Citrix SD-WAN 11.3

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

November 16, 2022

In diesen Versionshinweisen werden die Neuheiten, behobenen Probleme und bekannten Probleme beschrieben, die für Citrix SD-WAN Software Release 11 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.

Neue Features

Anwendungsorientierte Verbesserungen

Verbesserte API-basierte Klassifizierung von Anwendungsanbietern Die erste Paketklassifizierung des Microsoft Office 365-Datenverkehrs und des Citrix Cloud- und Gateway-Dienstverkehrs erfolgt unabhängig davon, ob der direkte Internet-Breakout für diesen Datenverkehr aktiviert ist oder nicht. Daher können anwendungsspezifische Regeln jetzt mit diesen Anwendungen konfiguriert werden, ohne dass Sie unbedingt den Datenverkehr ins Internet ausbrechen müssen.

[NSSDW-27821]

Link-Aggregation über LACP Zuvor wurde in LAG nur der Active-Backupmodus unterstützt. Ab Version 11.3 werden die protokollbasierten 802.3AD Link Aggregation Control Protocol-Verhandlungen (LACP) unterstützt. Das LACP ist ein Standardprotokoll und bietet mehr Funktionalität für LAGs.

[NSSDW-25021]

Unterstützung für IPv6 Citrix SD-WAN bietet die folgenden IPv6-Funktionen:

- **NDP-Routerankündigung** - In einem IPv6-Netzwerk multicast die SD-WAN-Appliance regelmäßig Router-Advertisement (RA) -Nachrichten, um ihre Verfügbarkeit anzukündigen und Informationen an die benachbarten Appliances im SD-WAN-Netzwerk zu übermitteln. Das Neighbor Discovery-Protokoll (NDP), das auf den SD-WAN-Appliances ausgeführt wird, verwendet diese Router-Advertisements, um die benachbarten Geräte auf demselben Link zu ermitteln Es bestimmt auch die Link-Layer-Adressen des anderen, findet Nachbarn und verwaltet Informationen zur Erreichbarkeit der Erreichbarkeit über die Wege zu aktiven Nachbarn.

> **Hinweis:**
>
> Citrix SD-WAN Orchestrator-Services unterstützen keine IPv6-Adressen.

Die folgenden Funktionen von Citrix SD-WAN Appliances unterstützen IPv6-Adressen:

- Funktionen der Managementebene
  - Verwaltungsoberfläche
  - RADIUS-Server
  - TACACS+ Server
  - SMTP-Server
  - syslog-Server
  - HTTP-Server
  - DNS-Server
  - App-Flow/IPFIX
  - SNMP
  - Remotelizenzierung
  - Zentrale Lizenzierung
  - NTP-Server
  - Positivliste
  - Neue Benutzeroberfläche für SD-WAN-Appliances
  - Diagnose

> **Hinweis**
>
> Wenn Sie nach der Konfiguration der oben aufgeführten Funktionen das IPv4- oder IPv6-Protokoll deaktivieren, funktionieren die Funktionen nicht wie erwartet.

- Merkmale der Datenebene
  - Statisches Routing
  - Internetdienst über IPv6-WAN-Verbindungen
  - Intranetdienst über IPv6-WAN-Verbindungen
  - Router-Werbung
  - DHCP-Kunde
  - DHCP-Server/Relay
  - Anwendung QoS
  - Firewall
  - Inband-Verwaltung
  - Hohe Verfügbarkeit
  - IP-Regeln
  - IPv6 wird über LTE-Verbindungen unterstützt

[NSSDW-1938, NSSDW-21915]

Verbesserungen bei der Sicherheit

Benutzerkonten Die Rollen des Netzwerkadministrators und des Sicherheitsadministrators in Citrix SD-WAN Center oder der Citrix SD-WAN Appliance-Benutzeroberfläche können die Konfiguration ändern und die Änderungen bereitstellen, um eine Site vollständig bereitzustellen. Der Sicherheitsadministrator kann den Schreibzugriff auf die Firewall auch für alle Benutzerkonten außer dem Superadministrator aktivieren oder deaktivieren.

[NSSDW-31045]

Erweiterte Edge-Sicherheitsunterstützung für Citrix SD-WAN 410 SE Appliance Citrix SD-WAN 410 SE Appliances unterstützen jetzt Advanced Edge Security-Funktionen mit Advanced Security Add-On-Lizenzen.

[NSSDW-27582]

Verbesserung der Benutzeroberfläche

Neue Benutzerschnittstelle Die neue Benutzeroberfläche von Citrix SD-WAN ist jetzt für Citrix SD-WAN 410 SE und Citrix SD-WAN SE VPX-Plattformen verfügbar.

> **HINWEIS**
>
> Die Provisioning der Citrix SD-WAN 210-SE-, 410 SE- oder VPX SE-Plattformen als MCN leitet Sie auf die ältere Benutzeroberfläche um.

[NSSDW-29803]

LTE-Verbesserungen

Unterstützung für USB LTE-Modems 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. Neben Citrix SD-WAN 110 SE, 110 LTE Wi-Fi, 210 SE und 210 LTE Wi-Fi wird die Unterstützung des externen USB-LTE-Modems nun auf die folgenden Plattformen ausgedehnt:

- Citrix SD-WAN 1100 SE / AE / PE
- Citrix SD-WAN 2100 SE / PE

- Citrix SD-WAN 110 SE Wi-Fi

[NSSDW-24523]

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.

[NSSDW-29811]

LTE Signalstärke Sie können die Informationen zur LTE-Signalstärke als Teil der Site-Berichte unter **Site > Berichte > Appliance Reports > LTE-Signal**anzeigen. Die Registerkarte **LTE-Signal** ist nur für Citrix SD-WAN 110 und 210 Appliances sichtbar.

[NSSDW-26505]

Plattform

Citrix SD-WAN 110-WiFi-SE Die Citrix SD-WAN 110-WiFi-SE-Plattform ist eine branchenseitige Appliance, die in Kleinst- und kleinen Zweigstellen, Remotestandorten/Einzelhandelsgeschäften, Privathaushalten und temporären Arbeitsstätten eingesetzt werden kann. Eine einzelne Box-in-Branch-Lösung trägt dazu bei, den Hardwarebedarf zu reduzieren und die Bereitstellung von Zweigstellen zu erleichtern. Die Citrix SD-WAN 110-Wifi-SE Appliance kann als Zugriffspunkt konfiguriert werden. Dadurch entfällt die Notwendigkeit, eine zusätzliche Access Point-Appliance zu verwalten, um ein WLAN zu erstellen. Die Geräte in Ihrem LAN können über Wi-Fi eine Verbindung zur Citrix SD-WAN 110-WiFi-SE Appliance herstellen.

> **HINWEIS**
>
> Citrix SD-WAN 11.3.0 ist die Mindest-Softwareversion, die Wi-Fi-Fifähigkeiten für das Citrix SD-WAN 110-LTE-Wifi und das Citrix SD-WAN 110-WiFi-SE-Modell unterstützt.

[NSSDW-1920]

Cloud-Verwaltung

Unterstützung für M5- und C5-Instanzen auf AWS Citrix SD-WAN hat Unterstützung für die M5- und C5-Instanzen in Amazon Web Services (AWS) eingeführt.

[NSSDW-23745]

AWS-Außenposten Citrix SD-WAN hat Unterstützung für die Funktion “AWS Outposts”eingeführt.

[NSSDW-23823]

NITRO Rest APIs für PE WANOP Einstellungen

Sie können jetzt WANOP Virtual Machine Appliance-Einstellungen in einer PE-Appliance mit Citrix SD-WAN NITRO REST APIs konfigurieren und abrufen. Diese neuen APIs sind für PE-unterstützte Plattformen verfügbar - 1100, 2100, 5100 und 6100. Detaillierte Informationen zur API-Nutzung erhalten Sie in der Citrix SD-WAN NITRO-API-Dokumentation unter dem Abschnitt **WAN-Optimierung**. Im Folgenden sind die **WANOP-Einstellungen** aufgeführt, die mit den NITRO-APIs konfiguriert werden können:

- KeyStore-Einstellungen
- Window Domain Join
- Delegieren von Benutzern
- SSL CA- und SSL-Zertifikat-Key-Paar
- SSL-Profil
- Sicheres Peering

[SDW-14532]

Verbesserungen bei SD-WAN Orchestrator

Wi-Fi Zugangspunkt Sie können eine Citrix SD-WAN-Appliance konfigurieren, die Wi-Fi als Wi-Fi Access Point unterstützt, sodass Sie keine zusätzliche Access Point-Appliance aufrechterhalten müssen, um ein WLAN zu erstellen. Die Geräte in Ihrem LAN können über Wi-Fi eine Verbindung zur Citrix SD-WAN-Appliance herstellen.

Die folgenden zwei Varianten der Citrix SD-WAN 110-Plattform unterstützen Wi-Fi und können als Zugangspunkt konfiguriert werden:

- Citrix SD-WAN 110-WiFi-SE
- Citrix SD-WAN 110-LTE-WLAN

Weitere Informationen zu den Plattformen finden Sie unter Citrix SD-WAN 110 SE.

Sie können Citrix SD-WAN-Appliances konfigurieren und verwalten, die über den Citrix SD-WAN Orchestrator-Dienst als Access Points konfiguriert sind. Mit dem Citrix SD-WAN Orchestrator-Dienst können Sie auch Wi-Fi-bezogene Berichte wie verbundene Geräte, verwendete Daten, Nutzungs- und Authentifizierungsfehlerprotokolle sowohl auf Netzwerkebene als auch auf Einzelstandortebene anzeigen.

Es gibt 2 Geographie-SKUs zur Unterstützung von 110 Wi-Fi SE und 110 LTE Wi-Fi SE, eine für die USA oder Kanada und die andere für Rest of World (ROW).

[NSSDW-1920, NSSDW-28612]

Verbesserungen bei der Sicherheit Firewall-Standardeinstellungen

Die Dropdownliste **Aktion, in der Sicherheitsprofile nicht inspiziert werden können**, wird eingeführt, um eine Aktion für die Pakete zu definieren, die einer Firewall-Regel entsprechen, ein Sicherheitsprofil aktivieren, aber vorübergehend nicht vom Edge-Security-Subsystem überprüft werden können. Wenn Sie **Ignorieren**auswählen, wird die entsprechende Firewallregel als nicht übereinstimmend behandelt, und die nächste Firewallregel wird in der Reihenfolge ausgewertet. Wenn Sie **Drop**auswählen, werden die Pakete, die der entsprechenden Firewall-Regel entsprechen, verworfen.

[SDW-9990]

IPS-Profile

Mit IPS-Profilen können Sie eine Kombination von IPS-Regeln für eine bestimmte Gruppe von Websites innerhalb des Netzwerks aktivieren. Wenn ein IPS-Profil aktiviert ist, überprüft es den Netzwerkverkehr nur für die Websites, mit denen das IPS-Profil verknüpft ist, und die in diesem Profil aktivierten IPS-Regeln. Sie können IPS-Profile auf Citrix SD-WAN Orchestrator-Diensten auf Netzwerkebene unter **Konfiguration > Sicherheit > Intrusion Prevention**erstellen.

[NSSDW-28281]

Anti-Malware

Sie können neue Dateitypen und MIME-Typen für das Anti-Malware-Scannen hinzufügen. Wenn Anti-Malware den Zugriff auf eine Website verweigert, können Sie einen externen Serverstandort festlegen, um Benutzer umzuleiten. Die Benutzer können auf die vom SD-WAN Orchestrator bereitgestellte Standard-Umleitungsseite umgeleitet werden, oder Sie können eine benutzerdefinierte Umleitungsseite erstellen.

[NSSDW-26640]

Webfilter-Option für erweiterte Edition

Für die Sicherheitsfunktionalität für die Webfilterung werden unter den **erweiterten Optionen die folgenden Optionen**für sicheres Durchsuchen hinzugefügt:

- Durchsetzung der sicheren Suche bei beliebten Suchmaschinen
- Beschränkungsmodus auf YouTube durchsetzen
- Erzwinge die Suche durch kinderfreundliche Suchmaschinen

[NSSDW-26636]

SSL Inspektion

Sie können jetzt die Secure Sockets Layer (SSL) -Prüfung für den Datenverkehr konfigurieren, der zu und von Ihrer Organisation fließt. Die SSL-Inspektion fängt, entschlüsselt und scannt das HTTPS und sichert den SMTP-Verkehr auf bösartige Inhalte. Sie können SSL-Regeln als Teil von Sicherheitsprofilen erstellen und Bedingungen definieren, unter denen der Datenverkehr einer SSL-Inspektion unterzogen wird.

Die SSL-Inspektion kann über Citrix SD-WAN Orchestrator konfiguriert werden. Die SSL-Inspektionsoption wurde unter **Konfiguration > Sicherheit** und **Konfiguration > Sicherheitsprofil > Neues Sicherheitsprofil**neu hinzugefügt.

[NSSDW-24377]

Behobene Probleme

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 Citrix 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-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.

NSSDW-29862: Die virtuelle SD-WAN Center-Maschine, die auf dem VMware ESXi-Hypervisor ausgeführt wird, bleibt möglicherweise hängen, während ein Snapshot erstellt wird.

NSSDW-31822: Bei der Verwaltung eines skalierbaren Netzwerks (> 500 Standorte), an dem der Controller (MCN oder RCN) und die Zweige jeweils mehrere WAN-Verbindungen haben, kann es bei einem Controller während eines größeren Konfigurationsupdates zu einer Dienstunterbrechung kommen.

NSSDW-31903: Bei der Durchführung einer erneuten Authentifizierung werden negative Werte für das Hoch- und Download-Programm in Wi-Fi-Client-Berichten angezeigt.

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

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

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-1309: Mit Citrix SD-WAN 11.1.x Release wurde das Azure Virtual WAN-Konfigurationsmodell von der **Verwendung vorab erstellter Intranetdienste** auf die **Auswahl von WAN-Verbindungen** für die automatische Erstellung von Intranetdiensten geändert. In diesem Fall wurde der Kunde von 10.x aktualisiert, und die höhere Version wurde nicht zusammen mit der vorherigen Azure Virtual WAN-Konfiguration entfernt. Mit dieser Änderung wurden doppelte Einträge erstellt, als die neue Site mit einer neuen SD-WAN Center-Bereitstellung bereitgestellt wurde. Infolgedessen schlug die Importkonfiguration fehl und die zuvor erstellten Azure Virtual WAN-Konfigurationen wurden nicht angezeigt.

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-Untermodelle über REST-APIs.

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).

SDWANHELP-1326: Nach dem Upgrade von Citrix SD-WAN auf Version 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 Instanz auf den Standardwert von 16 statischen virtuellen Pfaden zurück. Es führt zu undefiniertem Verhalten und möglichen Absturzszenarien, wenn mehr als 16 statische virtuelle Pfade konfiguriert sind.

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

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-Domänendienstrouten zum Exportieren der Route an andere verbundene Standorte funktioniert nicht.

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

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

SDWANHELP-1420: In der Citrix 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 Standortdiagnosetest nicht gleichzeitig für einen bestimmten Standort von der Peer-Appliance aus starten.

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

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

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

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.

SDWANHELP-1484: Ein Fehler bei der Verarbeitung von PCKS12-Bundles verhindert, dass Bündel, bei denen der Schlüssel vor der Verarbeitung des Zertifikats steht.

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

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-1507: Ein Problem im Konfigurationsmodul bestand darin, dass die Exportrouteneinstellung wahr war, während die Einstellung für die WAN-zu-WAN-Weiterleitung 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 über Top-Anwendungen einer Site nicht mit den Daten im Bericht Top Sites überein. Dies geschah aufgrund einer unerwünschten Regex-Übereinstimmung des Site-Namens.

SDWANHELP-1535: Wenn der 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-1537: Die Citrix SD-WAN Center-Authentifizierung für TACACS-basierte Benutzer scheiterte bei einigen Kombinationen von Kennwörtern mit $ und # Zeichen im Kennwort. Dieses Problem war in der Version 11.2.0 enthalten.

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

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

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

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

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-1643: Die Option **Packet Resequencing** in der IP QoS-Regel kann nicht deaktiviert werden, sobald sie auf aktiviert wurde.

SDWANHELP-1646: Der Management-Port darf nicht in der LAG hinzugefügt werden, daher haben wir die Verwaltungsschnittstelle während der Bildung der LAG nicht aufgelistet.

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 **Zertifikatsperrlisten** aktiviert wurden, trat ein Fehler auf, der wiederholte Download-Versuche der CRL verursachte.

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-23134: Nach dem Upgrade des MCN von 10.x auf 11.x Release versucht der MCN konsequent, das 10.x-Softwarepaket mit dem 11.x-Build auf die neu hinzugefügte Site zu übertragen.

- **Umgehung**: Führen Sie das Change Management erneut durch, um einen konsistenten Software-Push zu lösen

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-31082: Der Datenverkehr zwischen Wireless-Clients ist vom Datenpfad in der Citrix SD-WAN 110-Plattform isoliert. Infolgedessen ist es nicht Teil der Paketerfassung.

NSSDW-31476: Nach dem Konfigurationsupdate für den Einarmmodus mit der LAG-Schnittstelle geht der virtuelle Pfad aufgrund einer **ARP-Eintrittskonflikt** für VIPs der LAG-Schnittstelle im Router (PBR) ab.

- **Problemumgehung**: Wenn Sie ARP auf dem Router (PBR) löschen, wird der ARP-Eintrag richtig gelernt und der virtuelle Pfad wird angezeigt.

NSSDW-31696: Eine Änderung der SSL Inspection Root Certificate Authority (CA) und des Schlüssels wird nicht an die SD-WAN-Appliance weitergegeben, es sei denn, eine andere Edge-Sicherheitseinstellung wird ebenfalls geändert. Dies führt dazu, dass die SSL-Inspektion mit der vorherigen Stamm-CA durchgeführt wird.

- **Problemumgehung**: Ändern Sie eine andere Einstellung für Edge-Sicherheit, und führen Sie sie dann aus und aktivieren Sie sie. Dies löst den Download und die Anwendung der Root-Zertifizierungsstelle und des Schlüssels aus.

NSSDW-31998: Der DHCPv4- und DHCPv6-Modus auf der LTE-Schnittstelle kann dazu führen, dass das SD-WAN-Gerät nach Konfigurationsaktualisierungen die IP-Adresse verliert.

- **Problemumgehung**: Starten Sie den Dienst neu.

NSSDW-32110: Eine WAN-Verbindung, die als DHCP-Client konfiguriert ist, führt zu einem Virtual Path-Fehler. Dieses Problem tritt auf, wenn der Name der WAN-Verbindung geändert und das Änderungsmanagement durchgeführt wird.

- **Problemumgehung**: Starten Sie den Citrix Virtual Wan Service neu.

NSSDW-32139: Dynamic NAT funktioniert möglicherweise nicht ordnungsgemäß oder verursacht eine Dienstunterbrechung während der Konfigurationsupdates, wenn sie sowohl für IPv4 als auch für IPv6 in einem Internetdienst mit aktiviertem Internet Load Balancing verwendet wird.

NSSDW-32185: Ein Überwachungsfehler während der Konfiguration verhindert, dass Benutzer den Internetdienst auf einer Site konfigurieren, es sei denn, alle WAN-Verbindungen sind mit Zugriffsschnittstellen desselben IP-Typen konfiguriert.

NSSDW-32197: Die Wi-Fi-Funktion unterstützt keine Hochverfügbarkeit (HA) im Citrix SD-WAN 11.3-Release.

NSSDW-32212: Wenn Internetdienst für WAN-Verbindungen aktiviert ist, die über eine IPv6-Zugriffsschnittstelle verfügen, kann es nach dem Konfigurationsupdate zu einer Betriebsunterbrechung kommen.

- **Problemumgehung**: Starten Sie den Dienst neu.

NSSDW-32219: Wenn der Benutzer den Status des internen Modems einsehen möchte, zeigt die Legacy-Benutzeroberfläche auch den Status des externen Modems an.

NSSDW-32221: Aktivieren und Deaktivieren des externen Modems funktioniert nicht über die Legacy-Benutzeroberfläche.

- **Problemumgehung**: Verwenden Sie Citrix SD-WAN Virtual WAN CLI, um die ältere Benutzeroberfläche zu aktivieren/deaktivieren.

NSSDW-32257: Die Appliance-Einstellungen werden nicht auf Citrix SD-WAN angewendet, wenn sie von Citrix SD-WAN Center übertragen werden.

- **Problemumgehung**: Verwenden Sie RestAPI, um diese Appliance-Einstellungen festzulegen.

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-1733: Nachdem Citrix SD-WAN Center auf die 11.3-Softwareversion aktualisiert wurde, zeigt die Lizenzierungsseite die Anzahl der Lizenzgebühren in den **Lizenzdetails**an, obwohl alle Geräte, die bisher von diesem SD-WAN Center lizenziert waren, weiterhin lizenziert sind.

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. Wählton 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 für Citrix SD-WAN 11.3.1

October 28, 2021

Dieses Dokument mit Versionshinweisen beschreibt die Verbesserungen und Änderungen, behobenen und bekannten Probleme, die für das Citrix SD-WAN Release 11.3.1 bestehen.

> **Hinweis**
>
> Citrix SD-WAN 11.3.1a behebt die in https://support.citrix.com/article/CTX297155 beschriebenen Sicherheitslücken und ersetzt Version 11.3.1.

Neue Features

Konfiguration und Management

Citrix SD-WAN Neue Verbesserungen der Benutzeroberfläche für Clients

Die Citrix SD-WAN Neue Benutzeroberfläche enthält die folgenden Verbesserungen:

- Konfiguration von Management-IP-Zulassungslisten
- Metered Link-Statistiken.
- Orchestrator-Konnektivitätsstatus.
- Appliance-Modell, Bandbreite und Lizenztyp werden im Header angezeigt.

[NSSDW-33155]

Citrix SD-WAN Neues UI-Update

Das Erscheinungsbild der Citrix SD-WAN New UI wurde geändert, um die neue Farbe und Schriftart des Citrix Rebranding widerzuspiegeln.

[NSSDW-30842]

SNMP

Die folgenden SNMP-MIBs werden hinzugefügt:

- Appliance-Statistiken
  - Der Prozentsatz der CPU, der für die Appliance verwendet wird
  - Der Prozentsatz des für die Appliance verwendeten Arbeitsspeichers
- Tabelle WAN-Link-Statistiken
  - Die maximale physische LAN-zu-WAN-Rate in Kbps für die WAN-Verbindung
  - Die maximale physische RATE von WAN zu LAN in Kbps für die WAN-Verbindung
  - Der von LAN zu WAN erlaubte Rate in Kbit/s für die WAN-Link
  - Der erlaubte WAN-LAN-Zinssatz in Kbit/s für die WAN-Verbindung

[NSSDW-30592]

Default-/Fallback-Konfiguration

Ab Citrix SD-WAN 11.3.1 bietet Citrix SD-WAN die Möglichkeit, die statischen IP-Adressen manuell zu konfigurieren, die den WAN-Ports in Abwesenheit von DHCP zur Verwendung des In-Band-Managements für die Erstbereitstellung zugewiesen werden können.

[NSSDW-27033]

In-Band-Verwaltung

In-Band-Management unterstützt Gerätepaare mit hoher Verfügbarkeit. Die Appliances in einem Hochverfügbarkeitspaar kommunizieren über den In-Band-Zugriff miteinander.

[NSSDW-24534]

Schnittstellengruppen

Sie können eine virtuelle Schnittstelle in einer Schnittstellengruppe mithilfe des Kontrollkästchens **Aktivieren aktivieren** oder deaktivieren.

[NSSDW-24512]

Unterstützung für IPv6

NDP Router Advertisement - In einem IPv6-Netzwerk versendet die SD-WAN-Appliance regelmäßig Router Advertisement (RA) -Nachrichten, um ihre Verfügbarkeit bekannt zu geben und Informationen an die benachbarten Appliances im SD-WAN-Netzwerk zu übermitteln. Das Neighbor Discovery-Protokoll (NDP), das auf den SD-WAN-Appliances ausgeführt wird, verwendet diese Router-Advertisements, um die benachbarten Geräte auf demselben Link zu ermitteln Es bestimmt auch die Link-Layer-Adressen des anderen, findet Nachbarn und verwaltet Informationen zur Erreichbarkeit der Erreichbarkeit über die Wege zu aktiven Nachbarn.

> **Hinweis:**
>
> Citrix SD-WAN Orchestrator-Services unterstützen keine IPv6-Adressen.

Die folgenden Funktionen von Citrix SD-WAN Appliances unterstützen die IPv6-Adresse:

- Funktionen der Managementebene
  - Verwaltungsoberfläche
  - RADIUS-Server
  - TACACS+ Server
  - SMTP-Server
  - syslog-Server
  - HTTP-Server
  - DNS-Server
  - App-Flow/IPFIX
  - SNMP
  - Remotelizenzierung
  - Zentrale Lizenzierung
  - NTP-Server
  - Positivliste
  - Neue Benutzeroberfläche für SD-WAN-Appliances
  - Diagnose

> **Hinweis**
>
> Wenn Sie nach der Konfiguration der oben aufgeführten Funktionen das IPv4- oder IPv6-Protokoll deaktivieren, funktionieren die Funktionen nicht wie erwartet.

- Merkmale der Datenebene
  - Statisches Routing
  - Internetdienst über IPv6-WAN-Verbindungen
  - Intranetdienst über IPv6-WAN-Verbindungen
  - Router-Werbung
  - DHCP-Kunde
  - DHCP-Server/Relay
  - Anwendung QoS
  - Firewall
  - Inband-Verwaltung
  - Hohe Verfügbarkeit
  - IP-Regeln
  - IPv6 wird über LTE-Verbindungen unterstützt

[NSSDW-1938, NSSDW-21915]

Sonstiges

Überprüfen Sie die Punkt-VM-

Ab Citrix SD-WAN 11.3.1 wird die Check Point VM Version 80.20 und höher für die Provisioning von VM auf neuen Standorten unterstützt.

[NSSDW-30833]

Netzwerk

Dynamisches Routing

Sie können eine Router-ID für das gesamte Protokoll und auch eine Router-ID pro Routingdomäne konfigurieren. Mit dieser Verbesserung können Sie stabiles dynamisches Routing über mehrere Instanzen hinweg ermöglichen, wobei verschiedene Router-IDs auf stabile Weise konvergieren. Wenn Sie eine Router-ID für eine bestimmte Routingdomäne konfigurieren, überschreibt die spezifische Router-ID die Routingdomäne auf Protokollebene.

[NSSDW-30132]

PPPoE-Sitzungen

Ab der Citrix SD-WAN 11.3.1-Version wird ein zusätzlicher 8-Byte-PPPoE-Header für die Anpassung der TCP-Maximal-Segmentgröße (MSS) berücksichtigt. Der zusätzliche 8-Byte-PPPoE-Header passt den MSS in den Synchronisierungspaketen basierend auf der MTU an.

[NSSDW-22779]

Behobene Probleme

Konfiguration und Management

- Während der Datenbankarchivierung großer Netzwerke wurden die statistischen Datensätze auf der MCN-Appliance für einige Minuten nicht in die Statistikdatenbanktabellen eingefügt.

  [SDWANHELP - 1872]

- Während Schnittstellenänderungen verwendet VRRP möglicherweise immer noch alte Schnittstellendaten, die zu einem Core-Dump führen können.

  [SDWANHELP - 1867]

- Die Konfiguration der gehosteten Firewall auf der lokalen GUI wird nicht geladen, wenn sich die Firewall-VM im Status Shutdown befindet.

  [SDWANHELP-1839]

- Sie können das **Backup Management Network** nicht als **Keine** wählen, während Sie virtuelle IP-Adressen konfigurieren.

  [SDWANHELP - 1824]

- Das Feld “**Öffentliche IPv4-Adresse** “wurde im Abschnitt “**Basis** “des Konfigurationseditors ausgegraut.

  [SDWANHELP-1780]

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

  [NSSDW-32629]

- Appliance-Einstellungen werden nicht auf Citrix SD-WAN angewendet, wenn sie von Citrix SD-WAN Center übertragen werden.

  [NSSDW-32257]

- Ein Überwachungsfehler während der Konfiguration verhindert, dass Benutzer den Internetdienst auf einer Site konfigurieren, es sei denn, alle WAN-Verbindungen sind mit Zugriffsschnittstellen desselben IP-Typen konfiguriert.

  [NSSDW-32185]

Lizenz

- Wenn auf Citrix SD-WAN 110 und 210 Plattformen der Management-Port als Daten-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.

  [SDWANHELP-1866]

Sonstiges

- Wenn Sie die Anmeldeseite von Citrix SD-WAN Center 11.3.0 in einem Browser im Vollbildmodus anzeigen, werden das Citrix Logo und der Produktname nicht korrekt angezeigt.

  [SDWANHELP-1910]

- Die Rolle "Netzwerkadministrator"hat Zugriff auf die Ausführung der rollenspezifischen Aktivitäten des Sicherheitsadministrators, die gemäß der Definition der Rolle "Netzwerkadministrator"nicht zulässig sein dürfen.

  [SDWANHELP-1906]

- Der**Import** und **Export** großer Netzwerkkonfigurationen (wenn die Größe der Konfigurationsdatei 16 MB überschritten hat) in Citrix SD-WAN Center fehlgeschlagen.

  [SDWANHELP-1787]

- Die E-Mail-Benachrichtigung von Citrix SD-WAN Center fügt dem **AUTH-Befehl** ein zusätzliches CR-Zeichen hinzu, wodurch die SMTP-Sitzung beendet wird.

  [SDWANHELP-1736]

Netzwerk

- Wenn ein auf LAN-Seite oder über lokalen Dienst empfangenes Paket, das eine Fragmentierung erfordert, über LAN-GRE gesendet wird, stürzt der SD-WAN-Dienst ab.

  [SDWANHELP-1846]

- Bei einer Internetdienstroute in einer nicht standardmäßigen Routingdomäne und einer Pfadberechtigung wird die Internetroute nicht als nicht erreichbar markiert, wenn der Pfad ausfällt und die Remote-Site nicht konfiguriert ist, wenn der Pfad ausfällt und der Remote-Site nicht konfiguriert ist.

  [SDWANHELP-1400]

- Wenn Internet Service für WAN-Verbindungen aktiviert ist, die über eine IPv6-Zugriffsschnittstelle verfügen, kann es nach dem Konfigurationsupdate zu einer Betriebsunterbrechung kommen.

[NSSDW-32212]

- Die Wi-Fi-Fi-Feature unterstützt keine Hochverfügbarkeit (HA) im Citrix SD-WAN 11.3-Release.

  [NSSDW-32197]

- Dynamic NAT funktioniert möglicherweise nicht ordnungsgemäß oder verursacht eine Dienstunterbrechung während der Konfigurationsupdates, wenn sie sowohl für IPv4 als auch für IPv6 in einem Internetdienst mit aktiviertem Internet-Lastenausgleich verwendet wird.

  [NSSDW-32139]

- Der DHCPv4- und DHCPv6-Modus auf der LTE-Schnittstelle kann dazu führen, dass das SD-WAN-Gerät nach Konfigurationsaktualisierungen die IP-Adresse verliert.

  [NSSDW-31998]

Plattform und Systeme

- Wenn die NAT-Informationen der Firewall mit der CLI abgelegt werden, stürzt die Appliance ab.

  [SDWANHELP-1901]

- Die Firewallregeln erlauben die ICMP-Ping-Anfrage, die auf einer nicht vertrauenswürdigen Schnittstelle empfangen wurde, löscht jedoch die Ping-Antwort und daher stürzt der SD-WAN-Dienst ab.

  [SDWANHELP-1865]

- Wenn die transparente DNS-Weiterleitung aktiviert ist, kann die Verarbeitung großer DNS-Antwortpakete zu einem Stacküberlauf führen, da keine ordnungsgemäßen Grenzbedingungsprüfungen vorliegen. Ein Anwendungsfall ist, wenn der Cloud-Dienst möglicherweise IPs von DNS lernen muss, um die Klassifizierung der Standardkategorie von Office 365 zu ermöglichen.

  [SDWANHELP - 1891]

- Nach dem Upgrade des Citrix SD-WAN-Geräts auf die Version 11.2.2 fungieren mehr als ein VRRP-Gerät aufgrund der falschen VRRP-Anzeigenpaketgröße, die vom SD-WAN-Gerät gesendet wird, als **Master**.

  [SDWANHELP-1804]

- Wenn während der Erstellung des dynamischen virtuellen Pfads (DVP) die Protokollnachricht mit einem unerwarteten IP-Typ-Dienstwert (TOS) eingeht, kann dies zu einem Core-Dump führen.

  [SDWANHELP-1783]

- Für die Pfad-MTU-Erkennung werden die Pfad-MTU-Probe-Ereignisse zur Verarbeitung während eines Timerstarts in die Warteschlange gestellt. Ein Segmentierungsfehler tritt auf, wenn ein Sonde-Ereignis nicht gültig ist, wenn die tatsächliche Ausführung versucht wird.

  [SDWANHELP-1754]

- Wenn sich die Erreichbarkeit des GRE-Tunnels von UP nach Down ändert, werden die GRE-Tunnelrouten, die für einen GRE-Tunnel zugelassen sind, nicht mit der Änderung des Erreichbarkeitsstatus aktualisiert.

  [SDWANHELP-1623]

- In der Azure HA-Bereitstellung werden SD-WAN-Pfade nicht angezeigt, wenn die sekundäre Zugriffsschnittstelle für die WAN-Verbindung konfiguriert ist.

  [SDWANHELP-1578]

Bekannte Probleme

Konfiguration und Management

- Citrix SD-WAN UI zeigt einen Fehler an, wenn ein doppelter Name für DNS Proxy im Netzwerk verwendet wird.

  - Problemumgehung: Verwenden Sie einen eindeutigen netzwerkweiten Namen für DNS-Proxy.

  [NSSDW-33842]

- Wenn eine Appliance sowohl für DHCP-IPv4- als auch für DHCP-IPv6-Adressen konfiguriert ist, für das Netzwerk jedoch nur ein DHCP-IPv6-Server konfiguriert ist, wartet die Appliance weiterhin auf die DHCP-IPv4-Adresse und wird daher auch nicht mit der IPv6-Adresse zugewiesen.

  [NSSDW-33741]

- Wenn In-Band-HA konfiguriert ist, ermöglicht die SD-WAN-Benutzeroberfläche einem Benutzer, sich nur an einem der Ports (443, 444 oder 445) in einem Webbrowser anzumelden. Wenn sich ein Benutzer beispielsweise bei `https://<ip-address>` angemeldet hat und sich auf einer anderen Registerkarte bei `https://<ip-address>:444` anmeldet, wird der Benutzer von `https://<ip-address>`abgemeldet.

  - Problemumgehung: Verwenden Sie einen anderen unterstützten Webbrowser als den, der für den Zugriff auf das Citrix SD-WAN-Gerät verwendet wird.

  [NSSDW-33336]

- Das Aktivieren und Deaktivieren eines externen Modems funktioniert nicht über die Legacy-Benutzeroberfläche.

  - Problemumgehung: Verwenden Sie die SD-WAN Virtual WAN CLI, um externes Modem zu aktivieren/deaktivieren

  [NSSDW-32221]

- Wenn der Benutzer den Status des internen Modems einsehen möchte, zeigt die Legacy-Benutzeroberfläche auch den Status des externen Modems an.

  [NSSDW-32219]

- Eine WAN-Verbindung, die als DHCP-Client konfiguriert ist, führt zu einem Ausfall des virtuellen Pfads. Dieses Problem tritt auf, wenn der Name der WAN-Verbindung geändert und das Änderungsmanagement durchgeführt wird.

  - Problemumgehung: Starten Sie den Citrix Virtual Wan-Dienst neu.

  [NSSDW-32110]

- Der Orchestrator-Benutzeroberfläche und der Config-Compiler lassen sich nicht aus dem zulässigen Bereich des DHCP-Leasingintervalls herausgreifen, wodurch der DHCP-Daemon ausfällt.

  [NSSDW-25452]

Netzwerk

- Sobald SLAAC eine IP- und Gateway-Adresse von einem Router erfährt, wird SLAAC die IP nicht neu lernen, wenn sich das Gateway ändert oder wir die Netzwerksegmente ändern, selbst nach dem Neustart der SD-WAN-Appliance. Dies kann das Erhalten einer Adresse beim Verschieben von Ports verzögern.

  - Problemumgehung: Sie können manuell eine Release/Neuerlernung der SLAAC IP und Gateway IP über die Web-Benutzeroberfläche (oder die CLI) initiieren.

  [NSSDW-33807]

- Sobald SLAAC eine IP- und Gateway-Adresse von einem Router erfährt, lernt SLAAC das Gateway nicht neu, wenn sich das Gateway ändert (es sei denn und bis die aktuelle Adresse abläuft).

  Beispiel:

  - Die Zweigstelleneinheit lernt ihre IP und ihr Gateway von Gateway-1.
  - Der Netzwerkadministrator beschließt, Gateway-1 durch ein neues Gateway-2 zu ersetzen. Der Administrator konfiguriert Gateway-2 genauso wie Gateway-1, sodass Router-Advertisements die gleichen Präfixinformationen senden, die Gateway-1 gesendet hat. Gateway-2 hat jedoch eine andere Quelladresse als Gateway-1.
  - Die Zweigstellen-Appliance lernt nicht automatisch die IP von Gateway-2. (es sei denn und bis die aktuelle Adresse ein Timeout ist)

Problemumgehung: Sie können manuell eine Release/Neuerlernung der SLAAC IP- und Gateway-IP über die Web-Benutzeroberfläche (oder die CLI) initiieren

[NSSDW-33802]

- Ein Konfigurationsupdate kann dazu führen, dass der DHCP-Server, der auf der Präfix Delegation LAN Virtual Network Interface gehostet wird, nicht gestartet Beachten Sie, dass Prefix Delegation mit Citrix SD-WAN 11.3.1 Version nicht unterstützt wird.
  - Problemumgehung: Deaktivieren und aktivieren Sie den Citrix Virtual WAN-Dienst.

[NSSDW-33664]

- Die Aktivierung von Static NAT in einem Internet- oder Intranetdienst mit Proxy-NDP kann dazu führen, dass das SD-WAN auf NDP für Adressen reagiert, die anderen Hosts im Netzwerk gehören und von diesen verwendet werden.
  - Problemumgehung: Citrix empfiehlt Ihnen, Dynamic NAT anstelle von Static NAT mit Citrix SD-WAN 11.3.1 Release zu verwenden.

  [NSSDW-33653]

- Der Bandbreiten-Test zur Diagnose von Underlay-Sites wird in der Version Citrix SD-WAN 11.3.1 nicht unterstützt.

  [NSSDW-33597]

- 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 **Monitoring > PPPoE**).

  [NSSDW-25387]

Plattform und Systeme

- Wenn auf den folgenden Plattformen bei aktivierter HDX-Berichterstellung ein Parsing-Fehler auftritt, nachdem die Verbindung in HDX klassifiziert wurde und mit der Meldung von Statistiken beginnt, stürzt die Appliance bei einer neuen HDX-Verbindung ab:
  - Citrix SD-WAN 2100
  - Citrix SD-WAN 4100
  - Citrix SD-WAN 5100
  - Citrix SD-WAN 6100

[SDWANHELP-1882]

Versionshinweise für Citrix SD-WAN 11.3.2a Version

October 28, 2021

In diesem Dokument mit Versionshinweisen werden die Verbesserungen und Änderungen beschrieben, die für das Citrix SD-WAN Release Build 11.3.2a bestehen.

> **Hinweis**
>
> Citrix SD-WAN 11.3.2a-Version behebt die in https://support.citrix.com/article/CTX319135 beschriebenen Sicherheitslücken und ersetzt Citrix SD-WAN 11.3.2.

Neue Features

Die Erweiterungen und Änderungen, die in Build 11.3.2 verfügbar sind.

Netzwerk

Klassen

Citrix SD-WAN zeigt nur die Klassen an, bei denen der Datenverkehr auf virtuellen Pfaden und dynamischen virtuellen Pfaden fließt. Wenn eine Klasse angezeigt wird und **0** als Wert anzeigt, bedeutet dies, dass der zuvor fließende Verkehr jetzt gestoppt wurde. Wenn jedoch eine Klasse überhaupt nicht angezeigt wird, bedeutet dies, dass für diese Klasse nie ein Verkehrsfluss erfolgt ist, da der Status des virtuellen Pfaddienstes zurückgesetzt wurde (z. B. Softwareupgrade oder Neustart).

[NSSDW-33974]

Behobene Probleme

Die Probleme, die in Build 11.3.2 angesprochen werden.

Konfiguration und Management

Nach jedem Konfigurationsexport aus Citrix SD-WAN Center wurden die temporären Dateien im tmp-Ordner nicht bereinigt.

[SDWANHELP-2057]

Nach dem Hinzufügen einiger Netzwerkobjekte scheiterten die Konfigurationsüberwachung und der Export.

[SDWANHELP-2041]

Der Import einer großen Netzwerkkonfiguration von der Citrix SD-WAN Appliance in Citrix SD-WAN Center ist aufgrund von Beschränkungen der zulässigen Speicherressourcen fehlgeschlagen.

[SDWANHELP-2034]

Die E-Mail-Benachrichtigung von Citrix SD-WAN fügt dem **AUTH-Befehl** ein zusätzliches "CR"-Zeichen hinzu, wodurch die SMTP-Sitzung beendet wird.

[SDWANHELP-2028]

Wenn eine Appliance sowohl für die DHCP IPv4- als auch für die DHCP-IPv6-Adressen konfiguriert ist, das Netzwerk jedoch nur den DHCP IPv6-Server konfiguriert hat, wartet die Appliance weiterhin auf die DHCP-IPv4-Adresse und wird daher auch nicht mit der IPv6-Adresse zugewiesen.

[NSSDW-33741]

Eine WAN-Verbindung, die als DHCP-Client konfiguriert ist, führt zu einem Ausfall des virtuellen Pfads. Dieses Problem tritt auf, wenn der Name der WAN-Verbindung geändert und das Änderungsmanagement durchgeführt wird.

[NSSDW-32110]

Der Status des WAN-Linkpfads wird DEAD, wenn eine Citrix SD-WAN-Appliance einen neuen Port nicht erkennt.

[SDWANHELP-1998]

Installation und Upgrade

Wenn MPLS-WAN-Verbindungen für die Verwendung einer WAN-Link-Vorlage konfiguriert und für den Intranet-/Internetdienst aktiviert sind, tritt beim Kompilieren der Konfiguration ein unerwarteter Überwachungsfehler EC14203 auf.

Citrix SD-WAN 11.3.1 und ältere Versionen werfen möglicherweise keinen Fehler aus, wenn die zulässigen WAN-Verbindungsraten auf einen Wert festgelegt sind, der niedriger ist als die reservierte Mindestbandbreite, die für alle Dienste erforderlich ist, die die WAN-Verbindung verwenden, während MPLS WAN-Links mit WAN-Link-Vorlagen konfiguriert werden. Bei einem Upgrade auf Citrix SD-WAN 11.3.2 oder höher wird der Fehler angezeigt. Stellen Sie die korrekten zulässigen WAN-Verbindungsraten ein und aktivieren Sie die Konfiguration, bevor Sie das Upgrade durchführen.

[SDWANHELP-2134]

Sonstiges

Citrix SD-WAN Center GUI-Protokolle verbrauchen übermäßigen Speicherplatz, was zu einem Upgrade und einem STS-Fehler führt.

[SDWANHELP-1960]

Das Qualys-Sicherheitsscanner-Tool hat dazu geführt, dass einer der Dienste der Citrix SD-WAN-Appliance hohen Arbeitsspeicher verbraucht, was zu einer Reaktionsfähigkeit und einem Neustart der Appliance führte.

[SDWANHELP-1530]

Netzwerk

Nach dem Upgrade auf Citrix SD-WAN 11.3.1 schlägt das Klemmen von MSS (Maximum Segment Size) mit PPPoE fehl, wenn die Größe der Maximum Transmission Unit (MTU) auf 1492 Byte eingestellt ist.

[SDWANHELP-2048]

Häufige Änderungen an Routing-Tabellen an einer SD-WAN-Site zusammen mit der Konfigurationsupdate oder der Löschung dynamischer Routen können Probleme bei der Routensynchronisierung am Remotestandort verursachen.

[SDWANHELP-2043]

Wenn die In-Band-Verwaltung aktiviert ist und der RADIUS-Server über die Datenebene zugänglich ist, schlägt die Wi-Fi WPA2-Enterprise-Authentifizierung fehl.

[SDWANHELP-2032]

Anwendungsidentifikationsbezogene Einträge für Application Routing-, QoS- oder DNS-Funktionen werden regelmäßig zur Hash-Tabelle des First Packet Classifier (FPC) hinzugefügt. Wenn ein ausgehender Eintrag aus der Tabelle vertrieben wird, kann die Citrix SD-WAN Appliance manchmal abstürzen.

[SDWANHELP-1980]

Falls die Appliance über eine statische Route verfügt, die als Übersichtsroute konfiguriert ist, und eine andere Route mit demselben Präfix dynamisch erlernt wurde, fasst die Übersichtsroute keine Routen zusammen.

[NSSDW-34355]

Das Hinzufügen von Importfiltern zum Entfernen zuvor importierter OSPF/BGP-Routen kann zum Absturz von Diensten führen.

[NSSDW-34207]

Sobald SLAAC eine IP- und Gateway-Adresse von einem Router erfährt, wird SLAAC die IP nicht neu lernen, wenn sich das Gateway ändert oder wir die Netzwerksegmente ändern, selbst nach dem

Neustart der SD-WAN-Appliance. Dies kann das Erhalten einer Adresse beim Verschieben von Ports verzögern.

[NSSDW-33807]

Sobald SLAAC eine IP- und Gateway-Adresse von einem Router erfährt, lernt SLAAC das Gateway nicht neu, wenn sich das Gateway ändert (es sei denn und bis die aktuelle Adresse abläuft).

