert sind.



Überprüfen Sie die End-to-End-Datenverkehrsverbindung:

- Aus dem LAN-Subnetz der Zweigstelle, greifen Sie auf Internetressourcen zu.
- Stellen Sie sicher, dass der Datenverkehr über den Citrix SD-WAN IPsec-Tunnel zum Palo Alto Prisma Access geht.
- Überprüfen Sie, ob die Sicherheitsrichtlinie von Palo Alto auf den Datenverkehr auf der Registerkarte Überwachung angewendet wird.
- Überprüfen Sie, ob die Antwort von Internet zu Host in einem Zweig durchläuft.

Stateful Firewall und NAT-Unterstützung

May 10, 2021

Diese Funktion stellt eine Firewall bereit, die in die SD-WAN-Anwendung integriert ist. Die Firewall ermöglicht Richtlinien zwischen Diensten und Zonen und unterstützt Static NAT, Dynamic NAT (PAT) und Dynamic NAT mit Port-Forwarding. Weitere Firewall-Funktionen umfassen:

- Sicherheit für den Benutzerverkehr innerhalb des SD-WAN-Netzwerks (Unternehmen und Dienstleister)
- (Potential) Reduzierung externer Geräte (Unternehmen und Dienstleister)
- Verwenden des gleichen IP-Adressraums für mehrere Kunden: NAT-Fähigkeit (Service Provider)
- Anwenden mehrerer Firewalls aus globaler Sicht (Service Provider)
- Filtern von Verkehrsflüssen zwischen Zonen
- Filtern des Datenverkehrs zwischen Diensten innerhalb einer Zone
- Filtern des Datenverkehrs zwischen Diensten, die sich in verschiedenen Zonen befinden
- Filtern des Datenverkehrs zwischen Diensten an einem Standort

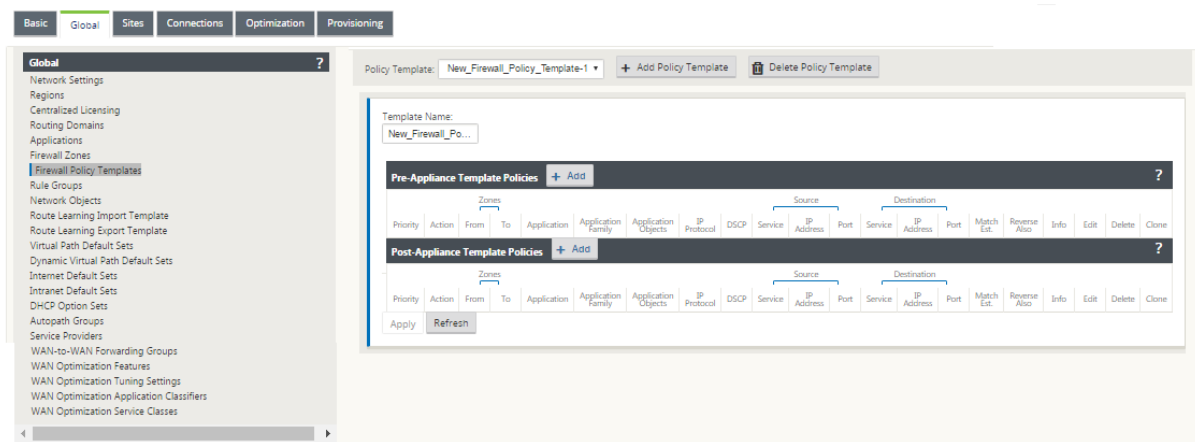
- Definieren von Filterrichtlinien zum Zulassen, Verweigern oder Zurückweisen von Flows
- Ablaufstatus für ausgewählte Flows verfolgen
- Globale Richtlinienvorlagen anwenden
- Unterstützung für Portadressübersetzung für Datenverkehr in das Internet an einem nicht vertrauenswürdigen Port sowie Portweiterleitung ein- und ausgehender
- Bereitstellen einer statischen Netzwerkadressübersetzung (statische NAT)
- Dynamische Netzwerkadressübersetzung (Dynamic NAT) bereitstellen
- Port-Adress-Übersetzung (PAT)
- Port-Weiterleitung

Um den Konfigurationsprozess zu vereinfachen, werden Firewall-Richtlinien auf globaler Konfigurationsebene erstellt. Diese globale Konfiguration besteht aus Richtlinienvorlagen für die Standortvorbereitung und nach der Appliance, die auf alle Standorte im SD-WAN-Netzwerk angewendet werden können.

Hinweis

Es wird aus Sicherheitsgründen nicht empfohlen, die Firewall im Fail-to-Wire-Inline-Modus zu verwenden.

Globale Richtlinienvorlagen



Vorrichtlinienvorlage

Priority:

100

From Zones

| Zone | Enable |
|-------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |
| Untrusted_Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|-------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |
| Untrusted_Internet_Zone | <input type="checkbox"/> |

Action:

Allow

Log Interval (s):

0

☐ Log Start

☐ Log End

Connection State Tracking:

Use Site Setting

Match Type:

IP Protocol

Application Objects:

Any

Application:

Application Family:

IP Protocol:

Any

DSCP:

Any

☒ Allow Fragments

☐ Reverse Also

☐ Match Established

Source Service Type:

Any

Source Service Name:

Any

Source IP:

*

Source Port:

*

Dest Service Type:

Any

Dest Service Name:

Any

Dest IP:

*

Dest Port:

*

Add

Cancel

Vorlage nach Policy-Richtlinien

Add

?

x

Priority:

100

From Zones

| Zone | Enable |
|-------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |
| Untrusted_Internet_Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|-------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| Internet_Zone | <input type="checkbox"/> |
| Untrusted_Internet_Zone | <input type="checkbox"/> |

Action:

Allow

Log Interval (s):

0

☐ Log Start

☐ Log End

Connection State Tracking:

Use Site Setting

Match Type:

IP Protocol

Application Objects:

Any

Application:

Application Family:

IP Protocol:

Any

DSCP:

Any

☒ Allow Fragments

☐ Reverse Also

☐ Match Established

Source Service Type:

Any

Source Service Name:

Any

Source IP:

*

Source Port:

*

Dest Service Type:

Any

Dest Service Name:

Any

Dest IP:

*

Dest Port:

*

Add

Cancel

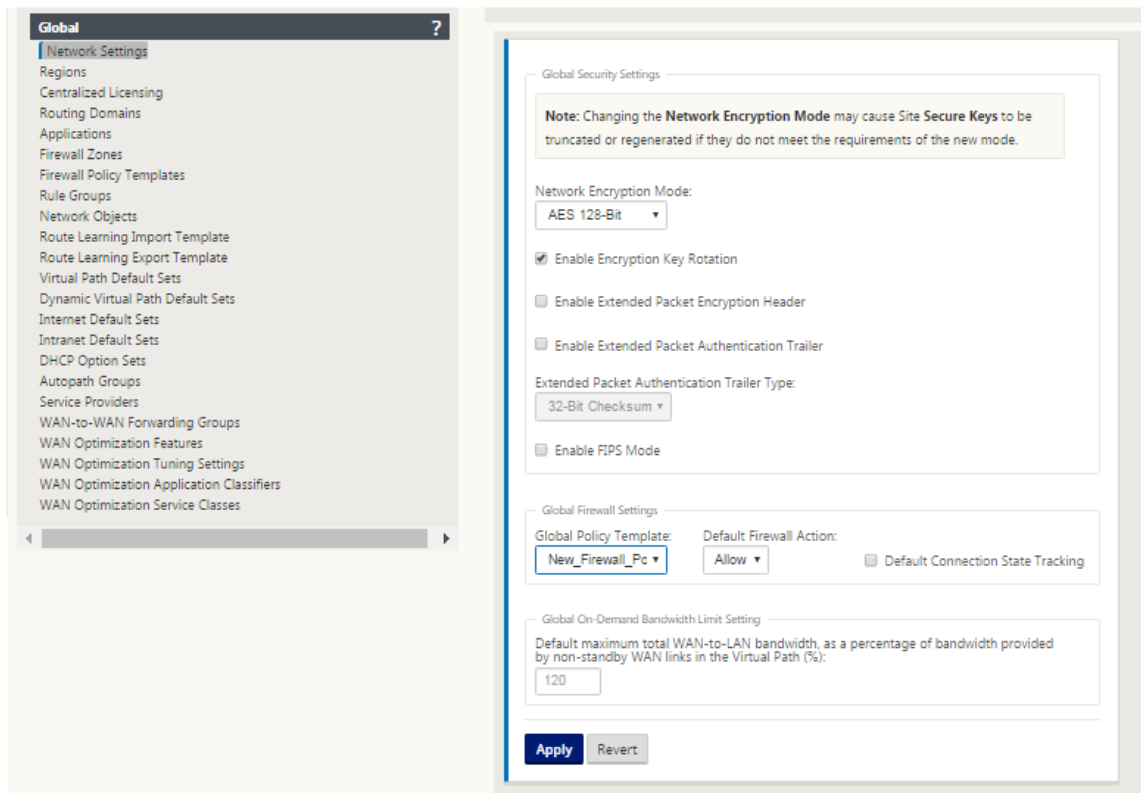
Globale Firewallinstellungen

May 10, 2021

Nachdem Sie die Firewallrichtlinienvorlagen erstellt haben, können Sie diese Richtlinie verwenden, um Firewallinstellungen für NetScaler SD-WAN-Netzwerk zu konfigurieren. Mit den globalen Firewallinstellungen können Sie die globalen Firewallparameter konfigurieren. Diese Einstellungen werden auf alle Websites im virtuellen WAN-Netzwerk angewendet.

So konfigurieren Sie globale Firewallinstellungen:

1. Navigieren Sie im **Konfigurations-Editor** zu **Global > Netzwerkeinstellungen** und klicken Sie auf das Symbol "Bearbeiten".



2. Wählen Sie im Abschnitt **Globale Firewallereinstellungen** Werte für die folgenden Optionen aus:
 - **Globale Richtlinienvorlage** - Wählen Sie eine Firewallrichtlinienvorlage aus, die auf alle Appliances im SD-WAN-Netzwerk angewendet werden soll, **Standardfirewall Aktionen** - Wählen Sie Zulassen aus, um Pakete zuzulassen, die nicht mit der Filterrichtlinie übereinstimmen. Wählen Sie Löschen aus, um die Pakete zu löschen, die nicht mit der Filterrichtlinie übereinstimmen, **Standardverbindungsstatusverfolgung** - Dies ermöglicht die Richtungszustandsverfolgung für TCP-, UDP- und ICMP-Flows, die nicht mit einer Filterrichtlinie oder NAT-Regel übereinstimmen. Dadurch wird der asymmetrische Fluss blockiert, selbst wenn keine Firewall-Richtlinien definiert sind.
3. Klicken Sie auf **Übernehmen**.

Hinweis

Sie können diese Einstellungen auch auf Standortebene konfigurieren. Dadurch wird die globale Einstellung außer Kraft gesetzt.

Erweiterte Firewallereinstellungen

May 10, 2021

Sie können die erweiterten Firewall Einstellungen für jeden Standort individuell konfigurieren. Dadurch werden die globalen Einstellungen außer Kraft gesetzt.

So konfigurieren Sie erweiterte Firewall Einstellungen:

1. Navigieren Sie im **Konfigurations-Editor** zu **Verbindungen > Site anzeigen > Firewall > Einstellungen**.

Section: Settings

| Priority | Name | Delete |
|----------|------------|--------|
| 100 | Policy_New | |

Advanced

Default Firewall Action: Allow | Default Connection State Tracking: Use Global Settings | ☒ Source Route Validation

Max New Connections per Source: 100 | Max Connections per Source: 0

Untracked and Denied Timeout (s): 30

TCP Initial Timeout (s): 120 | TCP Idle Timeout (s): 7440

TCP Closing Timeout (s): 60 | TCP Time Wait Timeout (s): 120 | TCP Closed Timeout (s): 10

UDP Initial Timeout (s): 30 | UDP Idle Timeout (s): 300

ICMP Initial Timeout (s): 30 | ICMP Idle Timeout (s): 60

Generic Initial Timeout (s): 30 | Generic Idle Timeout (s): 300

Apply Revert

2. Klicken Sie im Abschnitt **Richtlinienvorlage** auf **Hinzufügen**. Geben Sie Werte für die folgenden Parameter ein.

- **Priorität** - Die Reihenfolge, in der die Richtlinie auf dem Standort angewendet wird.
- **Name** - Der Name der Richtlinienvorlage, die auf der Site verwendet werden soll.

3. Klicken Sie auf **Erweitert**. Geben Sie Werte für die folgenden Parameter ein:

- **Standard-Firewall-Aktion** - Wählen Sie eine der folgenden Optionen aus.
 - **Globale Einstellung verwenden**- Verwenden der in den NetScaler SD-WAN-Einstellungen konfigurierten globalen Einstellung
 - **Zulassen**- Pakete, die keiner Filterrichtlinie entsprechen, sind zulässig.

- **Drop**- Pakete, die keiner Filterrichtlinie entsprechen, werden gelöscht.
 - **Standardverfolgung des Verbindungszustands** —Wählen Sie eine der folgenden Optionen aus.
 - **Globale Einstellung verwenden** - Verwenden der in den NetScaler SD-WAN-Einstellungen konfigurierten globalen Einstellung
 - **Keine Verfolgung** - Bidirektionale Verbindungszustandsverfolgung wird nicht für Pakete durchgeführt, die keiner Filterrichtlinie entsprechen.
 - **Spur** - Die bidirektionale Verbindungsstatusverfolgung wird auf TCP-, UDP- und ICMP-Paketen durchgeführt, die keiner Filterrichtlinie oder NAT-Regel entsprechen. Dadurch wird der asymmetrische Fluss blockiert, selbst wenn keine Firewall-Richtlinien definiert sind.
 - **Validierung der Quellroute:** Wenn diese Option aktiviert ist, werden Pakete gelöscht, wenn sie auf einer Schnittstelle empfangen werden, die sich von der Route des Pakets unterscheidet, wie durch die Quell-IP-Adresse bestimmt. Es wird nur die Route berücksichtigt, mit der das Paket derzeit übereinstimmen würde.
 - **Max. Neue Verbindungen pro Quelle:** Die maximale Anzahl nicht etablierter Verbindungen, die pro Quell-IP-Adresse zulässig sind. 0 bedeutet unbegrenzt. Verwenden Sie diese Einstellung, um Denial-of-Service-Angriffe auf die Firewall zu verhindern.
 - **Max. Verbindungen pro Quelle:** Die maximale Anzahl von Verbindungen, die pro Quell-IP-Adresse zulässig sind. 0 bedeutet unbegrenzt. Verwenden Sie diese Einstellung, um Denial-of-Service-Angriffe auf die Firewall zu verhindern.
4. Konfigurieren Sie die verschiedenen Timeout-Einstellungen und klicken Sie auf **Übernehmen**.

Zonen

May 10, 2021

Sie können Zonen im Netzwerk konfigurieren und Richtlinien definieren, um zu steuern, wie Verkehr Zonen ein- und verlässt. Standardmäßig werden die folgenden Zonen erstellt:

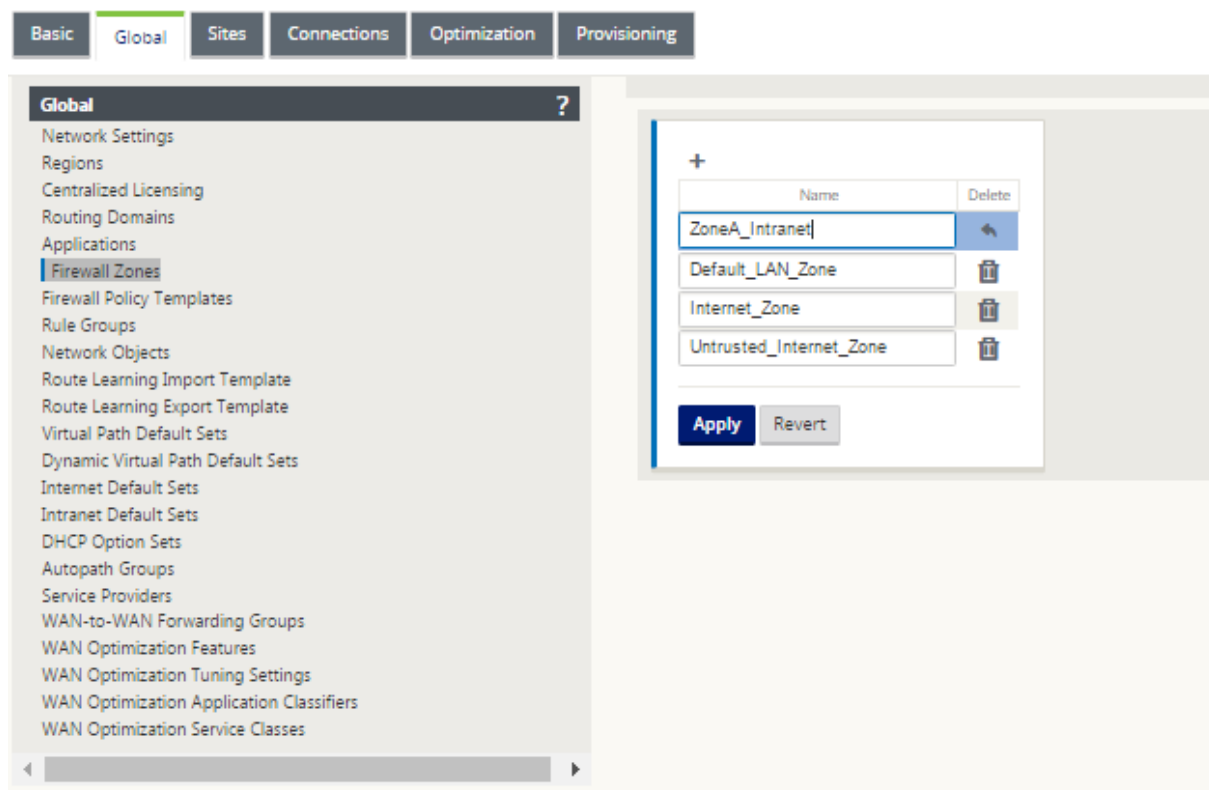
- Internet_Zone
 - Gilt für Datenverkehr zu oder von einem Internetdienst über eine vertrauenswürdige Schnittstelle.
- Untrusted_Internet_Zone

- Gilt für Datenverkehr zu oder von einem Internetdienst über eine nicht vertrauenswürdige Schnittstelle.
- Default_LAN_Zone
 - Gilt für den Datenverkehr zu oder von einem Objekt mit einer konfigurierbaren Zone, für die die Zone nicht festgelegt wurde.

Sie können eigene Zonen erstellen und den folgenden Objekttypen zuweisen:

- Virtuelle Netzwerkschnittstellen (VNI)
- Intranetdienste
- GRE Tunnel
- LAN IPsec-Tunnel

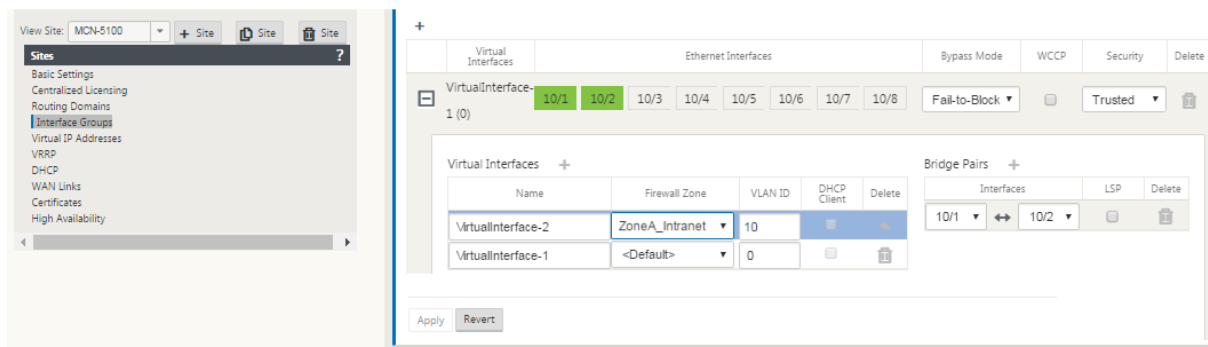
Die folgende Abbildung zeigt die drei vorkonfigurierten Zonen. Zusätzlich können Sie nach Bedarf eigene Zonen erstellen. In diesem Beispiel ist die Zone “ZoneA_Intranet” eine vom Benutzer erstellte Zone. Sie ist der virtuellen Schnittstelle des Bypass-Segments (Ports 1 und 2) der SD-WAN-Appliance zugewiesen.



Die Quellzone eines Pakets wird durch den Dienst oder die virtuelle Netzwerkschnittstelle bestimmt, auf der ein Paket empfangen wird. Die Ausnahme hiervon ist der virtuelle Pfadverkehr. Wenn der Datenverkehr in einen virtuellen Pfad eintritt, werden Pakete mit der Zone markiert, die den

Datenverkehr entspringt, und diese Quellzone wird durch den virtuellen Pfad übertragen. Dadurch kann das empfangende Ende des virtuellen Pfads eine Richtlinienentscheidung basierend auf der ursprünglichen Quellzone treffen, bevor er in den virtuellen Pfad gelangt.

Beispielsweise möchte ein Netzwerkadministrator Richtlinien definieren, damit nur der Datenverkehr von VLAN 30 am Standort A VLAN 10 am Standort B eingeben darf. Der Administrator kann jedem VLAN eine Zone zuweisen und Richtlinien erstellen, die den Datenverkehr zwischen diesen Zonen zulassen und den Datenverkehr aus anderen Zonen blockieren. Der folgende Screenshot zeigt, wie ein Benutzer VLAN 10 die Zone ZoneA_Intranet zuweisen würde. In diesem Beispiel wurde zuvor die Zone ZoneA_Intranet vom Benutzer definiert, um sie der Virtual Interface VirtualInterface-2 zuzuweisen.



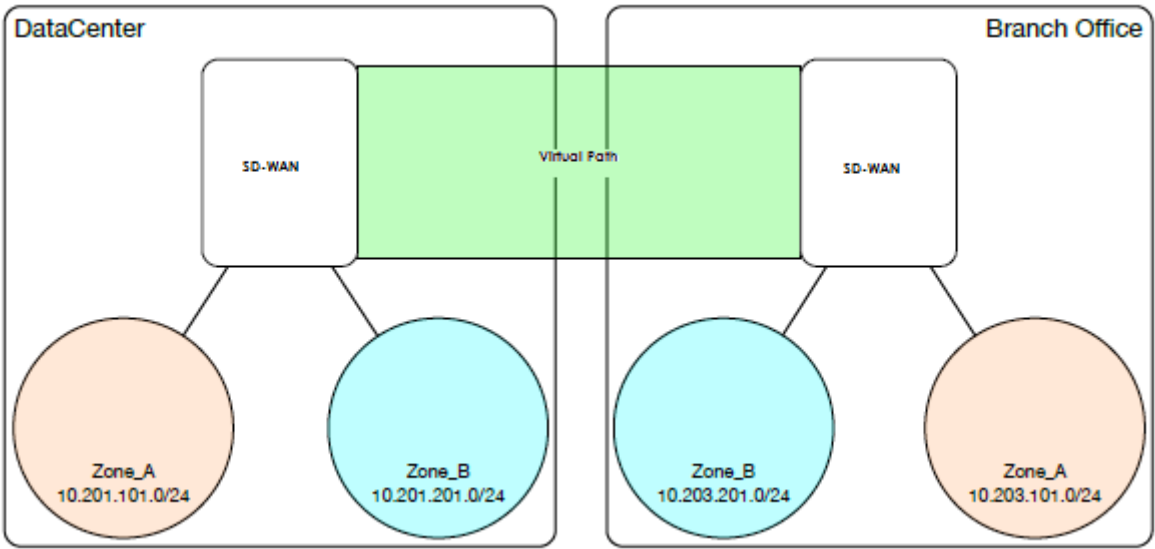
Die Zielzone eines Pakets wird basierend auf der Zielroute Übereinstimmung ermittelt. Wenn eine SD-WAN-Appliance das Zielsubnetz in der Routentabelle nachsucht, stimmt das Paket mit einer Route überein, der eine Zone zugewiesen ist.

- Quellzone
 - Nicht-virtueller Pfad: Ermittelt durch das Paket der virtuellen Netzwerkschnittstelle wurde am empfangen.
 - Virtueller Pfad: Ermittelt durch das Feld der Quellzone im Paketfluss-Header.
 - Virtuelle Netzwerkschnittstelle - das Paket wurde am Quellstandort empfangen.
- Ziellandgebiet
 - Ermittelt durch Zielroute Suche nach Paketen.

Routen, die mit Remote-Standorten im SD-WAN gemeinsam genutzt werden, verwalten Informationen über die Zielzone, einschließlich Routen, die über das dynamische Routing-Protokoll (BGP, OSPF) gelernt wurden. Mit diesem Mechanismus gewinnen Zonen globale Bedeutung im SD-WAN-Netzwerk und ermöglichen End-to-End-Filterung innerhalb des Netzwerks. Die Verwendung von Zonen bietet einem Netzwerkadministrator eine effiziente Möglichkeit, den Netzwerkverkehr basierend auf dem Kunden, der Geschäftseinheit oder der Abteilung zu segmentieren.

Die Fähigkeit der SD-WAN-Firewall ermöglicht es dem Benutzer, den Datenverkehr zwischen Diensten innerhalb einer einzigen Zone zu filtern oder Richtlinien zu erstellen, die zwischen Diensten in

verschiedenen Zonen angewendet werden können (siehe Abbildung unten). Im folgenden Beispiel haben wir Zone_A und Zone_B, von denen jeder eine virtuelle LAN Netzwerkschnittstelle hat.



Screenshot unten zeigt die Vererbung der Zone für eine virtuelle IP (VIP) von der zugewiesenen Virtual Network Interface (VNI).

| IP Address / Prefix | Virtual Interface | Firewall Zone | Identity | Private | Security | Delete |
|---------------------|--------------------|------------------|-------------------------------------|--------------------------|----------|--------|
| 172.16.187.11/24 | VirtualInterface-1 | Default_LAN_Zone | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Trusted | |
| 172.16.187.12/24 | VirtualInterface-1 | Default_LAN_Zone | <input type="checkbox"/> | <input type="checkbox"/> | Trusted | |

Richtlinien

May 10, 2021

Richtlinien bieten die Möglichkeit, bestimmte Verkehrsflüsse zu erlauben, zu verweigern, abzulehnen oder zu zählen und fortzusetzen. Die Anwendung dieser Richtlinien auf jeden Standort wäre schwierig, wenn die SD-WAN-Netzwerke wachsen. Um dieses Problem zu beheben, können Gruppen von Firewall-Filtern mit einer Firewall-Richtlinienvorlage erstellt werden. Eine Firewall-Richtlinienvorlage kann auf alle Sites im Netzwerk oder nur auf bestimmte Sites angewendet werden. Diese Richtlinien werden entweder als Vorlagen-Richtlinien für die Vorlagenvorbereitung oder nach Appliance-Vorlagen-Richtlinien sortiert. Sowohl die netzwerkweiten Richtlinien für die Vorab-Appliance als auch für die Post-Appliance-Vorlage werden auf globaler Ebene konfiguriert. Lokale Richtlinien werden auf Standortebene unter Verbindungen konfiguriert und gelten nur für diesen bestimmten Standort.

</

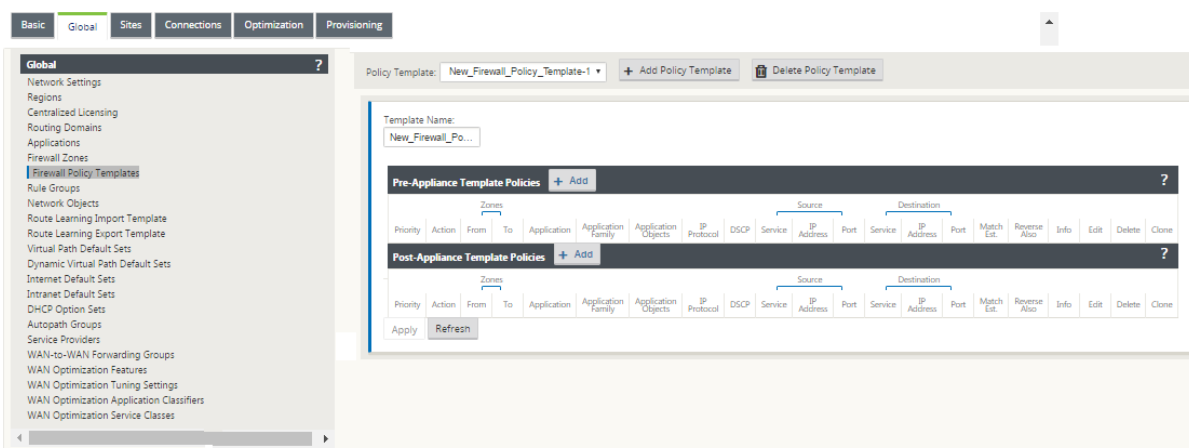
Richtlinien für Vorlagenvorlagen werden vor lokalen Standortrichtlinien angewendet. Lokale Standortrichtlinien werden als Nächstes angewendet, gefolgt von Richtlinien für die Vorlage nach der Appliance. Ziel ist es, den Konfigurationsprozess zu vereinfachen, indem Sie globale Richtlinien anwenden und gleichzeitig die Flexibilität beibehalten, standortspezifische Richtlinien anzuwenden.

Filterrichtlinienauswertungsreihenfolge

1. Vorlagenvorlagen —kompilierte Richtlinien aus allen PRE-Abschnitten.
2. Pre-Global —Aus dem Abschnitt “PRE” wurden Richtlinien zusammengestellt.
3. Lokal —Richtlinien auf Appliance-Ebene.
4. Lokal automatisch generiert —automatisch lokal generierte Richtlinien.
5. Post-Templates —kompilierte Richtlinien aus allen “POST”-Abschnitten.
6. Post-Global —Kompilierte Richtlinien aus dem Abschnitt “POST”.

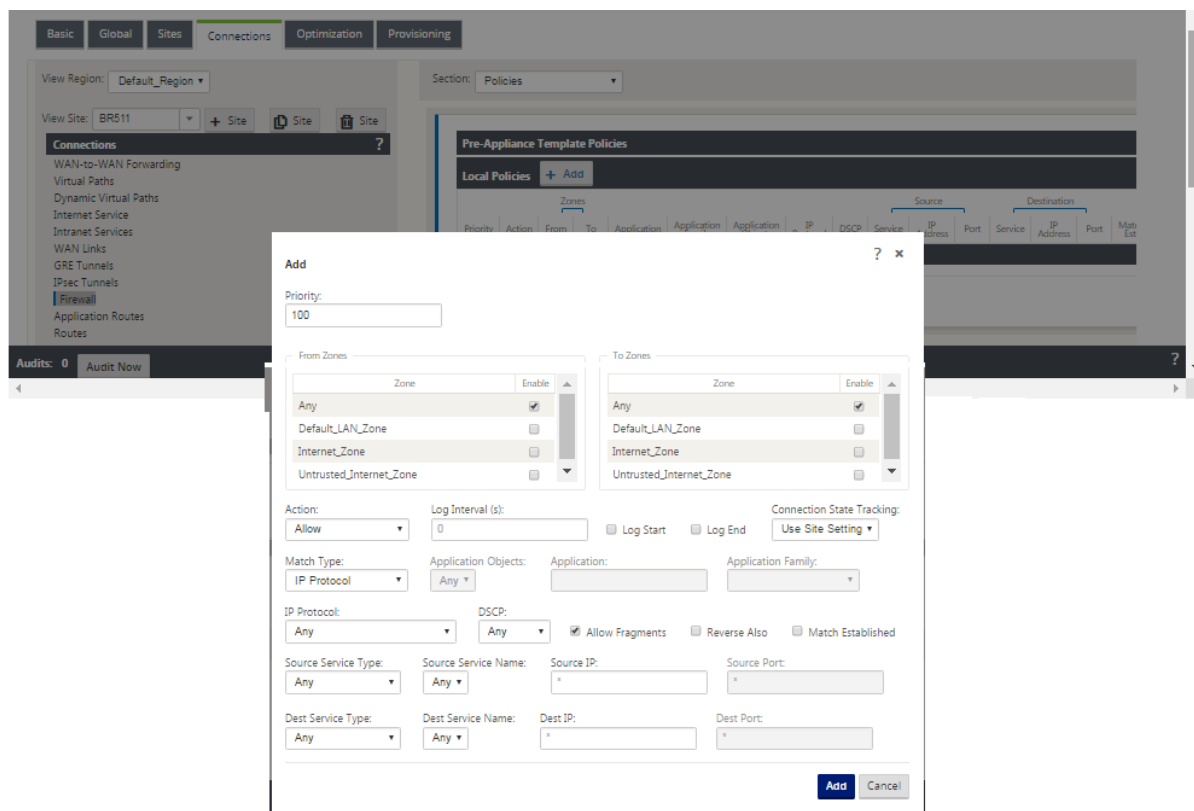
Richtliniendefinitionen - Global und Local (Site)

Sie können Richtlinien für Vorinstallierungs- und Nach-Appliance-Vorlagen auf globaler Ebene konfigurieren. Lokale Richtlinien werden auf Standortebene einer Appliance angewendet.



Der obige Screenshot zeigt die Richtlinienvorlage, die global für das SD-WAN-Netzwerk gelten würde. Um eine Vorlage auf alle Websites im Netzwerk anzuwenden, navigieren Sie zu **Global > Netzwerkeinstellungen > Globale Richtlinienvorlage**, und wählen Sie eine bestimmte Richtlinie aus. Auf Standortebene können Sie weitere Richtlinienvorlagen hinzufügen und standortspezifische Richtlinien erstellen.

Die spezifischen konfigurierbaren Attribute für eine Richtlinie werden im folgenden Screenshot angezeigt, diese sind für alle Richtlinien identisch.



Richtlinienattribute

- **Priorität** —Reihenfolge, in der die Richtlinie innerhalb aller definierten Richtlinien angewendet wird. Richtlinien mit niedrigerer Priorität werden vor Richtlinien mit höherer Priorität angewendet.
- **Zone** —Flows haben eine Quellzone und eine Zielzone.
 - **Von Zone** —Quellzone für die Richtlinie.
 - **To Zone** —Zielzone für die Richtlinie.
- **Aktion** —**Aktion**, die für einen abgestimmten Flow ausgeführt werden soll.
 - **Zulassen** —Erlauben Sie den Fluss durch die Firewall.
 - **Drop** —verweigern Sie den Fluss durch die Firewall, indem Sie die Pakete löschen.
 - **Zurückweisen** —verweigern Sie den Fluss durch die Firewall und senden Sie eine protokollspezifische Antwort. TCP sendet einen Reset, ICMP sendet eine Fehlermeldung.
 - **Count and Continue** —Zählen Sie die Anzahl der Pakete und Bytes für diesen Flow, und fahren Sie dann mit der Richtlinienliste fort.
- **Protokollintervall** —Zeit in Sekunden zwischen der Protokollierung der Anzahl der Pakete, die mit der Richtlinie übereinstimmen, mit der Firewall-Protokolldatei oder dem Syslog-Server, sofern diese konfiguriert ist.
 - **Log-Start** —Wenn diese Option aktiviert ist, wird ein Protokolleintrag für den neuen Flow erstellt.
 - **Log End** —Protokollieren Sie die Daten für einen Flow, wenn der Flow gelöscht wird.

Hinweis

Der Standardwert für Protokollintervall 0 bedeutet keine Protokollierung.

- **Track** —ermöglicht es der Firewall, den Status eines Flows zu verfolgen und diese Informationen in der Tabelle **Überwachung > Firewall > Verbindungen** anzuzeigen. Wenn der Flow nicht verfolgt wird, zeigt der Status NOT_TRACKED an. In der Tabelle finden Sie die Statusverfolgung auf Basis des Protokolls unten. Verwenden Sie die auf Standortebene unter **Firewall > Einstellungen > Erweitert > Standardverfolgung** definierte Einstellung.
 - **Keine Tracking** —Der Flusstatus ist nicht aktiviert.
 - **Track** —Zeigt den aktuellen Status des Flows an (der dieser Richtlinie entspricht).
- **Übereinstimmungstyp** —Wählen Sie einen der folgenden Übereinstimmungstypen

- **IP-Protokoll** —Wenn dieser Übereinstimmungstyp ausgewählt ist, wählen Sie ein IP-Protokoll aus, mit dem der Filter übereinstimmt. Die Optionen umfassen ANY, TCP, UDP ICMP and so
- **Anwendung** —Wenn dieser Übereinstimmungstyp ausgewählt ist, geben Sie die Anwendung an, die als Übereinstimmungskriterien für diesen Filter verwendet wird.
- **Anwendungsfamilie** —Wenn dieser Übereinstimmungstyp ausgewählt ist, wählen Sie eine Anwendungsfamilie aus, die als Übereinstimmungskriterien für diesen Filter verwendet wird.
- **Anwendungsobjekt** — Wenn dieser Übereinstimmungstyp ausgewählt ist, wählen Sie eine Anwendungsfamilie aus, die als Übereinstimmungskriterien für diesen Filter verwendet wird.

Weitere Hinweise zu Anwendung, Anwendungsfamilie und Anwendungsobjekt finden Sie unter [Anwendungsklassifizierung](#).

- **DSCP** —Ermöglicht dem Benutzer die Übereinstimmung mit einer DSCP-Tag-Einstellung.
- **Fragmente zulassen** —Zulassen von IP-Fragmenten, die mit dieser Filterrichtlinie übereinstimmen.

Hinweis

Die Firewall fügt fragmentierte Frames nicht wieder ein.

- **Auch umkehren** —Fügen Sie automatisch eine Kopie dieser Filterrichtlinie hinzu, wobei die Quell- und Zieleinstellungen umgekehrt sind.
- **Match Established** —Ordnen Sie eingehende Pakete für eine Verbindung ab, zu der ausgehende Pakete zugelassen wurden.
- **Quelldiensttyp** —in Bezug auf einen SD-WAN-Dienst —Lokal (zur Appliance), Virtueller Pfad, Intranet, IPhost oder Internet sind Beispiele für Dienstypen.
- **IPHost-Option** - Dies ist ein neuer Dienstyp für die Firewall und wird für Pakete verwendet, die von der SD-WAN-Anwendung generiert werden. Beispielsweise führt das Ausführen eines Pings über die Web-Benutzeroberfläche des SD-WAN zu einem Paket, das von einer virtuellen SD-WAN-IP-Adresse stammt. Wenn Sie eine Richtlinie für diese IP-Adresse erstellen, muss der Benutzer die Option IPhost auswählen.
- **Quelldienstname** —Name eines Dienstes, der an den Dienstyp gebunden ist. Wenn beispielsweise der virtuelle Pfad für den Quelldiensttyp ausgewählt ist, wäre dies der Name des spezifischen virtuellen Pfads. Dies ist nicht immer erforderlich und hängt vom ausgewählten Servicetyp ab.
- **Quell-IP-Adresse** —typische IP-Adresse und Subnetzmaske, mit der der Filter übereinstimmen soll.

- **Quellport** —Quellport, der von der spezifischen Anwendung verwendet wird.
- **Zieldiensttyp** —in Bezug auf einen SD-WAN-Dienst —Lokal (zur Appliance), Virtueller Pfad, Intranet, IPhost oder Internet sind Beispiele für Diensttypen.
- **Zieldienstname** - Name eines Dienstes, der an den Diensttyp gebunden ist. Dies ist nicht immer erforderlich und hängt vom ausgewählten Servicetyp ab.
- **Ziel-IP-Adresse:** Typische IP-Adresse und Subnetzmaske, mit der der Filter übereinstimmen soll.
- **Zielport** —Zielport, der von der spezifischen Anwendung verwendet wird (d. h. HTTP-Zielport 80 für das TCP-Protokoll).

Die Option Spur bietet viel mehr Details über einen Fluss. Die Statusinformationen, die in den Statustabellen nachverfolgt werden, sind unten aufgeführt.

Zustandstabelle für die Spuroption

Es gibt nur wenige Status, die konsistent sind:

- **INIT** - Verbindung erstellt, aber das anfängliche Paket war ungültig.
- **O_DENIED** - Pakete, die die Verbindung erstellt haben, werden von einer Filterrichtlinie verweigert.
- **R_DENIED** - Pakete aus dem Responder werden von einer Filterrichtlinie abgelehnt.
- **NOT_TRACKED** - Die Verbindung wird nicht stattdlich verfolgt, aber sonst erlaubt.
- **CLOSED** - Die Verbindung hat ein Zeitlimit überschritten oder wurde anderweitig durch das Protokoll geschlossen.
- **DELETED** - Die Verbindung wird gerade entfernt. Der DELETED Zustand wird fast nie gesehen.

Alle anderen Zustände sind protokollspezifisch und erfordern die Aktivierung der Stateful-Tracking.

TCP kann folgende Zustände melden:

- **SYN_SENT** - erste TCP SYN-Nachricht gesehen.
- **SYN_SENT2** - SYN-Nachricht in beide Richtungen gesehen, kein SYN+ACK (AKA simultaneous open).
- **SYN_ACK_RCVD** - SYN+ACK empfangen.
- **ESTABLISHED** - zweiter ACK empfangen, die Verbindung ist vollständig hergestellt.
- **FIN_WAIT** - erste FIN-Meldung wurde angezeigt.
- **CLOSE_WAIT** - FIN-Meldung in beide Richtungen angezeigt.

- **TIME_WAIT** - letzte ACK in beide Richtungen gesehen. Die Verbindung wird jetzt geschlossen und wartet auf erneutes Öffnen.

Alle anderen IP-Protokolle (insbesondere ICMP und UDP) haben die folgenden Zustände:

- **NEW** - Pakete in einer Richtung gesehen.
- **ESTABLISHED** - Pakete in beide Richtungen gesehen.

Netzwerkadressübersetzung (NAT)

May 10, 2021

Network Address Translation (NAT) führt die IP-Adressenerhaltung durch, um die begrenzte Anzahl registrierter IPv4-Adressen zu erhalten. Es ermöglicht privaten IP-Netzwerken, die nicht registrierte IP-Adressen verwenden, eine Verbindung zum Internet herzustellen. Die NAT-Funktion von Citrix SD-WAN verbindet Ihr privates SD-WAN-Netzwerk mit dem öffentlichen Internet. Sie übersetzt die privaten Adressen im internen Netzwerk in eine gesetzliche öffentliche Adresse. NAT sorgt auch für zusätzliche Sicherheit, indem nur eine Adresse für das gesamte Netzwerk im Internet Werbung gemacht wird und das gesamte interne Netzwerk versteckt. Citrix SD-WAN unterstützt die folgenden NAT-Typen:

- Statische 1:1 NAT
- Dynamische NAT (PAT- Port-Address-Übersetzung)
- Dynamische NAT mit Portweiterleitungsregeln

Hinweis

Die NAT-Funktion kann nur auf Standortebene konfiguriert werden. Es gibt keine globale Konfiguration (Vorlagen) für NAT. Alle NAT-Richtlinien werden aus einer Quell-NAT (SNAT)-Übersetzung definiert. Entsprechende Destination-NAT (DNAT) -Regeln werden automatisch für den Benutzer erstellt.

Statische NAT

May 10, 2021

Statische NAT ist eine 1:1 -Zuordnung einer privaten IP-Adresse oder eines Subnetzes innerhalb des SD-WAN-Netzwerks zu einer öffentlichen IP-Adresse oder Subnetz außerhalb des SD-WAN-Netzwerks.

Konfigurieren Sie Static NAT, indem Sie manuell die innere IP-Adresse und die externe IP-Adresse eingeben, in die sie übersetzt werden muss. Sie können statische NAT für die lokalen, virtuellen Pfade, Internet, Intranet und Inter-Routing-Domänendienste konfigurieren.

Eingehende und ausgehende NAT

Die Richtung für eine Verbindung kann entweder von innen nach außen oder von außen nach innen sein. Wenn eine NAT-Regel erstellt wird, wird sie je nach Richtungsübereinstimmungstyp auf beide Richtungen angewendet.

- **Eingehend:** Die Quelladresse wird für Pakete übersetzt, die im Dienst empfangen werden. Die Zieladresse wird für Pakete übersetzt, die über den Dienst übertragen werden. Beispiel: Internetdienst-zu-LAN-Dienst —Für empfangene Pakete (Internet zu LAN) wird die Quell-IP-Adresse übersetzt. Bei übertragenen Paketen (LAN to Internet) wird die Ziel-IP-Adresse übersetzt.
- **Ausgehend:** Die Zieladresse wird für Pakete übersetzt, die im Dienst empfangen wurden. Die Quelladresse wird für Pakete übersetzt, die über den Dienst übertragen werden. Beispielsweise LAN-Dienst zum Internetdienst —für übertragene Pakete (LAN zu Internet) wird die Quell-IP-Adresse übersetzt. Bei empfangenen Paketen (Internet to LAN) wird die Ziel-IP-Adresse übersetzt.

Zonenableitung

Die Quell- und Ziel-Firewallzonen für den eingehenden oder ausgehenden Datenverkehr sollten nicht identisch sein. Wenn sowohl die Quell- als auch die Ziel-Firewallzonen identisch sind, wird NAT nicht für den Datenverkehr ausgeführt.

Für ausgehende NAT wird die externe Zone automatisch vom Dienst abgeleitet. Jeder Dienst auf SD-WAN ist standardmäßig einer Zone zugeordnet. Beispielsweise ist der Internetdienst auf einer vertrauenswürdigen Internetverbindung mit der vertrauenswürdigen Internetzone verknüpft. Ebenso wird für einen eingehenden NAT die innere Zone vom Dienst abgeleitet.

Für einen Virtual Path Service NAT Zonenableitung nicht automatisch erfolgt, müssen Sie manuell die innere und äußere Zone eingeben. NAT wird nur für den Verkehr durchgeführt, der zu diesen Zonen gehört. Zonen können nicht für virtuelle Pfade abgeleitet werden, da sich innerhalb der virtuellen Pfadsubnetze möglicherweise mehrere Zonen befinden.

Konfigurieren statischer NAT-Richtlinien

Um statische NAT-Richtlinien zu konfigurieren, navigieren Sie im Konfigurations-Editor zu **Verbindungen > Firewall > Static NAT Policies**.

Edit ? x

Priority: 100

Direction: Outbound Service Type: Internet Service Name: Internet

Inside Zone: Default_LAN_Zo Inside IP Address: 172.57.79.179/32 Outside IP Address: 172.57.52.174/32

☐ Bind Responder Route ☐ Proxy ARP

Apply Cancel

- **Priorität:** Die Reihenfolge, in der die Richtlinie innerhalb aller definierten Richtlinien angewendet wird. Richtlinien mit niedrigerer Priorität werden vor Richtlinien mit höherer Priorität angewendet.
- **Richtung:** Die Richtung, in die der Verkehr fließt, aus der Perspektive der virtuellen Schnittstelle oder des Dienstes. Es kann sich entweder um eingehender oder ausgehender Datenverkehr handeln.
- **Diensttyp:** Die SD-WAN-Diensttypen, auf die die NAT-Richtlinie angewendet wird. Für statische NAT werden lokale, virtuelle Pfade, Internet-, Intranet- und Routingdomänendienste unterstützt.
- **Dienstname:** Wählen Sie einen konfigurierten Dienstnamen aus, der dem Diensttyp entspricht.
- **Inside Zone:** Der Match-Typ der Inside Firewall Zone, aus dem das Paket stammen muss, um die Übersetzung zu ermöglichen.
- **Outside Zone:** Der Match-Typ der externen Firewall-Zone, aus dem das Paket stammen muss, um die Übersetzung zu ermöglichen.
- **Inside IP Adresse:** Die innere IP-Adresse und das Präfix, auf die übersetzt werden muss, wenn die Übereinstimmungskriterien erfüllt sind.
- **Externe IP-Adresse:** Die äußere IP-Adresse und das Präfix, auf die die innere IP-Adresse übersetzt wird, wenn die Übereinstimmungskriterien erfüllt sind.
- **Bind-Responder-Route:** Stellt sicher, dass der Antwortdatenverkehr über denselben Dienst gesendet wird, an dem er empfangen wird, um ein asymmetrisches Routing zu vermeiden.
- **Proxy-ARP:** Stellt sicher, dass die Appliance auf lokale ARP-Anfragen nach der externen IP-Adresse reagiert.

Überwachen

Um NAT zu überwachen, navigieren Sie zu **Monitoring > Firewall-Statistiken > Verbindungen**. Für eine Verbindung können Sie sehen, ob NAT fertig ist oder nicht.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics:

Connections

Maximum entries to display: 50

Filtering: Application: Any Family: Any IP Protocol: Any Source Zone: Any Destination Zone: Any Source Service Type: Any Source Service Instance: Any Source IP: Source Port: Destination Service Type: Any Destination Service Instance: Any Destination IP: Destination Port:

Refresh

Clear Connections

Help

Show latest data

Show Additional Stats

Connections

| Application | Family | IP Protocol | Source | | | | Destination | | | | State | Is NAT | Sent | | | | Received | | | | Age (s) | | |
|---|-----------------|-------------|---------------|------|--------------|--------------|------------------|---------------|--------------|--------------|-----------------|---------------|-------------|-------|-----|------|----------|-------|-----|------|---------|-------|---|
| | | | IP Address | Port | Service Type | Service Name | IP Address | Port | Service Type | Service Name | | | Packets | Bytes | PPS | kbps | Packets | Bytes | PPS | kbps | | | |
| Internet Control Message Protocol(ICMP) | Network Service | ICMP | 172.57.79.179 | 3261 | Local | Guest_Ita_id | Default_LAN_Zone | 172.57.70.176 | 3261 | Internet | MCN-PA-Internet | Internet_Zone | ESTABLISHED | Yes | 6 | 504 | 1,004 | 0.675 | 6 | 504 | 1,004 | 0.675 | 6 |

Connections Displayed: 1

Connections In Use: 1/128000

Um die innere IP-Adresse zur externen IP-Adresszuordnung zu sehen, klicken Sie unter **Zugehörige Objekte** auf **NAT nach dem Routing** oder navigieren Sie zu **Monitoring > Firewall-Statistiken > NAT-Richtlinien**.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics:

NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any Service Type: Any Service Name: Any Inside IP: Inside Port: Outside IP: Outside Port:

Refresh

Show latest data.

Help

NAT Policies

| ID | Rule Type | Rule Parent | Direction | IP Protocol | Service Type | Service Name | Inside | | Outside | | Allow Related | Allow IPsec Passthrough | Allow GRE Passthrough | Packets Sent | Bytes Sent | Packets Received | Bytes Received | Connections | Related Objects |
|----|-----------|-------------|-----------|-------------|--------------|--------------|------------------|------|------------------|------|---------------|-------------------------|-----------------------|--------------|------------|------------------|----------------|-------------|-----------------|
| | | | | | | | IP Address | Port | IP Address | Port | | | | | | | | | |
| 1 | Static | - | Outbound | * | Internet | - | 172.57.79.179/32 | * | 172.57.52.174/32 | * | No | No | No | 1971 | 165564 | 1635 | 137340 | 1 | [Connections] |

NAT Policies Displayed: 1

NAT Policies In Use: 1/1000

Port Restricted Dynamic NAT Policies In Use: 0/100

Destination NAT Policies In Use: 0/100

Protokolle

Sie können Protokolle im Zusammenhang mit NAT in Firewall-Protokollen anzeigen. Um Protokolle für NAT anzuzeigen, erstellen Sie eine Firewallrichtlinie, die Ihrer NAT-Richtlinie entspricht, und stellen Sie sicher, dass die Protokollierung auf dem Firewallfilter aktiviert ist.

Edit ? x

Priority: Policy Type: **Built-in Firewall** ▼

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| gre_zone | <input type="checkbox"/> |
| Inter Routing Domain Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| gre_zone | <input type="checkbox"/> |
| Inter Routing Domain Zone | <input type="checkbox"/> |

Routing Domain: **Any** ▼

Traffic Match Type: **IP Protocol** ▼ IP Protocol: **Any** ▼ DSCP: **Any** ▼ ☐ Match Established

Application: Application Family: Application Objects: **Any** ▼

Source Service Type: **Any** ▼ Source Service Name: **Any** ▼ Source IP: Source Port:

Dest Service Type: **Any** ▼ Dest Service Name: **Any** ▼ Dest IP: Dest Port:

Actions

Action: **Allow** ▼ ☒ Allow Fragments Connection State Tracking: **Use Site Setting** ▼

Logging & Other Options

Log Interval (s): ☒ Log Start ☒ Log End ☐ Add Reverse Policy

Apply Cancel

Navigieren Sie zu **Logging/Monitoring > Log-Optionen**, wählen Sie **SDWAN_firewal.log** und klicken Sie auf **Protokoll anzeigen**.

Dashboard Monitoring **Configuration**

Configuration > Appliance Settings > **Logging/Monitoring**

Log Options Alert Options Alarm Options Syslog Server HTTP Server Application

View Log File

Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.

Filename: **SDWAN_firewal.log** ▼ Filter (Optional):

View Log

Download Log File

Filename: **S35mount_overlay.log** ▼ **Download Log**

Die NAT-Verbindungsdetails werden in der Protokolldatei angezeigt.

```

2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/firewall/connection-48704 Removed 3 Connections
2020-05-11T10:15:44.750109+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)

```

Dynamische NAT

May 10, 2021

Dynamic NAT ist eine Viele-zu-Eins-Zuordnung einer privaten IP-Adresse oder Subnetze innerhalb des SD-WAN-Netzwerks zu einer öffentlichen IP-Adresse oder Subnetz außerhalb des SD-WAN-Netzwerks. Der Datenverkehr aus verschiedenen Zonen und Subnetzen über vertrauenswürdige (innerhalb) IP-Adressen im LAN-Segment wird über eine einzelne öffentliche (externe) IP-Adresse gesendet.

Dynamische NAT-Typen

Dynamic NAT führt Port Address Translation (PAT) zusammen mit der IP-Adressenübersetzung durch. Portnummern werden verwendet, um zu unterscheiden, welcher Datenverkehr zu welcher IP-Adresse gehört. Eine einzelne öffentliche IP-Adresse wird für alle internen privaten IP-Adressen verwendet, jeder privaten IP-Adresse wird jedoch eine andere Portnummer zugewiesen. PAT ist eine kostengünstige Möglichkeit, mehrere Hosts die Verbindung mit dem Internet über eine einzelne öffentliche IP-Adresse zu ermöglichen.

- **Port restricted:** Port Restricted NAT verwendet denselben externen Port für alle Übersetzungen, die sich auf eine Inside IP Address und Port-Paar beziehen. Dieser Modus wird normalerweise verwendet, um Internet-P2P-Anwendungen zuzulassen.
- **Symmetrisch:** Symmetric NAT verwendet denselben externen Port für alle Übersetzungen, die sich auf eine Innen-IP-Adresse, einen Innenanschluss, eine externe IP-Adresse und ein Outside Port Tupel beziehen. Dieser Modus wird normalerweise verwendet, um die Sicherheit zu erhöhen oder die maximale Anzahl von NAT-Sitzungen zu erweitern.

Eingehende und ausgehende NAT

Die Richtung für eine Verbindung kann entweder von innen nach außen oder von außen nach innen sein. Wenn eine NAT-Regel erstellt wird, wird sie je nach Richtungsübereinstimmungstyp auf beide

Richtungen angewendet.

- **Ausgehend:** Die Zieladresse wird für Pakete übersetzt, die für den Dienst empfangen wurden. Die Quelladresse wird für Pakete übersetzt, die über den Dienst übertragen werden. Ausgehende dynamische NAT wird auf lokalen, Internet-, Intranet- und Inter-Routing-Domänendiensten unterstützt. Bei WAN-Diensten wie Internet- und Intranetdiensten wird die konfigurierte WAN-Link-IP-Adresse dynamisch als externe IP-Adresse gewählt. Geben Sie für lokale und inter-Routing-Domänendienste eine externe IP-Adresse an. Die Zone Außerhalb wird vom ausgewählten Dienst abgeleitet. Ein typischer Anwendungsfall für ausgehende dynamische NAT besteht darin, gleichzeitig mehreren Benutzern in Ihrem LAN den sicheren Zugriff auf das Internet über eine einzige öffentliche IP-Adresse zu ermöglichen.
- **Inbound:** Die Quelladresse wird für Pakete übersetzt, die für den Dienst empfangen wurden. Die Zieladresse wird für Pakete übersetzt, die über den Dienst übertragen werden. Eingehende dynamische NAT wird von WAN-Diensten wie Internet und Intranet nicht unterstützt. Es liegt ein expliziter Überwachungsfehler vor, der dasselbe angibt. Eingehende dynamische NAT wird nur für lokale und inter-Routing-Domänendienste unterstützt. Geben Sie eine externe Zone und eine externe IP-Adresse an, in die übersetzt werden soll. Ein typischer Anwendungsfall für eingehende dynamische NAT besteht darin, externen Benutzern Zugriff auf E-Mail- oder Webserver zu ermöglichen, die in Ihrem privaten Netzwerk gehostet werden.

Konfigurieren dynamischer NAT-Richtlinien

Um Dynamische NAT-Richtlinien zu konfigurieren, navigieren Sie im Konfigurations-Editor zu **Verbindungen > Firewall > Dynamische NAT-Richtlinien**.

? x

Add

Priority:
100

Direction: Outbound ▼ Type: Port Restricted ▼ Service Type: Internet ▼ Service Name: Internet ▼

Inside Zone: Any ▼ Inside IP Address: *

☒ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☒ Port Parity ☐ Bind Responder Route

Port Forwarding Rules +

| Protocol | Outside Port | Inside IP Address | Inside Port | Fragments | Log Interval (s) | Log Start | Log End | Connection State Tracking | Delete |
|----------|--------------|-------------------|-------------|-----------|------------------|-----------|---------|---------------------------|--------|
| | | | | | | | | | |

Add Cancel

- **Priorität:** Die Reihenfolge, in der die Richtlinie innerhalb aller definierten Richtlinien angewendet wird. Richtlinien mit niedrigerer Priorität werden vor Richtlinien mit höherer Priorität angewendet.

- **Richtung:** Die Richtung, in die der Verkehr fließt, aus der Perspektive der virtuellen Schnittstelle oder des Dienstes. Es kann sich entweder um eingehender oder ausgehender Datenverkehr handeln.
- **Typ:** Der Typ der auszuführenden dynamischen NAT, Port-restricted oder Symmetric.
- **Diensttyp:** Die SD-WAN-Diensttypen, auf die die dynamische NAT-Richtlinie angewendet wird. Eingehende dynamische NAT wird auf lokalen und inter-Routing-Domänendiensten unterstützt. Ausgehende dynamische NAT wird auf lokalen, Internet-, Intranet- und Inter-Routing-Domänendiensten unterstützt.
- **Dienstname:** Wählen Sie einen konfigurierten Dienstnamen aus, der dem Diensttyp entspricht.
- **Inside Zone:** Der Match-Typ der Inside Firewall Zone, aus dem das Paket stammen muss, um die Übersetzung zu ermöglichen.
- **Outside Zone:** Geben Sie für eingehenden Datenverkehr den Spieltyp der externen Firewallzone an, aus dem das Paket stammen muss, um die Übersetzung zu ermöglichen.
- **Inside IP Adresse:** Die innere IP-Adresse und das Präfix, auf die übersetzt werden muss, wenn die Übereinstimmungskriterien erfüllt sind. Geben Sie '*' ein, um eine innere IP-Adresse anzugeben.
- **Externe IP-Adresse:** Die äußere IP-Adresse und das Präfix, auf die die innere IP-Adresse übersetzt wird, wenn die Übereinstimmungskriterien erfüllt sind. Für ausgehenden Datenverkehr mit Internet- und Intranetdiensten wird die konfigurierte WAN-Link-IP-Adresse dynamisch als externe IP-Adresse gewählt.
- **Zugehörige zulassen:** Erlaubt Datenverkehr im Zusammenhang mit dem Flow, der der Regel entspricht. Beispielsweise bezieht sich die ICMP-Umleitung auf den spezifischen Fluss, der mit der Richtlinie übereinstimmt, wenn ein Fehler im Zusammenhang mit dem Flow aufgetreten ist.
- **IPsec Pass-Through:** Erlaubt die Übersetzung einer IPsec-Sitzung (AH/ESP).
- **GRE/PPTP Pass-Through:** Erlaubt die Übersetzung einer GRE/PPTP-Sitzung.
- **Portparität:** Wenn diese Option aktiviert ist, behalten externe Ports für NAT-Verbindungen die Parität bei (auch wenn der innere Port gerade ist, ungerade, wenn der externe Port ungerade ist).
- **Bind-Responder-Route:** Stellt sicher, dass der Antwortdatenverkehr über denselben Dienst gesendet wird, an dem er empfangen wird, um ein asymmetrisches Routing zu vermeiden.

Port-Weiterleitung

Dynamische NAT mit Portweiterleitung ermöglicht es Ihnen, bestimmten Datenverkehr an eine definierte IP-Adresse weiterzuleiten. Dies wird normalerweise für Hosts wie Webserver verwendet. Sobald der dynamische NAT konfiguriert ist, können Sie die Portweiterleitungsrichtlinien definieren. Konfigurieren Sie dynamische NAT für die IP-Adressenübersetzung und definieren Sie die Portweiterleitungsrichtlinie, um einen externen Port einem internen Port zuzuordnen. Dynamische

NAT-Portweiterleitung wird normalerweise verwendet, um Remotehosts die Verbindung zu einem Host oder Server in Ihrem privaten Netzwerk zu ermöglichen. Einen detaillierteren Anwendungsfall finden Sie unter [Citrix SD-WAN Dynamic NAT erklärt](#).

Add

Priority: 200

Direction: Inbound Type: Symmetric Service Type: Local Service Name: VirtualInterfac...

Inside IP Address: * Outside Zone: Internet_Zone Outside IP Address: 172.147.12.83

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☐ Bind Responder Route

Port Forwarding Rules +

| Routing Domain | Protocol | Outside Port | Inside IP Address | Inside Port | Fragments | Log Interval (s) | Log Start | Log End | Connection State Tracking | Delete |
|-----------------------|----------|--------------|-------------------|-------------|-------------------------------------|------------------|--------------------------|--------------------------|---------------------------|--------|
| Default_RoutingDomain | Both | 443 | 15.15.15.1 | 443 | <input checked="" type="checkbox"/> | 0 | <input type="checkbox"/> | <input type="checkbox"/> | Use Site Setting | |

Add **Cancel**

- **Protokoll:** TCP, UDP oder beides.
- **Externer Port:** Der externe Port, der an den internen Port weitergeleitet wird.
- **Inside IP Adresse:** Die innere Adresse, um passende Pakete weiterzuleiten.
- **Interner Port:** Der interne Port, an den der externe Port weitergeleitet wird.
- **Fragmente:** Erlaubt das Weiterleiten von fragmentierten Paketen.
- **Protokollintervall:** Sekunde zwischen der Protokollierung der Anzahl der Pakete, die der Richtlinie entsprechen, mit einem Syslog-Server.
- **Log-Start:** Wenn diese Option ausgewählt ist, wird ein neuer Protokolleintrag für den neuen Flow erstellt.
- **Log-Ende:** Protokolliert die Daten für einen Flow, wenn der Flow gelöscht wird.

Hinweis

Der Standardwert für Protokollintervall 0 bedeutet keine Protokollierung.

- **Track:** Die bidirektionale Verfolgung des Verbindungsstatus wird für TCP-, UDP- und ICMP-Pakete durchgeführt, die der Regel entsprechen. Diese Funktion blockiert Flows, die aufgrund von asymmetrischem Routing oder Ausfall der Prüfsumme, protokollspezifischen Validierung nicht legitim erscheinen. Die Statusdetails werden unter **Monitoring > Firewall > Connections** angezeigt.
- **Kein Tracking:** Die bidirektionale Verfolgung des Verbindungsstatus wird nicht für Pakete durchgeführt, die der Regel entsprechen.

Jede Portweiterleitungsregel hat eine übergeordnete NAT-Regel. Die externe IP-Adresse wird der übergeordneten NAT-Regel entnommen.

Automatisch erstellte dynamische NAT-Richtlinien

Dynamische NAT-Richtlinien für den Internetdienst werden in den folgenden Fällen automatisch erstellt:

- Konfigurieren des Internetdienstes auf einer nicht vertrauenswürdigen Schnittstelle (WAN-Verbindung).
- Aktivieren des Internetzugriffs für alle Routingdomänen auf einer einzigen WAN-Verbindung. Weitere Informationen finden Sie unter [Konfigurieren der Firewall-Segmentierung](#).
- Konfigurieren von DNS-Weiterleitungen oder DNS-Proxy auf SD-WAN. Weitere Informationen finden Sie unter [Domännennamensystem](#).

Überwachen

Um dynamische NAT zu überwachen, navigieren Sie zu **Monitoring > Firewall-Statistiken > Verbindungen**. Für eine Verbindung können Sie sehen, ob NAT fertig ist oder nicht.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Firewall

Firewall Statistics

Statistics

Connections

Maximum entries to display: 50

Filtering

Application: Any

Family: Any

IP Protocol: Any

Source Zone: Any

Destination Zone: Any

Source Service Type: Any

Source Service Instance: Any

Destination Service Type: Any

Destination Service Instance: Any

Source IP: *

Source Port: *

Destination IP: *

Destination Port: *

Refresh

Clear Connections

Help

Connections

| Application | Family | IP Protocol | IP Address | Port | Service Type | Service Name | Zone | IP Address | Port | Service Type | Service Name | Zone | State | Is NAT | Packets | Bytes | PPS | Kbps | Packets | Bytes |
|--------------------------|-----------------|-------------|--------------|-------|--------------|--------------|------------------|-------------|------|--------------|--------------------|-------------------------|-------------|--------|---------|-------|-------|-------|---------|-------|
| Domain Name Service(dns) | Network Service | UDP | 172.57.48.50 | 34202 | Local | VF-1-LAN-1 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | BR210_UTM-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 140 | 0.008 | 0.004 | 2 | 140 |
| Domain Name Service(dns) | Network Service | UDP | 172.57.48.50 | 42261 | Local | VF-1-LAN-1 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | BR210_UTM-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 140 | 0.008 | 0.004 | 2 | 140 |
| Domain Name Service(dns) | Network Service | UDP | 172.57.48.50 | 34058 | Local | VF-1-LAN-1 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | BR210_UTM-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 114 | 0.008 | 0.004 | 2 | 114 |
| Domain Name Service(dns) | Network Service | UDP | 172.57.48.50 | 50486 | Local | VF-1-LAN-1 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | BR210_UTM-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 114 | 0.008 | 0.004 | 2 | 114 |
| Domain Name Service(dns) | Network Service | UDP | 172.57.48.50 | 33928 | Local | VF-1-LAN-1 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | BR210_UTM-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 124 | 0.008 | 0.004 | 2 | 124 |
| Domain Name Service(dns) | Network Service | UDP | 172.57.48.50 | 50354 | Local | VF-1-LAN-1 | Default_LAN_Zone | 10.140.50.5 | 53 | Internet | BR210_UTM-Internet | Untrusted_Internet_Zone | ESTABLISHED | Yes | 2 | 124 | 0.008 | 0.004 | 2 | 124 |

Um die innere IP-Adresse zur Zuordnung von externen IP-Adressen weiter zu sehen, klicken Sie unter **Verwandte Objekte** auf **NAT vor der Route** oder **NAT nach der Route** oder navigieren Sie zu **Überwachung > Firewall-Statistiken > NAT-Richtlinien**.