Beispiel:

- Die Zweigstelleneinheit lernt ihre IP und ihr Gateway von Gateway-1.
- Der Netzwerkadministrator beschließt, Gateway-1 durch ein neues Gateway-2 zu ersetzen. Der Administrator konfiguriert Gateway-2 genauso wie Gateway-1, sodass Router-Advertisements die gleichen Präfixinformationen senden, die Gateway-1 gesendet hat. Gateway-2 hat jedoch eine andere Quelladresse als Gateway-1.
- Die Zweigstellen-Appliance lernt nicht automatisch die IP von Gateway-2. (es sei denn und bis die aktuelle Adresse ein Timeout ist)

[NSSDW-33802]

Ein Konfigurationsupdate kann dazu führen, dass der DHCP-Server, der auf der Präfix Delegation LAN Virtual Network Interface gehostet wird, nicht gestartet Präfixdelegierung wird mit Citrix SD-WAN 11.3.1 Version nicht unterstützt.

[NSSDW-33664]

Die Aktivierung von Static NAT in einem Internet- oder Intranetdienst mit Proxy-NDP kann dazu führen, dass das SD-WAN auf NDP für Adressen reagiert, die anderen Hosts im Netzwerk gehören und von diesen verwendet werden.

[NSSDW-33653]

Der Bandbreiten-Test zur Diagnose von Underlay-Sites wird in der Version Citrix SD-WAN 11.3.1 nicht unterstützt.

[NSSDW-33597]

Plattform und Systeme

Der Citrix Virtual WAN-Dienst wird möglicherweise neu gestartet, wenn das STS-Bundle generiert wird, während die dynamischen virtuellen Pfade (DVPs) aktiviert sind.

[SDWANHELP-2123]

Im Abschnitt **Systemstatus** im Dashboard der Legacy-Benutzeroberfläche wird die Fehlermeldung "**Systemdaten konnten nicht abgerufen werden, da das System ausgelastet ist**"angezeigt. **Klicken Sie auf Aktualisieren, um es erneut zu versuchen.** Dieses Problem tritt auf, wenn Site-Namen die Zeichenfolge "**Fertig** "enthalten.

[SDWANHELP-2098]

Eine Überprüfung der Filterrichtlinienregel wird während des Konfigurationsupdates durchgeführt, um zwischen neu erstellten und geänderten Regeln zu unterscheiden. Aufgrund einer fehlenden Vergleichsüberprüfung für `match\\_type`werden die meisten Verbindungen zum Internet von der Firewall blockiert `0\\_DENIED`

Die Problemumgehung besteht darin, die Standardregel von `Reject` auf `Drop` zu ändern.

[SDWANHELP-2078]

Wenn Echtzeitstatistiken für Anwendungsrouten entweder vom SD-WAN Orchestrator oder vom SD-WAN Branch-Gerät abgerufen werden, verliert das Gerät die Konnektivität und es wird ein Absturz beobachtet. Dies geschieht nur, wenn die Anzahl der Anwendungsrouten mehr als 16 beträgt (einschließlich automatisch generierter Anwendungsrouten).

[SDWANHELP-2066]

Wenn die HDX-Berichterstellung aktiviert ist und iHDX-Datenverkehr über die Citrix SD-WAN-Appliance läuft, beobachtet die Citrix SD-WAN-Appliance gelegentlich den Core-Dump.

[SDWANHELP-1957]

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-1739]

SD-WAN 210-Einheit

Einige Carrier erlauben nur IPv6-Datensitzungen, wenn das Packet Data Protocol (PDP) für IPv4 und (oder) IPv6 aktiviert ist.

[SDWANHELP-1777]

Bekannte Probleme

Die Probleme, die in Version 11.3.2 bestehen.

Konfiguration und Management

Eine benutzerdefinierte Domainnamen-basierte benutzerdefinierte Anwendungsregel konnte nicht erstellt werden. Die Option ist in der Benutzeroberfläche ausgegraut.

[SDWANHELP-2136]

Hochverfügbarkeits-Failover kann beim Generieren von STS mit Citrix SD-WAN 2100-Plattform auftreten, die im Hochverfügbarkeitsmodus bereitgestellt wird.

[SDWANHELP-2049]

E-Mail-Benachrichtigungen können nicht gesendet werden, wenn der SMTP-Servername als FQDN festgelegt ist. Dieses Problem tritt auf, wenn der DNS-Server Folgendes enthält:

- Mindestens 2 IPv4 A-Datensätze für den FQDN.
- Mindestens 1 IPv6 AAAA-Record für den FQDN.

[SDWANHELP-2027]

Wenn Out-of-Band-Verwaltungsschnittstellen verbunden sind, kann die DNS-Einstellung nur über die Benutzeroberfläche der Appliance aktualisiert werden.

Wenn die In-Band-Verwaltung konfiguriert ist, werden die mit der Benutzeroberfläche der Appliance aktualisierten DNS-Einstellungen nicht wirksam. Sie können die DNS-Einstellungen nur über die Benutzeroberfläche des Citrix SD-WAN Orchestrator-Dienstes aktualisieren.

[NSSDW-33932]

Citrix SD-WAN UI zeigt einen Fehler an, wenn ein doppelter Name für DNS Proxy im Netzwerk verwendet wird.

Problemumgehung: Verwenden Sie einen eindeutigen netzwerkweiten Namen für DNS-Proxy.

[NSSDW-33842]

Das Aktivieren und Deaktivieren eines externen Modems funktioniert nicht über die Legacy-Benutzeroberfläche.

Problemumgehung: Verwenden Sie die SD-WAN Virtual WAN CLI, um ein externes Modem zu aktivieren/deaktivieren

[NSSDW-32221]

Wenn der Benutzer den Status des internen Modems einsehen möchte, zeigt die Legacy-Benutzeroberfläche auch den Status des externen Modems an.

[NSSDW-32219]

Der Orchestrator-UI- und Konfigurations-Compiler fängt den zulässigen Bereich des DHCP-Lease-Intervalls nicht ab, was dazu führt, dass der DHCP-Daemon fehlschlägt.

[NSSDW-25452]

Sonstiges

Beim Klonen einer Site mit mehr als einer HA-Schnittstelle wird die zweite IP-Adresse der HA-Schnittstelle nicht geklont.

[SDWANHELP-2005]

Netzwerk

Das Aktualisieren der DNS-Einstellungen auf der Citrix SD-WAN 110 SE-Appliance mit einer statischen Verwaltungs-IP schlägt auf der neuen Benutzeroberfläche fehl, funktioniert jedoch auf der älteren Benutzeroberfläche.

[NSSDW-35639]

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-25387]

SD-WAN 210-Einheit

210 LTE-Modems starten kontinuierlich neu, wenn die Firmware auf **AUTO-SIM** eingestellt ist und sich die Firmware der Modems nicht im richtigen Zustand befindet.

Problemumgehung: Nehmen Sie die SIM-Karte heraus, wählen Sie eine geeignete Firmware für die SIM-Karte aus und legen Sie die SIM-Karte wieder ein.

[SDWANHELP-2080]

Neue Benutzeroberfläche für SD-WAN-Appliances

October 28, 2021

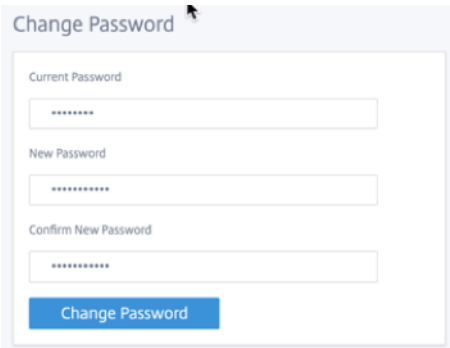
Eine neue Benutzeroberfläche (UI) wird für SD-WAN-Appliances eingeführt. Die neue Benutzeroberfläche wird mit den neuesten UI-Technologien erstellt. Das neue UI-Design verbessert die Sicherheit, hat ein verbessertes Aussehen und Gefühl, es ist leistungsfähiger, sicherer und reaktionsschneller. Die neue 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
Citrix SD-WAN 410 SE	11.3.0 weiter
Citrix SD-WAN SE VPX	11.3.0 weiter

Hinweis

- Durch die Provisioning des Citrix SD-WAN 210-SE, 410 SE oder VPX SE als MCN werden Sie auf die 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:

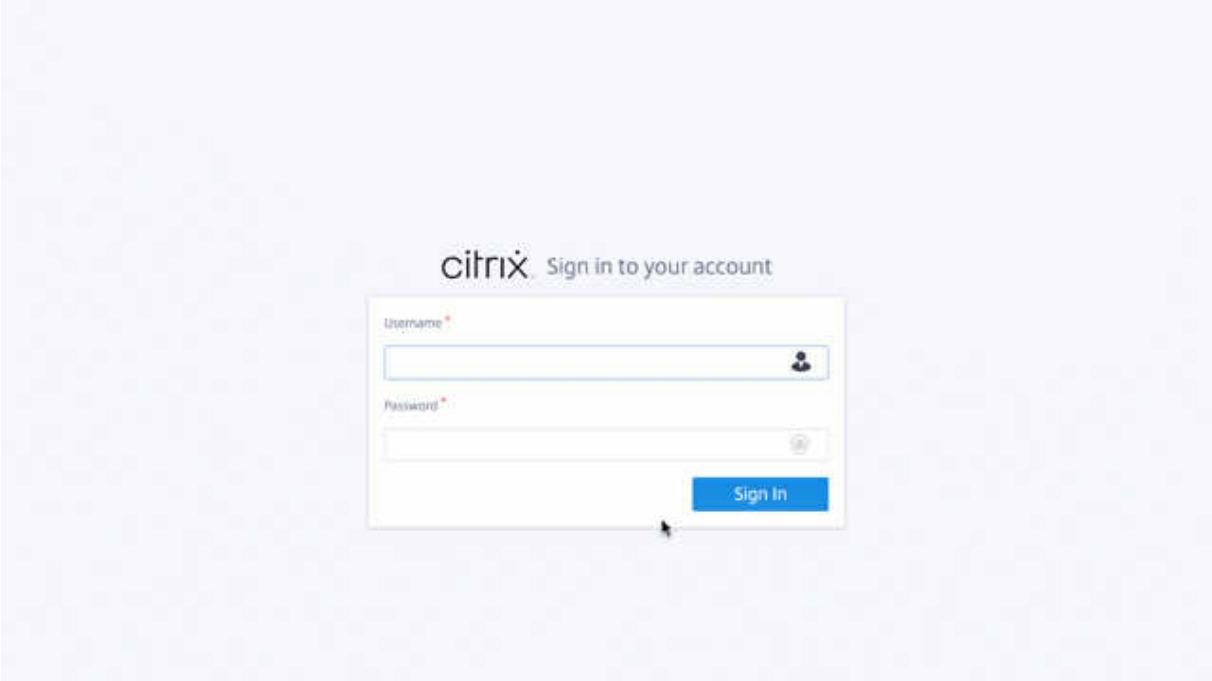
1. Öffnen Sie einen neuen Browser-Tab und navigieren Sie zu **https://** < management-ip >, um auf die neue Benutzeroberfläche der SD-WAN-Appliance zuzugreifen. Wenn Sie auf eine IPv6-Adresse zugreifen, geben Sie ein `https://<[IPv6 address]>`.

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

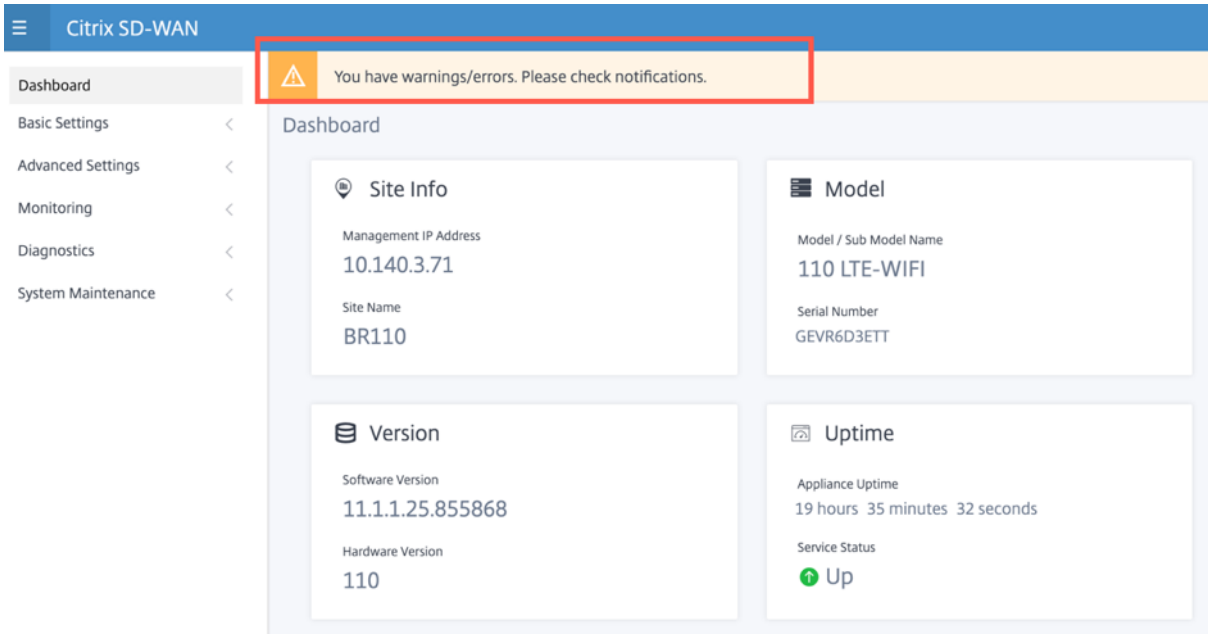
> **Hinweis**
>
> In dem Szenario, in dem das In-Band-Management aktiviert ist, kann die IP-Adresse der Schnittstelle bereitgestellt werden, **< management-ip >** um auf die neue Benutzeroberfläche zuzugreifen. Die In-Band-Verwaltung kann auf mehreren vertrauenswürdigen Schnittstellen aktiviert werden, 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.

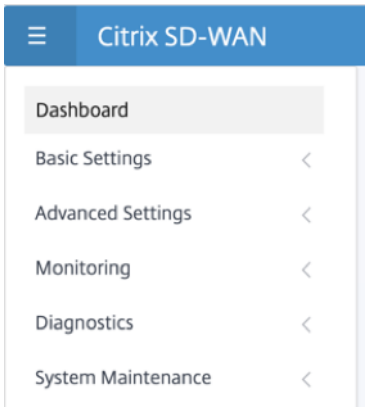


Sobald Sie sich erfolgreich angemeldet haben, sehen Sie, dass sich das Navigationsfeld auf der linken Seite befindet. Außerdem können Sie ein Benachrichtigungsbanner auf dem Dashboard sehen, wenn Warnungen oder Fehler vorliegen.



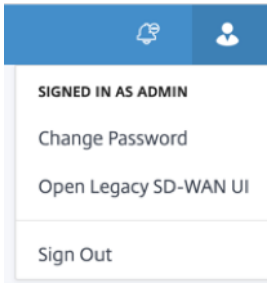
Navigation

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

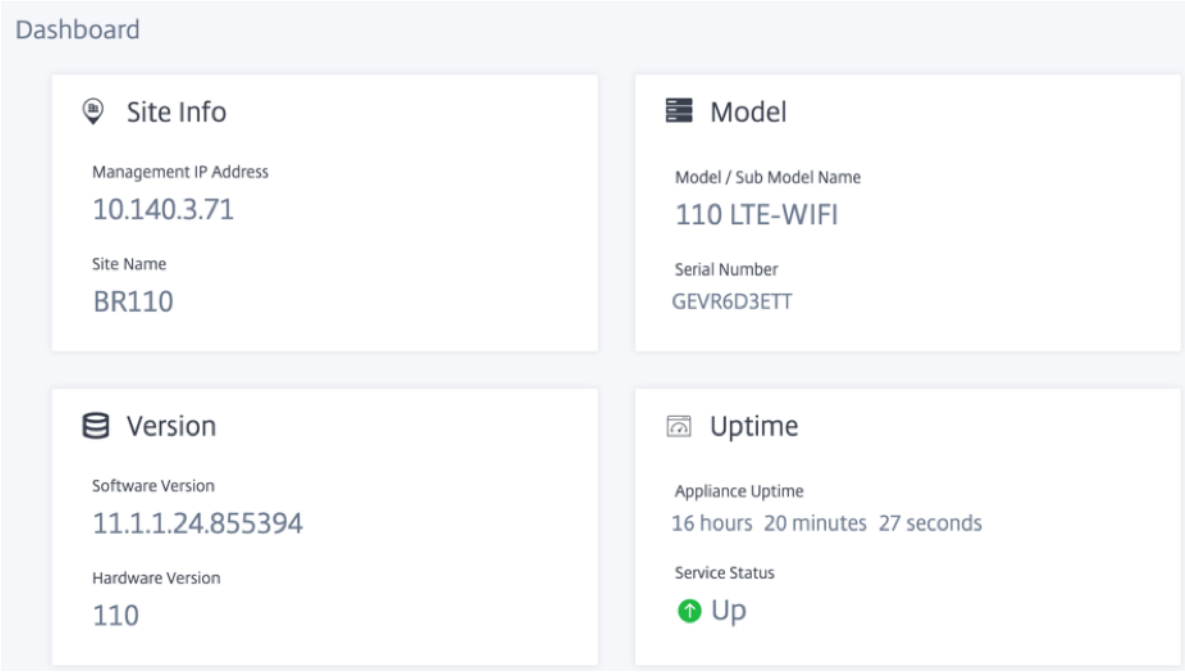
Das Benutzermenü in der oberen rechten Ecke zeigt die angemeldeten Benutzerdetails an. Sie können die Legacy-Benutzeroberfläche in einer neuen Browserregisterkarte **öffnen, indem Sie auf die Option Legacy SD-WAN UI** öffnen klicken. Klicken Sie auf das Glockensymbol für Benachrichtigungen.



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-/Untermodellnamen** und die **Seriennummer an**
- **Version** —Zeigt **Software-** und **Hardwareversion** an
- **Betriebszeit** - Zeigt **Appliance-Betriebszeit**, **Citrix Virtual WAN Service-Status und Status** der **Orchestrator-Konnektivität**an.
- **Hohe Verfügbarkeit** - Zeigt den HA-Status der lokalen und Peer-Appliance sowie die letzte erhaltene Zeit für HA-Updates an.
- **Metered Links** —Zeigt die Nutzungs- und Rechnungsdetails für Links an, auf denen die Messung aktiviert ist.



Grundeinstellungen

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

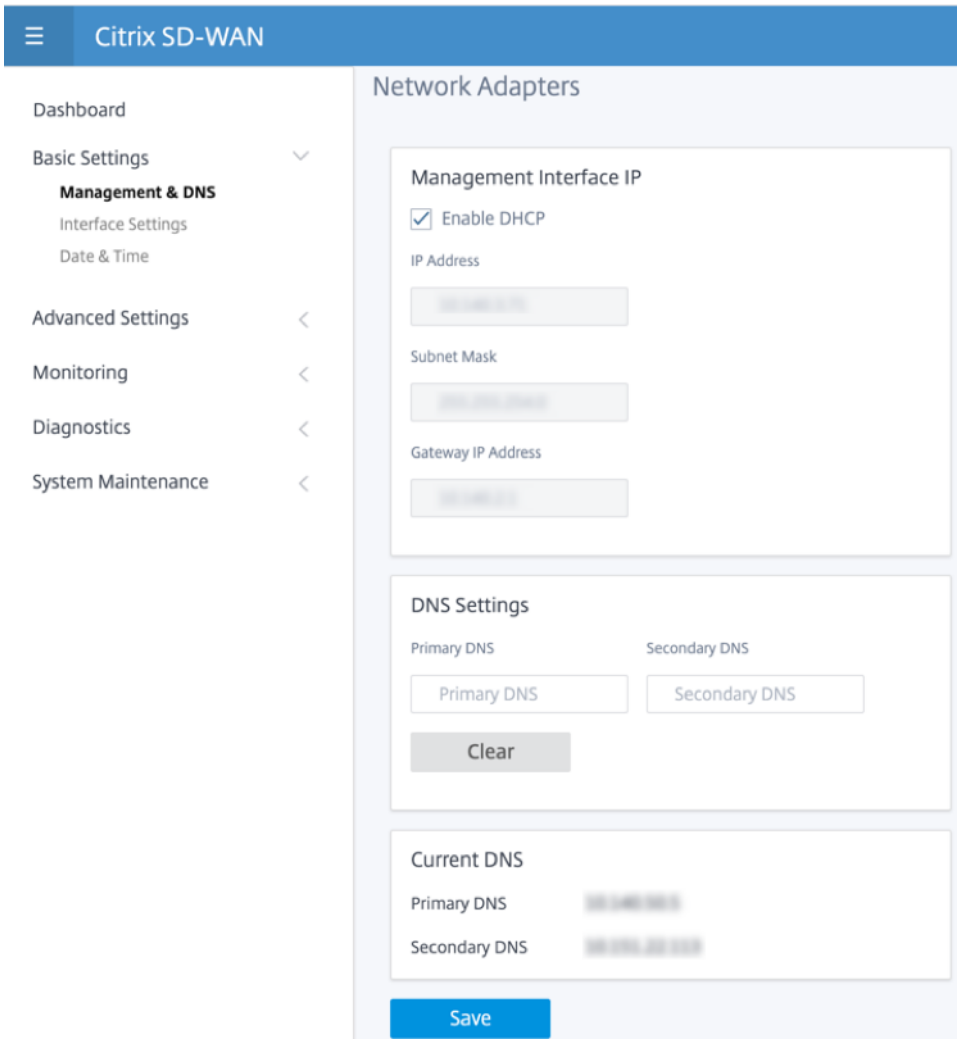
- Verwaltung und DNS
- Interface-Einstellungen
- Datum/Uhrzeit
- RADIUS-Server
- TACACS+ Server

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.

Die Zulassungsliste für die Verwaltungsoberfläche ist eine genehmigte Liste von IP-Adressen oder IP-Domains, die berechtigt sind, auf Ihre Verwaltungsschnittstelle zuzugreifen. Eine leere Liste ermöglicht den Zugriff auf Management Interface von allen Netzwerken aus. Sie können IP-Adressen hinzufügen, um sicherzustellen, dass die Verwaltungs-IP-Adresse nur für die vertrauenswürdigen Netzwerke zugänglich ist.

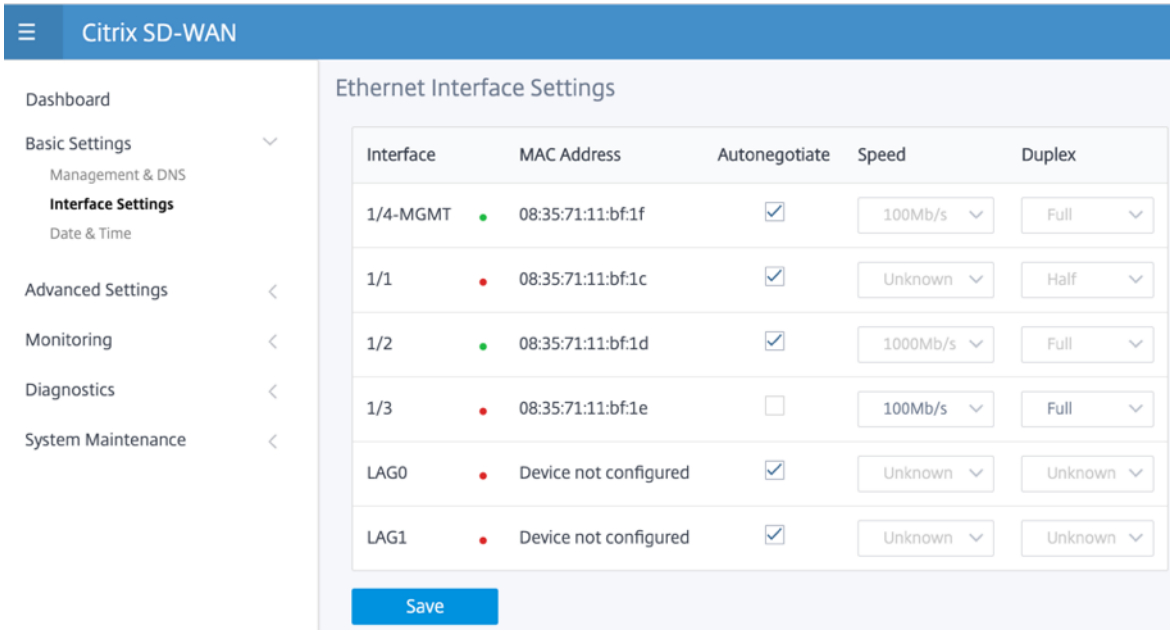
Um eine IPv4-Adresse zur zulässigen Liste hinzuzufügen oder zu entfernen, müssen Sie nur mit einer IPv4-Adresse auf die Verwaltungsschnittstelle der SD-WAN-Appliance zugreifen. Um eine IPv6-Adresse zur zulässigen Liste hinzuzufügen oder zu entfernen, müssen Sie auf die Verwaltungsschnittstelle der SD-WAN-Appliance nur mit einer IPv6-Adresse zugreifen



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**.

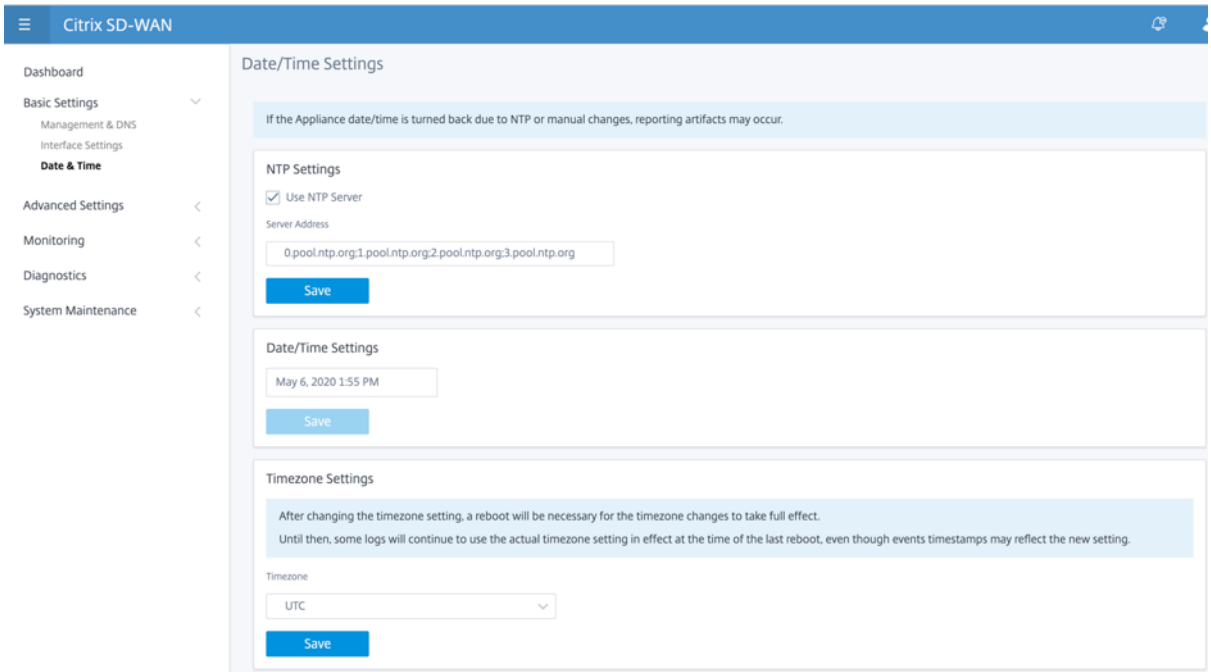
Interface-Einstellungen

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.



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.



RADIUS-Server

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

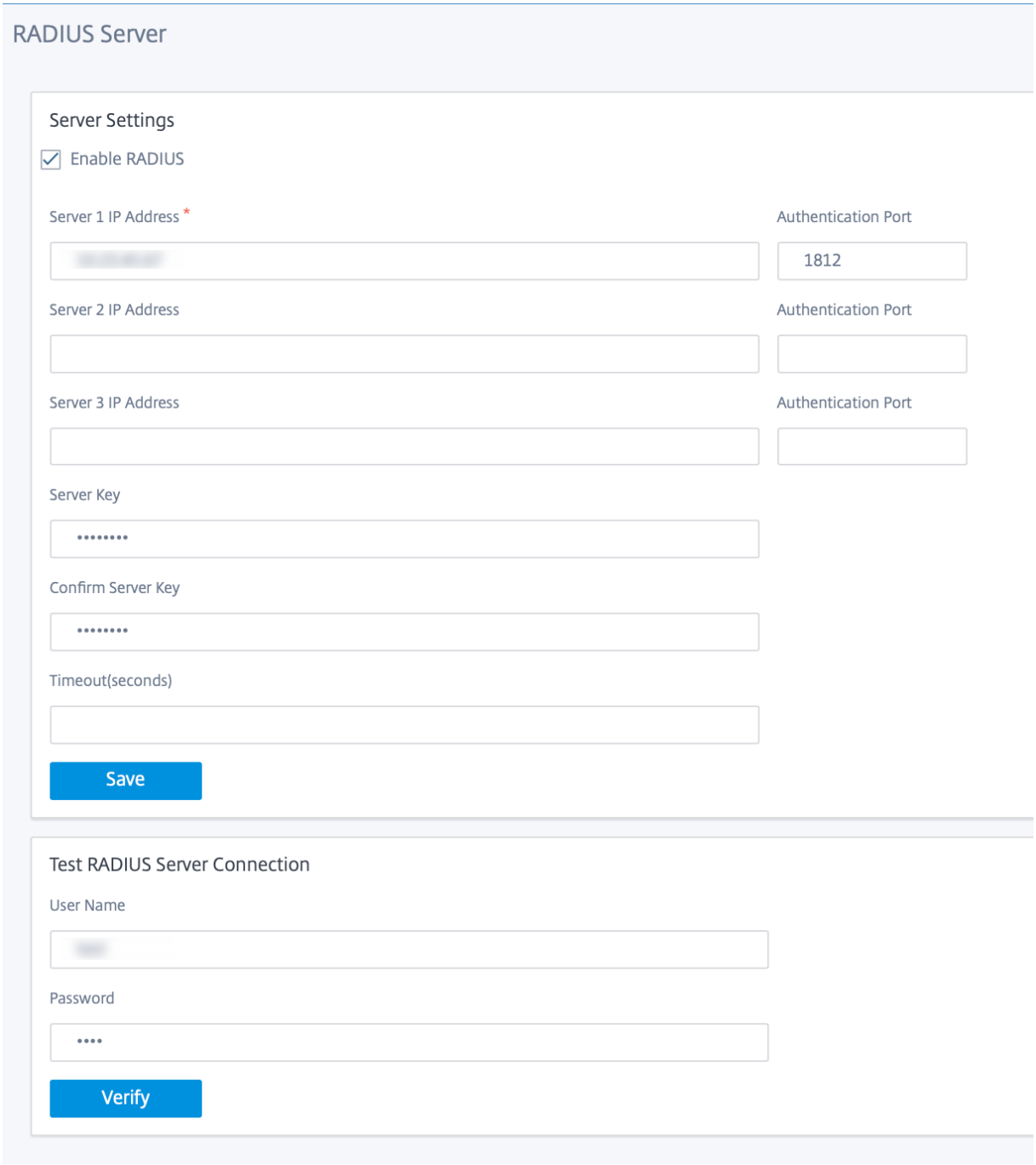
So konfigurieren Sie den RADIUS-Server:

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.

   > **HINWEIS**
   >
   > Um eine IPv6-Adresse zu konfigurieren, stellen Sie sicher, dass der RADIUS-Server auch mit einer IPv6-Adresse konfiguriert ist.

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**.



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.

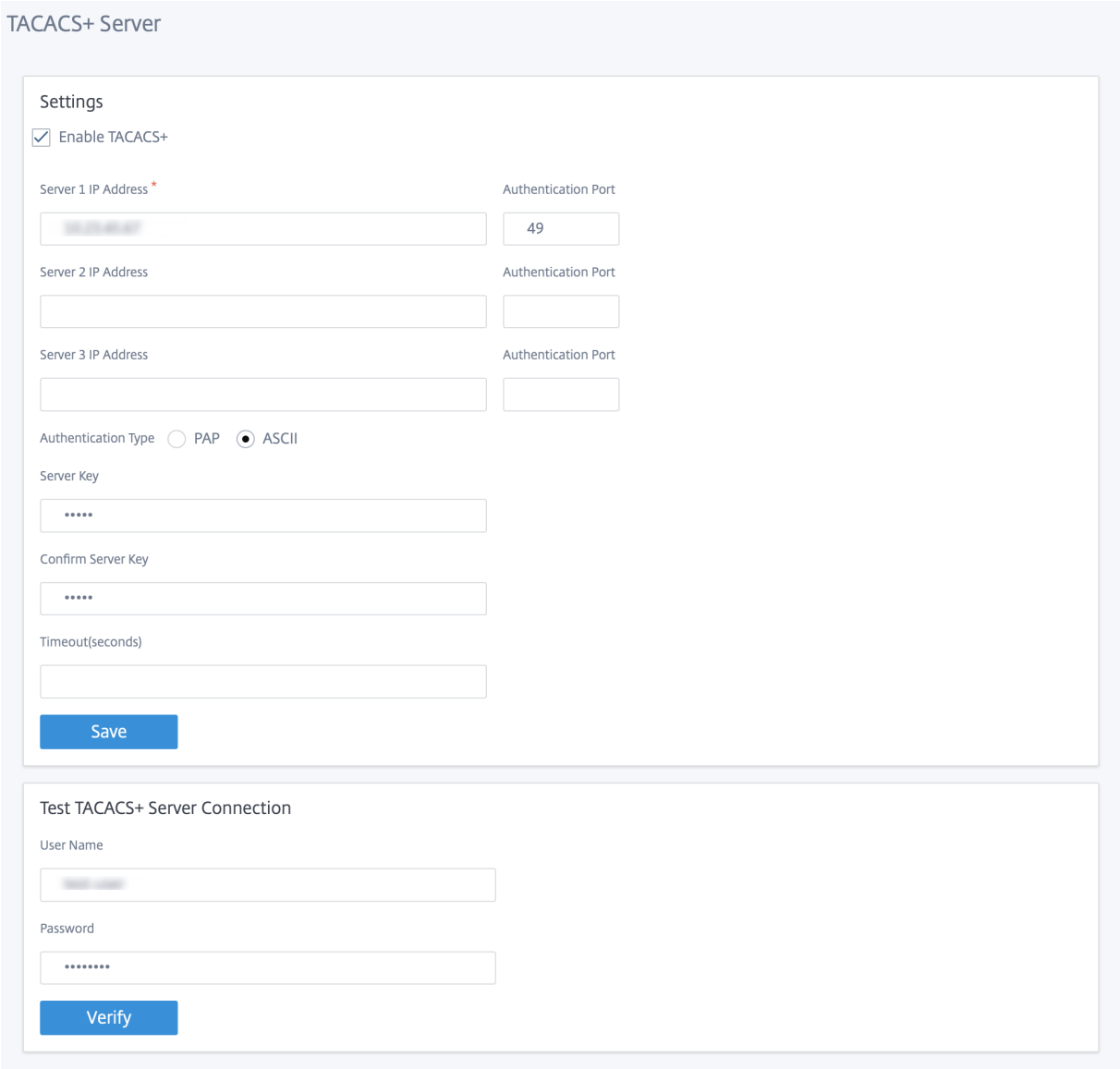
So konfigurieren Sie den TACACS+-Server:

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.

   > **HINWEIS**
   >
   > Um eine IPv6-Adresse zu konfigurieren, stellen Sie sicher, dass der TACACS+-Server auch mit einer IPv6-Adresse konfiguriert ist.

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**.



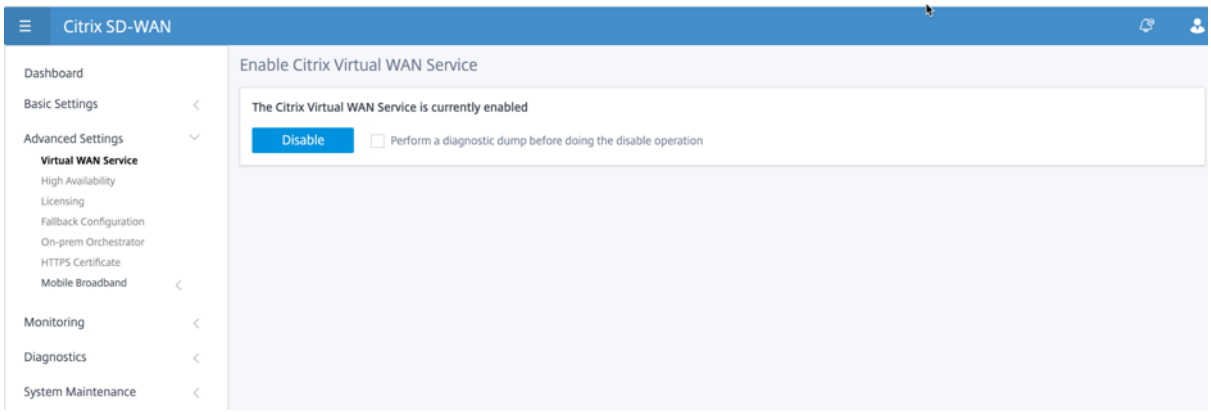
Erweiterte Einstellungen

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

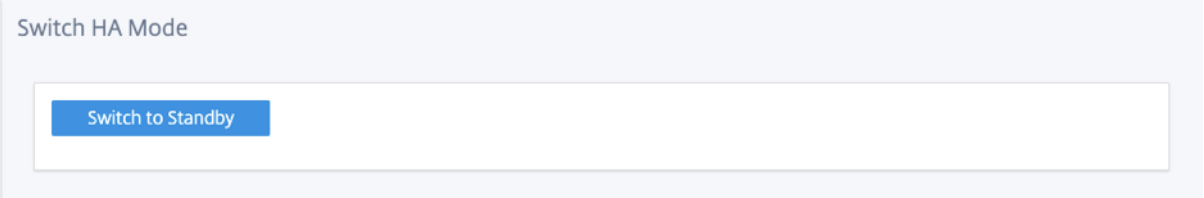
Citrix Virtual WAN-Dienst

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.



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.

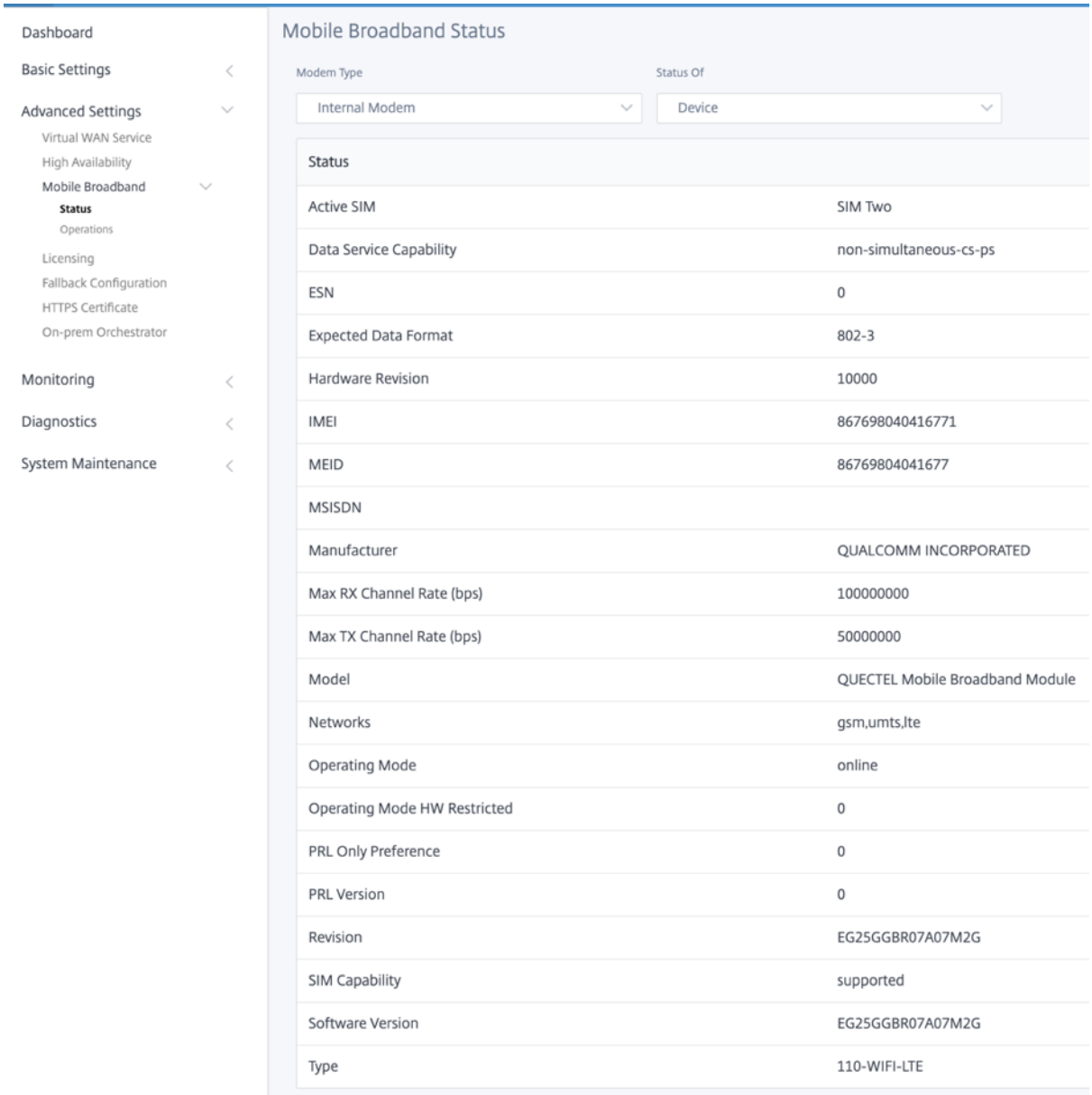
Perquisites für externes LTE-Modem:

- 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.



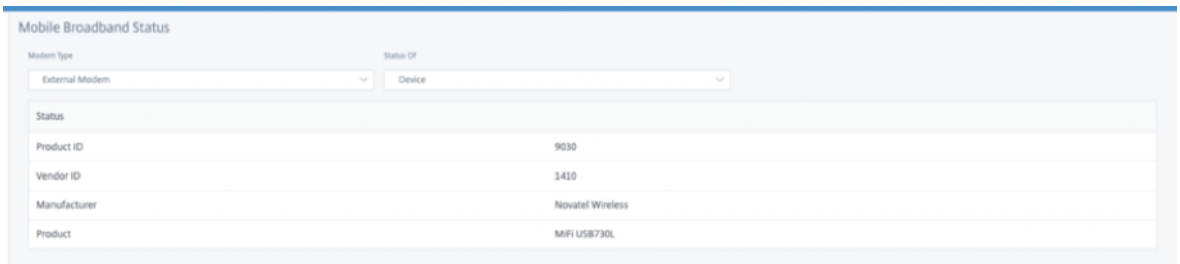
Im Folgenden finden Sie einige nützliche Statusinformationen:

- **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.



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

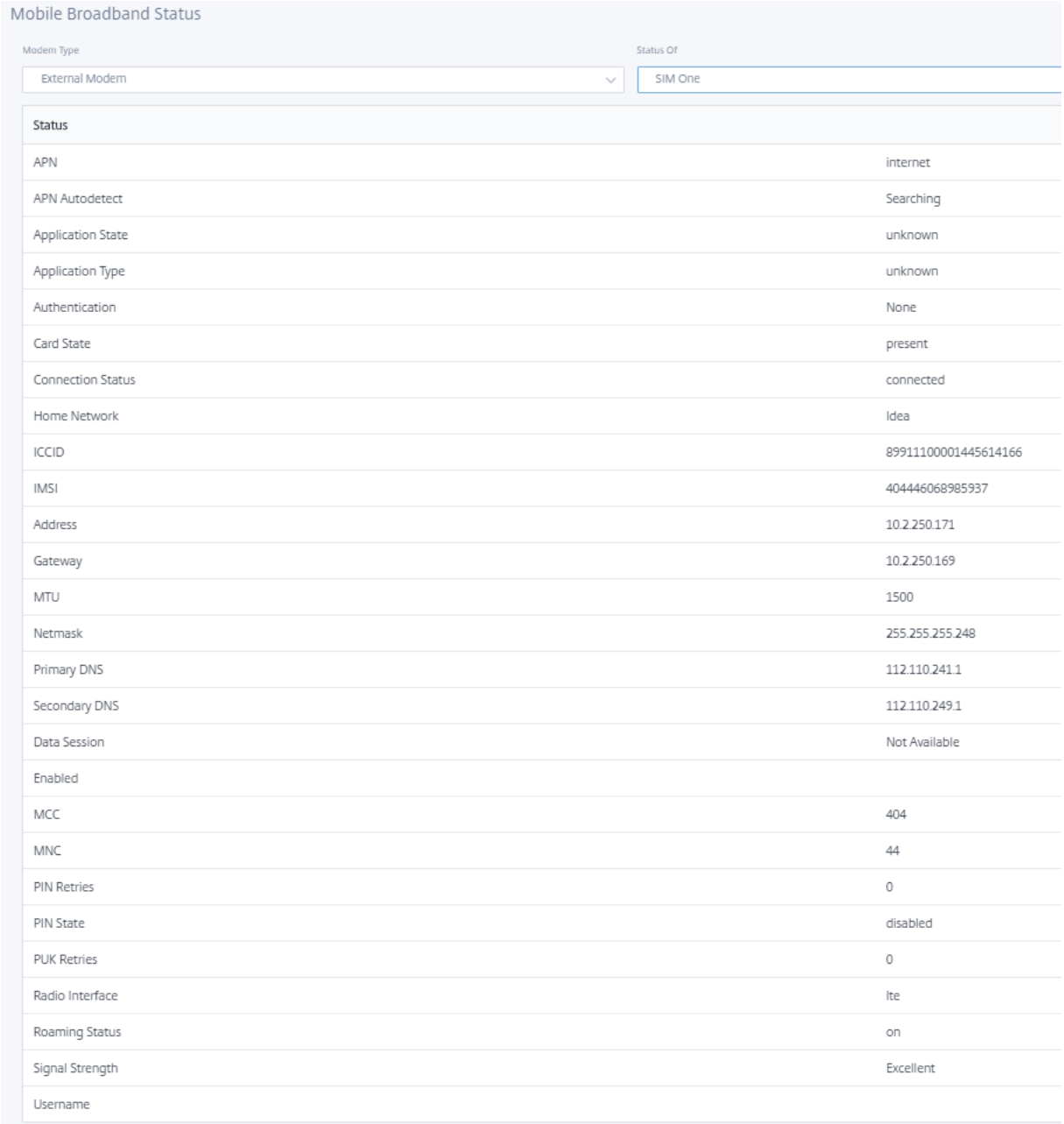
Mobile Broadband Status

Modem Type: External Modem

Status Of: 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.



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

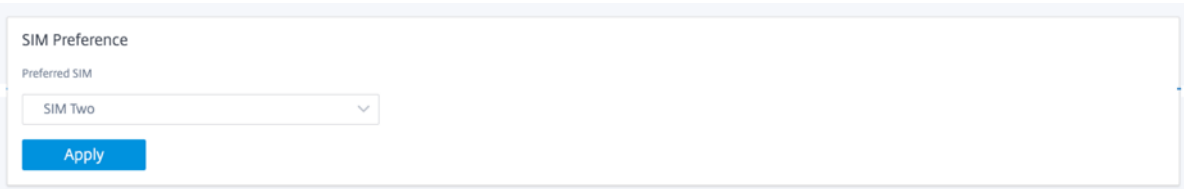
Vorgänge	Internes Modem	Externes Modem - CDC Ethernet	Externes Modem - MBIM und NCM
SIM-Präferenz	Ja - Für Geräte, die Dual-SIM unterstützen	Nein	Nein
SIM-PIN	Ja	Nein	Nein
APN-Einstellungen	Ja	Nein	Ja

Vorgänge	Internes Modem	Externes Modem - CDC Ethernet	Externes Modem - MBIM und NCM
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.

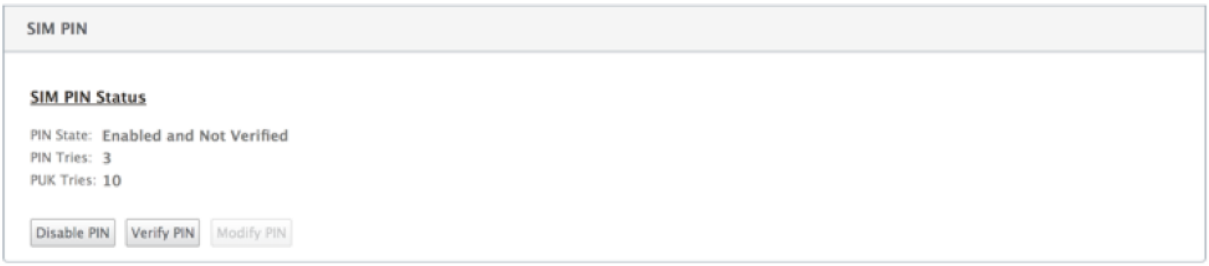
> **Hinweis**
>
> Die Option SIM-Einstellung ist für das Citrix SD-WAN 210-SE LTE Wi-Fi-Gerät nicht verfügbar, da es nur einen SIM-Kartensteckplatz hat.



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**.



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 Mobilfunkanbieters erhaltenen SIM-PUK zurücksetzen. Um die Blockierung einer SIM aufzuheben, klicken Sie auf **Sperre aufheben**. Geben Sie die vom Mobilfunkanbieter 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 Mobilfunkanbieter, um eine neue SIM-

> Karte zu erhalten.

APN-Einstellungen

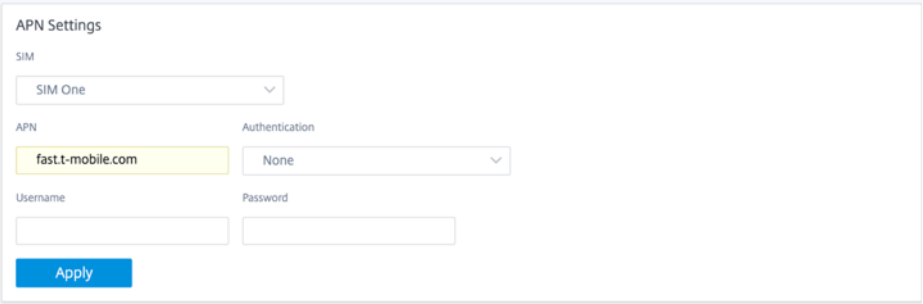
1. Um die APN-Einstellungen zu konfigurieren, navigieren Sie zu **Erweiterte Einstellungen > Mobiles Breitband > Operationen** und gehen Sie zum Abschnitt **APN-Einstellungen**.

   > **Hinweis**
   >
   > Rufen Sie die APN-Informationen vom Mobilfunkanbieter ab.

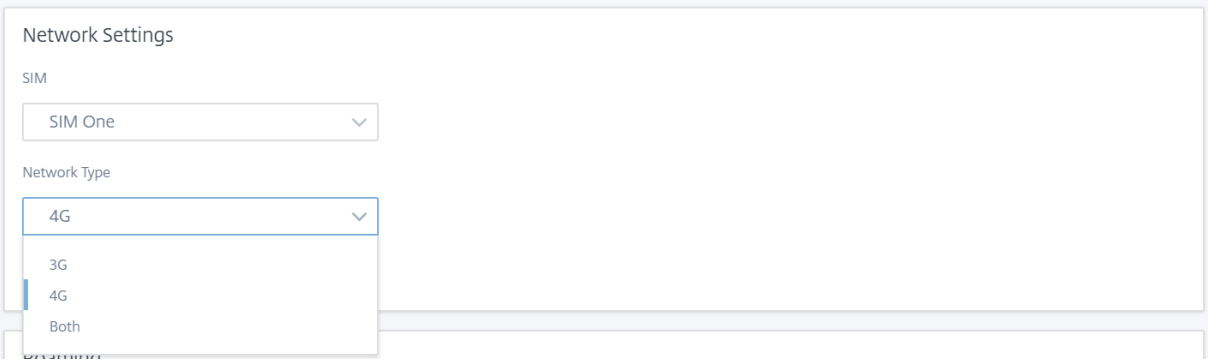
2. Wählen Sie die SIM-Karte aus und geben Sie den **APN, den Benutzernamen, das Kennwort** und die vom Mobilfunkanbieter bereitgestellte **Authentifizierung** ein. Sie können zwischen PAP, CHAP, PAPCHAP Authentifizierungsprotokollen wählen. Wenn der Anbieter keinen Authentifizierungstyp angegeben hat,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

   > **Hinweis**
   >
   > Alle diese Felder sind optional.

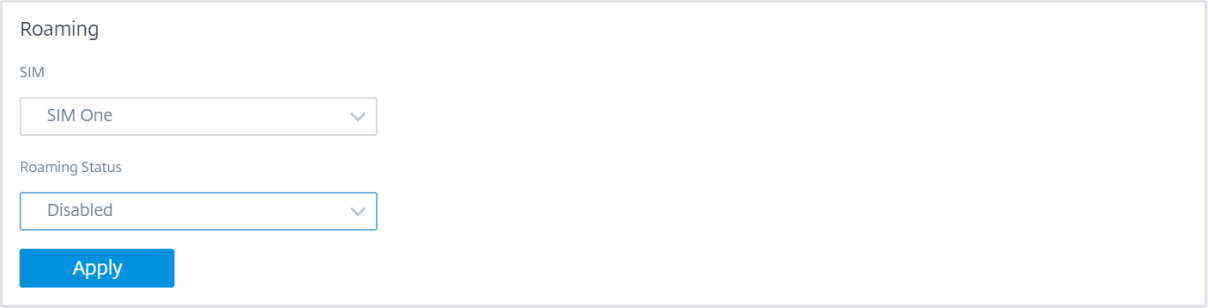
3. Klicken Sie auf **Apply**.



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.



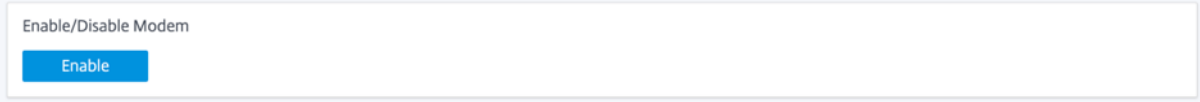
Roaming Die Roaming-Option ist standardmäßig auf Ihren LTE-Appliances aktiviert. Sie können sie deaktivieren.



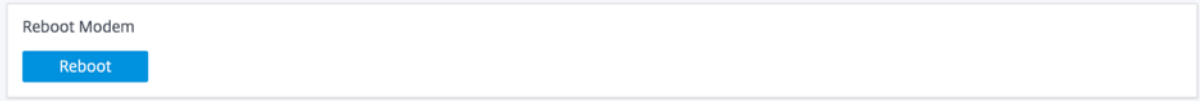
Firmware verwalten

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.

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

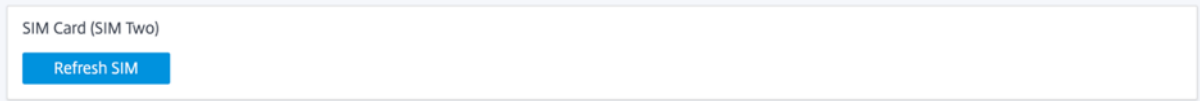


Modem neu starten Startet das Modem neu. Es kann bis zu 7 Minuten dauern, bis der Neustartvorgang abgeschlossen ist.



SIM aktualisieren Verwenden Sie 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.



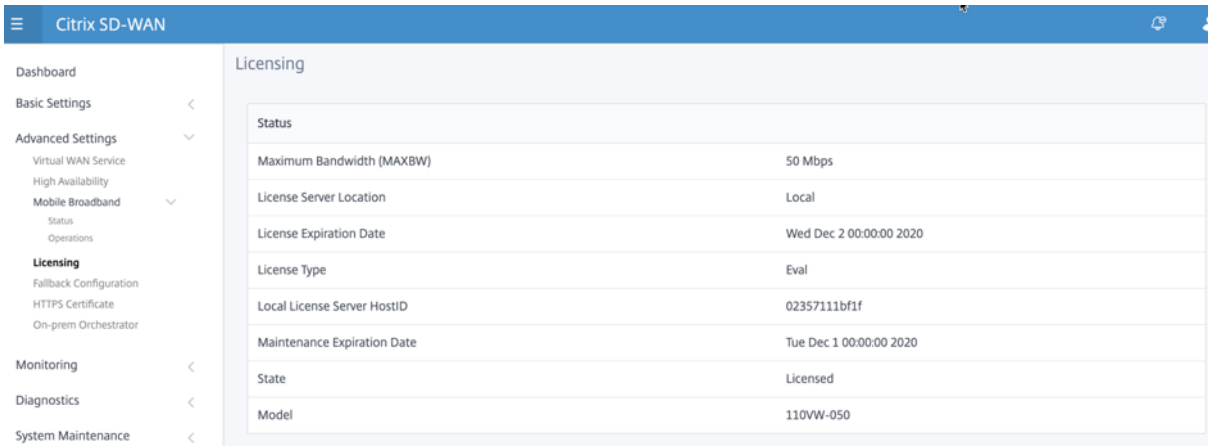
Mit dem Citrix SD-WAN Center können Sie alle LTE-Sites in Ihrem Netzwerk remote anzeigen und verwalten. Weitere Informationen finden Sie unter Remote-LTE-Standortverwaltung.

Weitere Informationen zur LTE-Konfiguration finden Sie unter Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Geräten und Konfigurieren der LTE-Funktionalitätauf 210 SE LTE-Geräten.

Informationen zur Konfiguration eines externen LTE-Modems finden Sie unter Konfigurieren eines externen USB-LTE-Modems.

Lizenzierung

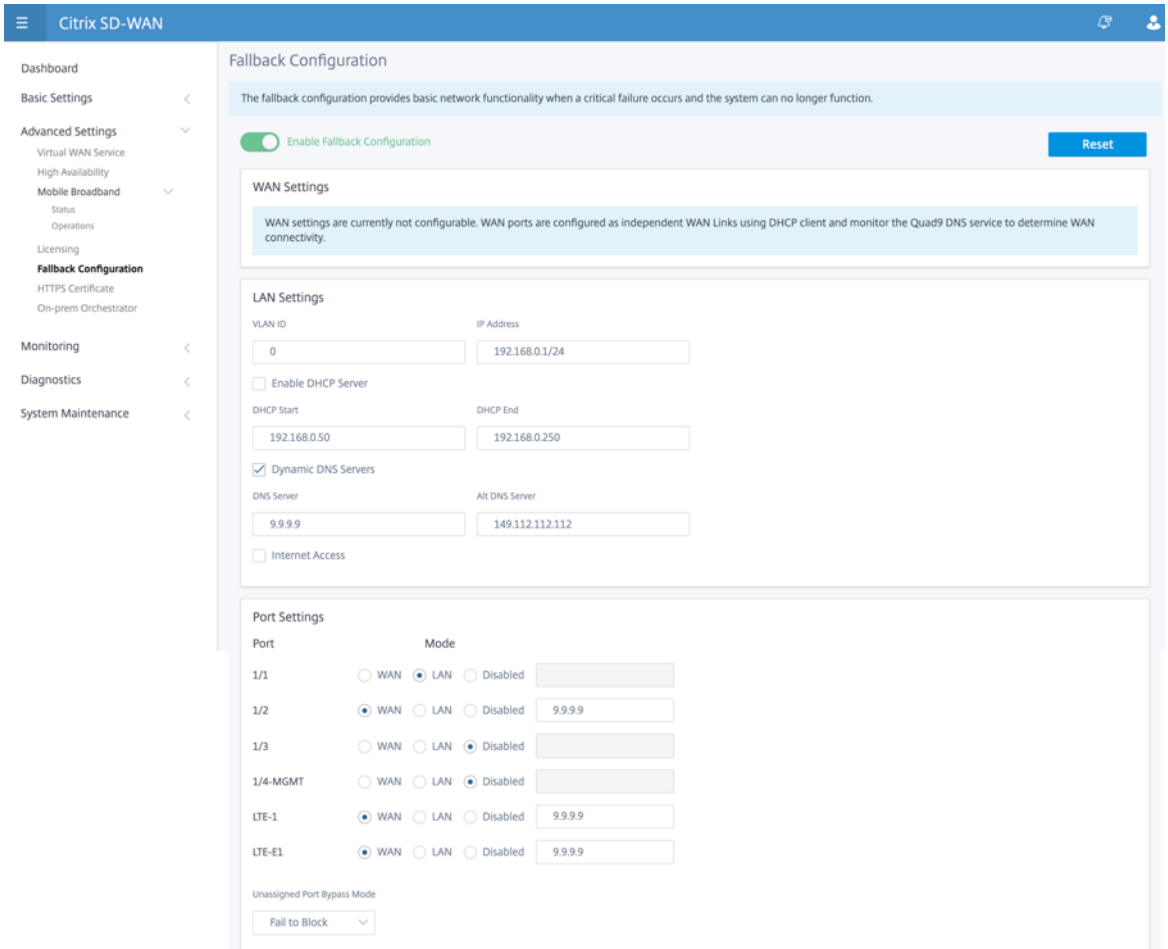
Auf der Seite "**Lizenzierung** "werden die Lizenzdetails wie Serverstandort, Modell, Lizenztyp usw. angezeigt.



> **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.

Default-/Fallback-Konfiguration

Auf der Seite "**Standard-/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**.

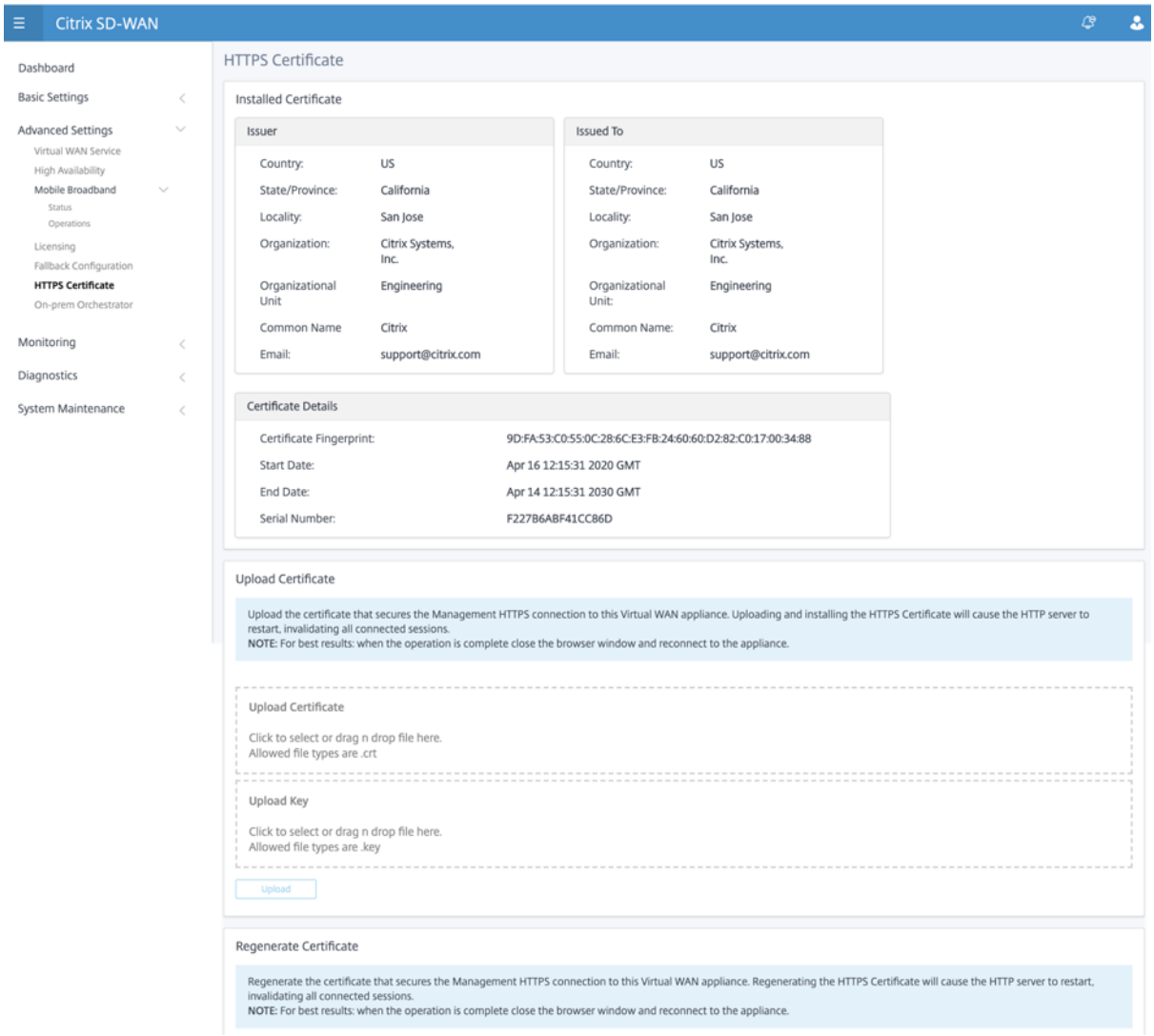


> **Hinweis**
>
> LTE-Schnittstellen können nicht mit einer statischen IP-Adresse konfiguriert werden.

Weitere Informationen finden Sie unter Standard-/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 Informationen finden Sie unter HTTPS-Zertifikate.



On-Prem Orchestrator

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.

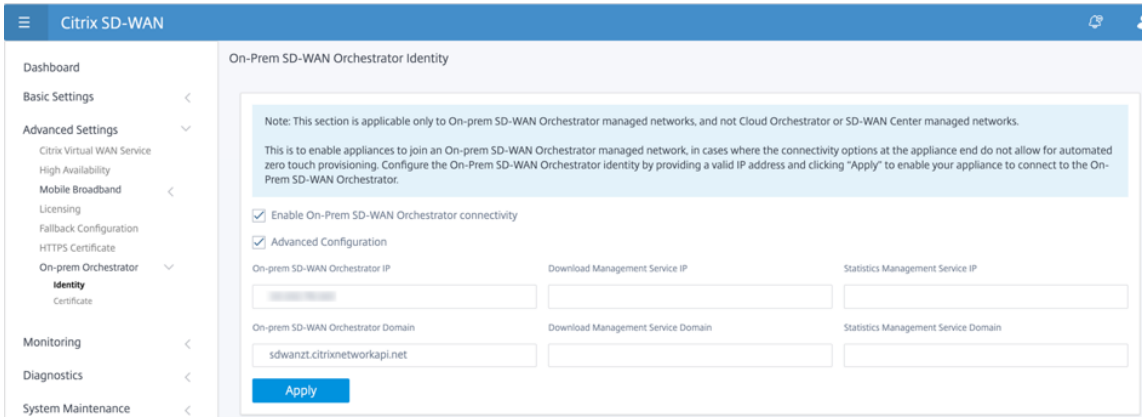
Sie können eine Verbindung zwischen der Citrix SD-WAN Appliance und dem Citrix On-Prem SD-WAN Orchestrator herstellen, indem Sie die Orchestrator-Konnektivität aktivieren und die On-Prem SD-WAN Orchestrator-Identität angeben.

> **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.comkonfiguriert 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 Statis-

tics 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/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. 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.

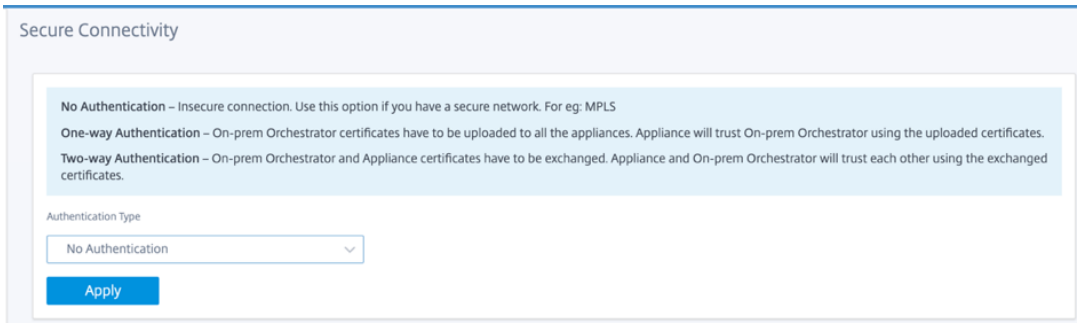
   Wenn der On-prem **Orchestrator-Authentifizierungstyp** aktiviert ist, kann sich die Appliance nur über die **Zwei-Wege-Authentifizierung**mit dem On-prem Orchestrator verbinden.

   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.

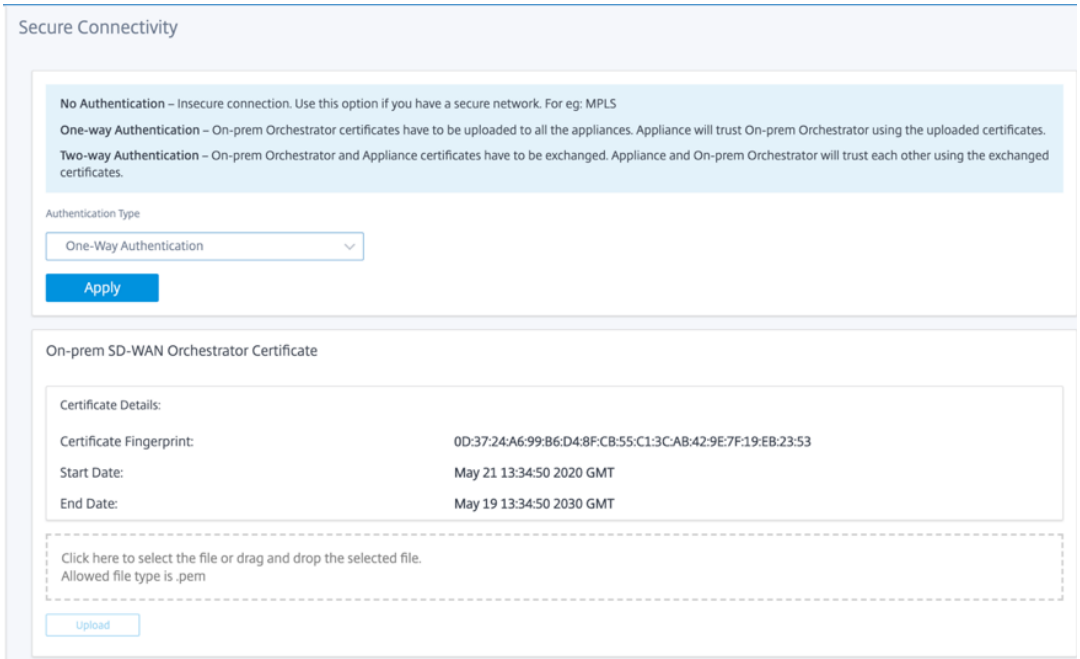
> **Hinweis**
>
> - Generierte Zertifikate sind selbstsignierte X509-Zertifikate.
> - Der Kunde muss die Zertifikate neu generieren, wenn das Zertifikat abgelaufen oder gefährdet ist.
> - Die Gültigkeit des Zertifikats beträgt 10 Jahre.
> - Sie können die Zertifikatdetails wie Fingerabdruck, Startdatum 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:

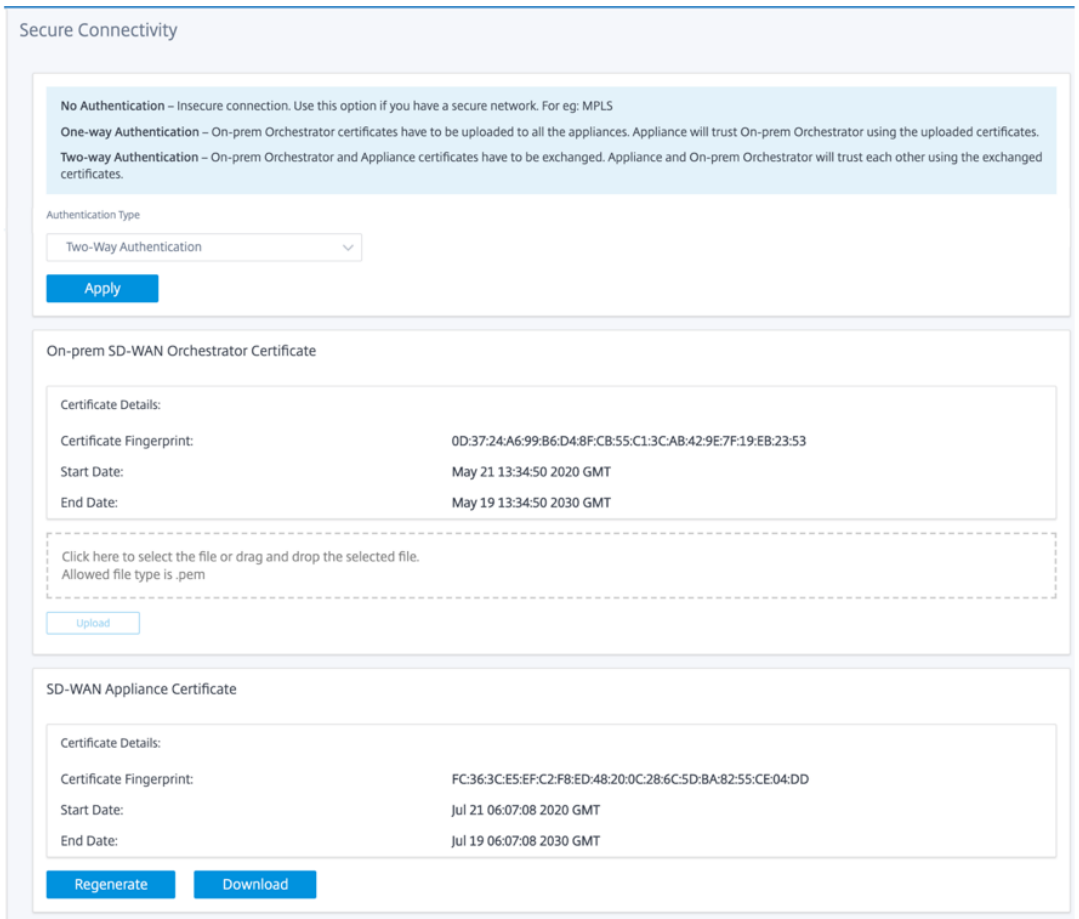
   - **Keine Authentifizierung** —Keine Authentifizierung zwischen dem On-prem SD-WAN Orchestrator und der SD-WAN Appliance, und es ist nicht erforderlich, die SD-WAN Appliance oder das On-prem SD-WAN Orchestrator-Zertifikat zu verwenden. Sie können diese Option jedoch verwenden, wenn Sie über ein sicheres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



   - **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.



- **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.



> **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

October 28, 2021

Hardwareanforderungen

Anweisungen zur 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 virtuelle Pfadverbindung mit der Appliance herstellen, auf der SD-WAN Release 11.3 ausgeführt wird. 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 gebündelt und mithilfe des **Änderungsmanagement-Assistenten im Management-Webinterface**, das auf dem Master Control Node (MCN) ausgeführt wird, an die Clients verteilt.

Wenn es sich um eine Erstinstallation handelt, müssen Sie das entsprechende Appliance-Paket auf jeder der Client-Appliances in Ihrem SD-WAN-Netzwerk manuell hochladen, ein Staging durchführen 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 werden.

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

Für jedes unterstützte SD-WAN-Appliance-Modell gibt es ein anderes Citrix SD-WAN-Softwarepaket. 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 im Datenblatt zur SD-WAN-Produktplattform-Edition auf der Website zum Herunterladen des Produkts.

SD-WAN Standard-Edition-Hardware-Appliances

Im Folgenden sind die unterstützten SD-WAN Standard Edition Hardware-Appliance-Modelle aufgeführt:

SD-WAN SE PLATFORM MODEL	ROLE
110-SE/110-LTE-WiFi/110-WiFi-SE	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)

Im Folgenden sind die unterstützten SD-WAN WAN Optimization (WANOP) -Appliance-Modelle aufgeführt:

SD-WAN WANOP PLATFORM MODELS	ROLE
WANOP 4100	Rechenzentrum-Appliance
WANOP 5100	Rechenzentrum-Appliance

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

Im Folgenden sind die unterstützten SD-WAN VPX Virtual Appliance (VPX-SE) Modelle aufgeführt:

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 den Voraussetzungen von Citrix SD-WAN Virtual VPX Standard Edition.

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

Im Folgenden sind die unterstützten SD-WAN WANOP Virtual Appliance (VPX-WANOP) Modelle aufgeführt:

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 Release-Version 10.1 wird die Enterprise Platform Edition in “Premium Edition”umbenannt.

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

Im Folgenden sind die unterstützten SD-WAN Premium (Enterprise) Edition Appliance-Modelle (SD-WAN PE) aufgeführt:

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

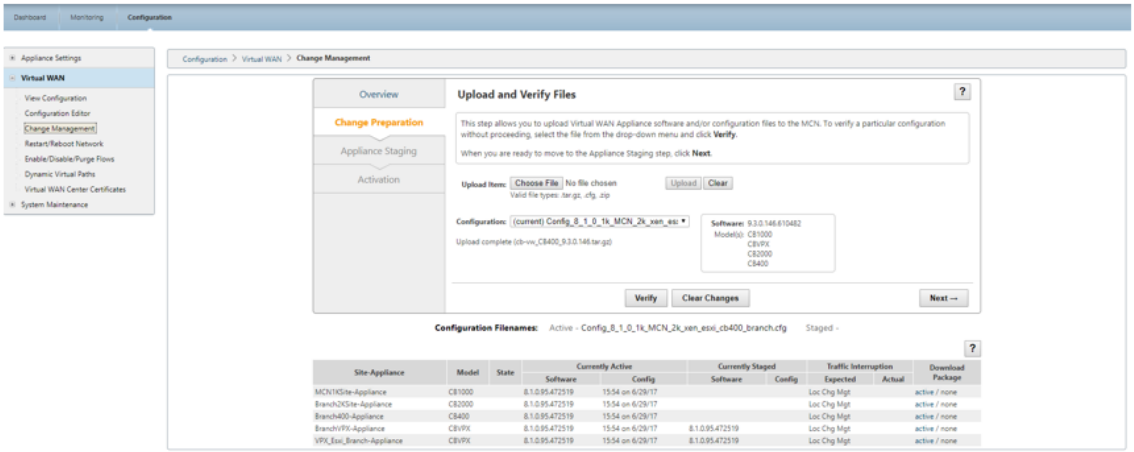
- Kunden, die ein Upgrade von Citrix SD-WAN Version 9.3.x durchführen, wird empfohlen, vor dem Upgrade auf eine Hauptversion auf 10.2.8 zu aktualisieren.
- Stellen Sie beim Durchführen eines Software-Upgrades sicher, dass das Staging für alle verbundenen Sites abgeschlossen ist, bevor Sie es aktivieren. 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

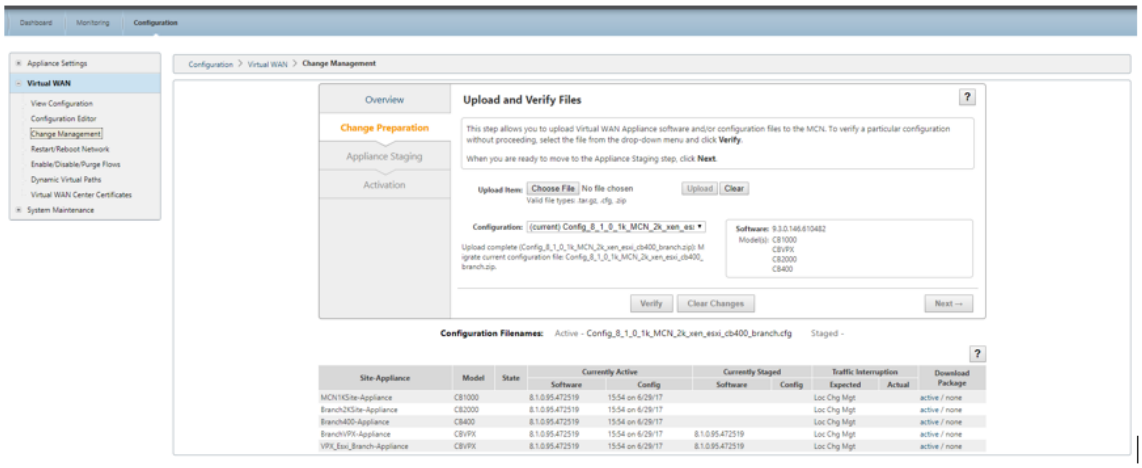
October 28, 2021

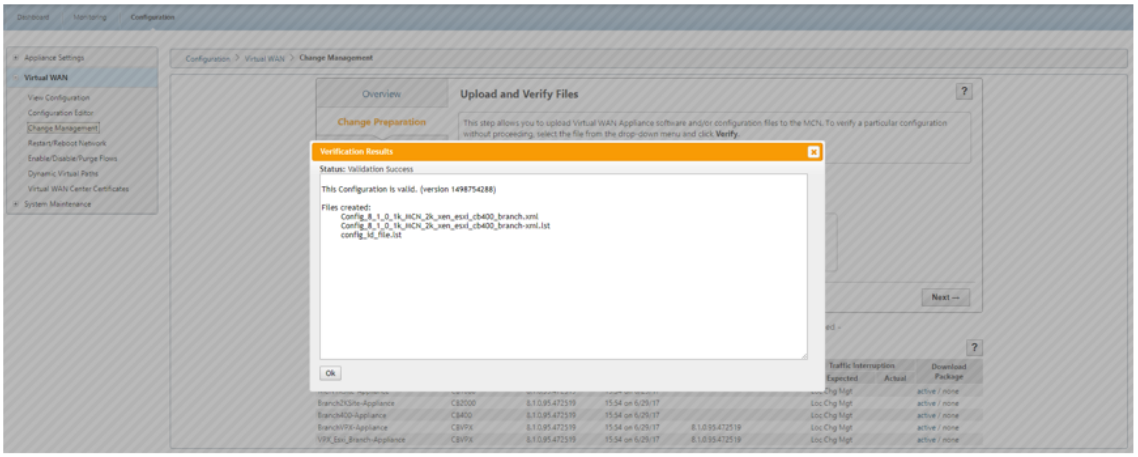
> **Hinweis:**
>
> Lassen Sie eine funktionierende Virtual WAN-Konfiguration erstellen, die 9.3.4 oder niedriger ausführt, mit virtuellen Pfaden von MCN zu den Zweigstandorten.

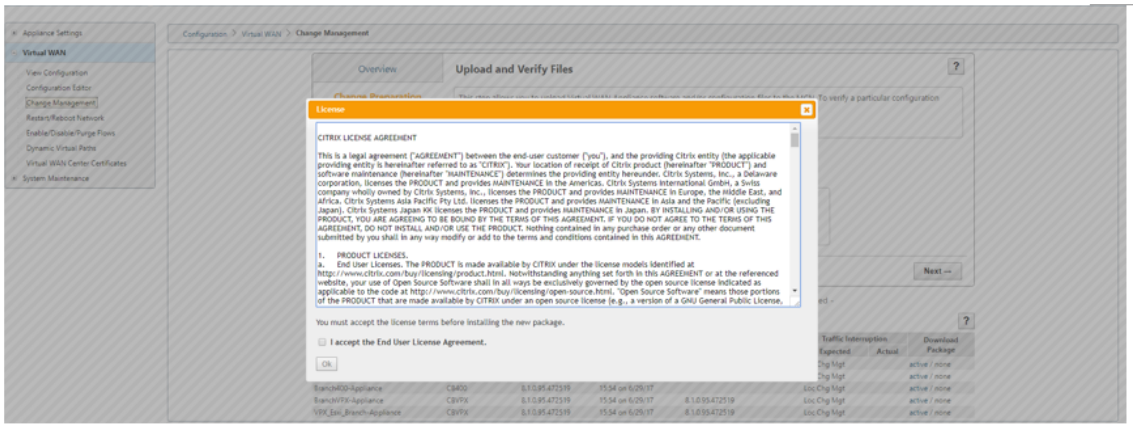
1. Navigieren Sie auf der MCN-Appliance zu **Konfiguration** > **Virtuelles WAN** > **Änderungsmanagement**.
2. Rufen Sie die zutreffende *cb-vw–9.3.5.23.tar.gz-Datei* <ApplianceModel>für alle Sites im virtuellen WAN-Netzwerk von der Citrix Downloadseiteab
3. Laden Sie die <ApplianceModel>Datei *cb-vw- -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.



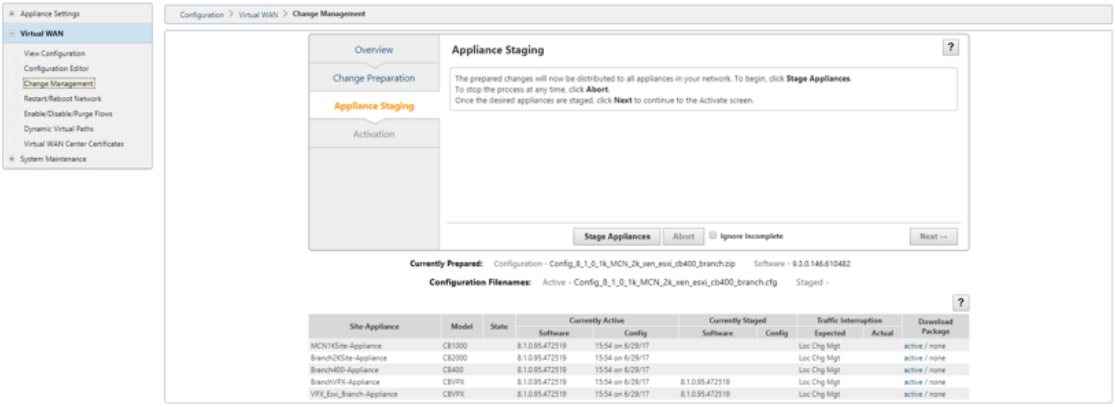
4. Klicken Sie auf **Weiter**, um fortzufahren.



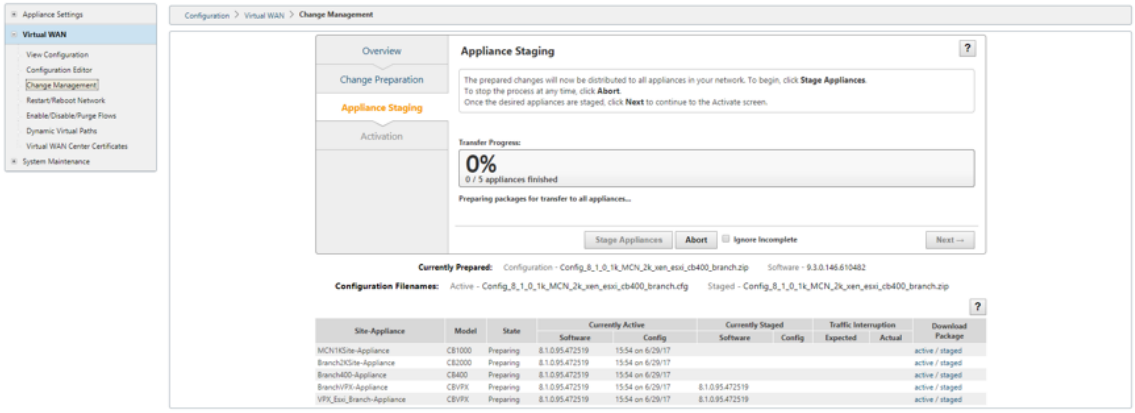


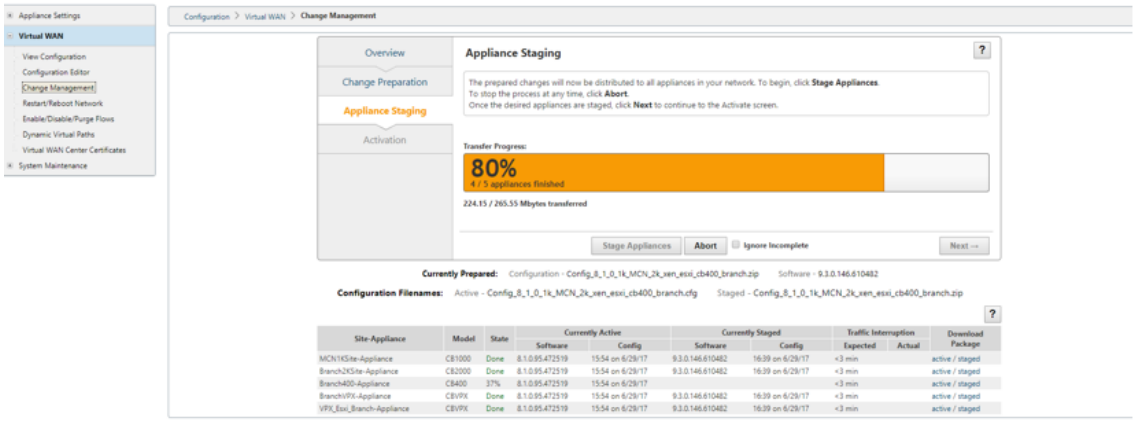


5. Nachdem Sie die Lizenzvereinbarung akzeptiert haben, navigieren Sie zu **Appliance Staging**, wo Appliances durch Klicken auf **Stage Appliances bereitgestellt**werden können.

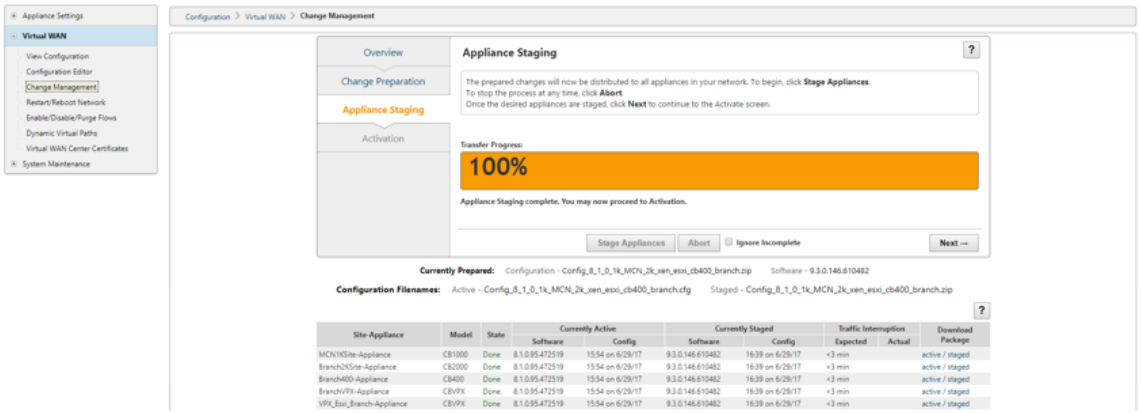


6. Der Status “Übertragungsfortschritt”wird im Rahmen der Vorbereitung und Bereitstellung der Softwarepakete für die Appliances angezeigt.