Der folgende Screenshot zeigt die Statistiken für die dynamische NAT-Regel vom Typ symmetrisch und die entsprechende Portweiterleitungsregel.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies
Maximum entries to display: 50
NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any
Service Type: Any Service Name: Any
Inside IP: * Inside Port: * Outside IP: * Outside Port: *
Refresh Show latest data.
Help

NAT Policies

| ID | Rule Type | Rule Parent | Direction | IP Protocol | Service Type | Service Name | Inside IP Address | Inside Port | Outside IP Address | Outside Port | Allow Related | Allow IPSec Passthrough | Allow GRE Passthrough | Packets Sent | Bytes Sent | Packets Received | Bytes Received | Connections | Related Objects |
|----|--------------|-------------|-----------|-------------|--------------|--------------|-------------------|-------------|--------------------|--------------|---------------|-------------------------|-----------------------|--------------|------------|------------------|----------------|-------------|-----------------|
| 1 | Dynamic Sym | - | Outbound | * | Internet | - | * | * | 172.147.12.83/32 | * | No | No | No | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | Port Forward | 1 | Outbound | * | Internet | - | 172.147.90.12/32 | 5001-5010 | 172.147.12.83/32 | 5001-5010 | No | No | No | 82 | 47232 | 8928 | 13374144 | 0 | |

NAT Policies Displayed: 2
NAT Policies In Use: 2/100
Port Restricted Dynamic NAT Policies In Use: 0/100
Destination NAT Policies In Use: 0/100

Wenn eine Portweiterleitungsregel erstellt wird, wird auch eine entsprechende Firewallregel erstellt.

Site: Branch1 + Site Site Site

Connections

WAN-to-WAN Forwarding
Virtual Paths
Dynamic Virtual Paths
Internet Service
Intranet Services
WAN Links
GRE Tunnels
IPsec Tunnels
Firewall
Application Routes
Routes
OSPF
BGP
Route Learning Properties
Inter Routing Domain Services
Multicast Groups
Applications

Pre-Appliance Template Policies

Local Policies + Add

| Priority | Routing Domain | Action | From | To | Application | Application Family | Application Objects | IP Protocol | DSCP | Service | IP Address | Port | Service | IP Address | Port | Match | Add | Info | Edit | Delete | Clone |
|----------|----------------|--------|---------------|----|-------------|--------------------|---------------------|-------------|------|----------|------------|---------|---------|------------|------|-------|-----|------|------|--------|-------|
| (auto) | * | Allow | * | * | * | * | * | Any | * | IP Host | * | * | * | * | * | * | | | | | |
| (auto) | * | Allow | Internet_Zone | * | * | * | * | Any | * | Internet | * | * | * | * | * | Yes | | | | | |
| (auto) | * | Allow | Internet_Zone | * | * | * | * | TCP (6) | * | Internet | * | 0-65535 | * | 15.15.15.1 | 443 | | | | | | |
| (auto) | * | Allow | Internet_Zone | * | * | * | * | UDP (17) | * | Internet | * | 0-65535 | * | 15.15.15.1 | 443 | | | | | | |
| (auto) | * | Drop | * | * | * | * | * | Any | * | Internet | * | * | * | * | * | | | | | | |

Post-Appliance Template Policies

Apply Refresh

Sie können die Statistiken der Filterrichtlinie anzeigen, indem Sie zu **Überwachung > Firewall-Statistiken > Filterrichtliniennavigieren**.

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics: Filter Policies
Maximum entries to display: 50
Filtering: Routing Domain: Any Application: Any Family: Any IP Protocol: Any
Filter Policy Action: Any Source Service Type: Any Source Service Name: Any Source IP: *
Source Port: * Destination Service Type: Any Destination Service Name: Any Destination IP: *
Destination Port: * Source Zone: Any Destination Zone: Any DSCP: Any
Refresh Show latest data.
Help

Filter Policies

Default Policy=Allow(Not Tracked) Packets=3414 Bytes=213489
Match In Progress Packets=0 Bytes=0

| ID | Routing Domain | Application | Family | IP Protocol | DSCP | Service Type | Service Name | IP Address | Port or ICMP Type | Zone | Service Type | Service Name | IP Address | Port or ICMP Code | Zone | Action | Conn Match Type | Track Connection | Allow Fragments | Log Connection Start | Log Connection End | Packets | Bytes | Related Objects |
|----|----------------|-------------|--------|-------------|------|--------------|--------------|------------|-------------------|---------------|--------------|--------------|---------------|-------------------|------|--------|-----------------|------------------|-----------------|----------------------|--------------------|---------|-------|-----------------|
| 1 | * | * | * | * | * | IPHost | - | * | NA | * | * | - | * | NA | * | Allow | Default | No | Yes | No | No | 0 | 0 | |
| 2 | * | * | * | * | * | Internet | - | * | NA | Internet_Zone | * | - | * | NA | * | Allow | Established | No | Yes | No | No | 0 | 0 | |
| 3 | * | * | * | TCP | * | Internet | - | * | * | Internet_Zone | * | - | 15.15.15.1/32 | 443 | * | Allow | Default | No | Yes | No | No | 0 | 0 | |
| 4 | * | * | * | UDP | * | Internet | - | * | * | Internet_Zone | * | - | 15.15.15.1/32 | 443 | * | Allow | Default | No | Yes | No | No | 0 | 0 | |
| 5 | * | * | * | * | * | Internet | - | * | NA | * | * | - | * | NA | * | Drop | Default | No | Yes | No | No | 0 | 0 | |

Protokolle

Sie können Protokolle im Zusammenhang mit NAT in Firewall-Protokollen anzeigen. Um Protokolle für NAT anzuzeigen, erstellen Sie eine Firewallrichtlinie, die Ihrer NAT-Richtlinie entspricht, und stellen Sie sicher, dass die Protokollierung auf dem Firewallfilter aktiviert ist.

Edit ? x

Priority: Policy Type: **Built-in Firewall**

Match Criteria

From Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| gre_zone | <input type="checkbox"/> |
| Inter Routing Domain Zone | <input type="checkbox"/> |

To Zones

| Zone | Enable |
|---------------------------|-------------------------------------|
| Any | <input checked="" type="checkbox"/> |
| Default_LAN_Zone | <input type="checkbox"/> |
| gre_zone | <input type="checkbox"/> |
| Inter Routing Domain Zone | <input type="checkbox"/> |

Routing Domain: **Any**

Traffic Match Type: **IP Protocol** IP Protocol: **Any** DSCP: **Any** ☐ Match Established

Application: Application Family: Application Objects: **Any**

Source Service Type: **Any** Source Service Name: **Any** Source IP: Source Port:

Dest Service Type: **Any** Dest Service Name: **Any** Dest IP: Dest Port:

Actions

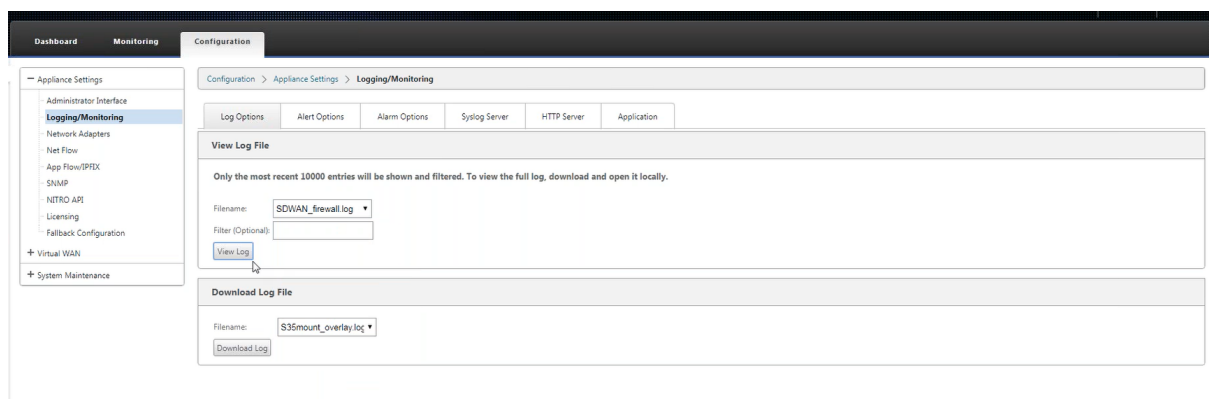
Action: **Allow** ☒ Allow Fragments Connection State Tracking: **Use Site Setting**

Logging & Other Options

Log Interval (s): ☒ Log Start ☒ Log End ☐ Add Reverse Policy

Apply Cancel

Navigieren Sie zu **Logging/Monitoring > Log-Optionen**, wählen Sie **SDWAN_firewal.log** und klicken Sie auf **Protokoll anzeigen**.



Die NAT-Verbindungsdetails werden in der Protokolldatei angezeigt.

```

2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/ NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:44.750109+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299955+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112659+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.646123+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)

```

Konfigurieren des virtuellen WAN-Dienstes

May 10, 2021

Die Citrix SD-WAN-Konfiguration beschreibt und definiert die Topologie Ihres Citrix SD-WAN Netzwerks. Bevor Sie ein SD-WAN-Netzwerk bereitstellen können, müssen Sie die Virtual WAN-Konfiguration definieren. Verwenden Sie hierzu den Konfigurations-Editor in der Citrix SD-WAN Verwaltungswebchnittstelle auf der MCN-Appliance.

Sicherheit und Verschlüsselung

Die Aktivierung der Verschlüsselung für SD-WAN (für die virtuellen Pfade) ist optional. Anweisungen zur Konfiguration dieser Funktion finden Sie im Abschnitt [Aktivieren und Konfigurieren von Virtual WAN-Sicherheit und Verschlüsselung \(optional\)](#)

Wenn die Verschlüsselung aktiviert ist, verwendet SD-WAN den Advanced Encryption Standard (AES), um den Datenverkehr über den virtuellen Pfad zu sichern. Sowohl AES-128-Bit- als auch 256-Bit-Chiffre (Schlüsselgrößen) werden von den SD-WAN-Appliances unterstützt und sind konfigurierbare Optionen. Sie können diese und die anderen Verschlüsselungsoptionen auswählen,

aktivieren und konfigurieren, indem Sie den Konfigurations-Editor im Management-Webinterface auf dem Management Control Node (MCN) verwenden. Sie müssen über Administratorzugriff auf den MCN verfügen, um die Konfiguration zu ändern und Ihre Änderungen über das SD-WAN-Netzwerk zu verteilen. Sobald der MCN gesichert ist, sind die Verschlüsselungseinstellungen und deren Verteilung ebenfalls sicher.

Die Authentifizierung zwischen Standorten funktioniert mit der virtuellen WAN-Konfiguration. Die Netzwerkkonfiguration verfügt über einen geheimen Schlüssel für jeden Standort. Für jeden virtuellen Pfad generiert die Netzwerkkonfiguration einen Schlüssel, indem die geheimen Schlüssel von den Standorten an jedem Ende des virtuellen Pfads kombiniert werden. Der anfängliche Schlüsselaustausch, der nach dem ersten Einrichten eines virtuellen Pfads erfolgt, hängt von der Fähigkeit ab, Pakete mit diesem kombinierten Schlüssel zu verschlüsseln und zu entschlüsseln.

Aktivieren des virtuellen WAN-Dienstes

Wenn es sich um eine Erstinstallation und Konfiguration handelt, müssen Sie den Virtual WAN-Dienst als letzten Schritt manuell auf jeder SD-WAN-Appliance in Ihrem Netzwerk aktivieren. Durch Aktivieren des Dienstes wird der Virtual WAN-Daemon aktiviert und gestartet.

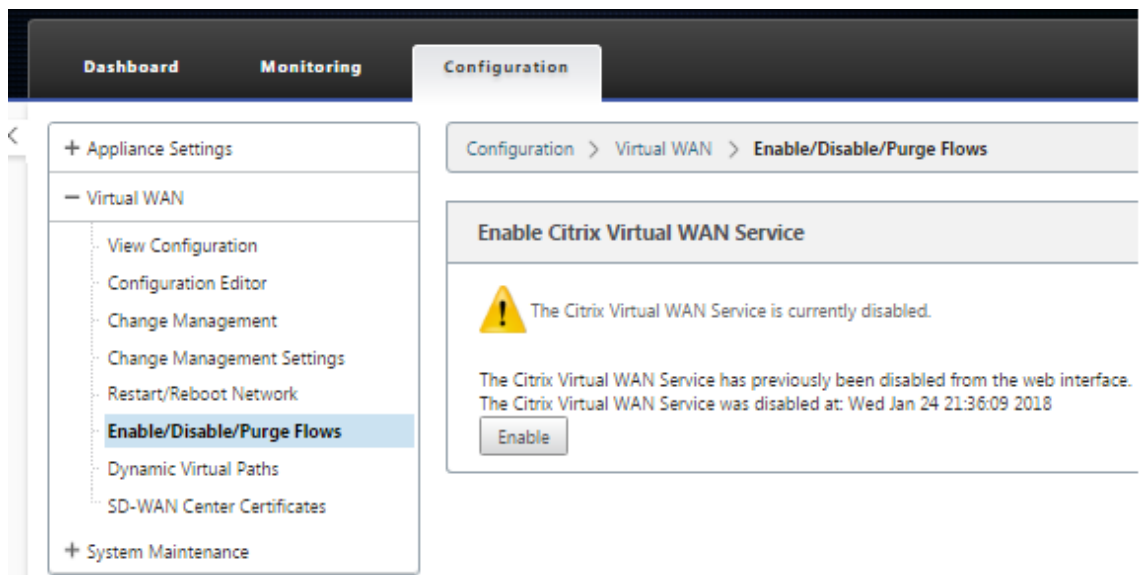
Hinweis

Wenn Sie eine vorhandene Bereitstellung neu konfigurieren, aktiviert der MCN den Dienst automatisch, wenn er die aktualisierten Appliance-Pakete an die Client-Sites verteilt. In diesem Fall können Sie diesen letzten Schritt überspringen.

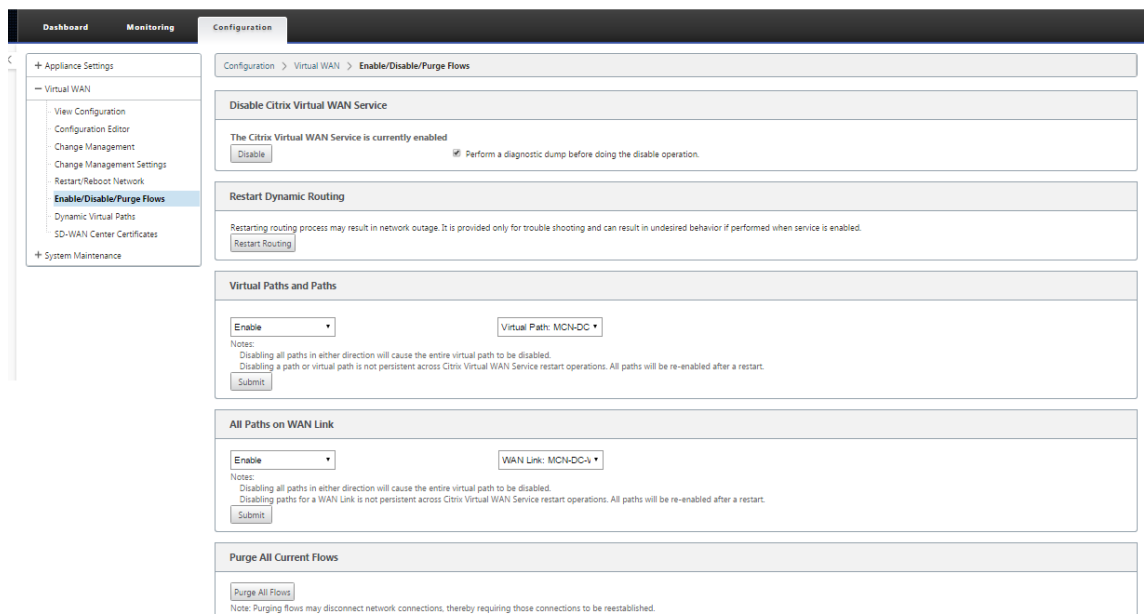
Gehen Sie folgendermaßen vor, um den virtuellen WAN-Dienst auf einer Appliance manuell zu aktivieren:

1. Melden Sie sich bei der Managementoberfläche der Appliance an, die Sie aktivieren möchten.
2. Wählen Sie die Registerkarte **Konfiguration** aus.
3. Öffnen Sie im Navigationsbereich den Virtual WAN-Zweig, und wählen Sie **Flows aktivieren/deaktivieren/löschen**.

Wenn der virtuelle WAN-Dienst deaktiviert ist, wird die Seite Virtuellen WAN-Dienst aktivieren angezeigt, wie unten dargestellt. Wenn der Dienst bereits aktiviert ist, wird die Seite Flows aktivieren/deaktivieren/löschen angezeigt.



4. Klicken Sie auf **Aktivieren**. Dadurch wird der Service aktiviert und die Seite **Flows aktivieren/deaktivieren/löschen** angezeigt.



Wenn der virtuelle WAN-Dienst aktiviert ist, wird im oberen Bereich der Seite eine entsprechende Statusmeldung angezeigt.

Hinweis

Diese Seite enthält auch Optionen zum Aktivieren/Deaktivieren bestimmter Pfade und virtueller Pfade in Ihrem Netzwerk sowie eine Option zum Löschen aller Flows.

Damit ist die Installation und Aktivierung des SD-WAN auf den MCN- und Zweigstandclient-Appliances

abgeschlossen. Sie können nun die Monitoring-Seiten verwenden, um die Aktivierung zu überprüfen und vorhandene oder potenzielle Konfigurationsprobleme zu diagnostizieren.

Konfigurieren der Firewall-Segmentierung

May 10, 2021

Virtual Route Forwarding (VRF) Firewall-Segmentierung bietet mehrere Routingdomänen Zugriff auf das Internet über eine gemeinsame Schnittstelle, wobei der Datenverkehr jeder Domäne von dem der anderen isoliert ist. Zum Beispiel können Mitarbeiter und Gäste über die gleiche Schnittstelle auf das Internet zugreifen, ohne dass jeder Zugriff auf den Verkehr des anderen erfolgt.

- Lokaler Gast-User Internetzugang
- Internet-Zugang für Mitarbeiter und Benutzer für definierte Anwendungen
- Mitarbeiter-Benutzer können alle anderen Traffic an den MCN weiterführen
- Erlauben Sie dem Benutzer, bestimmte Routen für bestimmte Routingdomänen hinzuzufügen.
- Wenn diese Funktion aktiviert ist, gilt diese Funktion für alle Routingdomänen.

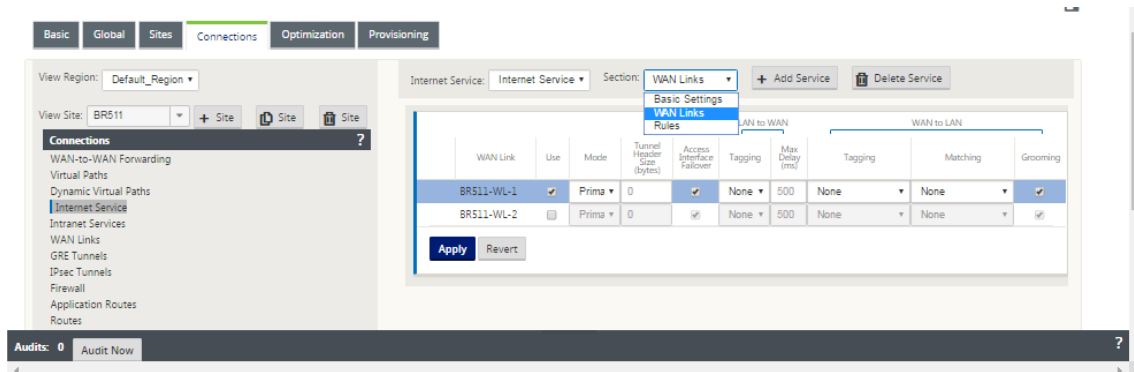
Sie können auch mehrere Zugriffsschnittstellen erstellen, um separate öffentliche IP-Adressen aufzunehmen. Beide Optionen bieten die erforderliche Sicherheit für jede Benutzergruppe.

Hinweis

Weitere Informationen finden Sie unter [Vorgehensweise VRFs konfigurieren](#).

So konfigurieren Sie Internetdienste für alle Routingdomänen:

1. Erstellen Sie Internetdienst für eine Site. Navigieren Sie zu **Verbindungen > Region anzeigen > Website anzeigen > [Sitenamen] > > Internet Service > Abschnitt > WAN-Links**, und aktivieren Sie unter WAN-Links das Kontrollkästchen **Verwenden**.



Hinweis

Sie sollten sehen, dass 0.0.0.0/0 Routen hinzugefügt werden, eine pro Routingdomäne, unter **Verbindungen > Region anzeigen > Website anzeigen > [Sitename] > Routen**.

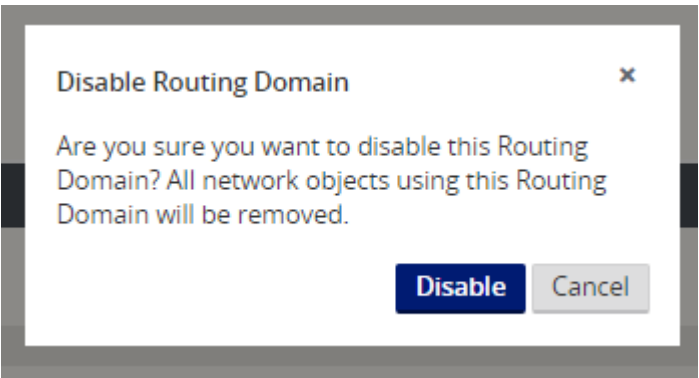
Search:

| Order | Network IP Address | Routing Domain | Cost | Service Type | Service Name | Gateway IP Address | Info | Edit | Delete |
|-------|--------------------|----------------|------|--------------|--------------|--------------------|------|------|--------|
| 1 | 10.200.247.41/24 | Default | 5 | Local | | | | | |
| 2 | 10.200.247.42/24 | Default | 5 | Local | | | | | |
| 3 | 10.200.247.6/24 | Default | 5 | Local | | | | | |
| 4 | 11.123.10.0/24 | | 5 | Intranet | Intranet-0 | | | | |
| 5 | 11.20.20.11/24 | Guest | 5 | Local | | | | | |
| 6 | 12.125.10.0/24 | | 5 | Internet | | | | | |
| 7 | 0.0.0.0/0 | Default | 5 | Internet | | | | | |
| 8 | 0.0.0.0/0 | Guest | 5 | Internet | | | | | |
| 9 | 0.0.0.0/0 | Default | 16 | Passthrough | | | | | |
| 10 | 0.0.0.0/0 | Guest | 16 | Passthrough | | | | | |

« < 1 > »

Es ist nicht mehr erforderlich, alle Routingdomänen im MCN aktiviert zu haben.

2. Wenn Sie Routingdomänen am MCN deaktivieren, wird die folgende Meldung angezeigt, wenn die Domänen an einem Zweigstandort verwendet werden:



3. Sie können bestätigen, dass jede Routingdomäne den Internetdienst verwendet, indem Sie die Spalte Routingdomäne in der Tabelle Flows der Webverwaltungsschnittstelle unter **Monitor > Flows** aktivieren.

Flows List

Toggle Columns

Both WAN Ingress and WAN Egress Flows

| Routing Domain | Source IP Address | Dest IP Address | Direction | Source Port | Dest Port | IPP | DSCP | Hit Count | Service Type | Service Name | LAN GW IP | Age (ms) | Packets | Bytes | PPS | Customer kbps | Conduit Overhead kbps | IPsec Overhead kbps | Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type |
|----------------|-------------------|-----------------|-------------|-------------|-----------|------|---------|-----------|--------------|--------------|-----------|----------|---------|-------|-------|---------------|-----------------------|---------------------|---------|-------|------------|------|-----------------------------|-------------------|
| Guest | 11.20.20.20 | 12.125.10.20 | WAN Ingress | 8 | 3335 | ICMP | default | 62 | INTERNET | - | LOCAL | 74 | 62 | 5208 | 1.013 | 0.681 | 0.000 | 0.000 | 202 | N/A | N/A | N/A | N/A | N/A |
| Default | 10.200.247.200 | 12.125.10.20 | WAN Ingress | 8 | 16185 | ICMP | default | 66 | INTERNET | - | LOCAL | 311 | 66 | 5544 | 1.009 | 0.678 | 0.000 | 0.000 | 202 | N/A | N/A | N/A | N/A | N/A |
| Guest | 12.125.10.20 | 11.20.20.20 | WAN Egress | 0 | 19456 | ICMP | default | 62 | INTERNET | - | LOCAL | 94 | 62 | 5208 | 1.013 | 0.681 | 0.000 | 0.000 | 202 | N/A | N/A | N/A | N/A | N/A |
| Default | 12.125.10.20 | 10.200.247.200 | WAN Egress | 0 | 3968 | ICMP | default | 66 | INTERNET | - | LOCAL | 328 | 66 | 5544 | 1.008 | 0.678 | 0.000 | 0.000 | 202 | N/A | N/A | N/A | N/A | N/A |

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

4. Sie können auch die Routingtabelle für jede Routingdomäne unter **Monitor > Statistik > Routen** überprüfen.

Routes for routing domain: Guest

Filter: in Any column

Show 100 entries Showing 1 to 5 of 5 entries

| Num | Network Addr | Gateway IP Address | Service | Firewall Zone | Reachable | Site IP Address | Site | Type | Protocol | Neighbor Direct | Cost | Hit Count | Eligible | Eligibility Type | Eligibility Value |
|-----|---------------|--------------------|-----------------|------------------------|-----------|-----------------|--------------|--------|----------|-----------------|------|-----------|----------|------------------|-------------------|
| 0 | 11.20.20.0/24 | * | Local | Default_LAN_Zone | YES | * | Angelina-CFB | Static | | | 5 | 318 | YES | N/A | N/A |
| 1 | 11.10.10.0/24 | * | DC-Angelina-CFB | Default_LAN_Zone | YES | * | DC | Static | | | 5 | 0 | YES | N/A | N/A |
| 2 | 0.0.0.0/0 | * | Internet | Untrusted_Internet_Zon | YES | * | * | Static | | | 5 | 159 | YES | N/A | N/A |
| 3 | 0.0.0.0/0 | * | Passthrough | Any | YES | * | * | Static | | | 16 | 0 | YES | N/A | N/A |
| 4 | 0.0.0.0/0 | * | Discard | Any | YES | * | * | Static | | | 16 | 0 | YES | N/A | N/A |

Showing 1 to 5 of 5 entries

Anwendungsfälle

In früheren Citrix SD-WAN-Versionen hatten virtuelle Routing und Weiterleitung die folgenden Probleme, die behoben wurden.

- Kunden verfügen über mehrere Routingdomänen an einem Zweigstandort, ohne dass alle Domänen im Rechenzentrum (MCN) berücksichtigt werden müssen. Sie benötigen die Möglichkeit, den Datenverkehr verschiedener Kunden auf sichere Weise zu isolieren.
- Kunden müssen in der Lage sein, über eine einzige zugängliche öffentliche IP-Adresse mit Firewall zu verfügen, damit mehrere Routingdomänen an einem Standort auf das Internet zugreifen können (über VRF lite hinaus).
- Kunden benötigen für jede Routingdomäne eine Internetroute, die verschiedene Dienste unterstützt.
- Mehrere Routingdomänen an einem Zweigstandort.
- Internetzugang für verschiedene Routingdomänen.

Mehrere Routingdomänen an einem Zweigstandort

Mit den Erweiterungen der Segmentierung Virtual Forwarding und Routing Firewall können Sie:

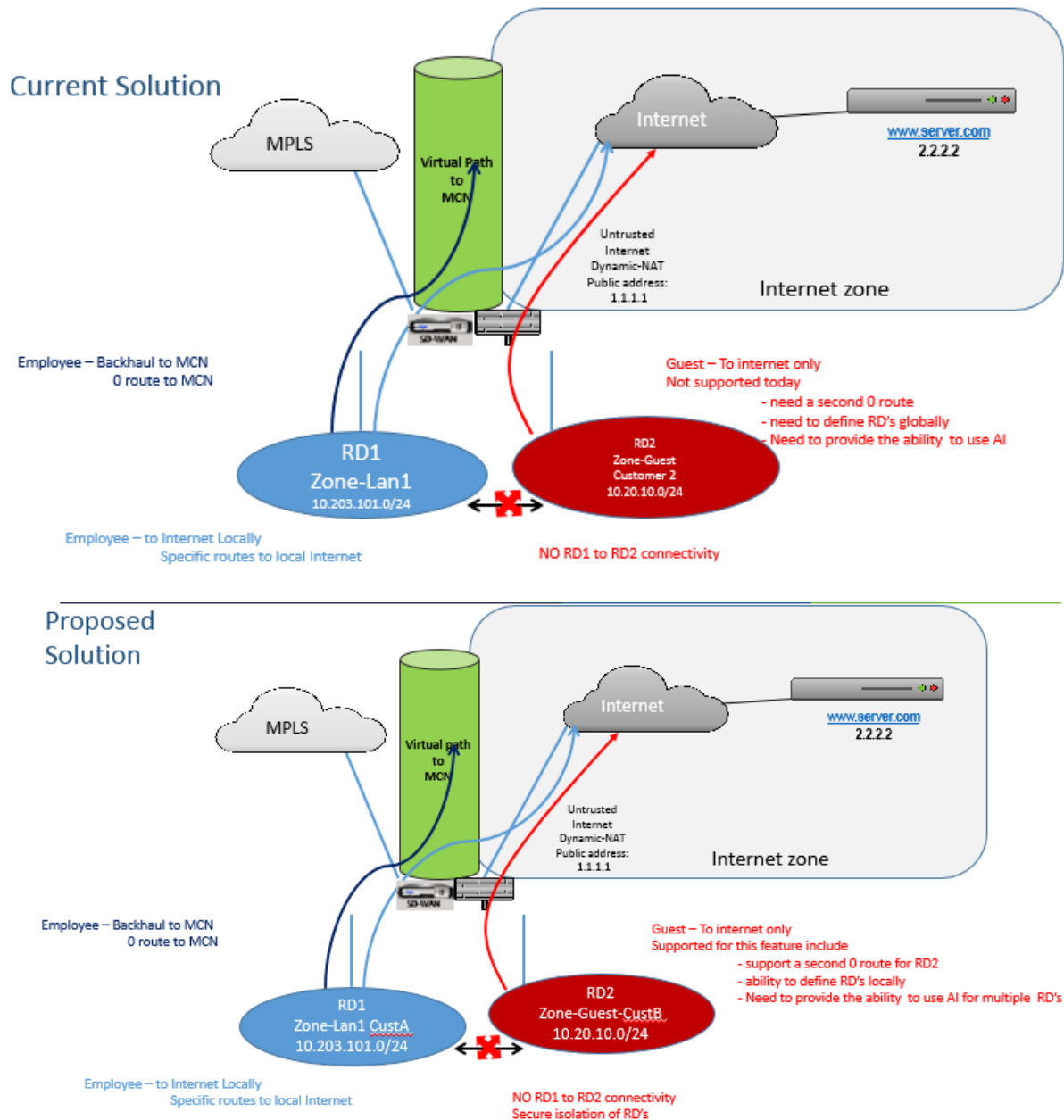
- Stellen Sie eine Infrastruktur am Standort der Zweigstelle bereit, die sichere Konnektivität für mindestens zwei Benutzergruppen unterstützt, z. B. Mitarbeiter und Gäste. Die Infrastruktur kann bis zu 16 Routingdomänen unterstützen.
- Isolieren Sie den Datenverkehr jeder Routingdomäne vom Datenverkehr einer anderen Routingdomäne.
- Bereitstellung des Internetzugangs für jede Routingdomäne
 - Eine gemeinsame Zugriffsoberfläche ist erforderlich und akzeptabel
 - Eine Zugriffsschnittstelle für jede Gruppe mit separaten öffentlichen IP-Adressen
- Traffic für den Mitarbeiter kann direkt an das lokale Internet weitergeleitet werden (spezifische Anwendungen)

- Traffic für den Mitarbeiter kann zur umfangreichen Filterung an den MCN weitergeleitet oder rücktransportiert werden (0 Route)
- Datenverkehr für die Routingdomäne kann direkt an das lokale Internet weitergeleitet werden (0 Route)
- Unterstützung bestimmter Routen pro Routingdomäne, falls erforderlich
- Routingdomänen sind VLAN-basiert
- Entfernt die Anforderung, dass sich die RD am MCN befinden muss
- Routingdomäne kann jetzt nur an einem Zweigstandort konfiguriert werden
- Ermöglicht das Zuweisen mehrerer RD zu einer Zugriffsoberfläche (einmal aktiviert)
- Jeder RD wird eine 0.0.0.0 Route zugewiesen
- Ermöglicht das Hinzufügen bestimmter Routen für eine RD
- Ermöglicht Datenverkehr von verschiedenen RD über dieselbe Zugriffsoberfläche in das Internet zu verlassen
- Ermöglicht das Konfigurieren einer anderen Zugriffsoberfläche für jede RD
- Muss eindeutige Subnetze sein (RD wird einem VLAN zugewiesen)
- Jede RD kann dieselbe FW-Standardzone verwenden
- Der Datenverkehr wird durch die Routingdomäne isoliert
- Ausgehende Flows haben die RD als Komponente des Flow-Headers. Ermöglicht SD-WAN die Zuordnung von Rückgabeflüssen zur korrekten Routingdomäne.

Voraussetzungen für die Konfiguration mehrerer Routingdomänen:

- Der Internetzugang wird konfiguriert und einem WAN-Link zugewiesen.
- Firewall für NAT konfiguriert und korrekte Richtlinien angewendet.
- Zweite Routingdomäne global hinzugefügt.
- Jede Routingdomäne, die einem Standort hinzugefügt wird.
- Stellen Sie unter **Sites** > Site-Name > **WAN-Links** > WL2 [Name] > **Access Interface** sicher, dass das Kontrollkästchen verfügbar ist und der Internetdienst korrekt definiert wurde. Wenn Sie das Kontrollkästchen nicht aktivieren können, ist der Internetdienst weder definiert noch einer WAN-Verbindung für die Site zugewiesen.

Bereitstellungsszenarien



Einschränkungen

- Der Internetdienst muss der WAN-Link hinzugefügt werden, bevor Sie den Internetzugriff für alle Routingdomänen aktivieren können. (Bis Sie dies tun, ist das Kontrollkästchen zum Aktivieren dieser Option ausgegraut).

Nachdem Sie den Internetzugriff für alle Routingdomänen aktiviert haben, fügen Sie automatisch eine Dynamic-NAT-Regel hinzu.

- Bis zu 16 Routingdomänen pro Site.
- Access Interface (AI): Einzelne AI pro Subnetz.
- Für mehrere AI ist ein separates VLAN für jede AI erforderlich.
- Wenn Sie zwei Routingdomänen an einem Standort haben und über einen einzelnen WAN-Link verfügen, verwenden beide Domänen dieselbe öffentliche IP-Adresse.
- Wenn der Internetzugriff für alle Routingdomänen aktiviert ist, können alle Sites an das Internet weitergeleitet werden. (Wenn eine Routingdomäne keinen Internetzugang erfordert, können Sie den Datenverkehr mit der Firewall blockieren.)
- Keine Unterstützung für dasselbe Subnetz in mehreren Routingdomänen.
- Es gibt keine Überwachungsfunktion
- Die WAN-Verbindungen werden für den Internetzugang freigegeben.
- Kein QOS pro Routingdomäne; First come first serve.

Zertifikatauthentifizierung

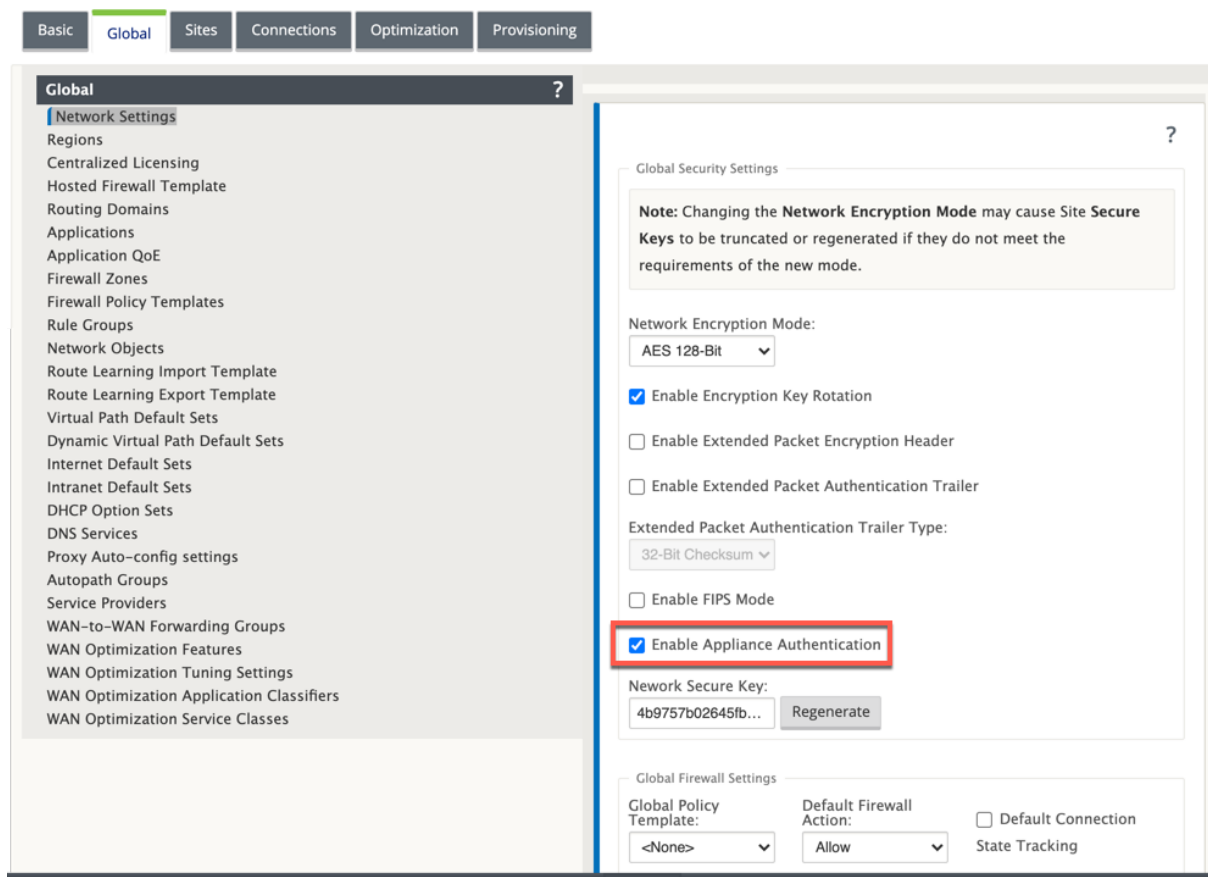
May 10, 2021

Citrix SD-WAN stellt sicher, dass sichere Pfade zwischen Appliances im SD-WAN-Netzwerk eingerichtet werden, indem Sicherheitstechniken wie Netzwerkverschlüsselung und IPsec-Tunnel für virtuelle Pfade verwendet werden. Zusätzlich zu den bestehenden Sicherheitsmaßnahmen wird die zertifikatsbasierte Authentifizierung in Citrix SD-WAN 11.0.2 eingeführt.

Mit der Zertifikatauthentifizierung können Organisationen Zertifikate verwenden, die von ihrer privaten Zertifizierungsstelle (Certificate Authority, CA) ausgestellt wurden, um Appliances zu authentifizieren. Die Appliances werden authentifiziert, bevor die virtuellen Pfade eingerichtet werden. Wenn beispielsweise eine Zweige-Appliance versucht, eine Verbindung mit dem Datencenter herzustellen und das Zertifikat aus dem Zweig nicht mit dem Zertifikat übereinstimmt, das das Rechenzentrum erwartet, wird der virtuelle Pfad nicht eingerichtet.

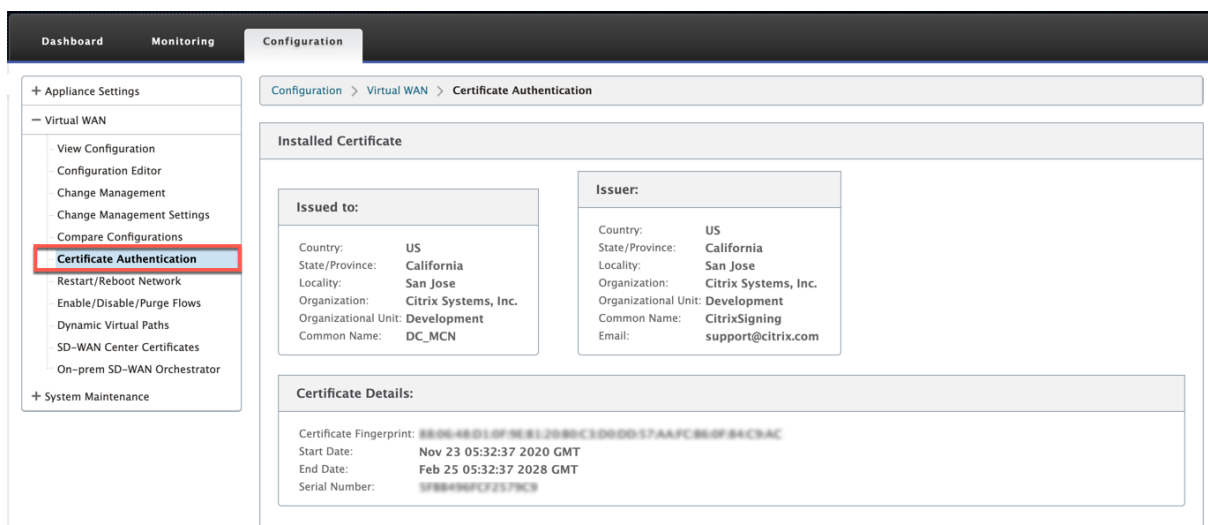
Das von der Zertifizierungsstelle ausgestellte Zertifikat bindet einen öffentlichen Schlüssel an den Namen der Appliance. Der öffentliche Schlüssel arbeitet mit dem entsprechenden privaten Schlüssel, der im Besitz der durch das Zertifikat identifizierten Appliance ist.

Um die Appliance-Authentifizierung zu aktivieren, navigieren Sie im Konfigurations-Editor zu **Global > Netzwerkeinstellungen** und wählen Sie **Einheitenauthentifizierung aktivieren** aus.



Nachdem die Konfiguration bereitgestellt und angewendet wurde, wird unter **Konfiguration** > **Virtuelles WAN** eine neue **Zertifikatauthentifizierungsoption** aufgeführt.

Sie können alle Zertifikate, die für die virtuelle Pfadauthentifizierung verwendet werden, auf der Seite **Zertifikatauthentifizierung** verwalten.



Hinweis

Wenn Sie die Appliance-Software von SD-WAN Version 11.0 auf Version 11.1 oder höher aktualisieren, deaktivieren Sie die Option **“Appliance-Authentifizierung aktivieren”** und führen Sie das Software-Upgrade durch. Sobald der Upgradevorgang abgeschlossen ist, wählen Sie die Option **“Appliance-Authentifizierung aktivieren”**.

Installiertes Zertifikat

Der Abschnitt **Installiertes Zertifikat** enthält eine Zusammenfassung des Zertifikats, das auf der Appliance installiert ist. Die Appliance verwendet dieses Zertifikat, um sich im Netzwerk zu identifizieren.

Der Abschnitt **Ausgestellt für** enthält Details darüber, an wen das Zertifikat ausgestellt wurde. Der **allgemeine Name** im Zertifikat stimmt mit dem Namen der Appliance überein, da das Zertifikat an den Appliance-Namen gebunden ist. Der Abschnitt **Aussteller** enthält die Details der Zertifikatsignierungsstelle, die das Zertifikat signiert hat. Zu den Zertifikatsdetails gehören der Fingerabdruck des Zertifikats, die Seriennummer und die Gültigkeitsdauer des Zertifikats.

| Installed Certificate | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--------------------------|--------------------------|-----------------|-------------|--------------------------|-----------|--------------------------|----------------------|----------------------|-------------|--------------|----|---|----------|----|-----------------|------------|-----------|----------|---------------|----------------------|----------------------|-------------|--------------|---------------|--------|--------------------|
| Issued to: <table> <tr> <td>Country:</td> <td>US</td> </tr> <tr> <td>State/Province:</td> <td>California</td> </tr> <tr> <td>Locality:</td> <td>San Jose</td> </tr> <tr> <td>Organization:</td> <td>Citrix Systems, Inc.</td> </tr> <tr> <td>Organizational Unit:</td> <td>Development</td> </tr> <tr> <td>Common Name:</td> <td>DC</td> </tr> </table> | Country: | US | State/Province: | California | Locality: | San Jose | Organization: | Citrix Systems, Inc. | Organizational Unit: | Development | Common Name: | DC | Issuer: <table> <tr> <td>Country:</td> <td>US</td> </tr> <tr> <td>State/Province:</td> <td>California</td> </tr> <tr> <td>Locality:</td> <td>San Jose</td> </tr> <tr> <td>Organization:</td> <td>Citrix Systems, Inc.</td> </tr> <tr> <td>Organizational Unit:</td> <td>Development</td> </tr> <tr> <td>Common Name:</td> <td>CitrixSigning</td> </tr> <tr> <td>Email:</td> <td>support@citrix.com</td> </tr> </table> | Country: | US | State/Province: | California | Locality: | San Jose | Organization: | Citrix Systems, Inc. | Organizational Unit: | Development | Common Name: | CitrixSigning | Email: | support@citrix.com |
| Country: | US | | | | | | | | | | | | | | | | | | | | | | | | | | |
| State/Province: | California | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Locality: | San Jose | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Organization: | Citrix Systems, Inc. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Organizational Unit: | Development | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Common Name: | DC | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Country: | US | | | | | | | | | | | | | | | | | | | | | | | | | | |
| State/Province: | California | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Locality: | San Jose | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Organization: | Citrix Systems, Inc. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Organizational Unit: | Development | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Common Name: | CitrixSigning | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Email: | support@citrix.com | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Certificate Details: <table> <tr> <td>Certificate Fingerprint:</td> <td></td> </tr> <tr> <td>Start Date:</td> <td>Aug 13 13:45:47 2019 GMT</td> </tr> <tr> <td>End Date:</td> <td>Aug 10 13:45:47 2029 GMT</td> </tr> <tr> <td>Serial Number:</td> <td></td> </tr> </table> | | Certificate Fingerprint: | | Start Date: | Aug 13 13:45:47 2019 GMT | End Date: | Aug 10 13:45:47 2029 GMT | Serial Number: | | | | | | | | | | | | | | | | | | | |
| Certificate Fingerprint: | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Start Date: | Aug 13 13:45:47 2019 GMT | | | | | | | | | | | | | | | | | | | | | | | | | | |
| End Date: | Aug 10 13:45:47 2029 GMT | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Serial Number: | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Identitätsbündel hochladen

Das Identity Bundle enthält einen privaten Schlüssel und das Zertifikat, das dem privaten Schlüssel zugeordnet ist. Sie können das von der Zertifizierungsstelle ausgestellte Appliance-Zertifikat in die Appliance hochladen. Das Zertifikatsbündel ist eine PKCS 12-Datei mit der Erweiterung .p12. Sie können wählen, um es mit einem Kennwort zu schützen. Wenn Sie das Kennwortfeld leer lassen, wird es als kein Kennwortschutz behandelt.

| Upload Identity Bundle (PKCS12) | |
|---|---------------------------------|
| File: | C:\ID\SD-WAN\11.0.2\S Browse... |
| Password: | |
| <input type="button" value="Upload Identity Bundle"/> | |

Zertifizierungsstellenpaket hochladen

Laden Sie das PKCS 12-Bundle hoch, das der Zertifikatsignierungsstelle entspricht. Das Zertifizierungsstellenpaket enthält die komplette Signaturkette, die Wurzel und die gesamte zwischengeschaltete Unterzeichnerautorität.

| Upload Certificate Authority Bundle (PKCS12) | |
|---|---------------------------------|
| File: | C:\ID\SD-WAN\11.0.2\S Browse... |
| <input type="button" value="Upload CA Bundle"/> | |

| Upload Network Certificates (PEM) | |
|--|---------------------------------|
| File: | C:\ID\SD-WAN\11.0.2\S Browse... |
| <input type="button" value="Upload Network Bundle"/> | |

Zertifizierungssignaturanforderung erstellen

Die Appliance kann eine nicht signierte Zertifizierung generieren und eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) erstellen. Die CA kann dann die CSR von der Appliance herunterladen, signieren und im PEM- oder DER-Format wieder auf die Appliance hochladen. Dies wird als Identitätszertifikat für die Appliance verwendet. Um eine CSR für eine Appliance zu erstellen, geben Sie den allgemeinen Namen der Appliance, die Organisationsdetails und die Adresse an.

| Create Certificate Signing Request (CSR) | | | |
|---|----------------|-------------------------------|----------|
| Common Name: | DC | Business name / Organization: | Citrix |
| Department Name / Organizational Unit: | Networks | Town / City: | New York |
| Province, Region, County or State: | USA | Country: | US |
| Email address: | johndoe@citrix | | |
| <input type="button" value="Create CSR"/> | | | |

Zertifikatssperrlisten-Manager

Eine Zertifikatssperrliste (Certificate Revocation List, CRL) ist eine veröffentlichte Liste von Zertifikatsseriennummern, die im Netzwerk nicht mehr gültig sind. Die CRL-Datei wird regelmäßig

heruntergeladen und lokal auf der gesamten Appliance gespeichert. Wenn ein Zertifikat authentifiziert wird, untersucht der Responder die CRL, um festzustellen, ob das Initiatorzertifikat bereits widerrufen wurde. Citrix SD-WAN unterstützt derzeit Version 1-CRLs im PEM- und DER-Format.

Um die Zertifikatsperrliste zu aktivieren, wählen Sie die Option Zertifikatsperrliste aktiviert aus. Geben Sie den Speicherort an, an dem die CRL-Datei verwaltet wird. HTTP-, HTTPS- und FTP-Speicherorte werden unterstützt. Geben Sie das Zeitintervall an, um die CRL-Datei zu überprüfen und herunterzuladen. Der Bereich beträgt 1–1440 Minuten.

Certificate Revocation List Management (CRL)

CRL Enabled:

☒

CRL URI:

CRL Update Interval (Minutes):

Update Settings

Hinweis

Der Reauthentifizierungszeitraum für einen virtuellen Pfad kann zwischen 10 und 15 Minuten liegen. Wenn das CRL-Aktualisierungsintervall auf eine kürzere Dauer festgelegt ist, kann die aktualisierte CRL-Liste eine derzeit aktive Seriennummer enthalten. Stellen Sie ein aktiv gesperrtes Zertifikat für kurze Zeit in Ihrem Netzwerk zur Verfügung.

AppFlow und IPFIX

September 26, 2023

AppFlow und IPFIX sind Flow-Exportstandards zur Identifizierung und Erfassung von Anwendungs- und Transaktionsdaten in der Netzwerkinfrastruktur. Diese Daten geben eine bessere Einsicht in die Auslastung und Leistung des Anwendungsdatenverkehrs.

Die gesammelten Daten, sogenannte Flow Records, werden an einen oder mehrere IPv4-Sammler übertragen. Die Kollektoren aggregieren die Flow-Datensätze und generieren Echtzeit- oder historische Berichte.

AppFlow

AppFlow exportiert Daten nur für HDX/ICA-Verbindungen. Sie können entweder TCP nur für HDX-Dataset-Vorlage oder die HDX-Dataset-Vorlage aktivieren. Das TCP nur für HDX-Dataset bietet [Multi-Hop-Daten](#). Das HDX-Dataset bietet [HDX Einblick Daten](#).

Hinweis

Die HDX-Vorlage ist nur für Citrix SD-WAN PE-Edition und Zwei-Box-Appliances verfügbar. Sie sollte auf der Rechenzentrum-Appliance aktiviert sein.

AppFlow Collectors wie Splunk und Citrix ADM verfügen über Dashboards, um diese Vorlagen zu interpretieren und zu präsentieren.

IPFIX

IPFIX ist ein Collector-Exportprotokoll, das zum Exportieren von Flow-Level-Daten für alle Verbindungen verwendet wird. Für jede Verbindung können Sie Informationen wie Paketanzahl, Byteanzahl, Diensttyp, Flussrichtung, Routingdomäne, Anwendungsname usw. anzeigen. IPFIX-Flows werden über die Management-Schnittstelle übertragen. Die meisten Collectors können IPFIX-Flow-Datensätze empfangen, müssen jedoch möglicherweise ein benutzerdefiniertes Dashboard erstellen, um die IPFIX-Vorlage zu interpretieren.

Die IPFIX-Vorlage definiert die Reihenfolge, in der der Datenstrom interpretiert werden soll. Der Collector erhält einen Vorlagendatensatz, gefolgt von den Datensätzen. Citrix SD-WAN verwendet die Vorlagen 611, 612 und 613, um IPFIX-Flussdaten zu exportieren.

Sie können **Application Flow Info (IPFIX)** wählen, um Datensätze gemäß den Vorlagen 611 und 612 zu exportieren. Wenn es Probleme beim Exportieren der Flow-Daten gibt, wählen Sie **Basic Properties (IPFIX)**, die Datensätze gemäß Vorlage 613 exportieren.

Die folgenden Tabellen enthalten eine detaillierte Liste der Flow-Daten, die jeder IPFIX-Vorlage zugeordnet sind.

Anwendungsfluss-Info (IPFIX) - V10-Vorlagen**Vorlagen-ID - 611**

| Infoelement (IE) | IE Name & ID | Typ und len | Beschreibung |
|------------------------|-------------------------|----------------|--------------|
| Beobachtungspunkt-ID | observationPointId, 138 | Unsigned32, 4 | |
| Prozess-ID exportieren | exportingProcessId, 144 | Unsigned32, 4 | |
| Flow-ID | flowId, 148 | Unsigned64, 8 | |
| Ipv4 SRC IP | sourceIPv4Address, 8 | Ipv4address, 4 | |

| Infoelement (IE) | IE Name & ID | Typ und len | Beschreibung |
|--|------------------------------|-------------------------|--|
| Ipv4 DST IP | destinationIpv4Address, 12 | Ipv4address, 4 | |
| Ipvversion | ipVersion, 60 | Unsigned8, 1 | |
| IP-Protokollnummer | protocolIdentifier, 4 | Unsigned8, 1 | |
| Padding | Nicht zutreffend | Unsigned16, 2 | |
| SRC-Port | sourceTransportPort, 7 | Unsigned16, 2 | |
| DST-Port | destinationTransportPort, 11 | Unsigned16, 2 | |
| Pkt Count | packetDeltaCount, 2 | Unsigned64, 8 | |
| Byte-Anzahl | octetDeltaCount, 1 | Unsigned64, 8 | |
| Zeit für den ersten Pkt in Mikrosekunden | flowStartMicroseconds, 154 | dateTimeMicroseconds, 8 | |
| Zeit für lastpkt in Mikrosekunden | flowEndMicroseconds, 155 | dateTimeMicroseconds, 8 | |
| IP ToS | ipClassOfService, 5 | Unsigned8, 1 | |
| Flow-Flags | tcpControlBits, 6 | Unsigned8, 2 | Derzeit auf 0 eingestellt. |
| Fließrichtung | flowDirection, 61 | Unsigned8, 1 | 0x00: ingress flow 0x01: egress flow WAN-WAN und LAN-LAN flows sind in SDWAN möglich |
| Eingangsschnittstelle | ingressInterface, 10 | Unsigned32, 4 | Citrix SD-WAN -Lastenausgleich Datenflüsse über mehrere Elementpfade, daher kann ein einzelner Datenfluss mehrere Eingabe-/Ausgabe-Schnittstellenkombinationen aufweisen. |

| Infoelement (IE) | IE Name & ID | Typ und len | Beschreibung |
|-----------------------|-----------------------|----------------------|--|
| Ausgabe-Schnittstelle | egressInterface, 14 | Unsigned32, 4 | Citrix SD-WAN -Lastenausgleich Datenflüsse über mehrere Elementpfade, daher kann ein einzelner Datenfluss mehrere Eingabe-/Ausgabe- Schnittstellenkombinationen aufweisen. |
| Eingabe-Vlan-ID | vlanId, 58 | Unsigned16, 2 | |
| Ausgabe-Vlan-ID | postVlanId, 59 | Unsigned16, 2 | |
| VRF ID | ingressVRFID, 234 | Unsigned32, 4 | |
| Flow Key Indikator | flowKeyIndicator, 173 | Unsigned64, 8 | Stellen Sie auf 0x1E037F. |
| Anwendungs-ID | applicationId, 95 | octetArray, variable | Die Anwendungs-ID ist identisch mit der ID der Anwendungen, die vom DPI-Modul klassifiziert werden. Die Anwendungs-IDs bleiben konstant. Die Anwendungs-IDs für benutzerdefinierte domänennamen- basierte Anwendungen ändern sich mit jedem Konfigurationsupdate. |

Vorlage 612

| Infoelement (IE) | IE Name & ID | Typ | Kommentar |
|----------------------------|----------------------------|------------|--|
| Anwendungs-ID | applicationId, 95 | octetArray | Die Anwendungs-ID ist identisch mit der ID der Anwendungen, die vom DPI-Modul klassifiziert werden. Die Anwendungs-IDs bleiben konstant. Die Anwendungs-IDs für benutzerdefinierte domänennamen-basierte Anwendungen ändern sich mit jedem Konfigurationsupdate. |
| Anwendungsname | applicationName, 96 | string | Gibt den Namen der Citrix SDWAN-spezifischen proprietären Anwendung an. |
| Beschreibung der Anwendung | applicationDescription, 94 | string | Gibt die Beschreibung der Anwendung an. |

Grundlegende Eigenschaften (IPFIX) —V9-konforme Vorlage - Vorlage 613

| Infoelement (IE) | IE Name & ID | Typ und len | Kommentar |
|--------------------|----------------------------|----------------|-----------|
| Ipv4 SRC IP | sourceIPv4Address, 8 | Ipv4address, 4 | |
| Ipv4 DST IP | destinationIPv4Address, 12 | Ipv4address, 4 | |
| Ipvversion | ipVersion, 60 | Unsigned8, 1 | |
| IP-Protokollnummer | protocolIdentifier, 4 | Unsigned8, 1 | |
| IP ToS | ipClassOfService, 5 | Unsigned8, 1 | |

| Infoelement (IE) | IE Name & ID | Typ und len | Kommentar |
|-----------------------|------------------------------|---------------|---|
| Fließrichtung | flowDirection, 61 | Unsigned8, 1 | 0x00: ingress flow 0x01: egress flow WAN-WAN und LAN-LAN flows sind in SDWAN möglich |
| SRC-Port | sourceTransportPort, 7 | Unsigned16, 2 | |
| DST-Port | destinationTransportPort, 11 | Unsigned16, 2 | |
| Pkt Count | packetDeltaCount, 2 | Unsigned64, 8 | |
| Byte-Anzahl | octetDeltaCount, 1 | Unsigned64, 8 | |
| Eingangsschnittstelle | ingressInterface, 10 | Unsigned32, 4 | Citrix SD-WAN -Lastenausgleich Datenflüsse über mehrere Elementpfade, daher kann ein einzelner Datenfluss mehrere Eingabe-/Ausgabe-Schnittstellenkombinationen aufweisen. |
| Ausgabe-Schnittstelle | egressInterface, 14 | Unsigned32, 4 | |
| Eingabe-Vlan-ID | vlanId, 58 | Unsigned16, 2 | Citrix SD-WAN -Lastenausgleich Datenflüsse über mehrere Elementpfade, daher kann ein einzelner Datenfluss mehrere Eingabe-/Ausgabe-Schnittstellenkombinationen aufweisen. |
| Ausgabe-Vlan-ID | postVlanId, 59 | Unsigned16, 2 | |

Einschränkungen

- Das Exportintervall für Net Flow wird von 15 Sekunden auf 60 Sekunden erhöht.

- AppFlow/IPFIX Flows werden über UDP übertragen, bei Verbindungsverlust werden nicht alle Daten erneut übertragen. Wenn das Exportintervall auf X Minuten festgelegt ist, speichert die Appliance nur X Minuten Daten. Das wird nach X Minuten Verbindungsverlust erneut übertragen.
- In Citrix SD-WAN Version 10, Version 2, werden die **AppFlow** Einstellungen für jede Appliance lokal vorgenommen, während in den vorherigen Versionen eine globale Einstellung war. Wenn die SD-WAN-Software-Version auf eine der vorherigen Versionen herabgestuft wird und AppFlow auf einer der Appliances konfiguriert ist, wird sie global auf alle Allianzen angewendet.

Konfigurieren von AppFlow/IPFIX

Sie können AppFlow /IPFIX auf einzelnen SD-WAN-Appliances konfigurieren oder im SD-WAN Center konfigurieren und die Konfiguration auf eine Gruppe von Appliances übertragen.

So konfigurieren Sie AppFlow /IPFIX auf SD-WAN-Appliances:

1. Navigieren Sie in der Citrix SD-WAN SE/PE-Webschnittstelle zu **Konfiguration > AppFlow/IPFIX**.
2. Klicken Sie auf **Aktivieren**.

The screenshot displays the 'AppFlow/IPFIX' configuration page in the Citrix SD-WAN 11.2 interface. The left-hand navigation pane lists various settings, with 'AppFlow/IPFIX' currently selected. The main configuration area is titled 'AppFlow Host Settings' and includes the following sections:

- AppFlow Host Settings:**
 - ☒ Enable
 - Data Update Interval (minutes):
 - Appflow Data Set:
 - ☒ TCP only for HDX
 - ☐ HDX
- AppFlow / IPFIX Collector 1:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☐ Application Flow Info (IPFIX)
 - ☐ Citrix ADM Citrix ADM user: Password:
- AppFlow / IPFIX Collector 2:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☐ Application Flow Info (IPFIX)
 - ☒ Citrix ADM Citrix ADM user: Password:
- AppFlow / IPFIX Collector 3:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☒ Application Flow Info (IPFIX)
 - ☐ Citrix ADM Citrix ADM user: Password:
- AppFlow / IPFIX Collector 4:**
 - IP Address: Port:
 - Data Set: ☒ Appflow ☒ Application Flow Info (IPFIX)
 - ☐ Citrix ADM Citrix ADM user: Password:

3. Geben Sie im Feld **Datenaktualisierungsintervall** das Zeitintervall in Minuten an, ab dem die Flow-Berichte in den AppFlow/IPFIX-Collector exportiert werden. Das maximale Intervall beträgt 10 Minuten.
4. Wählen Sie die **AppFlow Datenmengenvorlage** aus. Sie können eine der folgenden Datenmengenvorlagen auswählen:
 - **TCP nur für HDX (AppFlow):** Die AppFlow-Datenmengenvorlage zum Sammeln und Senden von Multi-Hop-Daten von ICA-Verbindungen an den AppFlow-Kollektor.
 - **HDX (AppFlow):** Die AppFlow Datenmengenvorlage zum Sammeln und Senden von HDX Insight-Daten von ICA-Verbindungen an AppFlow Collector.

Hinweis

Die **HDX-Vorlage** ist nur für Citrix SD-WAN PE- und Two Box-Appliances verfügbar.

5. Sie können bis zu vier AppFlow/IPFIX-Kollektoren konfigurieren. Geben Sie für jeden Kollektor die folgenden Parameter an:
 - **IP-Adresse:** Die IP-Adresse des externen AppFlow /IPFIX-Kollektorsystems.

- **Port:** Die Portnummer, auf der das externe AppFlow /IPFIX-Kollektorsystem wartet. Der Standardwert ist 4739. Sie können die Portnummer je nach verwendetem Kollektor ändern.
- **Application Flow Info (IPFIX):** Sendet Flow-Datensätze gemäß IPFIX-Vorlagen 611 und 612 an IPFIX-Sammler.
- **Grundlegende Eigenschaften (IPFIX):** Sendet Flow-Datensätze gemäß IPFIX-Vorlage 613 an IPFIX-Kollektoren.
- **Citrix ADM:** Wählen Sie diese Option aus, um Citrix ADM als AppFlow -Kollektor zu verwenden.

Hinweis

Citrix ADM unterstützt derzeit keine IPFIX-Sammlung.

- **Citrix ADM Benutzer:** Benutzername des Citrix ADM -Kollektors
- **Kennwort:** Citrix ADM Collector-Kennwort.

Der Benutzername und das Kennwort werden verwendet, um sich nahtlos bei Citrix ADM anzumelden und Flussdaten zu speichern.

6. Klicken Sie auf **Einstellungen anwenden**.

So konfigurieren Sie **AppFlow /IPFIX-Kollektor** mit Citrix SD-WAN Center:

1. Navigieren Sie in der Verwaltungsschnittstelle von Citrix SD-WAN Center zu **Konfiguration > Appliance-Einstellungen**.
2. Navigieren Sie zum Abschnitt **AppFlow /IPFIX** und wählen Sie **In Datei einschließen**.
3. Wählen Sie **IPFIX/AppFlow -Sammlung aktivieren aus**.

The screenshot shows the 'Appflow / IPFIX' configuration page in Citrix SD-WAN Center. The 'Include in File' checkbox is checked. Under 'Enable IPFIX / Appflow Collection', the 'Data Update Interval (minutes)' is set to 2. The 'Appflow Data Set' section has two radio buttons: 'HDX (Applicable only for DC sites - PE/Two-Box)' and 'TCP for HDX (Applicable for branch sites)'. Below this, there are four collector configurations. Each configuration includes fields for 'IPFIX / Appflow Collector', 'Port' (set to 4739), 'Citrix ADM User', and 'Password'. The 'Data Set' section for each collector has checkboxes for 'Appflow' and 'Application Flow Info (IPFIX)'. The first collector is configured with IP 10.102.77.246 and user 'admin'. The second collector is configured with IP 10.102.29.30 and user 'admin'. The third collector is configured with IP 10.110.89.50 and user 'admin'. The fourth collector is configured with IP 10.103.40.78 and user 'admin'.