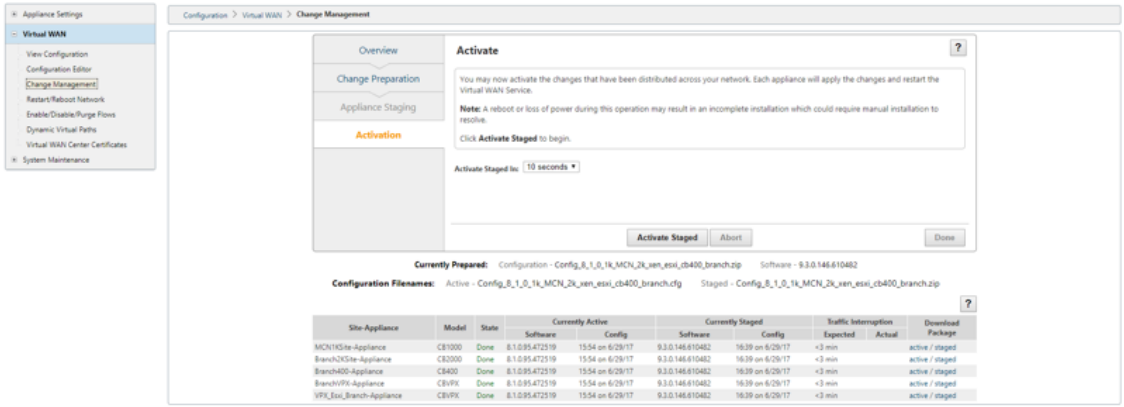


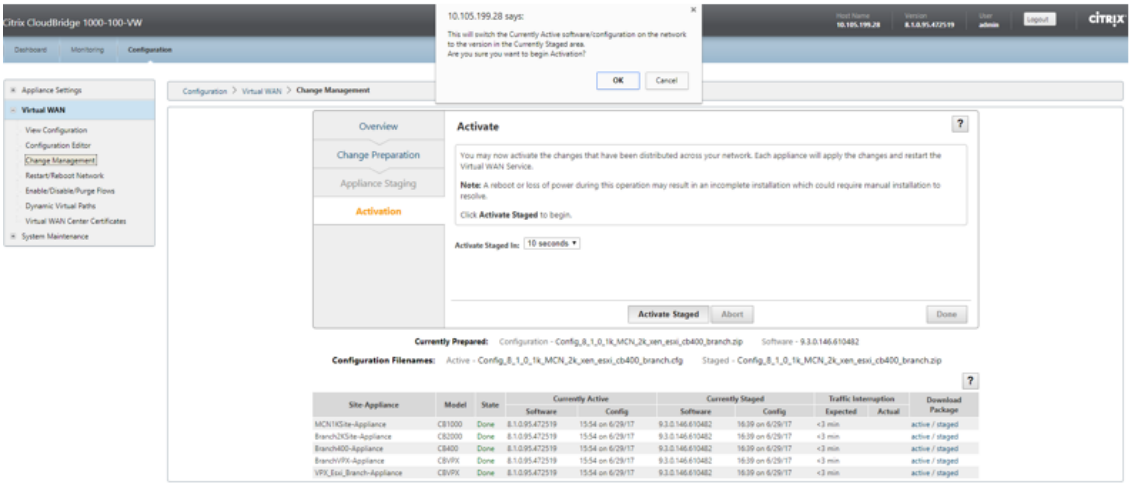


7. Klicken Sie auf **Weiter**, wenn Übertragungsfortschritt 100% anzeigt und die Schaltfläche aktiviert ist, um fortzufahren.

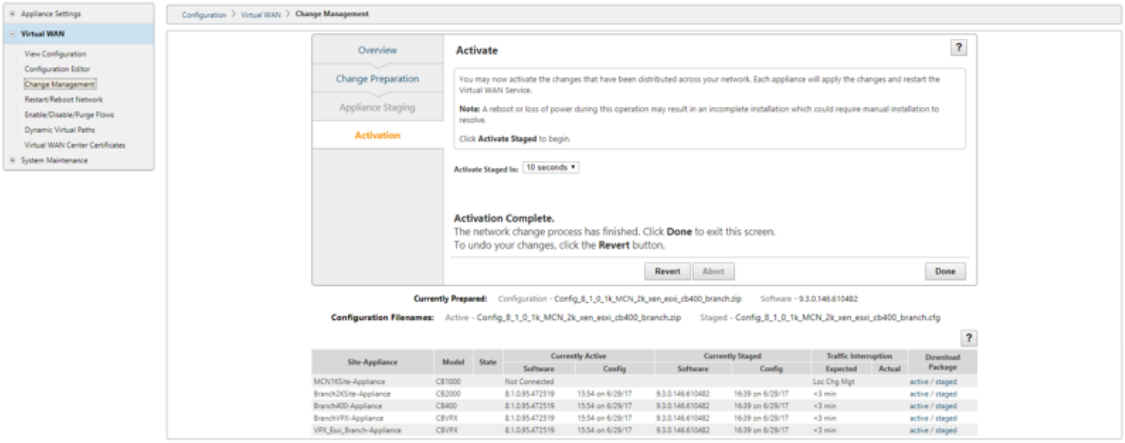


8. Klicken Sie auf der Seite **Aktivierung** auf **Staged aktivieren**, um mit der Aktivierung zu beginnen.





9. Nach Abschluss des Aktivierungs-Countdowns von 180 s klicken Sie auf **Fertig**.

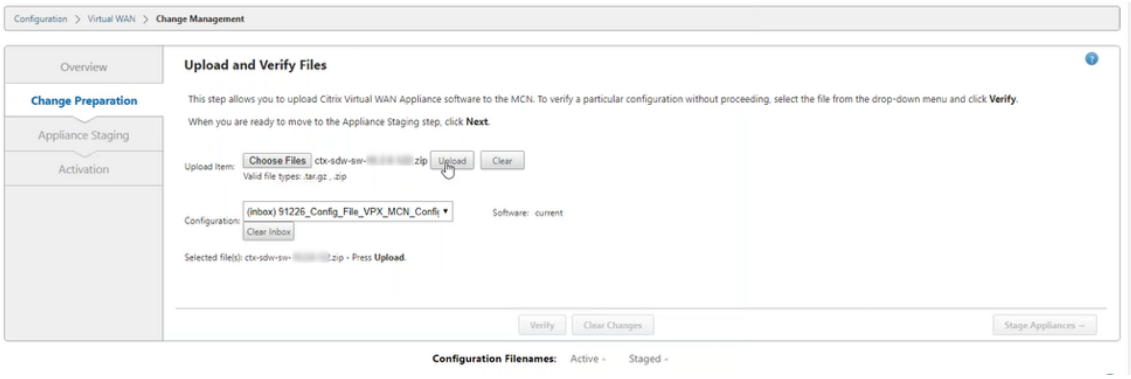


Upgrade auf 11.3 mit funktionierender Virtual WAN-Bereitstellung

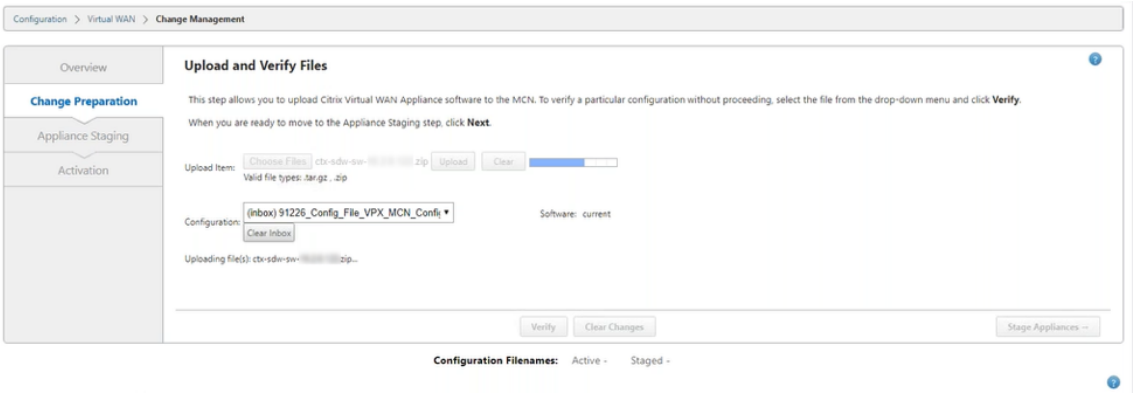
October 28, 2021

1. Klicken Sie auf der Seite **Change Management > Change Preparation** auf Choose **Files und wählen** Sie die Softwarepaketdatei *ctx-sdw-11.3.0.x.zip* aus. Klicken Sie auf **Upload**.

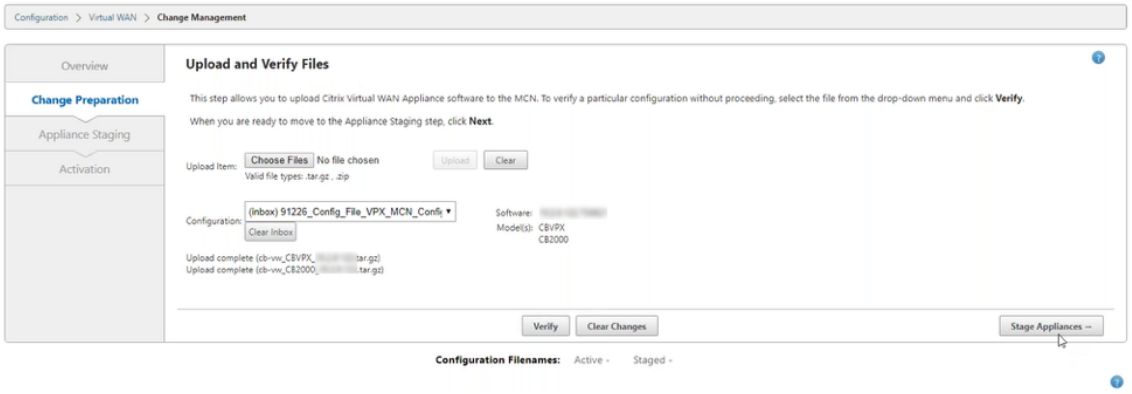
   > **Hinweis:**
   >
   > Sie können das Citrix SD-WAN Release 11.3-Softwarepaket von der Seite Downloads herunterladen.



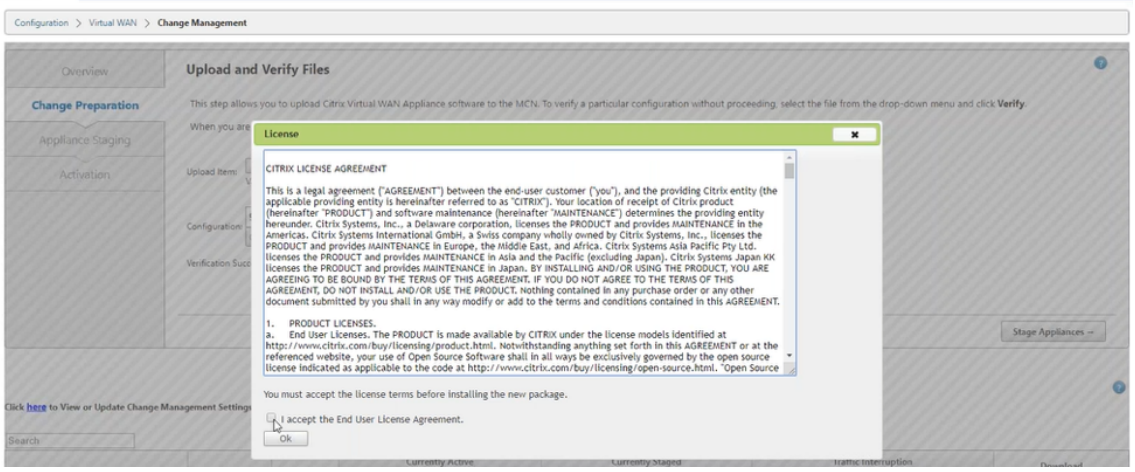
   Ein Fortschrittsbalken wird angezeigt, um den aktuellen Upload-Fortschritt anzuzeigen.



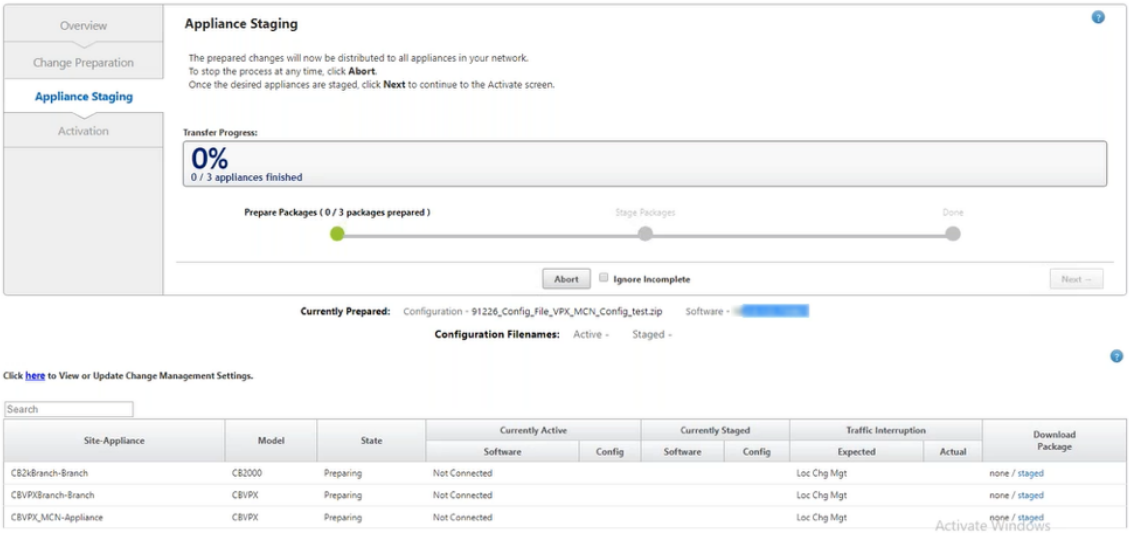
2. Nachdem der Upload-Vorgang erfolgreich war, werden relevante Appliance-Modelle angezeigt. Die Appliances würden basierend auf der Konfigurationsdatei aktualisiert.



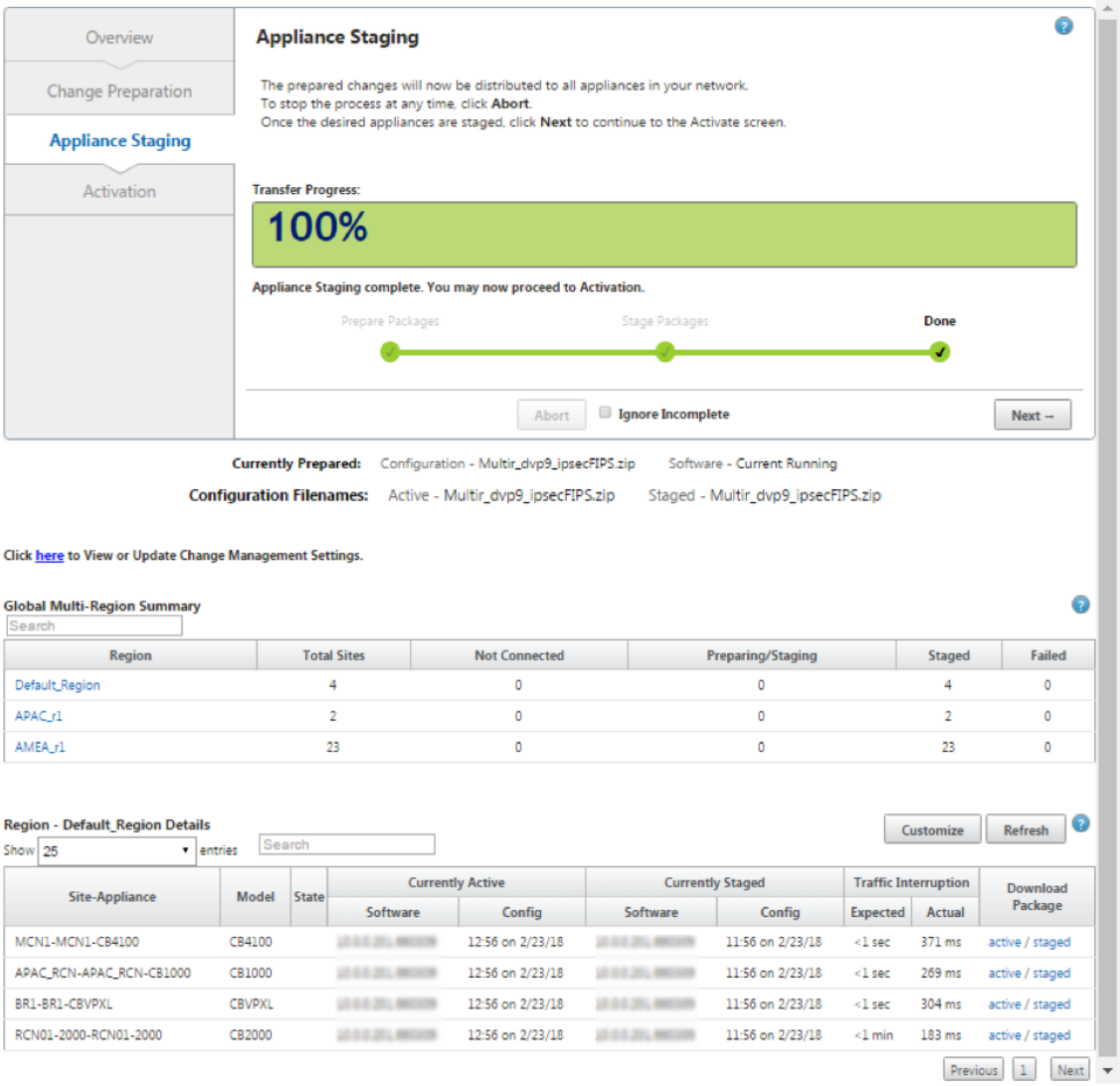
3. Klicken Sie auf **Stage Appliance**, um mit der Überprüfung der Konfigurationsdatei fortzufahren Die Seite mit der Lizenzvereinbarung zur Benutzerakzeptanz wird angezeigt. Klicken Sie auf **Ich akzeptiere die Endbenutzer-Lizenzvereinbarung** und klicken Sie auf **OK**.



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



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

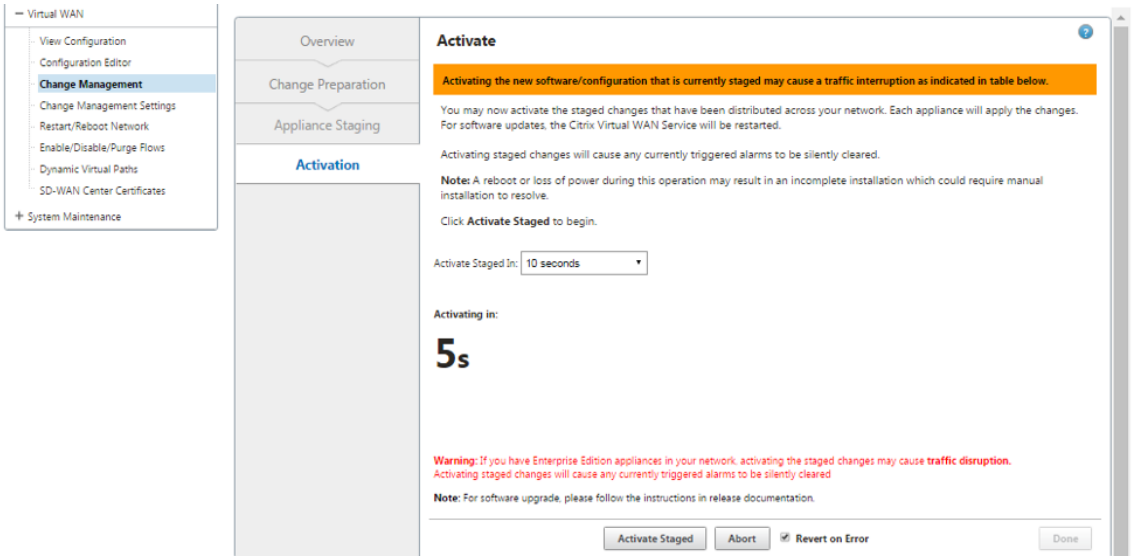


Die verschiedenen Status der Softwarepaketkonfiguration, die in der Übersichtstabelle angezeigt werden, weisen auf Folgendes hin:

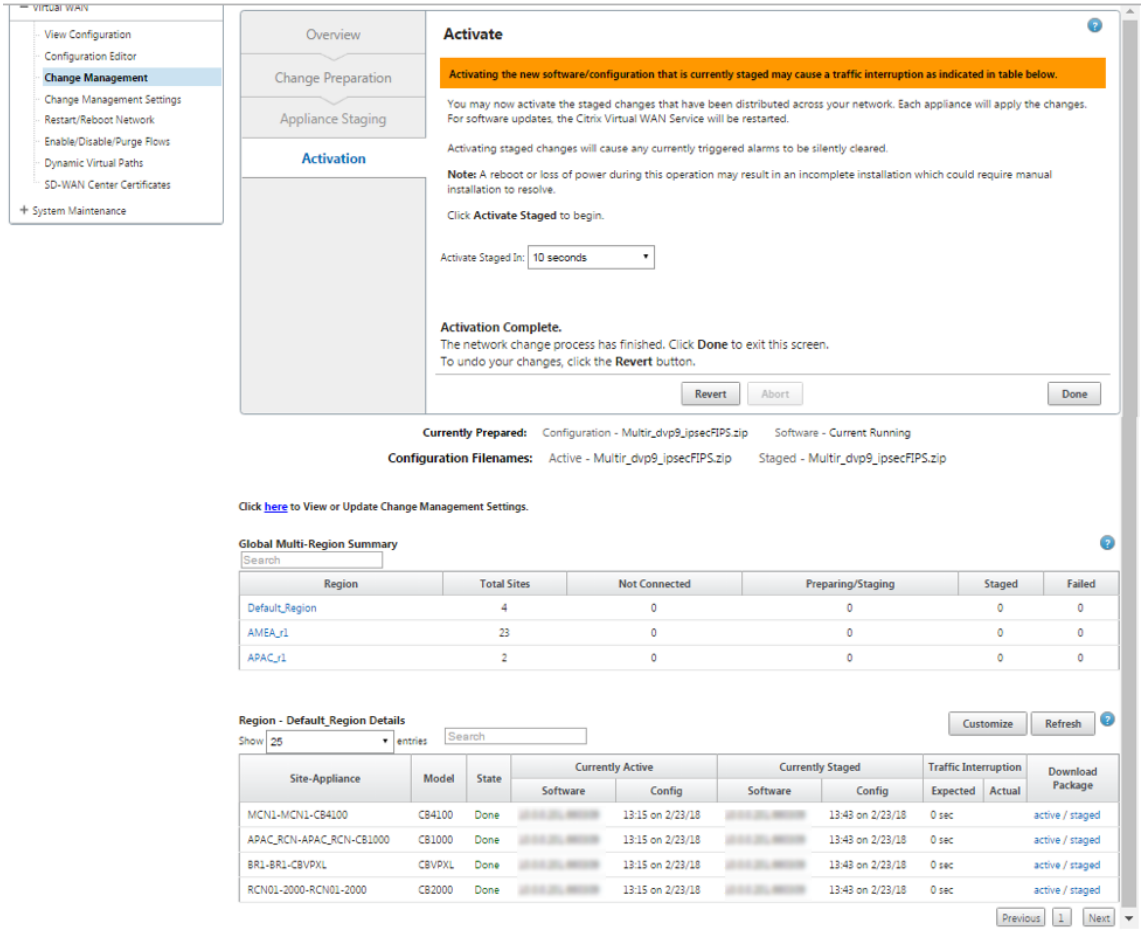
- **Vorbereiten** - Lokale Verarbeitung zur Vorbereitung des Update-Pakets für die Übertragung auf die Appliance.
- **Regions-Pakete vorbereiten** - Lokale Verarbeitung zur Vorbereitung des Update-Pakets für die Übertragung an RCN. (Gilt, wenn RCN Teil des Netzwerks ist).
- **Prozentsatz** - Prozent des auf das Gerät übertragenen Pakets.
- **Entpacken** - Remote-Appliance-Verarbeitung zum Anwenden des Update-Pakets.
- **Region übertragen** - Paket wird an RCN übertragen. (Gilt, wenn RCN Teil des Netzwerks ist).
- **Fehlgeschlagen** - Remote hat eine unvollständige Übertragung festgestellt.
- **Abgebrochen** - Vom Benutzer abgebrochen, wenn “Unvollständig ignorieren”während Stage Appliances aktiviert wurde

- **Nicht erforderlich** - Vorbereitetes bereitgestelltes Paket enthält diesen Site-Appliance-Namen nicht.
- **Nicht verbunden** - Local kann die aktiven Paketinformationen der Fernbedienung nicht sehen.

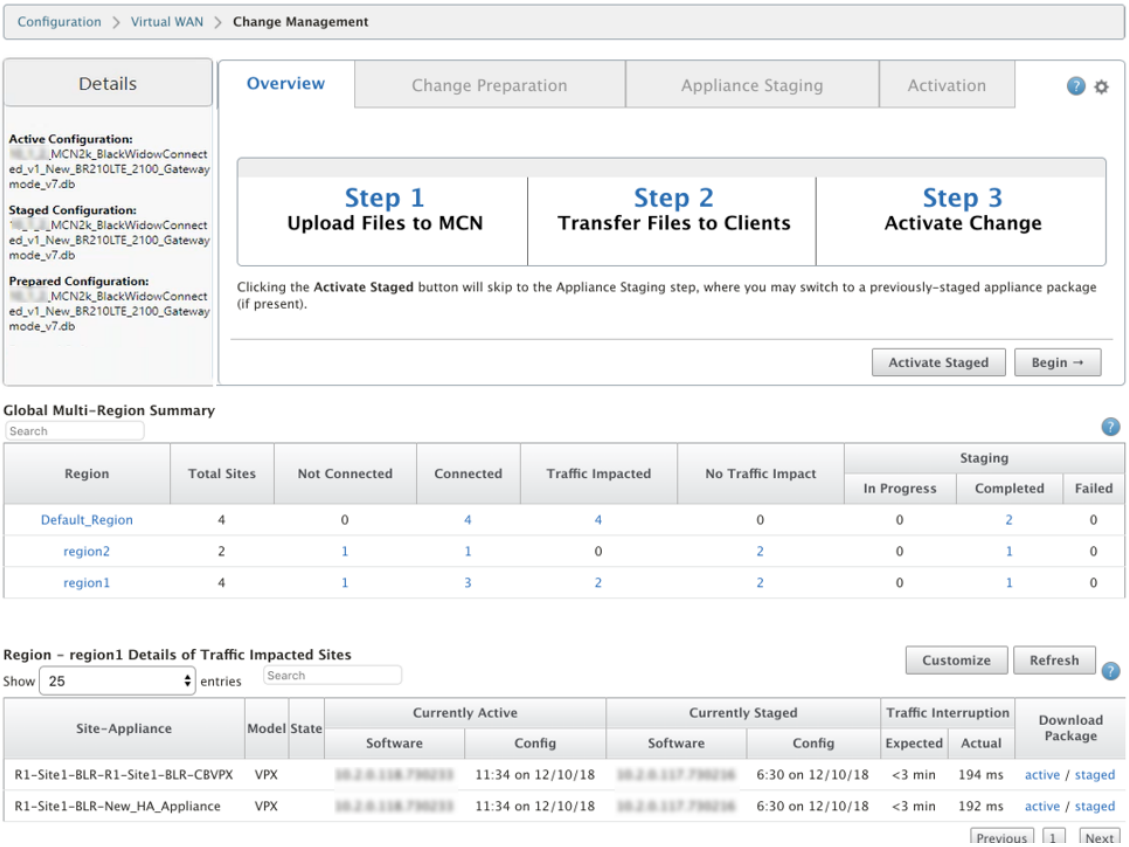
6. Klicken Sie auf “**Staged** aktivieren”, um die gestagte Software zu aktivieren.



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



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



Die Übersichtstabelle für mehrere Regionen enthält die folgenden Details:

- **Region** —Name der Region
- **Gesamtzahl der Standorte** - 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.
- **Beeinträchtigter Verkehr** - Gesamtzahl der Standorte, an denen der Verkehr in der Region betroffen ist.
- **Keine Auswirkungen auf den Verkehr** - Gesamtzahl der Standorte, an denen der Verkehr in der Region nicht beeinträchtigt wird.
- **Staging in Bearbeitung** —Gesamtzahl der Standorte, für die die lokale Verarbeitung versucht, ein Updatepaket für die Übertragung in der Region vorzubereiten.
- **Staging abgeschlossen** - Gesamtzahl der Standorte, für die das Staging in der Region abgeschlossen wurde.
- **Staging fehlgeschlagen** - Gesamtzahl der Standorte, für die 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 zum Eintrag für die **globale Tabelle mit mehreren Regionen**, um die regionsspezifischen Konfigurationsberichte zu filtern.

Region - Default_Region Details of Connected 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	
MCN-NY-MCN-NY-CB2000	2000		[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	82 s	active / staged
Def-Site1-SC-Def-Site1-SC-CBVPX	VPX		[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	209 s	active / staged
R1-RCN-MUM-R1-RCN-MUM-CBVPX	VPX	Done(auto)	[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	195 s	active / staged
R2-RCN-SA-R2-RCN-SA-CBVPX	VPX	Done(auto)	[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	199 s	active / staged

Previous 1 Next

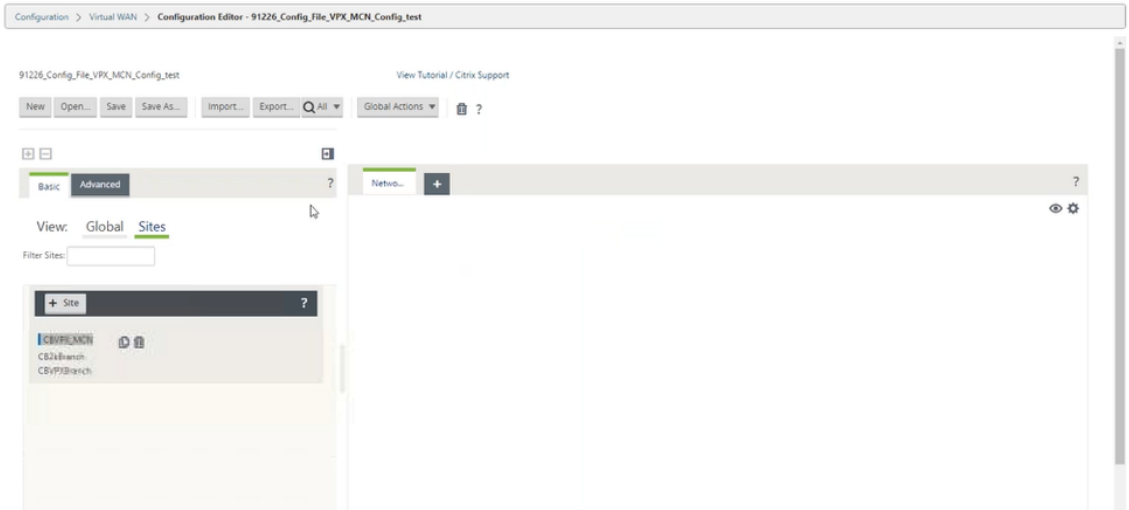
Navigieren Sie für die Bereitstellung von Multiregionen auf jedem RCN zur Seite **"Change Management Settings** "und planen Sie die Installation abhängiger Komponenten. Standardmäßig weist MCN/RCN die Installation von Zeitplänen zu, die täglich um 21:20:00 Uhr versucht werden, basierend auf der Softwareverfügbarkeit in den Filialen. Weitere Informationen finden Sie unter Änderungsverwaltungseinstellungen

Upgrade auf 11.3 ohne funktionierende virtuelle WAN-Bereitstellung

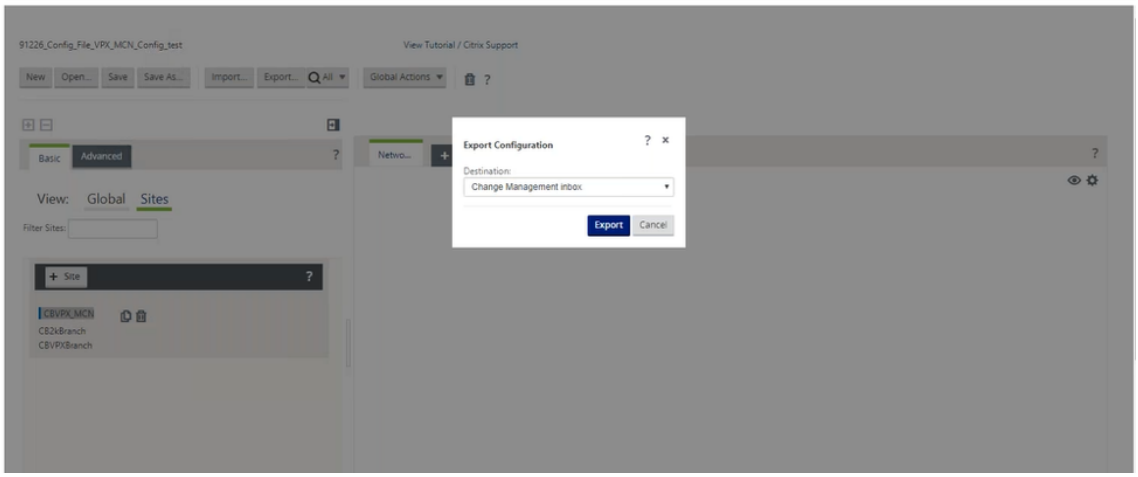
October 28, 2021

> Hinweis: Um die neuesten Funktionen von 11.3 zu konfigurieren, sollten Sie die MCN-Appliance auf die Software 11.3 einstellen. Weitere Informationen finden Sie unter Reimage Citrix SD-WAN Appliance-Software

1. Bereiten Sie die Konfiguration mit dem **Konfigurationseditor** vor, und speichern Sie die Konfiguration unter einem gültigen Namen. Weitere Informationen finden Sie unter Thema Konfiguration.

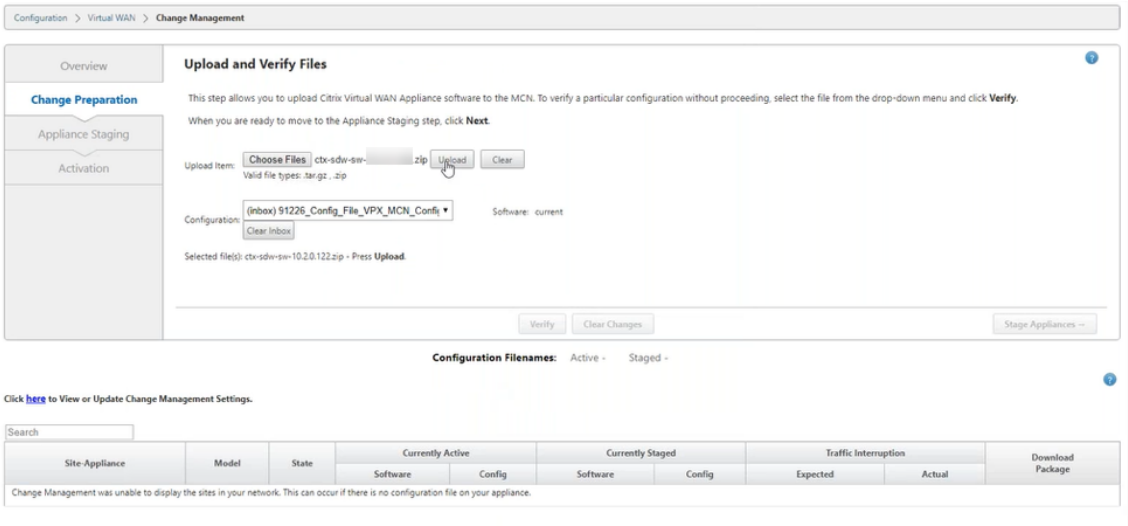


2. Exportieren Sie die gespeicherte Konfiguration nach Change Management. Klicken Sie auf **Exportieren** und wählen Sie **Change Management-Posteingang** als Ziel aus. Klicken Sie auf **Exportieren**.

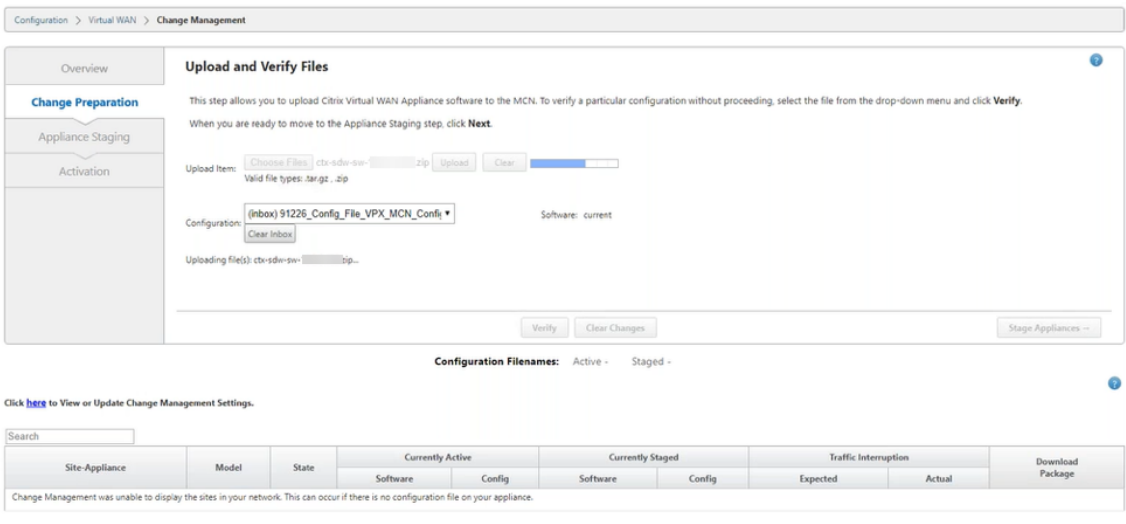


3. Klicken Sie auf der Seite **Change Management > Change Preparation** auf Choose **Files und wählen** Sie die Softwarepaketdatei *ctx-sdw-11.3.0.x.zip* aus. Klicken Sie auf **Upload**.

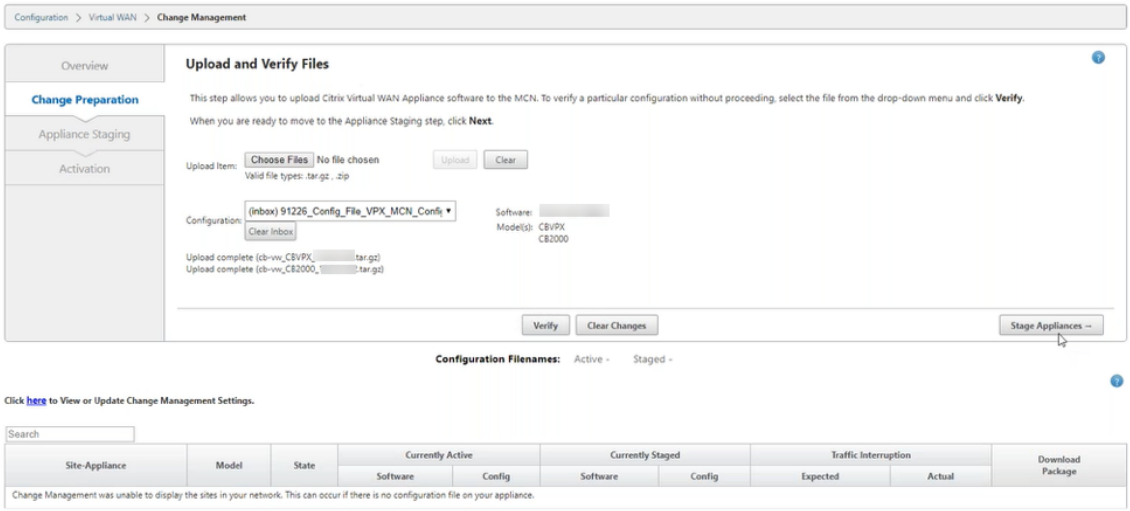
> **Hinweis:**
>
> Sie können das Citrix SD-WAN Release 11.3-Softwarepaket von der Seite Downloads herunterladen.



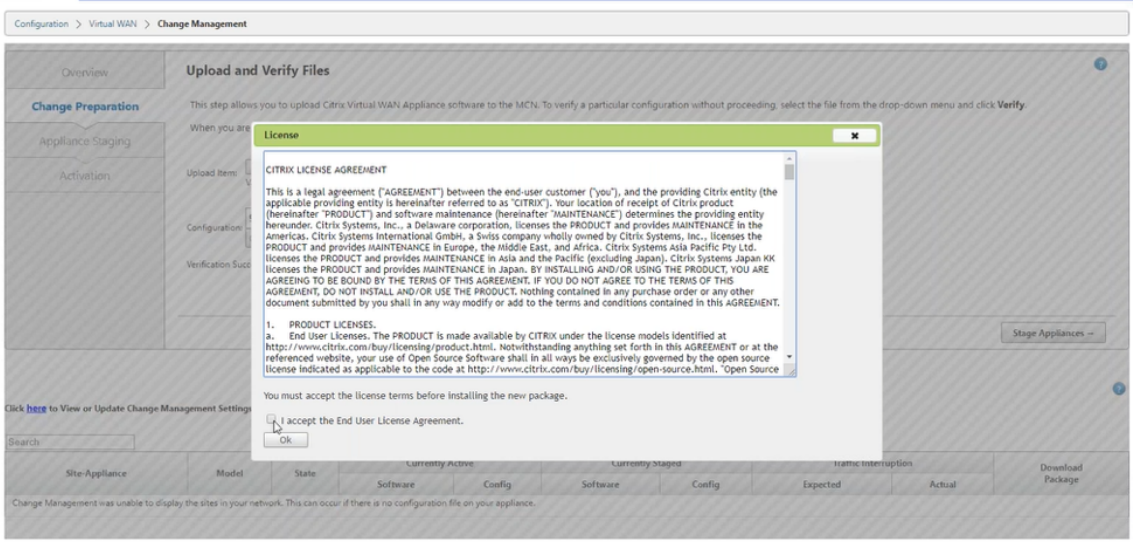
Ein Fortschrittsbalken wird angezeigt, um den aktuellen Upload-Fortschritt anzuzeigen.



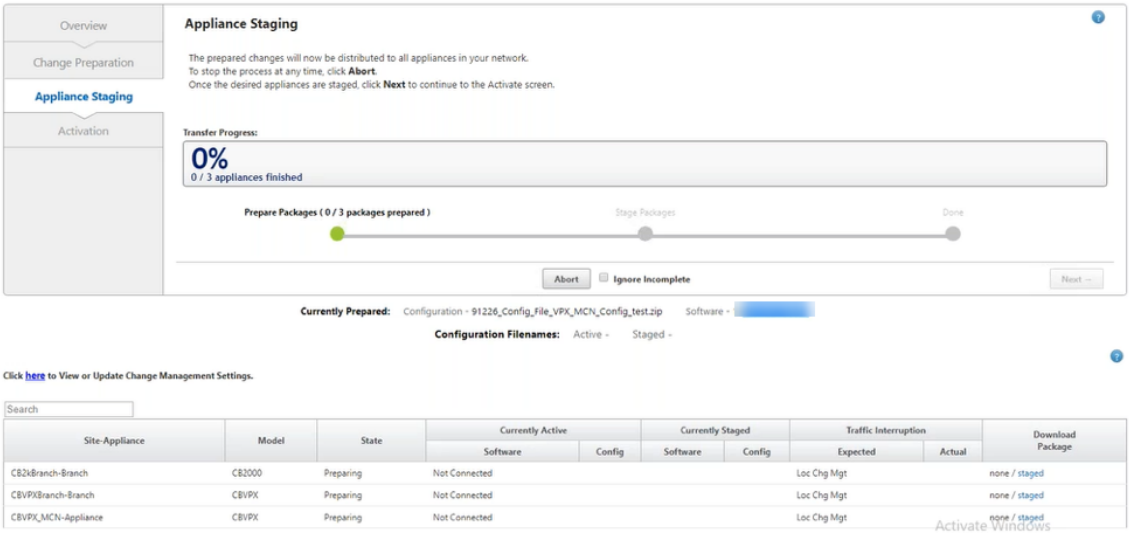
4. Nachdem der Upload-Prozess erfolgreich war, werden relevante Modelle angezeigt, die basierend auf der Konfigurationsdatei aktualisiert werden, die Informationen zu jedem Zweigplattformmodell enthält.