4. Geben Sie im Feld **Datenaktualisierungsintervall** das Zeitintervall in Minuten an, ab dem die AppFlow Berichte in den Kollektor AppFlow/IPFIX exportiert werden.

5. Wählen Sie die **AppFlow Datenmengenvorlage** aus. Sie können eine der folgenden Datenmengenvorlagen auswählen:

- **TCP nur für HDX:** Die AppFlow-Datenmengenvorlage zum Sammeln und Senden von MultiHop-Daten von ICA-Verbindungen an den AppFlow-Kollektor.
- **HDX:** Die AppFlow Datenmengenvorlage zum Sammeln und Senden von HDX Insight Daten von ICA-Verbindungen an AppFlow Collector.

Hinweis

Die **HDX-Vorlage** ist nur für Citrix SD-WAN PE- und Two Box-Appliances verfügbar.

6. Sie können bis zu vier AppFlow/IPFIX-Kollektoren konfigurieren. Geben Sie für jeden Kollektor die folgenden Parameter an:

- **IPFIX/AppFlow Collector:** Die IP-Adresse des externen AppFlow/IPFIX-Kollektorsystems.
- **Port:** Die Portnummer, auf der das externe AppFlow /IPFIX-Kollektorsystem wartet. Der Standardwert ist 4739. Sie können die Portnummer je nach verwendetem Kollektor ändern.
- **Application Flow Info:** Sendet Flow-Datensätze gemäß IPFIX-Vorlagen 611 und 612 an IPFIX-Kollektoren.
- **Grundlegende Eigenschaften (IPFIX):** Sendet Flow-Datensätze gemäß IPFIX-Vorlage 613 an IPFIX-Kollektoren.
- **Citrix ADM:** Wählen Sie diese Option aus, um Citrix ADM als AppFlow -Kollektor zu verwenden.

Hinweis

Citrix ADM unterstützt derzeit keine IPFIX-Sammlung.

- **Citrix ADM Benutzer:** Benutzername des Citrix ADM -Sammlers.
- **Kennwort:** Citrix ADM Collector-Kennwort.

Der Benutzername und das Kennwort werden verwendet, um sich nahtlos bei Citrix ADM anzumelden und Flussdaten zu speichern.

7. **Speichern** und **Exportieren** der Konfiguration in die verwalteten Appliances.

Hinweis

Wenn die SD-WAN Center-Version niedriger als 10.2 ist und die SD-WAN-Appliances Version 10.2 und höher ist, können Sie die folgenden Bedingungen beachten.

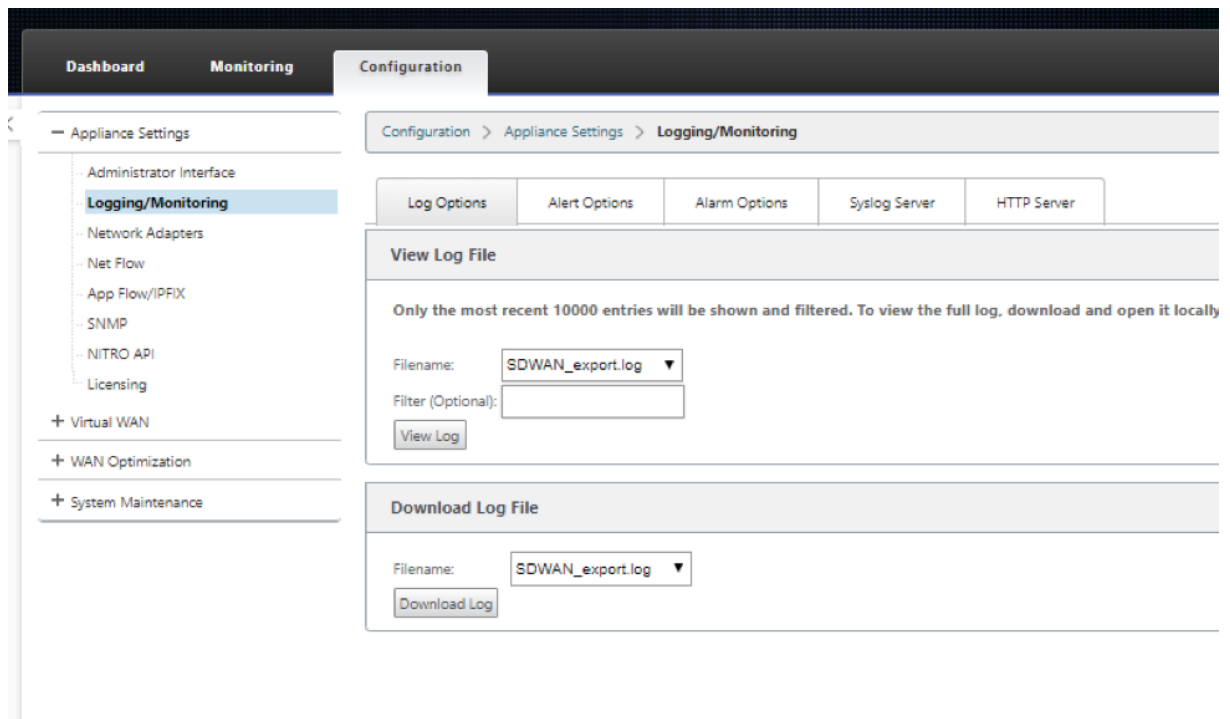
- Wenn lokale Kollektoren auf den Appliances aktiviert sind, wirkt sich die AppFlow /IPFIX-

Konfiguration, die vom SD-WAN-Center übertragen wurde, nicht auf die vorhandene Konfiguration aus.

- Wenn lokale Kollektoren auf den Appliances nicht aktiviert sind, wird die AppFlow/IPFIX-Konfiguration, die vom SD-WAN-Center übertragen wurde, auf die Appliance angewendet.
- Wenn die globale AppFlow/IPFIX-Konfiguration in der SD-WAN Center-Konfiguration aktiviert ist, sind alle lokalen Kollektoren auf den Appliances aktiviert.

Protokolldateien

Zur Behebung von Problemen im Zusammenhang mit AppFlow /IPFIX-Exportprotokollen können Sie die SDWAN_export.log-Dateien anzeigen und herunterladen. Navigieren Sie zu **Konfiguration > Protokollierung/Überwachung** und wählen Sie die Dateien **SDWAN_export.log** aus.



SNMP

November 16, 2022

Citrix SD-WAN unterstützt SNMPV1/V2-Funktionen und nur ein einzelnes Benutzerkonto für jede SNMPv3-Funktion. Diese Einschränkung bietet folgende Vorteile:

- Sicherstellung der SNMPv3-Konformität für Netzwerkgeräte

- Überprüfung der SNMPv3-Fähigkeit
- Einfache Konfiguration von SNMPv3

Um SNMPv3-Abfragen und Traps zu konfigurieren, navigieren Sie zum Abschnitt SNMPv3 auf der Seite **Konfiguration** -> **Einheiteneinstellungen** -> **SNMP** und füllen Sie die Felder nach Bedarf aus.

DashboardMonitoringConfiguration

<

— Appliance Settings

Administrator Interface

Logging/Monitoring

Network Adapters

Net Flow

App Flow

SNMP

NITRO API

Licensing

+ Virtual WAN

+ System Maintenance

Configuration > Appliance Settings > SNMP

Managers

Download MIB File

SNMP

UDP Port:161

System Description:Citrix Virtual WAN Appliance

System Contact:support@citrix.com

System Location:Citrix

SNMP v1/v2

☐ Enable v1/v2 Agent

Community String:public

☐ Enable v1/v2 Traps

Send v1/v2 Test Trap

Destination IP Address(es):

Port:162

SNMP v3

☐ Enable v3 Agent

User Name:

Password:

Verify Password:

Authentication:MD5

Encryption:None

☐ Enable v3 Traps

Send v3 Test Trap

Destination IP Address(es):

Port:162

User Name:

Password:

Verify Password:

Authentication:MD5

Encryption:None

Apply Settings

)

Standard MIB Support

Die folgenden Standard-MIBs werden von den SD-WAN-Appliances unterstützt.

| MIB | RFC (Definition Link) |
|--------------------------|---|
| 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 (teilweise) | https://www.ietf.org/rfc/rfc4293.txt |
| Q-BRIDGE-MIB (teilweise) | 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 |

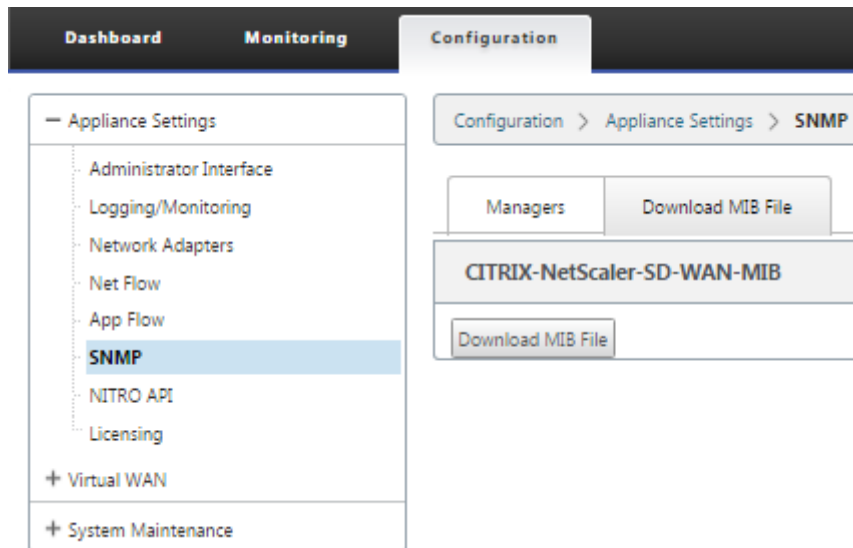
Sie müssen die folgenden SNMP-Dateien herunterladen, bevor Sie mit der Überwachung einer Citrix SD-WAN Appliance beginnen können:

- 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

Die MIB-Dateien werden von SNMPv3-Managern und SNMPv3-Trap-Listener verwendet. Zu den Dateien gehören die Unternehmens-MIBs der SD-WAN-Appliance, die SD-WAN-spezifische Ereignisse bereitstellen. So laden Sie MIB-Dateien in der SD-WAN-Webverwaltungsschnittstelle herunter:

1. Navigieren Sie zu **Konfiguration > Einheiteneinstellungen > SNMP > Seite MIB-Datei herunterladen**.
2. Wählen Sie die gewünschte **MIB-Datei** aus.
3. Klicken Sie **auf Ansicht**.

Die MIB-Datei wird im MIB-Browser geöffnet.



Hinweis

- Die Unterstützung dieser MIBs wird standardmäßig durch den **net-snmp snmpd-Daemon-Prozess** auf Linux-Systemen bereitgestellt. Die MIBs bilden die Grundlage für die Unterstützung von Netzwerkverwaltungsanwendungen.
- Das Ethernet-Port-Paket und die Byte-Zähler sind in **IF-MIB** in **ifTable**. Systeminformationen befinden sich im Systemobjekt.
- Ethernet-Ports sind in **ifTable** enthalten, daher muss das Gehen ausreichen, um sicherzustellen, dass das SNMP-Subsystem läuft.
- Unterstützung für **Q-BRIDGE-MIB** und **IP-MIB** bietet Unterstützung für die Netzwerk-Mapping-Anwendung.

Weitere Informationen zum Hinzufügen von SNMP-Manager, zum Konfigurieren von SNMP-Ansicht/Alarm und zum Hinzufügen von SNMP-Servern finden Sie in der CloudBridge 7.4-Dokumentation unter: [CloudBridge](#)

WAN-Optimierung

May 10, 2021

Die Citrix SD-WAN WANOP-Appliance optimiert WANOP-Verbindungen und sorgt so für maximale Reaktionsfähigkeit und Durchsatz. Die Citrix SD-WAN OP-Appliances arbeiten paarweise an jedem Ende einer Verbindung, um den Datenverkehr über die Verbindung zu beschleunigen. Im Folgenden sind einige der Funktionen von Citrix SD-WAN WANOP aufgeführt:

- Komprimierung
- TCP-Protokollbeschleunigung
- Verkehrsmanagement
- Anwendungsbeschleunigung
- Citrix XenApp/XenDesktop (HDX) Beschleunigung
- Integration
- Monitoring und Management

Informationen zur Installation, Bereitstellung und Feature-Konfiguration von Citrix SD-WAN WANOP 10.2 finden Sie in der Dokumentation: [Citrix SD-WAN WANOP](#). Die Funktionen und Verfahren für Citrix SD-WAN WANOP 10.2 ähneln den in der Citrix SD-WAN WANOP-Version dokumentierten Verfahren.

Sie können die WAN-Optimierungsfunktion auf Ihrer Citrix SD-WAN Premium Edition aktivieren und konfigurieren. Weitere Informationen finden Sie unter [Citrix SD-WAN Premium Edition](#).

Mit der WANOP Client-Plug-in-Software können Sie Netzwerkbeschleunigung auf allen Remote-Windows-Laptops oder -Workstations erreichen. Weitere Informationen finden Sie unter [WANOP-Client-Plug-in](#).

Citrix SD-WAN Premium Edition

May 10, 2021

Der Abschnitt enthält schrittweise Anweisungen zum Aktivieren und Konfigurieren der WAN-Optimierungsfunktionen für die SD-WAN Premium (Enterprise) Edition für Ihr Virtual WAN. Dazu verwenden Sie die Formulare für den Abschnitt **Optimierung** im **Konfigurationseditor** in der Webverwaltungsschnittstelle auf dem MCN.

Hinweis

Sie müssen eine SD-WAN Premium (Enterprise) Edition-Lizenz installiert haben, um auf die Funktionen der WAN-Optimierung in Ihrem Virtual WAN zuzugreifen, zu aktivieren, zu konfigurieren und zu aktivieren. SD-WAN Standard Edition unterstützt diese Funktionen nicht.

Es gibt zwei Schritte auf oberster Ebene zum Konfigurieren der Abschnittssätze und Parameter für die **Optimierung**. Diese sind wie folgt, in der Reihenfolge der Abhängigkeit aufgeführt:

1. Aktivieren Sie die WAN-Optimierung und passen Sie die **Standardkonfiguration** an, oder übernehmen Sie die Standardeinstellungen.

Die **Standardkonfiguration** wird als **Basisoptimierungskonfiguration** für alle Standorte verwendet, die für die WAN-Optimierung berechtigt sind. Die **Standardkonfiguration** ist vorkonfiguriert und kann angepasst werden.

Hinweis

Weitere Informationen finden Sie unter [Optimierung aktivieren und Standardeinstellungen konfigurieren](#).

2. (Optional) Passen Sie die WAN-Optimierungskonfiguration für jeden einzelnen Zweigstandort an, oder übernehmen Sie jeweils die **Standardsätze und -einstellungen**.

Standardmäßig wird die **Standardkonfiguration** zunächst auf jeden Zweigstandort angewendet, der für die WAN-Optimierung berechtigt ist. WAN-Optimierung wird nur für 1000-EE (Premium Edition) und 2000-EE (Premium Edition) Hardware-Appliances unterstützt. Für jeden unterstützten Zweigstandort können Sie eine beliebige Kombination der **Standardsätze** und -einstellungen oder einer beliebigen Teilmenge davon akzeptieren oder ändern. Anweisungen finden Sie unter [Konfigurieren der Optimierung für einen Zweigstandort](#).

Um diese Schritte abzuschließen, verwenden Sie die Konfigurationsformulare im Abschnitt **Optimierung** des **Konfigurationseditors**. Der Abschnitt "Optimierung" ist wie folgt organisiert:

- **Standardwerte** —Der Zweig **Standardwerte** enthält die folgenden untergeordneten Zweige, die wiederum ein oder mehrere Formulare zum Konfigurieren ihrer jeweiligen Sätze und Einstellungen enthalten:
 - **Standardfunktionen**
 - **Voreinstellungen für Tuning**
 - **Standardwerte Anwendungsklassifizierer (Satz)**
 - **Standard-Serviceklassen** (Set)
- **<Client Site Name>** —Der Konfigurationsbaum für den Abschnitt **Optimierung** enthält einen Zweig für jeden Clientknoten (Zweigstandort), der WAN-Optimierung unterstützt. Wenn es sich bei einem Clientknoten um ein nicht unterstütztes Appliance-Modell handelt, wird der Standort nicht in die Konfigurationsstruktur des Abschnitts **Optimierung** aufgenommen. Jeder Zweig im Baum enthält die folgenden untergeordneten Zweige, die wiederum ein oder mehrere Formulare zur Konfiguration ihrer jeweiligen Sätze und Einstellungen enthalten:

- **Standardfunktionen**
- **Voreinstellungen für Tuning**
- **Standardwerte Anwendungsklassifizierer** (festgelegt)
- **Standard-Serviceklassen** (Set)

Der folgende Abschnitt enthält Anweisungen zum Aktivieren der WAN-Optimierung für Ihr virtuelles WAN und zum Konfigurieren der **Standardsätze** und -einstellungen.

Optimierung aktivieren und Standardeinstellungen konfigurieren

May 10, 2021

Die Aktivierung der WAN-Optimierung in Ihrem virtuellen WAN erfordert die folgenden Verfahren:

1. Aktivieren Sie die WAN-Optimierung in den **Featureeinstellungen** des Abschnitts **Optimierung**.

Anweisungen für diesen Teil des Prozesses finden Sie in diesem Abschnitt.

2. Konfigurieren Sie die Richtlinieneinstellung **Beschleunigung** für jede entsprechende Serviceklasse in der Tabelle **Dienstklassen**.

Dieser Vorgang wird weiter ausgeführt, nachdem Sie den Rest der **Optimierungskonfiguration** abgeschlossen haben. Anweisungen finden Sie im Abschnitt [Konfigurieren von Standardserviceklassen für die Optimierung](#). Zu diesem Zeitpunkt wurde die WAN-Optimierung in Ihrer Konfiguration aktiviert, aber noch nicht aktiviert und in Ihrem Virtual WAN aktiviert. Um WAN-Optimierung in Ihrem Virtual WAN zu aktivieren und zu aktivieren, müssen Sie die Virtual WAN-Konfiguration abschließen und dann die Virtual WAN Appliance-Pakete auf den berechtigten Sites in Ihrer Bereitstellung generieren, bereitstellen und aktivieren, wie in den folgenden Kapiteln dieses Handbuchs beschrieben.

Gehen Sie folgendermaßen vor, um die WAN-Optimierung zu aktivieren und den Abschnitt Standardeinstellungen zu konfigurieren:

- a) Melden Sie sich bei Bedarf wieder an der Management-Weboberfläche an, und öffnen Sie den **Konfigurations-Editor**.

Gehen Sie folgendermaßen vor, um den **Konfigurations-Editor** zu öffnen:

- i. Wählen Sie oben auf der Seite die Registerkarte **Konfiguration**, um die **Konfigurations-Navigationsstruktur** (linker Bereich) zu öffnen.
- ii. Klicken Sie im Navigationsbaum links neben dem **Virtual WAN-Zweig** auf **+**, um diesen Zweig zu öffnen.

iii. Wählen Sie im Zweig **Virtual WAN** die Option **Konfigurations-Editor** aus.

b) Öffnen Sie das Konfigurationspaket, das Sie ändern möchten.

Klicken Sie auf **Öffnen**, um das Dialogfeld **Konfigurationspaket öffnen** anzuzeigen, und wählen Sie das Paket aus dem Dropdownmenü **Gespeicherte Pakete** aus.

Dadurch wird das ausgewählte Paket in den **Konfigurations-Editor** geladen und zur Bearbeitung geöffnet.

Wenn Sie über eine gültige und aktuelle Lizenz verfügen, die WAN-Optimierungsfunktionen enthält, ist der Abschnitt **Optimierung** im **Konfigurations-Editor** verfügbar.

Hinweis

Wenn der Abschnitt **Optimierung** nicht verfügbar ist, überprüfen Sie, ob Sie eine SD-WAN Premium (Enterprise) Edition-Lizenz in Ihrem Virtual WAN installiert haben. Die SD-WAN Standard Edition unterstützt keine WAN-Optimierungsfunktionen.

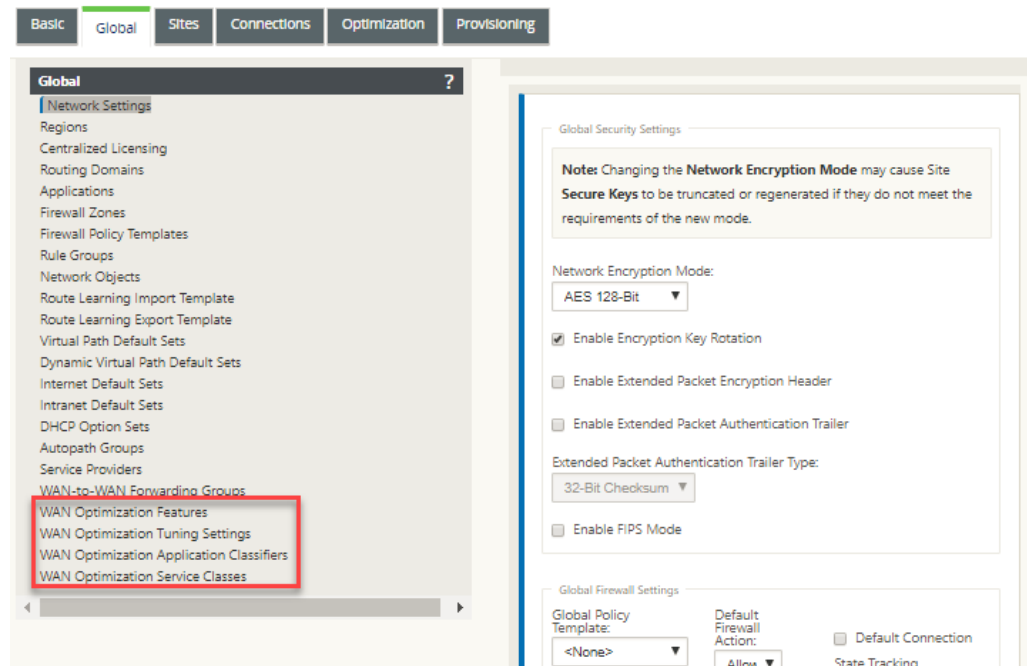
Einzelheiten und Anweisungen finden Sie in den folgenden Abschnitten:

- [Die SD-WAN-Editionen](#)
- [Lizenzierung](#)

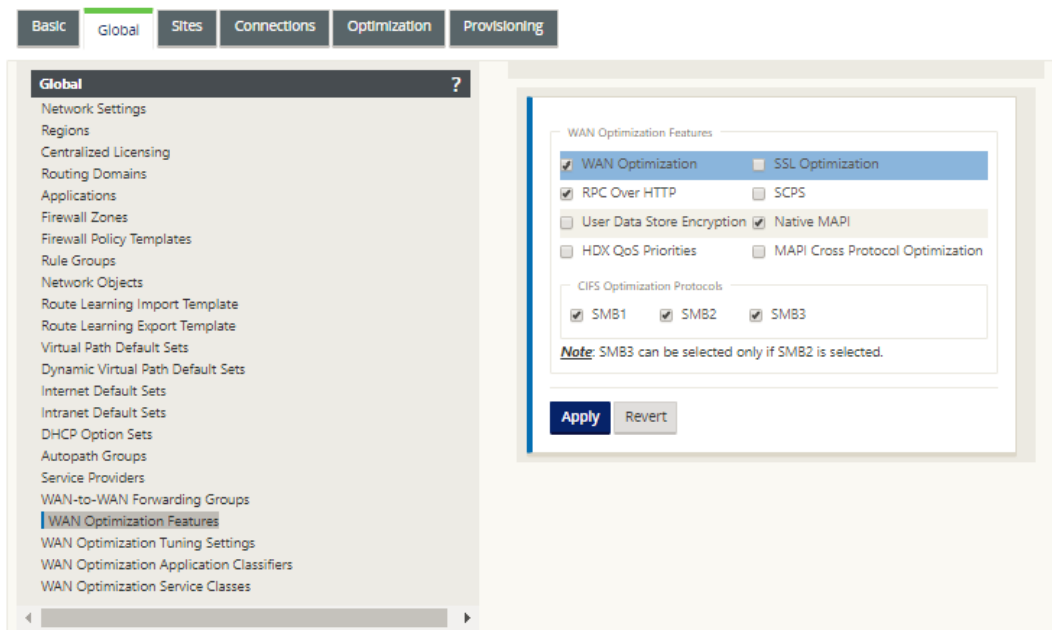
c) Klicken Sie auf die Registerkarte **Global**.

Sie können die folgenden Standardeinstellungen für die WAN-Optimierung auf der Registerkarte **Global** konfigurieren.

- WAN-Optimierungsfunktionen
- Einstellungen für die WAN-Optimierung
- Anwendungsklassifizierer für WAN-Optimierung
- WAN-Optimierungs-Service-Klasse



d) Klicken Sie auf **WAN-Optimierungsfunktionen**.



e) Aktivieren Sie das Kontrollkästchen **WAN-Optimierung**.

Das Kontrollkästchen **WAN-Optimierung** befindet sich in der oberen linken Ecke des Abschnitts ****WAN-Optimierungsfunktionen**. Dies ermöglicht das Bearbeiten des Formulars und zeigt die Schaltflächen ****Übernehmen** und **Zurücksetzen** an.

Hinweis

Dadurch wird diese Funktion nur zur Aktivierung ausgewählt. Die WAN-Optimierung wird im Abschnitt **Optimierung** oder im Konfigurationspaket erst aktiviert, wenn Sie auf **Anwenden** klicken, nachdem Sie die **Features-Konfiguration** abgeschlossen haben. Darüber hinaus müssen Sie auch die **Beschleunigungseinstellung** für jede entsprechende Serviceklasse in der Tabelle Service-Klassen konfigurieren, wie im **Optimierungskonfigurationsprozess** weiter beschrieben. (Anweisungen finden Sie im Abschnitt [Konfigurieren von Standardserviceklassen für die Optimierung](#)) Schließlich wird die WAN-Optimierung in Ihrem Virtual WAN erst aktiviert und aktiviert, wenn Sie die gesamte virtuelle WAN-Konfiguration abgeschlossen haben, und dann die Virtual WAN Appliance-Pakete auf den berechtigten Sites in Ihrem virtuellen WAN generiert, bereitgestellt, verteilt und aktiviert haben.

f) Konfigurieren Sie die **Feature-Einstellungen**.

Aktivieren Sie ein Kontrollkästchen, um eine Option auszuwählen oder zu deaktivieren. Sie können die im Formular vorausgewählten Standardeinstellungen akzeptieren oder die Einstellungen anpassen.

Hinweis

Standardmäßig werden die Einstellungen, die Sie auf der Registerkarte **Global** konfigurieren, automatisch auf jeden Zweigstandort angewendet, der in der Struktur enthalten ist. Sie können jedoch die **Optimierungskonfiguration** für einen bestimmten Zweig anpassen, wie im Abschnitt beschrieben [Konfigurieren der Optimierung für einen Zweigstandort](#).

Das Konfigurationsformular **Features** enthält zwei Abschnitte:

- **WAN-Optimierungsfunktionen**
- **CIFS-Optimierungsprotokolle**

Die Einstellungen für **WAN-Optimierungsfunktionen** lauten wie folgt:

- **WAN-Optimierung** —Aktivieren Sie das Kontrollkästchen, um die WAN-Optimierung für diese Konfiguration zu aktivieren. Dies ermöglicht auch Komprimierung, Deduplizierung und TCP-Protokolloptimierung.

Hinweis

Die Option WAN-Optimierung muss aktiviert sein, damit die anderen Optionen für den Abschnitt Optimierung verfügbar sind.

- **SCPS** —Aktivieren Sie das Kontrollkästchen, um die TCP-Protokolloptimierung für Satelliten-Links zu aktivieren.

- **HDX QoS-Prioritäten** —Aktivieren Sie das Kontrollkästchen, um die Optimierung des ICA-Datenverkehrs basierend auf der Priorisierung von HDX-Subkanälen zu ermöglichen.
- **MAPI Cross Protocol Optimization** —Aktivieren Sie das Kontrollkästchen, um die protokollübergreifende Optimierung des Microsoft Outlook (MAPI) -Verkehrs zu aktivieren.
- **SSL-Optimierung** —Aktivieren Sie das Kontrollkästchen, um die Optimierung für Traffic-Streams mit SSL-Verschlüsselung zu aktivieren.
- **RPC über HTTP** — Aktivieren Sie das Kontrollkästchen, um die Optimierung des Microsoft Exchange-Datenverkehrs zu aktivieren, der RPC über HTTP verwendet.
- **User Data Store Encryption** — Aktivieren Sie das Kontrollkästchen, um eine verbesserte Sicherheit der Daten durch die Verschlüsselung des WAN Optimization-Komprimierungsverlaufs zu ermöglichen.
- **Native MAPI** —Aktivieren Sie das Kontrollkästchen, um die Optimierung des Microsoft Exchange-Datenverkehrs zu aktivieren.

Die Optionen für **CIFS-Optimierungsprotokolle** lauten wie folgt:

- **SMB1** —Aktivieren Sie das Kontrollkästchen, um die Optimierung der Windows-Dateifreigabe zu aktivieren (SMB1)
- **SMB2** —Aktivieren Sie das Kontrollkästchen, um die Optimierung der Windows-Dateifreigabe zu aktivieren (SMB2)
- **SMB3** —Aktivieren Sie das Kontrollkästchen, um die Optimierung der Windows-Dateifreigabe (SMB3) zu aktivieren. Sie müssen zuerst die Option **SMB2** auswählen, bevor Sie **SMB3** auswählen können.

- g) Klicken Sie auf **Übernehmen**, um die ausgewählten **Standardfunktionen** zu aktivieren und dem Konfigurationspaket hinzuzufügen.

Der nächste Schritt besteht darin, die **Standardeinstellungen für die Optimierung** zu konfigurieren.

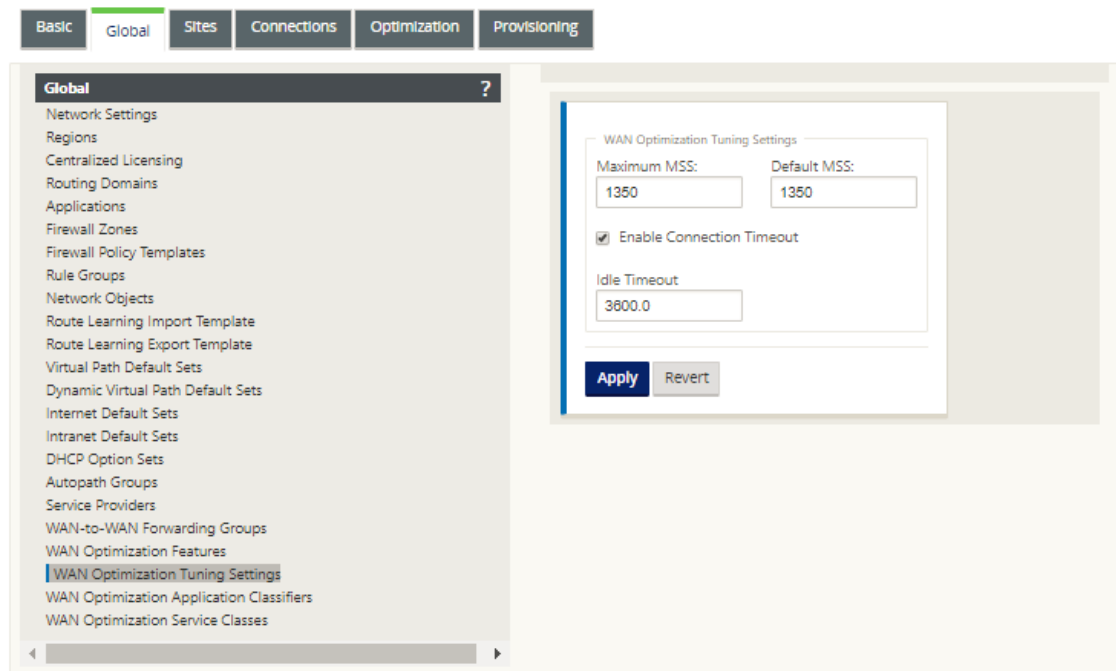
Konfigurieren der Standardoptimierungseinstellungen für die Optimierung

May 10, 2021

Sie können die Standardeinstellungen für die WAN-Optimierung auf der Registerkarte **Global** konfigurieren.

Gehen Sie folgendermaßen vor, um die **Standardeinstellungen** für die WAN-Optimierung zu konfigurieren:

1. Klicken Sie auf der Registerkarte **Global** auf **WAN-Optimierungseinstellungen**.



2. Wählen Sie die **Tuning-Einstellungen** aus und konfigurieren Sie sie.

Die Optionen **für die Tuning-Einstellungen** sind wie folgt:

- **Maximaler MSS** —Geben Sie die maximale Größe (in Byte) für die maximale Segmentgröße (MSS) für ein TCP-Segment ein.
- **Standard-MSS** —Geben Sie die Standardgröße (in Oktetten) für die MSS für TCP-Segmente ein.
- **Verbindungszeitüberschreitung aktivieren** —Wählen Sie diese Option, um die automatische Beendigung einer Verbindung zu aktivieren, wenn der Leerlaufschwellenwert überschritten wird.
- **Leerlaufzeitüberschreitung** —Geben Sie einen Schwellenwert (in Sekunden) ein, um anzugeben, wie viel Leerlaufzeit vor dem Beenden einer Leerlaufverbindung zulässig ist. Sie müssen zuerst **Verbindungszeitüberschreitung aktivieren** auswählen, bevor dieses Feld konfiguriert werden kann.

3. Klicken Sie auf **Übernehmen**.

Dadurch werden die geänderten **Tuning-Einstellungen** auf die globale Konfiguration angewendet.

Der nächste Schritt besteht darin, den Standardsatz von WAN Optimization Application Classifiers zu konfigurieren.

Konfigurieren von Standardanwendungsklassifizierern für die Optimierung

May 10, 2021

Sie können die Standard-Anwendungsklassifizierer-Einstellungen für die WAN-Optimierung auf der Registerkarte **Global** konfigurieren.

Gehen Sie folgendermaßen vor, um den Standardsatz von WAN Optimization Application Classifiers zu konfigurieren:

1. Klicken Sie auf der Registerkarte **Global** auf **WAN Optimization Application Classifiers**.

Dadurch wird die Tabelle **Anwendungsklassifizierer** geöffnet, in der der Standardsatz von Anwendungsklassifizierern angezeigt wird.

BasicGlobalSitesConnectionsOptimizationProvisioning

Global?

Network SettingsRegionsCentralized LicensingRouting DomainsApplicationsFirewall ZonesFirewall Policy TemplatesRule GroupsNetwork ObjectsRoute Learning Import TemplateRoute Learning Export TemplateVirtual Path Default SetsDynamic Virtual Path Default SetsInternet Default SetsIntranet Default SetsDHCP Option SetsAutopath GroupsService ProvidersWAN-to-WAN Forwarding GroupsWAN Optimization FeaturesWAN Optimization Tuning SettingsWAN Optimization Application ClassifiersWAN Optimization Service Classes

NameApplication GroupClassification ParametersEditDelete

ACTNETlegacy or non-ipTCP Port: 5411

AFSfile serverTCP Port: 1483, 7004

ALCHost accessTCP Port: 47806

ALHTTPTCP Port: 8008

AOL IM FilemessagingTCP Port: 2516-2518

ASP.NET Session StatesessionTCP Port: 42424

AURProuting protocolsTCP Port: 387

America OnLine (TCP)messagingTCP Port: 5191-5193

AppleTalklegacy or non-ipTCP Port: 548

AppleTalk Filing Protocollegacy or non-ipTCP Port: 2794

Arielcontent deliveryTCP Port: 419, 422

Avamarbackup and replicationTCP Port: 27000

Diese Tabelle ist auch ein Konfigurationsformular. Mit diesem Formular können Sie Anwendungsklassifizierer konfigurieren (bearbeiten), löschen und hinzufügen, um einen

benutzerdefinierten Standardsatz zu erstellen. Der geänderte Standardsatz für **Anwendungsklassifizierer** und die von Ihnen konfigurierten individuellen Anwendungsklassifizierer-Einstellungen werden automatisch als Standardwerte auf alle Zweigstandorts angewendet, die in der Abschnittsstruktur **Optimierung** enthalten sind.

Hinweis

Sie können auch den **Anwendungsklassifizierersatz** und die Einstellungen für jeden bestimmten Zweigstandort anpassen. Anweisungen finden Sie im Abschnitt [Konfigurieren der Optimierung für einen Zweigstandort](#).

- Um einen vorhandenen Anwendungsklassifikator zu konfigurieren, klicken Sie in der Spalte Bearbeiten des Klassifikationseintrags auf **Bearbeiten** (Bleistiftsymbol).

Dadurch wird ein Popup-Formular **Einstellungen bearbeiten** geöffnet, um den ausgewählten Anwendungsklassifikator zu konfigurieren.

- Geben Sie im Feld **Port** die Portnummer für den Anwendungsklassifikator ein, oder übernehmen Sie die Standardeinstellung.
- Hinzufügen oder Entfernen von Anwendungsgruppen in der Liste **Konfiguriert**, oder übernehmen Sie die Standardeinstellungen.
 - **So fügen Sie der Liste eine Anwendungsgruppe hinzu:** Wählen Sie sie in der Liste **Anwendungsgruppen** auf der linken Seite aus, und klicken Sie dann auf den Pfeil nach rechts hinzufügen (>), um die Gruppe der Liste **Konfiguriert** auf der rechten Seite hinzuzufügen.

Um alle **Anwendungsgruppen** gleichzeitig zur Liste hinzuzufügen, klicken Sie auf den doppelten Pfeil nach rechts hinzufügen (»).

- **So entfernen Sie eine Anwendungsgruppe aus der Liste:** Wählen Sie sie in der Liste **Konfiguriert** auf der rechten Seite aus, und klicken Sie dann auf den Pfeil nach links entfernen (<). Um alle **Anwendungsgruppen** gleichzeitig aus der Liste zu entfernen, klicken Sie auf den doppelten Pfeil nach links entfernen («).

5. Klicken Sie auf **Übernehmen**.

Dadurch werden Ihre Änderungen auf den Anwendungsklassifikator angewendet und das Formular **Konfiguration bearbeiten** wird ausgewiesen.

6. (Optional) Passen Sie den Standardsatz für **Anwendungsklassifikatoren** an.

Sie können Anwendungsklassifizierer hinzufügen oder löschen, um den Standardsatz wie folgt anzupassen:

- **So entfernen Sie einen Anwendungsklassifikator aus dem Set:**

Klicken Sie auf das Papierkorbsymbol in der Spalte **Löschen** eines **Application Classifier -Eintrags**, um diesen Eintrag aus der Tabelle zu entfernen.

- **So fügen Sie dem Set einen Anwendungsklassifikator hinzu:**

- a) Klicken Sie rechts neben dem **Verzweigungslabel Application Classifier** auf +.

Daraufhin wird das Formular Konfiguration **hinzufügen** angezeigt.

- b) Geben Sie den Namen und die Portnummer für den Anwendungsklassifikator in die Felder **Name** bzw. **Port** ein.

- c) Hinzufügen oder Entfernen von Anwendungsgruppen in der Liste **Konfiguriert**.

So fügen Sie der Liste eine Anwendungsgruppe hinzu: Wählen Sie sie in der Liste **Anwendungsgruppen** auf der linken Seite aus, und klicken Sie dann auf den Pfeil nach rechts hinzufügen (>), um die Gruppe der Liste **Konfiguriert** auf der rechten Seite hinzuzufügen. Um alle **Anwendungsgruppen** gleichzeitig zur Liste hinzuzufügen, klicken Sie auf den doppelten Pfeil nach rechts hinzufügen (»).

So entfernen Sie eine Anwendungsgruppe aus der Liste: Wählen Sie sie in der Liste **Konfiguriert** auf der rechten Seite aus, und klicken Sie dann auf den Pfeil nach links entfernen (<). Um alle **Anwendungsgruppen** gleichzeitig aus der Liste zu entfernen, klicken Sie auf den doppelten Pfeil nach links entfernen («).

- d) Klicken Sie auf **Übernehmen**.

Dadurch wird der neue Anwendungsklassifizierer zum Set hinzugefügt und das Formular Konfiguration **hinzufügen** wird ausgewiesen.

Der nächste Schritt besteht darin, den Standardsatz der WAN-Optimierungsdienstklassen zu konfigurieren.

Konfigurieren von Standardserviceklassen für die Optimierung

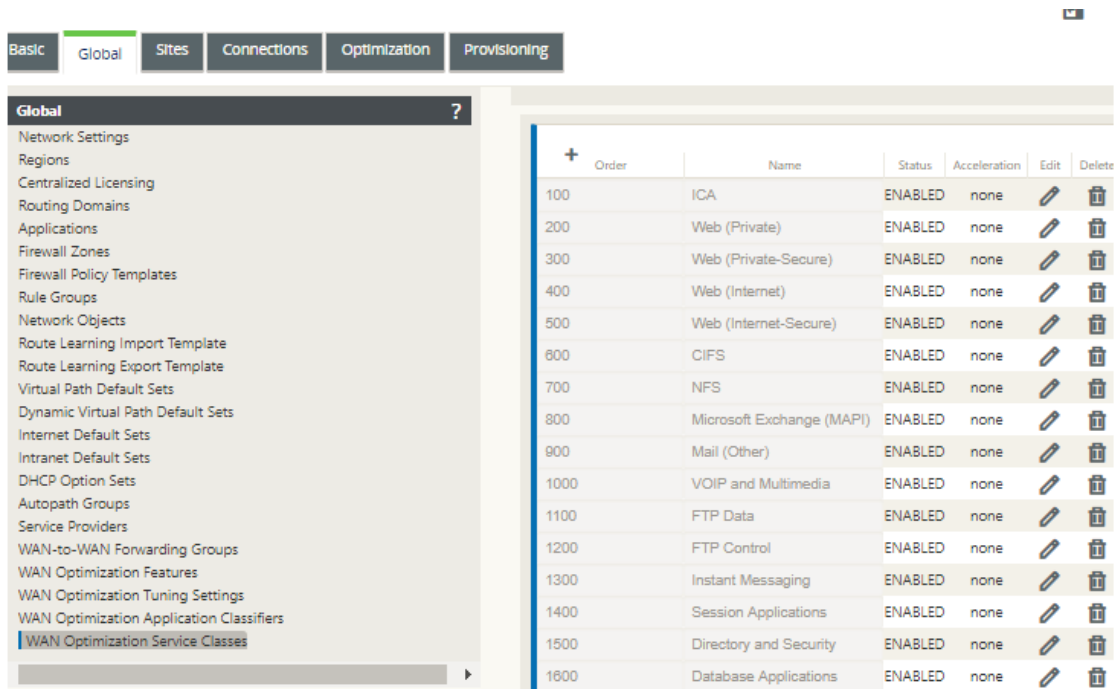
May 10, 2021

Sie können die Standardeinstellungen für die WAN-Optimierung auf der Registerkarte **Global** konfigurieren.

Gehen Sie folgendermaßen vor, um den Standardsatz von WAN-Optimierungsdienstklassen zu konfigurieren:

1. Klicken Sie auf der Registerkarte **Global** auf **WAN-Optimierungsdienstklassen**.

Dadurch wird die Tabelle **Service Classes** geöffnet, in der die Standardgruppe Service Classes angezeigt wird.



The screenshot shows the Citrix SD-WAN configuration interface. The 'Global' tab is selected, and the 'WAN Optimization Service Classes' section is expanded in the left sidebar. The main area displays a table of service classes.

| Order | Name | Status | Acceleration | Edit | Delete |
|-------|---------------------------|---------|--------------|------|--------|
| 100 | ICA | ENABLED | none | | |
| 200 | Web (Private) | ENABLED | none | | |
| 300 | Web (Private-Secure) | ENABLED | none | | |
| 400 | Web (Internet) | ENABLED | none | | |
| 500 | Web (Internet-Secure) | ENABLED | none | | |
| 600 | CIFS | ENABLED | none | | |
| 700 | NFS | ENABLED | none | | |
| 800 | Microsoft Exchange (MAPI) | ENABLED | none | | |
| 900 | Mail (Other) | ENABLED | none | | |
| 1000 | VOIP and Multimedia | ENABLED | none | | |
| 1100 | FTP Data | ENABLED | none | | |
| 1200 | FTP Control | ENABLED | none | | |
| 1300 | Instant Messaging | ENABLED | none | | |
| 1400 | Session Applications | ENABLED | none | | |
| 1500 | Directory and Security | ENABLED | none | | |
| 1600 | Database Applications | ENABLED | none | | |

Diese Tabelle ist auch ein Konfigurationsformular. Mit diesem Formular können Sie Service-Klassen konfigurieren (bearbeiten), löschen und hinzufügen, um einen benutzerdefinierten Standardsatz zu erstellen. Der geänderte standardmäßige **Service Classes** Set und die individuellen Einstellungen der Service Class, die Sie konfigurieren, werden automatisch als Standardwerte auf jeden Zweigstandort angewendet, der in der Abschnittsstruktur **Optimierung** enthalten ist.

Hinweis

Sie können auch den **Service Classes** Set und die Einstellungen für jeden bestimmten Zweigstandort anpassen. Anweisungen zum Anpassen der **Optimierungskonfiguration** für einen Zweigstandort finden Sie im Abschnitt [Konfigurieren der Optimierung für einen Zweigstandort](#).

- Um eine vorhandene Serviceklasse zu konfigurieren, klicken Sie in der Spalte Bearbeiten dieses Klasseneintrags in der Tabelle Dienstklassen auf **Bearbeiten** (Bleistiftsymbol).

Dadurch wird ein Popup-Formular **Einstellungen bearbeiten** geöffnet, um die ausgewählte Serviceklasse zu konfigurieren.

Edit

Name: Order: ☒ Enabled

Acceleration Policy:

☒ Enable AppFlow Reporting ☐ Exclude from SSL Tunnel

Filter Rules +

| Application | Source IP Address | Destination IP Address | Direction | Edit | Delete |
|-------------|-------------------|------------------------|---------------|------|--------|
| ICA,ICA CGP | | | BIDIRECTIONAL | | |

- Konfigurieren Sie die Grundeinstellungen für die Serviceklasse.

Die Grundeinstellungen sind wie folgt:

- **Aktiviert** —Wählen Sie diese Option, um die neue Service-Klasse zu aktivieren. Die Klasse ist standardmäßig aktiviert.
- **Beschleunigungsrichtlinie** —Wählen Sie eine Richtlinie aus dem Dropdownmenü **Beschleunigungsrichtlinie** aus. Es gibt folgende Optionen:
 - **disk** —Wählen Sie diese Richtlinie aus, um den Appliance-Datenträger als Speicherort für die Speicherung des Datenverkehrs anzugeben, der für die Komprimierung verwendet wird. Dadurch wird die DBC-Richtlinie (Disk Based Compression) für diese Serviceklasse aktiviert. Im Allgemeinen ist eine **Datenträgerrichtlinie** in der Regel die beste Wahl, da die Appliance automatisch den **Datenträger** oder **Speicher** als Speicherort auswählt, je nachdem, welcher für den Datenverkehr besser geeignet ist.

- **none** —Wählen Sie diese Option aus, wenn Sie keine Beschleunigungsrichtlinie für diese Serviceklasse aktivieren möchten. Eine Richtlinie von **keiner** wird in der Regel nur für nicht komprimierbaren verschlüsselten Datenverkehr und Echtzeitvideos verwendet.
- **Nur Flusssteuerung** —Wählen Sie diese Richtlinie aus, um die Komprimierung zu deaktivieren, aber die Beschleunigung der Flusssteuerung zu aktivieren. Wählen Sie diese Option für immer verschlüsselte Dienste und für den FTP-Steuerkanal aus.
- **Speicher** —Wählen Sie diese Richtlinie aus, um Speicher als Speicherort für die Speicherung des Datenverkehrs anzugeben, der für die Komprimierung verwendet wird.
- **AppFlow Reporting aktivieren** —Wählen Sie diese Option aus, um AppFlow Reporting für diese Service Class zu aktivieren. AppFlow ist ein Industriestandard für die Entsperrung von Anwendungstransaktionsdaten, die von der Netzwerkinfrastruktur verarbeitet werden. Die WAN Optimization AppFlow-Schnittstelle funktioniert mit jedem AppFlow-Kollektor, um Berichte zu generieren. Der Kollektor erhält detaillierte Informationen von der Appliance unter Verwendung des offenen AppFlow Standards (<http://www.appflow.org>).

Weitere Informationen zu AppFlow finden Sie in der Citrix CloudBridge 7.4-Produktdokumentation, die im Citrix Dokumentationsportal <http://docs.citrix.com/> verfügbar ist.

Hinweis

Um WAN Optimization AppFlow-Berichte anzuzeigen, wählen Sie die Registerkarte **Überwachung**, und öffnen Sie dann im Navigationsbaum (linken Bereich) den Zweig **WAN-Optimierung**, und wählen Sie **AppFlow** aus. Weitere Informationen unter [Virtuelles WAN überwachen](#).

- **Aus dem SSL-Tunnel ausschließen** —Wählen Sie diese Option aus, um den mit der Service-Klasse verknüpften Datenverkehr vom SSL-Tunneling auszuschließen.

4. Konfigurieren Sie die **Filterregeln** für die Dienstklasse.

Gehen Sie folgendermaßen vor, um eine vorhandene Regel zu bearbeiten:

- a) Klicken Sie in der Tabelle Filterregeln (unten im Formular) in der Spalte Bearbeiten der Regel, die Sie bearbeiten möchten, auf Bearbeiten (Bleistiftsymbol).

Dadurch werden die Filterregeln für die ausgewählte Filterregel angezeigt.

Edit

Name: ☒ Enabled

Acceleration Policy:

☒ Enable AppFlow Reporting ☐ Exclude from SSL Tunnel

Filter Rules +

Direction:

Applications:

Available: ACTNET, AFS, ALC, ALTHTP, AOL IM File

Configured: ICA, ICA CGP

Source IP Address: +

Destination IP Address: +

Apply Cancel

b) Wählen Sie im Dropdownmenü Richtung die Filterrichtung aus.

Wählen Sie eine der folgenden Optionen:

- **BIDIRECTIONAL**
- **UNIDIRECTIONAL**

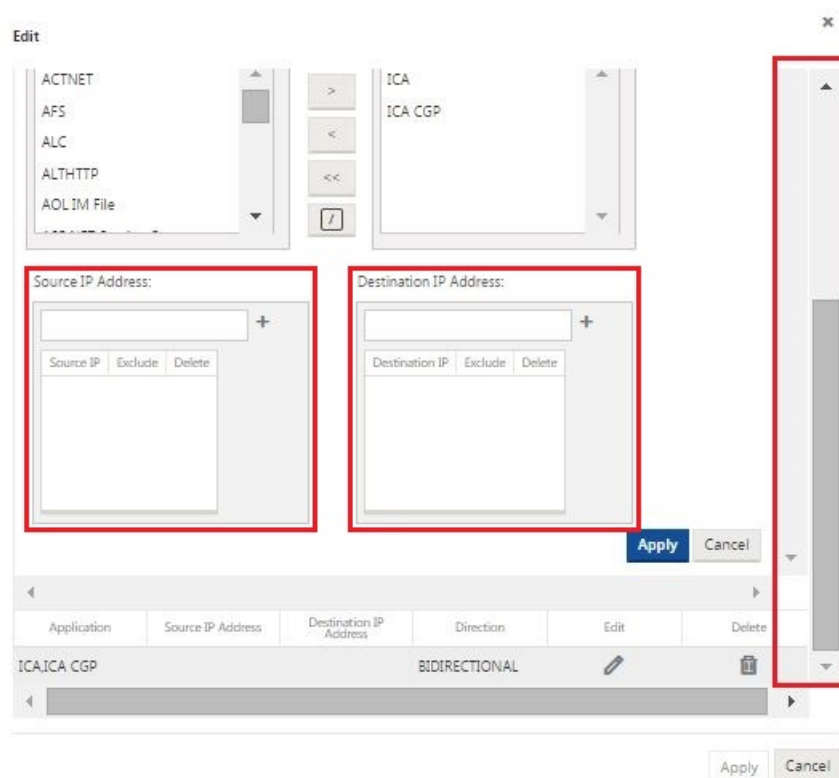
c) Hinzufügen oder Entfernen von Anwendungen in der Liste **Konfiguriert**.

So fügen Sie der Liste eine Anwendung hinzu: Wählen Sie sie in der Liste **Anwendungen** auf der linken Seite aus, und klicken Sie dann auf den Pfeil nach rechts hinzufügen (>), um die Gruppe der Liste **Konfiguriert** auf der rechten Seite hinzuzufügen. Um alle **Anwendungen** gleichzeitig zur Liste hinzuzufügen, klicken Sie auf den doppelten Pfeil nach rechts hinzufügen (>>).

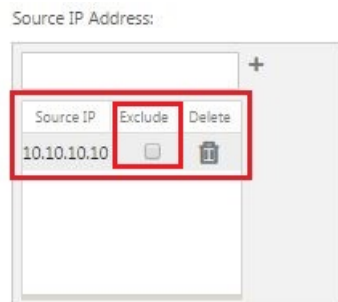
So entfernen Sie eine Anwendung aus der Liste: Wählen Sie sie in der Liste Konfiguriert auf der rechten Seite aus, und klicken Sie dann auf den Pfeil nach links entfernen (<). Um alle **Anwendungen** gleichzeitig aus der Liste zu entfernen, klicken Sie auf den doppelten Pfeil nach links entfernen (<<).

d) Scrollen Sie nach unten, um den abgeschnittenen Teil des Formulars anzuzeigen.

Der Abschnitt **Filterregeln** Einstellungen ist etwas lang, daher müssen Sie die Bildlaufleiten verwenden, um den abgeschnittenen Teil des Formulars anzuzeigen.

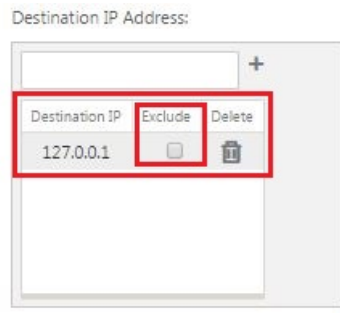


- e) Geben Sie die Quell-IP-Adresse in das Feld **Quell-IP-Adresse** ein.
- f) Klicken Sie rechts neben der soeben eingegebenen Quell-IP-Adresse auf **+**.
Dadurch wird die angegebene IP-Adresse zur Tabelle **Quell-IP-Adresse** hinzugefügt.



- g) Geben Sie an, ob die Quell-IP-Adresse für diese Filterregel eingeschlossen oder ausgeschlossen werden soll.
Aktivieren Sie das Kontrollkästchen **Ausschließen**, um die angegebene Quell-IP-Adresse von dieser Filterregel auszuschließen. Deaktivieren Sie das Kontrollkästchen, um die Adresse aufzunehmen.
- h) Geben Sie die Ziel-IP-Adresse in das Feld **Ziel-IP-Adresse** ein.
- i) Klicken Sie rechts neben der soeben eingegebenen Ziel-IP-Adresse auf **+**.

Dadurch wird die angegebene IP-Adresse zur Tabelle **Quell-IP-Adresse** hinzugefügt.



- j) Geben Sie an, ob die Ziel-IP-Adresse für diese Filterregel eingeschlossen oder ausgeschlossen werden soll.

Aktivieren Sie das Kontrollkästchen **Ausschließen**, um die angegebene Ziel-IP-Adresse von dieser Filterregel auszuschließen. Deaktivieren Sie das Kontrollkästchen, um die Adresse aufzunehmen.

- k) Klicken Sie auf **Übernehmen**.

Dadurch werden Ihre Änderungen auf die Regel angewendet und der Abschnitt **Filterregeln** Einstellungen ausgeblendet.

5. (Optional) Passen Sie die **Standard-Service-Classes** an .

Sie können Service-Klassen hinzufügen oder löschen, um den Standardsatz wie folgt anzupassen:

- **So entfernen Sie eine Service-Klasse aus dem Set:**

Klicken Sie auf das Papierkorbsymbol in der Spalte **Löschen** eines Service-Class-Eintrags in der Tabelle, um diesen Eintrag zu entfernen.

- **So fügen Sie dem Set eine Service-Klasse hinzu:**

- a) Klicken Sie rechts neben der **Service-Class-Verzweigungsbezeichnung** auf + .

Daraufhin wird das Formular Konfiguration **hinzufügen** angezeigt.

- b) Geben Sie den Namen für die neue Serviceklasse in das Feld **Name** ein.

- c) Konfigurieren Sie die neue Service-Klasse.

Die Schritte zum Konfigurieren einer neuen Serviceklasse sind dieselben wie beim Ändern einer vorhandenen Serviceklasse. Anweisungen hierzu finden Sie in den folgenden Schritten weiter oben in diesem Abschnitt:

3. Konfigurieren Sie die Grundeinstellungen für die Serviceklasse.

4. Konfigurieren Sie die Filterregeln für die Dienstklasse.

d) Klicken Sie auf **Hinzufügen**, um die neue Service-Klasse zum Standardsatz hinzuzufügen und das Formular Konfiguration **hinzufügen** zu schließen.

6. (Optional, empfohlen) **Speichern** Sie das Konfigurationspaket.

Sie haben nun die globale WAN-Optimierungskonfiguration abgeschlossen und können mit der Konfiguration der **Optimierungssätze** und -einstellungen für die Zweigstandorte beginnen.

Konfigurieren der Optimierung für einen Zweigstandort

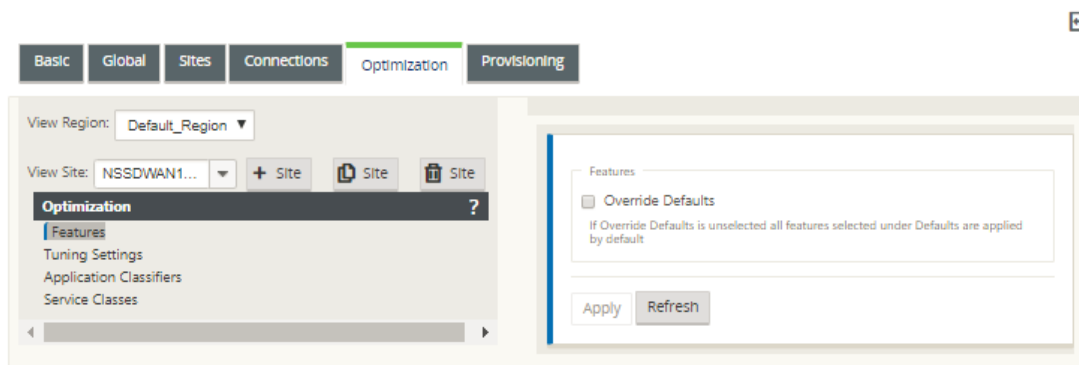
May 10, 2021

Nachdem Sie die globale Standardkonfiguration abgeschlossen haben, haben Sie die Möglichkeit, die Sätze und Einstellungen für die einzelnen Zweigstandorte anzupassen.

Die soeben konfigurierten globalen Einstellungen werden automatisch auf jeden Zweigstandort angewendet, der im Abschnitt **Optimierung** enthalten ist. Sie können die Standardeinstellungen akzeptieren oder die Konfiguration für einen bestimmten Zweig anpassen. Die Verfahren zum Konfigurieren der **Optimierungssätze** und -einstellungen für einen Zweigstandort sind dieselben wie beim Konfigurieren der globalen Standardwerte, mit einigen kleinen Unterschieden.

Gehen Sie wie folgt vor, um die **Optimierungskonfiguration** für einen Zweigstandort anzupassen:

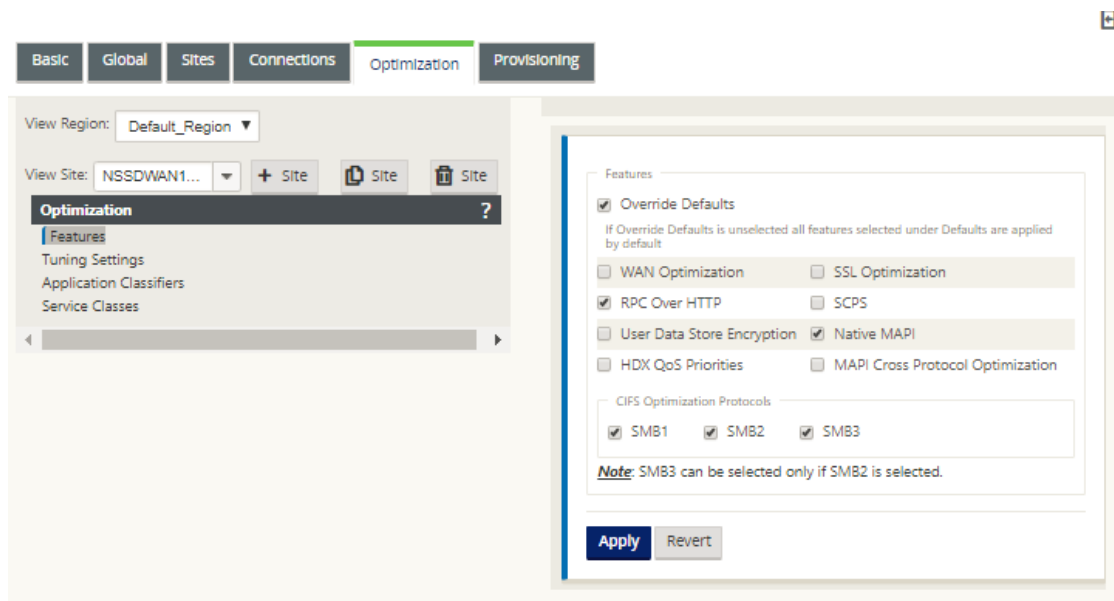
1. Klicken Sie auf die Registerkarte **Optimierung**, wählen Sie im Feld Site anzeigen eine Site aus.



2. Aktivieren Sie das Kontrollkästchen **Standardwerte überschreiben**.

Dadurch wird das Konfigurationsformular der obersten Ebene für diese Konfigurationskategorie angezeigt und zur Bearbeitung geöffnet.

Das folgende Bild zeigt ein Beispiel für die Konfiguration der obersten Ebene, in diesem Fall für den Satz **Features**.



3. Geben Sie Ihre Konfigurationsänderungen ein.

Ab diesem Zeitpunkt ist der Konfigurationsprozess für jede **Zweigstandortoptimierung** der gleiche wie für die entsprechende globale Abschnittskategorie. Anweisungen zum Konfigurieren einer bestimmten Kategorie von Sätzen oder Einstellungen finden Sie im folgenden Abschnitt:

- [Aktivieren der Optimierung und Konfigurieren der Einstellungen für Standardfunktionen.](#)
- [Konfigurieren der Standardoptimierungseinstellungen für die Optimierung.](#)
- [Konfigurieren von Standardanwendungsklassifizierern für die Optimierung.](#)
- [Konfigurieren von Standardserviceklassen für die Optimierung.](#)

4. (Optional, empfohlen) **Speichern** Sie das Konfigurationspaket.

Sie haben nun die Konfiguration der **Abschnittssätze** und -einstellungen für Ihr virtuelles WAN abgeschlossen.

SSL-Profil konfigurieren

May 10, 2021

Alle SSL-bezogenen Konfigurationen sind über den neuen Konfigurationseditor der Appliance verfügbar, um Sicherheit und Benutzerfreundlichkeit zu gewährleisten. Auf der SD-WAN Premium (Enterprise) Edition und Zwei-Box-Bereitstellungen werden Serviceklassen über den Konfigurationseditor konfiguriert, sodass Sie keine SSL-Profile anhängen können. Um dem Ausdruck der

SSL-Profilzuordnung zu einer Dienstklasse gerecht zu werden, wird der Workflow für SSL-Profile so geändert, dass Service-Klassen im Profilknoten angehängt werden können.

Eine der Einschränkungen besteht darin, dass das SSL-Profil an alle Regeln in einer Serviceklasse angehängt wird. Wenn Sie das SSL-Profil selektiv an eine bestimmte Regel anhängen müssen, wird die Konfiguration der Serviceklasse in detaillierte Regeln für die weitere Auswahl aufgeteilt.

Hinweis

SSL-Profilen können nur die Dienstklassen zugeordnet werden, deren Filterregeln auf unidirektional festgelegt sind.

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN web GUI. Under the 'SSL Profile' section, the 'Profile Name*' is 'Test'. The 'Profile Enabled' checkbox is checked, and 'Parse Subject Alternative Names' is unchecked. The 'Virtual Host Name' field is empty. The 'Service Classes' section is highlighted with a red box. It contains two lists: 'Available (19)' and 'Configured (3)'. The 'Available' list includes 'RPCovrHTTP', 'ICA', 'Web (Private)', and 'Web (Private-Secure)'. The 'Configured' list includes 'Iperf', 'Secure Applications', and 'Web (Internet-Secure)'. Below the lists, the 'Proxy Type' is set to 'Split'.

So erstellen Sie SSL-Profil auf der neuen Premium (Enterprise) Edition-Appliance im Rechenzentrum:

1. Wechseln Sie in der SD-WAN-Web-GUI zur Seite **Konfiguration > Sichere Beschleunigung**. Klicken Sie auf **Profil hinzufügen**. Erstellen Sie das **SSL-Profil**.

Dashboard

Monitoring

Configuration

+ Appliance Settings

+ Virtual WAN

+ WAN Optimization

Secure Acceleration

Certificate and Keys

User Data Store

+ System Maintenance

Configuration > WAN Optimization > Secure Acceleration

Secure Peering

Keystore Status
Opened

Secure Peering Status
Disabled


SSL Profile

Windows Domain

SSL Profiles

SSL acceleration allows the appliance to compress SSL traffic such as HTTPS and SSL-encrypted XenApp/XenDesktop (ICA/COP) traffic. Secure partner configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server-side NetScaler SD-WAN WO appliance (only) and SSL-specific configuration (called an SSL Profile) for each group of SSL servers. This step should be skipped on a client-side appliance.

Add Profile



Back

Create SSL Profile

☒ Manually add Profile

☐ Import Profile

Profile Name*

☒ Profile Enabled

☐ Parse Subject Alternative Names

Virtual Host Name

Service Classes

Available (21)Select All

ICA

+

Web (Private)

+

Web (Private-Secure)

+

Web (Internet)

+

Configured (0)Remove All

No items

Proxy Type

☐ Split

☒ Transparent

SSL Server's Private Key*

private_10_105_199_6

+

2. Geben **Sie auf der Seite SSL-Profil erstellen** einen Profilnamen ein, und wählen Sie **Serviceklassen** aus, die diesem Profil zugeordnet werden sollen. Wählen Sie **Proxytyp** und geben

Sie relevante Daten ein, und klicken Sie auf **Erstellen**.

Create SSL Profile

Manually add Profile

Import Profile

Profile Name*

SampleProfile

Profile Enabled

Parse Subject Alternative Names

Virtual Host Name

Service Classes

Available (20)Select All

Web (Private)+

ICA+

Web (Private-Secure)+

Web (Internet-Secure)+

Configured (1)Remove All

Web (Internet)-

Proxy Type

Split

Transparent

SSL Server's Private Key*

private_10_105_199_6

Create

Close

3. Nachdem SSL-Profil erfolgreich erstellt wurde und Service-Klasse zugeordnet ist, sehen Sie sich die SSL-Profilinformationen an, wie unten dargestellt.

| SSL Profile | | Windows Domain | |
|---------------|-------------|----------------|-----------------|
| Add | Edit | Delete | Action |
| Profile Name | Proxy Type | Profile In Use | Profile Enabled |
| SampleProfile | transparent | ✓ | ✓ |

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

864

Citrix WAN-Optimierungs-Client-Plug-In

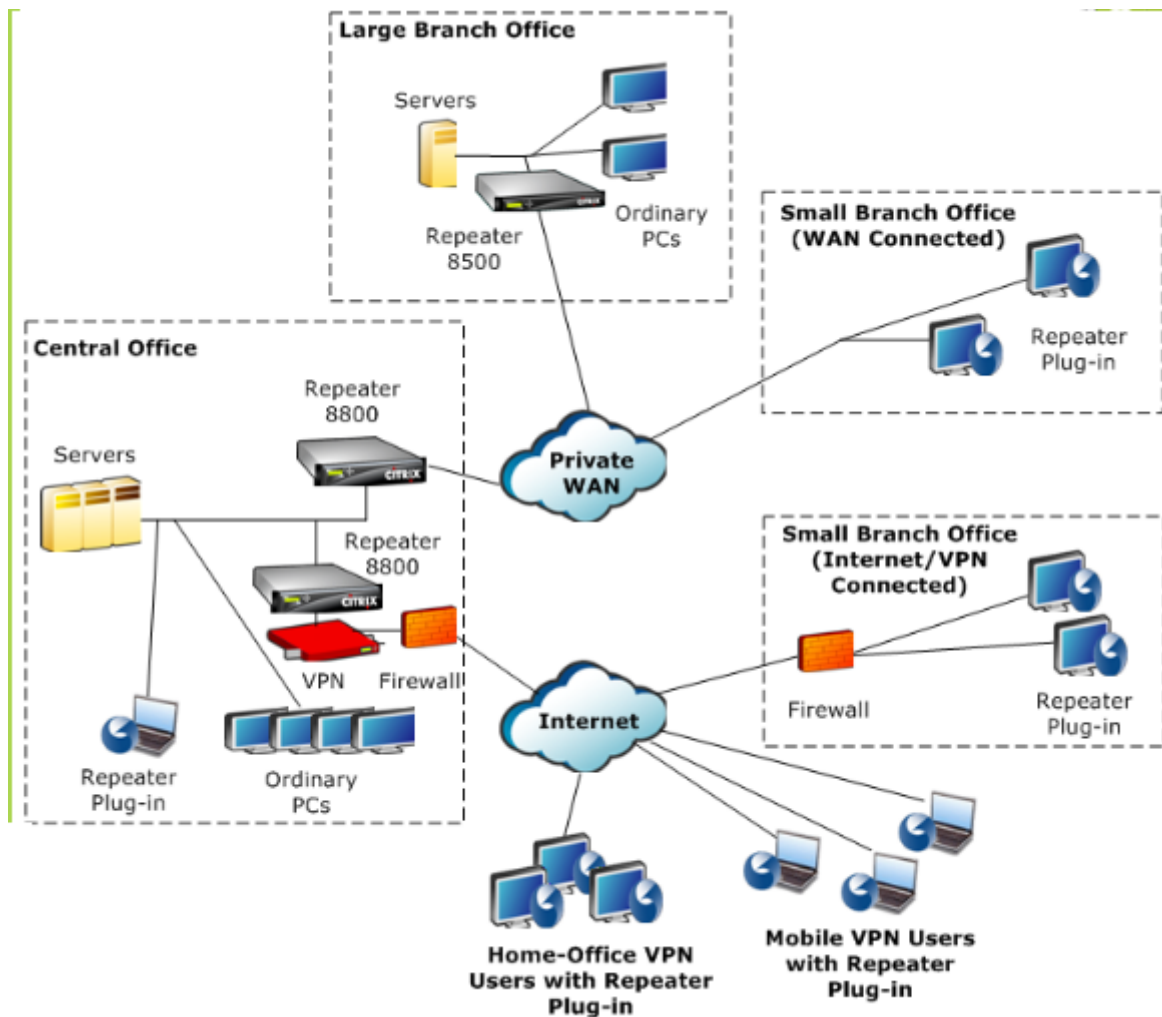
May 10, 2021

Das Citrix WANOP-Client-Plug-in ist ein softwarebasierter Netzwerkbeschleuniger, der auf Windows-Laptops und -Workstations ausgeführt wird und die Beschleunigung überall ermöglicht, nicht nur in Büros mit WANOP Client-Plug-in-Appliances. Es wird eine Verbindung mit einer Citrix WANOP Client-Plug-in-Appliance am anderen Ende der Verbindung hergestellt.

Die Prinzipien des WANOP Client-Plug-in-Betriebs sind im Allgemeinen identisch mit denen einer WANOP Client-Plug-in-Appliance. Themen, die nicht in der Plug-in-Dokumentation enthalten sind, finden Sie im größeren Dokumentationssatz.

Das Plug-In wird als Standard-Microsoft-Installationsdatei (MSI) verteilt. Die Plug-In-Bereitstellung erfordert eine Plug-in-spezifische Konfiguration der WANOP Client-Plug-in-Appliances an den anderen Enden der Links. Wenn Sie die MSI-Datei mit den DNS- oder IP-Adressen der WANOP-Client-Plug-in-Appliances und einigen anderen Parametern anpassen, müssen die Benutzer bei der Installation des Plug-ins auf ihren Windows-Computern keine Konfigurationsinformationen eingeben.

Abbildung 1. Typisches WANOP-Client-Plug-in-Netzwerk, das das WANOP-Client-Plug-in anzeigt



Hinweis

Das Plug-In wird von Citrix Receiver 1.2 oder höher unterstützt und kann von Citrix Receiver verteilt und verwaltet werden.

Hardware- und Softwareanforderungen

May 10, 2021

Auf der Client-Seite der beschleunigten Verbindung wird das WANOP Client-Plug-in auf Windows-Desktop- und Laptop-Systemen unterstützt, aber nicht auf Netbooks oder Thin Clients. Citrix empfiehlt die folgenden Hardwarespezifikationen für den Computer, auf dem das WANOP Client-Plug-In ausgeführt wird:

- Pentium 4-Klasse CPU

- 2 GB RAM
- 2 GB freier Speicherplatz

Das WANOP Client-Plug-in wird auf der Windows 10-Plattform unterstützt und benötigt folgende Systemanforderungen:

- 4 GB RAM
- 10 GB freier Speicherplatz

Das WANOP Client-Plug-in wird unter den folgenden Betriebssystemen unterstützt:

- Windows XP-Startseite
- Windows XP Professional
- Windows Vista (alle 32-Bit-Versionen von Home Basic, Home Premium, Business, Enterprise und Ultimate)
- Windows 7 (alle 32-Bit- und 64-Bit-Versionen von Home Basic, Home Premium, Professional, Enterprise und Ultimate)
- Windows 8 (32-Bit- und 64-Bit-Versionen der Premium (Enterprise) Edition)
- Windows 10 (32-Bit- und 64-Bit-Versionen der Premium (Enterprise) Edition)

Serverseitig unterstützen derzeit die folgenden Appliances WANOP Client-Plug-In-Bereitstellungen:

- Repeater 8500 Serie
- Repeater 8800 Serie
- WANOP Client Plug-in VPX
- WANOP Client-Plug-in 2000
- WANOP Client-Plug-in 3000
- WANOP Client-Plug-in 4000
- WANOP Client-Plug-in 5000

Funktionsweise des WANOP-Plug-Ins

May 10, 2021

WANOP Client Plug-in-Produkte verwenden Ihre bestehende WAN/VPN-Infrastruktur. Ein Computer, auf dem das Plug-In installiert ist, greift weiterhin wie vor der Installation des Plug-Ins auf LAN, WAN

und Internet zu. Es sind keine Änderungen an Routingtabellen, Netzwerkeinstellungen, Clientanwendungen oder Serveranwendungen erforderlich.

Citrix Access Gateway-VPNs erfordern eine geringe Menge an WANOP Client-Plug-in-spezifischen Konfigurationen.

Es gibt zwei Varianten hinsichtlich der Handhabung von Verbindungen durch das Plug-In und die Appliance: *Transparenter Modus* und *Redirector-Modus*. Redirector ist ein Legacy-Modus, der für neue Bereitstellungen nicht empfohlen wird.

- **Der transparente Modus** für die Beschleunigung von Plug-in-zu-Appliance ist der Beschleunigung von Appliance-zu-Appliance sehr ähnlich. Die WANOP Client-Plug-in-Appliance muss sich im Pfad befinden, der von den Paketen übernommen wird, wenn sie zwischen dem Plug-in und dem Server unterwegs sind. Wie bei der Appliance-zu-Appliance-Beschleunigung arbeitet der transparente Modus als transparenter Proxy, wobei die Quell- und Ziel-IP-Adresse sowie die Portnummern von einem Ende der Verbindung zum anderen beibehalten werden.
- **Der Umleitungsmodus** (nicht empfohlen) verwendet einen expliziten Proxy. Das Plug-In setzt ausgehende Pakete an die Redirector-IP-Adresse der Appliance um. Die Appliance wiederum liest die Pakete an den Server, während die Rücksendeadresse so geändert wird, dass sie auf sich selbst anstatt auf das Plug-In verweist. In diesem Modus muss die Appliance nicht physisch mit dem Pfad zwischen der WAN-Schnittstelle und dem Server verbunden sein (dies ist die ideale Bereitstellung).

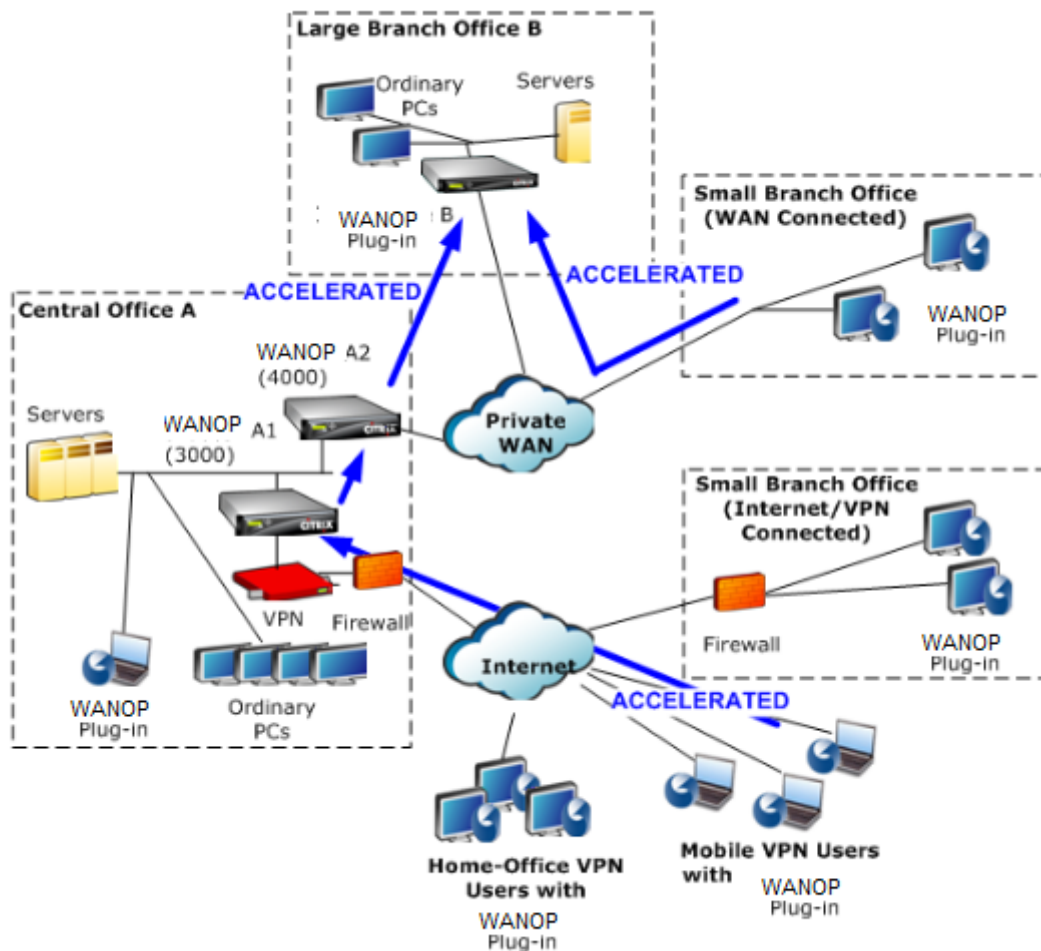
Best Practice: Verwenden Sie den transparenten Modus, wenn Sie können, und den Umleitungsmodus, wenn Sie müssen.

Transparenter Modus

Im transparenten Modus müssen die Pakete für beschleunigte Verbindungen die Ziel-Appliance passieren, genau wie bei der Beschleunigung von Appliance zu Appliance.

Das Plug-In ist mit einer Liste der Appliances konfiguriert, die für die Beschleunigung verfügbar sind. Es versucht, jede Appliance zu kontaktieren und eine Signalverbindung zu öffnen. Wenn die Signalverbindung erfolgreich ist, lädt das Plug-In die Beschleunigungsregeln von der Appliance herunter, die die Zieladressen für Verbindungen sendet, die die Appliance beschleunigen kann.

Abbildung 1. Transparenter Modus, Hervorhebung von drei Beschleunigungspfaden



Hinweis

- Verkehrsfluss: Der transparente Modus beschleunigt die Verbindungen zwischen einem WANOP Client-Plug-in und einer Plug-in-fähigen Appliance.
- Lizenzierung —Appliances benötigen eine Lizenz, um die gewünschte Anzahl von Plug-Ins zu unterstützen. Im Diagramm muss Repeater A2 nicht für die Plug-in-Beschleunigung lizenziert werden, da Repeater A1 die Plug-in-Beschleunigung für Standort A bereitstellt.
- Daisy-Chaining: Wenn die Verbindung auf dem Weg zur Ziel-Appliance mehrere Appliances durchläuft, muss für die Appliances in der Mitte Daisy-Chaining aktiviert sein, oder die Beschleunigung wird blockiert. Im Diagramm wird der Datenverkehr von Home-Office- und mobilen VPN-Benutzern, der für große Zweigstelle B bestimmt ist, durch Repeater B beschleunigt, damit dies funktioniert, müssen Repeater A1 und A2 die Verkettung aktiviert haben.

Wenn das Plug-In eine neue Verbindung öffnet, werden die Beschleunigungsregeln konsultiert. Wenn die Zieladresse einer der Regeln entspricht, versucht das Plug-In, die Verbindung zu beschleunigen,

indem Beschleunigungsoptionen an das anfängliche Paket in der Verbindung (das SYN-Paket) angefügt werden. Wenn eine dem Plug-In bekannte Appliance Beschleunigungsoptionen an das SYN-ACK-Antwortpaket anfügt, wird eine beschleunigte Verbindung mit dieser Appliance hergestellt.

Die Anwendung und der Server wissen nicht, dass die beschleunigte Verbindung hergestellt wurde. Nur die Plug-in-Software und die Appliance wissen, dass eine Beschleunigung stattfindet.

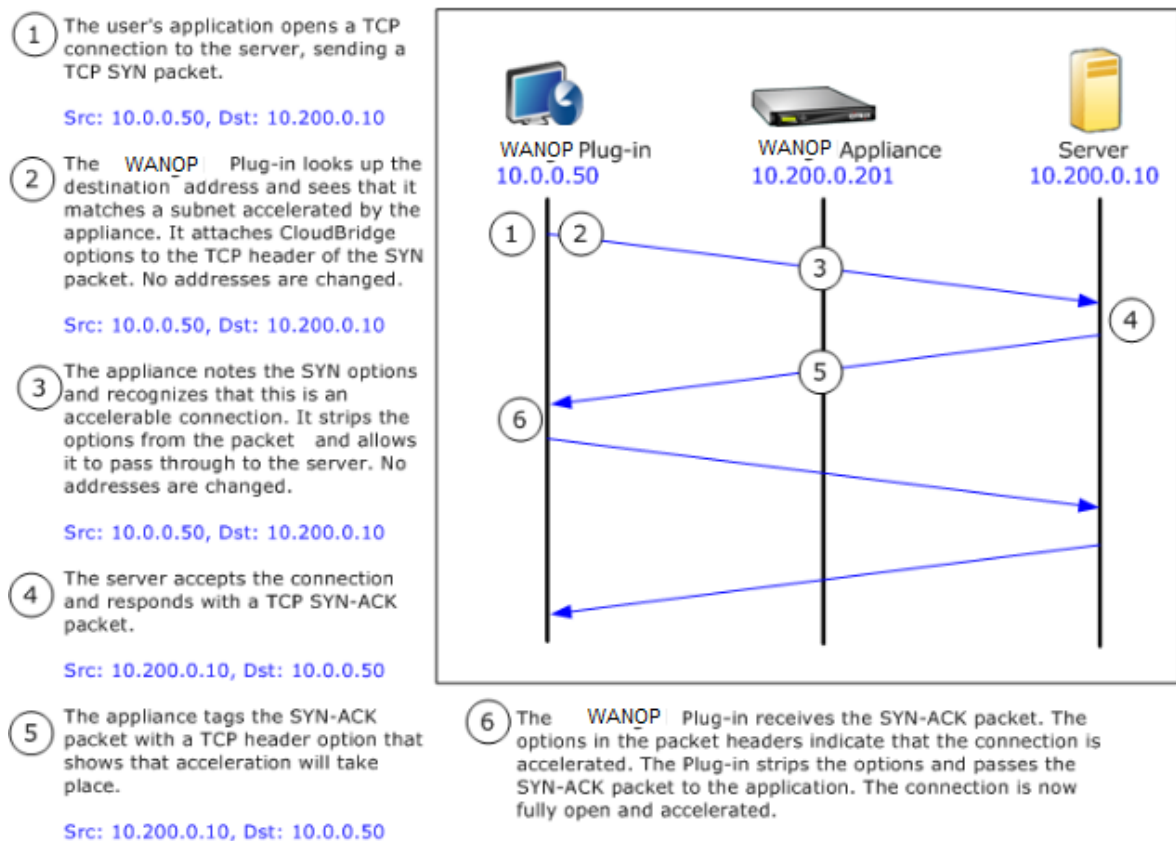
Der transparente Modus ähnelt der Beschleunigung von Appliance-zu-Appliance, ist jedoch nicht identisch mit dieser. Die Unterschiede sind:

- **Nur Clientinitiierte Verbindungen:** Der transparente Modus akzeptiert nur Verbindungen, die vom Plug-in-ausgestatteten System initiiert werden. Wenn Sie ein Plug-in-ausgestattetes System als Server verwenden, werden Serververbindungen nicht beschleunigt. Die Appliance-to-Appliance-Beschleunigung hingegen funktioniert unabhängig davon, welche Seite der Client ist und welche der Server ist. (Active-Mode FTP wird als Sonderfall behandelt, da die Verbindung, die die vom Plug-in angeforderte Datenübertragung initiiert, vom Server geöffnet wird.)
- **Signalverbindung** —Der transparente Modus verwendet eine Signalverbindung zwischen Plug-in und Appliance für die Übertragung von Statusinformationen. Die Beschleunigung von Appliance-zu-Appliance erfordert keine Signalverbindung, außer für sichere Peer-Beziehungen, die standardmäßig deaktiviert sind. Wenn das Plug-In eine Signalverbindung nicht öffnen kann, versucht es nicht, Verbindungen über die Appliance zu beschleunigen.
- **Daisy-Chaining** —Für eine Appliance, die sich im Pfad zwischen einem Plug-In und der ausgewählten Ziel-Appliance befindet, müssen Sie im Menü **Konfiguration: Tuning** die Daisy-Chaining-Funktion aktivieren.

Der transparente Modus wird häufig mit VPNs verwendet. Das WANOP Client-Plug-In ist mit den meisten IPsec- und PPTP-VPNs sowie mit Citrix Access Gateway VPNs kompatibel.

Die folgende Abbildung zeigt den Paketfluss im transparenten Modus. Dieser Paketfluss ist fast identisch mit der Beschleunigung von Appliance-zu-Appliance, mit der Ausnahme, dass die Entscheidung, ob versucht wird, die Verbindung zu beschleunigen, auf Beschleunigungsregeln basiert, die über die Signalverbindung heruntergeladen werden.

Abbildung 2. Paketfluss im transparenten Modus



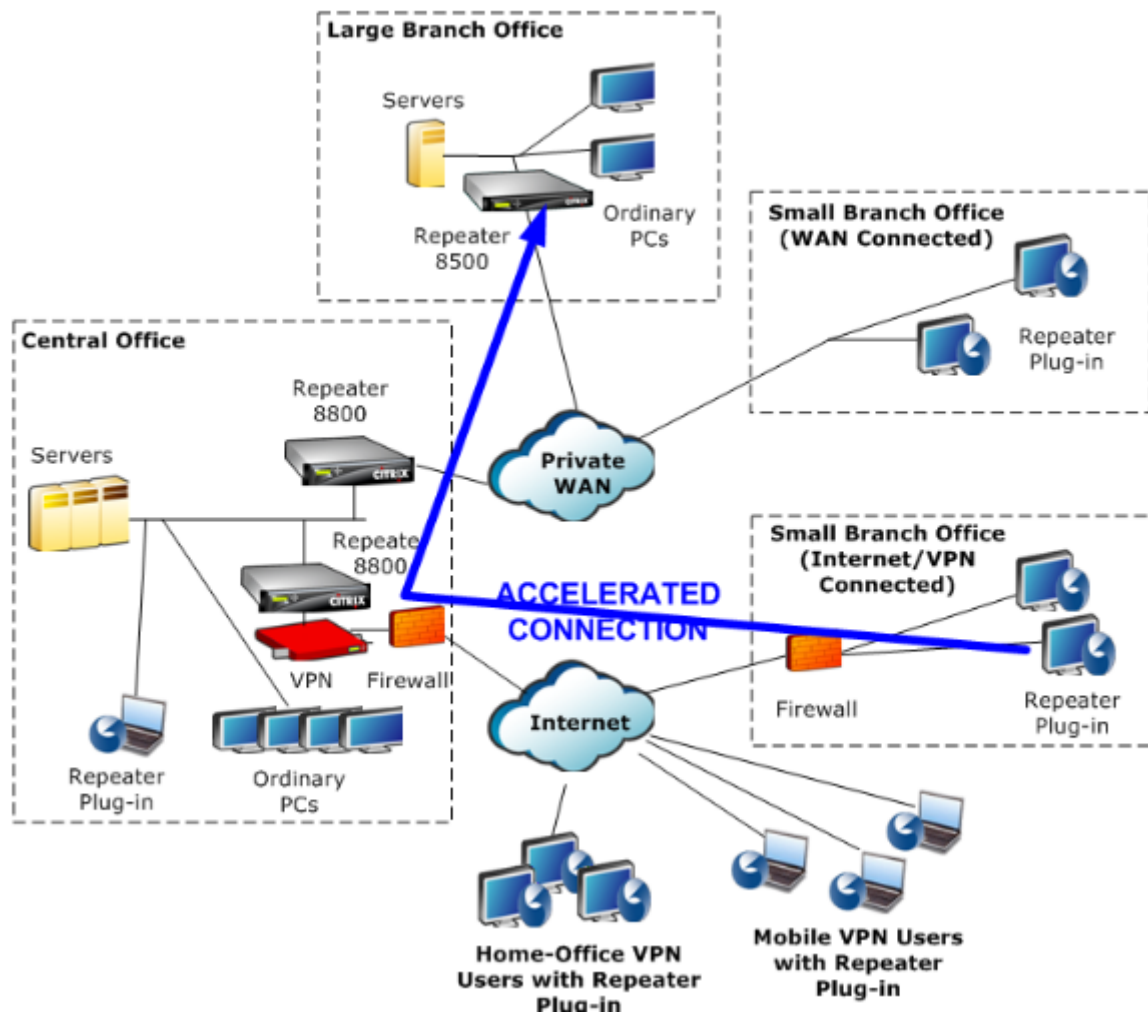
Umleitungsmodus

Der Umleitungsmodus funktioniert auf folgende Weise anders als der transparente Modus:

- Die WANOP Client-Plug-in-Software leitet die Pakete um, indem sie explizit an die Appliance adressieren.
- Daher muss die Umleitungsmodus-Appliance nicht den gesamten WAN-Link-Datenverkehr abfangen. Da beschleunigte Verbindungen direkt an sie adressiert werden, können sie überall platziert werden, solange sie sowohl vom Plug-in als auch vom Server erreicht werden können.
- Die Appliance führt ihre Optimierungen durch und leitet dann die Ausgabepakete an den Server um, wobei die Quell-IP-Adresse in den Paketen durch eine eigene Adresse ersetzt wird. Aus Sicht des Servers stammt die Verbindung von der Appliance.
- Der Rückkehrverkehr vom Server wird an die Appliance adressiert, die Optimierungen in Rückwärtsrichtung durchführt und die Ausgabepakete an das Plug-In weiterleitet.
- Die Zielporتنummern werden nicht geändert, sodass Netzwerküberwachungsanwendungen den Datenverkehr weiterhin klassifizieren können.

Die folgende Abbildung zeigt, wie der Redirector-Modus funktioniert.

Abbildung 1. Umleitungsmodus



Die folgende Abbildung zeigt den Paketfluss und die Adressenzuordnung im *Redirector-Modus*.

Abbildung 2. Paketfluss im Umleitungsmodus

- 1 The user's application opens a TCP connection to the server, sending a TCP SYN packet.

Src: 10.0.0.50, Dst: 10.200.0.10

- 2 The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.

Src: 10.0.0.50, Dst: 10.200.0.201

(10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

- 3 The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and giving itself as the src.

Src: 10.200.0.201, Dst: 10.200.0.10

- 4 The server accepts the connection and responds with a TCP SYN-ACK packet.

Src: 10.200.0.10, Dst: 10.200.0.201

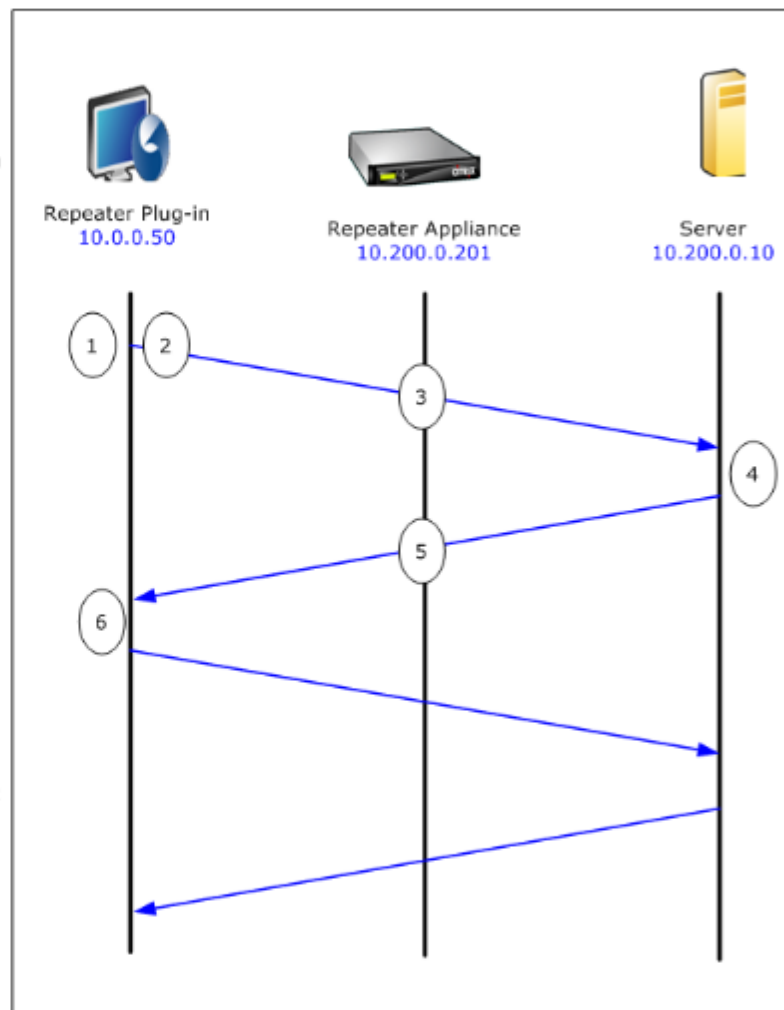
- 5 The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

Src: 10.200.0.201, Dst: 10.0.0.50

- 6 The connection is now fully open. The client and server send packets back and forth via the appliance.

While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.



So wählt das Plug-In eine Appliance aus

Jedes Plug-In ist mit einer Liste der Appliances konfiguriert, die es kontaktieren kann, um eine beschleunigte Verbindung anzufordern.

Die Appliances verfügen jeweils über eine Liste von *Beschleunigungsregeln*, d. h. eine Liste von Zieladressen oder Ports, zu denen die Appliance beschleunigte Verbindungen herstellen kann. Das Plug-In lädt diese Regeln von den Appliances herunter und gleicht die Zieladresse und den Port jeder Verbindung mit dem Regelsatz der einzelnen Appliance ab. Wenn nur eine Appliance eine bestimmte Verbindung beschleunigen kann, ist die Auswahl einfach. Wenn mehr als eine Appliance die Verbindung beschleunigen kann, muss das Plug-In eine der Appliances auswählen.

Die Regeln für die Geräteauswahl lauten wie folgt:

- Wenn alle Appliances, die zur Beschleunigung der Verbindung anbieten, Umleiter-Modus-Appliances sind, wird die ganz links in der Appliance-Liste des Plug-Ins ausgewählt. (Wenn die Appliances als DNS-Adressen angegeben wurden und der DNS-Eintrag mehrere IP-Adressen aufweist, werden auch diese von links nach rechts gescannt.)
- Wenn einige Appliances, die zur Beschleunigung der Verbindung anbieten, den Redirector-Modus verwenden und einige den transparenten Modus verwenden, werden die Appliances im transparenten Modus ignoriert, und die Auswahl erfolgt über die Appliances im Umleitungsmodus.
- Wenn alle Appliances, die zur Beschleunigung der Verbindung anbieten, den transparenten Modus verwenden, wählt das Plug-In keine bestimmte Appliance. Es initiiert die Verbindung mit den SYN-Optionen des WANOP Client-Plug-Ins, und je nachdem, welche Kandidateneinheit dem zurückgebenden SYN-ACK-Paket entsprechende Optionen anfügt, wird verwendet. Dadurch kann sich die Appliance, die tatsächlich dem Datenverkehr entspricht, mit dem Plug-In identifizieren. Das Plug-In muss jedoch über eine offene Signalverbindung mit der antwortenden Appliance verfügen, da sonst keine Beschleunigung stattfindet.
- Einige Konfigurationsinformationen gelten als global. Diese Konfigurationsinformationen stammen von der ganz links angezeigten Appliance in der Liste, für die eine Signalverbindung geöffnet werden kann.

Bereitstellen von Appliances zur Verwendung mit Plug-Ins

May 10, 2021

Die Clientbeschleunigung erfordert eine spezielle Konfiguration auf der WANOP Client-Plug-In-Appliance. Weitere Überlegungen sind die Platzierung der Appliance. Plug-Ins werden normalerweise

für VPN-Verbindungen bereitgestellt.

Verwenden Sie nach Möglichkeit eine dedizierte Appliance

Der Versuch, dieselbe Appliance sowohl für die Plug-in-Beschleunigung als auch für die Verbindungsbeschleunigung zu verwenden, ist oft schwierig, da die beiden Anwendungen manchmal dazu führen, dass sich die Appliance an verschiedenen Stellen im Rechenzentrum befindet, und die beiden Anwendungen können unterschiedliche Regeln der Service-Klasse aufrufen.

Darüber hinaus kann eine einzelne Appliance als Endpunkt für die Plug-in-Beschleunigung oder als Endpunkt für die Standort-zu-Standort-Beschleunigung dienen, kann aber nicht beide Zwecke gleichzeitig für dieselbe Verbindung dienen. Wenn Sie eine Appliance sowohl für die Plug-in-Beschleunigung für Ihr VPN als auch für die Standort-zu-Standort-Beschleunigung auf ein Remote-Rechenzentrum verwenden, erhalten Plug-in-Benutzer daher keine Standort-zu-Standort-Beschleunigung. Die Schwere dieses Problems hängt davon ab, wie viele der von Plug-in-Benutzern verwendeten Daten von Remote-Sites stammen.

Da die Ressourcen einer dedizierten Appliance nicht zwischen Plug-in- und Standort-zu-Site-Anforderungen aufgeteilt sind, bieten sie jedem Plug-in-Benutzer mehr Ressourcen und damit eine höhere Leistung.

Inline-Modus verwenden, wenn möglich

Eine Appliance sollte am selben Standort wie die von ihr unterstützte VPN-Einheit bereitgestellt werden. Typischerweise sind die beiden Einheiten in Einklang miteinander. Eine Inline-Bereitstellung bietet die einfachste Konfiguration, die meisten Funktionen und die höchste Leistung. Für beste Ergebnisse sollte die Appliance direkt mit der VPN-Einheit in Einklang stehen.

Appliances können jedoch einen beliebigen Bereitstellungsmodus verwenden, ausgenommen den Gruppenmodus oder den Hochverfügbarkeitsmodus. Diese Modi eignen sich sowohl für Appliance-zu-Appliance-Beschleunigung als auch für Client-zu-Appliance-Beschleunigung. Sie können allein (*transparenter Modus*) oder in Kombination mit dem Redirector-Modus verwendet werden.

Platzieren Sie die Appliances in einem sicheren Teil Ihres Netzwerks

Eine Appliance hängt genauso von Ihrer vorhandenen Sicherheitsinfrastruktur ab wie Ihre Server. Es sollte auf der gleichen Seite der Firewall (und VPN-Einheit, falls verwendet) wie die Server platziert werden.

NAT-Probleme vermeiden

Network Address Translation (NAT) auf der Plug-in-Seite wird transparent behandelt und ist kein Problem. Auf der Appliance-Seite kann NAT lästig sein. Wenden Sie die folgenden Richtlinien an, um eine reibungslose Bereitstellung sicherzustellen:

- Stellen Sie die Appliance in denselben Adressraum wie die Server ein, sodass alle Adressänderungen, die zum Erreichen der Server verwendet werden, auch auf die Appliance angewendet werden.
- Greifen Sie niemals auf die Appliance zu, indem Sie eine Adresse verwenden, die die Appliance nicht mit sich selbst verknüpft.
- Die Appliance muss auf die Server zugreifen können, indem sie dieselben IP-Adressen verwenden, unter denen Plug-in-Benutzer auf dieselben Server zugreifen.
- Kurz gesagt, wenden Sie NAT nicht auf die Adressen von Servern oder Appliances an.

Softboost Modus auswählen

Wählen Sie auf der Seite Einstellungen konfigurieren: Bandbreitenverwaltung die Option Softboost. Softboost ist die einzige Art der Beschleunigung, die mit dem WANOP Client Plug-in Plug-in unterstützt wird.

Definieren von Plug-in-Beschleunigungsregeln

Die Appliance verwaltet eine Liste von Beschleunigungsregeln, die den Clients mitteilen, welcher Datenverkehr beschleunigt werden soll. Jede Regel gibt eine Adresse oder ein Subnetz sowie einen Portbereich an, den die Appliance beschleunigen kann.

Was beschleunigt werden soll: Die Wahl des Datenverkehrs, der beschleunigt werden soll, hängt von der Verwendung der Appliance ab:

- VPN-Beschleuniger - Wenn die Appliance als VPN-Beschleuniger verwendet wird und der gesamte VPN-Datenverkehr durch die Appliance fließt, sollte der gesamte TCP-Datenverkehr unabhängig vom Ziel beschleunigt werden.
- Umleitungsmodus - Im Gegensatz zum transparenten Modus ist eine Appliance im Redirector-Modus ein expliziter Proxy, der dazu führt, dass das Plug-in seinen Datenverkehr an die Redirector-Modus-Appliance weiterleitet, selbst wenn dies nicht wünschenswert ist. Beschleunigung kann kontraproduktiv sein, wenn der Client Datenverkehr an eine Appliance weiterleitet, die vom Server entfernt ist, insbesondere wenn diese Dreiecksroute eine langsame oder unzuverlässige Verbindung einführt. Daher empfiehlt Citrix, Beschleunigungsregeln so zu konfigurieren, dass eine bestimmte Appliance nur ihre eigene Site beschleunigt.

- Sonstige Verwendung - Wenn das Plug-In weder als VPN-Beschleuniger noch im Redirector-Modus verwendet wird, sollten die Beschleunigungsregeln Adressen enthalten, die remote zu den Benutzern und lokal in Rechenzentren sind.

Definieren Sie die Regeln - Definieren Sie Beschleunigungsregeln auf der Registerkarte **Konfiguration: WANOP-Client-Plug-in: Beschleunigungsregeln**.

Regeln werden in der Reihenfolge ausgewertet, und die Aktion (Beschleunigen oder Ausschließen) wird von der ersten Übereinstimmungsregel übernommen. Damit eine Verbindung beschleunigt werden kann, muss sie mit einer Beschleunigungsregel übereinstimmen.

Die Standardaktion besteht darin, nicht zu beschleunigen.

Abbildung 1. Beschleunigungsregeln festlegen

Signaling Channel Configuration **Acceleration Rules** General Configuration

Repeater Plug-In: Acceleration Rules

Apply Cancel Add Delete Up Down

| Rule | Rule Type | Destination IP/Mask | Port |
|---------|------------|---------------------|------|
| 1 | Exclude | 10.200.33.102 | All |
| 2 | Exclude | 10.200.33.100 | All |
| 3 | Exclude | 10.200.33.104 | All |
| 4 | Exclude | 10.200.33.105 | All |
| 5 | Accelerate | 10.0.0.0/8 | All |
| Default | Exclude | All | All |

1. Auf der Registerkarte Konfiguration: WANOP Plug-in: Beschleunigungsregeln:

- Fügen Sie für jedes lokale LAN-Subnetz, das von der Appliance erreicht werden kann, eine Beschleunigungsregel hinzu. Das heißt, klicken Sie auf **Hinzufügen**, wählen Sie **Beschleunigen** aus, und geben Sie die Subnetz-IP-Adresse und -Maske ein.
 - Wiederholen Sie dies für jedes Subnetz, das lokal auf der Appliance ist.
2. Wenn Sie einen Teil des eingeschlossenen Bereichs ausschließen müssen, fügen Sie eine Ausschlussregel hinzu und verschieben Sie sie über die allgemeinere Regel. Beispielsweise sieht 10.217.1.99 wie eine lokale Adresse aus. Wenn es sich tatsächlich um den lokalen Endpunkt einer VPN-Einheit handelt, erstellen Sie eine Ausschlussregel für sie in einer Zeile oberhalb der Beschleunigungsregel für 10.217.1.0/24.
3. Wenn Sie Beschleunigung nur für einen einzelnen Port verwenden möchten (nicht empfohlen), z. B. Port 80 für HTTP, ersetzen Sie das Platzhalterzeichen im Feld Ports durch die spezifische

Portnummer. Sie können zusätzliche Ports unterstützen, indem Sie zusätzliche Regeln hinzufügen, eine pro Port.

4. Im Allgemeinen sollten Sie enge Regeln (in der Regel Ausnahmen) vor allgemeinen Regeln auflisten.
5. Klicken Sie auf **Übernehmen**. Änderungen werden nicht gespeichert, wenn Sie von dieser Seite weg navigieren, bevor Sie sie anwenden.

IP-Port-Nutzung

Verwenden Sie die folgenden Richtlinien für die Verwendung von IP-Ports:

- **Ports, die für die Kommunikation mit dem WANOP Client Plug-in verwendet werden**—Das Plug-In führt einen Dialog mit der Appliance über eine Signalverbindung, die standardmäßig auf Port 443 (HTTPS) ist, der über die meisten Firewalls erlaubt ist.
- **Ports, die für die Kommunikation mit Servern verwendet werden**—Die Kommunikation zwischen dem WANOP Client-Plug-in und der Appliance verwendet dieselben Ports, die der Client für die Kommunikation mit dem Server verwenden würde, wenn das Plug-in und die Appliance nicht vorhanden wären. Das heißt, wenn ein Client eine HTTP-Verbindung an Port 80 öffnet, stellt er eine Verbindung mit der Appliance an Port 80 her. Die Appliance wiederum kontaktiert den Server an Port 80.

Im Redirector-Modus wird nur der bekannte Port (d. h. der Zielport auf dem TCP SYN-Paket) beibehalten. Der flüchtige Port bleibt nicht erhalten. Im transparenten Modus bleiben beide Ports erhalten.

Die Appliance geht davon aus, dass sie mit dem Server an jedem vom Client angeforderten Port kommunizieren kann, und der Client geht davon aus, dass er mit der Appliance an jedem gewünschten Port kommunizieren kann. Dies funktioniert gut, wenn die Appliance denselben Firewallregeln wie die Server unterliegt. Wenn dies der Fall ist, gelingt jede Verbindung, die in einer direkten Verbindung erfolgreich wäre, in einer beschleunigten Verbindung.

Verwendung von TCP-Optionen und Firewalls

Die Parameter des WANOP Client-Plug-ins werden in den TCP-Optionen gesendet. TCP-Optionen können in jedem Paket auftreten und sind garantiert in den SYN- und SYN-ACK-Paketen vorhanden, die die Verbindung herstellen.

Die Firewall darf TCP-Optionen im Bereich von 24-31 (Dezimalzahl) nicht blockieren, da sonst keine Beschleunigung möglich ist. Die meisten Firewalls blockieren diese Optionen nicht. Eine Cisco PIX- oder ASA-Firewall mit Version 7.x-Firmware kann dies jedoch standardmäßig tun, und daher müssen Sie die Konfiguration anpassen.

Anpassen der Plug-In-MSI-Datei

May 10, 2021

Sie können Parameter in der WANOP-Client-Plug-in-Verteilungsdatei ändern, die im standardmäßigen Microsoft Installer (MSI) Format vorliegt. Die Anpassung erfordert die Verwendung eines MSI-Editors.

Hinweis

Die geänderten Parameter in Ihrem bearbeiteten MSI-Datei gilt nur für neue Installationen. Wenn vorhandene Plug-in-Benutzer auf eine neue Version aktualisieren, werden ihre vorhandenen Einstellungen beibehalten. Daher sollten Sie nach dem Ändern der Parameter Ihren Benutzern empfehlen, die alte Version zu deinstallieren, bevor Sie die neue installieren.

Best Practices:

Erstellen Sie einen DNS-Eintrag, der in die nächste Plug-in-fähige Appliance aufgelöst wird. Definieren Sie beispielsweise Repeater.MyCompany.com und lassen Sie es auf Ihre Appliance auflösen, wenn Sie nur über eine Appliance verfügen. Oder, wenn Sie beispielsweise fünf Appliances haben, haben Repeater.MyCompany..com Auflösung zu einer Ihrer fünf Appliances, wobei die Appliance aufgrund der Nähe zum Client oder zur VPN-Einheit ausgewählt wurde. Beispielsweise sollte ein Client, der eine Adresse verwendet, die einem bestimmten VPN zugeordnet ist, Repeater.MyCompany.com-Auflösung in die IP-Adresse der WANOP Client-Plug-in-Appliance sehen, die mit diesem VPN verbunden ist. Bauen Sie diese Adresse in Ihre Plug-in-Binärdatei mit einem MSI-Editor wie Orca ein. Wenn Sie Appliances hinzufügen, verschieben oder entfernen, wird durch Ändern dieser einzelnen DNS-Definition auf dem DNS-Server automatisch die Appliance-Liste der Plug-Ins aktualisiert.

Der DNS-Eintrag kann auch auf mehrere Appliances aufgelöst werden. Dies ist jedoch nicht wünschenswert, wenn alle Appliances identisch konfiguriert sind, da das Plug-In einige Merkmale der Appliance ganz links in der Liste übernimmt und sie global anwendet (einschließlich SSL-Komprimierungsmerkmalen). Dies kann zu unerwünschten und verwirrenden Ergebnissen führen, insbesondere wenn der DNS-Server die Reihenfolge der IP-Adressen für jede Anforderung rotiert.

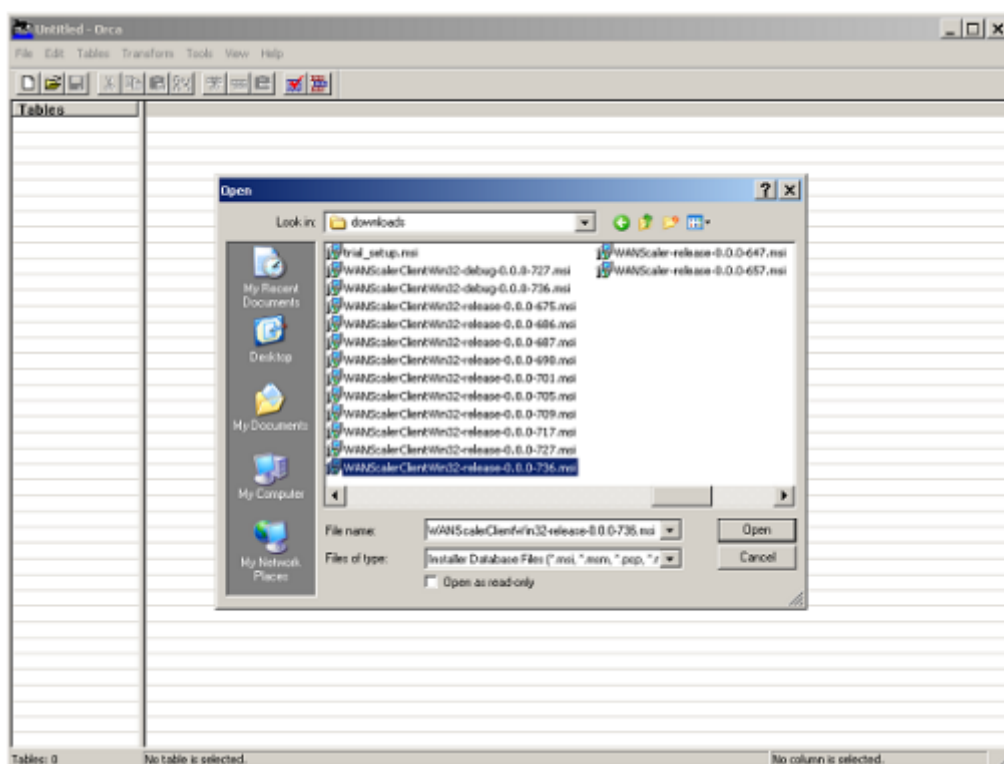
Installieren Sie den Orca MSI Editor:

Es gibt viele MSI-Editoren wie Orca, das Teil des kostenlosen Plattform-SDK von Microsoft ist und von Microsoft heruntergeladen werden kann.

- So installieren Sie den Orca MSI Editor
 1. Laden Sie die PSDK-x86.exe Version des SDK herunter und führen Sie es aus. Folgen Sie den Installationsanweisungen.

2. Sobald das SDK installiert ist, muss der Orca-Editor installiert werden. Er ist unter Microsoft Platform SDK\Bin\Orca.Msi. Starten Sie Orca.msi, um den eigentlichen Orca-Editor (orca.exe) zu installieren.
3. **Ausführen von Orca**—Microsoft stellt seine Orca-Dokumentation online bereit. In den folgenden Informationen wird beschrieben, wie Sie die wichtigsten WANOP Client Plug-in-Parameter bearbeiten.
4. Starten Sie Orca mit **Start > Alle Programme > Orca**. Wenn ein leeres Orca-Fenster angezeigt wird, öffnen Sie die MSI-Datei des WANOP Client Plug-in mit **Datei > Öffnen**.

Abbildung 1. Verwenden von Orca



5. Klicken Sie im Menü **Tabellen** auf **Eigenschaft**. Eine Liste aller bearbeitbaren Eigenschaften der MSI-Datei wird angezeigt. Bearbeiten Sie die in der folgenden Tabelle gezeigten Parameter. Um einen Parameter zu bearbeiten, doppelklicken Sie auf seinen Wert, geben Sie den neuen Wert ein, und drücken Sie die **EINGABETASTE**.

| Parameter | Beschreibung | Standard | Kommentare |
|--------------|---|----------|---|
| WSAPPLIANCES | Liste der Geräte | Ohne | Geben Sie hier die IP- oder DNS-Adressen Ihrer WANOP-Appliances in einer kommagetrennten Liste in Form von {appliance1, appliance2, appliance3} ein. Wenn sich der Port für die Signalisierung von Verbindungen vom Standard (443) unterscheidet, geben Sie den Port in der Form Appliance1:Port_Number an . |
| DBCMINSIZE | Minimaler Speicherplatz für die Komprimierung in Megabyte | 250 | Wenn Sie diesen Wert auf einen größeren Wert ändern (z. B. 2000), verbessert die Komprimierungsleistung, verhindert jedoch die Installation, wenn nicht genügend Speicherplatz vorhanden ist. Das Plug-In wird nur installiert, wenn zusätzlich zu dem Wert, den Sie für DBCMINSIZE angeben, mindestens 100 MB freier Speicherplatz vorhanden sind. |

| Parameter | Beschreibung | Standard | Kommentare |
|-------------|---|----------|---|
| EKEYPEM | Privater Schlüssel für das Plug-In. Teil des Zertifikat-/Schlüsselpaars, das für die SSL-Komprimierung verwendet wird | Ohne | Verwenden Sie Orcas Befehl Zelle einfügen. Die normale Einfügefunktion behält das Format der Taste nicht bei. Sollte ein privater Schlüssel im PEM-Format sein (beginnend mit — BEGIN RSA PRIVATE KEY—) |
| X509CERTPEM | Zertifikat für das Plug-In. Teil des Zertifikat-/Schlüsselpaars, das für die SSL-Komprimierung verwendet wird | Ohne | Verwenden Sie Orcas Befehl Zelle einfügen. Die normale Einfügefunktion behält das Format der Taste nicht bei. Sollte ein Zertifikat im PEM-Format sein (beginnend mit — BEGIN CERTIFICATE — —) |
| CACERTPEM | Zertifizierungsstellenzertifikate für das Plug-In. Wird mit SSL-Komprimierung verwendet | Ohne | Verwenden Sie Orcas Befehl Zelle einfügen. Die normale Einfügefunktion behält das Format der Taste nicht bei. Sollte ein Zertifikat im PEM-Format sein (beginnend mit — BEGIN CERTIFICATE — —) |

6. Klicken Sie im Menü Tabellen auf Eigenschaft. Eine Liste aller bearbeitbaren Eigenschaften der MSI-Datei wird angezeigt. Bearbeiten Sie die in der folgenden Tabelle gezeigten Parameter. Um einen Parameter zu bearbeiten, doppelklicken Sie auf seinen Wert, geben Sie

den neuen Wert ein, und drücken **Sie die EINGABETASTE**.

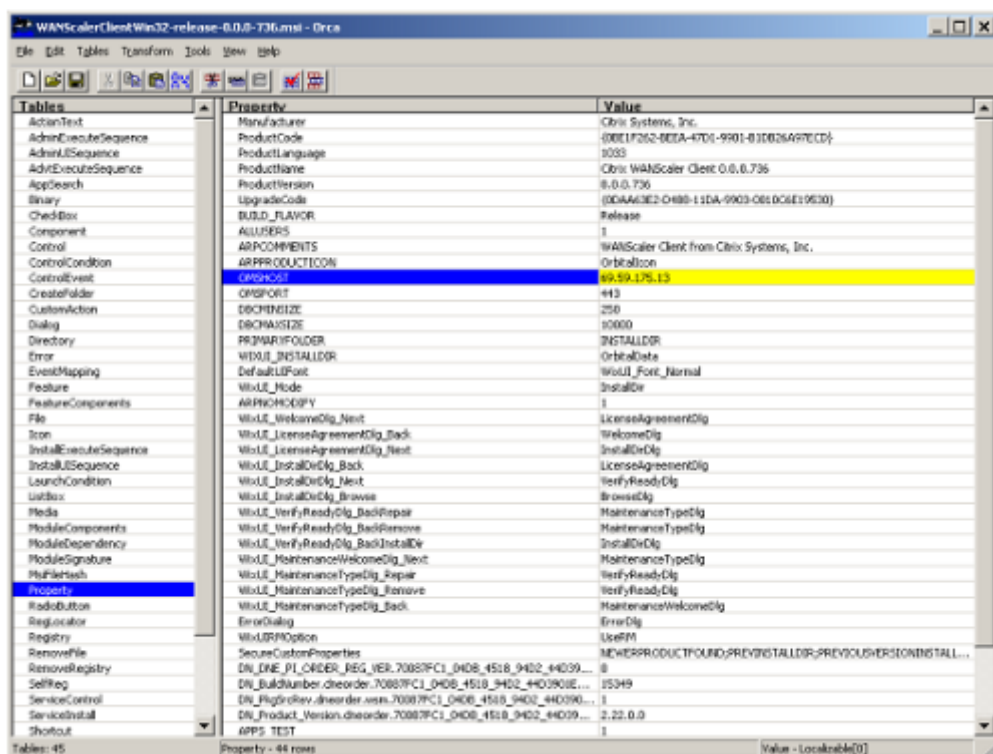
| Parameter | Beschreibung | Standard | Kommentare |
|--------------|------------------|----------|---|
| WSAPPLIANCES | Liste der Geräte | Ohne | Geben Sie hier die IP- oder DNS-Adressen Ihrer WANOP Client-Plug-in-Appliances in einer kommagetrennten Liste in Form von <i>{appliance1, appliance2, appliance3}</i> ein. Wenn sich der Port für die Signalisierung von Verbindungen vom Standard (443) unterscheidet, geben Sie den Port in der Form <i>Appliance1:Port_Number</i> an . |

| Parameter | Beschreibung | Standard | Kommentare |
|---------------|---|----------|---|
| DBCMINSIZE | Minimaler Speicherplatz für die Komprimierung in Megabyte | 250 | Wenn Sie diesen Wert auf einen größeren Wert ändern (z. B. 2000), verbessert die Komprimierungsleistung, verhindert jedoch die Installation, wenn nicht genügend Speicherplatz vorhanden ist. Das Plug-In wird nur installiert, wenn zusätzlich zu dem Wert, den Sie für DBCMINSIZE angeben, mindestens 100 MB freier Speicherplatz vorhanden sind. |
| PRIVATEKEYPEM | Privater Schlüssel für das Plug-In. Teil des Zertifikat-/Schlüsselpaars, das für die SSL-Komprimierung verwendet wird | Ohne | Verwenden Sie Orcas Befehl Zeile einfügen. Die normale Einfügefunktion behält das Format der Taste nicht bei. Sollte ein privater Schlüssel im PEM-Format sein (beginnend mit — BEGIN RSA PRIVATE KEY—) |

| Parameter | Beschreibung | Standard | Kommentare |
|-------------|---|----------|--|
| X509CERTPEM | Zertifikat für das Plug-In. Teil des Zertifikat-/Schlüsselpaars, das für die SSL-Komprimierung verwendet wird | Ohne | Verwenden Sie Orcas Befehl Zelle einfügen. Die normale Einfügefunktion behält das Format der Taste nicht bei. Sollte ein Zertifikat im PEM-Format sein (beginnend mit — BEGIN CERTIFICATE — —) |
| CACERTPEM | Zertifizierungsstellenzertifikate für das Plug-In. Wird mit SSL-Komprimierung verwendet | Ohne | Verwenden Sie Orcas Befehl Zelle einfügen. Die normale Einfügefunktion behält das Format der Taste nicht bei. Sollte ein Zertifikat im PEM-Format sein (beginnend mit — BEGIN CERTIFICATE — —) |

7. Wenn Sie fertig sind, verwenden Sie den Befehl **Datei: Speichern unter**, um die bearbeitete Datei unter einem neuen Dateinamen zu speichern, z. B. test.msi.

Abbildung 2: Bearbeiten von Parametern in Orca:



8. Wenn Sie fertig sind, verwenden Sie den Befehl **Datei: Speichern unter**, um die bearbeitete Datei unter einem neuen Dateinamen zu speichern, z. B. test.msi.

Ihre Plug-In-Software wurde nun angepasst.

Hinweis

Einige Benutzer haben einen Fehler in Orca gesehen, der dazu führt, dass Dateien auf 1 MB abgeschnitten werden. Überprüfen Sie die Größe der gespeicherten Datei. Wenn sie abgeschnitten wurde, erstellen Sie eine Kopie der Originaldatei und überschreiben Sie das Original mit dem Befehl Speichern.

Nachdem Sie die Appliance-Liste mit Orca angepasst und die angepasste MSI-Datei an Ihre Benutzer verteilt haben, muss der Benutzer bei der Installation der Software keine Konfigurationsinformationen eingeben.

Bereitstellen von Plug-Ins auf Windows-Systemen

May 10, 2021

Das WANOP Client-Plug-in ist eine ausführbare Microsoft-Installationsdatei (MSI), die Sie herunterladen und installieren, wie bei jedem anderen webverteilten Programm. Rufen Sie diese Datei im

MyCitrix-Abschnitt der Citrix.com -Website ab.

Hinweis:

Die Benutzeroberfläche des WANOP Client-Plug-ins bezeichnet sich selbst als **Citrix Acceleration Plug-in Manager**.

Die einzige Benutzerkonfiguration, die vom Plug-in benötigt wird, ist die Liste der Appliance-Adressen. Diese Liste kann aus einer kommagetrennten Liste von IP- oder DNS-Adressen bestehen. Die beiden Formen können gemischt werden. Sie können die Verteilungsdatei so anpassen, dass die Liste standardmäßig auf Ihre Appliance verweist. Nach der Installation ist der Betrieb transparent. Der Datenverkehr zu beschleunigten Subnetzen wird über eine entsprechende Appliance gesendet, und der gesamte andere Datenverkehr wird direkt an den Server gesendet. Die Benutzeranwendung ist sich nicht bewusst, dass dies geschieht.

Installation

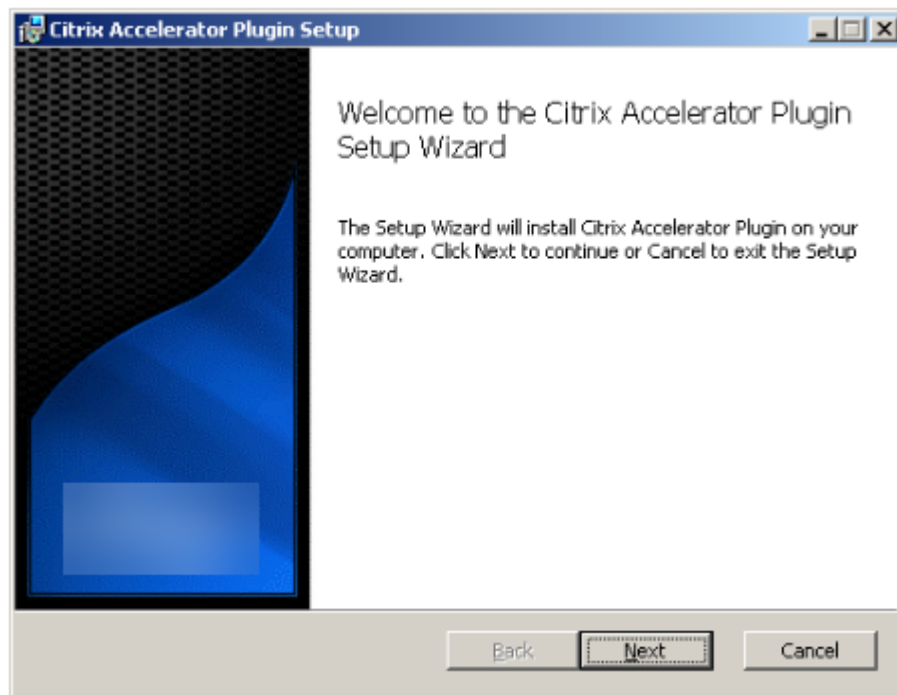
Voraussetzungen:

Windows 10 erfordert, dass alle Treiber über eine gültige digitale Signatur verfügen, um die Installation ohne Fehler durchzuführen.

So installieren Sie den WANOP Client Plug-in Plug-in Accelerator auf Windows-Systemen:

1. Die Datei Repeater*.msi ist eine Installationsdatei. Schließen Sie alle Anwendungen und alle Fenster, die möglicherweise geöffnet sind, und starten Sie das Installationsprogramm auf die übliche Weise (doppelklicken Sie in einem Dateifenster auf, oder verwenden Sie den Befehl run).

Abbildung 1. Bildschirm für die Erstinstallation:

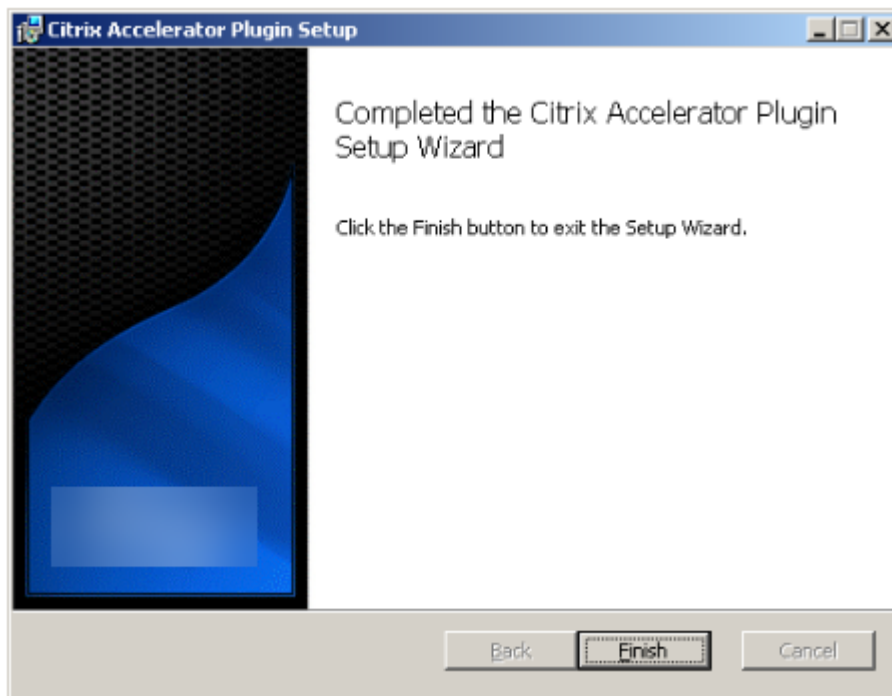


Die folgenden Schritte sind für eine interaktive Installation. Eine unbeaufsichtigte Installation kann mit dem Befehl durchgeführt werden:

msiexec /i client_msi_file /qn

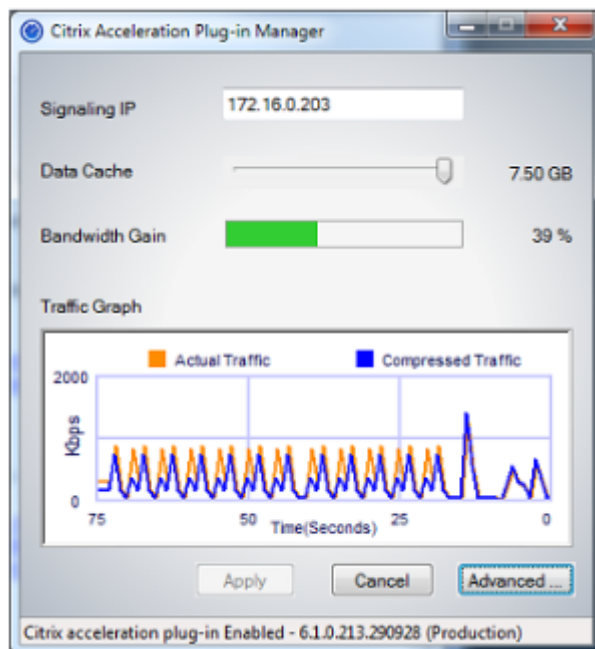
2. Das Installationsprogramm fragt nach dem Speicherort, an dem die Software installiert werden soll. Das angegebene Verzeichnis wird sowohl für die Clientsoftware als auch für den datenträgerbasierten Komprimierungsverlauf verwendet. Zusammen benötigen sie mindestens 500 MB Speicherplatz.
3. Wenn das Installationsprogramm abgeschlossen ist, werden Sie möglicherweise aufgefordert, das System neu zu starten. Nach einem Neustart startet das WANOP Client Plug-in Plug-in automatisch.

Abbildung 2. Bildschirm Endgültige Installation



4. Klicken Sie mit der rechten Maustaste auf das Accelerator-Symbol in der Taskleiste, und wählen Sie **Beschleunigung verwalten** aus, um den Citrix Plug-in Accelerator Manager zu starten.

Abbildung 3. Citrix Accelerator-Plug-in-Manager, Anfangsanzeige (Basisanzeige)



5. Wenn die MSI-Datei nicht für Ihre Benutzer angepasst wurde, geben Sie die Signaladresse und den Speicherplatz an, der für die Komprimierung verwendet werden soll:
- Geben Sie im Feld Appliances: Signaladressen die signalierende IP-Adresse Ihrer Appli-

ance ein. Wenn Sie mehr als eine Plug-in-fähige Appliance haben, führen Sie sie alle durch Kommas getrennt auf. Entweder IP- oder DNS-Adressen sind akzeptabel.

- Wählen Sie mithilfe des Schiebereglers Datencache den Speicherplatz aus, der für die Komprimierung verwendet werden soll. Mehr ist besser. 7,5 GB sind nicht zu viel, wenn Sie so viel Speicherplatz zur Verfügung haben.
- Drücken Sie Übernehmen.

Der WANOP Client Plug-in Accelerator läuft jetzt. Alle zukünftigen Verbindungen zu beschleunigten Subnetzen werden beschleunigt

Auf der Registerkarte Erweiterte Regeln des Plug-Ins sollte in der Liste Beschleunigungsregeln jede Appliance als Verbunden und die beschleunigten Subnetze jeder Appliance als Beschleunigt angezeigt werden. Wenn nicht, aktivieren Sie das IP-Feld Signaladressen und Ihre Netzwerkkonnektivität im Allgemeinen.