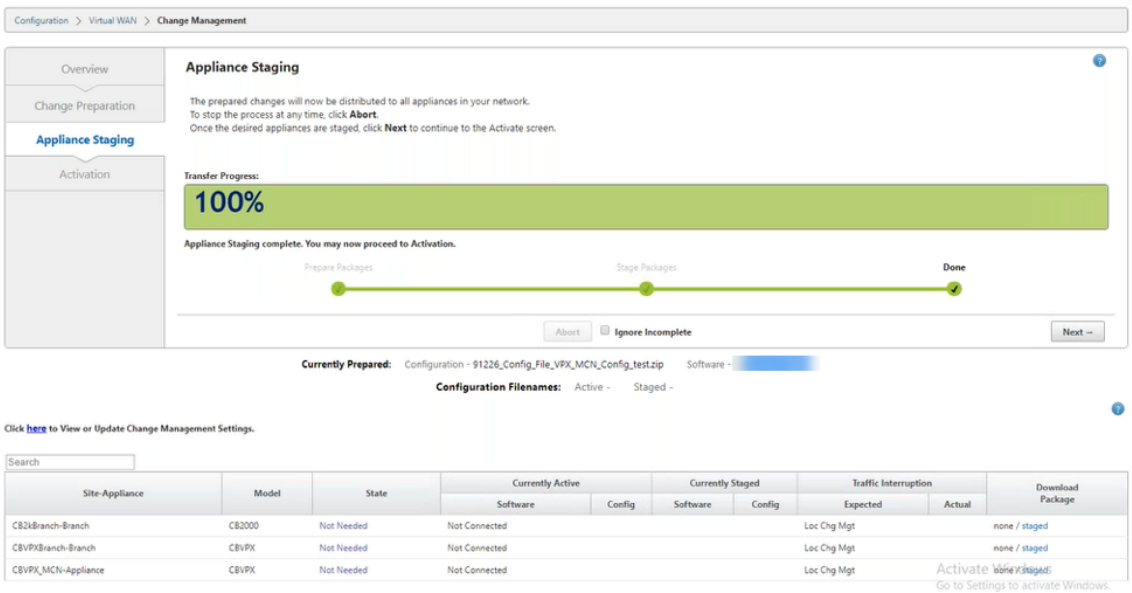
5. Klicken Sie auf **Stage Appliance**, um mit der Überprüfung der Konfigurationsdatei fortzufahren Die Seite mit der Lizenzvereinbarung zur Benutzerakzeptanz wird angezeigt. Klicken Sie auf **Ich akzeptiere die Endbenutzer-Lizenzvereinbarung** und klicken Sie auf **OK**.



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

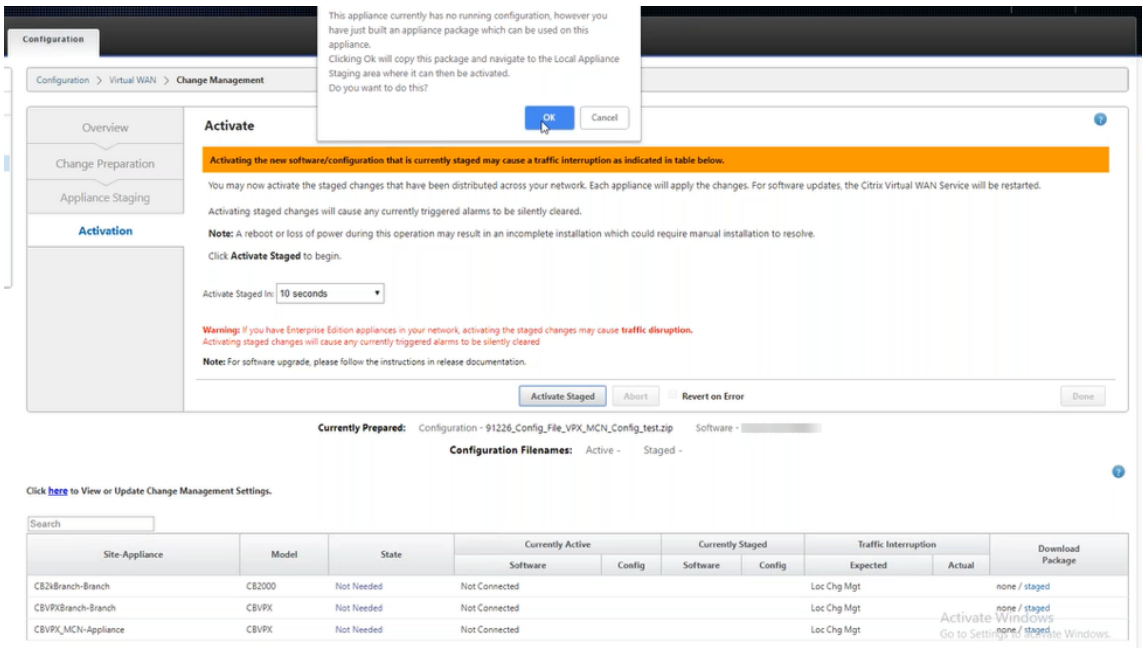


7. Sobald der Transferfortschritt zu 100% abgeschlossen ist, klicken Sie auf **Weiter**, um mit der Aktivierung fortzufahren.

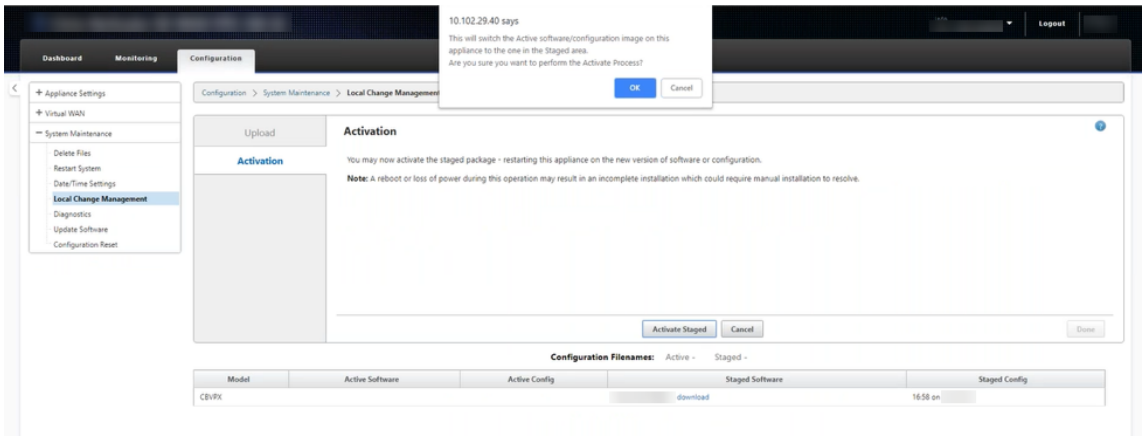


8. Klicken Sie auf **Activate Staged**. Eine Popup-Meldung zur Benutzerakzeptanz wird angezeigt, da dies das erste Mal ist, dass die Appliance bereitgestellt wird.

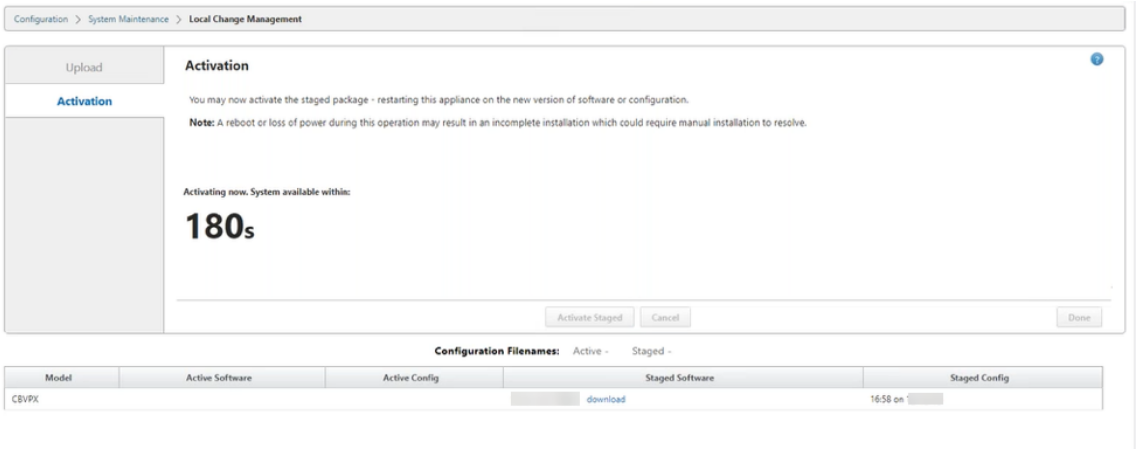
   Sie werden zur Seite **Lokale Änderungsverwaltung** weitergeleitet, um die lokale Appliance zu aktivieren. Klicken Sie auf **OK** um fortzufahren.



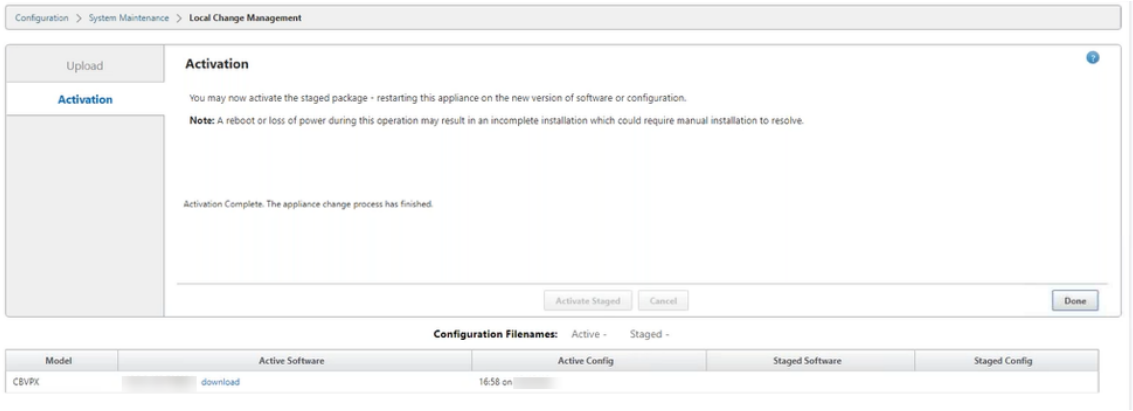
9. Klicken Sie im lokalen Änderungsmanagement auf **Activate Staged**. Eine Meldung zur Bestätigung der Aktivierung wird angezeigt. Klicken Sie auf **OK**.



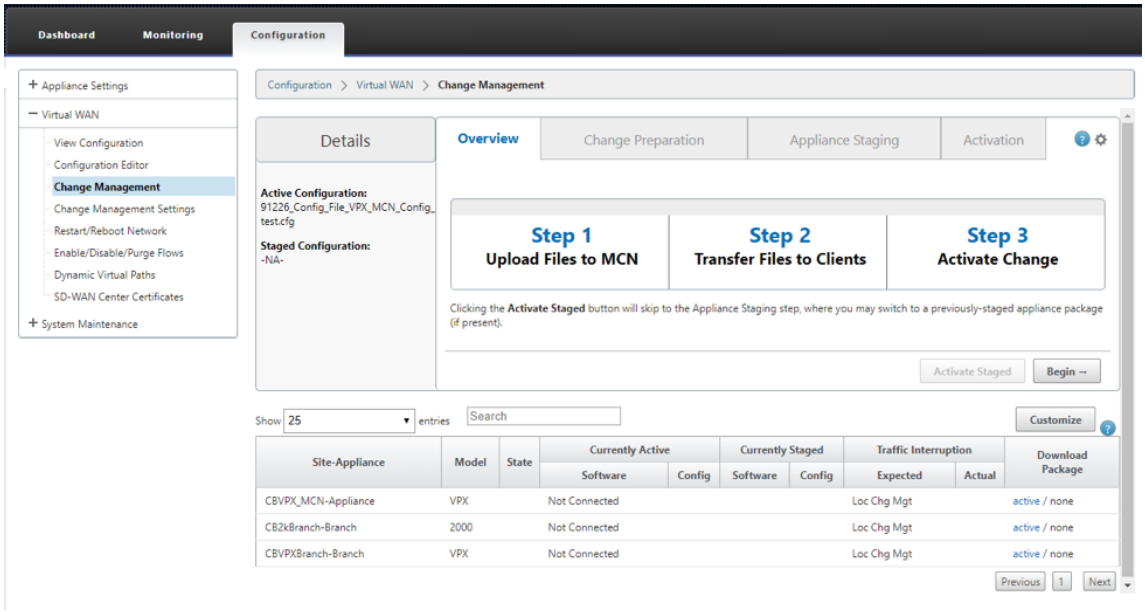
Die Aktivierung beginnt mit einem Countdown-Timer von 180 Sekunden.



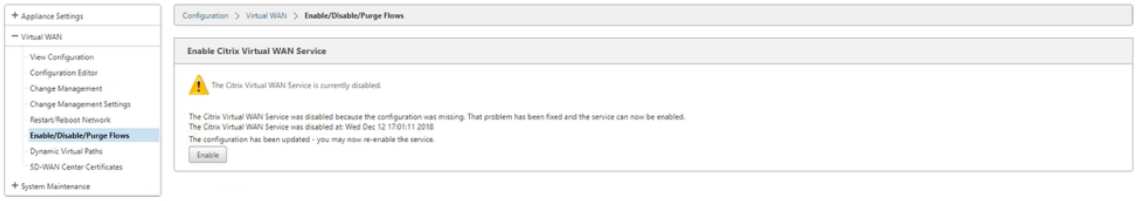
10. Nach dem Countdown zeigt eine Meldung an, dass die Aktivierung abgeschlossen ist. Klicken Sie auf **Fertig**, die Appliance startet neu.



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



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



Um weitere Sites zu konfigurieren und dem Netzwerk hinzuzufügen, folgen Sie dem Verfahren im Thema Zweigknoten konfigurieren.

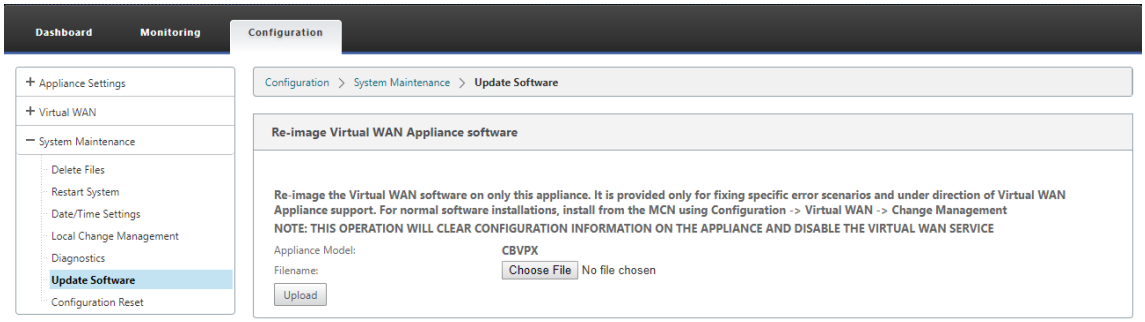
Reimage der Citrix SD-WAN Appliance-Software

October 28, 2021

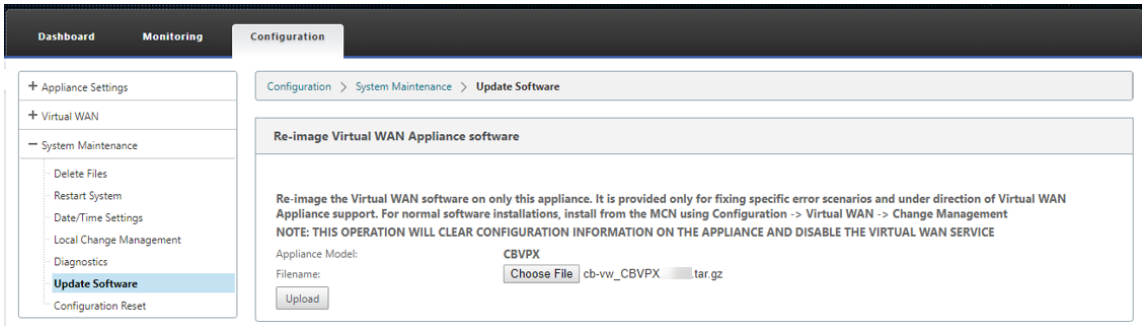
Laden Sie die Datei *.tar.gz* der erforderlichen Citrix SD-WAN-Softwareversion und -Plattform vom Citrix Downloads-Portal herunter.

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

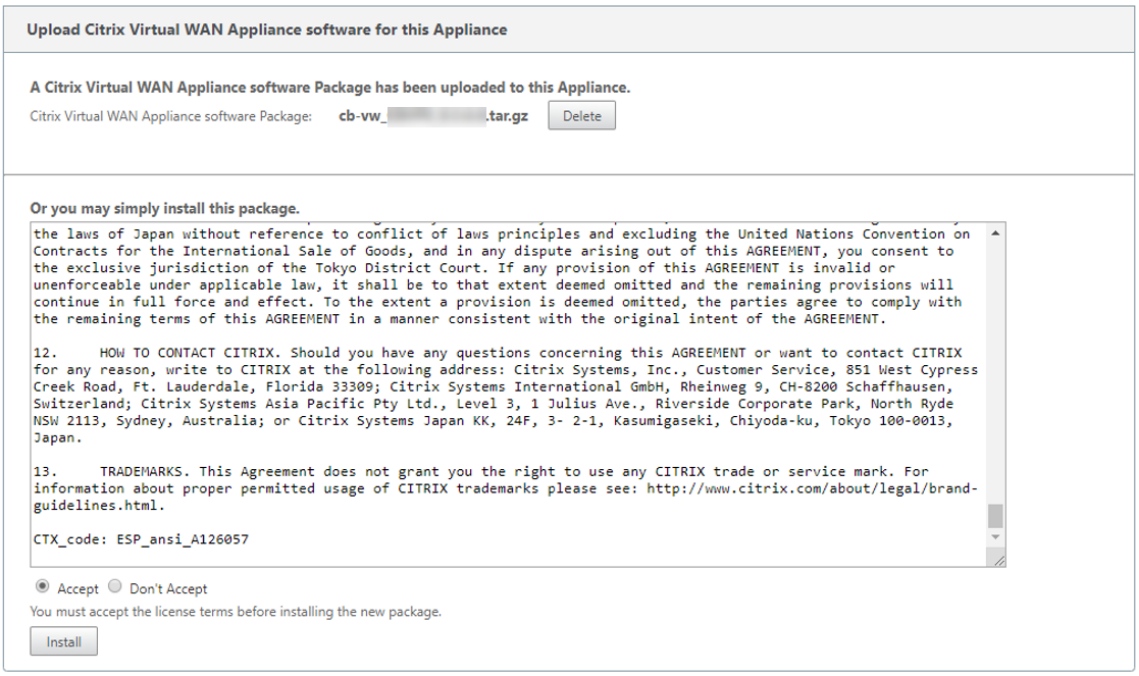
1. Navigieren Sie in der GUI der SD-WAN-Appliance zu **Konfiguration** > **Systemwartung** > **Update-Software**.



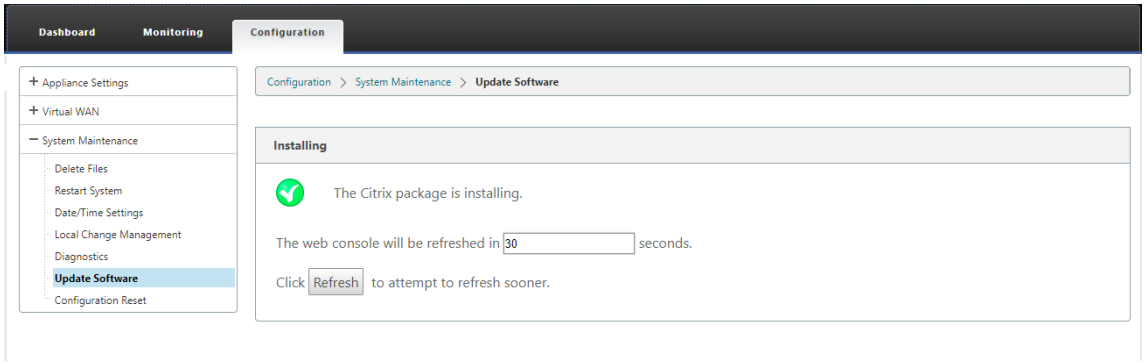
2. Klicken Sie auf **Datei auswählen** und wählen Sie die heruntergeladene Citrix SD-WAN Appliance-Software aus Klicken Sie auf **Upload**.



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



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



Teilweise Softwareupgrade mit lokalem Änderungsmanagement

October 28, 2021

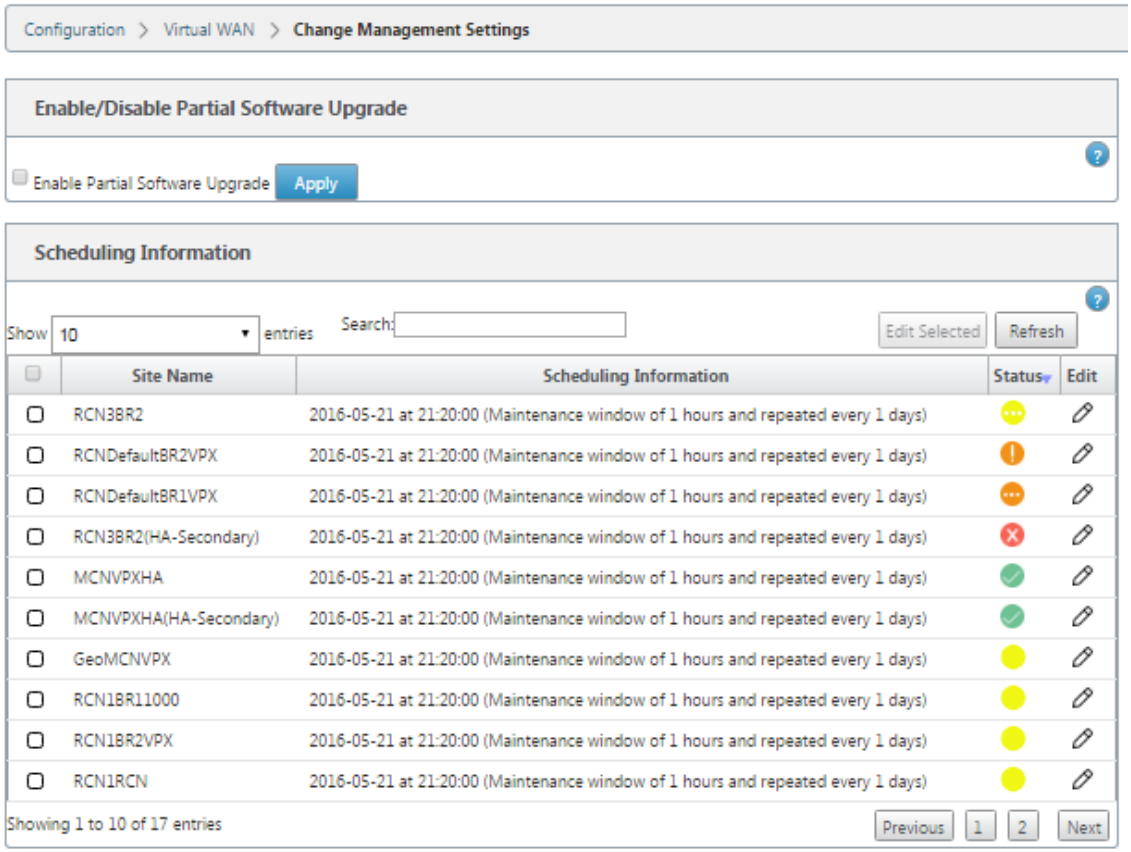
> **Wichtig**
>
> Standardmäßig ist die Option **Partielles Software-Upgrade** deaktiviert.

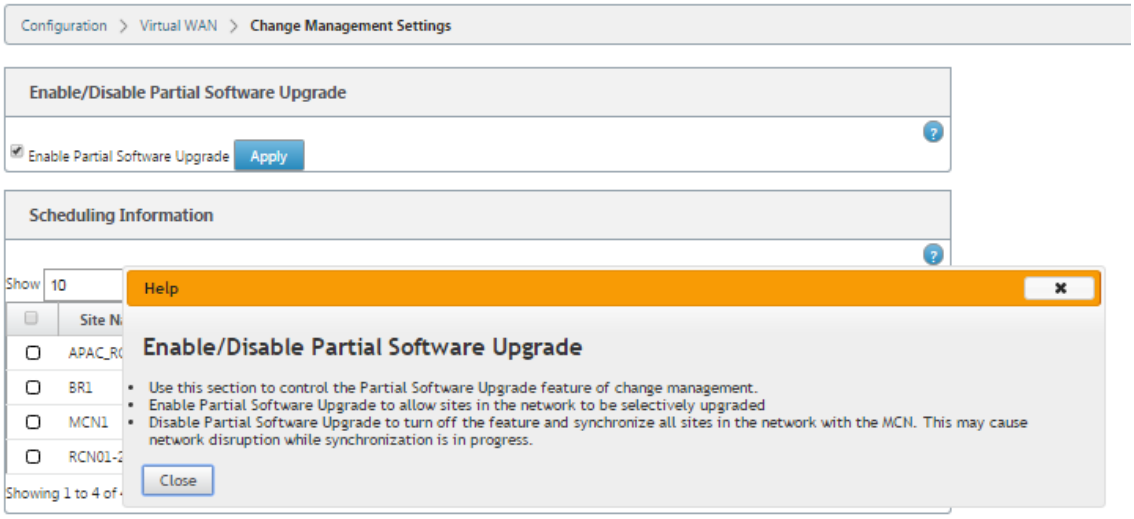
Mit der Option **Lokales Änderungsmanagement** können Sie eine neuere SD-WAN-Softwareversion auf einer Teilmenge von Client-Sites installieren. Dies wird durch die teilweise Software-Upgrade-Funktion erreicht, die es dem Netzwerkadministrator ermöglicht, die Software an Standorten im Netzwerk selektiv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

Voraussetzungen und Anforderungen

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

1. Haben Sie eine aktive SD-WAN Version 10.0 oder neuere Software. Klicken Sie auf 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.





2. Stationieren Sie eine 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 vom MCN aus eingesetzt werden. Stopp bei

Activate Staged Schritt des Change Managements.

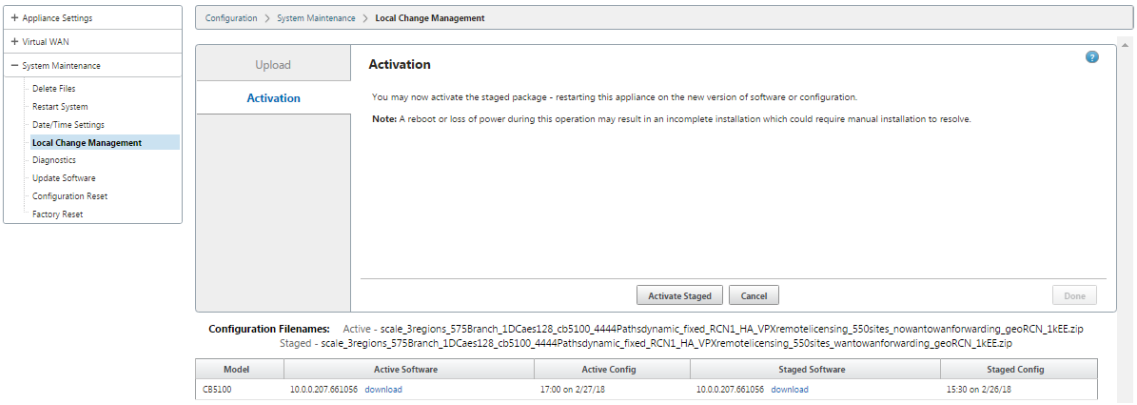
Für die Konfiguration des aktiven und partiellen Standorts muss die Software auf den MCN- und Zweigstandorten identisch sein. Es ist nicht möglich, einen anderen Featuresatz auf teilweise aktualisierten Sites aktiviert zu haben. Gehen Sie zu einzelnen Standorten, um das **lokale Änderungsmanagement**durchzuführen. Lesen Sie die nachstehenden Anweisungen für die Bereitstellung von Hochverfügbarkeit.

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

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

Upgrade-Zweigknoten ohne Hochverfügbarkeitsmodus

1. Navigieren Sie in der Webverwaltungsoberfläche von Citrix SD-WAN zum Zweigstandort, der durch den Teil-Site-Upgrade-Prozess aktualisiert werden muss.
2. Öffnen Sie das **lokale Änderungsmanagement**. Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Activate Staged**. Jeder Zweigstandort wird jetzt mit einer neuen Softwareversion installiert.



Aktualisieren von Zweigknoten im Hochverfügbarkeitsmodus

1. Navigieren Sie in der SD-WAN-Webverwaltungsoberfläche zum Zweigstandort, der durch das partielle Site-Upgrade aktualisiert werden muss.
2. Deaktivieren Sie den Dienst auf der Standby-Appliance.
3. Öffnen Sie auf der primären Appliance **Local Change Management**.
4. Klicken Sie auf **Activate Staged**. Diese Appliance wird jetzt 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 jetzt mit einer neuen Softwareversion installiert.
7. Nachdem die primären und Standby-Appliances den Aktivierungsvorgang abgeschlossen haben, aktivieren Sie den Dienst auf der Standby-Appliance.

Netzwerk aufrüsten

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

October 28, 2021

> **Hinweis**
>
> Nur die SD-WAN 1000- und 2000-WANOP-Appliances können auf SD-WAN Premium Edition-Appliances umgestellt werden.

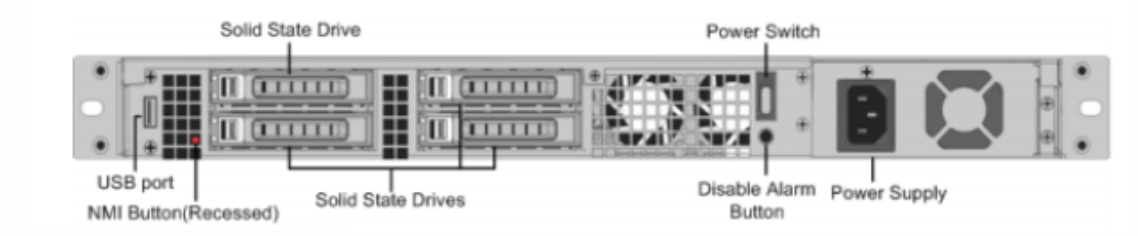
Voraussetzungen

- Stellen Sie sicher, dass Sie nur die 1000-Appliance konvertieren und nicht die 1000 WS. Die 1000 WS-Appliance unterstützt keine Konvertierung auf 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.

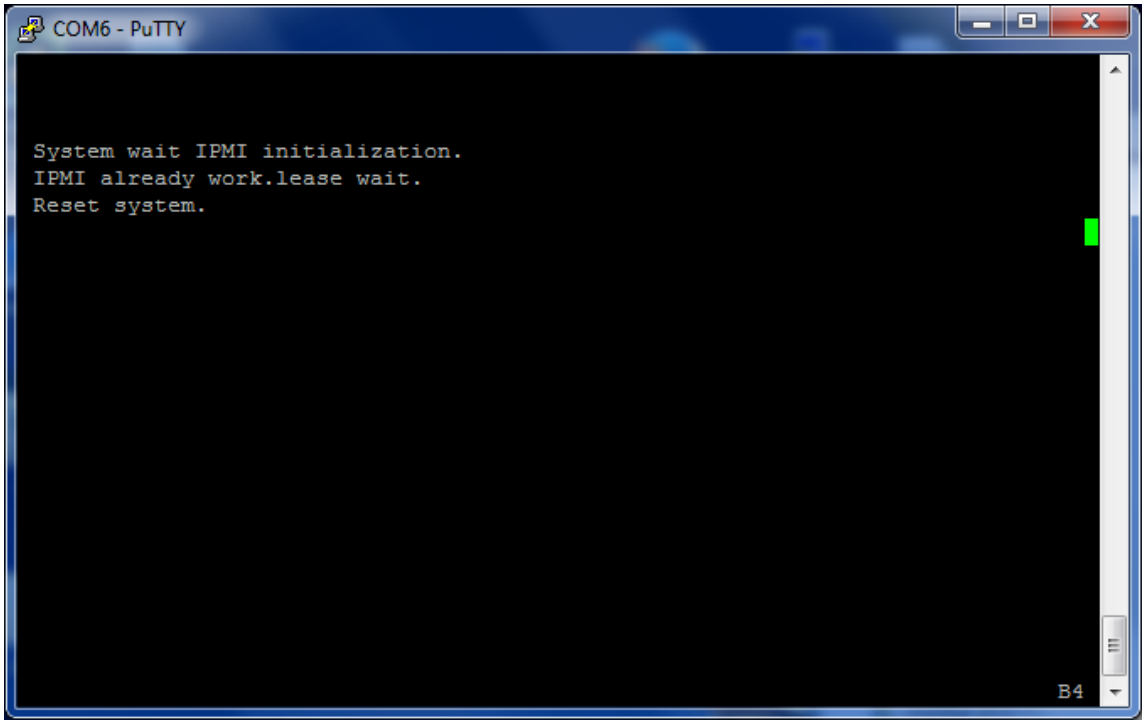


Wie konvertiert man mit einem USB-Stick

So rüsten Sie das Gerät mit einem USB-Stick auf:

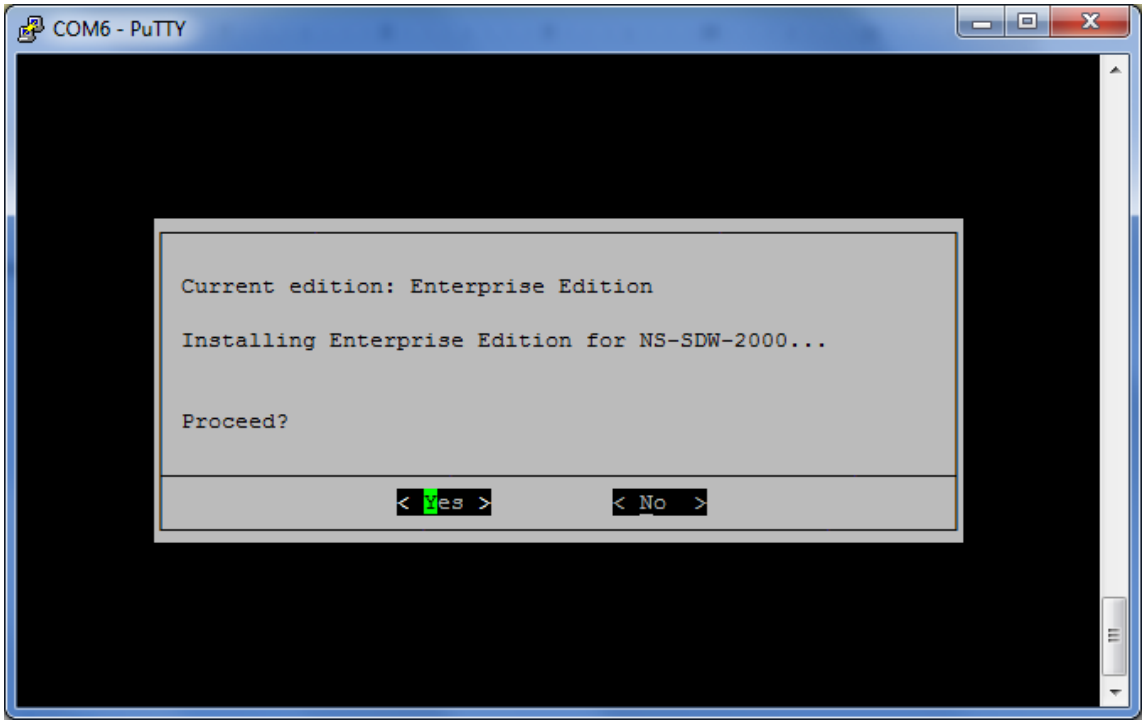
1. Stecken Sie den beiliegenden USB-Stick in die Citrix SD-WAN-Appliance.
2. Stellen Sie eine Verbindung zur seriellen Konsole des Geräts her.
3. Starten Sie die Appliance neu.
4. Wenn Sie während des Startvorgangs sehen, wie sich der Cursor über den Bildschirm bewegt, gehen Sie wie folgt vor:
   a) 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.

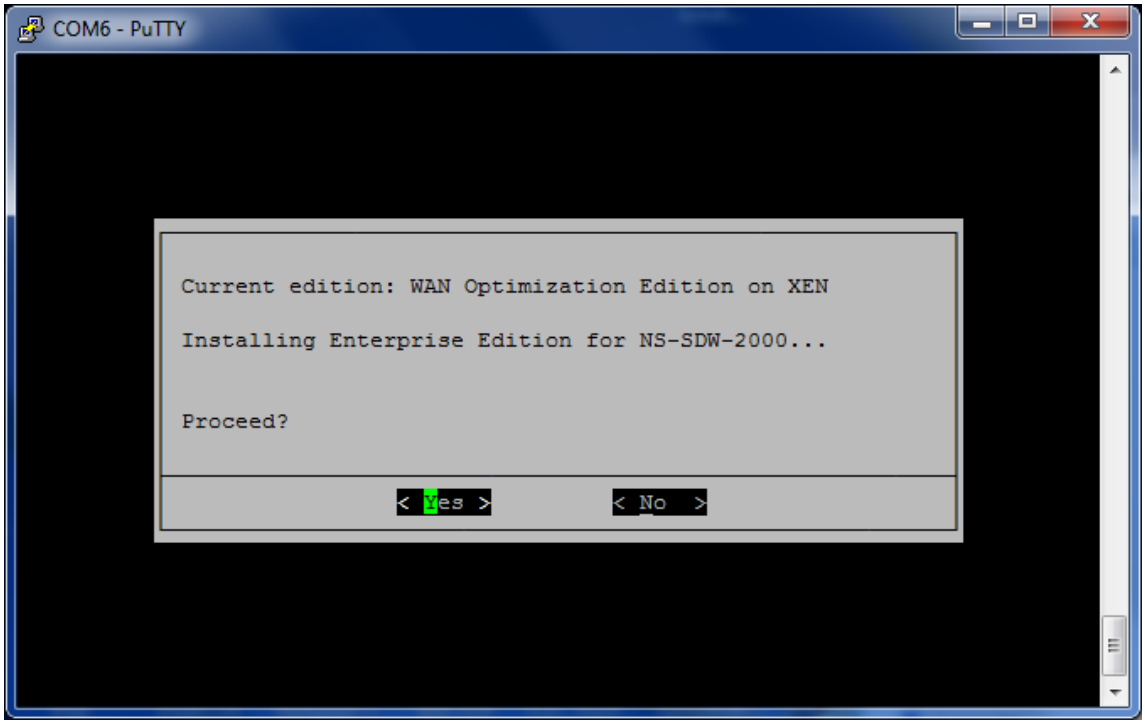
> **Hinweis**
>
> Die obigen Schritte sollten während des Neustarts der Appliance ausgeführt werden. Die Tastenanschläge sollten während der BIOS-Nachphase erfolgen, wie in Schritt 4 beschrieben.



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 es 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 dies bestätigen.





6. Wählen Sie auf Aufforderung die **Enterprise Edition**-Software-Upgrade-Option.
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 Platform Edition dauert der Upgrade-Prozess ungefähr 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; </en-us/citrix-sd-wan.html>.

Standard Edition in Premium Edition umwandeln

October 28, 2021

> **Wichtig**
>
> In Release-Version 10.1 wird die Plattform-Edition “Enterprise”in 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 **Change Management** herunter.

3. Aktualisieren Sie die Appliance mit dem heruntergeladenen Paket unter **Systemwartung** > **Update-Software** > **Reimage Virtual WAN Appliance**
4. Klicken Sie auf **Datei auswählen**, um die Datei *cb-vw_cb1000_x.x.x.x.tar.gz* bereitzustellen. 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

October 28, 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.

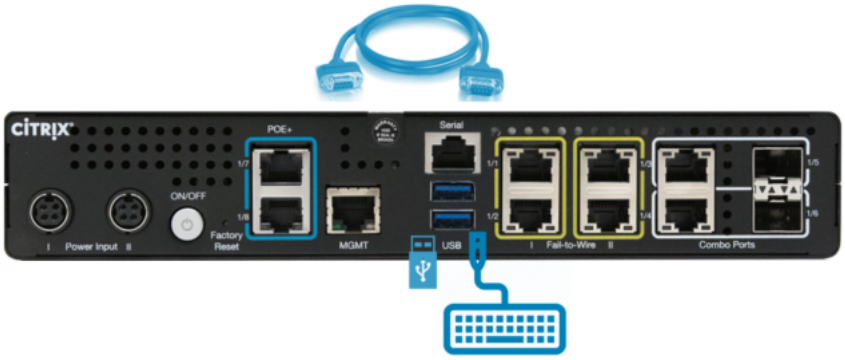
Die folgende Tabelle enthält Details zu den verfügbaren USB-FRU-Images und den von SD-WAN-Appliances unterstützten Editionen.

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

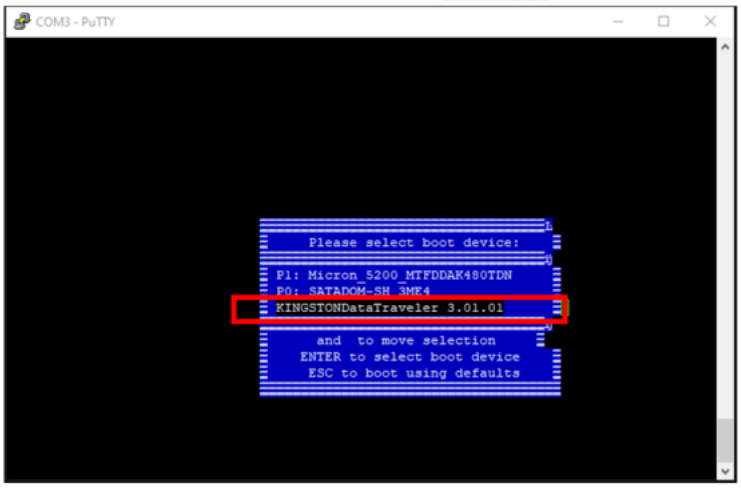
So führen Sie ein USB-Reimaging durch:

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.

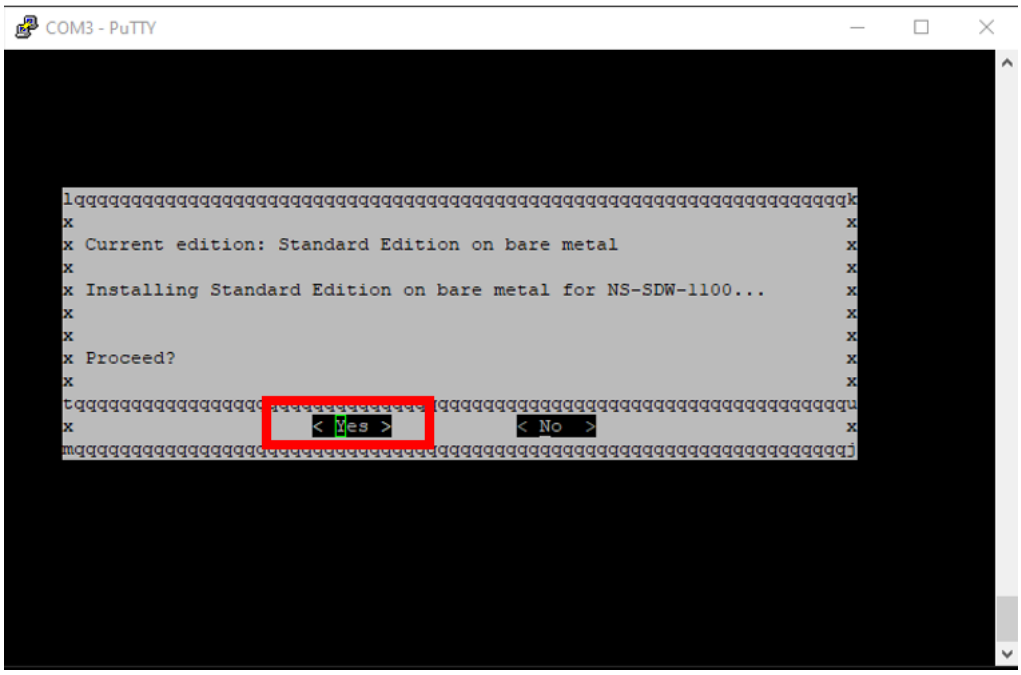
   > **Tipp**
   >
   > Wenn sich an der Appliance ein einzelner USB-Anschluss befindet, verwenden Sie einen USB-Splitter, um sowohl den USB-Stick als auch die USB-Tastatur anzuschließen.



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 **SHFT+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:

Ausgabebefehl '*management_ip*'

Ausgabebefehl '*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 finden Sie unter Edge-Sicherheit.

Citrix SD-WAN -Lizenzoptionen

October 28, 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 bei der Installation und Anwendung 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.

Unterstützung für Citrix SD-WAN Plattformsoftware

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-Optimierungsausgabe	Standard Edition	Premium Edition	Advanced Edition
Version 7.x	Ja	Nein	Nein	Nein
Veröffentlichung 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
Version 11.3	Ja	Ja	Ja	Ja

Informationen zum Anzeigen aller in Citrix SD-WAN Version 11.3 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 Bereitstellung von Lizenzen für SD-WAN-Plattform-Editionen umfasst 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 von Anwendungsfällen finden Sie im KB-Artikel CTX285157.

Lokale Lizenzierung

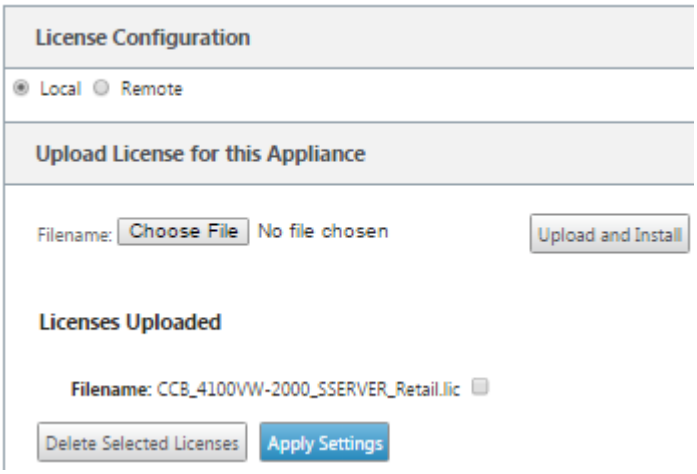
October 28, 2021

Mit der lokalen 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 Grace-Lizenz verfügbar. Sie müssen eine Lizenzdatei für eine aktive Netzwerkverbindung hochladen. Die Lizenzdateien werden basierend auf den Host-IDs der einzelnen Appliances generiert.