Problembehandlung bei Plug-Ins

Die Plug-in-Installation verläuft in der Regel reibungslos. Wenn nicht, überprüfen Sie die folgenden Probleme:

Häufige Probleme:

- Wenn Sie das System nicht neu starten, wird das WANOP Client-Plug-in nicht ordnungsgemäß ausgeführt.
- Ein stark fragmentierter Datenträger kann zu einer schlechten Komprimierungsleistung führen.
- Ein Beschleunigungsfehler (keine beschleunigten Verbindungen auf der Registerkarte **Diagnose**) weist normalerweise darauf hin, dass die Kommunikation mit der Appliance verhindert wird. Überprüfen Sie die Liste **Konfiguration: Beschleunigungsregeln** im Plug-In, um sicherzustellen, dass die Appliance erfolgreich kontaktiert wird und dass die Zieladresse in einer der Beschleunigungsregeln enthalten ist. Typische Ursachen für Verbindungsfehler sind:
 - Die Appliance wird nicht ausgeführt, oder die Beschleunigung wurde deaktiviert.
 - Eine Firewall entfernt die TCP-Optionen des WANOP Client-Plug-ins irgendwann zwischen dem Plug-in und der Appliance.
 - Das Plug-In verwendet ein nicht unterstütztes VPN.

Deterministischer Netzwerk-Enhancer Sperrfehler

In seltenen Fällen wird nach der Installation des Plug-Ins und dem Neustart des Computers die folgende Fehlermeldung zweimal angezeigt:

Deterministic Network Enhancer Installation erfordert zunächst einen Neustart, um gesperrte Ressourcen freizumachen. Führen Sie diese Installation erneut aus, nachdem Sie den Computer neu gestartet haben.

Sie umgehen das Problem wie folgt:

1. Gehen Sie zu **Software hinzufügen/entfernen** und entfernen Sie das WANOP Client-Plug-in, falls vorhanden.
2. Gehen Sie zu **Systemsteuerung > Netzwerkadapter > LAN-Verbindung > Eigenschaften**, suchen Sie den Eintrag für Deterministic Network Enhancer, deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **OK**. (Ihr Netzwerkadapter wird möglicherweise unter einem anderen Namen als LAN-Verbindung aufgerufen.)
3. Öffnen Sie ein Befehlsfenster und gehen Sie zu c:windowsinf (oder dem entsprechenden Verzeichnis, wenn Sie Windows an einem nicht standardmäßigen Speicherort installiert haben).
4. Geben Sie den folgenden Befehl ein:
finden Sie dne2000.cat oem*.inf
5. Suchen Sie die Datei oem*.inf mit der höchsten Zahl, die eine übereinstimmende Zeile zurückgegeben hat (die passende Zeile ist CatalogFile= dne2000.cat), und bearbeiten Sie sie. Zum Beispiel:
Notizblock oem13.inf
6. Löschen Sie alles außer den drei Zeilen oben, die mit Semikolons beginnen, und speichern Sie die Datei. Dadurch werden alle unangemessenen oder veralteten Einstellungen gelöscht und bei der nächsten Installation werden Standardwerte verwendet.
7. Wiederholen Sie die Installation.

Andere Installationsprobleme

Jedes Problem bei der Installation des WANOP Client-Plug-ins ist in der Regel das Ergebnis einer bestehenden Netzwerk-, Firewall- oder Antivirensoftware, die die Installation beeinträchtigt. Normalerweise gibt es nach Abschluss der Installation keine weiteren Probleme.

Wenn die Installation fehlschlägt, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Plug-in-Installationsdatei auf Ihr lokales System kopiert wurde.
2. Trennen Sie alle aktiven VPN/Remote-Netzwerkclients.
3. Deaktivieren Sie alle Firewall- und Antivirus-Software vorübergehend.
4. Wenn etwas davon schwierig ist, tun Sie, was Sie können.

5. Installieren Sie das WANOP Client-Plug-in neu.
6. Wenn dies nicht funktioniert, starten Sie das System neu und versuchen Sie es erneut.

WANOP-Plug-In-GUI-Befehle

May 10, 2021

Die Benutzeroberfläche des WANOP Client-Plug-ins wird angezeigt, wenn Sie mit der rechten Maustaste auf das Symbol des **Citrix Accelerator-Plug-ins** klicken und die Option **Beschleunigung verwalten** auswählen. Zuerst wird die Basic-Anzeige der GUI angezeigt. Es gibt auch ein Advanced Display, das auf Wunsch verwendet werden kann.

Basisanzeige

Auf der Seite Basic können Sie zwei Parameter festlegen:

- Das Feld Signaladressen gibt die IP-Adresse jeder Appliance an, mit der das Plug-In eine Verbindung herstellen kann. Citrix empfiehlt, nur eine Appliance aufzulisten, Sie können jedoch eine durch Kommas getrennte Liste erstellen. Dies ist eine geordnete Liste, wobei die ganz links Appliances Vorrang vor den anderen haben. Die Beschleunigung wird mit der ganz links stehenden Appliance versucht, für die eine Signalverbindung hergestellt werden kann. Sie können sowohl DNS-Adressen als auch IP-Adressen verwenden.

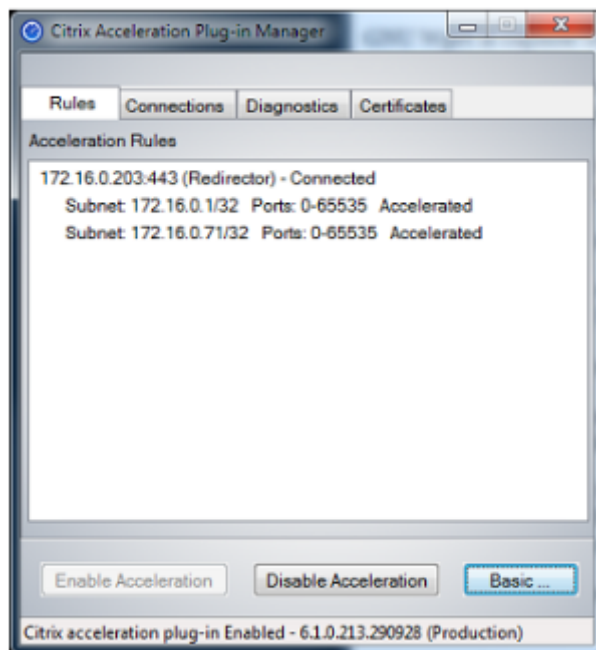
Beispiele: 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

- Der Schieberegler Datencache passt den Speicherplatz an, der dem datenträgerbasierten Komprimierungsverlauf des Plug-Ins zugewiesen ist. Mehr ist besser.

Darüber hinaus gibt es eine Schaltfläche, um zur erweiterten Anzeige zu wechseln.

Erweiterte Anzeige

Die Seite Erweitert enthält vier Registerkarten: Regeln, Verbindungen, Diagnose und Zertifikate.



Am unteren Rand der Anzeige befinden sich Schaltflächen, um die Beschleunigung zu aktivieren, die Beschleunigung zu deaktivieren und zur Seite Basic zurückzukehren.

Registerkarte Regeln

Auf der Registerkarte Regeln wird eine abgekürzte Liste der von den Appliances heruntergeladenen Beschleunigungsregeln angezeigt. Jedes Listenelement zeigt die Signaladresse und den Port der Appliance, den Beschleunigungsmodus (Redirector oder transparent) und den Verbindungsstatus, gefolgt von einer Zusammenfassung der Regeln der Appliance.

Registerkarte Verbindungen

Die Registerkarte **Verbindungen** listet die Anzahl der offenen Verbindungen verschiedener Typen auf:

- **Beschleunigte Verbindungen**—Die Anzahl der offenen Verbindungen zwischen dem WANOP Client Plug-in und Appliances. Diese Nummer enthält eine Signalverbindung pro Appliance, enthält jedoch keine beschleunigten CIFS-Verbindungen. Wenn Sie auf Mehr klicken, wird ein Fenster mit einer kurzen Zusammenfassung jeder Verbindung geöffnet. (Alle Schaltflächen Mehr ermöglichen es Ihnen, die Informationen im Fenster in die Zwischenablage zu kopieren, falls Sie sie für den Support freigeben möchten.)
- **Beschleunigte CIFS-Verbindungen**—Die Anzahl der offenen, beschleunigten Verbindungen mit CIFS-Servern (Windows File System). Dies entspricht normalerweise der Anzahl der bereitgestellten Netzwerkdateisysteme. Wenn Sie auf Mehr klicken, werden dieselben Informationen

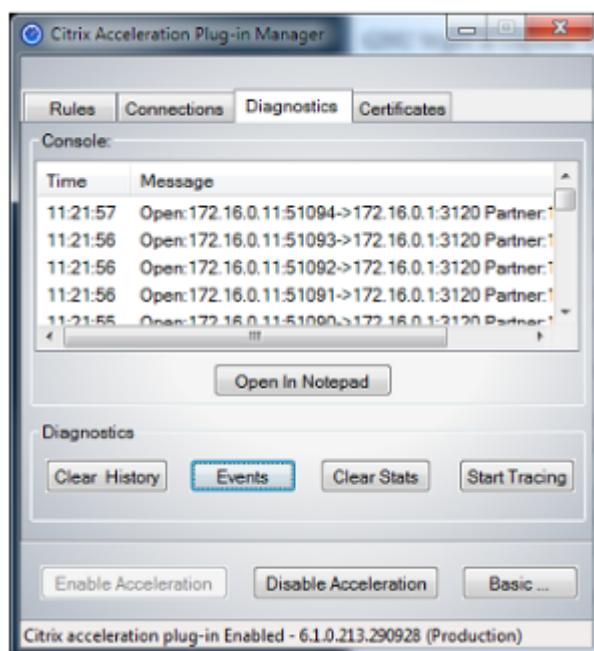
angezeigt wie bei beschleunigten Verbindungen sowie ein Statusfeld, das Aktiv meldet, wenn die CIFS-Verbindung mit den speziellen CIFS-Optimierungen des WANOP Client-Plug-ins ausgeführt wird.

- **Beschleunigte MAPI-Verbindungen**—Die Anzahl der offenen, beschleunigten Outlook/Exchange-Verbindungen.
- **Beschleunigte ICA-Verbindungen**—Die Anzahl der offenen, beschleunigten XenApp - und Xen-Desktop Verbindungen, die die ICA- oder CGP-Protokolle verwenden.
- **Nicht beschleunigte Verbindungen**—Öffnet Verbindungen, die nicht beschleunigt werden. Sie können auf Mehr klicken, um eine kurze Beschreibung anzuzeigen, warum die Verbindung nicht beschleunigt wurde. Normalerweise ist der Grund dafür, dass keine Appliance die Zieladresse beschleunigt, die als Dienstrichtlinienregel gemeldet wird.
- **Verbindungen öffnen/schließen**—Verbindungen, die nicht vollständig geöffnet sind, aber gerade geöffnet oder geschlossen werden (TCP-Verbindungen halb offen oder halb geschlossen). Die Schaltfläche Mehr zeigt einige zusätzliche Informationen zu diesen Verbindungen an.

Registerkarte Diagnose

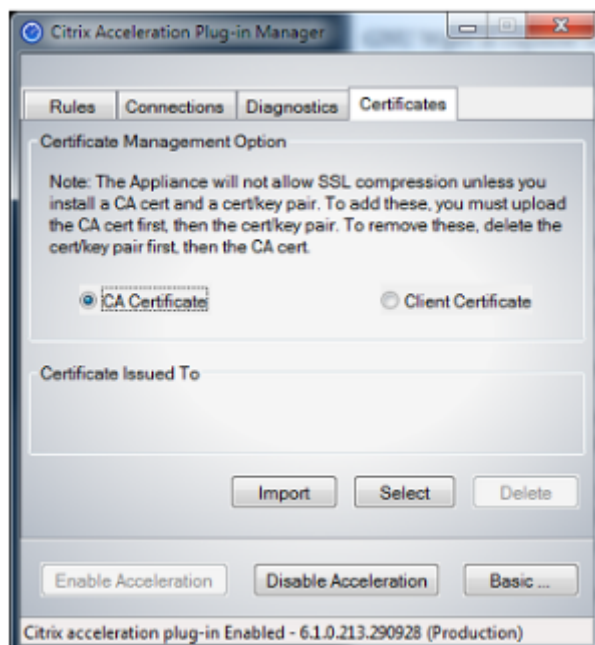
Auf der Seite Diagnose werden die Anzahl der Verbindungen in verschiedenen Kategorien sowie weitere nützliche Informationen angezeigt.

- **Ablaufverfolgung/Ablaufverfolgung starten**—Wenn Sie ein Problem melden, werden Sie möglicherweise von Ihrem Citrix Vertreter aufgefordert, eine Verbindungsverfolgung durchzuführen, um Probleme zu ermitteln. Diese Schaltfläche startet und stoppt die Ablaufverfolgung. Wenn Sie die Ablaufverfolgung beenden, werden die Ablaufverfolgungsdateien in einem Pop-upfenster angezeigt. Senden Sie sie auf die von ihm empfohlenen Mittel an Ihren Citrix Vertreter.
- **Verlauf löschen**—Dieses Feature sollte nicht verwendet werden.
- **Statistiken löschen**—Durch Drücken dieser Schaltfläche wird die Statistik auf der Registerkarte Leistung gelöscht.
- **Konsole**: Ein scrollbares Fenster mit aktuellen Statusmeldungen, meist Meldungen zum Öffnen und Schließen von Verbindungen, aber auch Fehler- und sonstige Statusmeldungen.



Registerkarte Zertifikate

Auf der Registerkarte Zertifikate können Sie Sicherheitsanmeldeinformationen für das optionale Secure Peering-Feature installieren. Mit diesen Sicherheitsanmeldeinformationen kann die Appliance überprüfen, ob es sich bei dem Plug-In um einen vertrauenswürdigen Client handelt oder nicht.



So laden Sie das CA-Zertifikat und das Zertifikatschlüsselpaar hoch:

1. Wählen Sie **CA-Zertifikatverwaltung** aus.
2. Klicken Sie auf **Importieren**.
3. Laden Sie ein Zertifizierungsstellenzertifikat hoch. Die Zertifikatdatei muss einen der unterstützten Dateitypen (.pem, .crt., .cer oder .spc) verwenden. Möglicherweise wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, den Zertifikatspeicher auszuwählen, den Sie verwenden möchten, und eine Liste mit Schlüsselwörtern anzuzeigen. Wählen Sie das erste Schlüsselwort in der Liste aus.
4. Wählen Sie **Clientzertifikatverwaltung** aus.
5. Klicken Sie auf **Importieren**.
6. Wählen Sie das Format des Zertifikatschlüsselpaars (PKCS12 oder PEM/DER).
7. Klicken Sie auf **Absenden**.

Hinweis

Bei PEM/DER gibt es separate Upload-Boxen für Zertifikat und Schlüssel. Wenn Ihr Zertifikatschlüsselpaar in einer einzigen Datei kombiniert wird, geben Sie die Datei zweimal an, einmal für jedes Feld.

Aktualisieren des WANOP-Plug-Ins

May 10, 2021

Um eine neuere Version des WANOP Client-Plug-ins zu installieren, befolgen Sie das gleiche Verfahren, das Sie bei der ersten Installation des Plug-Ins verwendet haben.

Deinstallieren des WANOP-Client-Plug-ins

Verwenden Sie zum Deinstallieren des WANOP-Client-Plug-ins das Windows-Dienstprogramm Software. Das WANOP Client-Plug-in wird in der Liste der aktuell installierten Programme als **Citrix Acceleration Plug-in** aufgeführt. Wählen Sie es aus und klicken Sie auf **Entfernen**.

Sie müssen das System neu starten, um die Deinstallation des Clients abzuschließen.

Problembehandlung beim WANOP-Plug-In

May 10, 2021

- **Problem:** Ich habe Probleme mit der Signalkanalkonnektivität. Wie kann ich diese Probleme lösen?

Lösung: Um Probleme mit der Signalkanalkonnektivität zu beheben, führen Sie die folgenden Schritte zur Fehlerbehebung durch:

- Stellen Sie sicher, dass Sie die Signalisierungs-IP-Adresse korrekt konfiguriert haben. Sie können dies tun, indem Sie die signalisierende IP-Adresse pingen und die Antwort überprüfen.
- Stellen Sie sicher, dass der Signalstatus auf der WANOP-Appliance aktiviert ist.
- Stellen Sie sicher, dass die im Netzwerk installierte Firewall die WANOP TCP-Optionen nicht entfernt.
- Stellen Sie sicher, dass eine gültige WANOP-Plug-In-Lizenz auf der WANOP-Appliance installiert ist.
- Stellen Sie sicher, dass die Konfiguration der Signalkanalquellenfilterung die IP-Adresse der Clientquelle nicht blockiert.
- Wenn Sie die LAN-Erkennung aktiviert haben, stellen Sie sicher, dass die RoundTrip-Zeit zwischen dem WANOP-Plug-In und der WANOP-Appliance ein akzeptabler Wert ist.

- **Problem:** Bei einer WANOP 4000-Appliance kann ich das WANOP-Plug-In nicht deaktivieren.

Ursache: Dies ist ein bekanntes Problem.

Auflösung: Keine. Sie können das WANOP-Plug-In auf einer WANOP 4000-Appliance nicht deaktivieren.

- **Problem:** Beim Herstellen einer Verbindung mit der WANOP-Appliance mithilfe des WANOP-Plug-Ins wird der folgende Fehlermeldungseintrag auf der Registerkarte Warnungen protokolliert:

Mehr WANOP-Plug-Ins als das aktuelle Limit von <Number> haben versucht, eine Verbindung zu dieser Appliance herzustellen.

Ursache: Die Anzahl der Verbindungen mit der WANOP-Appliance hat das Limit für lizenzierte Benutzer überschritten.

Lösung: Warten Sie entweder, bis ein Benutzer die Verbindung getrennt hat, oder beenden Sie eine Verbindung.

- **Problem:** Falsche Signalisierungs-IP-Adresse ist auf einer WANOP 4000- oder 5000-Appliance konfiguriert.

Lösung: Führen Sie folgende Schritte aus, um die Signalisierungs-IP-Adresse auf einer WANOP 4000- oder 5000-Appliance zu aktualisieren:

1. Melden Sie sich bei der NetScaler Instanz der WANOP-Appliance an.
 2. Navigieren Sie zur Seite Traffic Management > Load Balancing > Virtuelle Server > BR_LB_VIP_SIG.
 3. Aktualisieren Sie die signalisierende IP-Adresse.
 4. Speichern Sie die Konfiguration.
- **Problem:** CIFS- und ICA-Verkehr wird nicht beschleunigt.
- Lösung:** Um dieses Problem zu beheben, führen Sie die folgenden Schritte zur Fehlerbehebung durch:
- Stellen Sie sicher, dass Beschleunigungsregeln für IP-Adresse und Portnummern für das WANOP-Plug-In korrekt definiert sind.
 - Stellen Sie sicher, dass CIFS- oder ICA-Verbindungen hergestellt werden, nachdem die Signalverbindung erfolgreich war.
 - Überprüfen Sie die Beschleunigungsrichtlinie für die verwendete Serviceklasse.

SMB 3.1.1 Anschluss

May 10, 2021

Das SMB-Protokoll (Server Message Block) ist ein Netzwerk-Dateifreigabeprotokoll. Die Nachrichtepakete, die eine bestimmte Version des Protokolls definieren, werden als Dialekt bezeichnet. Das Common Internet File System (CIFS) Protocol ist ein Dialekt von SMB.

In Citrix SD-WAN Version 10 Version 1 wird das SMB 3.1.1-Protokoll auf den Plattformen Citrix SD-WAN WANOP und Premium Edition eingeführt.

Citrix SD-WAN WANOP unterstützt SMB 3.1.1-Verbindungen. Die SMB 3.1.1-Verbindungen sind anwendbar, wenn der Client Windows 10 ist und der Server Windows Server 2016 ist.

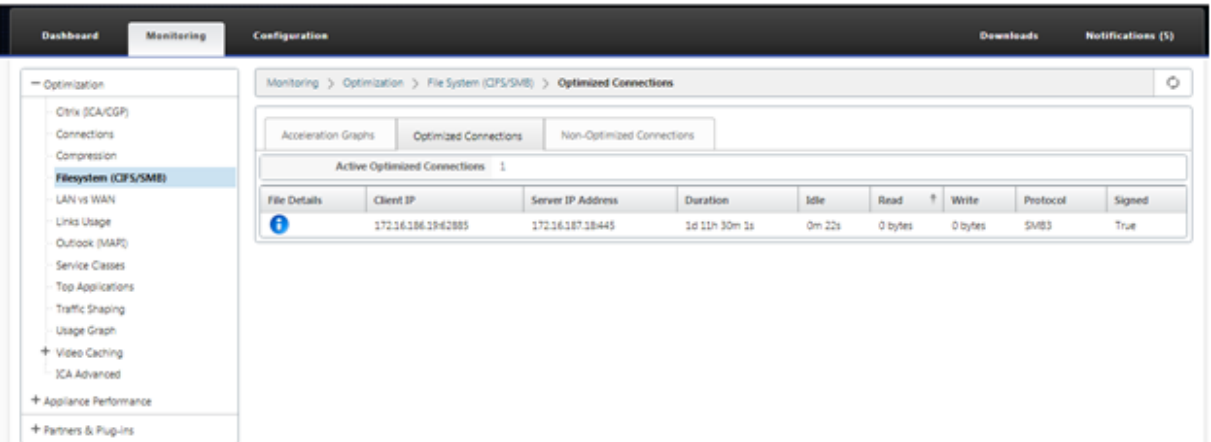
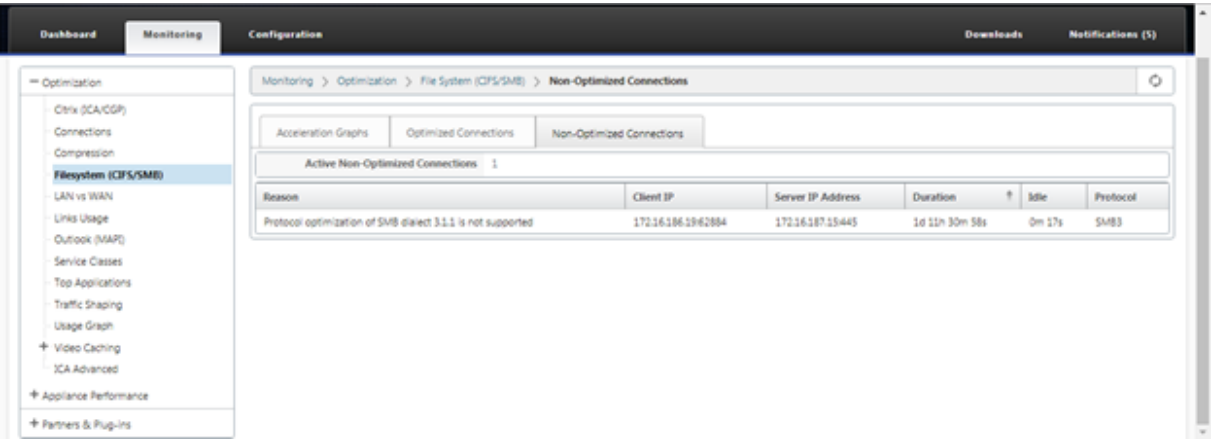
Wenn SMB 3.1.1-Datenverkehr das WANOP-Modul durchläuft:

- Es ist gezählt/sichtbar als Teil von SMB 3.1 CIFS unoptimierten Verbindungen
- Die folgende Ablaufverfolgungsmeldung wird angezeigt: “Diese Verbindung als SMB 3.1.1 wird nicht unterstützt”.

| Client | Server | SMB-Version |
|-------------|------------------|------------------|
| Windows 10 | Win 2016, 2012R2 | SMB 3.1.1, 3.0.2 |
| Windows 8.1 | SMB 3.0 | SMB 3.0 |
| Windows 7 | SMB 3.0 | SMB 3.0 |

Für nicht optimierte Verbindungen zeigt die Benutzeroberfläche der Citrix SD-WAN WANOP Appliance eine Meldung für SMB 3.1.1 an.

Navigieren Sie in der Benutzeroberfläche der Citrix SD-WAN WANOP Appliance zu **Überwachung > Dateisystem (CIFS/SMB)** . Klicken Sie auf die Registerkarte **Nicht optimierte Verbindungen**, die folgende Meldung wird angezeigt, *Protokolloptimierung des SMB-Dialekts 3.1.1 wird nicht unterstützt*. Es sind keine Protokolleinträge verfügbar, und es ist keine neue Konfiguration in SD-WAN WANOP erforderlich, um dies zu unterstützen.



Anleitungen

May 10, 2021

In den Anleitungen wird das Verfahren zum Konfigurieren der unterstützten Features von Citrix SD-WAN beschrieben. Diese Artikel enthalten Informationen über einige der folgenden wichtigen Funktionen:

Klicken Sie unten auf einen Feature-Namen, um die Liste der Anleitungen für dieses Feature anzuzeigen.

- [Virtuelles Routing und Weiterleitung](#)
- [Aktivieren von RED für QoS Fairness](#)
- [Konfiguration](#)
- [Dynamisches Routing](#)
- [DHCP-Server und DHCP-Relay](#)
- [Routenfilter](#)
- [IPsec-Beendigung und Überwachung](#)
- [Secure Web Gateway](#)
- [QoS](#)
- [FIPS-konformer Betrieb —IPsec-Tunnel](#)
- [Dynamische NAT-Konfiguration](#)
- [Adaptive Bandbreitenerkennung](#)
- [Aktive Bandbreitentests](#)
- [BGP-Erweiterungen](#)
- [Dienstklassenzuordnung mit SSL-Profilen](#)
- [Sicheres Peering und manuelles Secure Peering](#)
- [Zero Touch-Bereitstellung](#)
- [Bereitstellung im Zwei-Box-Modus](#)

Schnittstellengruppen

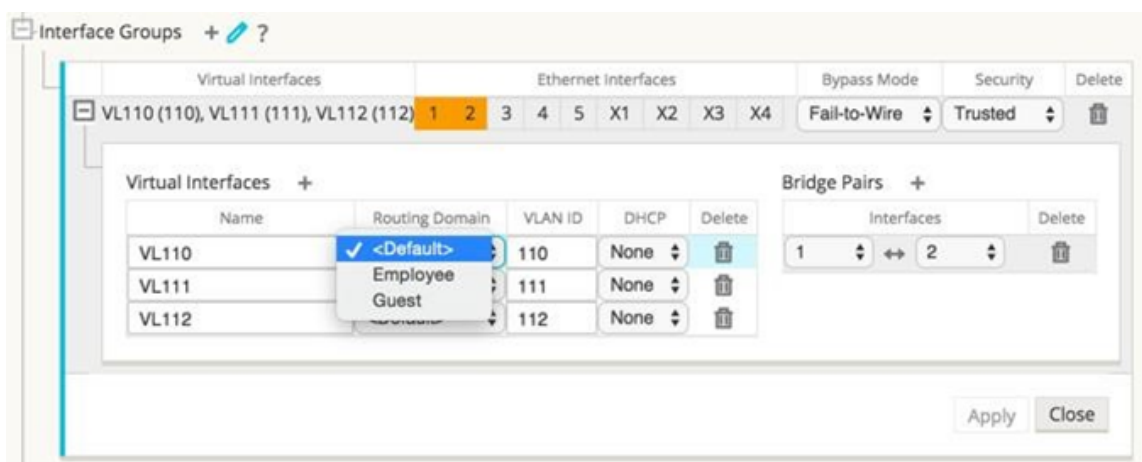
May 10, 2021

So konfigurieren Sie Schnittstellengruppen:

1. Navigieren Sie im **Konfigurations-Editor** zu **Sites** > **[Client-Sitenname]** > **Schnittstellengruppen**, und wählen Sie beim Konfigurieren virtueller Schnittstellen eine **Routingdomäne** aus dem Dropdownmenü aus. Ausführliche Anweisungen finden Sie unter [Konfigurieren von Schnittstellengruppen](#).

Hinweis

Nachdem virtuelle Schnittstellen einer bestimmten Routingdomäne zugeordnet sind, stehen nur diese Schnittstellen zur Verfügung, wenn diese Routingdomäne verwendet wird.



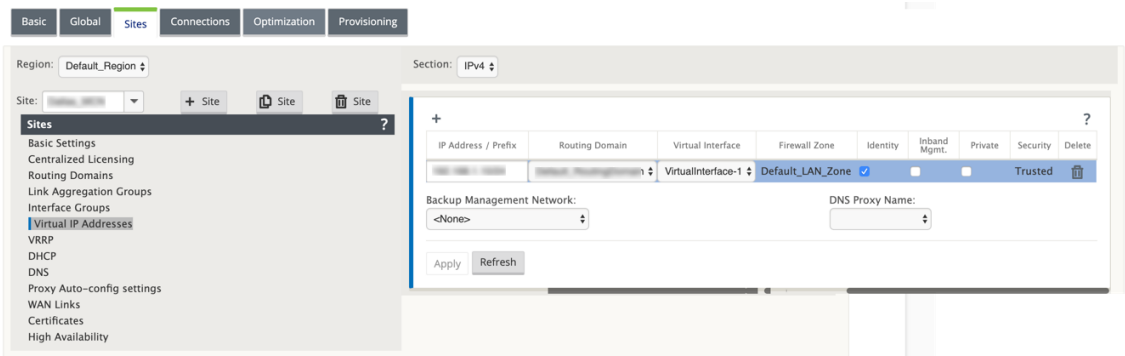
Konfigurieren der Identität virtueller IP-Adresse

May 10, 2021

Virtuelle Netzwerkschnittstelle kann mehrere IP-Adressen in gleichen oder verschiedenen Subnetzen hosten. Sie können jedoch nur eine virtuelle IP mit der Identität auf true festlegen, die für dynamische Routingprotokolle wie BGP/OSPF, DHCP-Server/Relay und In-Band-Verwaltung verwendet werden kann.

So konfigurieren Sie die Identität der virtuellen IP-Adresse:

1. Navigieren Sie im **Konfigurations-Editor** zu **Sites** > **[Site-Name]** > **Virtuelle IP-Adressen**.
2. Aktivieren Sie das Kontrollkästchen **Identität** für eine virtuelle IP-Adresse, um sie für IP-Dienste zu verwenden.



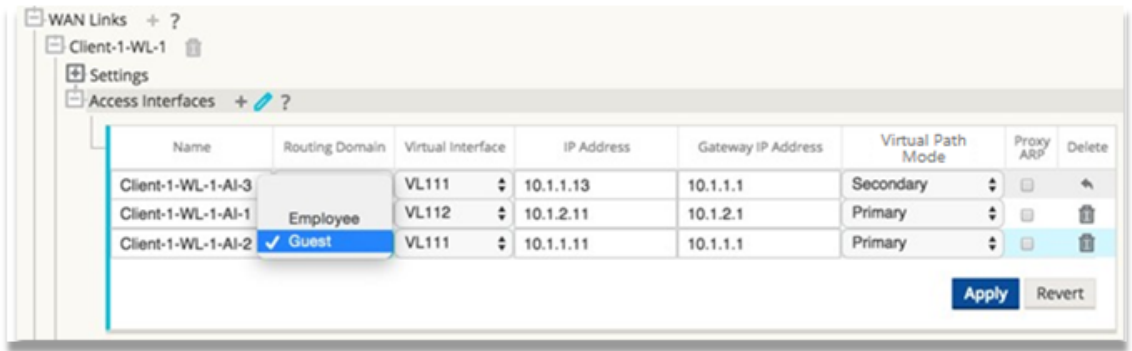
Konfigurieren der Zugriffsoberfläche

September 26, 2023

So konfigurieren Sie die Zugriffsoberfläche:

1. Navigieren Sie im **Konfigurations-Editor** zu **Standorte** > **[Client-Sitenname]** > **WAN-Links** > **[WAN-Linkname]** > **Zugriffsschnittstellen**.
2. Wählen Sie eine **Routingdomäne** aus dem Dropdownmenü, wenn Sie eine Access-Schnittstelle konfigurieren.

Ausführliche Anweisungen finden Sie im Abschnitt **Konfigurieren der Zugriffsoberfläche** im Thema [MCN konfigurieren](#).



Virtuelle IP-Adressen konfigurieren

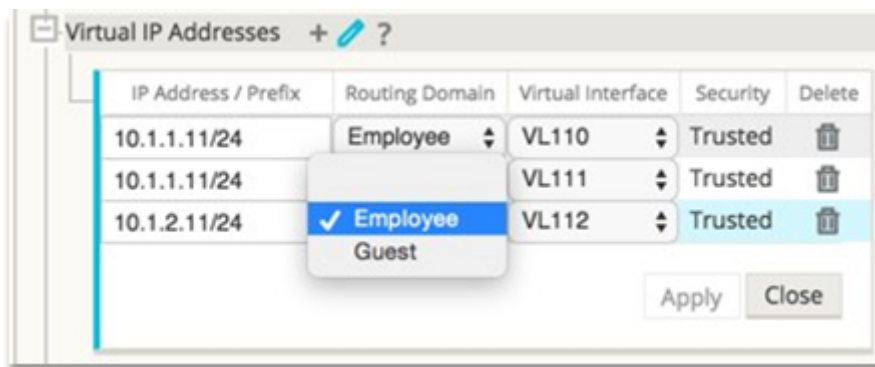
May 10, 2021

So konfigurieren Sie virtuelle IP-Adressen:

1. Navigieren Sie im **Konfigurations-Editor** zu **Sites > [Client-Sitenname]> Virtuelle IP-Adressen**.
2. Wählen Sie eine **Routingdomäne** aus dem Dropdownmenü, wenn Sie virtuelle IP-Adressen konfigurieren.

Ausführliche Anweisungen finden Sie unter [Konfigurieren von virtuellen IP-Adressen](#).

Die von Ihnen gewählte Routingdomäne legt fest, welche virtuellen Schnittstellen im Dropdownmenü verfügbar sind.



GRE Tunnel konfigurieren

May 10, 2021

So konfigurieren Sie GRE Tunnel:

1. Navigieren Sie im Konfigurations-Editor zu **Verbindungen > Standort> GRE Tunnel**. Die Quell-IP-Adresse kann nur auf vertrauenswürdigen Links aus der virtuellen Netzwerkschnittstelle ausgewählt werden.
2. Geben Sie einen Namen für den GRE Tunnel ein.
3. Wählen Sie die **Quell-IP-Adresse** aus dem Dropdownmenü aus. Die Routingdomäne bestimmt, welche Quell-IP-Adressen im Dropdownmenü verfügbar sind.
4. (Optional) Wählen Sie die **Public Source IP** aus. Dieses Feld kann leer sein, wenn diese Adresse mit der Quell-IP übereinstimmt.
5. Geben Sie die **Ziel-IP-Adresse** des GRE Tunnels ein.
6. Geben Sie die **IP/Präfix-Adresse** des GRE Tunnels ein.
7. Klicken Sie auf **Prüfsumme**, wenn Sie Prüfsumme im GRE Tunnel Header verwenden möchten.

8. Geben Sie einen Wert für die **Keepalive-Periode** in Sekunden ein. Wenn Sie 0 konfigurieren, wird kein Keepalive-Paket übertragen, aber der GRE Tunnel wird aktiv sein.
9. Geben Sie einen Wert für die **Keepalive-Wiederholungen ein**. Dieser Wert bestimmt, wie oft die Keepalive-Wiederholungsversuche durchgeführt werden, bevor die SD-WAN-Appliance den GRE-Tunnel deaktiviert.

Weitere Informationen finden Sie [GRE-Tunnel konfigurieren](#) auf der MCN-Website.

| Name | Source IP | Public Source IP | Destination IP | Tunnel IP / Prefix | Checksum | Keepalive Period (s) | Keepalive Retries | Delete |
|--------------------|-----------|------------------|----------------|--------------------|----------|----------------------|-------------------|--------|
| Appliance-Tunnel-1 | * | | * | * | MD5 | 10 | 3 | |

Apply Revert

Weitere Informationen zum Sichern von Web-Gateway mit GRE-Tunneln finden Sie unter; [Secure Web Gateway](#)

Dynamische Pfade für Zweigkommunikation einrichten

May 10, 2021

Angesichts der Nachfrage nach VoIP- und Videokonferenzen bewegt sich der Verkehr zunehmend zwischen Büros. Es ist ineffizient, vollständige Netzverbindungen über Rechenzentren einzurichten, was zeitaufwändig sein kann.

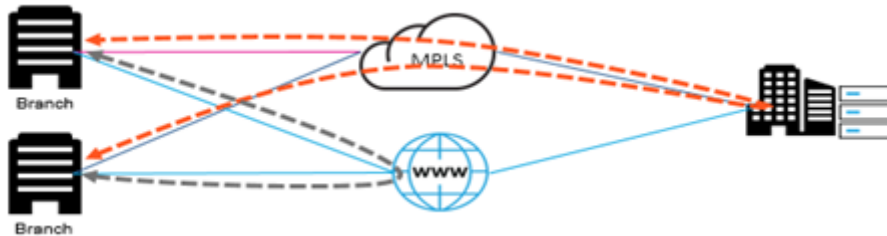
Mit Citrix SD-WAN müssen Sie nicht die Pfade zwischen jedem Büro konfigurieren. Sie können die Funktion Dynamischer Pfad aktivieren, und die SD-WAN-Lösung erstellt automatisch Pfade zwischen Büros bei Bedarf. Die Sitzung verwendet zunächst einen vorhandenen festen Pfad. Und wenn Bandbreite und Zeitschwelle erreicht sind, wird ein Pfad dynamisch erstellt, wenn dieser neue Pfad bessere Leistungsmerkmale aufweist als der feste Pfad. Der Sitzungsverkehr wird über den neuen Pfad übertragen. Dies führt zu einer effizienten Ressourcennutzung. Pfade existieren nur dann, wenn sie benötigt werden, und reduzieren den Datenverkehr, der vom und zum Rechenzentrum übertragen wird.

Weitere Vorteile des SD-WAN-Netzwerks sind:

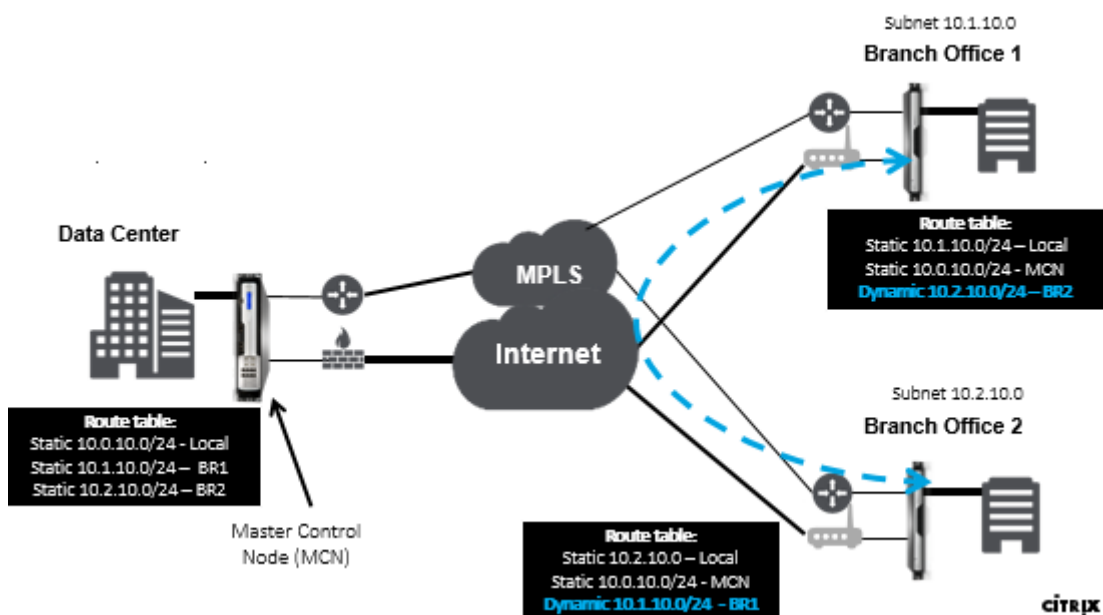
- Bandbreiten- und PPS-Schwellenwerte für Zweigverbindungen
- Reduzierung der Bandbreitenanforderungen im Rechenzentrum und außerhalb des Rechenzentrums bei minimaler Latenz
- Pfade, die nach Bedarf erstellt werden, hängen von festgelegten Schwellenwerten ab
- Dynamische Freigabe von Netzwerkressourcen, wenn nicht erforderlich

- Reduzierung der Belastung des Master-Kontrollknotens und der Latenz

Kommunikation von Zweig zu Zweig mithilfe dynamischer virtueller Pfade:



SD-WAN-Netzwerk mit dynamischem Pfad:

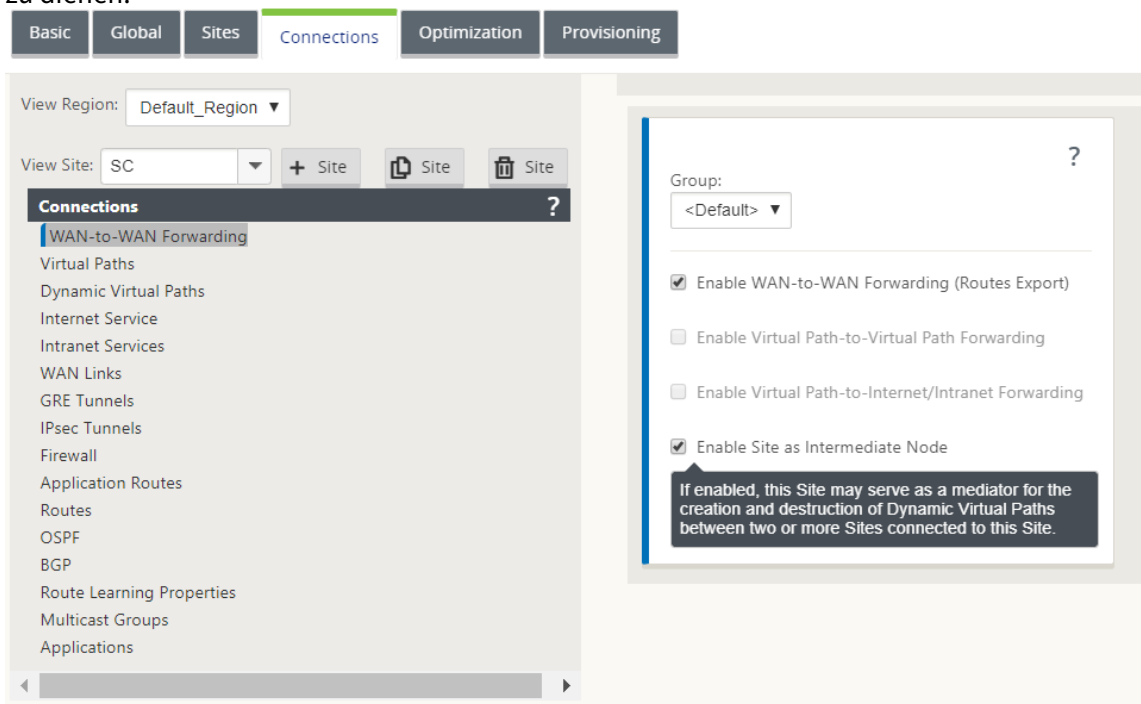


- Dynamische virtuelle Pfade werden für große Bereitstellungen wie Unternehmen verwendet.
- Kleinere Bereitstellungen verwenden statische virtuelle Pfade und beliebige virtuelle Pfade
- Verwenden Sie immer statische virtuelle Pfade zwischen zwei Rechenzentren (DC zu DC)
- Nicht alle WAN-Pfade müssen für die Verwendung des dynamischen virtuellen Pfads konfiguriert werden
- Jede SD-WAN-Appliance verfügt über eine begrenzte Anzahl dynamischer virtueller Pfade (8 dynamisch niedrigste Grenze, 8 statische niedrigste Grenze = insgesamt 16), die konfiguriert werden können.

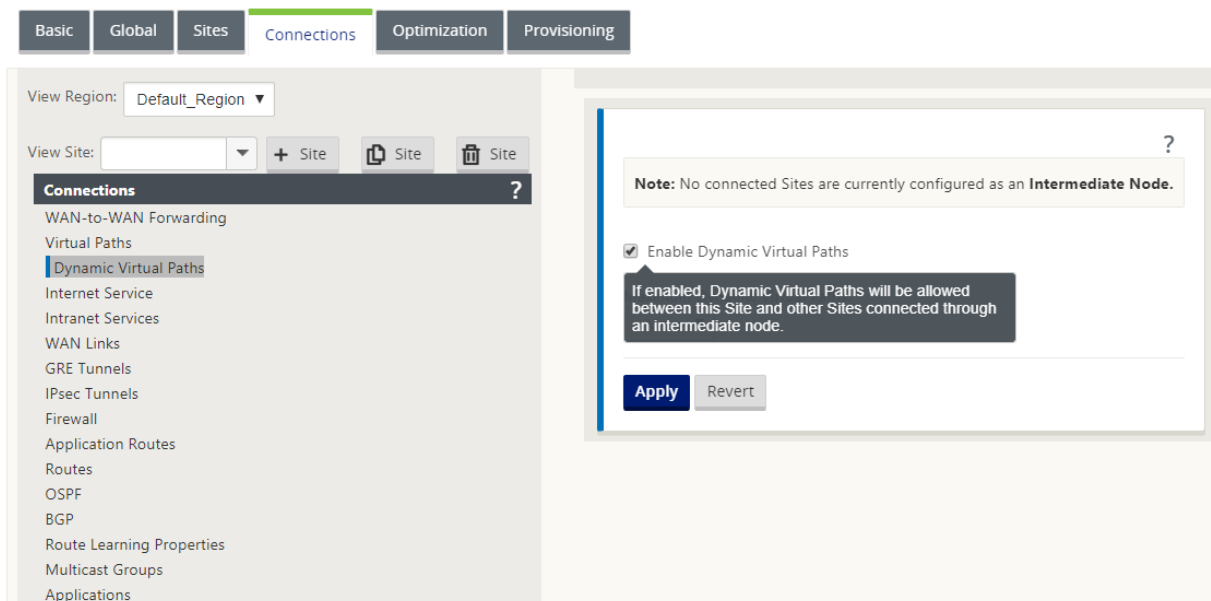
So aktivieren Sie dynamischen virtuellen Pfad in der SD-WAN-GUI

So aktivieren Sie dynamische virtuelle Pfade:

1. Erstellen Sie in der Citrix SD-WAN GUI im Bereich **Verbindungen** eine WAN-zu-WAN-Weiterleitungsgruppe.
2. Navigieren Sie zu **Verbindungen > [Client-Standortname] > WAN-zu-WAN-Weiterleitung**.
3. Aktivieren Sie **WAN to WAN Forwarding**, damit die Site als Proxy für die Multi-Hop-Site dienen kann.
4. **Site als Zwischenknoten** aktivieren
5. Navigieren Sie zu **Verbindungen > Remotestandort > WAN-zu-WAN-Weiterleitung**.
6. Aktivieren Sie die WAN-zu-WAN-Weiterleitung, um die Site als Proxy für Multi-Hop-Site an Site zu dienen.

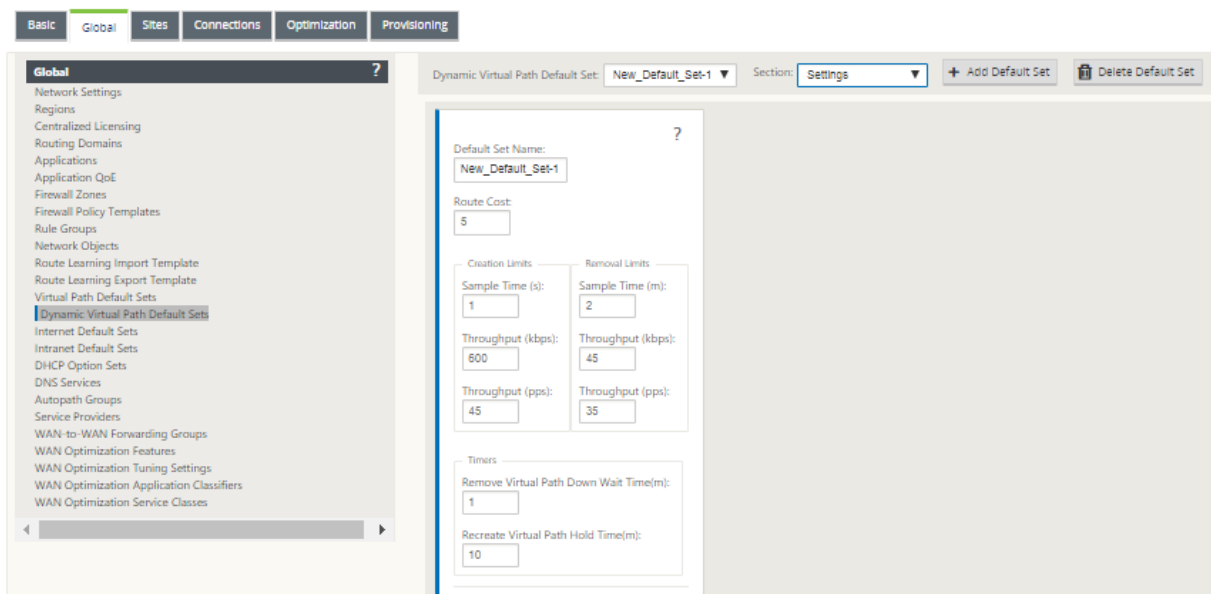


7. Navigieren Sie zu **Verbindungen > Remotestandort > Virtueller Pfad > Dynamischer virtueller Pfad**.
8. Aktivieren Sie **dynamische virtuelle Pfade**.
9. Legen Sie die maximale Anzahl dynamischer Pfade fest.



So erstellen Sie einen dynamischen virtuellen Pfad

- Die Konfiguration bestimmt, wann ein dynamischer virtueller Pfad aktiv oder heruntergefahren ist.
- Konfigurieren Sie die Anzahl der Beispielpakete (pps) oder Bandbreite (kbps) innerhalb eines Zeitrahmens.
- Kann global oder mit WAN-Link am Intermediate Node konfiguriert werden.



Wan-zu-WAN-Weiterleitung

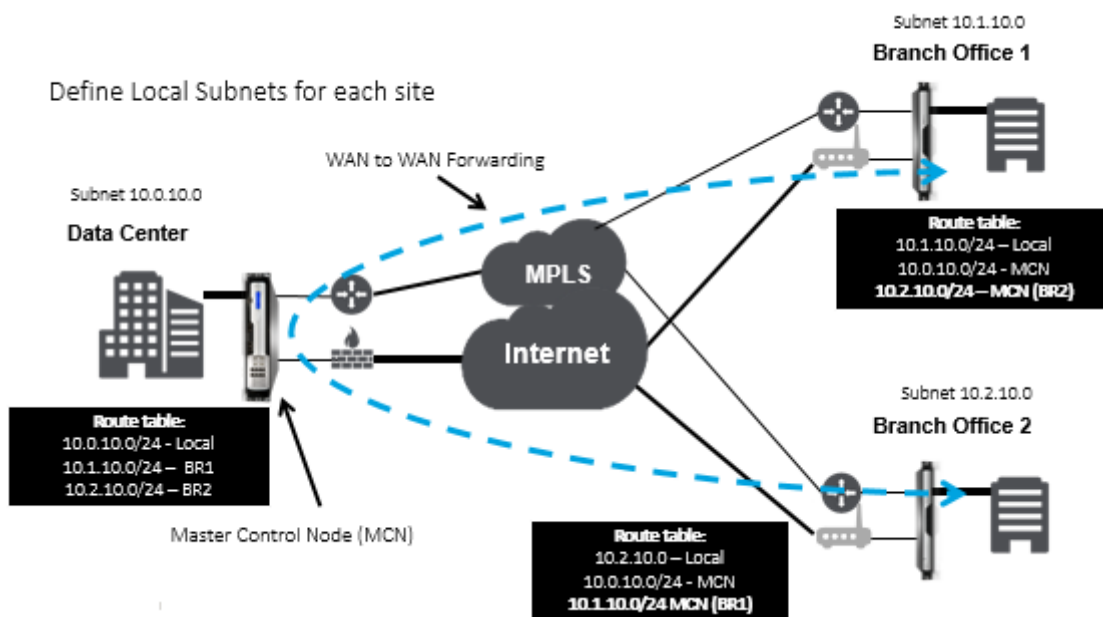
May 10, 2021

Das Aktivieren der WAN-zu-WAN-Weiterleitung auf dem MCN ermöglicht es dem MCN, Routen für Remote-Standorte anzukündigen.

- Kunden kennen die lokalen Routen von MCN und anderen Routen des Clientstandorts
- Aus Kundensicht werden alle Routen als MCN-Routen betrachtet

Wenn die WAN-zu-WAN-Weiterleitung auf dem MCN nicht aktiviert ist, treten im Kundennetzwerk Probleme mit der Kommunikation von Zweig zu Zweig auf.

Appliances, die im Clientmodus ausgeführt werden, kennen andere Zweigsubnetze nicht, bis die WAN-zu-WAN-Weiterleitung im MCN aktiviert ist. Wenn Sie diese Option aktivieren, werden die SD-WAN-Knoten der Zweigstelle auf andere Zweigsubnetze aufmerksam. Der Verkehr, der zu anderen Zweigstellen bestimmt ist, wird an MCN weitergeleitet. MCN leitet es zum richtigen Ziel.



Überwachung und Fehlerbehebung

May 10, 2021

Sie können die Webverwaltungsschnittstelle der Citrix SD-WAN -Appliance verwenden, um unterstützte Funktionen zu überwachen und zu beheben. Im Folgenden finden Sie die Links zu den Themen Überwachung und Problembehandlung für Citrix SD-WAN Appliances.

[Virtuelles WAN überwachen](#)

[Statistische Informationen anzeigen](#)

[Anzeigen von Flussinformationen](#)

[Anzeigen von Berichten](#)

[Firewall-Statistiken anzeigen](#)

[Diagnosetool](#)

[Verbesserte Pfadzuordnung und Bandbreite](#)

[Fehlerbehebung bei Management-IP](#)

[Aktive Bandbreitentests](#)

[Adaptive Bandbreitenerkennung](#)

Virtuelles WAN überwachen

May 10, 2021

Grundlegende Informationen für eine Appliance anzeigen

Verwenden Sie einen Browser, um eine Verbindung mit der Managementoberfläche der Appliance herzustellen, die Sie überwachen möchten, und klicken Sie auf die Registerkarte **Dashboard**, um grundlegende Informationen für diese Appliance anzuzeigen.

Auf der Seite **Dashboard** werden die folgenden grundlegenden Informationen für die lokale Appliance angezeigt:

Systemstatus:

- **Name** —Dies ist der Name, den Sie der Appliance zugewiesen haben, als Sie sie dem System hinzugefügt haben.
- **Modell** —Dies ist die Modellnummer der virtuellen WAN-Appliance.
- **Einheitenmodus** —Gibt an, ob diese Appliance als primärer oder sekundärer MCN oder als Client-Appliance konfiguriert wurde.
- **Verwaltungs-IP-Adresse** — Dies ist die Verwaltungs-IP-Adresse für die Appliance.
- **Betriebszeit der Appliance** — Gibt die Dauer an, für die die Appliance seit dem letzten Neustart ausgeführt wurde.

- **Dienstverfügbarkeit** —Gibt die Dauer an, für die der virtuelle WAN-Dienst seit dem letzten Neustart ausgeführt wurde.

Status des virtuellen Pfaddiensts:

[Name der virtuellen Pfad-Site]—Zeigt den Status aller virtuellen Pfade an, die dieser Appliance zugeordnet sind. Wenn der Virtual WAN-Dienst aktiviert ist, ist dieser Abschnitt auf der Seite enthalten. Wenn der virtuelle WAN-Dienst deaktiviert ist, werden anstelle dieses Abschnitts ein Warnsymbol (Goldrute-Delta) und eine entsprechende Warnmeldung angezeigt.

Lokale Versionsinformationen:

- **Softwareversion** — Dies ist die Version des Softwarepakets CloudBridge Virtual Path, das derzeit auf der Appliance aktiviert ist.
- **Build on** —Dies ist das Builddatum für die Produktversion, die derzeit auf der lokalen Appliance ausgeführt wird.
- **Hardware-Version** —Dies ist die Hardware-Modellnummer und Version der Appliance.
- **Version der Betriebssystempartition** — Dies ist die Version der Betriebssystempartition, die derzeit auf der Appliance aktiv ist.

Die folgende Abbildung zeigt eine Beispielseite für das Dashboard.

| Dashboard | Monitoring | Configuration |
|---|------------|---------------|
| System Status | | |
| Name: MCN_23 Model: VPX Sub-Model: BASE Appliance Model: MCN Serial Number: 67e0772c-5190-a2ee-d183-9244189b30a0 Management IP Address: 10.102.78.154 Appliance Uptime: 6 days, 13 hours, 22 minutes, 23.0 seconds Service Uptime: 6 days, 13 hours, 14 minutes, 46.0 seconds Routing Domain Enabled: Default_RoutingDomain | | |
| Local Versions | | |
| Software Version: 10.1.0.111.690027 Built On: Jun 21 2018 at 23:42:30 Hardware Version: VPX OS Partition Version: 4.6 | | |
| Virtual Path Service Status | | |
| Virtual Path MCN_23-Site1: Uptime: 6 days, 13 hours, 11 minutes, 45.0 seconds. | | |

Statistische Informationen anzeigen

May 10, 2021

Dieser Abschnitt enthält grundlegende Anweisungen zum Anzeigen von Virtual WAN-Statistikinformationen.

1. Melden Sie sich bei der Managementoberfläche für den MCN an.

2. Wählen Sie die Registerkarte **Überwachung**.

Dadurch wird die Navigationsstruktur **Überwachung** im linken Fensterbereich geöffnet. Standardmäßig wird auch die Seite **Statistiken** angezeigt, auf der im Feld **Anzeigen** vordefinierte **Pfade** angezeigt werden. Diese enthält eine detaillierte Tabelle der Pfadstatistiken.

Hinweis

Wenn Sie zu einer anderen Seite **Überwachung** navigieren (z. B. **Flows**), können Sie zu dieser Seite zurückkehren, indem Sie im Navigationsbaum **Überwachung** (linker Bereich) die Option **Statistik** auswählen.

| Num | From Link | To Link | Path State | Virtual Path Service State | Virtual Path Service Type | BOWT | Jitter (mS) | Loss % | kbps | Congestion |
|-----|--------------|--------------|------------|----------------------------|---------------------------|------|-------------|--------|-------|------------|
| 1 | MCN-DC-WL-1 | Branch1-WL-1 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 59.95 | NO |
| 2 | MCN-DC-WL-1 | Branch1-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.72 | NO |
| 3 | MCN-DC-WL-2 | Branch1-WL-1 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.72 | NO |
| 4 | MCN-DC-WL-2 | Branch1-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 11.82 | NO |
| 5 | Branch1-WL-1 | MCN-DC-WL-1 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.89 | NO |
| 6 | Branch1-WL-1 | MCN-DC-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 25.19 | NO |
| 7 | Branch1-WL-2 | MCN-DC-WL-1 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 11.84 | NO |
| 8 | Branch1-WL-2 | MCN-DC-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.73 | NO |

Mit Version 11.1.0 wird die NDP-Option (Neighbor Discovery Protocol) zum Debuggen von Neighbor Discovery-Problemen hinzugefügt.

1. Wählen Sie die NDP-Option aus dem Dropdownmenü Anzeigen aus, und Sie können den Status von NDP zusammen mit den IPv6-Adressen anzeigen.

| Num | Interface | VLAN | IP Addr | MAC Addr | Type | State | Is Router | Clear NDP Entry |
|-----|-----------|------|-------------------------|-------------------|------------|---------------------|-----------|-----------------|
| 0 | 2 | 0 | 2607:f0d0:2001:a::20 | 02:63:d7:64:85:4e | PERSISTENT | NDP_STATE_REACHABLE | Y | |
| 1 | 2 | 0 | fe80::63:d7ff:fe64:854e | 02:63:d7:64:85:4e | END_USER | NDP_STATE_STALE | N | Clear |

2. Wählen Sie WAN-Link aus dem Dropdownmenü. Sie können die IPv6-Adresse auch anzeigen, wenn Sie auf der Registerkarte IP-Adresse konfiguriert haben.

Statistics

Show: WAN Link

Enable Auto Refresh

 5 seconds

Refresh

Show latest data.

WAN Link Statistics

Filter:

Any column

Apply

Show 100 entries Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

| WAN Link | Access Interface | IP Address | Proxy Address | Proxy ARP State | MAC | Last ARP Reply Age (ms) |
|----------------|---------------------|---------------------|---------------|-----------------|-----|-------------------------|
| demo_cl1_inet | N/A | 2607:fd0:2001:b::10 | N/A | N/A | N/A | N/A |
| demo_cl1_inet2 | N/A | 172.16.100.1 | N/A | N/A | N/A | N/A |
| demo_cl2_inet | N/A | 2607:fd0:2001:c::10 | N/A | N/A | N/A | N/A |
| demo_cl2_inet2 | N/A | 172.16.150.1 | N/A | N/A | N/A | N/A |
| demo_mcn_inet | demo_mcn_inet-AI-1 | 2607:fd0:2001:a::10 | N/A | N/A | N/A | N/A |
| demo_mcn_inet2 | demo_mcn_inet2-AI-1 | 172.16.200.1 | N/A | DISABLED | N/A | N/A |

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

Virtual Path Service Data Rates

Filter:

Any column

Apply

3. Sie können auch die Access Interface-Statistiken anzeigen.

DashboardMonitoringConfiguration

Monitoring > Statistics

Statistics

Show: Access Interfaces

Enable Auto Refresh

 5 seconds

Refresh

Show latest data.

Access Interface Statistics

Filter:

Any column

Apply

Show 100 entries Showing 1 to 2 of 2 entries

First

Previous

1

Next

Last

| WAN Link | Access Interface | IP Address | Proxy Address | Proxy ARP State | MAC | Last ARP Reply Age (ms) |
|----------------|---------------------|---------------------|---------------|-----------------|-----|-------------------------|
| demo_mcn_inet | demo_mcn_inet-AI-1 | 2607:fd0:2001:a::10 | N/A | N/A | N/A | N/A |
| demo_mcn_inet2 | demo_mcn_inet2-AI-1 | 172.16.200.1 | N/A | N/A | N/A | N/A |

Showing 1 to 2 of 2 entries

First

Previous

1

Next

Last

Virtual Path Service Data Rates:

Filter:

Any column

Apply

Show 100 entries Showing 1 to 8 of 8 entries

First

Previous

1

Next

Last

| WAN Link | Access Interface | Service Name | Direction | Virtual Path Service Packets | Virtual Path Service kB | Delta Virtual Path Service Packets | Delta Virtual Path Service kB | Virtual Path Service kbps | IP,TCP,UDP Header Compression Bytes Saved |
|---------------|--------------------|-------------------|-----------|------------------------------|-------------------------|------------------------------------|-------------------------------|---------------------------|---|
| demo_mcn_inet | demo_mcn_inet-AI-1 | demo_mcn-demo_cl2 | Recv | 20220845 | 3240115.88 | 413 | 74.23 | 46.47 | 0 |
| demo_mcn_inet | demo_mcn_inet-AI-1 | demo_mcn-demo_cl1 | Recv | 20196856 | 3252489.44 | 289 | 30.05 | 18.82 | 0 |

4. Öffnen Sie das Drop-down-Menü **Anzeigen**.

Neben den **Statistiken**Pfade, NDP, Access Interfaceund **WAN-Links**bietet das Menü **Anzeigen** auch mehrere weitere Optionen zum Filtern und Anzeigen statistischer Informationen.

Statistics

Flows

Routing Protocols

Firewall

IKE/Psec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRPP Protocol

Monitoring > Statistics

Statistics

Show: Paths (Summary) ☐ Enable Auto Refresh 5 seconds Refresh ☒ Show latest data.

Filter

Access Interfaces

Applications

Classes

Virtual Path Services

Ethernet

Ethernet MAC Learning

Intranet

New Observed Protocols

Paths (Summary)

Paths (Detailed)

Routes

Application Routes

Application QoS

Rules

Rule Groups

Site

WAN Link

MPLS Queues

WAN Link Usage

Path column

Apply

Show 100 entries

| | To Link | Path State | Virtual Path Service State | Virtual Path Service Type | BOWT | Jitter (mS) | Loss % | kbps | Congestion |
|---|--------------|------------|----------------------------|---------------------------|------|-------------|--------|-------|------------|
| 1 | Branch1-WL-1 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 59.95 | NO |
| 2 | Branch1-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.72 | NO |
| 3 | Branch1-WL-1 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.72 | NO |
| 4 | Branch1-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 11.82 | NO |
| 5 | MCN-DC-WL-1 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.89 | NO |
| 6 | MCN-DC-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 25.19 | NO |
| 7 | Branch1-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 11.84 | NO |
| 8 | Branch1-WL-2 | GOOD | GOOD | Static | 2 | 3 | 0.00 | 8.73 | NO |

Showing 1 to 8 of 8 entries

Sandwidth calculated over the last 41278.42 seconds

First

Previous

1

Next

Last

Wählen Sie im Menü **Anzeigen** einen Filter aus, um eine Tabelle mit statistischen Informationen für dieses Thema anzuzeigen.

Anzeigen von Flussinformationen

May 10, 2021

Dieser Abschnitt enthält grundlegende Anweisungen zum Anzeigen von Virtual WAN-Flussinformationen.

Gehen Sie folgendermaßen vor, um Flussinformationen anzuzeigen:

1. Melden Sie sich bei der Managementoberfläche für den MCN an, und wählen Sie die Registerkarte **Überwachung** . Es öffnet die **Monitoring-Navigationsstruktur** im linken Bereich.

2. Wählen Sie im Navigationsbaum den Zweig **Flows** aus. Es zeigt die Seite “**Flows** “mit **LAN zu WAN an**, die im Feld “**Flow-Typ** “vorausgewählt ist.

Statistics

Flows

Routing Protocols

Firewall

IKE/Psec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRPP Protocol

Monitoring > Flows

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display: 50

Filter (Optional): Help

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

Toggle Columns

| Source IP Address | Dest IP Address | Direction | Source Port | Dest Port | IPP | IP DSCP | Hit Count | Service Type | Service Name | LAN GW IP | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type |
|-------------------|-----------------|------------|-------------|-----------|-----|---------|-----------|--------------|----------------|-----------|----------|---------|-------|-------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|
| 172.147.21.53 | 172.147.12.83 | LAN to WAN | 2312 | 50829 | TCP | default | 3 | Virtual Path | MCN-DC-Branch1 | LOCAL | 5292 | 2 | 104 | 0.237 | 0.099 | 0.100 | 0.000 | 65 | N/A | 13 | INTERACT |
| 172.147.12.83 | 172.147.21.53 | WAN to LAN | 50829 | 2312 | TCP | default | 3 | Virtual Path | MCN-DC-Branch1 | LOCAL | 5328 | 3 | 180 | 0.355 | 0.170 | 0.151 | 0.000 | 132 | N/A | N/A | I |

Total LAN to WAN flows displayed: 1 out of 1

Total WAN to LAN flows displayed: 1 out of 1

3. Wählen Sie den **Flow-Typ**aus. Das Feld **Flow-Art** befindet sich im Abschnitt **Flows auswählen** oben auf der Seite **Flows** . Neben dem Feld “**Flow-Typ** “befindet sich eine Reihe von Kontrollkästchens zur Auswahl der Flussinformationen, die Sie anzeigen möchten. Sie können ein oder mehrere Kontrollkästchens aktivieren, um die anzuzeigenden Informationen zu filtern.

- 4. Wählen Sie im Dropdownmenü neben **diesem Feld die Option Max. Flows, die angezeigt** werden sollen.
- 5. Sie bestimmt die Anzahl der Einträge, die in der Tabelle **Flows** angezeigt werden sollen. Die Optionen sind: **50, 100, 1000**.
- 6. (Optional) Geben Sie Suchtext in das Feld **Filter** ein. Es filtert die Tabellenergebnisse so, dass nur Einträge, die den Suchtext enthalten, in der Tabelle angezeigt werden.

Tipp

Um detaillierte Anweisungen zur Verwendung von Filtern zum Verfeinern der Ergebnisse der **Flow-Tabelle** anzuzeigen, klicken Sie rechts neben dem Feld **Filter** auf **Hilfe**. Um die Hilfeanzeige zu schließen, klicken Sie unten links im Abschnitt **Flows auswählen** auf **Aktualisieren**.

- 7. Klicken Sie auf **Aktualisieren**, um die Filterergebnisse anzuzeigen. Die Abbildung zeigt eine gefilterte Beispielanzeige der **Flows-Seite** mit allen ausgewählten Flow-Typen.

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☒ Internet Load Balancing Table

☒ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

172.79.2.83

Help

Refresh

Flows Data

Toggle Columns

Both LAN to WAN and WAN to LAN Flows

| Source IP Address | Dest IP Address | Direction | Source Port | Dest Port | IPP | IP DSCP | Hit Count | Service Type | Service Name | LAN GW IP | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps |
|-------------------|-----------------|------------|-------------|-----------|-----|---------|-----------|--------------|--------------|-----------|----------|---------|---------|-------|---------------|----------------------------|
| 172.79.2.83 | 172.79.1.42 | LAN to WAN | 9281 | 58689 | TCP | default | 9577 | Virtual Path | DC-BR | LOCAL | 5332 | 12038 | 1020734 | 0.079 | 0.033 | 0.031 |
| 172.79.2.83 | 172.79.1.42 | LAN to WAN | 9281 | 58690 | TCP | default | 9631 | Virtual Path | DC-BR | LOCAL | 5346 | 12199 | 1075706 | 0.079 | 0.033 | 0.031 |
| 172.79.1.42 | 172.79.2.83 | WAN to LAN | 58689 | 9281 | TCP | default | 18025 | Virtual Path | DC-BR | LOCAL | 5346 | 18025 | 1294598 | 0.157 | 0.052 | 0.062 |
| 172.79.1.42 | 172.79.2.83 | WAN to LAN | 58690 | 9281 | TCP | default | 18244 | Virtual Path | DC-BR | LOCAL | 5360 | 18244 | 1389118 | 0.157 | 0.052 | 0.062 |

Total LAN to WAN flows displayed: 2 out of 305
Total WAN to LAN flows displayed: 2 out of 305

Internet Load Balancing Flows

| LAN IP | WAN IP | Age (mS) | WAN Link | Flow Count |
|--------|--------|----------|----------|------------|
|--------|--------|----------|----------|------------|

Note: Only the active flows will be displayed and the total number of flows include active and inactive flows.

TCP Terminated Flows

| Source IP Address | Dest IP Address | Source Port | Dest Port | IPP | Age (mS) | From Wan kbps | To Wan kbps | Bytes Pending To LAN | Bytes Pending To WAN | State |
|-------------------|-----------------|-------------|-----------|-----|----------|---------------|-------------|----------------------|----------------------|-------|
|-------------------|-----------------|-------------|-----------|-----|----------|---------------|-------------|----------------------|----------------------|-------|

Total TCP Terminated flows displayed: 0 out of 305

- 8. (Optional) Wählen Sie die Spalten aus, die in die Tabelle aufgenommen werden sollen. Gehen Sie wie folgt vor:
- 9. Klicken Sie auf **Spalten umschalten**. Die Schaltfläche **Spalten umschalten** befindet sich direkt oberhalb der rechten oberen Ecke der Tabelle **Flows**. Es zeigt alle nicht ausgewählten Spalten

an und öffnet ein Kontrollkästchen über jeder Spalte, um diese Spalte auszuwählen oder zu deaktivieren. Deaktivierte Spalten werden ausgegraut angezeigt, wie in der Abbildung gezeigt.

Hinweis

Standardmäßig sind alle Spalten ausgewählt, was dazu führen kann, dass die Tabelle in der Anzeige abgeschnitten wird, wodurch die Schaltfläche **Spalten umschalten** wird. Ist dies der Fall, wird unter der Tabelle eine horizontale Bildlaufleiste angezeigt. Schieben Sie die Bildlaufleiste nach rechts, um den abgeschnittenen Abschnitt der Tabelle anzuzeigen und die Schaltfläche **Spalten umschalten** anzuzeigen. Wenn die Bildlaufleiste nicht verfügbar ist, versuchen Sie, die Breite Ihres Browserfensters zu ändern, bis die Bildlaufleiste angezeigt wird.

Monitoring > Flows

Balancing Table

TCP Termination Table

Apply

| Hit Count | Service Type | Service Name | LAN GW IP | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type |
|-----------|--------------|--------------|-----------|----------|---------|---------|-------|---------------|----------------------------|---------------------|---------|-------|------------|------------------|-----------------------------|---------------------|
| 9598 | Virtual Path | DC-BR | LOCAL | 2435 | 12065 | 1023038 | 0.033 | 0.023 | 0.013 | 0.000 | 12 | 9 | REALTIME | DC-WL-2->BR-WL-1 | N/A | Duplicate, Reliable |
| 9652 | Virtual Path | DC-BR | LOCAL | 2434 | 12226 | 1078010 | 0.033 | 0.023 | 0.013 | 0.000 | 12 | 9 | REALTIME | DC-WL-2->BR-WL-1 | N/A | Duplicate, Reliable |
| 18064 | Virtual Path | DC-BR | LOCAL | 2448 | 18064 | 1297454 | 0.048 | 0.028 | 0.019 | 0.000 | 89 | N/A | N/A | N/A | N/A | Duplicate, Reliable |
| 18283 | Virtual Path | DC-BR | LOCAL | 2447 | 18283 | 1391974 | 0.048 | 0.028 | 0.019 | 0.000 | 89 | N/A | N/A | N/A | N/A | Duplicate, Reliable |

10. Aktivieren Sie ein Kontrollkästchen, um eine Spalte auszuwählen oder die Auswahl aufzuheben.
11. Klicken Sie auf **Übernehmen** (oberhalb der rechten oberen Ecke der Tabelle). Es werden die Auswahloptionen geschlossen und die Tabelle aktualisiert, um nur die ausgewählten Spalten einzubeziehen.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

172.79.2.83

Help

Refresh

Flows Data

Toggle Columns

Both LAN to WAN and WAN to LAN Flows

| Source IP Address | Dest IP Address | Direction | Source Port | Dest Port | Hit Count | Service Type | Service Name | LAN GW IP | Age (mS) | Packets | Bytes |
|-------------------|-----------------|------------|-------------|-----------|-----------|--------------|--------------|-----------|----------|---------|---------|
| 172.79.2.83 | 172.79.1.42 | LAN to WAN | 9281 | 58689 | 9613 | Virtual Path | DC-BR | LOCAL | 12022 | 12084 | 1024626 |
| 172.79.2.83 | 172.79.1.42 | LAN to WAN | 9281 | 58690 | 9667 | Virtual Path | DC-BR | LOCAL | 12040 | 12246 | 1080066 |
| 172.79.1.42 | 172.79.2.83 | WAN to LAN | 58689 | 9281 | 18092 | Virtual Path | DC-BR | LOCAL | 12040 | 18092 | 1299440 |
| 172.79.1.42 | 172.79.2.83 | WAN to LAN | 58690 | 9281 | 18312 | Virtual Path | DC-BR | LOCAL | 12056 | 18312 | 1394758 |

Total LAN to WAN flows displayed: 2 out of 306

Total WAN to LAN flows displayed: 2 out of 306

DPI-Anwendungen im SD-WAN Center

In früheren Versionen können rund 4.000 Anwendungen identifiziert werden, die mit 800 Diensten konfiguriert sind (550 virtuelle Pfade, 256 Intranetdienste). Das Speichern dieser Daten würde sich auf die gesamte Systemleistung auswirken (CPU-Zyklen und Speicherplatz, der zum Speichern der Daten benötigt wird). Es hat auch Auswirkungen, wenn die Berichterstattung über Daten pro Verwendung oder Pfad unterstützt wird.

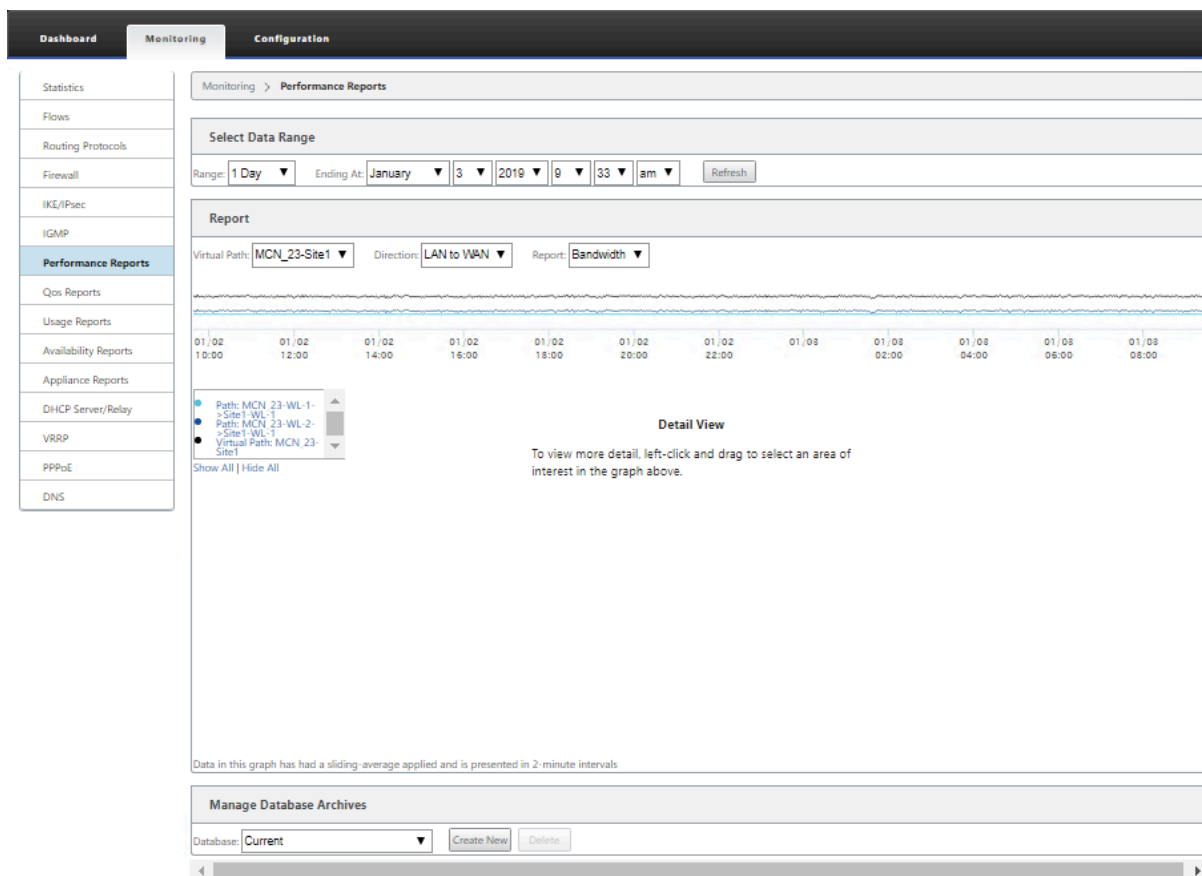
Während der Datenpfad Informationen über jede Anwendung in einer Minute gesammelt, die pro Minute Statistiken Berichterstattung bestimmt die Top 100 Anwendungen und Bericht über das Aggregat aller anderen Anwendungen als andere. Wenn es eine große Vielfalt an verfolgbaren Anwendungen in ihrem Netzwerk gibt, kann dies die Klarheit der Daten beeinträchtigen, insbesondere wenn wir die Nutzung einer Anwendung im Laufe der Zeit verfolgen und die Anwendung unter den Top 100 fällt.

Anzeigen von Berichten

May 10, 2021

Dieser Abschnitt enthält grundlegende Anweisungen zum Generieren und Anzeigen von Virtual WAN-Berichten über die lokale Appliance mithilfe der Managementweboberfläche. Eine Appliance kann

bis zu 30 Archive verwalten und die ältesten Archive löschen, die mehr als 30 Einträge sind.



Hinweis

Berichte, die auf der Managementweboberfläche generiert werden, gelten nur für die lokale Appliance. Verwenden Sie das Virtual WAN Center-Webinterface, um Berichte für das virtuelle WAN zu generieren und anzuzeigen.

Gehen Sie folgendermaßen vor, um Virtual WAN-Berichte zu generieren und anzuzeigen:

1. Melden Sie sich beim Management Web Interface für den MCN an, und wählen Sie die Registerkarte **Überwachung**.

Dadurch wird die Navigationsstruktur **Überwachung** im linken Fensterbereich geöffnet.

2. Wählen Sie im Navigationsbaum einen Berichtstyp aus.

Die Berichtstypen werden im Navigationsbaum direkt unter dem Zweig **Flows** als Zweige aufgeführt.



Folgende Berichtstypen sind verfügbar:

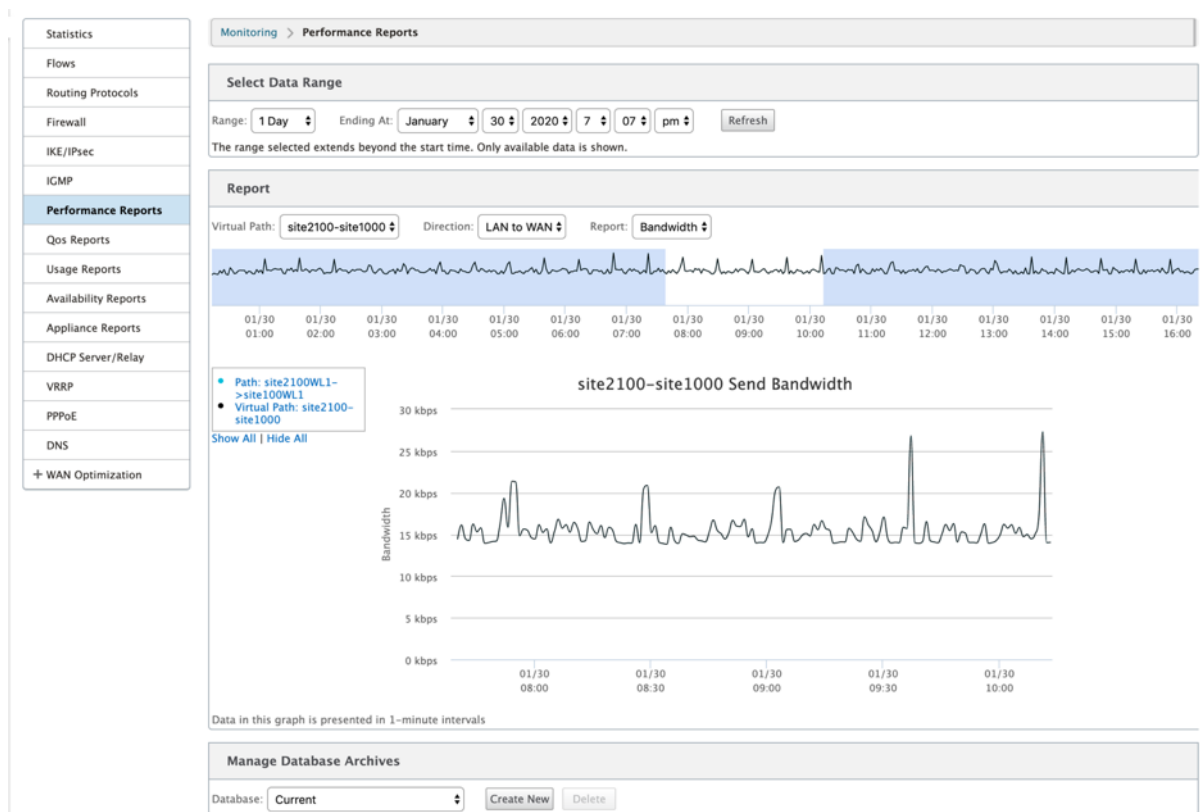
- **Leistungsberichte**
- **QoS-Berichte**
- **Nutzungsberichte**
- **Verfügbarkeitsberichte**
- **Appliance-Berichte**

3. Wählen Sie die Berichtsoptionen aus.

Zusätzlich zu den verschiedenen Berichtstypen gibt es für jeden Berichtstyp zahlreiche Optionen und Filter zur Verfeinerung von Berichtsergebnissen.

Performance-Berichte

Citrix SD-WAN kann Leistungsstatistiken auf Standort-, virtueller Pfad- oder Richtungsebene (LAN zu WAN und WAN zu LAN) anzeigen. Mit Citrix SD-WAN können Sie Metriken erfassen, die die Effizienz der einzelnen Links in Millisekunden anzeigen. Um weitere Details anzuzeigen, klicken Sie mit der linken Maustaste, und wählen Sie einen bestimmten Pfad- oder Zeitrahmen in der Diagrammlinie aus.

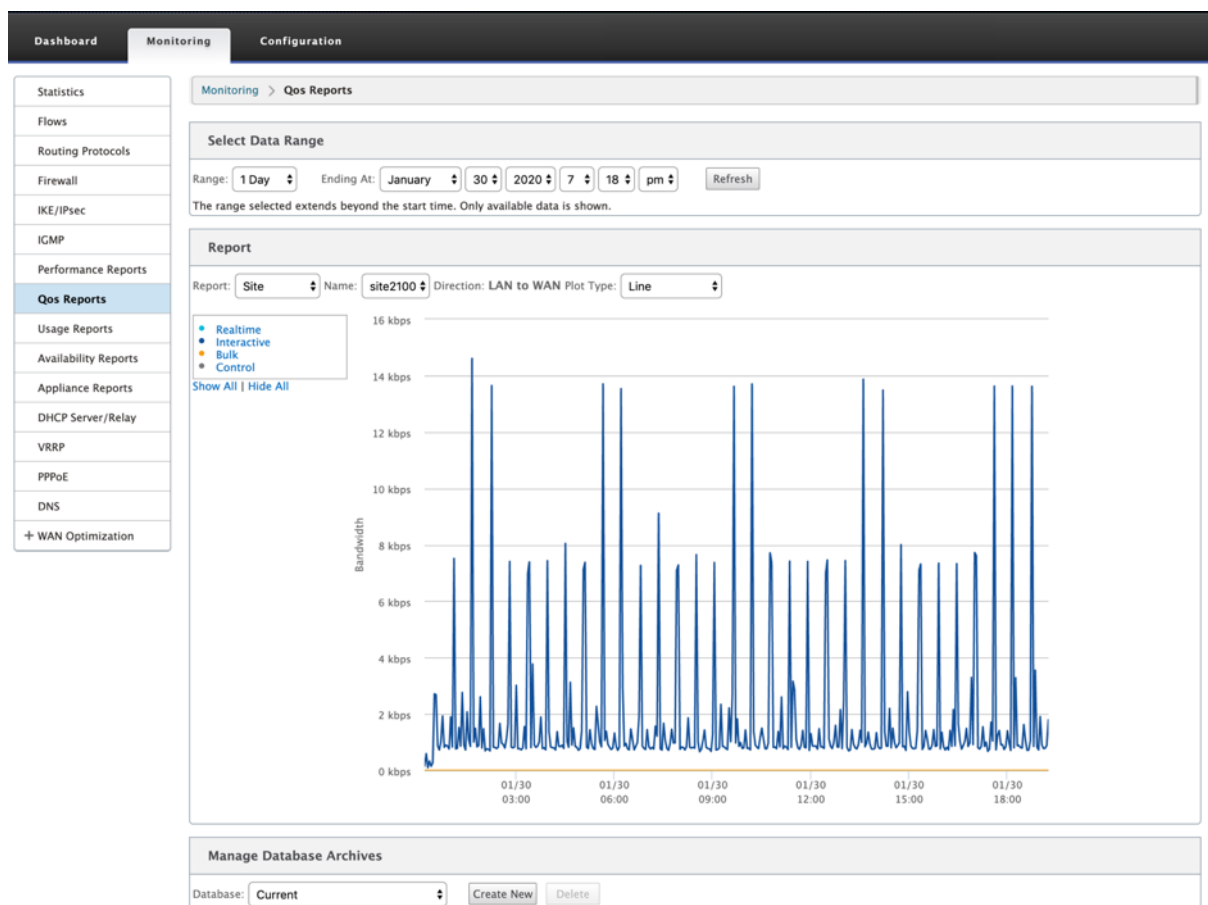


Sie können den Datenbereich nach Bedarf mit den folgenden Feldern auswählen, um den Leistungsbericht anzuzeigen:

- **Virtueller Pfad:** Wählen Sie den virtuellen Pfad aus der Dropdown-Liste aus.
- **Richtung:** Wählen Sie die Richtung nach Bedarf aus (LAN zu WAN oder WAN to LAN).
- **Bericht:** Wählen Sie die folgenden Netzwerkparameter aus, um den Bericht anzuzeigen:
 - Bandbreite
 - Latenz
 - Jitter
 - Verlust
 - Qualität

QoS-Berichte

Sie können den Anwendungs-QoS-Bericht überwachen, z. B. die Anzahl der Pakete oder Bytes, die auf jeder Site, WAN-Verbindung, Virtual Path und Pfadebene hochgeladen, heruntergeladen oder gelöscht werden.

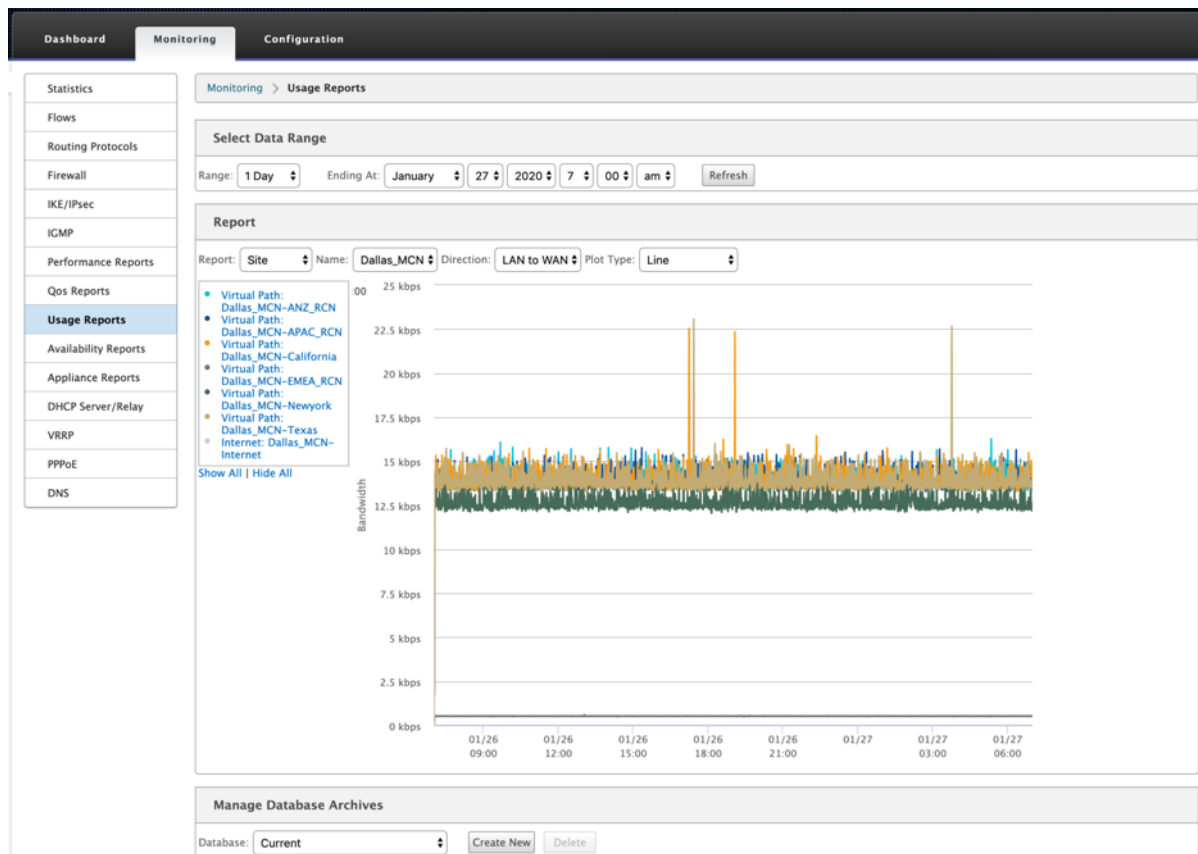


Sie können die folgenden Metriken anzeigen:

- **Echtzeit:** Bandbreite, die von Anwendungen verbraucht wird, die zum Echtzeit-Klassentyp in der Citrix SD-WAN SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
- **Interaktiv:** Bandbreite, die von Anwendungen verbraucht wird, die zum interaktiven Klassentyp in der Citrix SD-WAN SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).
- **Bulk:** Bandbreite, die von Anwendungen verbraucht wird, die zum Massen-Klassentyp in der Citrix SD-WAN SD-WAN-Konfiguration gehören. Diese Anwendungen beinhalten wenig menschliches Eingreifen und werden meist von den Systemen selbst gehandhabt (zum Beispiel FTP, Backup-Operationen).
- **Steuerung:** Bandbreite zur Übertragung von Steuerungspaketen, die Routing-, Planungs- und Linkstatistikinformationen enthalten.

Nutzungsberichte

Die Verwendungsberichte liefern die Informationen zur Verwendung virtueller Pfade.



- **Bericht:** Wählen Sie **Site** oder **WAN-Link** aus der Dropdown-Liste aus, um den Bericht anzuzeigen.
- **Name:** Wählen Sie den Namen der Site oder des WAN-Link aus der Dropdown-Liste aus.
- **Richtung:** Wählen Sie die Richtung nach Bedarf aus (LAN zu WAN oder WAN to LAN).
- **Plottyp:** Wählen Sie den Plottyp aus der Dropdown-Liste (Linie oder Fläche) aus.

Verfügbarkeitsberichte

In diesem Bericht können Sie die Verfügbarkeitsdaten von WAN-Links, Pfaden und virtuellen Pfaden anzeigen. Sie können auch zu einem bestimmten Zeitrahmen wechseln, z. B. 1 Stunde, 24 Stunden und 7 Tage, um die verfügbaren Daten anzuzeigen. Die Daten Paths und Virtual Paths werden in einem Format **DD:HH:MM:SS** dargestellt.

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Availability Reports

Select Timeframe

For the period from 7:01 on 1/26/2020 to 7:01 on 1/27/2020 | Switch to: 1 hour | 24 hours | 7 days | All Available Data

All times are represented in days (if available), hours (if available), minutes and seconds. DD:HH:MM:SS

Paths and Virtual Paths

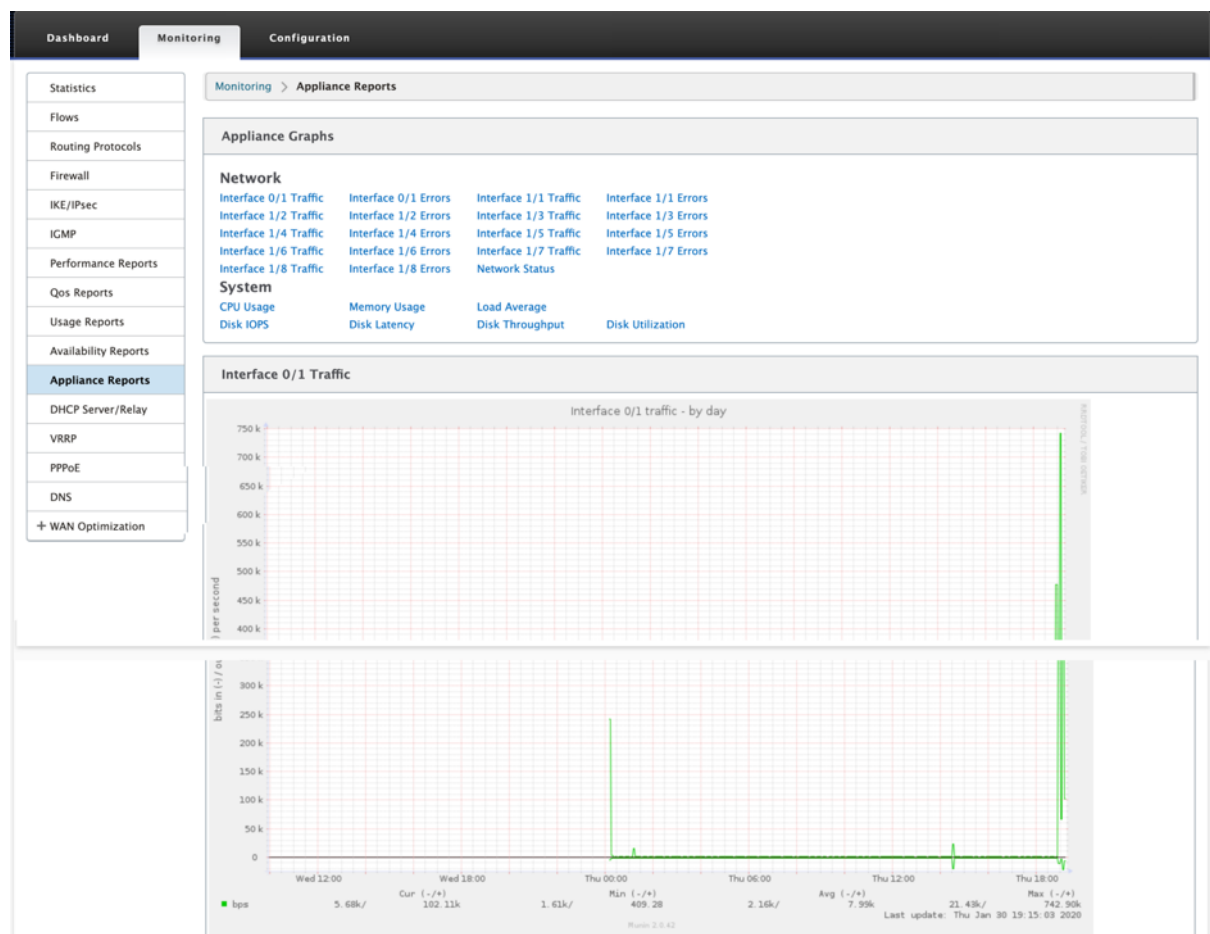
| | Uptime | Goodtime | Badtime | | | | Downtime | | | Incidents | | | |
|--------------------------------------|------------|------------|---------|------------|---------|------|------------|------------|------|-----------|------|---------|------|
| | | | Total | Loss | Silence | Peer | Total | Silence | Peer | Total | Loss | Silence | Peer |
| Virtual Path Dallas_MCN-ANZ_RCN | 1:00:00:00 | 1:00:00:00 | 0:00 | 0:00 | 5 | | | | | | | | |
| Dallas_MCN-queue1->ANZ_RCN-queue1 | 1:00:00:00 | 1:00:00:00 | 0:00 | --- | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | 0 | --- | 0 | 0 |
| ANZ_RCN-queue1->Dallas_MCN-queue1 | 1:00:00:00 | 23:59:10 | 0:50 | 0:00 | 0:50 | --- | 0:00 | 0:00 | --- | 5 | 0 | 5 | --- |
| Virtual Path Dallas_MCN-APAC_RCN | 1:00:00:00 | 1:00:00:00 | 0:00 | 0:00 | 14 | | | | | | | | |
| Dallas_MCN-queue1->APAC_RCN-queue1 | 1:00:00:00 | 1:00:00:00 | 0:00 | --- | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | 0 | --- | 0 | 0 |
| APAC_RCN-queue1->Dallas_MCN-queue1 | 1:00:00:00 | 23:57:40 | 2:20 | 0:00 | 2:20 | --- | 0:00 | 0:00 | --- | 14 | 0 | 14 | --- |
| Virtual Path Dallas_MCN-California | 1:00:00:00 | 23:59:42 | 0:18 | 0:00 | 2 | | | | | | | | |
| Dallas_MCN-queue1->California-queue1 | 23:58:36 | 23:58:36 | 0:00 | --- | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | 2 | --- | 0 | 2 |
| California-queue1->Dallas_MCN-queue1 | 1:00:00:00 | 23:59:40 | 0:20 | 0:00 | 0:20 | --- | 0:00 | 0:00 | --- | 2 | 0 | 2 | --- |
| Virtual Path Dallas_MCN-EMEA_RCN | 0:00 | 0:00 | 0:00 | 1:00:00:00 | 0 | | | | | | | | |
| Dallas_MCN-queue1->EMEA_RCN-queue2 | 0:00 | 0:00 | 0:00 | --- | 0:00 | 0:00 | 1:00:03:45 | 1:00:03:45 | 0:00 | 0 | --- | 0 | 0 |
| EMEA_RCN-queue2->Dallas_MCN-queue1 | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | --- | 1:00:03:45 | 1:00:03:45 | --- | 0 | 0 | 0 | --- |
| Virtual Path Dallas_MCN-Newyork | 1:00:00:00 | 1:00:00:00 | 0:00 | 0:00 | 8 | | | | | | | | |
| Dallas_MCN-WL-2->Newyork-WL-2 | 0:00 | 0:00 | 0:00 | --- | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | 0 | --- | 0 | 0 |
| Dallas_MCN-queue1->Newyork-queue1 | 1:00:00:00 | 1:00:00:00 | 0:00 | --- | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | 0 | --- | 0 | 0 |
| Newyork-WL-2->Dallas_MCN-WL-2 | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | --- | 1:00:03:45 | 1:00:03:45 | --- | 0 | 0 | 0 | --- |
| Newyork-queue1->Dallas_MCN-queue1 | 1:00:00:00 | 23:58:40 | 1:20 | 0:00 | 1:20 | --- | 0:00 | 0:00 | --- | 8 | 0 | 8 | --- |
| Virtual Path Dallas_MCN-Texas | 1:00:00:00 | 23:59:42 | 0:18 | 0:00 | 12 | | | | | | | | |
| Dallas_MCN-queue1->Texas-queue1 | 23:58:35 | 23:58:35 | 0:00 | --- | 0:00 | 0:00 | 0:00 | 0:00 | 0:00 | 2 | --- | 0 | 2 |
| Texas-queue1->Dallas_MCN-queue1 | 1:00:00:00 | 23:58:00 | 2:00 | 0:00 | 2:00 | --- | 0:00 | 0:00 | --- | 12 | 0 | 12 | --- |

WAN Links

| | Uptime | Downtime | Incidents |
|-------------------|------------|------------|-------------|
| Dallas_MCN-WL-2 | 0:00 | 1:00:00:00 | 1 |
| Dallas_MCN-queue1 | 1:00:00:00 | 0:00 | No downtime |

Appliance-Berichte

Appliance-Bericht liefert Berichte zum Netzwerkverkehr und zur Systemverwendung. Klicken Sie auf die einzelnen Links, um das Appliance-Diagramm nach Tag, wöchentlich, monatlich und jährlich anzuzeigen oder zu überwachen.



Firewall-Statistiken anzeigen

May 10, 2021

Nachdem Sie Firewall- und NAT-Richtlinien konfiguriert haben, können Sie die Statistiken der Verbindungen, Firewall-Richtlinien und NAT-Richtlinien als Berichte anzeigen. Sie können die Berichte mit den verschiedenen Filterparametern filtern.

Hinweise zum Konfigurieren von Firewall- und NAT-Richtlinien finden Sie unter [Stateful Firewall und NAT-Unterstützung](#).

Verbindungen

Sie können die Statistiken für Anwendungen für die Firewall-Richtlinie überprüfen. Auf diese Weise können Sie alle Verbindungen anzeigen, die mit der ausgewählten Anwendung übereinstimmen,

woher sie kommen, wohin sie gehen und wie viel Datenverkehr sie generieren. Sie können sehen, wie die Firewall-Richtlinien auf den Datenverkehr für jede Anwendung wirken.

Sie können die Verbindungsstatistiken mit den folgenden Parametern filtern:

- Anwendung - Die Anwendung, die als Filterkriterien für die Verbindung verwendet wird.
- Familie - Die Anwendungsfamilie, die als Filterkriterien für die Verbindung verwendet wird.
- IP-Protokoll - Das von der Verbindung verwendete IP-Protokoll.
- Quellzone - Die Zone, aus der die Verbindung stammt.
- Zielzone - Die Zone, von der der reagierende Datenverkehr stammt.
- Quelldiensttyp - Der Dienst, von dem die Verbindung stammt.
- Quelldienstinstanz - Die Instanz des Dienstes, von dem die Verbindung stammt.
- Quell-IP - Die IP-Adresse, von der die Verbindung stammt, Eingabe in punktierter Dezimalnotation mit einer optionalen Subnetzmaske.
- Quellport - Der Port oder der Bereich der Ports, von denen die Verbindung stammt. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Zieldiensttyp - Der Dienst, von dem der antwortende Datenverkehr stammt.
- Zieldienstinstanz - Die Instanz des Dienstes, von dem der antwortende Datenverkehr stammt.
- Ziel-IP - Die IP-Adresse des antwortenden Geräts, Eingabe in punktierter Dezimalnotation mit optionaler Subnetzmaske.
- Zielport - Der Port oder der Bereich von Ports, die vom antwortenden Gerät verwendet werden. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.

Filterrichtlinien

Mit Richtlinien können Sie Aktionen für Verkehrsflüsse festlegen. Gruppe von Firewallfiltern werden mithilfe von Firewall-Richtlinienvorlagen erstellt und können auf alle Websites im Netzwerk oder nur auf bestimmte Websites angewendet werden.

Sie können den Statistikbericht für alle Filterrichtlinien anzeigen und mit den folgenden Parametern filtern.

- Anwendungsobjekt - Das Application-Objekt, das als Filterkriterien in der Firewallrichtlinie verwendet wird.
- Anwendung - Die Anwendung, die als Filterkriterien in der Firewall-Richtlinie verwendet wird
- Familie - Die Anwendungsfamilie, die als Filterkriterien in der Firewall-Richtlinie verwendet wird.
- IP-Protokoll - Das IP-Protokoll, mit dem die Filterrichtlinie übereinstimmt.
- DSCP: Das DSCP-Tag, dem die Filterrichtlinie entspricht.
- Filterrichtlinienaktion - Die Aktion, die von der Richtlinie ausgeführt wird, wenn ein Paket mit dem Filter übereinstimmt.
- Quelldiensttyp - Der Dienst, von dem die Verbindung stammt.

- Quelldienstname - Die Instanz des Dienstes, von dem die Verbindung stammt.
- Quell-IP - Die IP-Adresse, von der die Verbindung stammt, Eingabe in punktierter Dezimalnotation mit einer optionalen Subnetzmaske.
- Quellport - Der Port oder der Bereich der Ports, von denen die Verbindung stammt. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Zieldiensttyp - Der Dienst, für den der reagierenden Datenverkehr bestimmt ist.
- Zieldienstname - Gegebenenfalls der Dienst, für den der reagierenden Datenverkehr bestimmt ist.
- Ziel-IP - Die IP-Adresse des antwortenden Geräts, Eingabe in punktierter Dezimalnotation mit optionaler Subnetzmaske.
- Zielport - Der Port oder der Bereich von Ports, die vom antwortenden Gerät verwendet werden. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Quellzone - Die Ursprungszone, die mit der Filterrichtlinie übereinstimmt.
- Zielzone - Die Antwortzone, die mit der Filterrichtlinie übereinstimmt.

NAT-Richtlinien

Sie können die Statistiken aller NAT (Network Address Translation) -Richtlinien anzeigen und den Bericht mithilfe der folgenden Parameter filtern.

- IP-Protokoll - Das IP-Protokoll, mit dem die NAT-Richtlinie übereinstimmt.
- NAT-Typ - Der von der NAT-Richtlinie verwendete NAT-Typ.
- Dynamischer NAT-Typ - Der Typ von Dynamic NAT, der von der NAT-Richtlinie verwendet wird.
- Diensttyp - Der von der NAT-Richtlinie verwendete Diensttyp.
- Dienstname - Die Instanz des Dienstes, der von der NAT-Richtlinie verwendet wird.
- Inside IP - Die innere IP-Adresse, Eingabe in punktierte Dezimalnotation mit einer optionalen Subnetzmaske.
- Inside Port - Der von der NAT-Richtlinie verwendete interne Portbereich. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Externe IP - Die externe IP-Adresse, Eingabe in punktierter Dezimalnotation mit einer optionalen Subnetzmaske.
- Externer Port - Der von der NAT-Richtlinie verwendete externe Portbereich. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.

So zeigen Sie Firewall-Statistiken an:

1. Navigieren Sie zu **Überwachung > Firewall**.
2. Wählen Sie im Feld Statistik die Option **Verbindungen, Filterrichtlinien oder NAT-Richtlini**en nach Bedarf aus.
3. Legen Sie die Filterkriterien nach Bedarf fest.

Monitoring > Firewall

Firewall Statistics

Statistics: **Connections**

Maximum entries to display: 50

Filtering:

Application: Any Family: Any

IP Protocol: Any Source Zone: Any Destination Zone: Any

Source Service Types: Any Source Service Instances: Any Source IP: Source Port:

Destination Service Types: Any Destination Service Instances: Any Destination IP: Destination Port:

Refresh Show latest data Show Drops

Clear Connections Help

Connections

| Application | Family | IP Protocol | Source | | | Destination | | | State | Is NAT | Packets | Bytes | | | | |
|-----------------------------------|----------|-------------|---------------|-------|--------------|----------------|------|---------------|-------|--------|--------------------|------------------|-------------|----|----|------|
| | | | IP Address | Port | Service Type | IP Address | Port | Service Type | | | | | | | | |
| Unknown virtual protocol(unknown) | Standard | TCP | 172.147.12.83 | 49546 | Virtual Path | MCN-DC-Branch1 | Any | 172.147.21.53 | 2312 | Local | VirtualInterface-1 | Default_LAN_Zone | ESTABLISHED | No | 57 | 3710 |

Connections Displayed: 1
Connections In Use: 1/128000

4. Klicken Sie auf **Aktualisieren**.

Diagnose

September 26, 2023

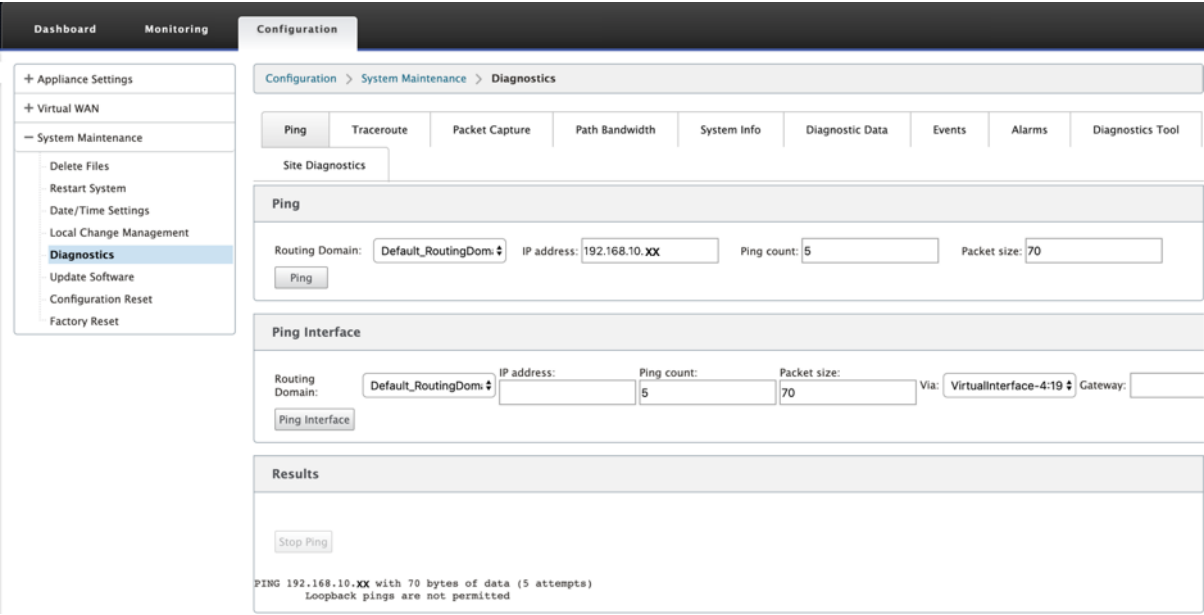
Citrix SD-WAN Diagnostics-Dienstprogramme bieten die folgenden Optionen zum Testen und Untersuchen von Konnektivitätsproblemen:

- Ping
- Traceroute
- Paketerfassung
- Pfad-Bandbreite
- Systeminformationen
- Diagnose-Daten
- Ereignisse
- Alarme
- Diagnose-Tool
- Standortdiagnose

Die Diagnoseoptionen im **Citrix SD-WAN Dashboard** steuern die Datenerfassung.

Ping

Um die **Ping-Option** zu verwenden, navigieren Sie zu **Konfiguration > Diagnose** und wählen Sie **Ping** aus. Sie können Ping verwenden, um die Erreichbarkeit des Hosts und die Netzwerkkonnektivität zu überprüfen.

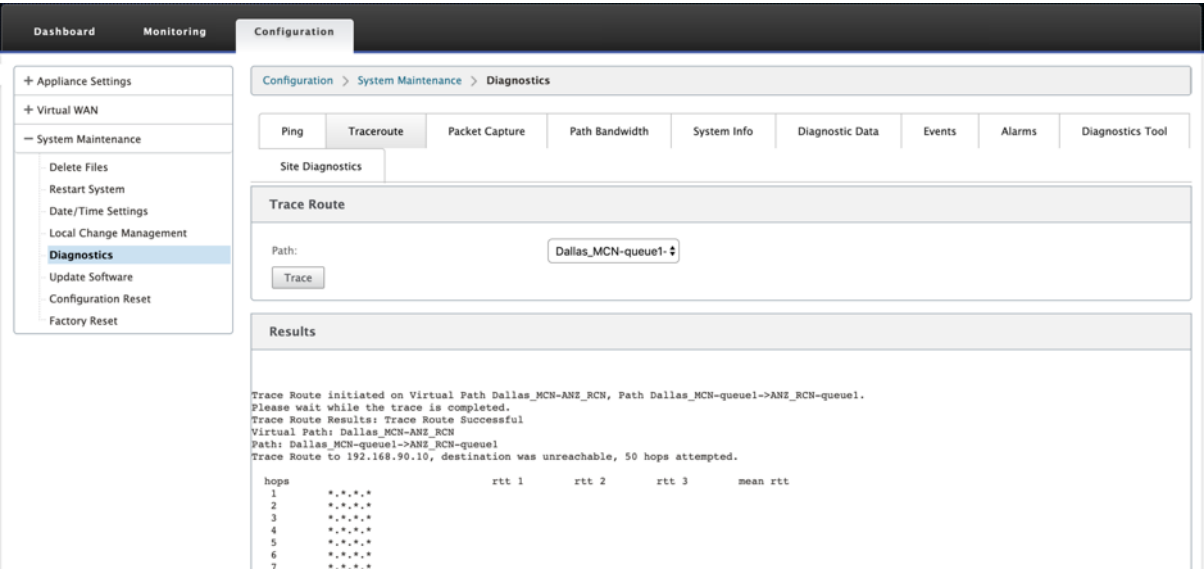


Wählen Sie die Routing-Domäne aus. Geben Sie eine gültige IP-Adresse, die Anzahl der Ping-Zähler (Anzahl der Ping-Anfragen zu senden) und die Paketgröße (Anzahl der Datenbytes) an. Klicken Sie auf **Ping stoppen**, um eine laufende Ping-Suche

Sie können über eine bestimmte Oberfläche pingen. Wählen Sie die Routingdomäne aus und geben Sie die IP-Adresse mit Ping-Anzahl und Paketgröße an und wählen Sie die virtuelle Schnittstelle aus der Dropdown-Liste aus.

Traceroute

Um die Option **Traceroute** zu verwenden, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Traceroute** aus.



Traceroute hilft dabei, den Pfad oder die Route zu einem Remoteserver zu erkennen und anzuzeigen. Verwenden Sie die Option **Traceroute** als Debugging-Tool, um die Fehlerpunkte in einem Netzwerk zu erkennen.

Wählen Sie einen Pfad aus der Dropdownliste aus und klicken Sie auf **Trace**. Sie können die Details im Abschnitt **Ergebnisse** einsehen.

Paketerfassung

Sie können die Option **Paketerfassung** verwenden, um das Echtzeit-Datenpaket abzufangen, das über die ausgewählte aktive Schnittstelle an der ausgewählten Site läuft. Die Paketerfassung hilft Ihnen bei der Analyse und Behebung von Netzwerkproblemen.

Dashboard

Monitoring

Configuration

+ Appliance Settings

+ Virtual WAN

- System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Factory Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Site Diagnostics

Packet Capture

Interfaces:

X 1/1 X 1/2 X 1/4 X 1/6

Duration (seconds):

30

Max # of packets to view:

5000

Capture Filter (Optional):

Capture

Note: Capture file size will not exceed 575 MB. Once the packet capture file reaches this size, packet capturing will be stopped. Atleast 1 interface needs to be selected to trigger a packet capture.

Gathering Requested Data

Generating packet capture information...

Packet Capture Successful

Packet Capture File

A binary file containing the packet data captured during the last successful packet capture. This file can be opened in Wireshark for analysis.

The downloaded Packet capture file displays internal labels for interface names. Here are the mappings for this platform:
MGMT -> tn-mgt0
1/1 -> dpdk-1_1
1/4 -> dpdk-1_4
1/2 -> dpdk-1_2
1/6 -> dpdk-1_6

Download

Packet View

| # | Interface Name | Protocol | Time | Length | Source | Destination | Src |
|-----|----------------|----------|------------------------------------|--------|--------------|--------------|------|
| 1. | 1/2 | UDP | May 8, 2019 06:06:30.415518572 UTC | 1442 | 172.168.1.10 | 152.168.1.10 | 4980 |
| 2. | 1/2 | UDP | May 8, 2019 06:06:30.415524972 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 3. | 1/2 | UDP | May 8, 2019 06:06:30.415628324 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 4. | 1/2 | UDP | May 8, 2019 06:06:30.415648675 UTC | 1442 | 172.168.1.10 | 152.168.1.10 | 4980 |
| 5. | 1/2 | UDP | May 8, 2019 06:06:30.415858329 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 6. | 1/2 | UDP | May 8, 2019 06:06:30.415873459 UTC | 1442 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 7. | 1/2 | UDP | May 8, 2019 06:06:30.416073413 UTC | 1442 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 8. | 1/2 | UDP | May 8, 2019 06:06:30.416232216 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 9. | 1/1 | TCP | May 8, 2019 06:06:30.321504133 UTC | 1384 | 152.168.1.51 | 172.168.1.52 | 80 |
| 10. | 1/2 | UDP | May 8, 2019 06:06:30.416266227 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 11. | 1/2 | UDP | May 8, 2019 06:06:30.416435190 UTC | 1442 | 172.168.1.10 | 152.168.1.10 | 4980 |
| 12. | 1/2 | UDP | May 8, 2019 06:06:30.416525402 UTC | 114 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 13. | 1/1 | TCP | May 8, 2019 06:06:30.321511153 UTC | 54 | 152.168.1.52 | 172.168.1.51 | 2307 |
| 14. | 1/2 | UDP | May 8, 2019 06:06:30.416529932 UTC | 114 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 15. | 1/1 | TCP | May 8, 2019 06:06:30.321514773 UTC | 54 | 152.168.1.52 | 172.168.1.51 | 2163 |
| 16. | 1/2 | UDP | May 8, 2019 06:06:30.416651685 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 17. | 1/2 | UDP | May 8, 2019 06:06:30.416693075 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 18. | 1/2 | UDP | May 8, 2019 06:06:30.416783167 UTC | 1442 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 19. | 1/2 | UDP | May 8, 2019 06:06:30.416881149 UTC | 1442 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 20. | 1/2 | UDP | May 8, 2019 06:06:30.417039802 UTC | 1442 | 152.168.1.10 | 172.168.1.10 | 4980 |
| 21. | 1/2 | UDP | May 8, 2019 06:06:30.417127644 UTC | 114 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 22. | 1/2 | UDP | May 8, 2019 06:06:30.417132114 UTC | 114 | 172.168.1.10 | 152.168.1.10 | 4980 |
| 23. | 1/2 | UDP | May 8, 2019 06:06:30.417135804 UTC | 1442 | 172.168.1.10 | 152.168.2.10 | 4980 |
| 24. | 1/1 | TCP | May 8, 2019 06:06:30.321517954 UTC | 54 | 152.168.1.52 | 172.168.1.51 | 6265 |
| 25. | 1/2 | UDP | May 8, 2019 06:06:30.417178605 UTC | 114 | 172.168.1.10 | 152.168.1.10 | 4980 |
| 26. | 1/1 | TCP | May 8, 2019 06:06:30.321648046 UTC | 1384 | 172.168.1.51 | 152.168.1.52 | 80 |

Geben Sie die folgenden Eingaben für den Paketerfassungsvorgang an:

- **Schnittstellen** - Aktive Schnittstellen sind für die Paketerfassung für die SD-WAN-Appliance verfügbar. Wählen Sie eine Schnittstelle aus oder fügen Sie Schnittstellen aus der Dropdownliste hinzu. Mindestens eine Schnittstelle muss ausgewählt werden, um eine Paketerfassung auszulösen.

Hinweis:

Die Möglichkeit, die Paketerfassung über alle Schnittstellen gleichzeitig auszuführen, hilft,

die Problembehandlungsaufgabe zu beschleunigen.

- **Dauer (Sekunden)** —Dauer (in Sekunden) wie lange die Daten erfasst werden müssen.
- **Max. Anzahl der anzuzeigenden Pakete** - Maximalbegrenzung der Pakete, die im Ergebnis der Paketerfassung angezeigt werden sollen.
- **Capture-Filter (Optional)** - Das optionale Capture-Filter-Feld akzeptiert eine Filterzeichenfolge, die verwendet wird, um zu bestimmen, welche Pakete erfasst werden. Pakete werden mit der Filterzeichenfolge verglichen und wenn das Vergleichsergebnis wahr ist, wird das Paket erfasst. Wenn der Filter leer ist, werden alle Pakete erfasst. Weitere Informationen finden Sie unter [Capture-Filter](#).

Im Folgenden finden Sie einige Beispiele für diesen Capture-Filter:

- **Ether proto\ ARP** - Erfasst nur ARP-Pakete
- **Ether proto\ IP** - Erfasst nur IPv4-Pakete
- **VLAN 100** —Erfasst nur Pakete mit einem VLAN von 100
- **Host 10.40.10.20** - Erfasst nur IPv4-Pakete zum oder vom Host mit der Adresse 10.40.10.20
- **Net 10.40.10.0 Mask 255.255.255.0** - Erfasst nur IPv4-Pakete im Subnetz 10.40.10.0/24
- **IP proto\ TCP** - Erfasst nur IPv4/TCP-Pakete
- **Port 80** - Erfasst nur IP-Pakete zu oder von Port 80
- **Portbereich 20—30** - Erfasst nur IP-Pakete zu oder von den Ports 20 bis 30

Hinweis

Die maximale Größe der Aufnahmedatei beträgt bis zu 575 MB. Sobald die Paketerfassungsdatei diese Größe erreicht hat, wird die Paketerfassung gestoppt.

Klicken Sie auf **Capture**, um das Ergebnis der Paketerfassung anzuzeigen. Sie können auch eine Binärdatei herunterladen, die die Paketdaten enthält, die während der letzten erfolgreichen Paketerfassung erfasst wurden.

Sammeln angeforderter Daten

In dieser Tabelle sehen Sie den Status der Generierung von Paketerfassungsinformationen (ob die Paketerfassung erfolgreich ist oder keine Paketerfassung ist).

Paket-Capture-Datei

Pakete werden während der letzten erfolgreichen Paketerfassung als Binärdaten erfasst. Sie können die Binärdatei herunterladen, um die Paketinformationen offline zu analysieren. Der Name der

Schnittstellen unterscheidet sich in der heruntergeladenen Datei im Vergleich zur GUI-Schnittstelle. Um die interne Schnittstellenzuordnung anzuzeigen, klicken Sie auf die Option Hilfe.

Packet Capture File

A binary file containing the packet data captured during the last successful packet capture. This file can be opened in Wireshark for analysis.

The downloaded Packet capture file displays internal labels for interface names. Here are the mappings for this platform:

MGMT -> tn-mgt0
1/4 -> dpdk-1_4
1/1 -> dpdk-1_1
1/5 -> dpdk-1_5
1/2 -> dpdk-1_2
LTE-1 -> dpdk-lte_1

Download

Help

Sie benötigen **Wireshark** Software 2.4.13 Version oder höher, um die Binärdatei zu öffnen und zu lesen.

The image shows a Wireshark packet capture analysis. The top pane displays a list of 29 captured packets, all of which are UDP packets from source IP 10.103.40.80 to destination IP 192.168.60.15. The selected packet (No. 1) is expanded in the middle pane, showing the following details:

- Ethernet II**: Src: Intel (10:00:00:00:00:00), Dst: Intel (10:00:00:00:00:00), Type: IPv4 (0x0800)
- Internet Protocol Version 4**: Src: 10.103.40.80, Dst: 192.168.60.15, Len: 36, TOS: 0
- User Datagram Protocol**: Src Port: 593, Dst Port: 593, Len: 26

The bottom pane shows the raw packet data in hexadecimal and ASCII format.

Paket-Ansicht

Wenn die Größe der Paketerfassungsdatei größer ist, dauert es länger, bis der Rendervorgang für die Paketansicht abgeschlossen ist. In diesem Fall wird empfohlen, die Datei herunterzuladen und **Wire-shark** zur Analyse zu verwenden, anstatt sich auf das Ergebnis der **Packet View** zu verlassen.

Pfad-Bandbreite

Um die Funktion **Pfadbandbreite** zu verwenden, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Pfadbandbreite** aus.

Dashboard

Monitoring

Configuration

Appliance Settings

Virtual WAN

System Maintenance

System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Instant Path Bandwidth Testing

Path:MCN-5100-WL-2->BR572

Test

Results

Minimum Bandwidth: 936564 kbps

Maximum Bandwidth: 1213863 kbps

Average Bandwidth: 1109046 kbps

Schedule Path Bandwidth Testing

Add

Path NameFrequencyDay of WeekHourMinute

Apply Settings

History Path Bandwidth Testing Result

Show 50 entriesShowing 1 to 27 of 27 entries

| Num | From Link | To Link | Test Time | Min Bandwidth (kbps) | Max Bandwidth (kbps) | Avg Bandwidth (kbps) |
|-----|----------------|---------------|------------------------|----------------------|----------------------|----------------------|
| 1 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 2:01:03 PM | 2883972 | 5099707 | 4357330 |
| 2 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 4:01:03 PM | 3109115 | 3872000 | 3616157 |
| 3 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 6:01:04 PM | 3041280 | 4119960 | 3518949 |
| 4 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 8:01:04 PM | 2769377 | 3700672 | 3276124 |
| 5 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 10:01:04 PM | 409245 | 3574153 | 2489269 |
| 6 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 12:01:04 AM | 2481756 | 4001684 | 3198214 |
| 7 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 2:01:04 AM | 2548653 | 3872000 | 3236546 |
| 8 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 4:01:03 AM | 3204413 | 3992628 | 3642649 |
| 9 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 6:01:03 AM | 2997677 | 4672357 | 3664018 |
| 10 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 8:01:04 AM | 2248258 | 6288360 | 3612666 |
| 11 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 10:01:04 AM | 2410236 | 3372387 | 2816032 |
| 12 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 12:01:03 PM | 2613600 | 4401852 | 3563752 |
| 13 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 2:01:04 PM | 2324266 | 4059961 | 3101910 |
| 14 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 4:01:03 PM | 2179340 | 3684970 | 2929146 |
| 15 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 6:01:03 PM | 2613600 | 3589493 | 3021890 |
| 16 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 8:01:03 PM | 1676056 | 3499980 | 2655200 |
| 17 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 10:01:03 PM | 1954093 | 3558944 | 2975884 |
| 18 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 12:01:03 AM | 2161116 | 3784398 | 2902068 |
| 19 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 2:01:04 AM | 2968971 | 4079765 | 3821158 |
| 20 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 4:01:04 AM | 3514004 | 4181760 | 3893381 |
| 21 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 6:01:03 AM | 3358843 | 4059961 | 3756691 |
| 22 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 8:01:03 AM | 3216738 | 4245441 | 3716351 |
| 23 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 10:01:04 AM | 3558944 | 4202773 | 3932908 |
| 24 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 12:01:03 PM | 3427672 | 4267102 | 3838552 |
| 25 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 2:01:04 PM | 2674061 | 4224000 | 3608676 |
| 26 | RCN1-5100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 4:01:03 PM | 2816000 | 6288360 | 4165337 |
| 27 | MCN-5100-WL-2 | BR572-WL-1 | 2/19/2018, 5:23:04 PM | 936564 | 1213863 | 1109046 |

Showing 1 to 27 of 27 entries

Aktive Bandbreitentests ermöglichen Ihnen die Möglichkeit, einen sofortigen Pfadbandbreitentest über eine öffentliche Internet-WAN-Verbindung durchzuführen oder öffentliche WAN-Bandbreitentests zu bestimmten Zeiten auf einer wiederkehrenden Basis durchzuführen.

Die **Pfadbandbreitenfunktion** ist nützlich, um zu demonstrieren, wie viel Bandbreite zwischen zwei Standorten während neuer und vorhandener Installationen verfügbar ist. Auch zum Testen von

Pfaden, um das Ergebnis von Einstellungs- und Bestätigungsänderungen zu bestimmen, z. B. das Anpassen von DSCP-Tag-Einstellungen oder zulässigen Bandbreitenraten. Weitere Informationen finden Sie unter [Aktive Bandbreitentests](#).

Systeminfo

Die Seite **Systeminformationen** enthält die Systeminformationen, Details zu Ethernet-Ports und den Lizenzstatus.

Um die Systeminformationen anzuzeigen, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Systeminformationen**.

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

— System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

System Information

Name: Dallas_MCN

Appliance Mode: MCN

Hardware Model: 4000

Software Version: 11.0.0.72.760315

Built On: Apr 10 2019 at 19:08:49

OS Partition Version: 5.1

Serial Number: HNXCJCRGJX

BIOS version: 4.2a

Hard Disk Usage

| Partition | Usage |
|-----------|-------|
| Active OS | 51% |
| /home | 18% |

[View Details](#)

Ethernet Ports

| | | |
|-------|------|-------------------|
| 0/1: | mgt0 | 0acc4:7a:85:ce:62 |
| 1/1: | la0 | be:0af7:be:76:3d |
| 1/2: | wa0 | e6:18:31:22:b9:84 |
| 1/3: | la1 | 86:c0:b7:3c:03:5d |
| 1/4: | wa1 | 8e:4bf2:fd:86:75 |
| 1/5: | la2 | da:6c:7c:73:d4:84 |
| 1/6: | wa2 | be:e3:26:7e:2b:99 |
| 1/7: | la3 | 82:af:6a:d8:74:72 |
| 1/8: | wa3 | a2:af:76:6f:90:a2 |
| 10/1: | la4 | 96:9a:df:97:77:eb |
| 10/2: | wa4 | 76:5d:15:d9:f0:26 |

License Status

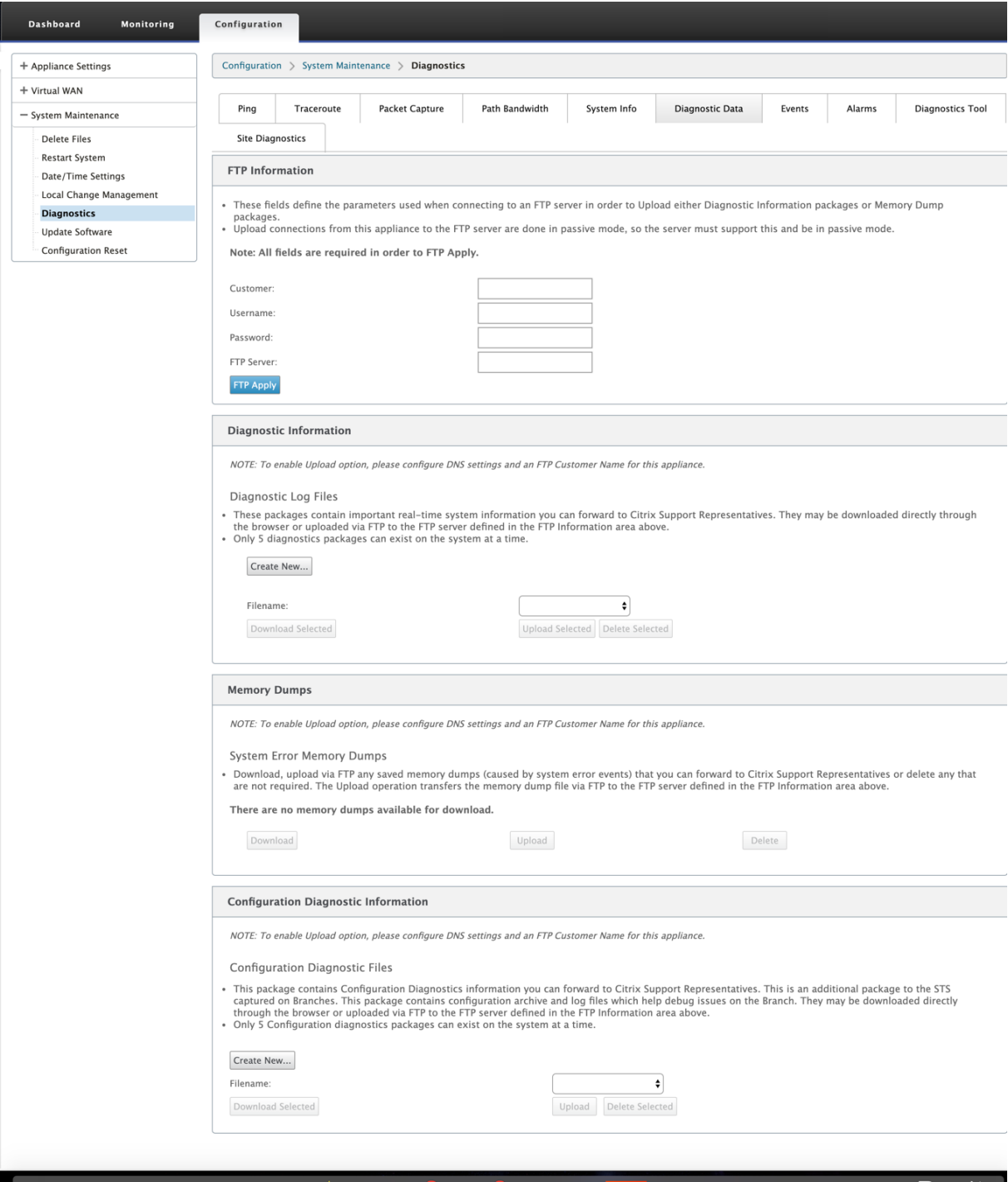
| | |
|------------------------------|-------------------------|
| State: | Licensed |
| License Server HostID: | 02c47a85ce62 |
| Model: | 4000VW-2000 |
| Maximum Bandwidth (MAXBW): | 2000 Mbps |
| License Type: | Retail |
| Maintenance Expiration Date: | Sun Dec 1 00:00:00 2019 |
| License Expiration Date: | Mon Dec 2 00:00:00 2019 |

In den **Systeminformationen** werden alle Parameter aufgeführt, die nicht auf ihre Standardwerte eingestellt sind. Diese Informationen sind schreibgeschützt. Es wird vom Support verwendet, wenn eine Art von Fehlkonfiguration vermutet wird. Wenn Sie ein Problem melden, werden Sie möglicherweise aufgefordert, einen oder mehrere Werte auf dieser Seite zu überprüfen.