Sie können die Lizenz für SD-WAN-Appliances mithilfe der 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-Webmanagementschnittstelle zu **Configuration > Appliance Settings > Licensing**.
2. Wählen Sie **Local** und laden Sie die Lizenz hoch. Klicken Sie auf **Upload and Install**.
3. Speichern Sie Ihre Änderungen, indem Sie auf **Apply Settings** klicken.



Remotelizenzierung

October 28, 2021

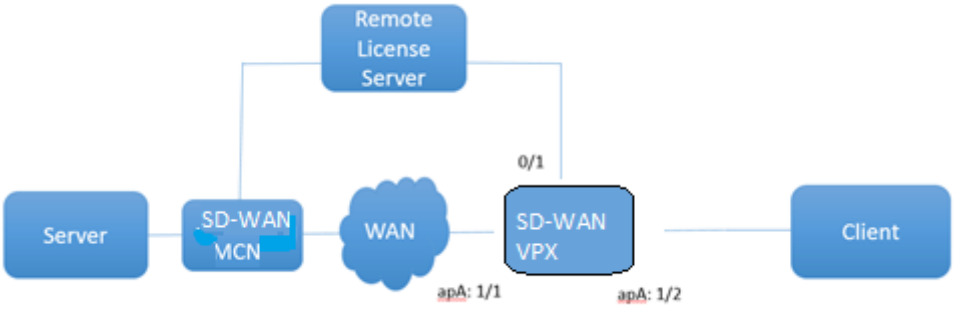
Voraussetzungen für die Verwendung von Remotelizenzserver für SD-WAN-Appliances.

- NTP muss sowohl für Lizenzserver als auch für SD-WAN konfiguriert sein (Datum und Uhrzeit müssen synchron sein)

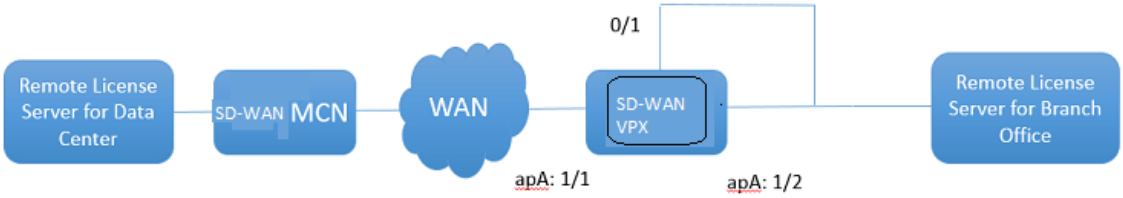
- Es wird empfohlen, die neueste Lizenzserverversion zu verwenden:
  - Release 9.1, 9.2: 11.13.1 L.S
  - Release 10.0, 10.1, 10.2, 11.0, 11.0.1, 11.0.2: 11.14.1 L.S
  - Release 11.0.3, 11.1, 11.2: 11.16.3 L.S

Anwendungsfälle:

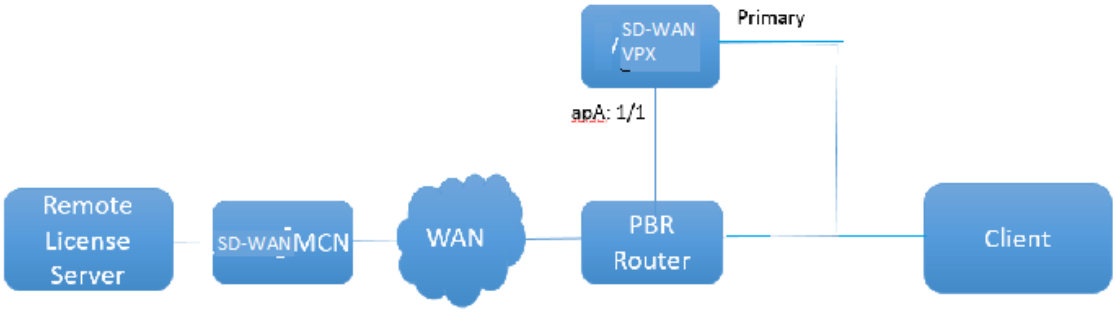
1. Remote-Lizenzserver, der über das Verwaltungsnetzwerk erreichbar ist, ohne Daten/apA-Ports zu verwenden.



2. Remote-Lizenzserver im Zweignetzwerk.

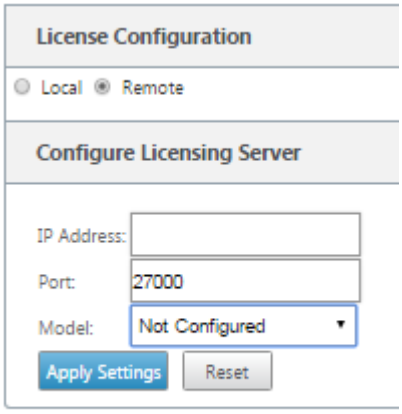


3. SD-WAN VPX-SE - PBR-Bereitstellung in der Zweigstelle.

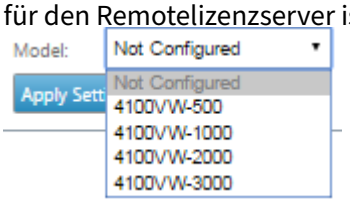


Remotelizenz:

1. Navigieren Sie in der SD-WAN-Webmanagementschnittstelle zu **Configuration > Appliance Settings > Licensing**.
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 Remotelizenzserver ist 27000.



> **Wichtig**
>
> - Wenn Sie Remotelizenzen für SD-WAN-Appliance mit SD-WAN Center installieren möchten, stellen Sie sicher, dass Sie die zentralisierte Lizenzierung auf der SD-WAN MCN-Appliance in den globalen Einstellungen des SD-WAN Web Management Interface Configuration Editor aktivieren.
> - Citrix SD-WAN Center unterstützt keine IPv6-Adresse.

Zentrale Lizenzierung

October 28, 2021

Da die Netzwerkbereitstellungen mit einer großen Anzahl von Netzwerkknoten wachsen, wird die Verwaltung und Lizenzierung von Appliances umständlich. Um diesen Prozess für das effiziente Onboarding der SD-WAN-Appliances und den einfachen Netzwerkbetrieb zu vereinfachen, wurde ein zentralisiertes Lizenzierungsmodell für das SD-WAN-Netzwerk eingeführt.

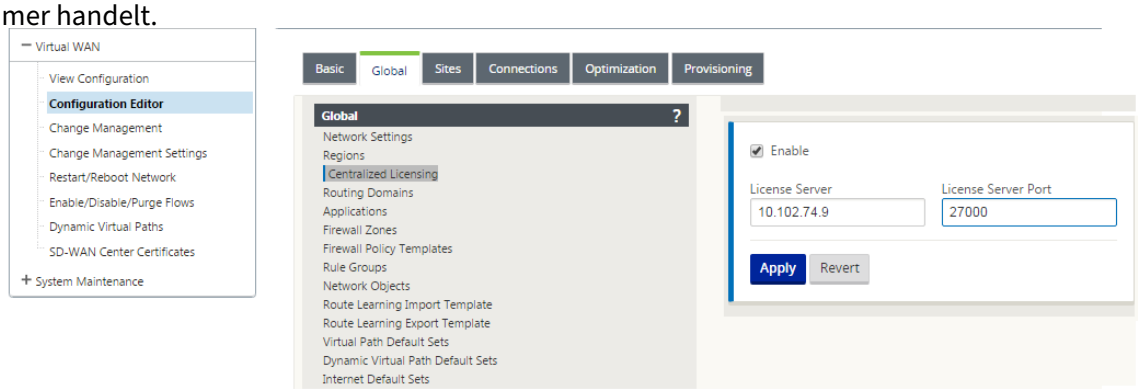
In dem neuen zentralisierten Lizenzmodell bietet die Webmanagement-Schnittstelle des SD-WAN Centers (SD-WAN Appliance Management and Reporting Portal) Lizenzierungsdienste für einzelne SD-WAN-Appliances im Netzwerk, ohne dass Sie sich bei der Appliance anmelden müssen.

Die IP-Adresse des SD-WAN-Centers wird in der GUI der SD-WAN-Appliance unter **Global > Zentralisierte Lizenzierung**bereitgestellt. Diese IP-Adresse wird über die Konfigurationspakete oder Updates an einzelne Appliances weitergegeben. Wenn die IP-Adresse geändert wird, müssen Sie den Change Management-Prozess durchlaufen, um die Appliances zu übertragen. Die globale Einstellung kann durch die lokalen Site-Einstellungen außer Kraft gesetzt werden.

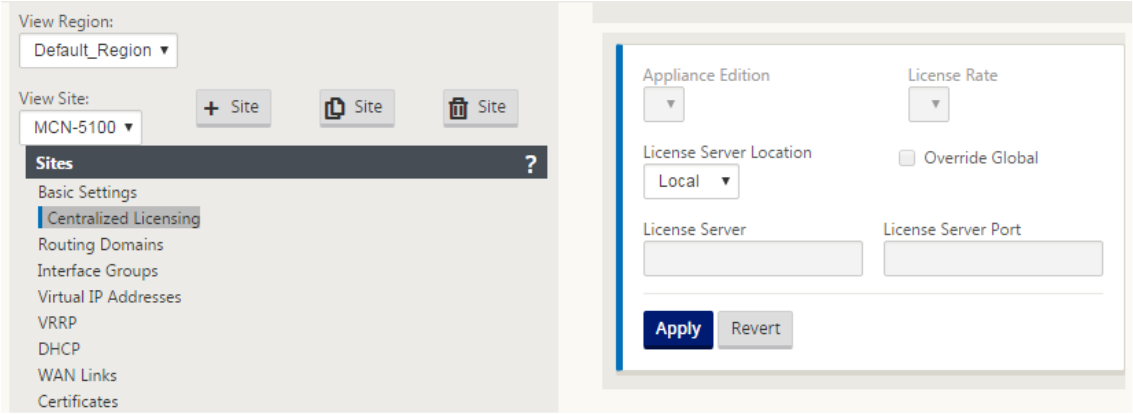
Die Lizenzbandbreite kann mit dem Appliance-Modell für Site-Einstellungen ausgewählt werden. Die WAN-Links-Bandbreite wird anhand der ausgewählten Lizenz geprüft.

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

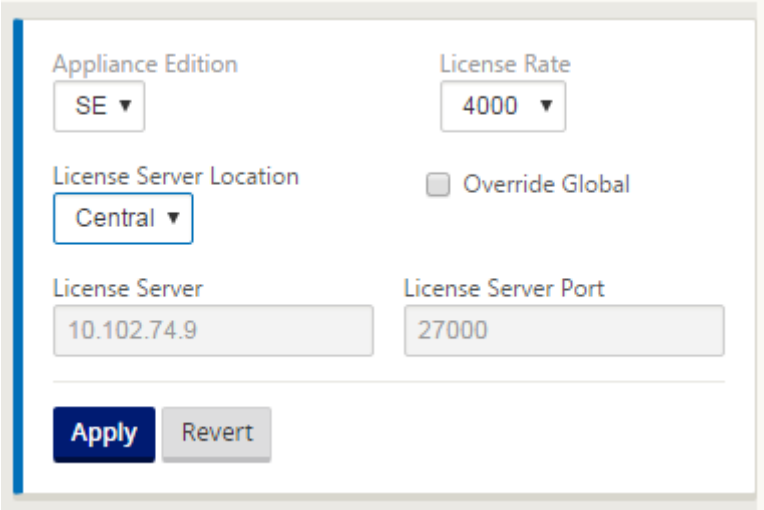
1. Navigieren Sie zu **Konfiguration** > **Virtuelles WAN** > **Konfigurationseditor** Öffnen Sie ein virtuelles WAN-Konfigurationspaket oder erstellen Sie ein neues. Das Konfigurationspaket wird geöffnet.
2. Navigieren Sie zur Registerkarte **Global**. Wählen Sie **Zentralisierte Lizenzierung aus**. 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 IP-Adresse des SD-WAN Center-Managements an, damit das Konfigurationspaket für den SD-WAN MCN oder Zweigstellengeräte die Lizenz von SD-WAN Center herunterladen kann.
4. Geben Sie **27000** für den **License Server Port** ein, bei dem es sich um eine Standardportnummer handelt.



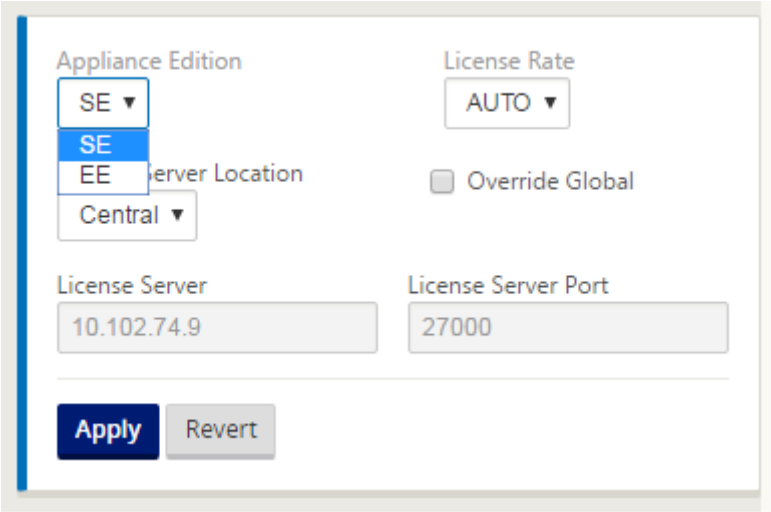
5. Klicken Sie auf **Apply**.
6. Navigieren Sie zur Registerkarte **Sites**. Wählen Sie MCN oder Zweigstandort unter **Standort anzeigen**aus, abhängig von der Region und dem Standort, für den Sie die zentrale Lizenzierung verwalten möchten.
7. Wählen Sie **Zentralisierte Lizenzierung aus**. Die Optionen für die zentralen Lizenzierung werden angezeigt. Standardmäßig ist die Option **Lokal** für den **Standort des Lizenzservers**ausgewählt.



8. Klicken Sie auf das Dropdownmenü und wählen Sie **Central**, um den Standardort 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. Zum Beispiel; Der Lizenzserver könnte die IP-Adresse des SD-WAN Center sein, das die Appliances im Netzwerk verwaltet.

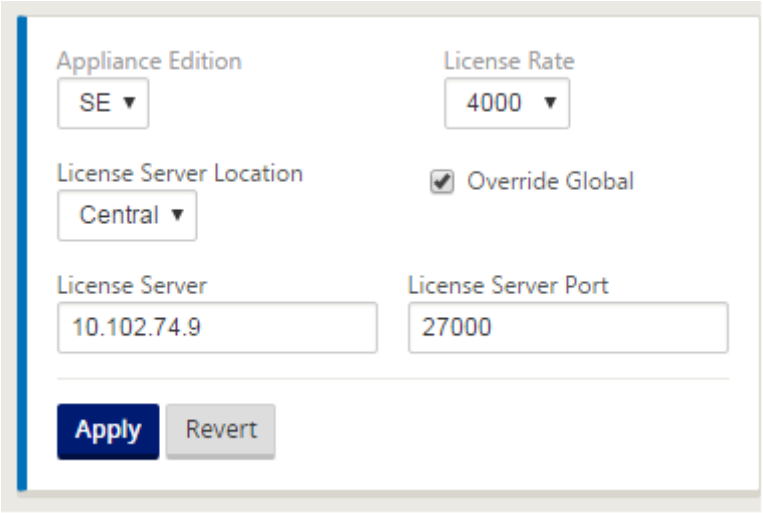


9. Wählen Sie die **Appliance Edition** und den **Lizenzpreis** abhängig von den zu installierenden Appliances. Klicken Sie auf **Übernehmen**.



Hinweis: Sie können die in den globalen Einstellungen der Konfiguration bereitgestellten Lizenzserverinformationen außer Kraft setzen.

10. Wählen Sie **Global überschreiben** aus, 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 Zweigstellen und MCN-Sites verwalten, die für ein bestimmtes SD-WAN-Appliance-Konfigurationspaket von dem von Ihnen konfigurierten Lizenzierungsserver aus konfiguriert sind.

Der Lizenzserver kann ein SD-WAN Center-Verwaltungsportal sein, das über den Änderungsmanagementprozess Lizenzen von der Netzwerkkonfiguration an die Standorte erwirbt.

Lizenz basierend auf Bandbreitenzuweisung:

Jede Appliance kann eine Lizenz mit einer Bandbreitenstufe wählen, die größer oder gleich der konfigurierten Bandbreite ist. Wenn die konfigurierte Bandbreitenlizenz nicht verfügbar ist, wird die

Möglichkeit für eine Appliance hinzugefügt, die nächsthöhere Bandbreitenlizenz auszuwählen. Diese Funktion gilt sowohl für die zentrale als auch für die Remotelizenzserverfunktionalität. Beispiel:

- Wenn Sie drei Lizenzen mit 410—200 Mbit/s 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 alle Lizenzen mit 410—200 Mbit/s verwenden können.
- Wenn Sie jeweils eine Lizenz mit einer Lizenz von 410-20 Mbit/s und einer Lizenz von 410—200 Mbit/s haben. Standort A ist so konfiguriert, dass er 50 Mbit/s verbraucht, dann kann Standort A eine Lizenz von 410—200 Mbit/s verwenden.

Nachfrist der Lizenz:

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

> **Hinweis**
>
> Wenn der ausgewählte Lizenzsatz nicht mit der konfigurierten WAN-Link-Rate übereinstimmt, wird die folgende Meldung auf der Appliance-GUI für Lizenzierungsereignisse angezeigt.
>
> Meldung: Die konfigurierte zulässige Gesamtrate (LAN zu WAN) NNNN (Kbps) darf das Doppelte der Lizenzrate nicht überschreiten, die NNNN (Kbps) ist
>
> Schweregrad: WARNUNG
>
> Ereignisse: Syslog, E-Mail

Verwalten von Lizenzen

October 28, 2021

Citrix SD-WAN-Appliance-Lizenzen werden durch Kommunikation mit dem Remote-Lizenzdienst verwaltet, um nach Lizenzen zu suchen. Wenn die Appliance lizenziert ist, wird der Netzwerkbetrieb ohne Unterbrechung fortgesetzt. Wenn die Appliance nicht lizenziert ist, wird der Grace-Lizenzmodus initiiert.

SD-WAN-Appliance-Lizenzverwaltungsprozess:

1. Jede Site kommuniziert mit Remote Server oder SD-WAN Center über das Web-Management-Interface. 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 das Gerät in einen Grace-Modus. Die Checkout-Methode bestimmt den Lizenzstatus. Dieser Status kann "Real" , "Grace"oder "Verweigert"lauten, die vom SD-WAN Center an die Appliance gesendet werden. Jedes Mal, wenn eine Appliance das SD-WAN Center für den Lizenzstatus erreicht, wird die neue Lizenz eingecheckt 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 Schonfrist beträgt 30 Tage, daher geht das Gerät nach dem Verlust von 2 Herzschlägen in die Kulanzzeit über. Während dieser 30 Tage muss die Kommunikation wiederhergestellt werden. Nach der Wiederherstellung kehrt das Gerät in den normalen Betriebsmodus zurück. Wenn die Kommunikation NICHT wiederhergestellt wird, wird die Appliance in den nicht lizenzierten Zustand versetzt und folgt dem Verfahren zum Ablauf unlizenziert/ des Lizenzablaufs.

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

- Die MCN-Appliance hat keine anfängliche Nachfrist. Es muss lizenziert sein, um aufzutauchen.

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

- Der Client-Knoten verfügt über eine 30-tägige Nachfrist mit oder ohne ZTD-Funktionalität.
- Die Appliance ist mit einer 30 Tage gültigen OOB-Lizenzdatei aktiviert.
- Sie haben 30 Tage Zeit, um eine Lizenzdatei hochzuladen oder sich über den zentralisierten Lizenzserver lizenzieren zu lassen.
- Wenn das Gerät lizenziert ist, funktioniert es 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

October 28, 2021

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

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

Die zentralisierte Lizenzierung verfügt über eine Protokolldatei, um das Funktionieren von Nachfrist, nicht lizenziert, lizenziert, Kommunikationsstatus und Ausfällen zu verfolgen.

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

Gnadenfrist:

1. Für Out-of-Box-Client-Knoten wird eine 30-tägige Kulanzfrist bereitgestellt. Die Benachrichtigung zeigt an, dass sich die Appliance im Out-of-Box-Modus befindet und eine gültige Lizenz benötigt. Diese Option verwendet eine Grace-Lizenzdatei.
2. Ablauf der Lizenz: Nach Ablauf der Lizenz wird eine 30-tägige Nachfrist gewährt. Die Benachrichtigung zeigt an, dass der Grund für die Nachfrist der Ablauf der Lizenz ist und eine Verlängerung erforderlich ist.
3. Verlust der Kommunikation mit dem SD-WAN Center: Nach 2 Herzschlägen geht die Appliance 30 Tage lang in den Kulanzmodus. Die Benachrichtigung zeigt an, dass der Grund für die Nachfrist ein Kommunikationsfehler ist.

Konfiguration

October 28, 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 Upgrade-Verfahren 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.

Zweig konfigurieren: Das Verfahren zum Hinzufügen eines Zweigstandorts ähnelt dem Erstellen und Konfigurieren des MCN-Standorts. Einige Konfigurationsschritte und -einstellungen unterscheiden sich jedoch geringfügig für einen Zweigstandort. Sobald Sie einen ersten Zweigstandort hinzugefügt haben, können Sie außerdem für Standorte mit demselben Appliance-Modell die Funktion **Klonen**

(Duplizieren) verwenden, um den Prozess des Hinzufügens und Konfigurierens dieser Sites zu optimieren. Wie beim Erstellen des MCN-Standorts müssen Sie zum Einrichten eines Zweigstandorts den **Konfigurationseditor** im Management-Webinterface auf der MCN-Appliance verwenden. Der **Konfigurationseditor** ist nur verfügbar, wenn die Schnittstelle auf den **MCN-Konsolenmodus** eingestellt ist.

Konfigurieren Sie den virtuellen Pfad zwischen MCN und Zweigstandorten: Konfigurieren Sie den Virtual Path Service zwischen dem MCN und jedem der Clientstandorte (Zweigstellen). 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.

> **HINWEIS**
>
> Citrix SD-WAN Orchestrator-Dienste unterstützen keine IPv6-Adressen.

Die folgenden Funktionen von Citrix SD-WAN Appliances unterstützen die IPv6-Adresse von Citrix SD-WAN 11.3 Release:

- Funktionen der Managementebene
  - Verwaltungsoberfläche
  - RADIUS-Server
  - TACACS+ Server
  - SMTP-Server
  - syslog-Server
  - HTTP-Server
  - DNS-Server
  - App-Flow/IPFIX
  - SNMP
  - Remotelizenzierung
  - Zentrale Lizenzierung
  - NTP-Server
  - Positivliste
  - Neue Benutzeroberfläche für SD-WAN-Appliances
  - Diagnose

  > **HINWEIS Wenn Sie**
  >
  > nach der Konfiguration der oben aufgeführten Funktionen mit der Management-IPv6-

> Adresse das IPv6-Protokoll unter **Appliance-Einstellungen > Netzwerkadapter** deaktivieren, funktionieren die Funktionen nicht wie erwartet.

- Merkmale der Datenebene
  - Statisches Routing
  - Internetdienst über IPv6-WAN-Verbindungen
  - Intranetdienst über IPv6-WAN-Verbindungen
  - Router-Werbung
  - DHCP-Kunde
  - DHCP-Server/Relay
  - Anwendung QoS
  - Firewall
  - Inband-Verwaltung
  - Hohe Verfügbarkeit
  - IP-Regeln
  - IPv6 wird über LTE-Verbindungen unterstützt

> **HINWEIS**
>
> IPv6-Adressen werden in den folgenden Konfigurationen nicht unterstützt:
>
> - Dynamisches Routing (OSPF/BGP)
> - Redundanzprotokoll für virtuelle Router
> - Unterstützung für Premium-Edition oder Zwei-Box
> - Direkte Cloud
> - VNF/Firewall von Drittanbietern
> - Netflow
> - Header-Komprimierung für IPv6-Pakete
> - Anwendungs-Routing
> - Office-365-Unterstützung
> - Präfix-Delegierungsgruppe

Erstinstallation

September 26, 2023

Diese Verfahren müssen für jede Appliance abgeschlossen sein, die Sie zu Ihrem SD-WAN hinzufügen möchten. Folglich erfordert dieser Prozess eine gewisse Abstimmung mit Ihren Site-Administratoren

in Ihrem gesamten Netzwerk, um sicherzustellen, dass die Appliances zum richtigen Zeitpunkt vorbereitet und einsatzbereit sind. Sobald der Master Control Node (MCN) konfiguriert und bereitgestellt ist, können Sie Ihrem SD-WAN jederzeit Client-Appliances (Client-Knoten) hinzufügen.

Für jede Appliance, die Sie zu Ihrem virtuellen WAN hinzufügen möchten, müssen Sie Folgendes tun.

1. Richten Sie die SD-WAN Appliance-Hardware und alle virtuellen SD-WAN VPX-Appliances (SD-WAN VPX-VW) ein, die Sie bereitstellen werden.
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. Stellen Sie den **Timeout-Schwellenwert** für die Konsolensitzung auf einen hohen oder den Maximalwert ein.

   > **Warnung**
   >
   > Wenn Ihre Konsolensitzung abläuft oder Sie sich vor dem Speichern Ihrer 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 dringend empfohlen, das **Timeout-Intervall** der Konsolensitzung auf einen hohen Wert festzulegen, wenn Sie ein Konfigurationspaket erstellen oder ändern oder andere komplexe Aufgaben ausführen.

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.

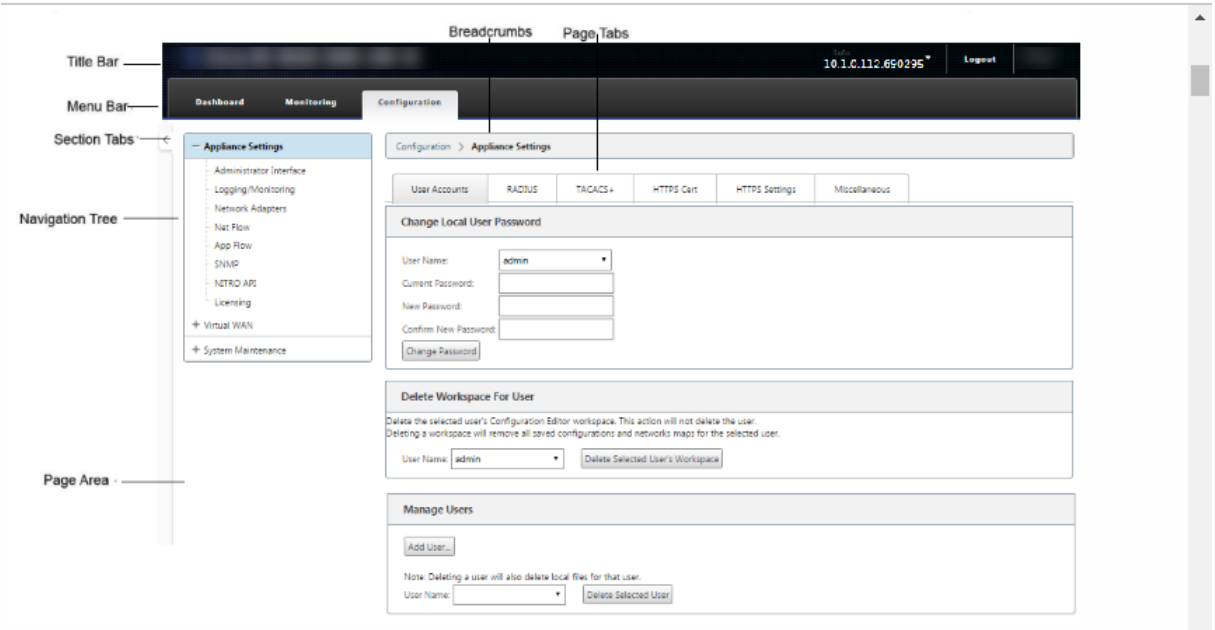
Übersicht über das Layout des Web Interface (UI)

October 28, 2021

Dieser Abschnitt enthält grundlegende Navigationsanweisungen und eine Navigations-Roadmap der Seitenhierarchie der SD-WAN-Webverwaltungsoberfläche. Außerdem werden spezielle Navigationsanweisungen für den **Konfigurationseditor** und den **Änderungsverwaltungsassistenten**bereitgestellt

Basic Navigation

Die folgende Abbildung zeigt die grundlegenden Navigationselemente des Web Management Interface und die Terminologie, mit der sie identifiziert wurden.



Die grundlegenden Navigationselemente lauten wie folgt:

- **Titelleiste** —Zeigt die Modellnummer der Appliance, die 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 auf jedem Management-Webinterface-Bildschirm unter der Titelleiste angezeigt wird. Dies enthält die Abschnittsregisterkarten zum Anzeigen des Navigationsbaums und Seiten für einen ausgewählten Abschnitt.
- **Abschnittsregisterkarten** —Die Abschnittsregisterkarten befinden sich in der Hauptmenüleiste oben auf der Seite. Dies sind die Top-Level-Kategorien für die Seiten und Formulare des Web Management Interface. 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. Dadurch 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 Navigationsmöglichkeiten:
  - Klicken Sie auf eine Abschnittsregisterkarte, um den Navigationsbaum und die Seitenhierarchie für diesen Abschnitt anzuzeigen.

  - Klicken Sie neben einem Zweig im Baum auf + (Pluszeichen), um die verfügbaren Seiten für dieses Zweigthema anzuzeigen.
  - Klicken Sie auf einen Seitennamen, um diese Seite im Seitenbereich anzuzeigen.
  - Klicken Sie —(Minuszeichen) neben einem Zweiggegenstand, um die Filiale zu schließen.

- **Brotkrumen** —Dies zeigt den Navigationspfad zur aktuellen Seite an. Die Brotkrumen befinden sich oben auf dem 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 zum Anzeigen weiterer untergeordneter Seiten für dieses Thema oder Konfigurationsformular. Diese befinden sich oben im Seitenbereich, direkt unter den Breadcrumbs. Manchmal (wie beim **Änderungsmanagement-Assistenten**) befinden sich Registerkarten im linken Bereich des Seitenbereichs zwischen dem Navigationsbaum und dem Arbeitsbereich der Seite.
- **Größenänderung des Seitenbereichs -** Bei einigen Seiten können Sie die Breite des Seitenbereichs (oder der Abschnitte davon) vergrößern oder verkleinern, um mehr Felder in einer Tabelle oder einem Formular anzuzeigen. In diesem Fall befindet sich am rechten Rand eines Seitenbereichs, eines Formulars oder einer Tabelle eine graue, vertikale Größenänderungsleiste. Bewegen Sie den Cursor über die Größenänderungsleiste, bis sich der Cursor in einen bidirektionalen Pfeil verwandelt. Klicken und ziehen Sie dann die Leiste nach rechts oder links, um die Bereichsbreite 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.

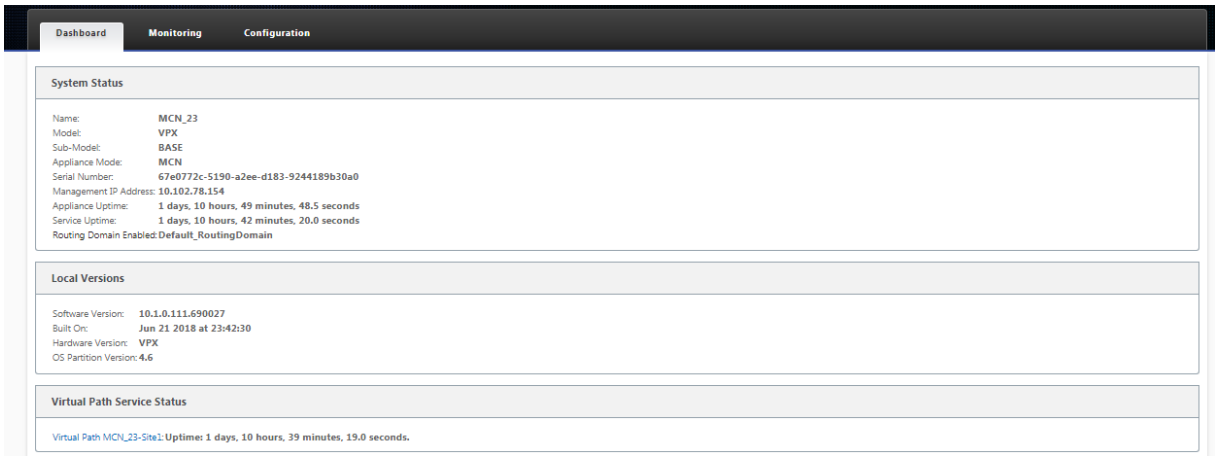
Dashboard für die Webmanagement-Benutzeroberfläche

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

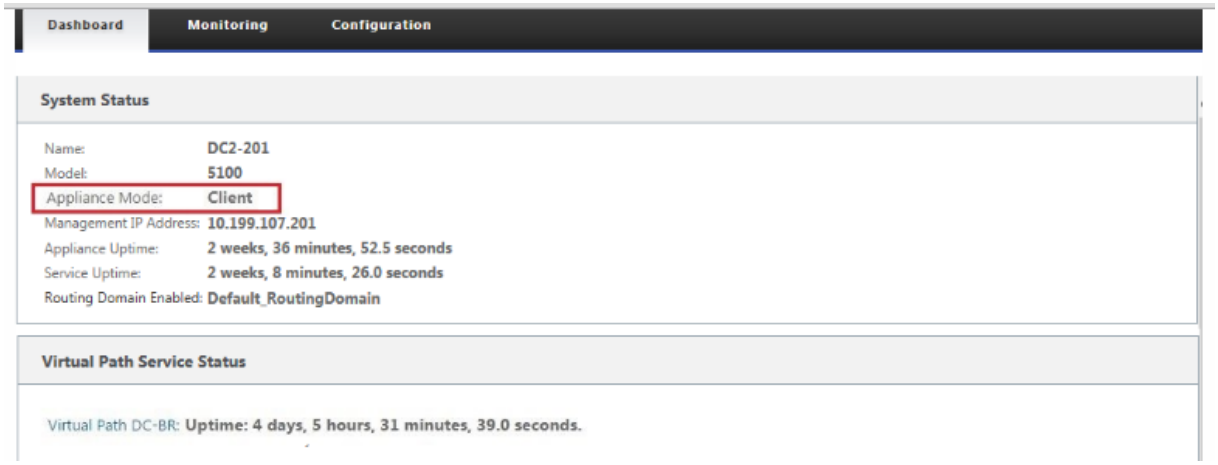
Auf der Seite **Dashboard** werden die folgenden grundlegenden Informationen für die Appliance angezeigt:

- Systemstatus
- Status des virtuellen Pfaddienstes
- Versionsinformationen zum lokalen Appliance-Softwarep

Die folgende Abbildung zeigt ein Beispiel für eine Master Control Node (MCN)-Appliance-**Dashboard**-Anzeige.



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



Konfigurationseditor

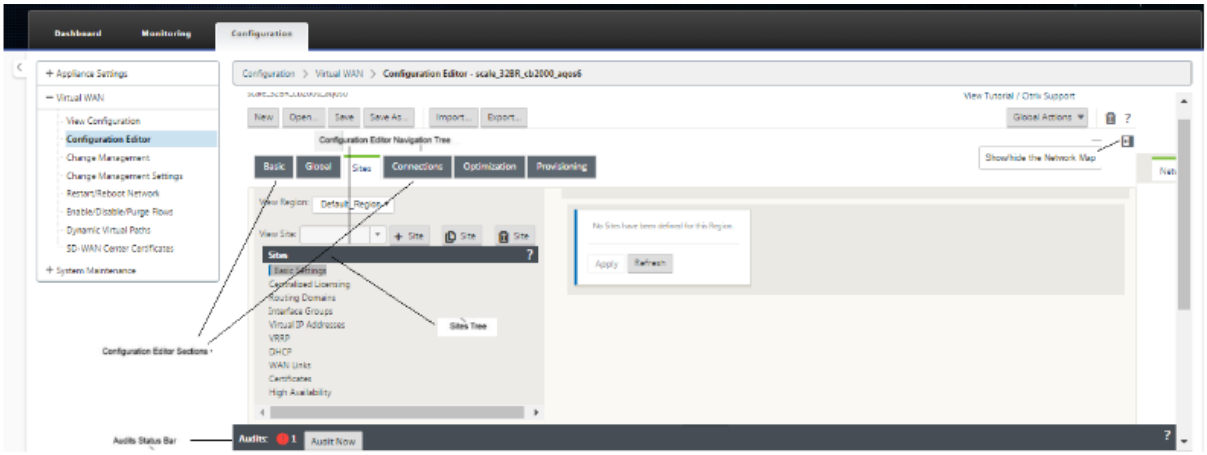
Mit dem Konfigurationseditor können Sie Virtual WAN-Appliance-Standorte, Verbindungen, Optimierung und Provisioning hinzufügen und konfigurieren sowie die Virtual WAN-Konfiguration erstellen und definieren.

Der Konfigurationseditor ist nur verfügbar, wenn sich die Webverwaltungsschnittstelle im MCN-Konsolenmodus befindet. Standardmäßig ist das Webinterface auf einer neuen Appliance auf den Clientmodus eingestellt. Sie müssen die Moduseinstellung auf MCN-Konsole ändern, bevor Sie auf den Konfigurationseditor zugreifen können. Anweisungen hierzu finden Sie im Abschnitt Umschalten des Management-Webinterface in den MCN-Konsolenmodus.

Gehen Sie wie folgt vor, um zum **Konfigurationseditor**zu navigieren:

1. Melden Sie sich auf der MCN-Appliance beim Web Management Interface an.1. Wählen Sie die Registerkarte **Konfiguration**. Klicken Sie im Navigationsbaum neben dem **Virtual WAN**-Zweig im Baum auf **+**. Dadurch werden die verfügbaren Seiten für die Kategorie **Virtual WAN** angezeigt. Wählen Sie im Zweig Virtual WAN des Baums den **Konfigurationseditor** aus.

   In der folgenden Abbildung werden die grundlegenden Navigations- und Seitenelemente des **Konfigurationseditors** sowie die zu ihrer Identifizierung verwendete Terminologie beschrieben.



Im Folgenden werden die primären Navigationselemente des **Konfigurationseditors** beschrieben, auf die in diesem

- **Menüleiste des Konfigurationseditors** - Dies befindet sich oben im Seitenbereich, direkt unter den Breadcrumbs-Links. Die Menüleiste enthält die primären Aktivitätsschaltflächen für **Konfigurationseditor**-Operationen. Zusätzlich befindet sich am äußersten rechten Rand der Menüleiste die Linkschaltfläche **Tutorial anzeigen**, um das Tutorial zum **Konfigurationseditor** zu starten. Das Tutorial führt Sie durch eine Reihe von Blasenbeschreibungen für jedes Element der Anzeige des **Konfigurationseditors**.
- **Abschnittsbaum des Konfigurationseditors** —Dies ist der Stapel dunkelgrauer Balken, der sich im linken Bereich des Seitenbereichs des **Konfigurationseditors** befindet. Jeder graue Balken repräsentiert einen Abschnitt auf oberster Ebene. Klicken Sie auf einen Abschnittsnamen, um die Unterzweige für diesen Abschnitt anzuzeigen.
- **Abschnitte Baumzweige** —Klicken Sie im Abschnittsbaum auf einen Abschnittsnamen, um einen Abschnittszweig zu öffnen. Jeder Abschnittszweig enthält einen oder mehrere Unterzweige von Konfigurationskategorien und Formularen, die wiederum mehr untergeordnete Zweige und Formulare enthalten können.
- **Sites-Baum** —Hier werden die Site-Knoten aufgeführt, die zu der Konfiguration hinzugefügt wurden, die derzeit im **Konfigurationseditor**geöffnet ist. Im Abschnittsbaum. Klicken Sie auf einen Site-Namen, um den Zweig für diese Site zu öffnen. Klicken Sie auf die Site, um eine

Filiale zu schließen. Ausführliche Anweisungen zum Navigieren und Verwenden der **Sites-Baumstruktur** und der Konfigurationsformulare finden Sie in den folgenden Abschnitten:

  - Einrichten des Master Control Node (MCN) -Sites
  - Hinzufügen und Konfigurieren der Zweigstandorte

- **Statusleiste für Audits** —Dies ist der dunkelgraue Balken am unteren Rand der Seite "**Konfigurationseditor**", der sich über die gesamte Breite des Bildschirms "Management-Webinterface" erstreckt. Die Statusleiste "**Audits** "ist nur verfügbar, wenn der **Konfigurationseditor** 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 ungelösten Audit-Warnungen für diese Konfiguration anzuzeigen.

Änderungsmanagement-Assistenten

Die **Änderungsmanagement-Assistenten** führen Sie durch den Prozess des Hochladens, Herunterladens, Stagens und Aktivierens der Virtual WAN-Software und -Konfiguration auf der Master Control Node (MCN) -Appliance und den Client-Appliances. Es gibt zwei Versionen des **Änderungsmanagement-Assistenten**, eine für systemweites ("globales") Virtual WAN-Änderungsmanagement und eine für das lokale Änderungsmanagement, wie folgt:

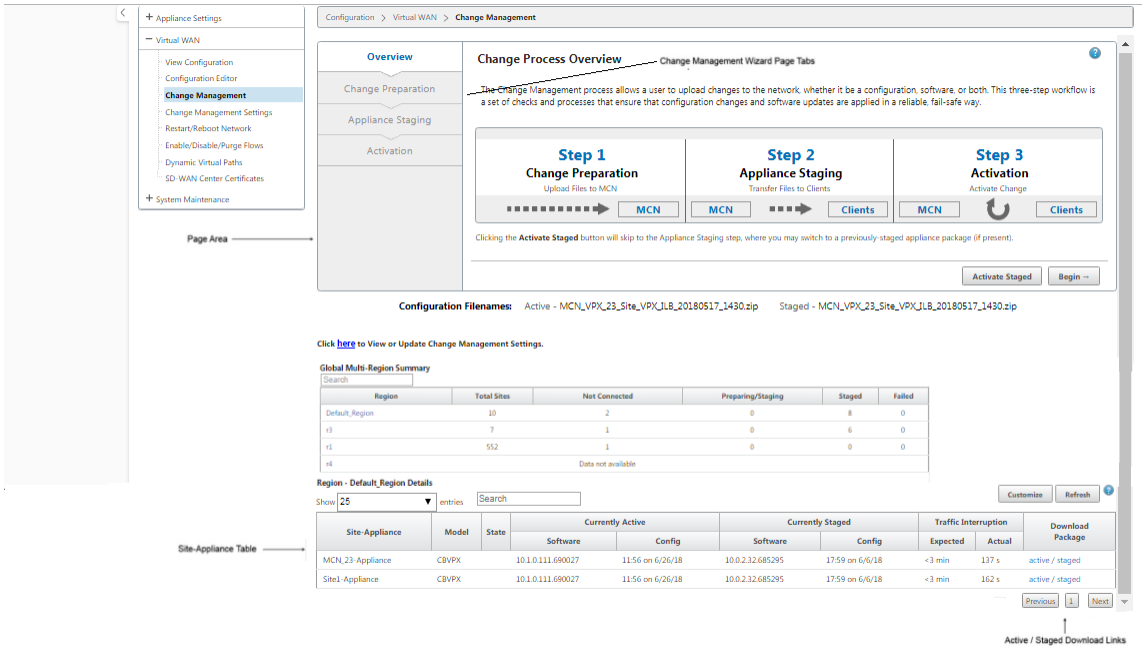
- **MCN (Global) Change Management-Assistent** —**Der globale MCN Change Management-Assistent** ist die primäre (Haupt-) Version und nur im Web Management Interface der MCN Appliance verfügbar. Verwenden Sie diese, um die Virtual WAN-Appliance-Pakete zu generieren, die für jeden Typ von Virtual WAN Appliance 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 globalen **MCN-Änderungsmanagement-Assistenten** zum Erstellen der Appliance-Pakete finden Sie im Abschnitt Vorbereiten der Virtual WAN Appliance-Pakete auf dem MCN.
- **Assistent für lokales Änderungsmanagement** —**Der Assistent für die lokale Änderungsverwaltung** ist im Web Management Interface verfügbar, das sowohl auf dem MCN als auch auf allen Clientknoten-Appliances ausgeführt wird. Verwenden Sie diese Option, um das entsprechende Virtual WAN-Appliance-Paket, das Ihrem virtuellen WAN hinzugefügt werden soll, auf eine lokalen Appliance hochzuladen, ein Staging durchzuführen und es zu aktivieren. Sie können diesen Assistenten auch verwenden, um ein aktualisiertes Appliance-Paket speziell auf den lokalen MCN oder auf eine einzelne lokale virtuelle WAN-Appliance hochzuladen, die bereits in Ihrem Netzwerk bereitgestellt ist.

Verwenden des globalen MCN-Änderungsmanagement-Assistenten

Gehen Sie wie folgt vor, um den globalen **MCN-Änderungsmanagement-Assistenten** zu öffnen:

1. Melden Sie sich beim Web Management Interface auf der MCN-Appliance an.
2. Wählen Sie die Registerkarte **Konfiguration** aus. Klicken Sie im Navigationsbaum neben dem **Virtual WAN**-Zweig im Baum auf **+**.
3. In dem Zweig **Virtual WAN**. Wählen Sie **Änderungsmanagement**aus.

   Daraufhin wird die erste Seite des **Änderungsmanagement-Assistenten** angezeigt, die Seite "**Change Process Overview**", wie in der folgenden Abbildung dargestellt.



4. Um den Assistenten zu starten, klicken Sie auf **Beginnen**.

   Vollständige Anweisungen zur Verwendung des Assistenten zum Hochladen, Stagen 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 **Änderungsmanagement-Assistent** enthält die folgenden Navigationselemente:

- **Seitenbereich**—Hier werden die Formulare, Tabellen und Aktivitätsschaltflächen für jede Seite des **Änderungsverwaltungs-Assistenten** angezeigt.
- **Seitenregisterkarten des Änderungsverwaltungsassistenten** —Die Seitenregisterkarten befinden sich im linken Bereich des Seitenbereichs auf jeder Seite des Assistenten. Reg-

isterkarten werden in der Reihenfolge aufgeführt, in der die entsprechenden Schritte im Assistentenprozess 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 weist auf eine inaktive Registerkarte hin. Registerkarten sind inaktiv, bis alle Abhängigkeiten (vorherige Schritte) fehlerfrei erfüllt wurden.

- **Tabelle "Appliance-Site** "—Dies befindet sich auf den meisten Seiten des Assistenten am Ende des Seitenbereichs des Assistenten. Die Tabelle enthält Informationen zu jeder konfigurierten Appliance-Site und Links zum Herunterladen der aktiven oder bereitgestellten Appliance-Pakete für dieses Appliance-Modell und die Site. Ein Paket in diesem Zusammenhang ist ein Zip-Dateibündel, das das entsprechende SD-WAN-Softwarepaket für dieses Appliance-Modell und das angegebene Konfigurationspaket enthält. Der Abschnitt "**Konfigurationsdateinamen** "über der Tabelle zeigt den Paketnamen für die aktuell aktiven und gestagten Pakete auf der lokalen Appliance.
- **Aktive/gestagte Download-Links** —Diese befinden sich im Feld **Paket herunterladen** (Spalte ganz rechts) jedes Eintrags in der **Appliance-Site-Tabelle**. Klicken Sie auf einen Link in einem Eintrag, um das aktive oder bereitgestufte Paket für diese Appliance-Site herunterzuladen.
- **Beginnen** —Klicken Sie auf **Beginnen**, um den Prozess des **Änderungsmanagement-Assistenten** zu starten und zur Registerkarte **Änderungsvorbereitung** zu gelangen.
- **Staged aktivieren** — Wenn dies keine erste Bereitstellung ist und Sie die aktuell gestagte 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

October 28, 2021

Gehen Sie wie folgt vor, um Citrix SD-WAN Appliance-Hardware (physische Appliance) einzurichten:

1. Richten Sie das Chassis ein.

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

2. Verbinde die Stromversorgung.

   a) Stellen Sie sicher, dass der Netzschalter auf Aus eingestellt ist.
   b) Stecken Sie das Netzkabel in das Gerät und eine Steckdose.
   c) Drücken Sie den Netzschalter auf der Vorderseite des Geräts.

3. Verbinden Sie die Stromversorgung.

   a) Stellen Sie sicher, dass der Netzschalter auf Aus eingestellt ist.
   b) Stecken Sie das Netzkabel in das Gerät und eine Steckdose.
   c) Drücken Sie den Netzschalter auf der Vorderseite des Geräts.

4. Verbinden Sie den Management-Port des Geräts mit einem PC.

   Sie müssen die Appliance zur Vorbereitung auf den Abschluss des nächsten Vorgangs an einen PC anschließen und die Verwaltungs-IP-Adresse für die Appliance festlegen.

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

SD-WAN VPX-SE Managementport

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 das SD-WAN VPX-SE nicht konfiguriert haben, als Sie die virtuelle VPX-Maschine erstellt haben, müssen Sie dies jetzt tun, wie im Abschnitt Konfigurieren der Verwaltungs-IP-Adresse für den SD-WAN VPX-SEbeschrieben.

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 das SD-WAN VPX-SE nicht konfiguriert haben, als Sie die virtuelle VPX-Maschine erstellt haben, müssen Sie dies jetzt tun, wie im Abschnitt Konfigurieren der Verwaltungs-IP-Adresse für den SD-WAN VPX-SEbeschrieben.

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.

Citrix SD-WAN Appliances unterstützen sowohl IPv4- als auch IPv6-Protokolle. Sie können IPv4, IPv6 oder beides (Dual Stack) konfigurieren. Wenn sowohl die IPv4- als auch die IPv6-Protokolle konfiguriert sind, hat das IPv4-Protokoll Vorrang vor dem IPv6-Protokoll.

> **HINWEIS:**
>
> - Um eine IPv4- oder IPv6-Adresse in funktionsspezifischen Konfigurationen zu konfigurieren, stellen Sie sicher, dass das gleiche Protokoll als Management-Interface-Protokoll aktiviert und konfiguriert ist. Wenn Sie beispielsweise eine IPv6-Adresse für einen SMTP-Server konfigurieren möchten, stellen Sie sicher, dass eine IPv6-Adresse als Verwaltungsschnittstellenadresse konfiguriert ist.
> - Link-lokale Adressen (IPv6-Adressen, die mit “fe80”beginnen) sind nicht erlaubt.

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 Management-IP-Adresse für das 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 zu 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 Ethernet-Kabels an den Management-Port der Appliance und das andere Ende an den Standard-Ethernet-Anschluss des PCs 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 Ihre Netzwerkschnittstelleneinstellungen und ändern Sie die IP-Adresse für Ihren PC wie folgt:

   - 192.168.100.50

4. Ändern Sie die Einstellung **Subnet Mask** 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 das Gerät 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 zu einem SD-WAN-Gerät herstellen.
   >
   > Ignorieren Sie alle Browserzertifikatwarnungen für das Management-Webinterface.

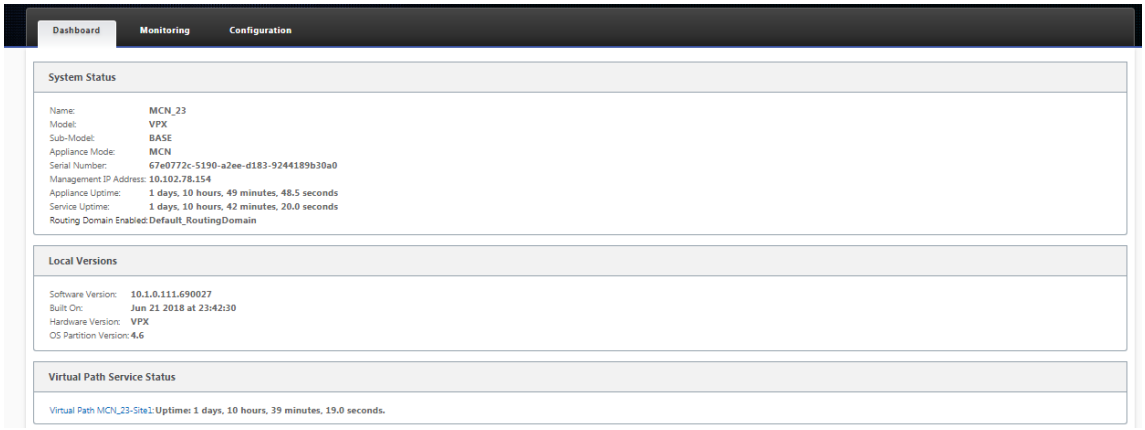
   Dadurch wird der Anmeldebildschirm der SD-WAN-Verwaltungswebschnittstelle auf der angeschlossenen Appliance geöffnet.

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. Achten Sie darauf, das Kennwort an einem sicheren Ort aufzuzeichnen, da die Wiederherstellung des Kennworts möglicherweise ein Zurücksetzen der Konfiguration erfordert.

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



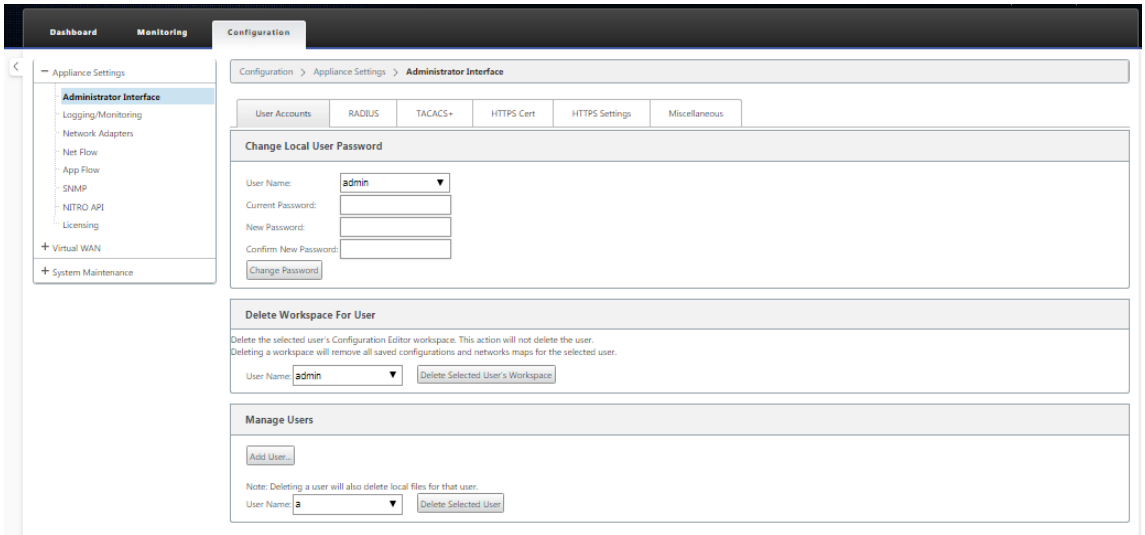
Wenn Sie sich zum ersten Mal bei der Management-Weboberfläche einer Appliance anmelden, zeigt das **Dashboard** ein Warnsymbol (Goldenrod Delta) und eine Warnmeldung an, die angibt, dass der SD-WAN-Dienst deaktiviert ist und die Lizenz nicht installiert wurde. Im Moment können Sie diese Warnung ignorieren.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

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

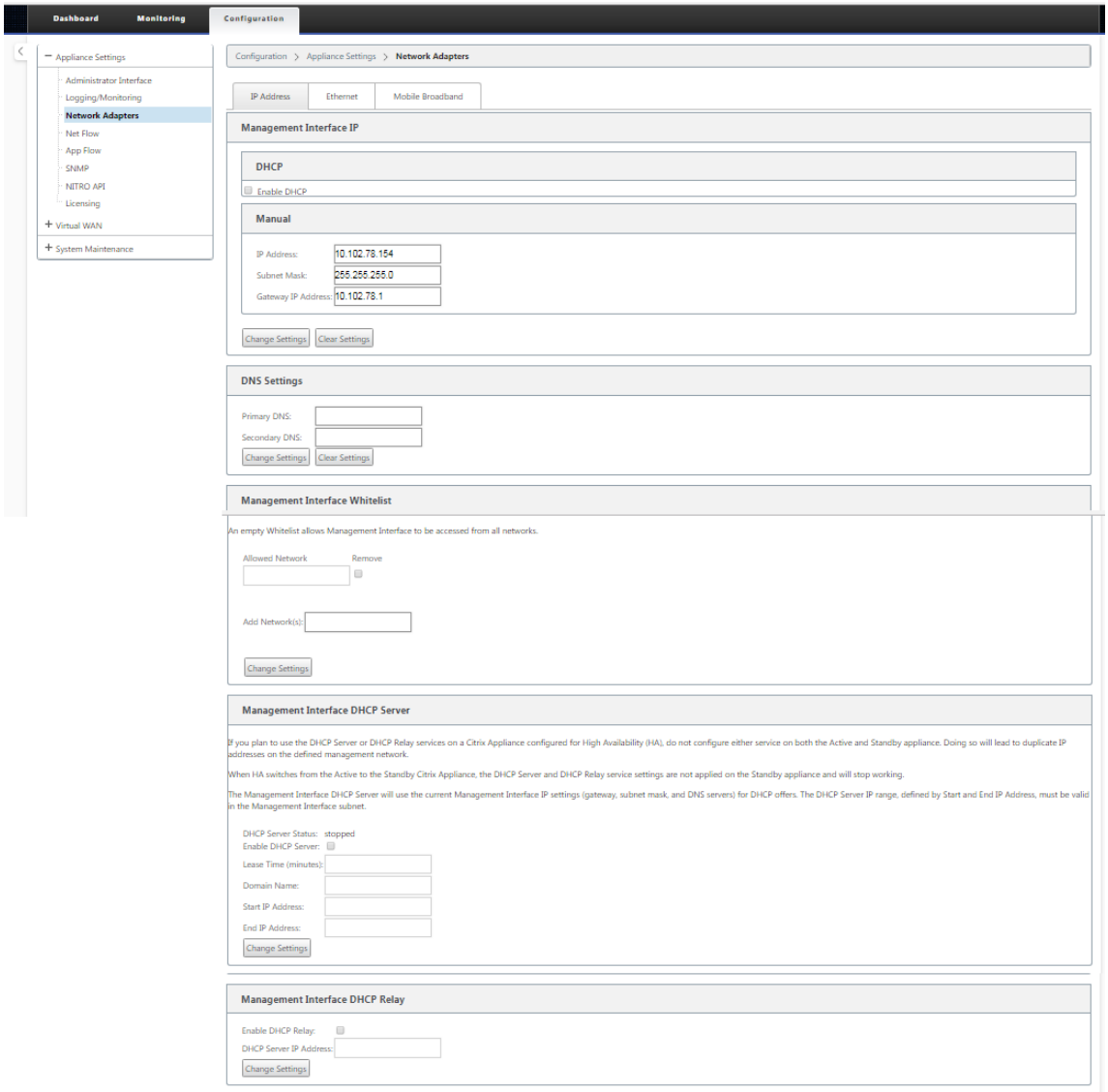
   Dadurch wird die **Konfigurationsnavigationsstruktur** im linken Bereich des Bildschirms angezeigt. Der **Konfigurationsnavigationsbaum** enthält die folgenden drei Hauptzweige:

   - Appliance-Einstellungen
   - Virtuelles WAN
   - System-Pflege

   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.



9. Aktivieren Sie auf der Registerkarte “IP-Adresse”eine der folgenden Optionen:

   - **IPv4-Protokoll**: Um die IPv4-Adresse zu aktivieren, **aktivieren Sie das Kontrollkästchen IPv4** aktivieren. Das Dynamic Host Control Protocol (DHCP) weist jedem Gerät im Netzwerk dynamisch eine IP-Adresse und andere Netzwerkkonfigurationsparameter zu. Wählen Sie **DHCP aktivieren**, um die IP-Adresse dynamisch zuzuweisen. Um die IP-Adresse manuell zu konfigurieren, geben Sie die folgenden Details an:

     - IP-Adresse
     - Subnetzmaske

  - Gateway-IP-Adresse

- **IPv6-Protokoll**: Um die IPv6-Adresse zu aktivieren, **aktivieren Sie das Kontrollkästchen IPv6** aktivieren. Sie können die IPv6-Adresse manuell konfigurieren oder DHCP oder SLAAC aktivieren, um die IP-Adresse automatisch zuzuweisen.

  Um manuell zu konfigurieren, geben Sie die folgenden Details an:

  - IP-Adresse
  - Prefix

  Um SLAAC zu konfigurieren, aktivieren Sie das Kontrollkästchen **SLAAC**. SLAAC weist jedem Gerät im Netzwerk automatisch eine IPv6-Adresse zu. SLAAC ermöglicht es einem IPv6-Client, seine eigenen Adressen mithilfe einer Kombination aus lokal verfügbaren Informationen und Informationen zu generieren, die von Routern über das Neighbor Discovery Protocol (NDP) beworben werden.

  Um DHCP zu konfigurieren, aktivieren Sie das Kontrollkästchen **DHCP**. Um zustandloses DHCP zu aktivieren, aktivieren Sie die Kontrollkästchen **SLAAC** und **DHCP**.

- **Sowohl IPv4- als auch IPv6-Protokolle**: **Aktivieren Sie die Kontrollkästchen IPv6aktivieren und IPv4** aktivieren, um sowohl IPv4- als auch IPv6-Protokolle zu aktivieren. In solchen Szenarien verfügt die SD-WAN-Appliance über eine IPv4-Verwaltungs-IP-Adresse und eine IPv6-Verwaltungsadresse.

> **HINWEIS:**
>
> - Die Verwaltungs-IP-Adresse muss für jede Appliance eindeutig sein.
> - Die Abschnitte **Management Interface DHCP Server** und **DHCP Relay** auf der Registerkarte IP-Adresse sind nur anwendbar, wenn das IPv4-Protokoll in der Verwaltungsschnittstelle aktiviert ist.

10. Klicken Sie auf **Change Settings**. Ein Bestätigungsdialogfeld wird 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**
>
> Das Ändern der IP-Adresse für Ihren PC schließt automatisch die Verbindung zur Appliance und beendet Ihre Anmeldesitzung auf der Management-Weboberfläche.

13. Trennen Sie das Gerät vom PC und verbinden Sie das Gerät mit Ihrem Netzwerk-Router oder Switch. Trennen Sie das Ethernet-Kabel vom PC, aber trennen Sie es nicht von Ihrem Gerät. Verbinden Sie das freie Ende des Kabels mit Ihrem Netzwerk-Router oder Switch.

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

14. Testen Sie die Verbindung. Öffnen Sie auf einem mit Ihrem Netzwerk verbundenen PC einen Browser und geben Sie die Verwaltungs-IP-Adresse ein, die Sie für die Appliance im folgenden Format konfiguriert haben:

    Für IPv4-Adresse: `https://<IPv4 address>`

    Beispiel:`https://10.10.2.3`

    Für IPv6-Adresse: `https://<[IPv6 address]>`

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

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

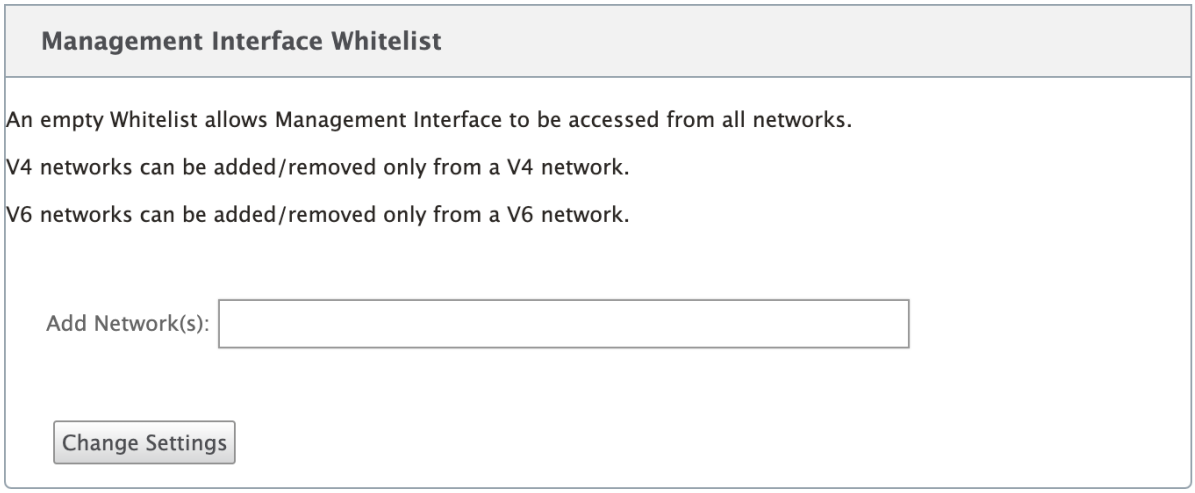
    > **Tipp**
    >
    > Melden Sie sich nach der Überprüfung der Verbindung nicht von der Management-Weboberfläche ab. Sie verwenden es, um die verbleibenden Aufgaben abzuschließen, die in den folgenden Abschnitten beschrieben werden.

    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.

Zulassungsliste der Verwaltungsschnitt

Die zulässige Liste ist eine genehmigte Liste von IP-Adressen oder IP-Domains, die die Berechtigung zum Zugriff auf Ihre Verwaltungsschnittstelle haben. Eine leere Liste ermöglicht den Zugriff auf Management Interface von allen Netzwerken aus. Sie können IP-Adressen hinzufügen, um sicherzustellen, dass die Verwaltungs-IP-Adresse nur für die vertrauenswürdigen Netzwerke zugänglich ist.

Um eine IPv4-Adresse zur zulässigen Liste hinzuzufügen oder zu entfernen, müssen Sie nur mit einer IPv4-Adresse auf die Verwaltungsschnittstelle der SD-WAN-Appliance zugreifen. Um eine IPv6-Adresse zur zulässigen Liste hinzuzufügen oder zu entfernen, müssen Sie auf die Verwaltungsschnittstelle der SD-WAN-Appliance nur mit einer IPv6-Adresse zugreifen.



Datum und Uhrzeit festlegen

October 28, 2021

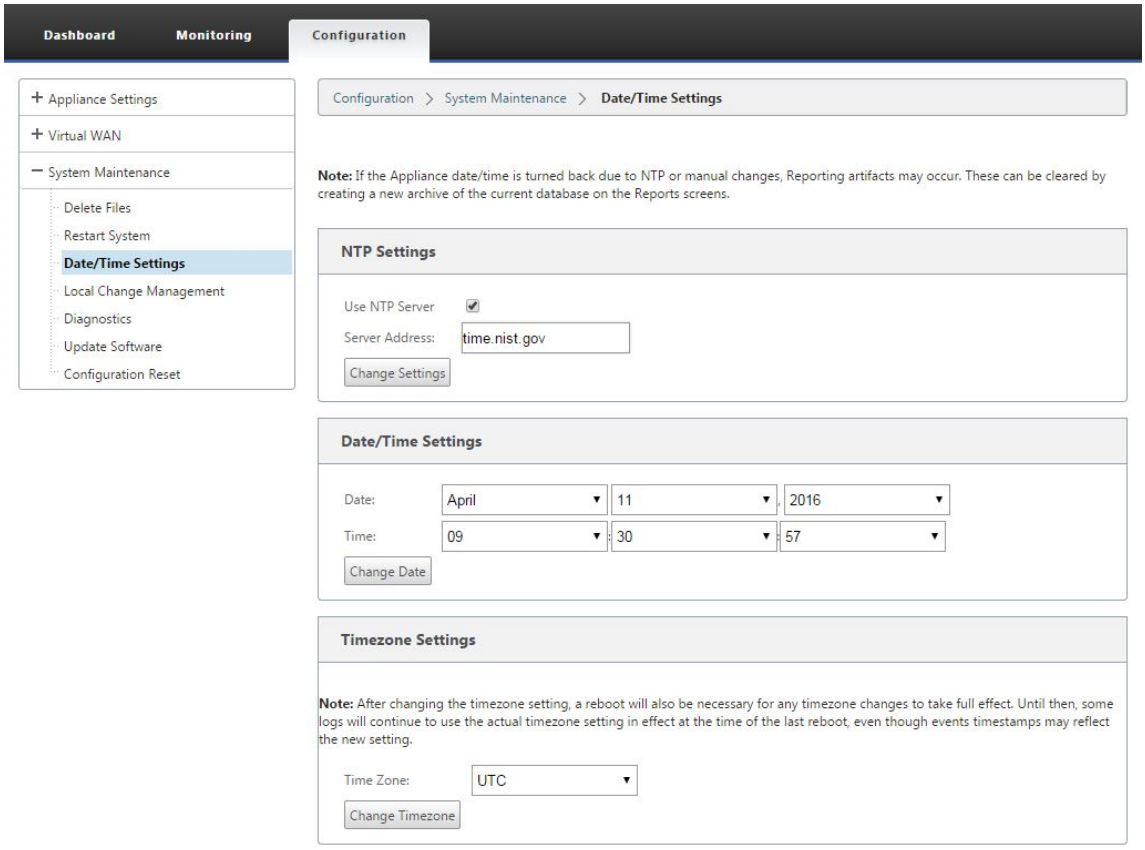
Bevor Sie die SD-WAN-Softwarelizenz auf einer Appliance installieren, müssen Sie Datum und Uhrzeit auf der Appliance festlegen.

> **Hinweis**
>
> Sie müssen diesen Vorgang für jede Appliance wiederholen, die Sie zu Ihrem Netzwerk hinzufügen möchten.

Gehen Sie folgendermaßen vor, um Datum und Uhrzeit festzulegen:

1. Melden Sie sich beim Management-Webinterface auf der Appliance an, die Sie konfigurieren.
2. Wählen Sie in der Hauptmenüleiste die **Registerkarte Konfiguration.**

   Dadurch wird die **Konfigurationsnavigationsstruktur** im linken Bereich des Bildschirms angezeigt.
3. Öffnen Sie den **Zweig Systemwartung** im Navigationsbaum.
4. Wählen Sie unter dem **Zweig Systemwartung die Option Datum/Uhrzeit Einstellungen** Daraufhin wird die Seite **Datums-/Uhrzeiteinstellungen** wie folgt angezeigt.



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

> **Hinweis**
>
> Wenn Sie die Zeitzoneneinstellung ändern müssen, müssen Sie dies tun, bevor Sie Datum und Uhrzeit festlegen, 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 das Zeitzonenupdate abgeschlossen ist, werden im oberen Bereich der Seite ein Symbol für eine Erfolgsalarmierung (grünes Häkchen) und eine Statusmeldung angezeigt.

7. (Optional) Aktivieren Sie den NTP-Serverdienst.

   a) Wählen Sie **NTP-Server verwenden**.
   b) Geben Sie die Serveradresse in das Feld **Serveradresse** ein.
   c) Klicken Sie auf **Change Settings**.
      Ein Erfolgswarnsymbol (grünes Häkchen) und eine Statusmeldung werden angezeigt, wenn das Update abgeschlossen ist.

8. Wählen Sie den Monat, den Tag und das Jahr aus den Dropdownmenüs des Feldes **Datum** aus.

9. Wählen Sie die Stunde, Minuten und Sekunden aus den Dropdownmenüs des **Zeitfelds** aus.
10. Klicken Sie auf **Datum ändern**.

> **Hinweis:**
>
> Dies aktualisiert die Datums- und Uhrzeiteinstellung, zeigt jedoch kein Erfolgswarnsymbol oder eine Statusmeldung an.

Der nächste Schritt besteht darin, den **Timeout-Schwellenwert** für die Konsolensitzung auf den Maximalwert festzulegen. Dieser Schritt ist optional, wird jedoch empfohlen. Dies 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 Hochladen und Installieren der SD-WAN-Softwarelizenzdateifortfahren.

> **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

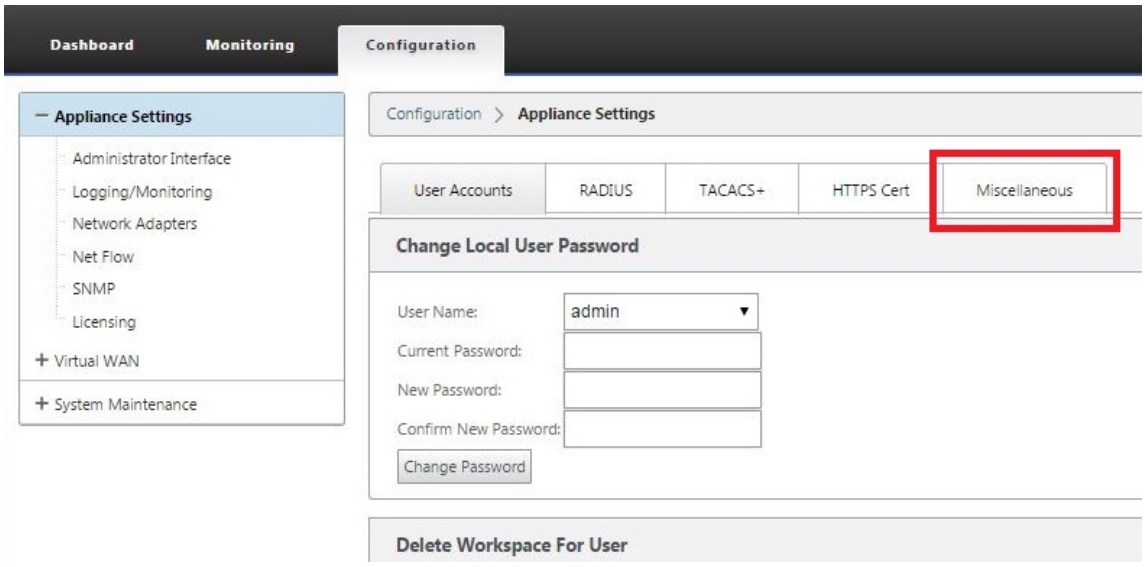
October 28, 2021

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. Die Standardeinstellung 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 **Timeout-Intervall** der Konsolensitzung zurückzusetzen

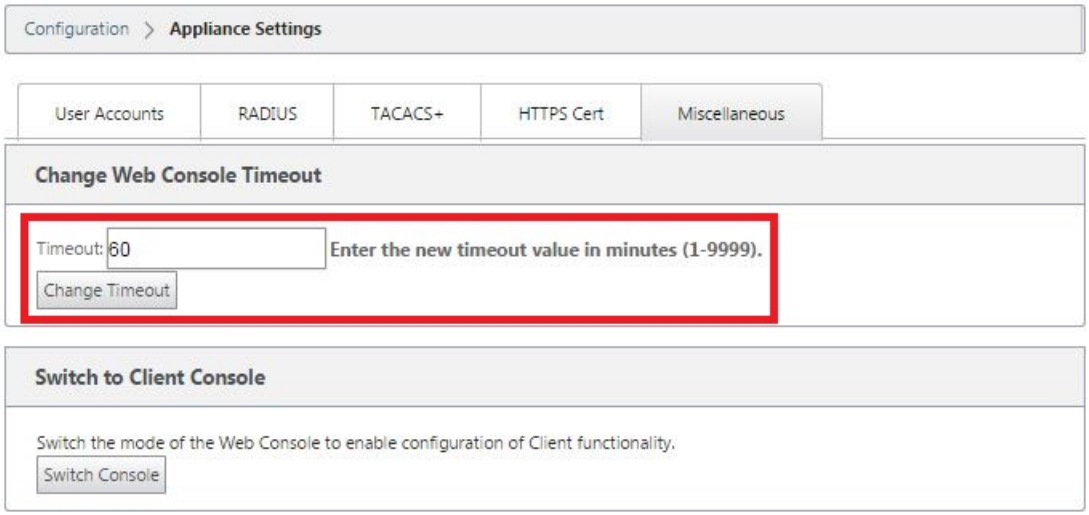
1. Wählen Sie die Registerkarte **Konfiguration** aus, und wählen Sie dann den Zweig **Appliance-Einstellungen** in der Navigationsstruktur aus.

Dadurch wird die Seite **Appliance-Einstellungen** angezeigt, wobei die Registerkarte **Benutzerkonten** standardmäßig vorausgewählt ist.



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

   Dadurch wird die Registerkarte **Verschiedenes** angezeigt.



3. Geben Sie den **Timeout-Wert** für die Konsole ein.

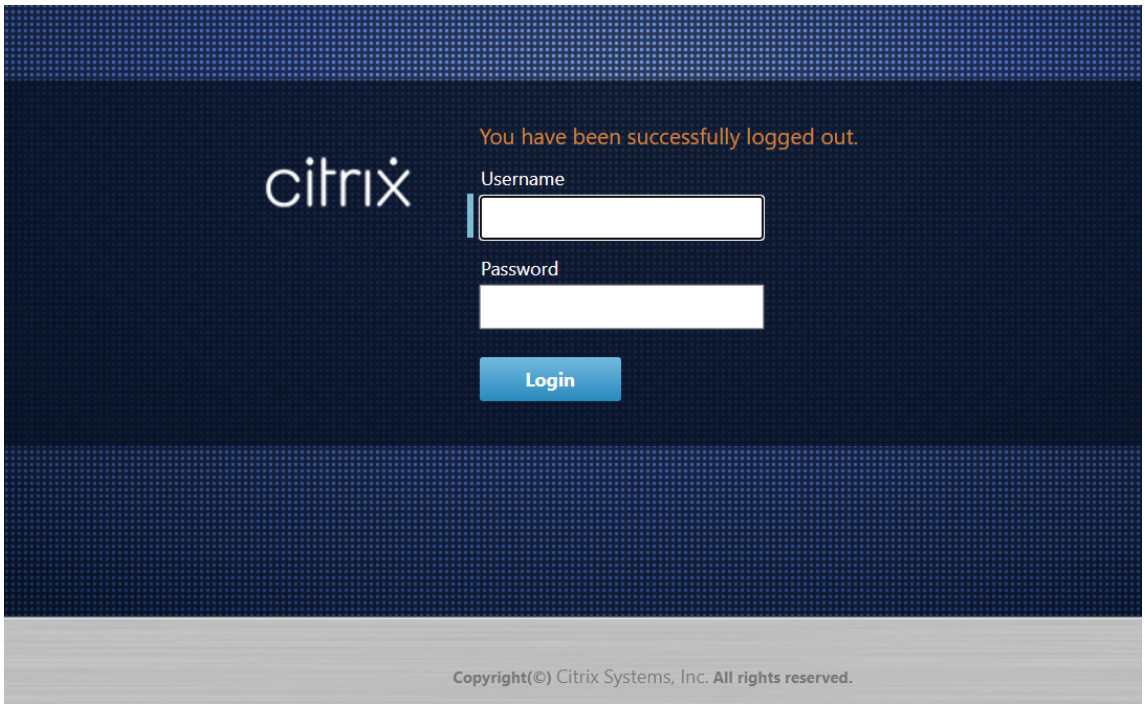
   Geben Sie im Feld **Timeout** des Abschnitts **Timeout der Webkonsole ändern** einen höheren Wert (in Minuten) bis zum Maximalwert von 9999 ein. Der Standardwert ist 60, was für eine erste Konfigurationssitzung viel zu kurz ist.

   > **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 **Timeout ändern**.

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

   Nach einem kurzen Intervall (ein paar Sekunden) wird die Sitzung beendet und Sie werden automatisch vom Management-Webinterface abgemeldet. Die Anmeldeseite wird angezeigt.



5. Geben Sie den Benutzernamen des Administrators (*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.

Alarme konfigurieren

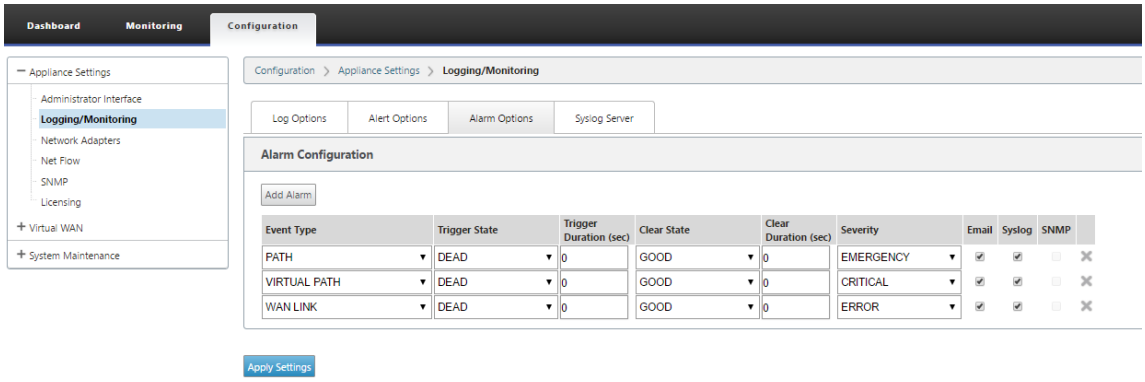
October 28, 2021

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

Ein Alarm ist eine konfigurierte Warnung, die aus einem Ereignistyp, einem Auslösezustand, einem Löschzustand und einem Schweregrad besteht.

So konfigurieren Sie Alarmeinstellungen:

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



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

   - **Ereignistyp**: Die SD-WAN-Appliance kann Alarme für bestimmte Subsysteme oder Objekte im Netzwerk auslösen, diese werden als Ereignistypen bezeichnet. 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 und IPSEC_TUNNEL.
   - **Triggerstatus:** Der Ereignisstatus, der einen Alarm für einen Ereignistyp auslöst. Die verfügbaren Optionen für den Triggerstatus hängen vom ausgewählten Ereignistyp ab.
   - **Triggerdauer**: Die Dauer in Sekunden, dies bestimmt, wie schnell das Gerät einen Alarm auslöst. Geben Sie ‘0’ein, um sofortige Benachrichtigungen zu erhalten, oder geben Sie einen Wert zwischen 15-7200 Sekunden ein. Alarme werden nicht ausgelöst, wenn innerhalb des Zeitraums der Triggerdauer mehrere Ereignisse auf demselben Objekt auftreten. Weitere Alarme werden nur ausgelöst, wenn ein Ereignis länger als die Triggerdauer andauert.

- **Clear State**: Der Ereignisstatus, der einen Alarm für eine Ereignisart löscht, nachdem der Alarm ausgelöst wurde. Die verfügbaren Clear State-Optionen hängen vom ausgewählten Trigger-Status ab.
- **Dauer löschen:** Die Dauer in Sekunden, dies bestimmt, wie lange gewartet werden muss, 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 Alarmen angezeigt, die gesendet werden, wenn der Alarm ausgelöst oder gelöscht wird, und in der Zusammenfassung des ausgelösten Alarms.
- **E-Mail**: Alarmauslöser und klare Warnungen für die Ereignisart werden per E-Mail gesendet.
- **Syslog**: Alarmauslöser und Clear Alerts für den Ereignistyp werden über Syslog gesendet.
- **SNMP**: Alarmauslöser und Löschwarnungen für den Ereignistyp werden per SNMP-Trap gesendet.

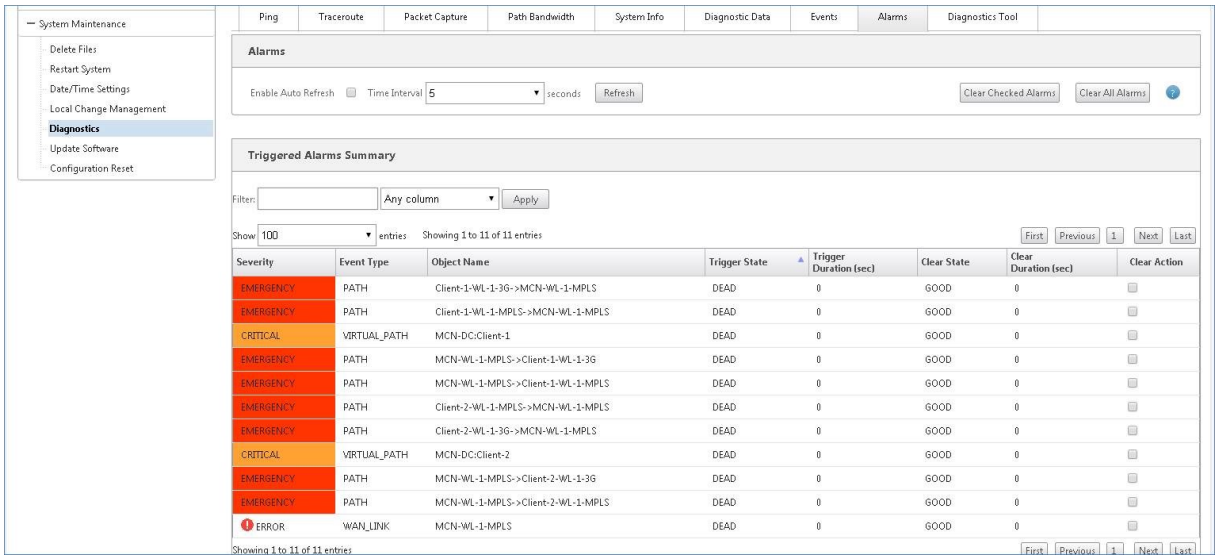
4. Fügen Sie nach Bedarf weitere Alarme hinzu.
5. Klicken Sie auf **Einstellungen anwenden**.

Anzeigen von ausgelösten Alarmen

So zeigen Sie eine Zusammenfassung aller ausgelösten Alarme an:

Navigieren Sie in der SD-WAN-Webverwaltungsoberfläche zu **Konfiguration> Systemwartung > Diagnose**>**Alarme**.

Eine Liste aller ausgelösten Alarme wird angezeigt.



Clearing ausgelöste Alarme

So löschen Sie ausgelöste Alarme manuell:

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

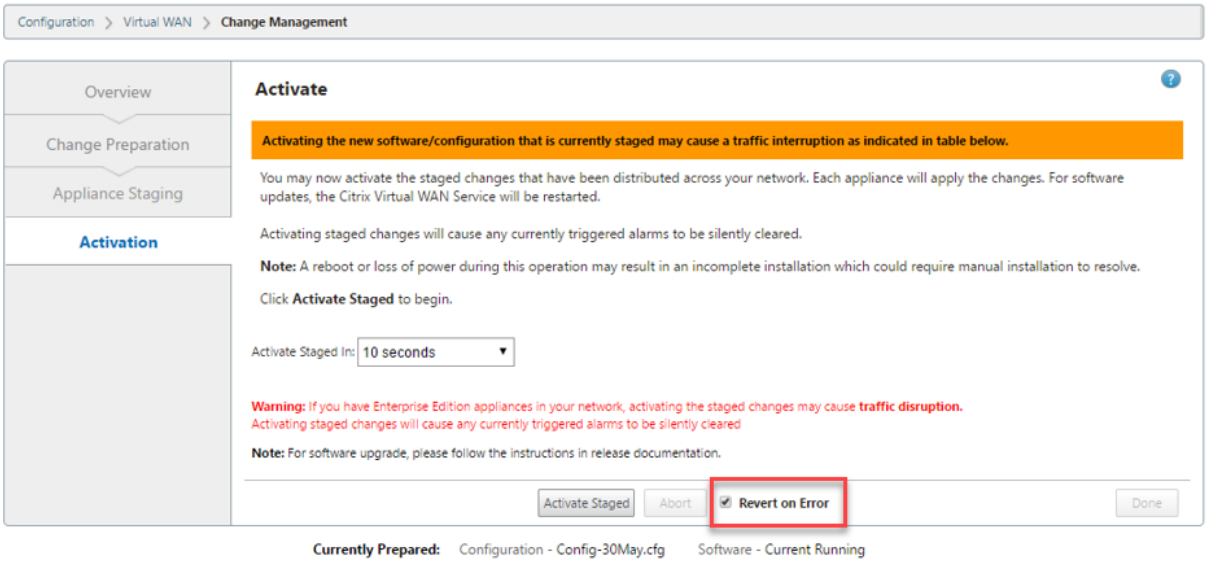
Rollback konfigurieren

October 28, 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:

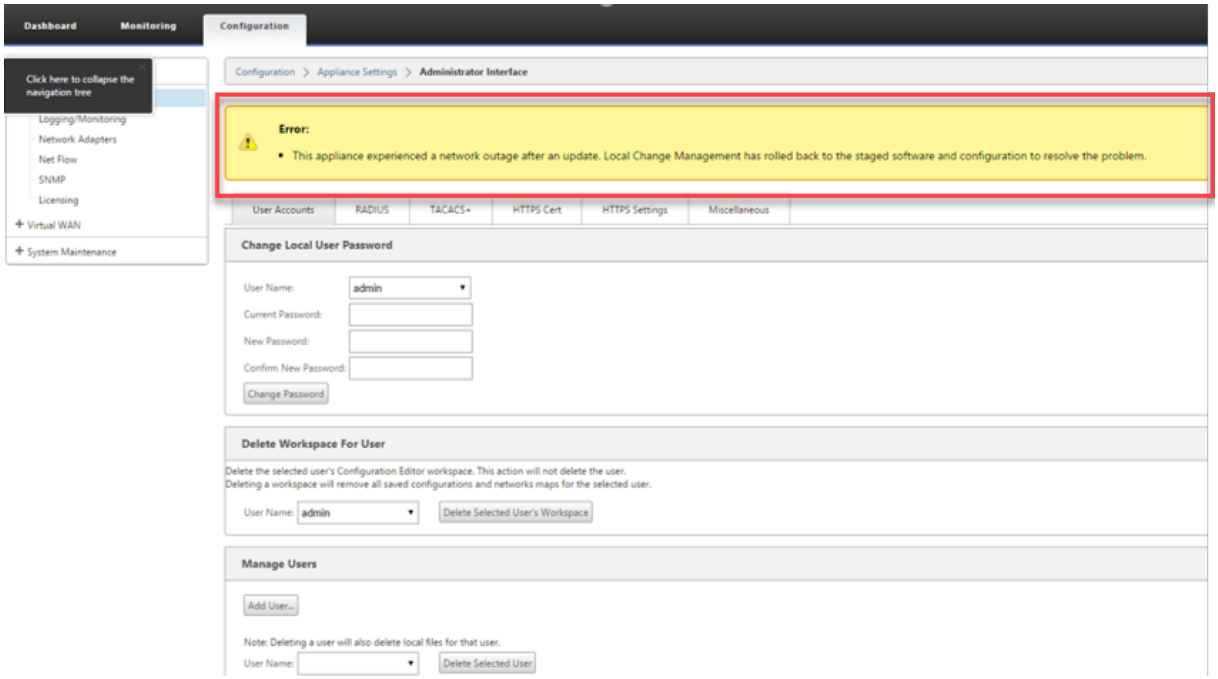
- Nach einem Software-Upgrade ist der virtuelle Pfad tot und der Dienst wird deaktiviert, wenn der Software-Absturz auftritt.
- Nach den Konfigurationsänderungen ist der virtuelle Pfad ohne Software-Absturz tot.
- Wenn die Konfiguration für die MCN-Appliance selbst ein Netzwerkproblem auf der MCN-Website 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.