Diagnosedaten

Mit **Diagnosedaten** können Sie das Diagnosedatenpaket zur Analyse durch das Citrix Support-Team generieren. Sie können das **Diagnostics-Protokolldateienpaket** herunterladen und es mit dem Citrix Support-Team teilen.

Um die **Diagnosedaten** anzuzeigen, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Diagnosedaten**.



Die **Diagnosedaten** beinhalten:

- **FTP-Informationen** —Geben Sie die Details der FTP-Parameter an und klicken Sie auf **FTP Übernehmen**. Die FTP-Informationen, die erforderlich sind, um einen FTP-Server anzuschließen, um ein Diagnoseinformation hochzuladen.
- **Diagnoseinformationen** —Das Diagnoseprotokolldateipaket enthält Systeminformationen in

Echtzeit, die über den Browser heruntergeladen oder per FTP auf den FTP-Server hochgeladen werden können.

Hinweis:

Nur fünf Diagnosepakete können gleichzeitig auf dem System vorhanden sein.

- **Diagnoseinformationen zur Konfiguration** —In der Version Citrix SD-WAN 11.0 ist die Netzwerkkonfigurationsdatei nicht in den für den Zweig gesammelten Diagnoseinformationen verfügbar. Geben Sie für jeden Supportfall die Diagnoseinformationen des Zweigs und die Konfigurationsdiagnoseinformationen vom Steuerknoten an, an den der Zweig angeschlossen ist.

Um Konfigurationsdiagnoseinformationen von der Control-Knoten-GUI zu sammeln, navigieren Sie zu **Konfiguration > Systemwartung > Diagnose > Diagnosedaten** > unter **Konfigurationsdiagnoseinformationen** und klicken Sie auf **Neu erstellen**.

Klicken Sie nach Abschluss der Erstellung der **Konfigurationsdiagnoseinformationen** auf **Ausgewählte Datei herunterladen** und stellen Sie diese Datei dem Citrix Support zur Verfügung ODER verwenden Sie den FTP-Apply-Vorgang, der auf derselben Seite verfügbar ist, um diese Datei zu FTP zu erstellen.

- **Speicherabbilder** —Sie können die Systemfehler-Memory-Dump-Datei herunterladen oder hochladen und dem Citrix Support-Team geben. Sie können die Dateien auch löschen, wenn dies nicht erforderlich ist.

HINWEIS:

Standardmäßig befindet sich die Option **Hochladen** im deaktivierten Modus. Um es zu aktivieren, konfigurieren Sie **DNS-Einstellungen** und einen **FTP-Kundennamen** für diese Appliance.

Ereignisse

Verwenden Sie die Funktion **Ereignisse**, um die generierten Ereignisse hinzuzufügen, zu überwachen und zu verwalten. Es hilft, Ereignisse in Echtzeit zu identifizieren, sodass Sie Probleme sofort beheben

und die Citrix SD-WAN Appliance effektiv ausführen können. Sie können Ereignisse im CSV-Format herunterladen.

Um ein Ereignis hinzuzufügen, wählen Sie Objekttyp, Ereignistyp und Schweregrad aus der Dropdown-liste aus und klicken Sie auf **Ereignis hinzufügen**.

Um **Ereignisse** anzuzeigen, navigieren Sie zu **Konfiguration** erweitern Sie **Systemwartung > Diagnose** und wählen Sie **Ereignisse** aus.

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

System Maintenance

Diagnose

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

Insert Event

Object Type:USER EVENT

Event type:UNDEFINED

Severity:DEBUG

Add Event

Download Events

There are currently 85 in the Events database, spanning from event 245471 at 2019-03-24 05:35:54 to event 245555 at 2019-04-21 06:23:16. You can download some or all of them in CSV format. You may wish to limit the amount to download because some common spreadsheet programs limit you to 65,536 rows.

Download events starting from2019March24535

54Download (85 events)

Alert Count

| Alert Type | Alerts Sent |
|------------------|-------------|
| Emails: | 0 |
| Syslog Messages: | 0 |
| SNMP Traps: | 5 |

View Events

Quantity:1000

Filter: Object Type = AnyEvent type = AnySeverity = Any

Reload Events Table

| ID | Object ID | Object Name | Object Type | Time | Event Type | Severity | Description |
|--------|-----------|---------------|---------------|---------------------|------------|----------|--|
| 245555 | 25 | License_Alert | LICENSE_EVENT | 2019-04-21 06:23:16 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |
| 245554 | 25 | License_Alert | LICENSE_EVENT | 2019-04-20 06:23:01 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |
| 245553 | 25 | License_Alert | LICENSE_EVENT | 2019-04-19 06:22:46 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |
| 245552 | 25 | License_Alert | LICENSE_EVENT | 2019-04-18 06:22:31 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |
| 245551 | 25 | License_Alert | LICENSE_EVENT | 2019-04-17 06:22:15 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |
| 245550 | 25 | License_Alert | LICENSE_EVENT | 2019-04-16 06:22:00 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |
| 245549 | 25 | License_Alert | LICENSE_EVENT | 2019-04-15 06:21:44 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |
| 245548 | 25 | License_Alert | LICENSE_EVENT | 2019-04-14 06:21:29 | WARNING | CRITICAL | The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps). |

Sie können Citrix SD-WAN so konfigurieren, dass Ereignisbenachrichtigungen für verschiedene Ereignistypen wie **E-Mails**, **SNMP-Traps** oder **Syslog-Nachrichten** gesendet werden.

Sobald die Benachrichtigungseinstellungen für E-Mail, SNMP und Syslog-Benachrichtigungen konfiguriert sind, können Sie den Schweregrad für verschiedene Ereignistypen auswählen und den Modus (E-Mail, SNMP, Syslog) zum Senden von Ereignisbenachrichtigungen auswählen.

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

937

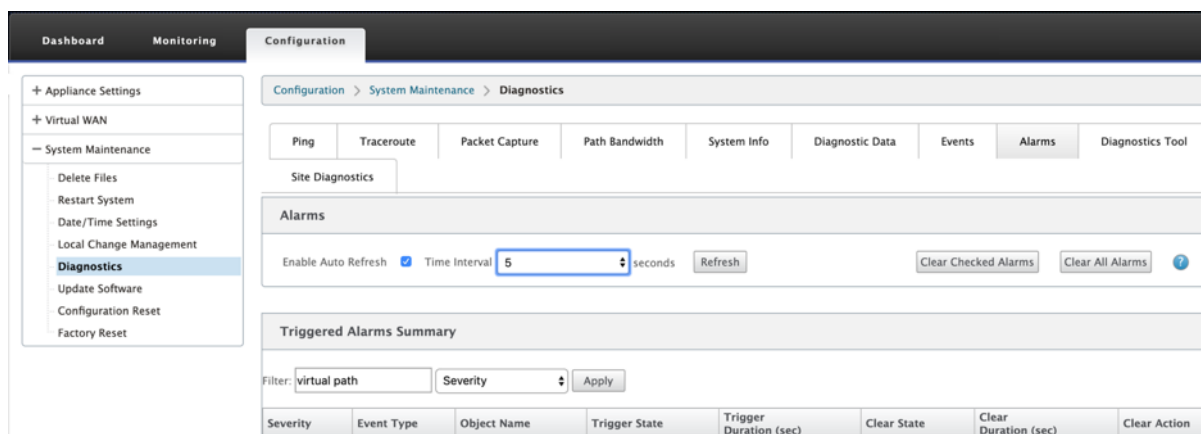
Benachrichtigungen werden für Ereignisse generiert, die dem angegebenen Schweregrad für den Ereignistyp entsprechen oder darüber liegen.

Sie können die Ereignisdetails in der Tabelle **Ereignisse anzeigen anzeigen**. Die Ereignisdetails enthalten die folgenden Informationen.

- **ID** —Ereignis-ID.
- **Objekt-ID** - Die ID des Objekts, das das Ereignis generiert.
- **Objektname** - Der Name des Objekts, das das Ereignis generiert.
- **Objekttyp** —Der Typ des Objekts, das das Ereignis generiert.
- **Zeit** —Die Uhrzeit, zu der das Ereignis generiert wurde.
- **Ereignisart** —Der Status des Objekts zum Zeitpunkt des Ereignisses.
- **Schweregrad** —Der Schweregrad des Ereignisses.
- **Beschreibung** —Eine Textbeschreibung des Ereignisses.

Alarme

Sie können den ausgelösten Alarm anzeigen und löschen. Um **Alarme** anzuzeigen, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Alarme** aus.



Wählen Sie die Alarme aus, die Sie löschen möchten, und klicken Sie auf **Überprüfte Alarme löschen** oder klicken Sie auf **Alle Alarme** löschen, um alle Alarme zu löschen.

Sie können die folgende Zusammenfassung aller ausgelösten Alarme anzeigen:

- **Schweregrad** —Der Schweregrad wird in den Alarmen angezeigt, die gesendet werden, wenn der Alarm ausgelöst oder gelöscht wird, und in der Zusammenfassung des ausgelösten Alarms.
- **Ereignistyp** —Die SD-WAN-Appliance kann Alarme für bestimmte Subsysteme oder Objekte im Netzwerk auslösen. Diese Alarme werden als Ereignisarten bezeichnet.
- **Objektname** —Der Name des Objekts, das das Ereignis generiert.
- **Triggerstatus** —Der Ereignisstatus, der einen Alarm für einen Ereignistyp auslöst.

- **Triggerdauer (Sek.)** —Die Dauer in Sekunden bestimmt, wie schnell das Gerät einen Alarm auslöst.
- **Clear State** —Der Ereignisstatus, der einen Alarm für eine Ereignisart löscht, nachdem der Alarm ausgelöst wurde.
- **Dauer löschen (sec)** —Die Dauer in Sekunden bestimmt, wie lange gewartet werden muss, bevor ein Alarm ausgelöst wird.
- **Klare Aktion** —Die Aktion, die beim Löschen von Alarmen ergriffen wird.

Diagnose-Tool

Das **Diagnose-Tool** wird verwendet, um Testverkehr zu generieren, mit dem Sie Netzwerkprobleme beheben können, die zu folgenden Ergebnissen führen können:

- Häufiger Wechsel des Pfadstatus von gut nach schlecht.
- Schlechte Anwendungsleistung.
- Höherer Paketverlust

In den meisten Fällen treten diese Probleme aufgrund einer auf Firewall und Router konfigurierten Ratenbegrenzung, falschen Bandbreiteneinstellungen, niedriger Verbindungsgeschwindigkeit, Prioritätswarteschlange auf, die vom Netzbetreiber festgelegte Prioritätswarteschlange usw. Das Diagnosetool ermöglicht es Ihnen, die Ursache solcher Probleme zu identifizieren und zu beheben.

Das Diagnosetool entfernt die Abhängigkeit von Drittanbieter-Tools wie iPerf, die manuell auf dem Rechenzentrums- und Branch-Hosts installiert werden müssen. Es bietet mehr Kontrolle über die Art des gesendeten Diagnoseverkehrs, die Richtung, in der der Diagnoseverkehr fließt, und den Pfad, auf dem der Diagnoseverkehr fließt.

Das Diagnose-Tool ermöglicht die Generierung der folgenden zwei Arten von Verkehr:

- **Steuerung:** Generiert Traffic ohne QoS/Scheduling auf die Pakete angewendet. Infolgedessen werden die Pakete über den in der Benutzeroberfläche ausgewählten Pfad gesendet, auch wenn der Pfad zu diesem Zeitpunkt nicht der beste ist. Dieser Verkehr wird verwendet, um bestimmte Pfade zu testen und hilft, ISP-bezogene Probleme zu identifizieren. Sie können diese auch verwenden, um die Bandbreite des ausgewählten Pfades zu bestimmen.
- **Daten:** Simuliert den vom Host generierten Verkehr mit SD-WAN-Verkehrsverarbeitung. Da QoS/Scheduling auf die Pakete angewendet wird, werden die Pakete über den besten verfügbaren Pfad gesendet. Traffic wird über mehrere Pfade gesendet, wenn der Lastausgleich aktiviert ist. Dieser Verkehr wird verwendet, um Probleme im Zusammenhang mit QoS/Scheduler zu beheben.

Hinweis

Um einen Diagnosetest auf einem Pfad durchzuführen, müssen Sie den Test auf den Geräten an

beiden Enden des Pfades starten. Starten Sie den Diagnosetest als Server auf einer Appliance und als Client auf der anderen Appliance.

So verwenden Sie das Diagnose-Tool:

1. Klicken Sie auf beiden Appliances auf **Konfiguration > Systemwartung > Diagnose > Diagnose-Tool**.

2. Wählen Sie im Feld **Toolmodus** die Option **Server** auf einer Appliance aus und wählen Sie **Client** auf der Appliance aus, die sich am Remote-Ende des ausgewählten Pfades befindet.
3. Wählen Sie im Feld **Traffic Type** die Art des Diagnoseverkehrs aus, entweder **Steuerung** oder **Daten**. Wählen Sie auf beiden Geräten denselben Traffic-Typ aus.
4. Geben Sie im Feld **Port** die **TCP/UDP-Portnummer** an, über die der Diagnoseverkehr gesendet wird. Geben Sie dieselbe Portnummer auf beiden Appliances an.
5. Geben Sie im Feld **Iperf**, falls vorhanden, IPERF-Befehlszeilenoptionen an.

Hinweis

Sie müssen die folgenden IPERF-Befehlszeilenoptionen nicht angeben:

- -c: Clientmodus Option wird durch das Diagnose-Tool hinzugefügt.
- -s: Die Option für den Servermodus wird vom Diagnosetool hinzugefügt.
- -B: Die Bindung von IPERF an eine bestimmte IP/Schnittstelle erfolgt vom Diagnose-tool abhängig vom ausgewählten Pfad.
- -p: Die Portnummer wird im Diagnose-Tool angegeben.
- -i: Ausgabeintervall in Sekunden.
- -t: Gesamtdauer des Tests in Sekunden.

- 6. Wählen Sie die WAN-zu-LAN-Pfade aus, auf denen Sie den Diagnoseverkehr senden möchten. Wählen Sie auf beiden Appliances denselben Pfad aus.
- 7. Klicken Sie auf beiden Geräten auf **Start**.

Das Ergebnis zeigt den Modus (Client oder Server) der ausgewählten Appliance und den TCP- oder UDP-Port an, auf dem der Test ausgeführt wird. Es zeigt regelmäßig die übertragenen Daten und die Bandbreite an, die für das angegebene Intervall genutzt wurde, bis die Gesamtdauer des Tests erreicht ist.

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

Diagnostics Tool

Tool Mode: ClientTraffic Type: DataPort: 10

Iperf:LAN to WAN Paths: MCN_184_78-Broadband

Start

Results

stop

Client connecting to 172.16.31.10, TCP port 10
Binding to local address 172.16.21.10
TCP window size: 112 KByte (default)

| [ID] | Interval | Transfer | Bandwidth |
|-------|--------------|-------------|----------------|
| [3] | 0.0~ 1.0 sec | 10.1 MBytes | 84.9 Mbits/sec |
| [3] | 1.0~ 2.0 sec | 11.9 MBytes | 99.6 Mbits/sec |
| [3] | 2.0~ 3.0 sec | 13.4 MBytes | 112 Mbits/sec |
| [3] | 3.0~ 4.0 sec | 15.1 MBytes | 127 Mbits/sec |
| [3] | 4.0~ 5.0 sec | 14.5 MBytes | 122 Mbits/sec |
| [3] | 5.0~ 6.0 sec | 14.5 MBytes | 122 Mbits/sec |
| [3] | 6.0~ 7.0 sec | 15.1 MBytes | 127 Mbits/sec |
| [3] | 7.0~ 8.0 sec | 15.1 MBytes | 127 Mbits/sec |
| [3] | 8.0~ 9.0 sec | 15.6 MBytes | 131 Mbits/sec |
| [3] | 9.0~10.0 sec | 16.0 MBytes | 134 Mbits/sec |
| [3] | 0.0~10.0 sec | 141 MBytes | 118 Mbits/sec |

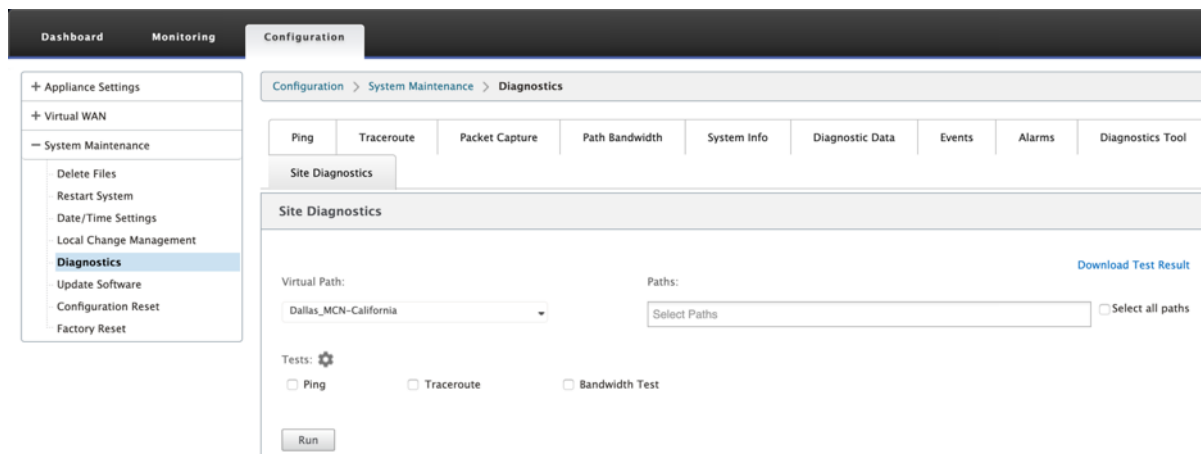
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

941

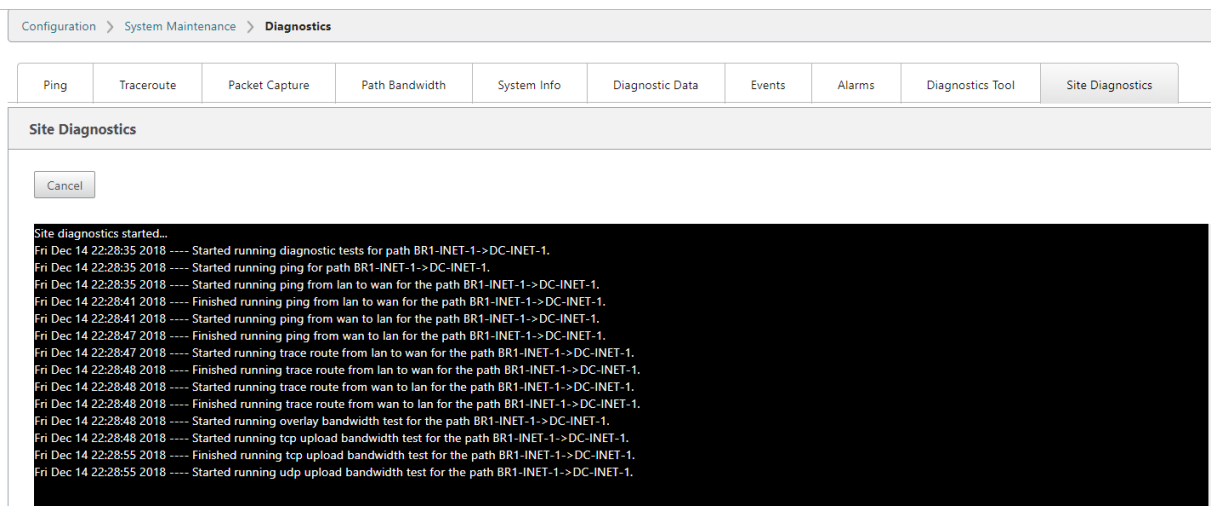
Site-Diagnose

Sie können die Bandbreitennutzung testen, pingen und Traceroute für die WAN-Verbindungen durchführen, die an verschiedenen Standorten im Citrix SD-WAN-Netzwerk konfiguriert wurden. Es enthält Informationen, die bei der Behebung von Problemen in der vorhandenen Konfiguration helfen.

Um **Standortdiagnose** zu verwenden, navigieren Sie zu **Konfiguration** erweitern Sie **Systemwartung > Diagnose** und wählen Sie **Diagnose-Tool**.



- **Schnittstellenstatus:** Gibt den Namen der Schnittstelle, die Anzahl der mit der Schnittstelle verknüpften Firewall-Zonen, die VLAN-ID und die zugehörigen Ports an.
- **Pfadstatus:** Enthält die Details der privaten Ziel-IP, Gateway-IP, Öffentliche Ziel-IP, Partner-IP, Öffentliche Partner-IP-Adressen. Es zeigt auch den Status des Gateway-ARP und der Pfad-MTU an.
- **Ping-Ergebnis:** Gibt die Richtung, den Status, die Anzahl (einschließlich der Anzahl der Versuche und Fehler) und die RTT des Pings an.
- **Traceroute-Ergebnis:** Gibt die Richtung, den Status, die Anzahl der Hops und die IP-Adresse oder RTT der Hops an.
- **Bandbreitenergebnis:** Liefert den Status von TCP und UDP zusammen mit der verwendeten Bandbreite (in KBit/s) für das Overlay- und Underlay-Netzwerk. Im Vergleich zu UDP ist die von TCP verwendete Bandbreite höher, da UDP bandbreitenbasiert ist und daher nur die konfigurierte Bandbreite verwendet. TCP ist ein Hochlaufprotokoll; basierend auf der zugrunde liegenden Netzwerkkonfiguration kann die Nutzung eine höhere Bandbreite im Vergleich zur konfigurierten Bandbreite melden.



Verbesserte Pfadzuordnung und Bandbreitennutzung

May 10, 2021

Erweiterungen zur Pfadzuordnung und Bandbreitennutzung werden auf der Registerkarte Überwachung implementiert, um Datenverkehrsflüsse anzuzeigen. Wenn beispielsweise nur ein virtueller Pfad eine Netzwerkverbindung bereitstellt und dieser virtuelle Pfad inaktiv wird, wird ein neuer optimaler Pfad ausgewählt, und der anfängliche Pfad wird zum letzten besten Pfad. Dieses Szenario wird implementiert, wenn der Bedarf an Bandbreite geringer ist und nur ein Pfad gewählt wird.

Wenn mehr als ein virtueller Pfad eine Verbindung bereitstellt, bemerken Sie einen aktuellen besten Pfad und den nächstbesten Pfad, falls verfügbar. Wenn nur ein Pfad zur Verarbeitung des Datenverkehrs vorhanden ist, vorausgesetzt, dass mehr als zwei Pfade verarbeitet werden und die Pfadtabelle mit zwei Pfaden aktualisiert wird, zeigt die Registerkarte Überwachung in der SD-WAN-GUI für Flows den aktuellen besten Pfad als ersten Pfad und den nächsten separaten Pfad mit Komma als den letzten besten Pfad an. Dieses Szenario wird implementiert, wenn mehr Pfade mit Bedarf an Bandbreite benötigt werden.

Überwachen von DPI-Anwendungsinformationen in der SD-WAN-GUI

Der Name des DPI-Anwendungsobjekts im Monitoring-Flow wird gespeichert und auf der Seite **SD-WAN-GUI-Überwachung -> Flows** angezeigt. Zur Identifizierung der DPI-Anwendung wird eine Quick-Info angezeigt.

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Monitoring > Flows

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows Toggle Columns

| Source IP Address | Dest IP Address | Direction | Source Port | Dest Port | IPP | IP DSCP | Hit Count | Service Type | Service Name | LAN GW IP | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps |
|-------------------|-----------------|------------|-------------|-----------|-----|---|-----------|--------------|--------------|-----------|----------|---------|----------|-------|---------------|----------------------------|
| 172.16.14.99 | 172.16.19.167 | LAN to WAN | 80 | 2189 | TCP | default | 41572 | Virtual Path | DC-BR | LOCAL | 758 | 41571 | 14527110 | 2.072 | 6.337 | 0.8 |
| 172.16.14.99 | 172.16.19.162 | LAN to WAN | 80 | 3161 | TCP | Override = NO Demote on Large Packets = NO | | | | | 361 | 41525 | 14427708 | 2.099 | 6.488 | 0.8 |
| 172.16.14.99 | 172.16.19.161 | LAN to WAN | 80 | 6310 | TCP | Separate TCP ACK Class = NO Packet Sequence Inorder = YES | | | | | 60 | 41827 | 14468200 | 2.115 | 6.341 | 0.8 |
| 172.16.14.99 | 172.16.19.170 | LAN to WAN | 80 | 10844 | TCP | Inorder Holdtime: 900 Late Packet Action = DISCARD | | | | | 360 | 41863 | 14393387 | 2.110 | 6.285 | 0.8 |
| 172.16.14.99 | 172.16.19.164 | LAN to WAN | 80 | 3387 | TCP | Packet Duplication = NO Persistent Paths = NO | | | | | 358 | 41798 | 14472656 | 2.070 | 6.284 | 0.8 |
| 172.16.14.215 | 172.16.19.99 | LAN to WAN | 9321 | 80 | TCP | Reliable = YES | | | | | 14 | 43483 | 2592802 | 2.145 | 1.022 | 0.8 |
| 172.16.14.99 | 172.16.19.167 | LAN to WAN | 80 | 4200 | TCP | TCP Standalone ACKs = NO | | | | | 112 | 41705 | 14426227 | 2.114 | 6.348 | 0.8 |
| 172.16.14.99 | 172.16.19.169 | LAN to WAN | 80 | 3161 | TCP | Check Flow TOS = NO | | | | | 356 | 40970 | 14508376 | 2.054 | 6.299 | 0.8 |
| 172.16.14.218 | 172.16.19.99 | LAN to WAN | 3371 | 80 | TCP | GRE Header Compression = NO | | | | | 407 | 42980 | 2552820 | 2.043 | 0.967 | 0.8 |
| 172.16.14.99 | 172.16.19.166 | LAN to WAN | 80 | 1116 | TCP | Packet Aggregation = NO | | | | | 113 | 41286 | 14568312 | 2.047 | 6.220 | 0.8 |
| 172.16.14.213 | 172.16.19.99 | LAN to WAN | 17082 | 80 | TCP | TCP Termination = NO | | | | | 161 | 42915 | 2556999 | 2.114 | 1.006 | 0.8 |
| 172.16.14.217 | 172.16.19.99 | LAN to WAN | 4090 | 80 | TCP | Rule ID = 1 VLAN ID = 0 App Rule ID = N/A DPI Application = http | | | | | 364 | 42530 | 2540882 | 2.059 | 0.983 | 0.8 |

Überwachung von Pfadinformationen für den Datenfluss in der SD-WAN-GUI

Es ist möglich, dass basierend auf der eingehenden Datenverkehrsrate eine oder mehrere Pfade erforderlich sind, um den Datenverkehr zu verarbeiten.

Überprüfen Sie die folgenden Szenarien, um zu bestimmen, wie Pfadzuordnung durchgeführt wird:

Lastausgleich Übertragungsmodus:

Die folgende Abbildung zeigt das Szenario, wenn der Datenverkehr initiiert wird und alle Pfade gut sind. Ein optimierter Pfad wird gewählt, da der Bandbreitenbedarf ausreicht, um von einem Pfad bedient zu werden. Sie stellen fest, dass nur ein Pfad **DC-MCN-Internet > BR1-VPX-Internet** gewählt wird und der Typ des Übertragungstyps als **Load Balanced** angezeigt wird.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

| Service Name | LAN GW IP | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|----------------|-----------|----------|---------|--------|--------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|-----------------------------------|-----------------------------|-------------------------|-------------|
| DC-MCN-BR1-VPX | LOCAL | 3 | 291 | 435918 | 85.373 | 1023.106 | 36.881 | 0.000 | 52 | N/A | 15 | BULK | DC-MCN-Internet->BR1-VPX-Internet | N/A | Load Balanced, Reliable | iperf |

Die folgende Abbildung zeigt, wenn der Datenverkehr fließt und die WAN-Attribute des Pfads beeinträchtigt werden. Sie stellen fest, dass ein neuer Pfad für die Verarbeitung von Datenverkehr ohne Unterbrechung ausgewählt wird. In diesem Fall können Sie mit der Pfadzuordnungsfunktion angeben, dass der aktuelle beste Pfad, der den Datenverkehr verarbeitet, **DC-MCN-Internet2 -> BR1-VPX-Internet** ist und der letzte beste Pfad, der den Datenverkehr verarbeitet hat, **DC-MCN-Internet -> BR1-VPX-Internet** ist.

Der letzte beste Pfad in diesem Beispiel ist ein Indikator dafür, welcher Pfad die Verbindung früher bedient hat.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

| Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|---------|---------|-------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|--|-----------------------------|-------------------------|-------------|
| 728 | 1090544 | 0.983 | 11.778 | 0.425 | 0.000 | 52 | N/A | 15 | BULK | DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet | N/A | Load Balanced, Reliable | iperf |

Die folgende Abbildung zeigt, dass, wenn der Datenverkehr läuft und mehr als ein Pfad für die Datenverarbeitung aufgrund der Nachfrage in Bandbreite ausgewählt wird, wie unten gezeigt, mehr als ein Pfad ausgewählt wird, wenn der Datenverkehr gesendet wird. Anders als im obigen Fall kann es hier mehr als zwei Pfade geben, die den Datenverkehr bedienen, aber in der GUI werden nur die beiden besten Pfade angezeigt, die derzeit dem Datenverkehr dienen.

Beachten Sie **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-Internet2->BR1-VPX-Internet**sind die beiden Pfade, die in der Tabelle **Flows Data**angezeigt werden.

Hinweis

Wie angegeben, werden nur maximal zwei Pfade in der Flow-Tabelle angezeigt.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

| ets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|-----|---------|---------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|--|-----------------------------|-------------------------|-------------|
| 155 | 1280790 | 318.598 | 3818.082 | 137.634 | 0.000 | 52 | N/A | 15 | BULK | DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-Internet-2->BR1-VPX-Internet | N/A | Load Balanced, Reliable | iperf |

Die folgende Abbildung zeigt, dass, wenn der aktuelle beste Pfad, der **DC-MCN-Internet->BR1-VPX-Internet ist, in WAN-Attributen** nicht verfügbar/inaktiv/degradiert ist, der aktuell beste Pfad wird zuerst im Pfadabschnitt der Tabelle **Flows Data** angezeigt gefolgt von dem letzten besten Pfad, der dem Verkehr dient.

Da das **DC-MCN-Internet->BR1-VPX-Internet** nicht mehr am besten war, wurde ein neuer aktueller bester Pfad vom System als **DC-MCN-MPLS->BR1-VPX-MPLS** gewählt, und der letzte beste Pfad, der aktiv Verbindung zusammen mit dem aktuellen besten Pfad dient, ist **DC-MCN-Internet2->BR1-VPX-Internet**, da beide für den aktuellen Datenverkehr Bedarf an Bandbreite benötigt werden.

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

| ackets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|--------|---------|---------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|--|-----------------------------|-------------------------|-------------|
| 2764 | 4140472 | 170.434 | 2042.476 | 73.627 | 0.000 | 52 | N/A | 15 | BULK | DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet | N/A | Load Balanced, Reliable | iperf |

Doppelter Übertragungsmodus

Der allgemeine Paketduplizierungsmodus stellt sicher, dass zunächst zwei Pfade für die Verarbeitung von Paketen derselben Verbindung verwendet werden, um eine zuverlässige Zustellung durch Duplizieren von Paketen über zwei separate Pfade zu gewährleisten.

Bei der Pfadzuordnung stellen Sie fest, dass zwei Pfade im Pfadabschnitt der Flow-Tabelle verwendet werden, solange zwei Pfade vorhanden sind, um Flows durch Duplizieren zu verarbeiten.

Die folgende Abbildung zeigt, dass wen Verkehr fließt, es kann bemerkt werden, dass zwei Pfade gezeigt werden, um den Verkehr zu verarbeiten. Im Gegensatz zu jedem anderen Modus, selbst wenn der Datenverkehr weniger Bandbreite erfordert, die nur durch einen Pfad bereitgestellt werden kann, wird dieser Modus immer den Datenverkehr über zwei Pfade duplizieren, um eine zuverlässige Anwen-

dungsbereitstellung zu gewährleisten.

Sie sehen in der folgenden Abbildung zwei Pfade im Pfadabschnitt der Tabelle **Flows Data** ; **DC-MCN-Internet2->BR-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS** .

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☐ Internet Load Balancing Table

☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

| Flow ID | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|---------|---------|---------|---------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|--|-----------------------------|---------------------|-------------|
| 3 | 551 | 32640 | 88.836 | 42.100 | 38.377 | 0.000 | 0 | N/A | 9 | BULK | DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS | N/A | Duplicate, Reliable | iperf |
| 4 | 1651 | 2362062 | 262.860 | 3008.560 | 113.555 | 0.000 | 72 | N/A | N/A | N/A | N/A | N/A | Duplicate, Reliable | iperf |

Die folgende Abbildung zeigt, dass, wenn der Datenverkehr fließt, wenn einer der aktuellen besten Pfade inaktiv wird, ein anderer Pfad ausgewählt wird, und es weiterhin zwei Pfade als Teil des Pfadabschnitts in der Tabelle **Flows Data** gibt.

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☐ Internet Load Balancing Table

☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

| Flow ID | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type |
|---------|----------|---------|----------|---------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|--|-----------------------------|---------------------|
| CAL | 10 | 9692 | 530732 | 75.025 | 32.705 | 32.411 | 0.000 | 0 | N/A | 9 | BULK | DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet | N/A | Duplicate, Reliable |
| CAL | 0 | 34213 | 49055970 | 267.264 | 3066.058 | 115.458 | 0.000 | 72 | N/A | N/A | N/A | N/A | N/A | Duplicate, Reliable |

Übertragungsmodus für Persistente Pfade

Persistenter Pfadübertragungsmodus hilft, Pakete eines Flusses basierend auf der Pfadlatenzimpedanz beizubehalten.

Die folgende Abbildung zeigt nur einen Pfad, der der beste Pfad ist, der derzeit die Flows und seine Pakete verarbeitet. Es gibt keine Nachfrage nach Bandbreite und ein Pfad dient alles. Derzeit gibt es nur einen besten Pfad, der **DC-MCN-Internet->BR1-VPX-Internet** ist.

Flows Data

Toggle Columns

| Service Type | Service Name | LAN GW IP | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|--------------|----------------|-----------|----------|---------|-------|-------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|-----------------------------------|-----------------------------|-------------------|-------------|
| Local Path | DC-MCN-BR1-VPX | LOCAL | 662 | 3 | 4494 | 1.127 | 13.511 | 0.487 | 0.000 | 4 | N/A | 9 | BULK | DC-MCN-Internet->BR1-VPX-Internet | N/A | Persistent | iperf |

Die folgende Abbildung zeigt, dass, wenn der Pfad **DC-MCN-Internet->BR1-VPX-Internet** latenzanfällig wird oder deaktiviert ist, Sie feststellen, dass der neue Pfad wirksam wird und der aktuelle Pfad **DC-MCN-Internet->BR1-VPX-Internet** zum letzten besten Pfad wird.

Der neue Pfad Abschnitt zeigt also **DC-MCN-MPLS->BR1-VPX-MPLS**, **DC-MCN-Internet->BR1-VPX-Internet**.

Flows Data

Toggle Columns

| IN / IP | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|---------|----------|---------|-------|-------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|--|-----------------------------|-------------------|-------------|
| ICAL | 950 | 41 | 61418 | 0.992 | 11.894 | 0.429 | 0.000 | 4 | N/A | 9 | BULK | DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet | N/A | Persistent | iperf |

Im persistenten Modus können mehrere Pfade für die Verarbeitung des Datenverkehrs ausgewählt werden. In diesem Fall zeigt die grafische Benutzeroberfläche sowohl die Pfade mit dem besten als auch die nächsten besten im Pfadabschnitt der Flow-Tabelle vom Anfang des Verkehrsflusses an.

Die folgende Abbildung zeigt, dass der Fluss zunächst nur mehr als zwei Pfade benötigt und dauerhaft bleibt, solange es keine Pfadlatenz-Impedanzüberquerung (50 ms) gibt. Die beiden Pfade werden als dargestellt: **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS**.

Flows Data

Toggle Columns

| | Age (mS) | Packets | Bytes | PPS | Customer kbps | Virtual Path Overhead kbps | IPsec Overhead kbps | Rule ID | App Rule ID | Class | Class Type | Path | Hdr Compression Saved Bytes | Transmission Type | Application |
|---|----------|---------|----------|---------|---------------|----------------------------|---------------------|---------|-------------|-------|------------|--|-----------------------------|-------------------|-------------|
| L | 51 | 6368 | 367504 | 128.449 | 59.303 | 55.490 | 0.000 | 2 | N/A | 9 | BULK | DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS | N/A | Persistent | iperf |
| L | 1 | 9694 | 13894396 | 195.491 | 2241.576 | 84.452 | 0.000 | 74 | N/A | N/A | N/A | | N/A | Persistent | iperf |

Angenommen, einer der besten Pfade, die **DC-MCN-Internet** in hohe Latenz geht oder deaktiviert ist. Dadurch wird ein neuer Pfad angezeigt und der neue Pfad kann der beste Pfad sein oder könnte der zweitbeste Pfad sein, basierend auf der Entscheidung der Pfadauswahl zu diesem Zeitpunkt.

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 | Persistent | iperf |

Fehlerbehebung bei Management-IP

May 10, 2021

Im Folgenden sind die möglichen Szenarien aufgeführt, die beim Konfigurieren der DHCP-IP-Adresse auftreten können. Es enthält auch Best Practices und Empfehlungen für die Konfiguration der DHCP-Verwaltungs-IP-Adresse bei der Bereitstellung von SD-WAN-Appliances.

Diese Empfehlungen gelten für alle Plattformmodelle von SD-WAN; Standard Edition, WANOP und Premium (Enterprise) Edition - Physikalische und virtuelle Appliances.

Hinweis

Alle Hardwaremodellen von SD-WAN-Appliances werden mit einer werkseitigen Standardverwaltungs-IP-Adresse ausgeliefert. Stellen Sie sicher, dass Sie während des Setup-Vorgangs die erforderliche DHCP-IP-Adresse für die Appliance konfigurieren.

Allen virtuellen Modellen von SD-WAN-Appliances (VPX-Modelle) und Appliances, die in AWS-Umgebung bereitgestellt werden können, ist keine werkseitige Standard-IP-Adresse zugewiesen.

Appliances werden eingeschaltet, ohne dass DHCP-Server erreichbar sind:

- Ursachen:
 - Ethernet-Verwaltungskabel wird getrennt
 - DHCP-Dienst ist für das angeschlossene Netzwerk ausgefallen
- Erwartetes Verhalten
 - Appliances mit aktiviertem DHCP-Dienst wiederholen die DHCP-Anforderung alle 300 Sekunden (Standardwert). Das tatsächliche Intervall beträgt ca. 7 Minuten
 - Daher erwerben Appliances mit aktiviertem DHCP-Dienst DHCP-Adressen innerhalb von 7 Minuten, nachdem DHCP-Server verfügbar sind. Die Verzögerung reicht von 0 bis 7 Minuten

Die zugewiesene DHCP-Adresse läuft ab:

- Erwartetes Verhalten:
 - Appliances mit aktiviertem DHCP-Dienst versuchen, die Lease zu erneuern, bevor die Adresse abläuft
 - Appliances beginnen mit der neuen DHCP-Erkennung, wenn die Verlängerung fehlschlägt

Appliances mit aktiviertem DHCP-Dienst werden von einem DHCP-aktivierten Subnetz in ein anderes Subnetz verschoben:

- Ursachen: Appliances wechseln von einem zugewiesenen DHCP-Subnetz in ein anderes DHCP-Subnetz
- Erwartetes Verhalten:
 - Bei einer dauerhaften DHCP-IP-Adresszuweisung müssen die Appliances möglicherweise neu gestartet werden, um eine IP-Adresse vom neuen DHCP-Server abrufen zu können.
 - Nach Ablauf der DHCP-Lease können Appliances das DHCP-Erkennungsprotokoll erneut initiieren, wenn der aktuelle DHCP-Server nicht erreichbar ist.

- Appliances erwerben neue IP-Adressen mit einer Verzögerung von 8 Minuten. Die Gateway IP-Adresse wird in der GUI und CLI nicht geändert. Es wird aktualisiert, nachdem der Neustartvorgang abgeschlossen ist.

Empfehlung:

- Weisen Sie immer eine permanente Lease für DHCP-Adressen zu, die Citrix SD-WAN Appliances zugewiesen sind (physisch/virtuell). Auf diese Weise können Appliances eine vorhersehbare Verwaltungs-IP-Adresse haben.

Sitzungsbasierte HTTP-Benachrichtigungen

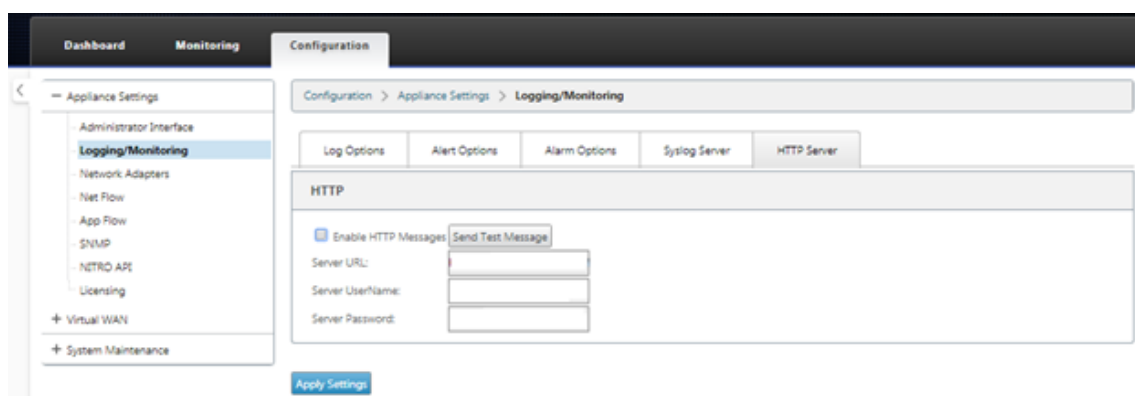
May 10, 2021

Sie können jetzt Ereignis- und Alarmberichte für generische HTTP-POST-API-Dienstanforderungen in der Benutzeroberfläche der Citrix SD-WAN Appliance konfigurieren. Die Konfiguration des HTTP-Alarms und der Ereignisbenachrichtigung ähnelt den E-Mail- und SNMP-Ereignissen für Ereignisse und Alarmer, die in SD-WAN unterstützt werden.

Die sitzungsbasierte HTTP-Postbenachrichtigung wird an einen externen Dienst gesendet, z. B. Service Now. Die Ereignisbenachrichtigungen für den HTTP-Server können in der Benutzeroberfläche der Citrix SD-WAN Appliance und im Citrix SD-WAN Center konfiguriert werden.

So konfigurieren Sie HTTP-POST-Benachrichtigungen in der Benutzeroberfläche der Citrix SD-WAN-Appliance:

1. Navigieren Sie zu **Konfiguration > Logging/Überwachung > HTTP-Server**.



2. Klicken Sie auf **HTTP-Nachrichten aktivieren**.
3. Geben Sie die **Server-URL** des HTTP-Servers ein, von dem Sie Benachrichtigungen erhalten möchten. Geben Sie den **Serverbenutzernamen** und das **Serverkennwort** ein.

Configuration > Appliance Settings > Logging/Monitoring

Log Options Alert Options Alarm Options Syslog Server HTTP Server

HTTP

☒ Enable HTTP Messages [Send Test Message](#)

Server URL:

Server UserName:

Server Password:

[Apply Settings](#)

4. Klicken Sie auf **Einstellungen anwenden**. Die Seite wird aktualisiert, nachdem die Einstellungen für die HTTP-Server-Benachrichtigungen angewendet wurden.

Hinweis

Verwenden Sie die Option **Testnachricht senden**, um zu überprüfen, ob die HTTP-Serververbindung erfolgreich ist.

So fügen Sie Warnbenachrichtigungen für HTTP-Serversitzung hinzu:

1. Wechseln Sie auf der Seite **Logging/Überwachung** zur Registerkarte **Alarmoptionen**.
2. Klicken Sie auf **Alarm hinzufügen**.

Configuration > Appliance Settings > Logging/Monitoring

Log Options Alert Options Alarm Options Syslog Server HTTP Server

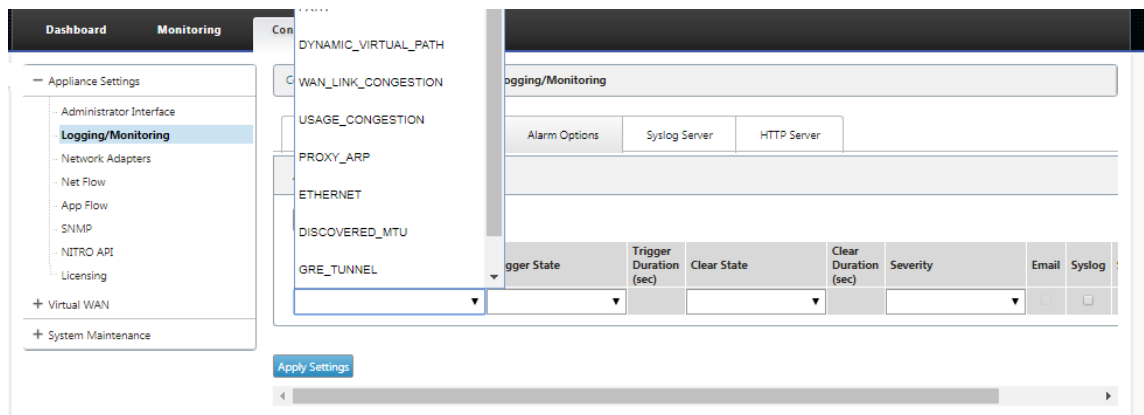
Alarm Configuration

[Add Alarm](#)

| Event Type | Trigger State | Trigger Duration (sec) | Clear State | Clear Duration (sec) | Severity | Email | Syslog |
|----------------------|----------------------|------------------------|----------------------|----------------------|----------------------|--------------------------|--------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |

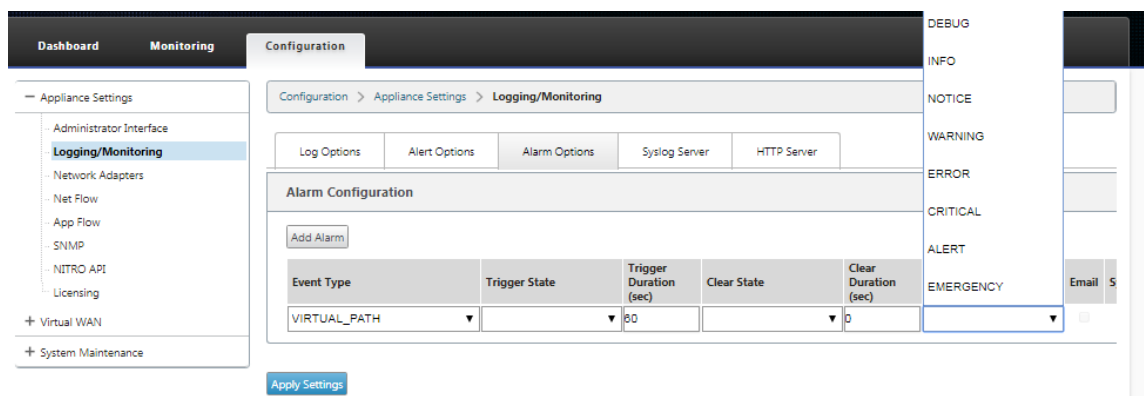
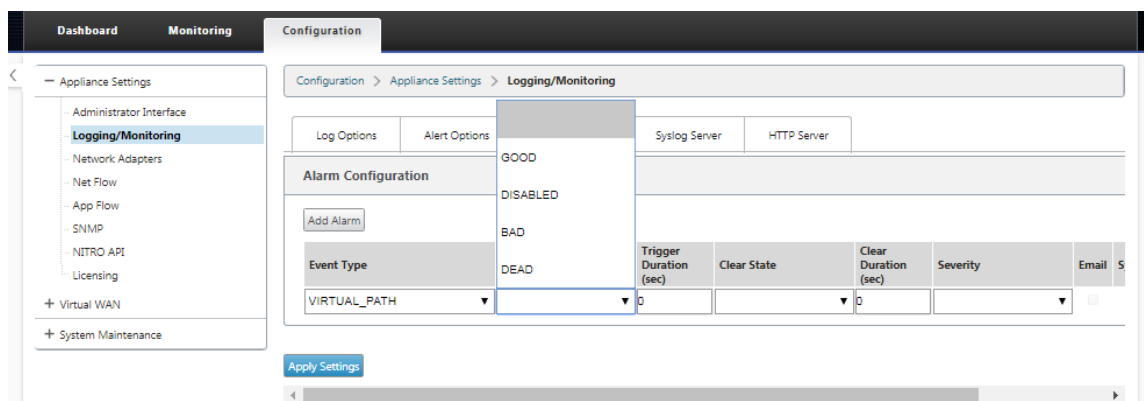
[Apply Settings](#)

3. Wählen Sie in der Dropdown-Liste einen **Ereignistyp** aus.



4. Wählen Sie folgende Alarmbenachrichtigungszustände für den gewählten **Ereignistyp** aus. Der Triggerstatus und der Clear-Status ändern sich entsprechend dem ausgewählten Ereignistyp.

- Auslösezustand —GOOD, DISABLED, BAD, DEAD
- Auslösedauer —Zeit in Sekunden
- Clear State - GOOD, DISABLED, BAD, DEAD
- Dauer löschen —Zeit in Sekunden
- Schweregrad —DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, EVENT, EMERGENCY



5. Aktivieren Sie die Kontrollkästchen **Syslog** und **HTTP**, um Benachrichtigungen zu empfangen, die für die Ereignisse Syslog und HTTP-Server spezifisch sind. Klicken Sie auf **Einstellungen**

anwenden.

Configuration > Appliance Settings > Logging/Monitoring

Log OptionsAlert OptionsAlarm OptionsSyslog ServerHTTP Server

Alarm Configuration

Add Alarm

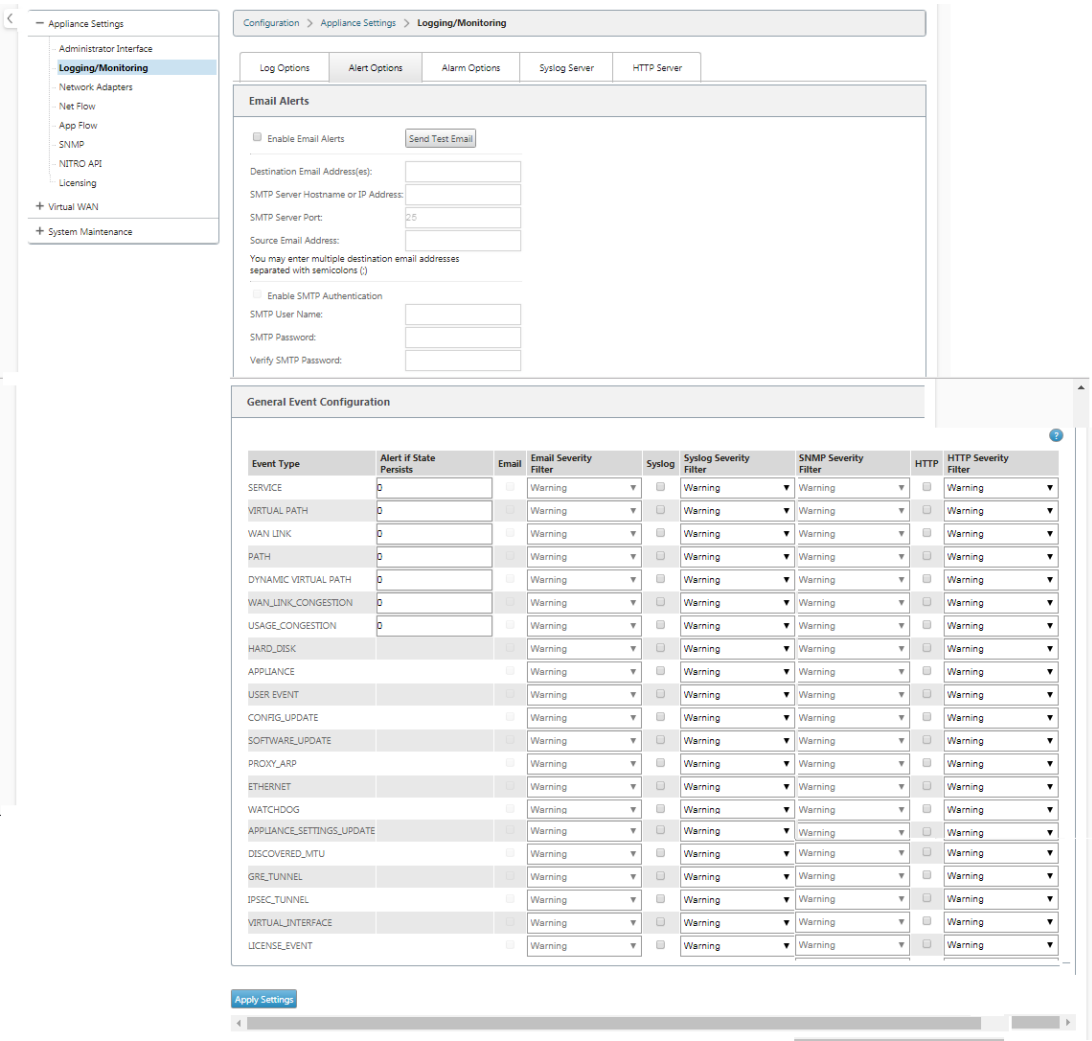
| Event Type | Trigger State | Trigger Duration (sec) | Clear State | Clear Duration (sec) | Severity | Email | Syslog | SNMP | HTTP |
|--------------|---------------|------------------------|-------------|----------------------|----------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|
| VIRTUAL_PATH | DEAD | 60 | BAD | 60 | NOTICE | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Apply Settings

So konfigurieren Sie Ereignisoptionen:

Wechseln Sie zur Registerkarte **Warnungsoptionen** . Wählen Sie auf der Seite **Allgemeine Ereigniskonfiguration** den HTTP-Server-Benachrichtigungsfilter für einen **Ereignistyp** aus, und klicken Sie auf **Einstellungen anwenden** .

- HTTP
- HTTP-Schweregrad Filter



Konfigurieren von HTTP-Benachrichtigungen in Citrix SD-WAN Center

So konfigurieren Sie HTTP-Benachrichtigungen:

1. Navigieren Sie zu **Fehler > Benachrichtigungseinstellungen > HTTP**.

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Nitro API

<

Event Viewer

Notification Settings

Severity Settings

Fault / Notification Settings / HTTP

Email AlertsSNMP TrapsSyslogHTTP

HTTP

☒ Enable HTTP Messages

Server Url:
https://10.102.78.154/tes...

Server Username:
admin

Server Password:
password

Apply

Send Test Message

2. Geben Sie die **Server-URL**, den **Serverbenutzernamen** und das **Serverkennwort** für den HTTP-Server ein.
3. Klicken Sie auf **Anwenden**

So konfigurieren Sie Einstellungen für den Schweregrad:

1. Rufen Sie die Seite **Einstellungen für Schweregrad** auf. Klicken Sie auf **Aktivieren**, um die Überwachung von HTTP-Benachrichtigungen für einen ausgewählten Ereignistyp zu starten.

| | | Email | | Syslog | | SNMP | | HTTP | |
|----------------------|-------------------------|--------------------------|-----------------|--------------------------|-----------------|--------------------------|-----------------|--------------------------|-----------------|
| Event Type | Alert if State Persists | Enable | Severity Filter | Enable | Severity Filter | Enable | Severity Filter | Enable | Severity Filter |
| SERVICE | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| VIRTUAL PATH | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| WANLINK | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| PATH | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| DYNAMIC VIRTUAL PATH | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| WAN LINK CONGESTION | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| USAGE CONGESTION | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |

Enable sending event notifications via HTTP Notifications for the current Event Type.

2. Sie können die E-Mail-, Syslog-, SNMP- und HTTP-Ereignisbenachrichtigungen für die folgenden Ereignistypen überwachen. Klicken Sie auf **Übernehmen**.

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Nitro API

<

Event Viewer

Notification Settings

Severity Settings

Fault / Severity Settings

| Event Type | Alert If State Persists | Email | | Syslog | | SNMP | | HTTP | |
|---------------------------|-------------------------|--------------------------|-----------------|--------------------------|-----------------|--------------------------|-----------------|--------------------------|-----------------|
| | | Enable | Severity Filter | Enable | Severity Filter | Enable | Severity Filter | Enable | Severity Filter |
| SERVICE | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| VIRTUAL PATH | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| WANLINK | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| PATH | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| DYNAMIC VIRTUAL PATH | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| WAN LINK CONGESTION | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| USAGE CONGESTION | Alert Immediately ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| HARD DISK | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| APPLIANCE | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| USER EVENT | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| CONFIG UPDATE | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| SOFTWARE UPDATE | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| PROXY ARP | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| ETHERNET | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| WATCHDOG | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| SD WAN CENTER SYSTEM | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| APPLIANCE SETTINGS UPDATE | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| SD WAN CENTER USER | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| SD WAN CENTER STORAGE | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| SD WAN CENTER DATABASE | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| CONNECTION TO VIRTUAL WAN | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| DISCOVERED MTU | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| GRE TUNNEL | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| IPSEC TUNNEL | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| VIRTUAL INTERFACE | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |
| LICENSE EVENT | | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ | <input type="checkbox"/> | WARNING ▼ |

Apply

Aktive Bandbreitentests

May 10, 2021

Aktive Bandbreitentests ermöglichen Ihnen die Möglichkeit, einen sofortigen Pfadbandbreitentest über eine öffentliche Internet-WAN-Verbindung durchzuführen oder öffentliche WAN-Bandbreitentests zu bestimmten Zeiten auf einer wiederkehrenden Basis durchzuführen. Diese

Funktion ist nützlich, um zu demonstrieren, wie viel Bandbreite zwischen zwei Standorten während neuer und bestehender Installationen zur Verfügung steht, sowie zum Testen von Pfaden, um das Ergebnis von Einstellungs- und Bestätigungsänderungen zu bestimmen, z. B. das Anpassen von DSCP-Tag-Einstellungen oder zulässigen Bandbreitenraten.

So verwenden Sie die aktive Bandbreitenprüffunktion:

1. Navigieren Sie zu **Systemwartung > Diagnose > Pfadbandbreite**.
2. Wählen Sie den gewünschten **Pfad** aus und klicken Sie auf **Test**.

The screenshot displays the Citrix SD-WAN 11.2 web interface. The left sidebar shows the navigation menu with 'Diagnostics' selected. The main content area is titled 'Configuration > System Maintenance > Diagnostics'. Under the 'Diagnostics' tab, the 'Path Bandwidth' sub-tab is active. The 'Instant Path Bandwidth Testing' section shows a selected path 'MCN-5100-WL-2->BR572-1' and a 'Test' button. Below this, the 'Results' section displays summary statistics: Minimum Bandwidth: 288584 kbps, Maximum Bandwidth: 1213863 kbps, and Average Bandwidth: 1109046 kbps. The 'Schedule Path Bandwidth Testing' section includes an 'Add' button and a table for scheduling tests. The 'History Path Bandwidth Testing Result' section shows a table of test results with columns for Num, From Link, To Link, Test Time, Min Bandwidth (kbps), Max Bandwidth (kbps), and Avg Bandwidth (kbps). The table contains 27 entries, showing a range of bandwidth values over time.

| Num | From Link | To Link | Test Time | Min Bandwidth (kbps) | Max Bandwidth (kbps) | Avg Bandwidth (kbps) |
|-----|----------------|---------------|------------------------|----------------------|----------------------|----------------------|
| 1 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 2:01:03 PM | 2883972 | 5099707 | 4357330 |
| 2 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 4:01:03 PM | 3109115 | 3872000 | 3616157 |
| 3 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 6:01:04 PM | 3041280 | 4119960 | 3518949 |
| 4 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 8:01:04 PM | 2769377 | 3700672 | 3276124 |
| 5 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/17/2018, 10:01:04 PM | 409245 | 3574153 | 2489269 |
| 6 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 12:01:04 AM | 2481756 | 4001684 | 3198214 |
| 7 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 2:01:04 AM | 2548853 | 3872000 | 3236546 |
| 8 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 4:01:03 AM | 3204413 | 3982628 | 3642643 |
| 9 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 6:01:03 AM | 2997677 | 4672357 | 3664018 |
| 10 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 8:01:04 AM | 2248258 | 6288360 | 3612666 |
| 11 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 10:01:04 AM | 2410236 | 3372387 | 2816032 |
| 12 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 12:01:03 PM | 2613600 | 4401852 | 3563752 |
| 13 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 2:01:04 PM | 2324266 | 4059961 | 3101910 |
| 14 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 4:01:03 PM | 2173340 | 3684370 | 2929146 |
| 15 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 6:01:03 PM | 2613600 | 3589493 | 3021690 |
| 16 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 8:01:03 PM | 1676056 | 3499380 | 2655230 |
| 17 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/18/2018, 10:01:03 PM | 1954093 | 3558944 | 2975884 |
| 18 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 12:01:03 AM | 2161116 | 3784398 | 2902068 |
| 19 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 2:01:04 AM | 2986971 | 4079765 | 3821158 |
| 20 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 4:01:04 AM | 3514084 | 4181760 | 3893381 |
| 21 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 6:01:03 AM | 3358843 | 4059961 | 3756691 |
| 22 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 8:01:03 AM | 3216738 | 4245441 | 3716351 |
| 23 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 10:01:04 AM | 3558944 | 4202773 | 3932908 |
| 24 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 12:01:03 PM | 3427672 | 4267102 | 3838552 |
| 25 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 2:01:04 PM | 2874061 | 4224000 | 3608676 |
| 26 | RCN1-S100-WL-1 | MCN-5100-WL-1 | 2/19/2018, 4:01:03 PM | 2816000 | 6288360 | 4165337 |
| 27 | MCN-5100-WL-2 | BR572-1 | 2/19/2018, 5:23:04 PM | 936564 | 1213863 | 1109046 |

Die Ausgabe zeigt die durchschnittliche Bandbreite an, die als Wert verwendet wird, um die zulässige Rate für die WAN-Link-Mindest- und Maximalbandbreitenergebnisse des Tests festzulegen. Zusammen mit der Möglichkeit, die Bandbreite zu testen, können Sie nun die Konfigurationsdatei ändern, um die erlernte Bandbreite zu verwenden. Dies geschieht über die Option "Auto Learn" unter **Site > [Sitename] > WAN-Links > [WAN-Link-Name] > Einstellungen** und

wenn aktiviert, verwendet das System die gelernte Bandbreite.

Sie können auch wiederkehrende Tests der Pfadbandbreite in wöchentlichen, täglichen oder stündlichen Intervallen planen.

Schedule Path Bandwidth Testing

Add

| Path Name | Frequency | Day of Week | Hour | Minute | |
|-------------------|-----------|-------------|------|--------|---|
| DC_MPLS2->Branch_ | every day | Sunday | 0 | 0 | X |
| | every day | Sunday | 0 | 0 | ↺ |

Apply Settings

Hinweis

Unten auf dieser Seite wird eine Historie der Pfadbandbreiten-Testergebnisse angezeigt und die Ergebnisse werden alle sieben Tage archiviert.

Schedule Path Bandwidth Testing

Add

| Path Name | Frequency | Day of Week | Hour | Minute |
|-----------|-----------|-------------|------|--------|
|-----------|-----------|-------------|------|--------|

Apply Settings

History Path Bandwidth Testing Result

show 50 entries Showing 1 to 14 of 14 entries Search

| Num | From Link | To Link | Test Time | Min Bandwidth (kbps) | Max Bandwidth (kbps) | Avg Bandwidth (kbps) |
|-----|---------------|---------------|-----------------------|----------------------|----------------------|----------------------|
| 1 | BR_1-INET-1* | DC_MCN-INET-1 | 3/29/2017, 1:29:54 AM | 363140 | 780616 | 525927 |
| 2 | BR_1-INET-1* | DC_MCN-INET-1 | 3/29/2017, 1:30:00 AM | 281995 | 573073 | 430345 |
| 3 | BR_1-INET-1* | DC_MCN-INET-1 | 3/29/2017, 1:30:06 AM | 317568 | 636640 | 480818 |
| 4 | BR_1-MPLS-1 | DC_MCN-MPLS-1 | 3/29/2017, 1:34:00 AM | 440056 | 1083357 | 725514 |
| 5 | DC_MCN-INET-1 | BR_1-INET-1* | 3/29/2017, 1:34:10 AM | 506768 | 786784 | 638673 |
| 6 | DC_MCN-INET-1 | BR_1-INET-1* | 3/29/2017, 1:34:18 AM | 462584 | 1388712 | 669232 |
| 7 | DC_MCN-INET-1 | BR_1-WL-1 | 3/29/2017, 1:34:27 AM | 380679 | 727895 | 533286 |
| 8 | DC_MCN-MPLS-1 | BR_1-MPLS-1 | 3/29/2017, 1:35:12 AM | 26823 | 35495 | 30578 |
| 9 | DC_MCN-INET-1 | BR_1-INET-1* | 3/29/2017, 1:36:09 AM | 350097 | 733929 | 591542 |
| 10 | DC_MCN-INET-1 | BR_1-INET-1* | 3/29/2017, 1:36:47 AM | 476024 | 789756 | 639048 |
| 11 | DC_MCN-INET-1 | BR_1-WL-1 | 3/29/2017, 1:36:56 AM | 446292 | 777674 | 608533 |

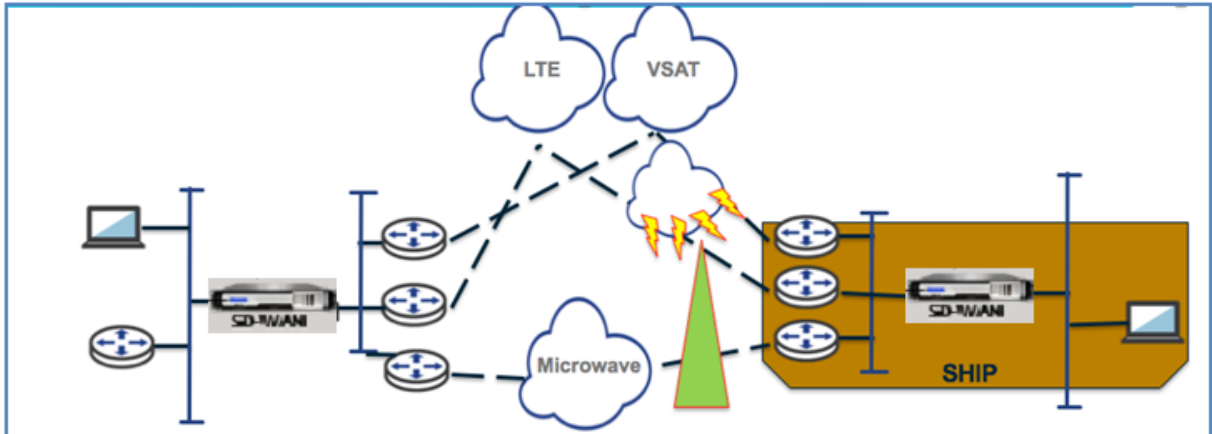
Adaptive Bandbreitenerkennung

May 10, 2021

Diese Funktion gilt für Netzwerke mit VSAT, LOS, Microwave, 3G/4G/LTE WAN-Verbindungen, für die die verfügbare Bandbreite je nach Wetter- und Umgebungsbedingungen, Standort und Standortverhältnissen variiert. Es ermöglicht den SD-WAN-Appliances, die Bandbreitenrate auf dem WAN-Link dynamisch basierend auf einem definierten Bandbreitenbereich (minimale und maximale

WAN-Verbindungsrate) anzupassen, um die maximale verfügbare Bandbreite zu nutzen, ohne die Pfade BAD zu markieren.

- Höhere Bandbreitenzuverlässigkeit (über VSAT, Mikrowelle, 3G/4G und LTE)
- Höhere Vorhersehbarkeit der adaptiven Bandbreite gegenüber vom Benutzer konfigurierten Einstellungen



So aktivieren Sie adaptive Bandbreitenerkennung:

Für diese Funktion ist die Option Empfindlichkeit bei schlechten Verlusten erforderlich, um als Voraussetzung aktiviert (Standard/Benutzerdefiniert) zu sein. Sie können es unter **Global > Autopath Groups > [Name der Autopath-Gruppe] > Bad Loss Sensitive** aktivieren.

1. Aktivieren Sie die **Adaptive Bandbreitenerkennung** unter **Global > Autopath-Gruppen > [Name der Autopath-Gruppe] > Bad Loss Sensitive**.
2. Navigieren Sie zu **Konfigurations-Editor > Standorte > [Sitenname] > WAN-Links > [WAN-Link-Name] > Einstellungen > Erweiterte Einstellungen**.

3. Aktivieren Sie das Kontrollkästchen **Adaptive Bandbreitenerkennung**, und geben Sie einen Wert in das Feld **Minimale akzeptable Bandbreite** ein.

4. Zeigen Sie die Tabelle **Verwendung und zulässige Sätze** an, indem Sie zu **Monitor > Statistik > WAN-Link-Nutzung > Nutzung** und **zulässige Sätze** navigieren.

Usages and Permitted Rates

Filter: in Any column

Show 100 entries Showing 1 to 4 of 4 entries

| WAN Link | Service | Direction | Packets | Packets KB | Delta Packets | Delta KB | Kbps | Permitted Kbps | Congestion |
|-----------------|-----------------|-----------|----------|-------------|---------------|----------|---------|----------------|------------|
| BR1_VPX-WL-INET | MCN_VPX-BR1_VPX | Recv | 5437658 | 3467411.62 | 0 | 0 | 0 | 25 | NO |
| BR1_VPX-WL-INET | MCN_VPX-BR1_VPX | Send | 7598365 | 559484464 | 118 | 8.39 | 12.69 | 5905 | N/A |
| BR1_VPX-WL-MPLS | MCN_VPX-BR1_VPX | Recv | 58537274 | 41745181.34 | 6562 | 5203.86 | 7872.71 | 8105 | NO |
| BR1_VPX-WL-MPLS | MCN_VPX-BR1_VPX | Send | 20640095 | 1497892080 | 229 | 17.25 | 26.1 | 5880 | N/A |

Showing 1 to 4 of 4 entries

Bewährte Methoden

May 10, 2021

Die folgenden Themen enthalten die Best Practices, die bei der Entwicklung, Planung und Ausführung der Citrix SD-WAN -Lösung im Netzwerk beachtet werden müssen.

[Sicherheit](#)

[Routing](#)

[QoS](#)

[WAN-Links](#)

Sicherheit

May 10, 2021

Dieser Artikel beschreibt bewährte Sicherheitsmethoden für die Citrix SD-WAN Lösung. Es enthält allgemeine Sicherheitshinweise für Citrix SD-WAN Bereitstellungen.

Citrix SD-WAN Bereitstellungsrichtlinien

Um die Sicherheit während des Bereitstellungslebenszyklus aufrechtzuerhalten, empfiehlt Citrix folgende Sicherheitsüberlegungen:

- Physische Sicherheit
- Appliance-Sicherheit

- Netzwerksicherheit
- Verwaltung und Verwaltung

Physische Sicherheit

Bereitstellen von Citrix SD-WAN-Appliances in einem sicheren Serverraum —Die Appliance oder Server, auf der Citrix SD-WAN installiert ist, sollte in einem sicheren Serverraum oder einer eingeschränkten Rechenzentrumseinrichtung untergebracht werden, wodurch die Appliance vor unbefugtem Zugriff geschützt wird. Der Zugang sollte mindestens durch einen elektronischen Kartenleser gesteuert werden. Der Zugriff auf die Appliance wird von CCTV überwacht, das kontinuierlich alle Aktivitäten zu Überwachungszwecken aufzeichnet. Wenn ein Einbruch, elektronische Überwachungssystem sollte eine Warnung an das Sicherheitspersonal für sofortige Reaktion senden.

Schützen Sie Front-Panel- und Konsolenanschlüsse vor unbefugtem Zugriff —Sichern Sie die Appliance in einem großen Käfig oder Rack mit physischer Schlüsselzugriffskontrolle.

Stromversorgung schützen - Stellen Sie sicher, dass das Gerät mit einer unterbrechungsfreien Stromversorgung (USV) geschützt ist.

Appliance-Sicherheit

Sichern Sie zum Schutz der Appliance das Betriebssystem eines Servers, der eine virtuelle Citrix SD-WAN Appliance (VPX) hostet, führen Sie Remote-Softwareupdates durch und folgen Sie den Methoden der sicheren Lebenszyklusverwaltung:

- Sichern Sie das Betriebssystem des Servers Hosting einer Citrix SD-WAN VPX-Appliance - Eine Citrix SD-WAN VPX-Appliance wird als virtuelle Appliance auf einem Standardserver ausgeführt. Der Zugriff auf den Standardserver sollte durch rollenbasierte Zugriffskontrolle und starke Kennwortverwaltung geschützt werden. Außerdem empfiehlt Citrix regelmäßige Updates für den Server mit den neuesten Sicherheitspatches für das Betriebssystem und aktuellste Antivirensoftware auf dem Server.
- Remote-Softwareupdates ausführen - Installieren Sie alle Sicherheitsupdates, um bekannte Probleme zu beheben. Auf der Webseite Security Bulletins können Sie sich anmelden und aktuelle Sicherheitswarnungen erhalten.
- Befolgen Sie Secure Lifecycle Management Practices - Um eine Appliance bei der Neubereitstellung oder Initiierung von RMA und der Stilllegung sensibler Daten zu verwalten, führen Sie die Gegenmaßnahmen zur Datenerinnerung durch, indem Sie die persistenten Daten von der Appliance entfernen.

Netzwerksicherheit

Verwenden Sie für die Netzwerksicherheit nicht das Standard-SSL-Zertifikat. Verwenden Sie Transport Layer Security (TLS), wenn Sie auf die Administratorschnittstelle zugreifen, schützen Sie die nicht routingfähige Verwaltungs-IP-Adresse der Appliance, konfigurieren Sie eine Hochverfügbarkeits-Einrichtung und implementieren Sie die Sicherheitsvorkehrungen für Administration und Management entsprechend der Bereitstellung.

- Verwenden Sie nicht das Standard-SSL-Zertifikat - Ein SSL-Zertifikat von einer seriösen Zertifizierungsstelle vereinfacht die Benutzererfahrung für Internetanwendungen. Im Gegensatz zu der Situation mit einem selbstsignierten Zertifikat oder einem Zertifikat von der seriösen Zertifizierungsstelle erfordern Webbrowser keine Benutzer, das Zertifikat von der seriösen Zertifizierungsstelle zu installieren, um eine sichere Kommunikation mit dem Webserver zu initiieren.
- Transport Layer Security beim Zugriff auf Administratorschnittstelle verwenden - Stellen Sie sicher, dass die Verwaltungs-IP-Adresse nicht über das Internet zugänglich ist oder zumindest durch eine gesicherte Firewall geschützt ist. Stellen Sie sicher, dass die LOM-IP-Adresse nicht über das Internet zugänglich ist oder zumindest durch eine gesicherte Firewall geschützt ist.
- Sichere Verwaltungs- und Verwaltungskonten —Erstellen Sie ein alternatives Administratorkonto, legen Sie starke Kennwörter für Administrator- und Viewerkonten fest. Wenn Sie den Remote-Kontozugriff konfigurieren, sollten Sie die extern authentifizierte administrative Verwaltung von Konten mithilfe von RADIUS und TACAS konfigurieren. Ändern Sie das Standardkennwort für die Administratorbenutzerkonten, konfigurieren Sie NTP, verwenden Sie den Standardwert für die Sitzungszeitüberschreitung, verwenden Sie SNMPv3 mit SHA-Authentifizierung und AES-Verschlüsselung.

Citrix SD-WAN Overlay-Netzwerk schützt Daten, die das SD-WAN-Overlay-Netzwerk durchlaufen.

Sichere Administratorschnittstelle

Ersetzen Sie für einen sicheren Zugriff auf die Webverwaltung Standardsystemzertifikate, indem Sie Zertifikate von einer seriösen Zertifizierungsstelle hochladen und installieren. Wechseln Sie zu **Konfiguration> Einheitseneinstellungen> Administratorschnittstelle** in der Benutzeroberfläche der SD-WAN-Appliance.

Benutzerkonten:

- Kennwort des lokalen Benutzers ändern
- Benutzer verwalten

HTTPS-Zertifikate:

- Zertifikat

- Schlüssel

Sonstiges:

- Timeout der Webkonsole

The screenshot displays the 'Administrator Interface' for the 'HTTPS Cert' configuration. The left sidebar shows the navigation menu with 'Appliance Settings' expanded, and 'Administrator Interface' selected. The main content area has tabs for 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', 'HTTPS Settings', and 'Miscellaneous'. The 'HTTPS Cert' tab is active, showing the 'Installed Certificate' section. This section includes two tables: 'Issued to:' and 'Issuer:', both containing fields for Country, State/Province, Locality, Organization, Organizational Unit, Common Name, and Email. Below these is the 'Certificate Details' section, which displays the Certificate Fingerprint, Start Date, End Date, and Serial Number. At the bottom, there are two sections: 'Upload HTTPS Certificate Files' and 'Regenerate HTTPS Certificate', each with a 'Choose File' button and a 'No file chosen' message.

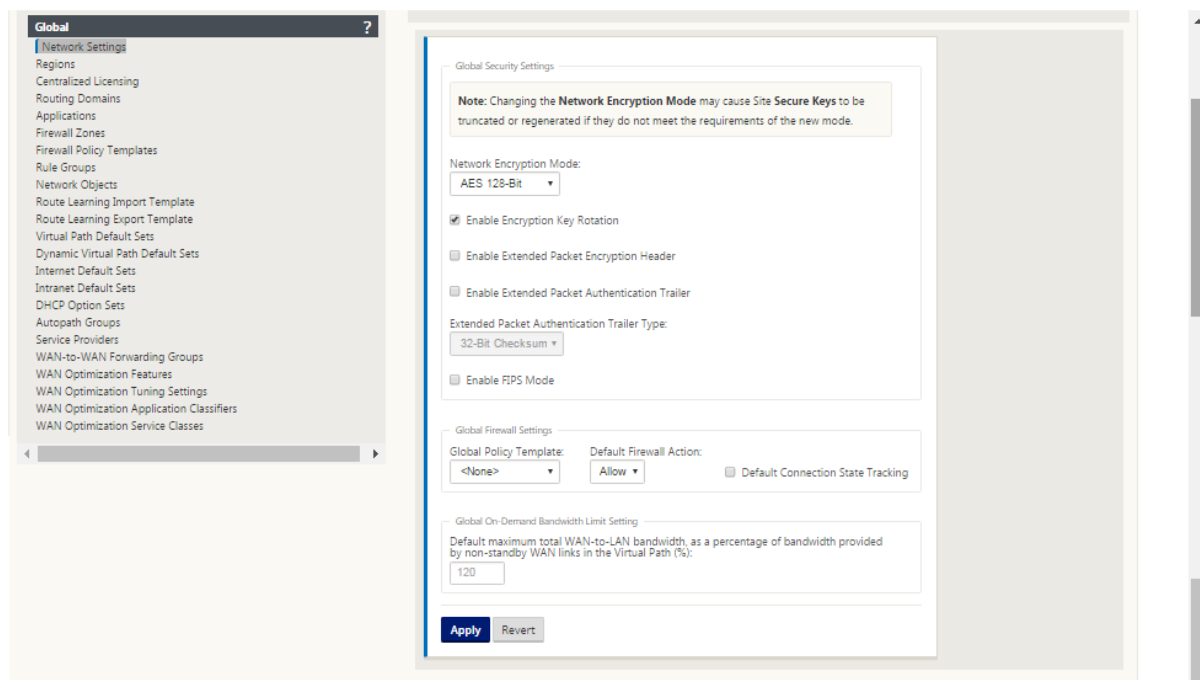
Konfigurations-Editor > Global > Netzwerkeinstellungen

Globale Firewall-Einstellungen:

- Globale Richtlinienvorlage
- Standard-Firewall-Aktionen
- Standardverfolgung des Verbindungszustands

Globale Verschlüsselungseinstellungen für virtuelle Pfade:

- AES 128-Bit (Standard)
- Drehung des Verschlüsselungsschlüssels (Standard)
- Extended Packet Encryption Header
- Erweiterter Paketauthentifizierungstrailer



Globale Verschlüsselungseinstellungen für virtuelle Pfade

- Die AES-128-Datenverschlüsselung ist standardmäßig aktiviert. Es wird empfohlen, AES-128 oder mehr Schutz der AES-256-Verschlüsselungsstufe für die Pfadverschlüsselung zu verwenden. Stellen Sie sicher, dass “Encryption Key Rotation aktivieren” so eingestellt ist, dass die Schlüsselregenerierung für jeden virtuellen Pfad mit aktivierter Verschlüsselung durch einen Elliptic Curve Diffie-Hellman-Schlüsselaustausch in Intervallen von 10-15 Minuten gewährleistet ist.

Wenn das Netzwerk zusätzlich zur Vertraulichkeit (d. h. Manipulationsschutz) eine Nachrichtenauthentifizierung erfordert, empfiehlt Citrix die Verwendung der IPsec-Datenverschlüsselung. Wenn nur Vertraulichkeit erforderlich ist, empfiehlt Citrix die Verwendung der erweiterten Header.

- Extended Packet Encryption Header ermöglicht es, dass ein zufällig vorangestellter Zähler am Anfang jeder verschlüsselten Nachricht vorangestellt wird. Bei Verschlüsselung dient dieser Zähler als zufälliger Initialisierungsvektor, deterministisch nur mit dem Verschlüsselungsschlüssel. Dies randomisiert die Ausgabe der Verschlüsselung und liefert eine starke Nachricht, die nicht zu unterscheiden ist. Beachten Sie, dass diese Option, wenn sie aktiviert ist, den Paket-Overhead um 16 Byte erhöht
- Extended Packet Authentication Trailer fügt einen Authentifizierungscode an das Ende jeder verschlüsselten Nachricht an. Dieser Trailer ermöglicht die Überprüfung, dass Pakete während des Transports nicht geändert werden. Beachten Sie, dass diese Option den Paketaufwand erhöht.

Firewall-Sicherheit

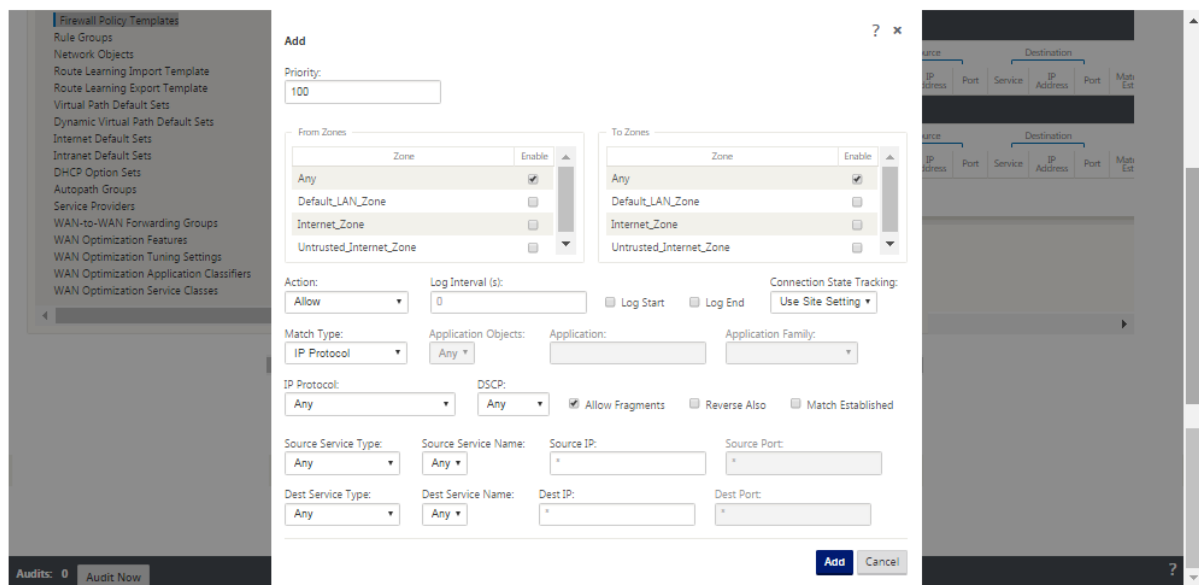
Die empfohlene Firewall-Konfiguration ist mit einer standardmäßigen Firewall-Aktion, die zuerst alle verweigert, und dann Ausnahmen hinzufügen. Bevor Sie Regeln hinzufügen, dokumentieren und überprüfen Sie den Zweck der Firewall-Regel. Verwenden Sie nach Möglichkeit Stateful Inspection und Application Level Inspection. Vereinfachen Sie Regeln und eliminieren Sie redundante Regeln. Definieren und befolgen Sie einen Änderungsverwaltungsprozess, der Änderungen an **Firewalleinstellungen** verfolgt und überprüft. Legen Sie die Firewall für alle Appliances fest, um Verbindungen über die Appliance mithilfe der globalen Einstellungen zu verfolgen. Die Verfolgung von Verbindungen überprüft, ob Pakete ordnungsgemäß gebildet sind und für den Verbindungsstatus geeignet sind. Erstellen Sie Zonen, die der logischen Hierarchie des Netzwerks oder der Funktionsbereiche der Organisation entsprechen. Beachten Sie, dass Zonen global signifikant sind und geografisch unterschiedliche Netzwerke als dieselbe Sicherheitszone behandelt werden können. Erstellen Sie möglichst spezifische Richtlinien, um das Risiko von Sicherheitslücken zu reduzieren und die Verwendung von **Alle in Zulassen**-Regeln zu vermeiden. Konfigurieren und Verwalten einer globalen Richtlinienvorlage, um eine grundlegende Sicherheitsstufe für alle Appliances im Netzwerk zu erstellen. Definieren Sie Richtlinienvorlagen basierend auf funktionalen Rollen von Appliances im Netzwerk und wenden Sie sie gegebenenfalls an. Definieren Sie Richtlinien nur bei Bedarf an einzelnen Standorten.

Globale Firewall-Vorlagen - Firewall-Vorlagen ermöglichen die Konfiguration globaler Parameter, die sich auf den Betrieb der Firewall auf einzelnen Appliances auswirken, die in der SD-WAN-Overlay-Umgebung arbeiten.

Standard-Firewall-Aktionen —Zulassen aktiviert Pakete, die keiner Filterrichtlinie entsprechen, sind zulässig. Verweigern aktiviert Pakete, die keiner Filterrichtlinie entsprechen, werden gelöscht.

Standardverbindungsstatusverfolgung —Aktiviert die bidirektionale Verbindungsstatusverfolgung für TCP-, UDP- und ICMP-Flows, die nicht mit einer Filterrichtlinie oder NAT-Regel übereinstimmen. Asymmetrische Flows werden blockiert, wenn diese aktiviert ist, auch wenn keine Firewall-Richtlinien definiert sind. Die Einstellungen können auf Siteebene definiert werden, wodurch die globale Einstellung außer Kraft gesetzt wird. Wenn asymmetrische Flüsse an einem Standort möglich sind, empfiehlt es sich, dies auf Standort- oder Richtlinienenebene und nicht global zu aktivieren.

Zonen - Firewallzonen definieren logische Sicherheitsgruppen von Netzwerken, die mit dem Citrix SD-WAN verbunden sind. Zonen können auf virtuelle Schnittstellen, Intranetdienste, GRE Tunnel und LAN IPsec-Tunnel angewendet werden.



WAN-Link-Sicherheitszone

Nicht vertrauenswürdige Sicherheitszone sollte für WAN-Verbindungen konfiguriert werden, die direkt mit einem öffentlichen (unsicheren) Netzwerk verbunden sind. Untrusted setzt die WAN-Verbindung auf den sichersten Zustand, sodass nur verschlüsselter, authentifizierter und autorisierter Datenverkehr in der Schnittstellengruppe akzeptiert werden kann. ARP und ICMP an die virtuelle IP-Adresse sind die einzigen anderen Datenverkehrstypen zulässig. Diese Einstellung stellt außerdem sicher, dass nur verschlüsselter Datenverkehr von den Schnittstellen gesendet wird, die der Interface-Gruppe zugeordnet sind.

Routing-Domänen

Routingdomänen sind Netzwerksysteme, die eine Reihe von Routern enthalten, die zum Segmentieren des Netzwerkverkehrs verwendet werden. Neu erstellte Kerne werden automatisch der Standard-Routingdomäne zugeordnet.

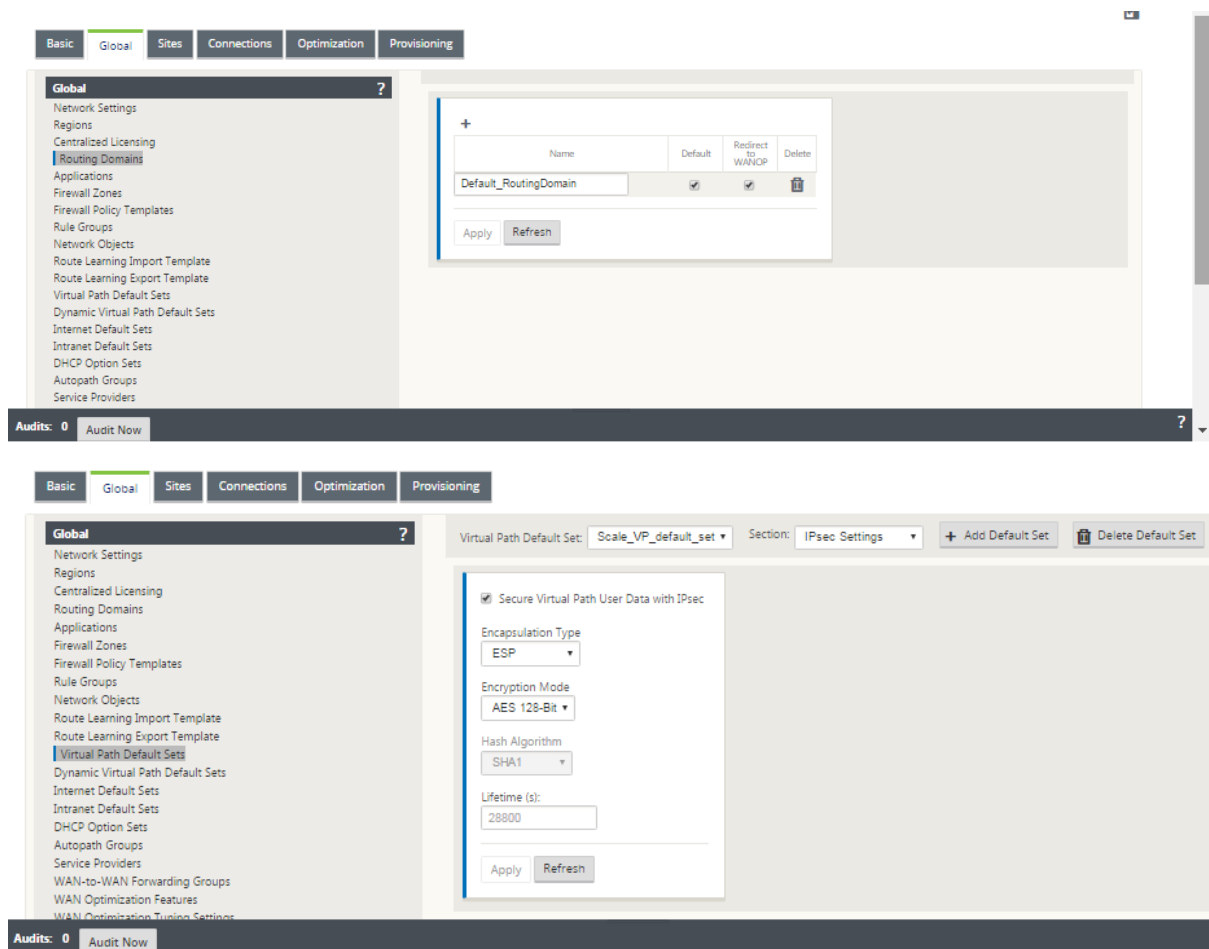
Konfigurations-Editor > Global

Routing-Domänen

- Default_RoutingDomain

IPsec-Tunnel

- Standardsätze
- Sichern Sie Benutzerdaten virtueller Pfade mit IPsec



IPsec-Tunnel

IPsec-Tunnel sichern sowohl Benutzerdaten als auch Header-Informationen. Citrix SD-WAN Appliances können feste IPsec-Tunnel auf der LAN- oder WAN-Seite mit Nicht-SD-WAN-Peers aushandeln. Für IPsec-Tunnel über LAN muss eine Routingdomäne ausgewählt werden. Wenn der IPsec-Tunnel einen Intranetdienst verwendet, wird die Routingdomäne vom gewählten Intranetdienst vorab festgelegt.

Der IPsec-Tunnel wird über den virtuellen Pfad eingerichtet, bevor Daten über das SD-WAN-Overlay-Netzwerk fließen können.

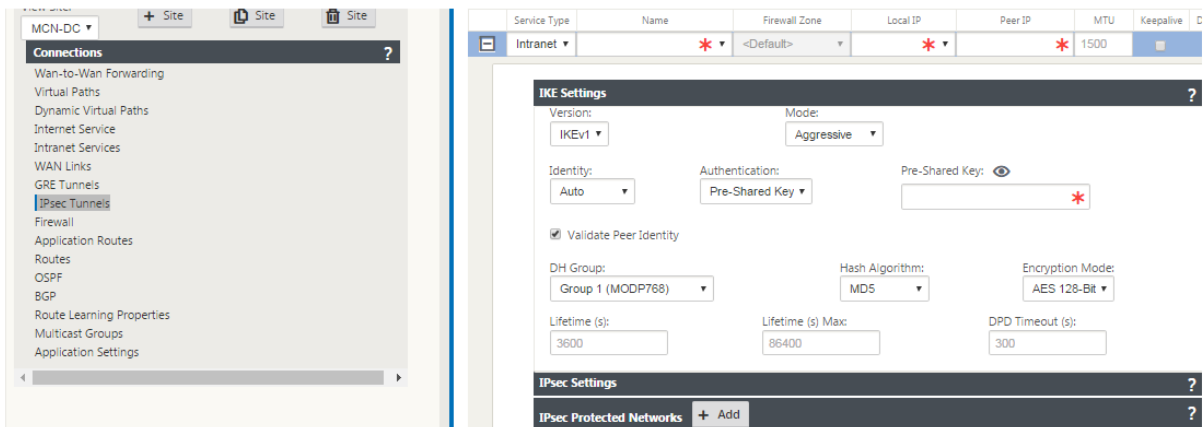
- Encapsulation Type Optionen umfassen ESP - Daten sind gekapselt und verschlüsselt, ESP+Auth —Daten werden mit einem HMAC gekapselt, verschlüsselt und validiert, AH —Daten werden mit einem HMAC validiert.
- Der Verschlüsselungsmodus ist der Verschlüsselungsalgorithmus, der verwendet wird, wenn ESP aktiviert ist.
- Hash-Algorithmus wird verwendet, um einen HMAC zu generieren.

- Die Lebensdauer ist eine bevorzugte Dauer in Sekunden für eine IPsec-Sicherheitszuordnung. 0 kann unbegrenzt verwendet werden.

IKE-Einstellungen

Internet Key Exchange (IKE) ist ein IPsec-Protokoll, das zum Erstellen einer Sicherheitszuordnung (SA) verwendet wird. Citrix SD-WAN Appliances unterstützen sowohl IKEv1- als auch IKEv2-Protokolle.

- Der Modus kann entweder Hauptmodus oder Aggressiver Modus sein.
- Identität kann automatisch sein, um Peer zu identifizieren, oder eine IP-Adresse kann verwendet werden, um die IP-Adresse des Peers manuell anzugeben.
- Die Authentifizierung ermöglicht die Authentifizierung mit vordefinierten Schlüsseln oder das Zertifikat als Authentifizierungsmethode.
- Validate Peer Identity aktiviert die Validierung der Peer-Identität des IKE, wenn der ID-Typ des Peers unterstützt wird, andernfalls aktivieren Sie diese Funktion nicht.
- Diffie-Hellman-Gruppen sind für die IKE-Schlüsselgenerierung mit Gruppe 1 bei 768-Bit, Gruppe 2 bei 1024-Bit und Gruppe 5 bei 1536-Bit-Gruppe verfügbar.
- Hash-Algorithmus umfasst MD5, SHA1 und SHA-256 hat Algorithmen sind für IKE-Nachrichten verfügbar.
- Verschlüsselungsmodi umfassen AES-128, AES-192 und AES-256 Verschlüsselungsmodi sind für IKE-Nachrichten verfügbar.
- Zu den IKEv2-Einstellungen gehören Peer-Authentifizierung und Integritätsalgorithmus.



Konfigurieren der Firewall

Folgende häufig auftretende Probleme können durch Überprüfung der Konfiguration des Upstream-Routers und der Firewall identifiziert werden:

- MPLS-Warteschlangen/QoS-Einstellungen: Stellen Sie sicher, dass der UDP-gekapselte Datenverkehr zwischen virtuellen SD-WAN-IP-Adressen aufgrund von **QoS-Einstellungen** auf den Zwischengeräten im Netzwerk nicht beeinträchtigt wird.
- Der gesamte Datenverkehr auf den im SD-WAN-Netzwerk konfigurierten WAN-Verbindungen sollte von der Citrix SD-WAN Appliance mit dem richtigen Diensttyp (virtueller Pfad, Internet, Intranet und Lokal) verarbeitet werden.
- Wenn der Datenverkehr die Citrix SD-WAN Appliance umgehen und denselben zugrunde liegenden Link verwenden muss, sollten angemessene Bandbreitenreservierungen für den SD-WAN-Datenverkehr auf dem Router vorgenommen werden. Außerdem sollte die Verbindungskapazität in der SD-WAN-Konfiguration entsprechend konfiguriert werden.
- Stellen Sie sicher, dass der Zwischenrouter bzw. Firewall keine UDP-Flut- und/oder PPS-Grenzwerte erzwungen hat. Dadurch wird der Datenverkehr gedrosselt, wenn er über den virtuellen Pfad gesendet wird (UDP-gekapselt).

Routing

May 10, 2021

In diesem Artikel werden Best Practices für die Citrix SD-WAN Lösung beschrieben.

Internet-/Intranet-Routingdienst

Wenn der Internetdienst nicht für den internetgebundenen Datenverkehr konfiguriert ist und stattdessen entweder eine **lokale** Route oder eine **Passthrough-Route** so konfiguriert ist, dass sie den Gateway Router erreichen. Der Router verwendet die WAN-Verbindungen, die auf der SD-WAN-Appliance konfiguriert sind, was zu einem Problem mit einem Überabonnement führt.

Wenn eine Internetroute im MCN als **Lokal** konfiguriert ist, wird sie von allen Zweig-SD-WAN-Sites gelernt und standardmäßig als **Virtual Path Route** konfiguriert. Dies bedeutet, dass der internetgebundene Datenverkehr in der Zweig-Appliance über den virtuellen Pfad an MCN weitergeleitet wird.

Routing-Priorität

Die Reihenfolge der Weiterleitungspriorität:

- Präfixübereinstimmung: Die längsten Präfixe stimmen überein.
- Service: Lokal, Virtual Path Service, Internet, Intranet, Passthrough
- Routenkosten

Routingasymmetrie

Stellen Sie sicher, dass keine Routingasymmetrie im Netzwerk vorhanden ist (die NetScaler SD-WAN-Appliance sendet Datenverkehr nur in eine Richtung). Dies führt zu Problemen mit der Firewall-Verbindungsverfolgung und Deep Packet Inspection.

QoS

May 10, 2021

Berücksichtigen Sie bei der Konfiguration von QoS Folgendes:

- Verstehen Sie Ihre Netzwerkdatenverkehrsmuster und -anforderungen. Möglicherweise müssen Sie die **QoS-Klassenstatistiken** beobachten und Warteschlangentiefen ändern und/oder den Standardanteil der QoS-Klasse ändern, um Tail-Drops zu vermeiden, wie in QoS-Statistiken gezeigt.
- Manchmal wird das gesamte Subnetz zu einer Regel hinzugefügt, um die Konfiguration zu erleichtern, anstatt Regeln für bestimmte Anwendungs-IP-Adressen zu erstellen. Durch das Hinzufügen des gesamten Subnetzes zu einer Regel wird der gesamte Datenverkehr im Subnetz fälschlicherweise einer Regel zugeordnet. Daher können die QoS-Klassen, die dieser Regel zugeordnet sind, zu Taildrop und schlechter Anwendungsleistung oder Benutzererfahrung führen.

WAN-Links

May 10, 2021

Citrix SD-WAN Plattformen unterstützen bis zu 8 öffentliche Internetverbindungen und 32 private MPLS-Verbindungen. In diesem Artikel werden Best Practices für die Konfiguration von WAN-Verbindungen für die Citrix SD-WAN Lösung beschrieben.

Punkte, die Sie beim Konfigurieren von WAN-Links merken müssen:

- Konfigurieren Sie die **zulässige und physische** Rate als tatsächliche WAN-Verbindungsbandbreite. Wenn die gesamte WAN-Verbindungskapazität nicht von der SD-WAN-Appliance genutzt werden soll, ändern Sie die **Zulässige** Rate entsprechend.
- Wenn Sie sich der Bandbreite nicht sicher sind und die Verknüpfungen nicht zuverlässig sind, können Sie die Funktion **Auto Learn** aktivieren. Die Funktion **Auto Learn** lernt nur die zugrunde liegende Verbindungskapazität und verwendet in Zukunft denselben Wert.

- Wenn die zugrunde liegende Verbindung nicht stabil ist und keine feste Bandbreite garantiert (z. B. 4G-Verbindungen), verwenden Sie die Funktion **Adaptive Bandbreitenerkennung**.
- Es wird nicht empfohlen, **Auto Learn** und **Adaptive Bandwidth Detection** auf derselben WAN-Verbindung zu aktivieren.
- Konfigurieren Sie das MCN/RCN manuell mit der physikalischen Rate von Ingress/Egress für alle WAN-Verbindungen, da es der zentrale Punkt der Bandbreitenverteilung zwischen mehreren Zweigen ist.
- Wenn Auto-Learn nicht verwendet wird, verwenden Sie zuverlässige Verbindungen zu SLAs, die keine zufällige Kapazitätsänderung aufweisen, um die Zuverlässigkeit wichtiger Rechenzentrums-Workloads/-Services zu erhöhen.
- Wenn der zugrunde liegende Link nicht stabil ist, ändern Sie die folgenden Pfadeinstellungen:
 - Verlusteinstellungen
 - Instabilitätssensitive deaktivieren
 - Stillzeit
- Verwenden Sie **das Diagnose-Tool**, um den Verbindungszustand/-kapazität zu überprüfen.
- Wenn SD-WAN im **Einarmsmodus** bereitgestellt wird, stellen Sie sicher, dass Sie die physische Kapazität der zugrunde liegenden Verbindung nicht überlaufen.

Status des ISP-Links überprüfen

Bei neuen Bereitstellungen vor der SD-WAN-Bereitstellung und beim Hinzufügen einer neuen ISP-Verknüpfung zur vorhandenen SD-WAN-Bereitstellung:

- Überprüfen Sie den Linktyp. Zum Beispiel; MPLS, ADSL, 4G.
- Netzwerkeigenschaften. Zum Beispiel - Bandbreite, Verlust, Latenz und Jitter.

Diese Informationen helfen bei der Konfiguration des SD-WAN-Netzwerks gemäß Ihren Anforderungen.

Netzwerktopologie

Es wird häufig beobachtet, dass spezifischer Netzwerkverkehr die Citrix SD-WAN Appliances umgeht und dieselbe zugrunde liegende Verbindung verwendet, die im SD-WAN-Netzwerk konfiguriert ist. Da SD-WAN keine vollständige Transparenz über die Link-Auslastung hat, besteht die Wahrscheinlichkeit, dass SD-WAN den Link überzeichnet, was zu Performance- und PATH-Problemen führt.

Provisioning

Punkte, die bei der Provisioning von SD-WAN berücksichtigt werden sollten:

- Standardmäßig erhalten alle Zweige und WAN-Dienste (Virtual Path/Internet/Intranet) den gleichen Anteil an der Bandbreite.
- Provisioningstandorte müssen geändert werden, wenn zwischen den Verbindungsstandorten eine hohe Disparität hinsichtlich der Bandbreitenanforderungen oder Verfügbarkeit besteht.
- Wenn dynamische virtuelle Pfade zwischen maximal verfügbaren Standorten aktiviert sind, wird die WAN-Verbindungskapazität zwischen dem statischen virtuellen Pfad zu DC und den dynamischen virtuellen Pfaden gemeinsam genutzt.

Häufig gestellte Fragen

May 10, 2021

Hohe Verfügbarkeit

Was ist der Unterschied zwischen High Availability und Secondary (Geo) Appliance?

- Hohe Verfügbarkeit gewährleistet Fehlertoleranz. Die sekundäre (Geo-) Appliance ermöglicht die Disaster Recovery.
- Hochverfügbarkeit kann für MCN, RCN und Zweige-Appliances konfiguriert werden. Sekundäre (Geo-) Appliance kann nur für MCN und RCNs konfiguriert werden.
- Hochverfügbarkeits-Appliances werden am selben Standort oder geografischen Standort konfiguriert. Eine Zweigeinheit an einem anderen geografischen Standort ist als sekundäre (Geo) MCN/RCN-Einheit konfiguriert.
- Die primäre und sekundäre Appliance mit hoher Verfügbarkeit sollten dieselben Plattformmodelle sein. Die sekundäre (Geo) -Appliance ist möglicherweise das gleiche Plattformmodell wie die primäre MCN/RCN.
- Hochverfügbarkeit hat eine höhere Priorität gegenüber sekundären (Geo). Wenn eine Appliance (MCN/RCN) mit High Availability and Secondary (Geo) -Appliance konfiguriert ist, wird die sekundäre Hochverfügbarkeits-Appliance aktiv, wenn die Appliance ausfällt. Wenn beide Hochverfügbarkeits-Appliances ausfallen oder wenn der Standort des Rechenzentrums abstürzt, wird die sekundäre (Geo) Appliance aktiv.
- Bei Hochverfügbarkeit erfolgt der primäre bzw. sekundäre Switchover sofort oder innerhalb von 10-12 Sekunden, abhängig von der Hochverfügbarkeitsbereitstellung. Der primäre MCN/RCN-zu-sekundäre (Geo) MCN/RCN-Umschalter erfolgt nach 15 Sekunden, nachdem der primäre inaktiv ist.

- Mit der Hochverfügbarkeitskonfiguration können Sie die primäre Rückgewinnung konfigurieren. Sie können die primäre Rückgewinnung für die sekundäre (Geo) -Appliance nicht konfigurieren. Die primäre Rückgewinnung erfolgt automatisch, nachdem die primäre Appliance wieder zurück ist und der Haltezeitgeber abgelaufen ist.

Upgrade in einem Schritt

Hinweis

WANOP, SVM und XenServer Supplemental/HFS werden als Betriebssystemkomponenten betrachtet.

Sollte ich *.tar.gz* oder ein einzelnes Schritt-Upgrade *.zip-Paket* verwenden, um von meiner aktuellen Version (8.1.x, 9.1.x, 9.2.x) auf 9.3.x zu aktualisieren?

Verwenden Sie die *TAR.gz-Dateien* der betreffenden Plattformen, um die SD-WAN-Software auf 9.3.x zu aktualisieren. Nachdem die SD-WAN-Software auf die Version 9.3.x aktualisiert wurde, führen Sie die Änderungsverwaltung mithilfe des Pakets *.zip* durch, um Softwarepakete für Betriebssystemkomponenten zu übertragen/zu verlagern. Nach der Aktivierung überträgt der MCN Betriebssystemkomponenten für alle relevanten Zweige.

Nach dem Upgrade auf 9.3.0 mit einem Einzelschritt-Upgrade-Paket (*.zip-Datei*) tun, muss ich ausführen *Upg-Upgrade* auf jeder Appliance?

Nein, Betriebssystemsoftwareupdate/-upgrade wird durch das Einzelschritt-Upgrade *.zip-Paket* übernommen und es wird gemäß den Planungsdetails installiert, die Sie in den Änderungsverwaltungseinstellungen der jeweiligen Standorte angegeben haben.

Warum sollte ich *.tar.gz* gefolgt von *.zip-Paket* verwenden, um von früher als 9.3 auf 9.3.x zu aktualisieren, und warum nicht direkt *.zip-Paket* von 9.3.x verwenden?

Ein Einzelschritt-Upgrade-Paket wird ab 9.3.0.161 unterstützt und bei früheren Versionen (vor Release 9.3) wird dieses Paket nicht erkannt. Wenn das Paket Upgrade *.zip* in den Change Management-Posteingang hochgeladen wird, gibt das System einen Fehler aus, der besagt, dass das Paket nicht erkannt wird. Daher aktualisieren Sie zuerst die SD-WAN-Software auf Version 9.3 oder höher und führen Sie dann das Change Management mithilfe des *ZIP-Pakets*.

Wie werden die Betriebssystemkomponenten durch ein einzelnes Schritt-Upgrade installiert, wenn *upg-Upgrade* wird nicht durchgeführt?

Der MCN transferiert/stellt Betriebssystemkomponenten Softwarepakete basierend auf dem Appliance-Modell auf, nachdem das Änderungsmanagement mit einem einzigen Schritt *upgrade.zip-Paket* abgeschlossen wurde. Nach der Aktivierung startet der MCN die Softwarepakete der Betriebssystemkomponenten für die Zweige, die sie für das geplante Update/Upgrade benötigen, zu übertragen/zu stempeln.

Wie installiere ich Betriebssystemkomponenten, ohne für spätere Installationen zu planen?

Setzen Sie den Wert des **Wartungsfensters** auf '0' für die sofortige Installation der Betriebssystemkomponenten.

Hinweis

Die Installation wird nur gestartet, wenn die Appliance das gesamte Paket empfangen hat, das für die Site benötigt wird, selbst wenn der Wert des **Wartungsfensters** auf '0' festgelegt ist.

Was ist die Verwendung der Planung der Installation? Kann ich die Fahrplananweisungen verwenden, um VW alleine zu aktualisieren?

Die geplante Installation wurde in SD-WAN Version 9.3 eingeführt und gilt nur für Betriebssystemkomponenten und nicht für VW-Software-Upgrades. Bei einem Upgrade in einem Schritt müssen Sie sich nicht bei jeder Appliance anmelden, um das Upgrade der Betriebssystemkomponenten durchzuführen. Mit der Planungsoption können Sie die Installation der Betriebssystemkomponenten zu einem anderen Zeitpunkt als dem Upgrade der VW-Softwareversion planen.

Warum werden die Planungsinformationen auf der Seite Einstellungen für die Änderungsverwaltung standardmäßig nach dem Plandatum angezeigt und was bedeutet das?

Auf der Seite **Einstellungen für die Änderungsverwaltung** werden die standardmäßigen Planungsinformationen angezeigt: *Start: 2016-05-21 21:20:00, Fenster: 1, Wiederholung: 1, Einheit: Tage*. Wenn das Datum ein vergangenes Datum ist, bedeutet dies, dass die geplante Installation auf der Zeit und anderen Parametern wie Wartungsfenster, Wiederholfenster und Einheit basiert und nicht auf dem Datum.

Was ist der Standardzeitplan Installationsdatum/-zeit auf eingestellt, ist die allgemeine oder lokale Appliance abhängig?

Standardmäßig wird die Planungsdetails auf '2016-05-21 um 21:20:00 (Wartungsfenster von 1 Stunde und alle 1 Tag wiederholt)' gesetzt. Diese Details sind abhängig vom Standort der lokalen Appliance.

Wie kann ich Betriebssystemkomponenten sofort installieren, ohne auf das Wartung/geplante Fenster zu warten?

Setzen Sie den Wert des **Wartungsfensters** auf 0 auf der Seite **Einstellungen für die Änderungsverwaltung**. Dadurch wird die geplante Installationszeit außer Kraft gesetzt.

Welches Paket sollte ich für das Upgrade verwenden, wenn die aktuelle Softwareversion 9.3.x oder höher ist?

Verwenden Sie ein Upgrade *.zip-Paket* in einem Schritt, um auf eine höhere Version zu aktualisieren, wenn die aktuelle Softwareversion 9.3.x oder höher.

Wann werden die OS-Komponentendateien in die Zweige übertragen/bereitgestellt?

Die Betriebssystemkomponentendateien werden in relevante Zweige übertragen, nachdem die Aktivierung abgeschlossen ist, wenn Change Management mit einem einzigen Schritt *upgrade.zip-Paket* durchgeführt wird, um das System zu aktualisieren.

Welche Appliances erhalten OS-Komponentendateien, Ist sie plattformabhängig oder alle Zweige erhalten sie?

Appliances, die auf Hypervisor basieren, wie z. B. **SD-WAN —400, 800, 1000, 2000 SE** und Bare Metal **SD-WAN —2100**, die mit EE-Lizenz ausgeführt werden, erhalten Betriebssystemkomponenten für das Upgrade.

Wie funktioniert die Terminplanung?

Standardmäßig wird die Planungsdetails auf *2016-05-21 um 21:20:00 (Wartungsfenster von 1 Stunde und wiederholt jeden 1 Tag)* gesetzt, und es bedeutet, dass das System überprüft, ob neue Software für die Installation verfügbar ist, da der Wiederholungswert auf **1 Tage** festgelegt ist und Wartungsfenster von **1 Stunden** und die Installation wird ab **21.05.2016 um 21:20:00 Uhr** (lokale Appliance-Zeit) ausgelöst bzw. versucht (falls neue Software verfügbar ist).

Wie erfahre ich, ob die Betriebssystemkomponenten aktualisiert wurden?

In der Spalte **Status** sehen Sie ein grünes Häkchen. Wenn Sie den Mauszeiger darüber zeigen, sehen Sie die Meldung **Upgrade ist erfolgreich**.

Wie kann ich die Installation von Betriebssystemkomponenten für RCN und seine Zweige planen?

Die Planung für RCN erfolgt über die Seite **Einstellungen für die MCN Change Management** . Für RCN-Zweige müssen Sie sich bei der jeweiligen RCN anmelden und die Zeitplandetails festlegen.

Wo kann ich den Status der geplanten Installation abrufen?

Der Status der geplanten Installation für RCN kann auf der Seite **Einstellungen für die MCN Change Management** abgerufen werden. Für RCN-Zweige müssen Sie sich beim jeweiligen RCN anmelden, um den Status zu erhalten.

Wie erhalte ich den Status der geplanten Installation?

Verwenden Sie die Schaltfläche “Aktualisieren” auf der Seite **Einstellungen für die Änderungsverwaltung**, um den Status von MCN bzw. RCN für Zweige in Standardregion bzw. RCN abzurufen.

Scheduling Information

Show100▼entries

Search:

Edit Selected

Refresh

| <input type="checkbox"/> | Site Name | Scheduling Information | Status | Edit |
|--------------------------|------------------------|--|--------|------|
| <input type="checkbox"/> | GeoMCNVPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | MCNVPXHA | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | MCNVPXHA(HA-Secondary) | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN1BR11000 | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN1BR2VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN1RCN | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN2BR1VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN2BR2VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN2BR3VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN2RCN | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN2RCN(HA-Secondary) | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN3BR1VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN3BR2 | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN3BR2(HA-Secondary) | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCN3RCN2100 | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCNDefaultBR1VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |
| <input type="checkbox"/> | RCNDefaultBR2VPX | 2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days) | | |

Showing 1 to 17 of 17 entries

Previous1Next

Kann ich die *tar.gz-Datei* verwenden, um auf die nächste Version zu aktualisieren, wenn ein Einzelschritt-Upgrade für das vorherige Software-Upgrade verwendet wurde?

Sie können die *tar.gz-Datei* zum Aktualisieren verwenden, es wird jedoch nicht empfohlen, da Sie ein Software-Upgrade mithilfe des durchführen können.*upg-Datei*. Laden Sie zur Aktualisierung der Betriebssystemkomponentensoftware hoch, indem Sie sich bei jeder entsprechenden Appli-ance anmelden. Ab Version 9.3, Version 1, wird die Seite **Betriebssystemsoftware aktualisieren** abgeschrieben. Daher können Sie die Änderungsverwaltung mithilfe des Pakets *.zip* durchführen, um Betriebssystemkomponenten zu aktualisieren.

Wie können wir die aktuellen laufenden Versionen von Betriebssystemkomponenten validieren?

Jetzt können Sie die aktuell ausgeführten Versionen von Betriebssystemkomponenten nicht über die Benutzeroberfläche überprüfen. Sie können sich von jeder Konsole aus anmelden oder STS aufrufen, um diese Informationen anzuzeigen.

Welchen Unterschied würde es machen, wenn ich Bare Metal Geräte in meinem Netzwerk habe? Beein-trächtigt sich die Planung auf Bare-Metal-/Virtual Appliances?

Bare Metal Appliances wie **SD-WAN —410.2100,4100,5100 SD-WAN** betreiben nur SD-WAN-Software.

Bare Metal Appliances benötigen keine OS-Komponentenpakete. Diese Plattformen werden in Bezug auf die Softwareanwendungen mit SD-WAN VPX-SE-Appliances behandelt. Der MCN wird keine OS-Komponentenpakete an diese Appliances übertragen. Das Festlegen von Planungsinformationen wird für diese Appliances nicht wirksam, da sie über keine Betriebssystemkomponenten verfügen, für die ein Upgrade erforderlich ist.

Wie funktioniert SSU in Hochverfügbarkeitsumgebung/Bereitstellung?

Bei der Hochverfügbarkeitsbereitstellung bei MCN haben wir eine Einschränkung, bei der der aktive MCN Switch/umschaltet die Rolle des primären MCN während des Change Managements und der Standby/Secondary MCN übernimmt. In diesem Fall können Sie die Änderungsverwaltung erneut mit dem *ZIP-Paket* auf dem aktiven MCN für die Pakete durchführen oder Sie können wieder zum primären MCN wechseln, indem Sie die Rolle des aktiven MCN umschalten, sodass der ursprüngliche primäre MCN die Rolle übernehmen kann, damit die OS-Komponentenpakete auf andere Zweige.

Wie funktioniert ein Upgrade in einem Schritt in der Hochverfügbarkeitsumgebung bzw. -bereitstellung?

Beim Upgrade in einem Schritt in der Hochverfügbarkeitsbereitstellung wird die Rolle des primären MCN und des Standby-MCN umgeschaltet. Dies ist eine Einschränkung. Führen Sie in diesem Fall die Änderungsverwaltung mit dem *ZIP-Paket* auf dem aktiven MCN erneut aus. Alternativ können Sie zurück zum primären MCN wechseln, indem Sie die Rolle des aktiven MCN umschalten, sodass der ursprüngliche primäre MCN OS-Komponentenpakete in den Zweigen versetzt werden kann.

Wird ein Upgrade in einem Schritt für die Zero-Touch-Bereitstellung unterstützt, um die Appliances neu zu starten?

Ja, es kann verwendet werden.

Kann ich ein Upgrade für meine eigenständige WANOP Appliance mit einem Schritt durchführen?

- Nein.

Kann ich ein Upgrade in einem Schritt verwenden, um eine eigenständige WANOP-Appliance zu aktualisieren, die im Zwei-Box-Modus bereitgestellt wird?

Nein. Nur SD-WAN-Appliance, die Teil des Zwei-Box-Modus ist, würde aktualisiert und nicht die eigenständige WANOP-Appliance.

Welches Paket sollte ich für ein Upgrade auf ein mehrstufiges Netzwerk verwenden?

Verwenden Sie das Einzelschritt-Upgrade-Paket *ns-sdw-sw- <release-version>.zip*, wenn die aktuelle Softwareversion 9.3.x oder höher ist. MCN kümmert sich um das Staging-Paket zu RCN und RCNs führen das Staging des Softwarepaket zu den jeweiligen Branches durch.

Nach dem Hochladen der Datei *ns-sdw-sw-<release-version>.zip* sehe ich nur ein Plattformmodell unter aktueller Software?

Ab Release 10.0 wird die Unterstützung für die Skalierungsarchitektur eingeführt, um die Verarbeitung eines Einzelschritt-Upgrades zu beschleunigen. Sie können nur das MCN-Plattformmodell unter aktueller Software sehen. Andere Appliance-Pakete werden angezeigt/verarbeitet, wenn Sie die Schaltfläche **Verifizieren** oder **Stage Appliance** wählen.

Welche Pakete werden für VPX/VPXL/Bare Metal Appliances für RCN bereitgestellt?

Das Paket wird zu RCNs bereitgestellt, da RCNs-Zweige von jedem Plattformmodell sein können. Daher benötigen sie alle Pakete.

Wie erhält mein Zweigstandort hinter dem RCN OS-Komponentenpakete, wenn RCN eine VPX-Appliance ist und Zweig eine Appliance ist, die diese Pakete benötigt?

RCN stellt nach Aktivierung des SD-WAN VW-Softwarepakets das entsprechende Paket in den Zweig ein, der die OS-Komponentenpakete benötigt.

Kann ich während der Stagingphase Unvollständig ignorieren wählen und mit der nächsten Phase des Änderungsmanagements fortfahren? Welche Auswirkungen hat es auf Websites, die das Staging nicht abgeschlossen haben, wenn diese Schaltfläche ausgewählt ist?

Ja, Sie können auf **Unvollständige ignorieren** klicken. Dadurch wird die Schaltfläche **Weiter** aktiviert, und die Fortschrittsleiste wird angezeigt. Diese Option wird für Szenarien bereitgestellt, in denen die Site nicht erreichbar ist und die Änderungsverwaltung immer noch darauf wartet, dass das Staging für diese Site abgeschlossen ist, sodass Benutzer mit der nächsten Stufe fortfahren können, indem sie den Stagen-Status ignorieren und mit der Aktivierung fortfahren können. Nachdem die Site auftaucht, setzt MCN das Paket nach Abschluss der Aktivierung ein.

Teilweise Software-Upgrade

Was ist ein teilweises Upgrade und wie kann ich es verwenden?

Teilweise Aktualisierung der Standortsoftware ist eine neue Funktion, die in Release 10.0 eingeführt wurde. Sie können die neuere Version von Release 10.x aus dem MCN staged-Software-Version auf der Seite **Local Change Management** auf ausgewählten Standorten/Zweigen aktivieren. Stellen Sie vor der Aktivierung der bereitgestellten Software auf Standort/Zweig sicher, dass das Kontrollkästchen von MCN aktiviert ist.

- Diese Funktion ist in der Standardeinstellung deaktiviert. Der vorhandene Korrekturmechanismus hält das Netzwerk synchron. Der Benutzer muss festlegen, dass teilweise Standortaktualisierungen zugelassen werden sollen, indem er ein Kontrollkästchen auf der Seite **Konfiguration > Verwaltungseinstellungen ändern** aktiviert.
- Teilweise Software-Upgrade kann nur auf einem Zweig oder RCNs durchgeführt werden und nicht auf dem MCN.

Im Folgenden finden Sie die Verwendung/Szenario, in der ein teilweises Software-Upgrade verwendet werden kann:

Überprüfen Sie, ob ein Softwarepatch mit relevanten Änderungen kompatibel ist und für eine bestimmte Site funktioniert (wobei ein teilweises Site-Upgrade durchgeführt wird). Überprüfen Sie, ob die aktualisierte Software wie erwartet funktioniert. Dies hilft, die neue Software zu validieren und an einem bestimmten Standort zu beheben, bevor das gesamte Netzwerk mit der neuen Software aktualisiert wird.

Kann ich diese Funktion verwenden, um ein Upgrade von:

- 10.0 bis 10.x
- 10.0.x bis 10.0.y
- 11.0 bis 11.y
- 11.0.x bis 11.0.y
- Alle oben genannten

Teilweise Standortsoftware-Aktualisierung ist nur anwendbar, wenn die Appliance die Softwareversion 10.x und neuer ausführt und innerhalb derselben Hauptversion der Software verwendet werden kann. Es kann zwischen den Versionen 10.0 bis 10.0.x/10.x verwendet werden. Nur im Rahmen eines teilweisen Upgrades der Standortsoftware kann die Konfiguration nicht geändert werden.

Kann ich eine neue Funktion testen, die im Rahmen eines partiellen Software-Upgrades getestet werden soll, indem ich sie über die Konfiguration aktiviere?

Nein, bei einem teilweisen Software-Upgrade muss jetzt die Active und Staged Config identisch sein. Nur Software-Version kann sich ändern.

Kann ich das partielle Software-Upgrade für RCN deaktivieren?

Nein, teilweise Software-Upgrade kann nur über MCN aktiviert oder deaktiviert werden. Bei RCN befindet sich das Feature im schreibgeschützten Modus.

Kann ich das partielle Software-Upgrade verwenden, wenn ich als 9.3.x und 10.0.x aktiv bin?

Nein, die Appliance sollte ab Version 10.0 als aktive Software ausgeführt werden.

Was passiert, wenn die Option partielle Software-Aktualisierung von MCN deaktiviert ist, während einige Zweige bereits über diese Funktion aktualisiert werden?

MCN sendet eine Benachrichtigung an alle Appliances im Netzwerk, dass die Funktion partielle Software-Aktualisierung deaktiviert ist, und dann werden alle Appliances im Netzwerk von MCN automatisch korrigiert, damit sie mit der aktiven und der Version im Staging übereinstimmen. Beachten Sie jedoch, dass MCN erwartet, dass die Option "Staged aktivieren" auf der Aktivierungsseite von **Change Management** geklickt wird. Sie können das Netzwerk aktivieren, indem Sie auf **Staged aktivieren** klicken oder auf **Vorbereitung ändern** klicken, um den Status abubrechen, indem Sie die Bestätigung akzeptieren.

Änderungsmanagement —Rollback

Was ist Rollback-Funktion im Änderungsverwaltungsprozess?

Ab Version 9.3 ermöglicht das Rollback der Änderungsverwaltung das Rollback auf die Arbeitskonfiguration, wenn unerwartete Ereignisse wie T2-App-Absturz oder Virtual Path nach einem Konfigurationsupdate inaktiv werden. Das Netzwerk und die Appliances werden nach dem Konfigurationsupdate 10 Minuten lang überwacht, und während dieses Intervalls, wenn die folgenden Bedingungen erfüllt sind (sofern der Benutzer die Funktion aktiviert hat), wird die Staged-Konfiguration aktiviert. Die Active Software wird auf Staged zurückgesetzt.

Was sind die Kriterien für den Neustart des Konfigurationsrollbacks?

Das Rollback tritt auf, wenn die folgenden Szenarien auftreten:

1. MCN - Nach der Änderung der Konfigurations-/Software, wenn der Dienst t2_app aufgrund eines Absturzes innerhalb von 30 Minuten deaktiviert wird.
2. MCN - Nach der Konfigurations-/Software-Änderung, wenn der Virtual Path Service nach der Aktivierung 30 Minuten oder länger heruntergefahren ist. Die Rollback-Funktion wird an den Standorten gestartet.
3. Site - Wenn die Site nach der Konfigurations-/Softwareveränderung die Kommunikation mit MCN verliert, wird die Rollback-Funktion initiiert.
4. Site - Nach der Konfigurations-/Software-Änderung wird t2_app Dienst aufgrund eines Absturzes innerhalb von 30 Minuten deaktiviert.

Was passiert nach dem Rollback?

Nach dem Rollback der Konfiguration wird die fehlerhafte Konfiguration/Software als Staged Software dargestellt.

Wie werden Benutzer benachrichtigt, dass ein Rollback aufgetreten ist?

Ein gelbes Banner oben in der GUI besagt, dass Config aufgrund entsprechender Fehler zurückgesetzt wird, wird angezeigt. Sie können auch sehen, dass es Change Management-Status-Tabelle ist. Es zeigt **Konfigurationsfehler** oder **Softwarefehler** an, der dem Standort entspricht, für den ein Rollback aufgetreten ist.

Wird sowohl Konfiguration als auch Software zurückgesetzt?

Ja, wenn ein Software-Upgrade zusammen mit der Konfiguration durchgeführt wird und ein Rollback-Szenario auftritt, dann wird auch Software zurückgesetzt.

Was passiert, wenn es ein Problem in MCN gibt und die Verbindung mit allen Standorten abstürzt oder verliert?

Das gesamte Netzwerk wird mit Ausnahme von MCN zurückgesetzt. Benachrichtigung wird angezeigt, und alle Sites zeigen den Rollback-Status im Bereich Änderungsverwaltung an. Sie können das Problem auf MCN manuell beheben.

Können wir diese Funktion deaktivieren?

Ja, wir können diese Funktion kurz vor der Aktivierung deaktivieren. Diese Funktion ist jedoch standardmäßig aktiviert.

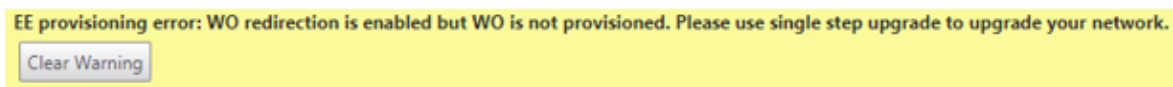
Wie interagiert Rollback mit partieller Software-Aktualisierung, wenn ich über ein mehrstufiges Netzwerk verfüge?

- Wenn das partielle Software-Upgrade deaktiviert ist und ein Standort in einer Region (oder im RCN) zurückgesetzt wird, wird die Region mit dem Problem zurückgesetzt und nach Abschluss des Rollbacks an den MCN weitergeleitet. Infolgedessen wird der MCN und der Rest des Netzwerks zurückgesetzt. Sowohl der RCN in der Region, die zurückgesetzt wurde, als auch der MCN zeigen das Rollback-Banner an, dass der MCN das Rollback-Banner am RCN nicht automatisch schließen kann.
- Wenn ein teilweises Software-Upgrade aktiviert ist und ein Standort in einer Region (oder im RCN) zurückgesetzt wird, wird nur dieser Bereich zurückgesetzt. Das Rollback-Ereignis wird nicht an den MCN weitergegeben. Infolgedessen verlässt der MCN die Region. Der MCN zeigt kein Rollback-Banner an und rollt nicht selbst oder das Netzwerk zurück.

In beiden Szenarien zeigt der RCN das Rollback-Banner an, bis es geschlossen wird. Weil es von MCN nicht automatisch verworfen werden kann.

2100 Premium (Enterprise) Edition

Was zeigt die folgende Meldung an, wenn eine 2100 EE Appliance auf Version 10.0 aktualisiert wird?



Die Appliance verfügt über eine EE-Lizenz oder die WANOP-Umleitung ist über MCN aktiviert. Sie können die Installation von WANOP-Komponenten planen, um mit der Provisioning von WANOP-Features auf dieser Plattform zu beginnen.

Verwandte Informationen

- [Zero Touch-Bereitstellung über LTE](#)
- [Konfigurieren des sekundären MCN in HA](#)

Referenzmaterial

May 10, 2021

Anwendungssignaturbibliothek

Eine Liste der Anwendungen, die die Citrix SD-WAN Appliances mithilfe der Deep Packet Inspection identifizieren können.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).