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.

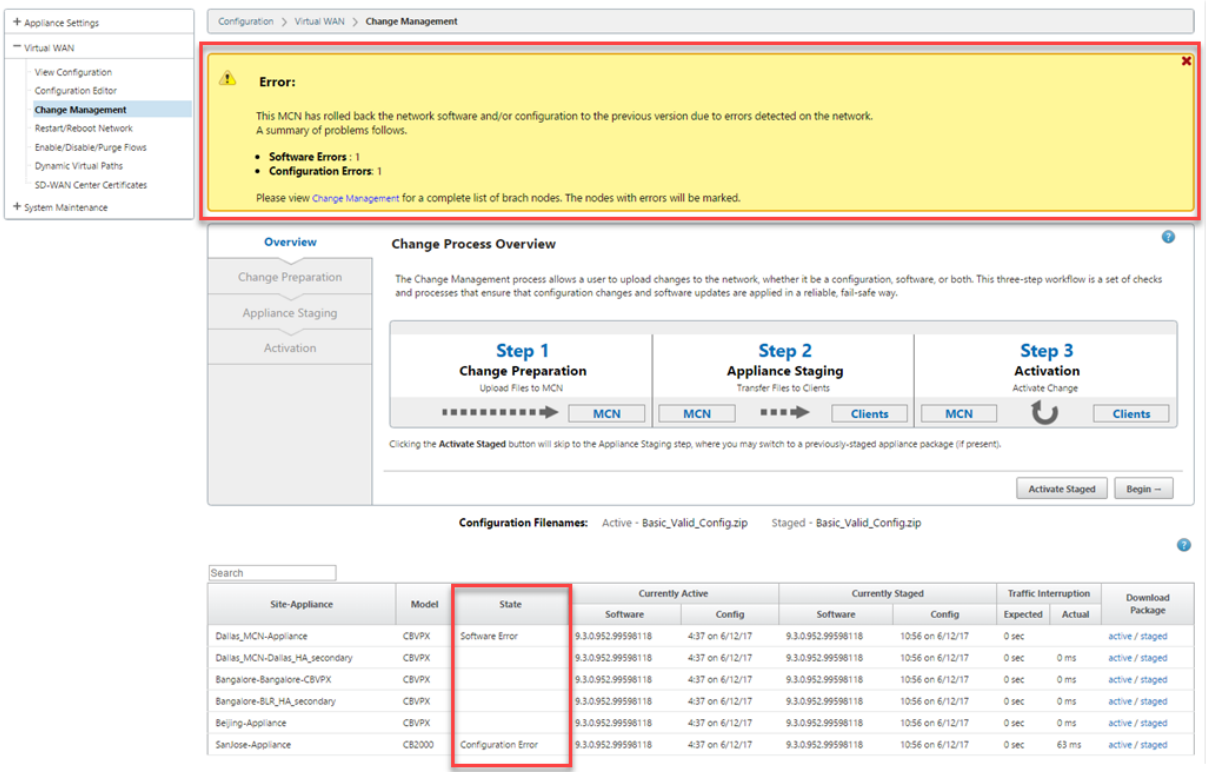
Der Client generiert ein kritisches Schweregrad für das SOFTWARE_UPDATE-Objekt, wenn ein Appliance-Absturz erkannt wird, oder generiert ein kritisches Schweregrad für das CONFIG_UPDATE-Objekt, wenn ein Netzwerkausfall erkannt wird.



Wenn **Fehler wiederherstellen** aktiviert ist, überwachen die Client-Appliances etwa 30 Minuten lang selbst. Wenn die Software innerhalb von 30 Minuten abstürzt oder wenn das Netzwerk 30 Minuten lang nicht verfügbar 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, wird die Art des aufgetretenen Fehlers gemeldet. In der Fehlermeldung wird eine zusammengefasste Anzahl der Fehler angezeigt.



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

October 28, 2021

Der **SD-WAN Master Control Node (MCN)** ist die Head End-Appliance im virtuellen 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 Upgrade-Verfahren 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:

- Bereitstellungsschritte im virtuellen WAN PBR-Modus (CTX201577)

  http://support.citrix.com/article/CTX201577
- Bereitstellungsschritte für den virtuellen WAN-Gatewaymodus (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 das Management-Webinterface in den **MCN-Konsolenmodus**.
2. Fügen Sie die MCN-Site hinzu.
3. Konfigurieren Sie die virtuellen Schnittstellengruppen für den 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 Zugriffsschnittstellen für den MCN-Site.
8. Konfigurieren Sie die Routen für den MCN-Standort.
9. (Optional) Konfigurieren Sie Hochverfügbarkeit für den MCN-Standort.
10. (Optional) Konfigurieren Sie Virtual WAN-Sicherheit und Verschlüsselung.
11. Benennen und speichern Sie die MCN-Site-Konfiguration.

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

MCN Übersicht

October 28, 2021

Der **Master Control Node (MCN)** ist die zentrale virtuelle 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 veranschaulicht die grundlegenden Rollen und den Kontext der MCN (Rechenzentrum) und Client (Zweigknoten) -Appliances für eine Virtual WAN Edition-Bereitstellung.

Zur MCN-Konsole wechseln

October 28, 2021

Um die MCN-Site hinzuzufügen und zu konfigurieren, müssen Sie sich zuerst beim Management-Webinterface auf der Appliance anmelden, die Sie zur MCN-Rolle heraufstufen, und das Management-Webinterface in den **MCN-Konsolenmodus** umschalten. Der**MCN-Konsolenmodus** ermöglicht den Zugriff auf den Konfigurationseditor im Management-Webinterface, mit dem Sie derzeit verbunden sind. Sie können dann den **Konfigurationseditor** verwenden, um die MCN-Site hinzuzufügen und zu konfigurieren.

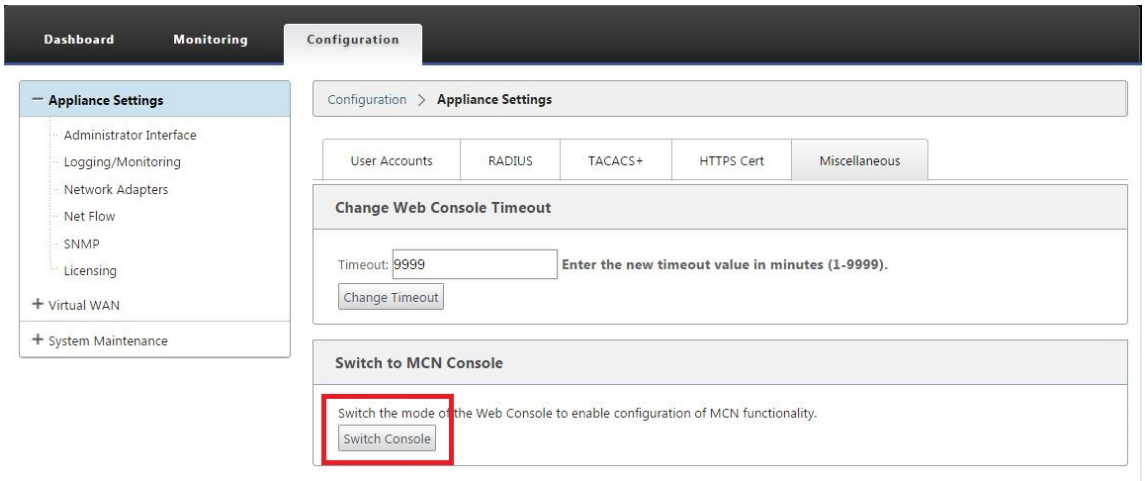
> **Hinweis**
>
> Das Umschalten in den **MCN-Konsolenmodus** ändert nur den Betriebsmodus des Management-Webinterface-Modus und nicht die aktive Rolle der Appliance selbst. Um eine Appliance in die Rolle des MCN zu befördern, müssen Sie zuerst den MCN-Site hinzufügen und konfigurieren und das Konfigurations- und Softwarepaket auf der angegebenen MCN-Appliance aktivieren.

Gehen Sie wie folgt vor, um das Management-Webinterface in den **MCN-Konsolenmodus** umzuschalten:

1. Melden Sie sich beim Management-Webinterface auf der Appliance an, die Sie als MCN konfigurieren möchten.
2. Klicken Sie in der Hauptmenüleiste des Hauptbildschirms des Management Webinterface auf **Konfiguration** (blauer Balken oben auf der Seite).
3. Öffnen Sie in der Navigationsstruktur (linker Bereich) den Zweig **Appliance-Einstellungen** und klicken Sie auf **Administratorschnittstelle**.

   Dadurch wird die Seite Administratorschnittstelle im mittleren Bereich angezeigt.
4. Wählen Sie die Registerkarte **Verschiedenes**.

   Dadurch wird die Seite **Verschiedene Verwaltungseinstellungen** angezeigt.



   Am unteren Rand der Registerkarte **Verschiedenes** befindet sich der Abschnitt **Wechseln zu [Client > MCN-Konsole. 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 **Switch to Client Console.**

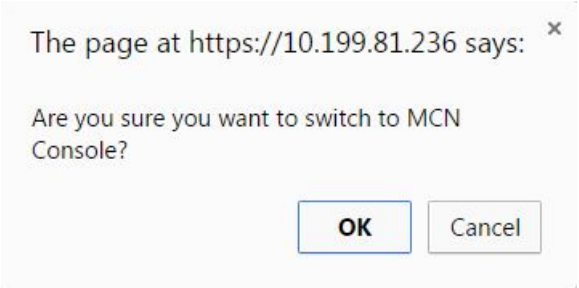
   Standardmäßig ist eine neue Appliance auf den **Client-Konsolenmodus** eingestellt.

   Der**MCN-Konsolenmodus** aktiviert den Zweig des **Konfigurationseditors** im Navigationsbaum. Der **Konfigurationseditor** ist nur auf der MCN-Appliance verfügbar.

> **Hinweis**
>
> Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie sicher, dass die Appliance immer noch auf den Standardwert eingestellt ist (**Client-Konsolenmodus**). Die Abschnittsüberschrift sollte lauten: **Wechseln zur MCN-Konsole**.

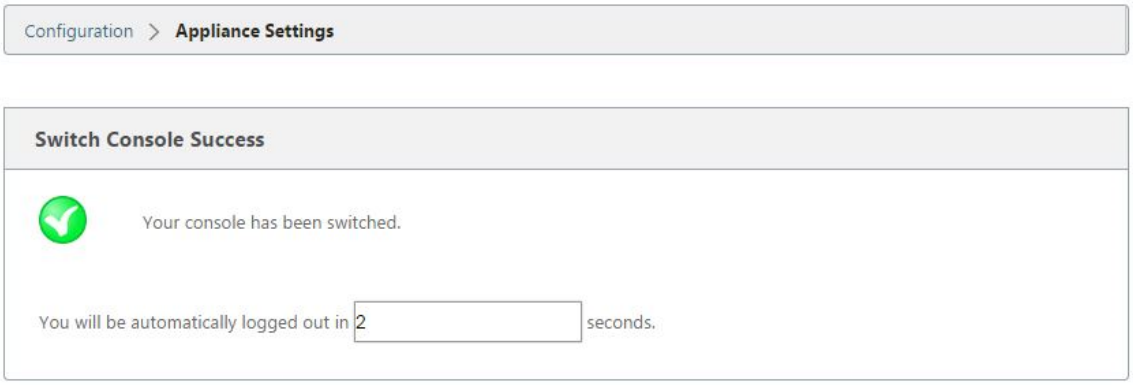
5. Klicken Sie auf **Switch-Modus**, um den Appliance-Modus auf den **MCN-Konsolenmodus** einzustellen.

   Daraufhin wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, zu bestätigen, dass Sie in den MCN-Modus wechseln möchten.

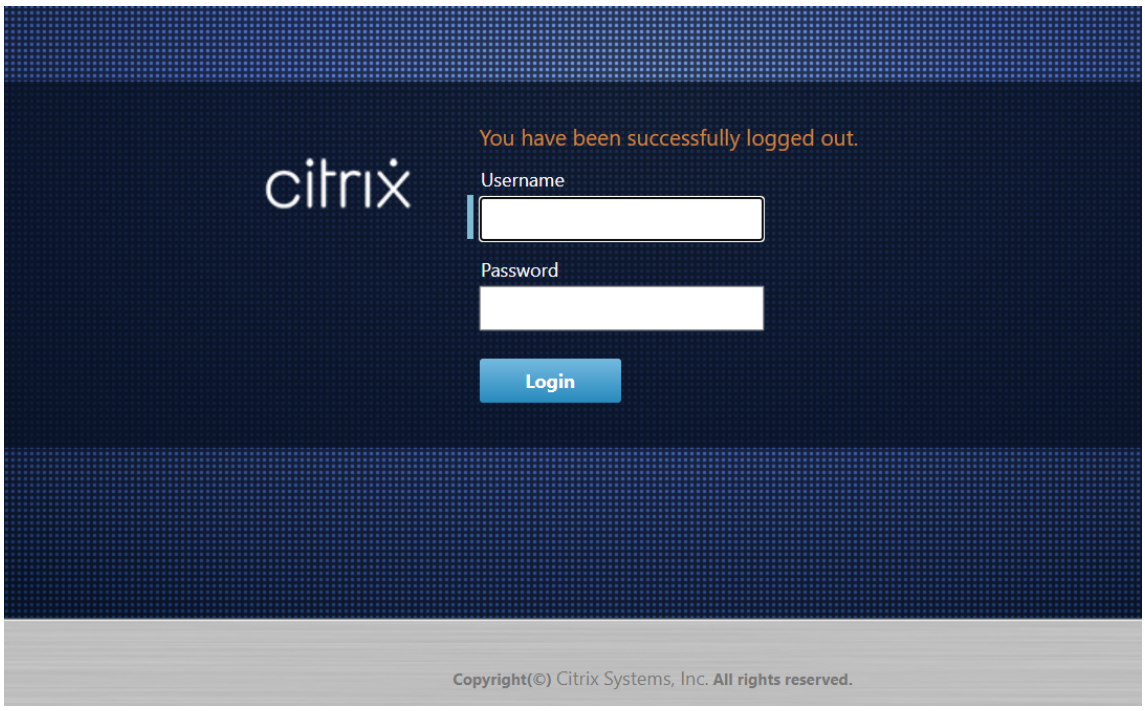


6. Klicken Sie auf **OK**.

   Dadurch wird der Konsolenmodus in den **MCN-Konsolenmodus** versetzt und die aktuelle Sitzung beendet. Eine Erfolgsmeldung wird zusammen mit einem Countdown-Status angezeigt, der die Anzahl der verbleibenden Sekunden vor dem Beenden der Sitzung angibt.



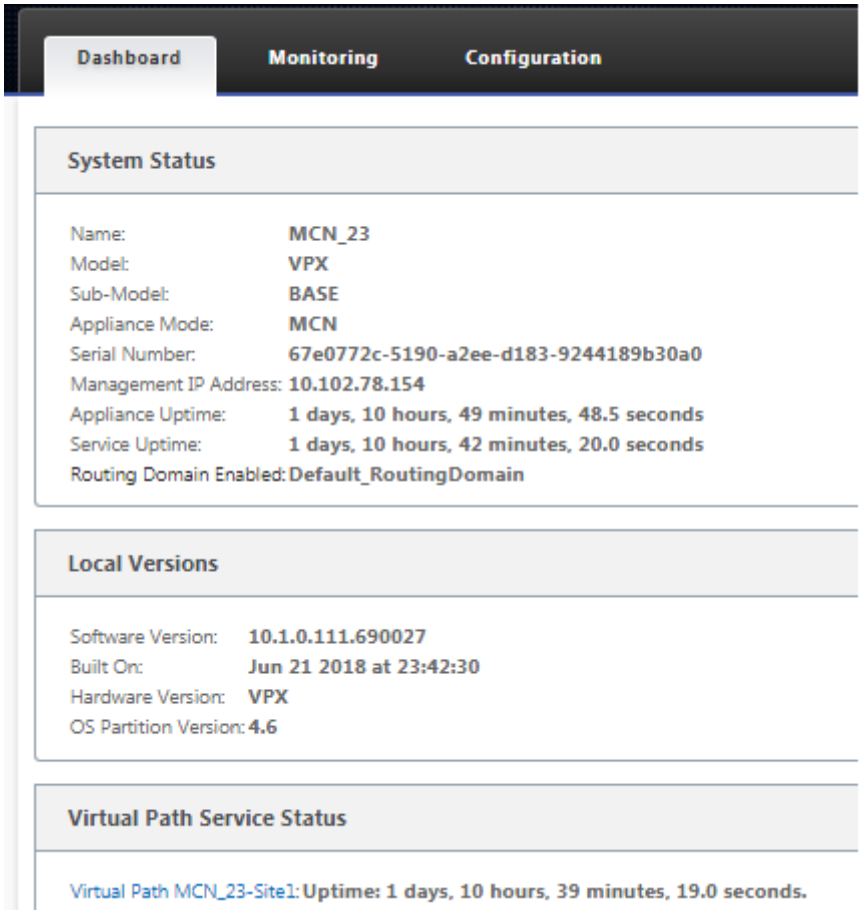
   Nach Abschluss des Countdowns wird die Sitzung beendet und die Anmeldeseite wird angezeigt.



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

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

   Nach dem Anmelden wird das **Dashboard** angezeigt und zeigt nun an, dass sich die Appliance im MCN-Modus befindet.



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

October 28, 2021

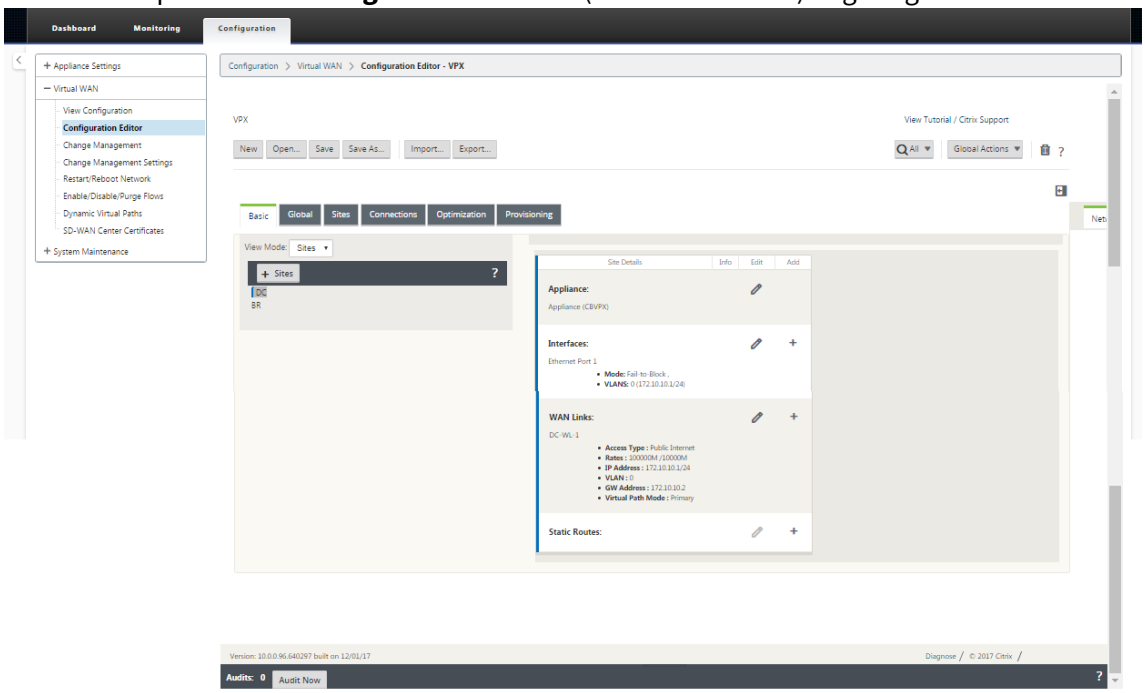
Der erste Schritt besteht darin, ein neues Konfigurationspaket zu öffnen und die MCN-Site zur neuen Konfiguration hinzuzufügen.

> **Hinweis**
>
> Der **Konfigurationseditor** ist nur im **MCN-Konsolenmodus** verfügbar. Wenn die Option **Konfigurationseditor** im Virtual WAN-Zweig der Navigationsstruktur nicht verfügbar ist, finden Sie im Abschnitt Umschalten des Management-Webinterface in den MCN-KonsolenmodusAnweisungen zum Ändern des Konsolenmodus.
>
> Es wird empfohlen, das Konfigurationspaket häufig oder an Schlüsselpunkten in der Konfigura-

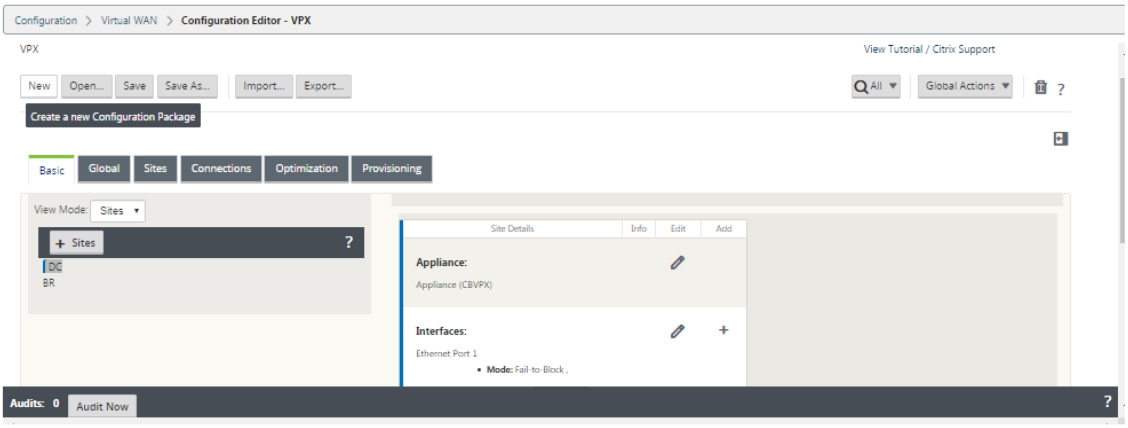
> tion zu speichern. Anweisungen finden Sie im Abschnitt Benennen, Speichern und Sichern der MCN-Site-Konfiguration.
>
> **Warnung**
>
> Wenn die Konsolensitzung ein Timeout auftritt oder Sie sich vor dem Speichern Ihrer Konfiguration vom Management-Webinterface abmelden, gehen alle nicht gespeicherten 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. Die Standardeinstellung 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 Festlegen des Timeout-Intervalls für Konsolensitzungen (Optional)

Gehen Sie folgendermaßen vor, um die MCN-Appliance-Site hinzuzufügen und mit der Konfiguration zu beginnen:

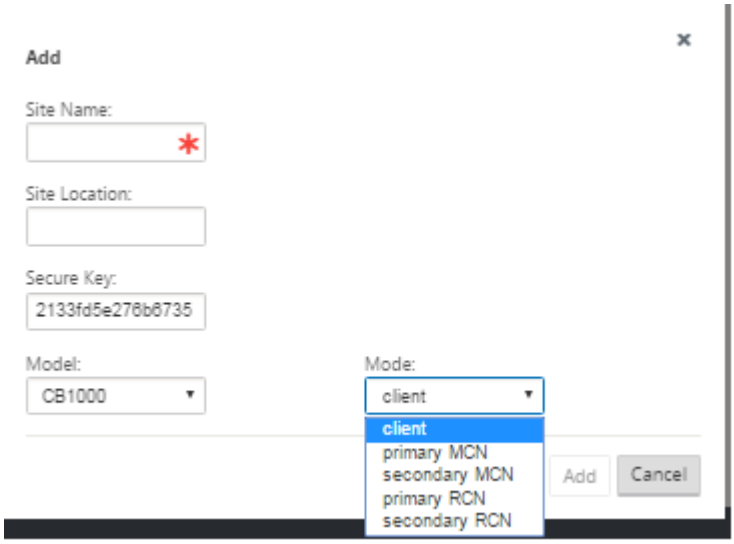
1. Navigieren Sie in der Navigationsstruktur zu **Virtual WAN** > **Configuration Editor**. Dadurch wird die Hauptseite des **Konfigurationseditors** (mittlerer Bereich) angezeigt.



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.

Führen Sie folgende Schritte aus:

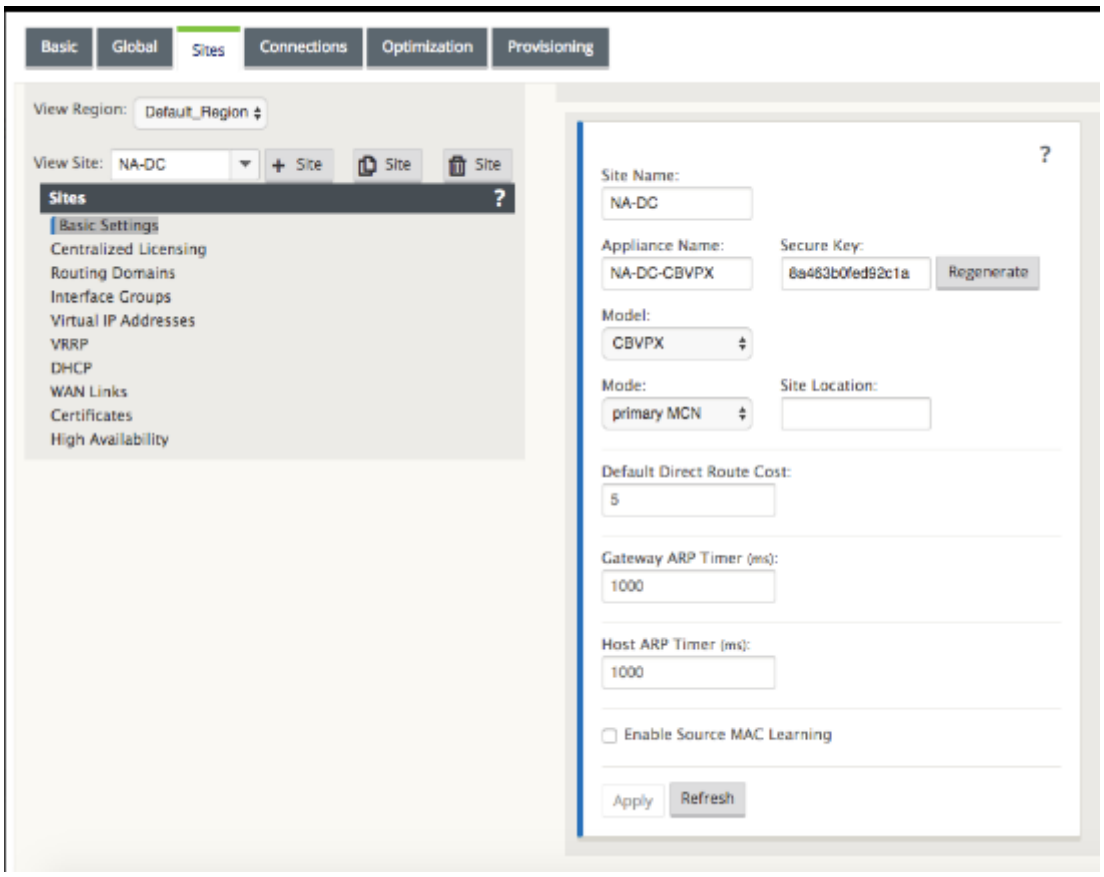
1. Geben Sie den **Site-Namen und densicheren Schlüssel**ein.
2. Wählen Sie das **Gerätemodell**aus.
3. Wählen Sie den **Modus**aus.
4. Wählen Sie den **primären MCN** als Modus aus.

> **Hinweis**
>
> Im Menü **Modelloptionen** werden die generischen Modellnamen für die unterstützten Appliance-Modelle aufgeführt. Die generischen Namen enthalten nicht das Modellsuffix der Standard Edition, sondern entsprechen den entsprechenden SD-WAN Appliance-Modellen. Wählen Sie die entsprechende Modellnummer für dieses SD-WAN Appliance-Modell aus.

> (Wählen Sie beispielsweise 4000 aus, wenn es sich um eine SD-WAN 4000-SE-Appliance handelt.)
>
> Einträge dürfen keine Leerzeichen enthalten und müssen im Linux-Format vorliegen.

So fügen Sie eine Site hinzu:

1. Klicken Sie auf **Hinzufügen**, um die Website hinzuzufügen. Dadurch wird die neue Site zur **Sitestruktur** hinzugefügt und das Konfigurationsformular **Grundeinstellungen** für die neue Site angezeigt.



   Nachdem Sie auf **Übernehmen**geklickt haben, werden Audit-Warnungen angezeigt, die darauf hinweisen, dass weitere Maßnahmen erforderlich sind. Ein Roter-Punkt- oder Goldenrod-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 reicht von 1.000 ms bis 180.000 ms. Die Konfiguration des Host-

ARP-Timers ist nicht auf den Management-Port anwendbar.

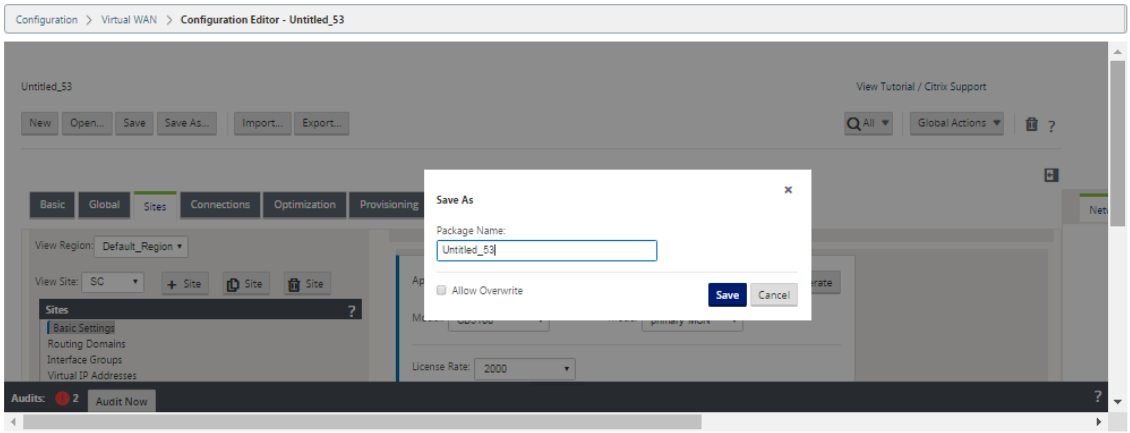
2. Geben Sie die Grundeinstellungen für die neue Site ein, oder übernehmen Sie die Standardeinstellungen. In Citrix SD-WAN Bereitstellungen wie Gateway und One-Arm werden beim häufigen Empfang der ARP-Anforderungen die Zugriffspunkte überlastet, was sich auf den Datenfluss auswirkt. Sie können jetzt ARP-Timer so konfigurieren, dass sie die ARP-Anfragen mit bestimmten Intervall-Zeiten senden. Das Zeitintervall ist in Sekunden konfiguriert. Sie können ARP-Zeitintervalle bei der Konfiguration der Rechenzentrums-Site auf der Registerkarte **Grundeinstellungen** in der Benutzeroberfläche der Citrix SD-WAN Appliance konfigurieren.
3. (Optional, empfohlen) Speichern Sie die laufende Konfiguration.

Wenn Sie die Konfiguration nicht in einer Sitzung abschließen können, können Sie sie jederzeit speichern, sodass Sie später zurückkehren können, um sie abzuschließen. 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 **Konfigurationseditors** (oben im Seitenbereich) auf **Öffnen**. Daraufhin wird ein Dialogfeld zur Auswahl der Konfiguration angezeigt, 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 **Konfigurationseditors**). Dadurch wird das Dialogfeld **Speichern** unter geöffnet.



2. Geben Sie den Namen des Konfigurationspakets ein. Wenn Sie die Konfiguration in einem vorhandenen Paket speichern, wählen Sie vor dem Speichern unbedingt **Überschreiben zulassen**.
3. Klicken Sie auf **Speichern**.

So konfigurieren Sie 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.

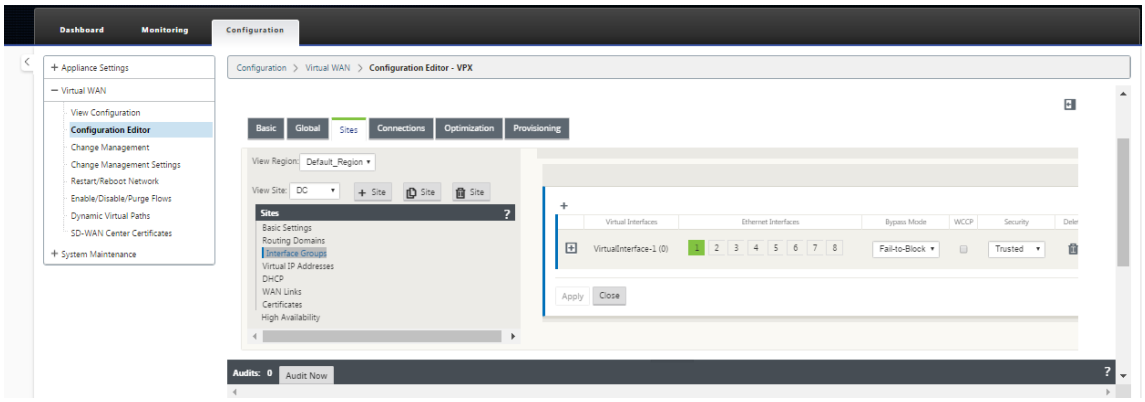
Im Folgenden sind einige Richtlinien für die Konfiguration von Virtual Interface-Gruppen aufgeführt:

- Verwenden Sie logische Namen, die die Gruppe am besten beschreiben.
- Vertrauenswürdige Netzwerke sind Netzwerke, die hinter einer Firewall geschützt sind.
- Virtuelle Schnittstellen verknüpfen Schnittstellen zu Fail-to-Wire (FTW) -Paaren.
- 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.

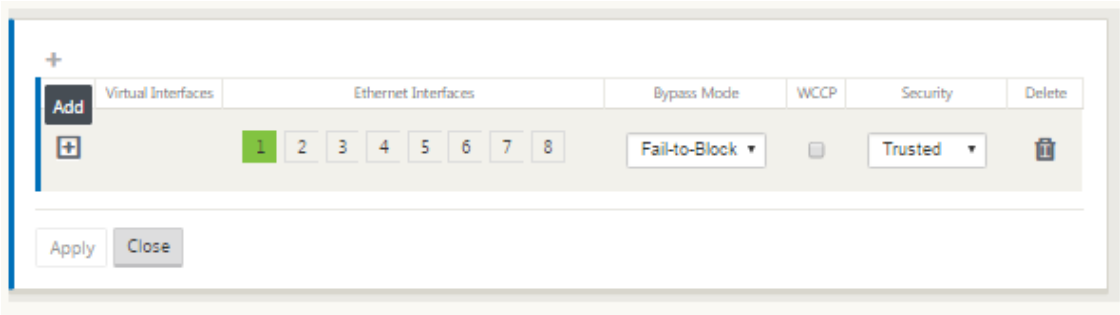
> **Hinweis**
>
> Weitere Richtlinien und Informationen zur Konfiguration von virtuellen Schnittstellengruppen finden Sie im Abschnitt Virtuelles Routing und Weiterleitung.

Gehen Sie folgendermaßen vor, um der neuen MCN-Site eine virtuelle Schnittstellengruppe hinzuzufügen:

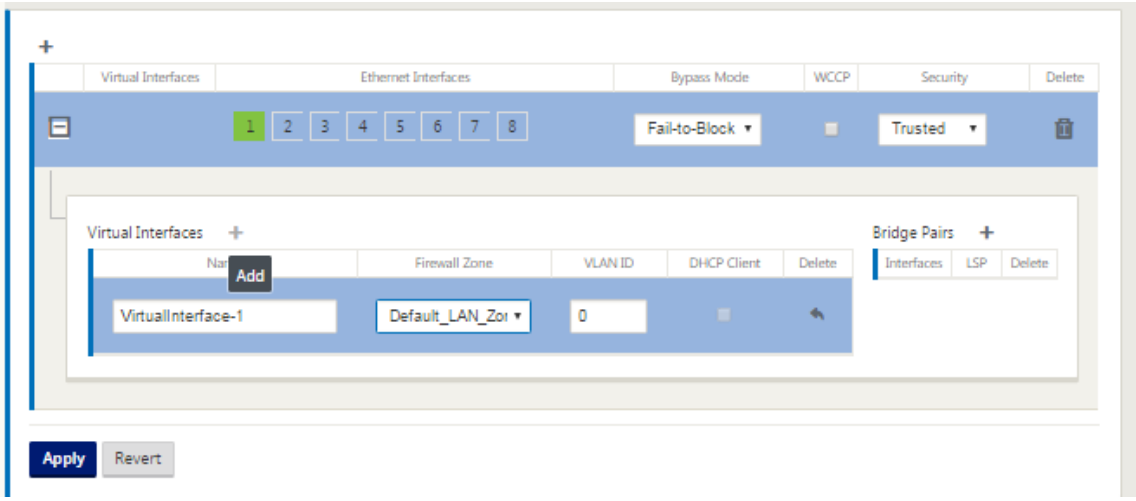
1. Wenn Sie in der Ansicht **Sites** des **Konfigurationseditors**fortfahren, wählen Sie die **Site aus dem Dropdownmenü Site anzeigen** aus. Dadurch wird die Konfigurationsansicht für den ausgewählten Standort geöffnet.



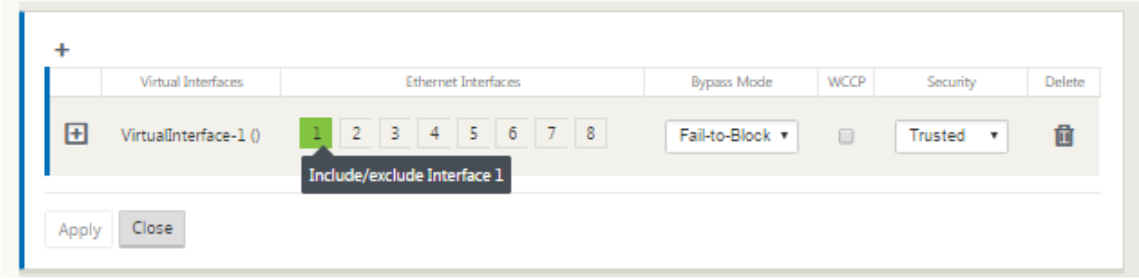
2. Klicken Sie auf **+**, um die **Gruppe der virtuellen Schnittstelle** hinzuzufügen. Dadurch wird der Tabelle ein neuer leerer Eintrag für die virtuelle Schnittstelle hinzugefügt und zur Bearbeitung geöffnet.



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 einzuschließen/auszuschließen. Sie können beliebig viele Schnittstellen auswählen, die in die Gruppe aufgenommen werden sollen.

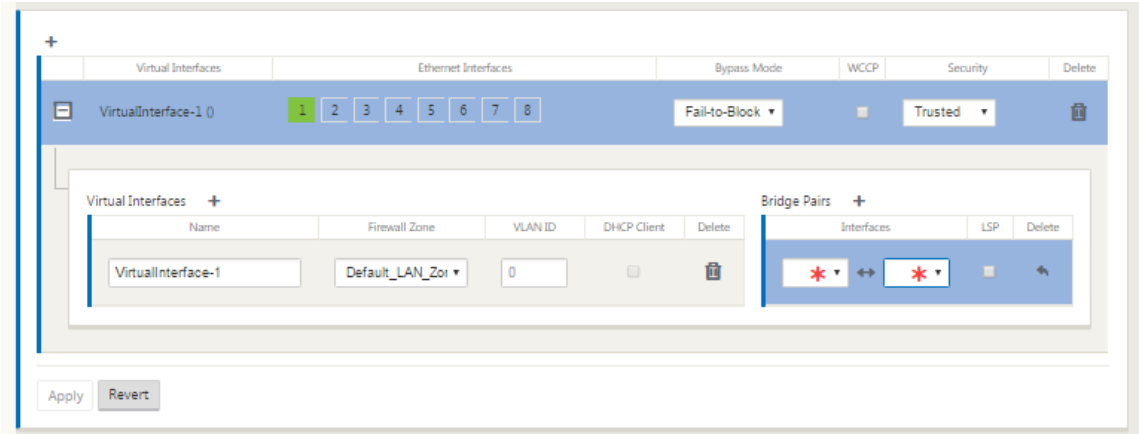


5. Wählen Sie im Dropdownmenü den **Umgehungsmodus** (keine Standardeinstellung). Der **Bypass-Modus** legt das Verhalten von Bridge-gekoppelten Schnittstellen in der virtuellen Schnittstellengruppe im Falle eines Ausfalls oder Neustarts einer Appliance oder eines Dienstes fest. Die Optionen sind: **Fail-to-Wire** oder **Fail-to-Block**.

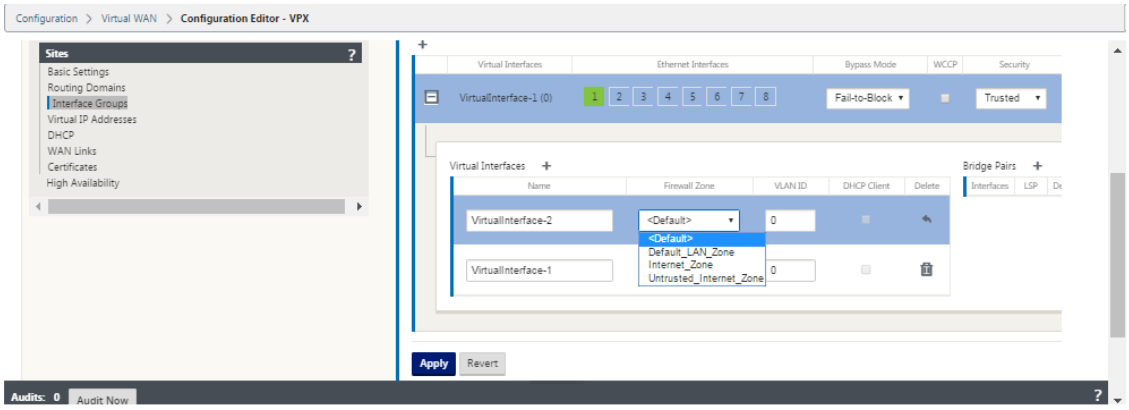
6. Wählen Sie im Dropdownmenü die **Sicherheitsstufe** aus. Dies gibt die Sicherheitsstufe für das Netzwerksegment der Virtual Interface Group an. Die Optionen sind: **Vertrauenswürdig** oder

Nicht vertrauenswürdig. Vertrauenswürdige Segmente sind durch eine Firewall geschützt (Standard ist Trusted).

7. Klicken Sie am linken Rand des virtuellen Interface, das Sie hinzugefügt haben, 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, unter dem auf dieses virtuelle Interface verwiesen wird.
   - **Firewall-Zone** - Wählen Sie eine Firewall-Zone aus dem Dropdownmenü aus.
   - **VLAN-ID** —Dies ist die ID zum Identifizieren und Markieren des Datenverkehrs zur 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 Dropdownmenü 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 **+**. Dadurch wird ein neuer **Bridge Pairs** Eintrag hinzugefügt und 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 Pairs**.
12. Klicken Sie auf **Apply**. 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 gehen Sie wie oben gezeigt vor.

So konfigurieren Sie die virtuelle IP-Adresse für den MCN

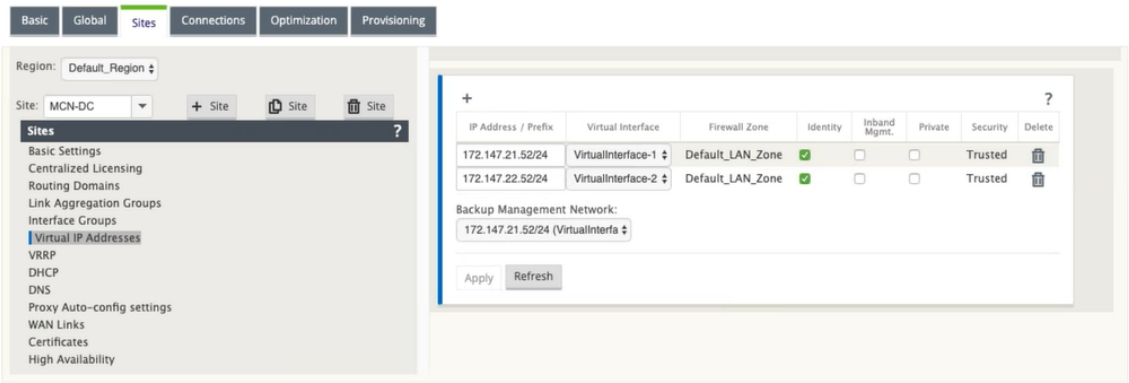
Der nächste Schritt besteht darin, die virtuellen IP-Adressen für den Standort zu konfigurieren und sie der entsprechenden Gruppe zuzuweisen.

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 die neue Site angezeigt.
2. Klicken Sie auf **+** rechts neben **Virtuelle IP-Adressen**, um eine Adresse hinzuzufügen. Dadurch wird das Formular zum Hinzufügen und Konfigurieren einer neuen virtuellen IP-Adresse geöffnet.
3. Geben Sie die ****IP-Adresse/Präfixinformationen**** ein und wählen Sie das **virtuelle Interface** aus, mit dem 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. Firewallzone, Identität, Privat und Sicherheit.

5. Wählen Sie **Inband Mgmt** aus, damit die virtuelle IP-Adresse eine Verbindung zu Verwaltungsdiensten wie Web UI und SSH herstellen kann.

   > **Hinweis:**
   >
   > Die Schnittstelle sollte vom Sicherheitstyp **Trusted** und **Identity** aktiviert sein.

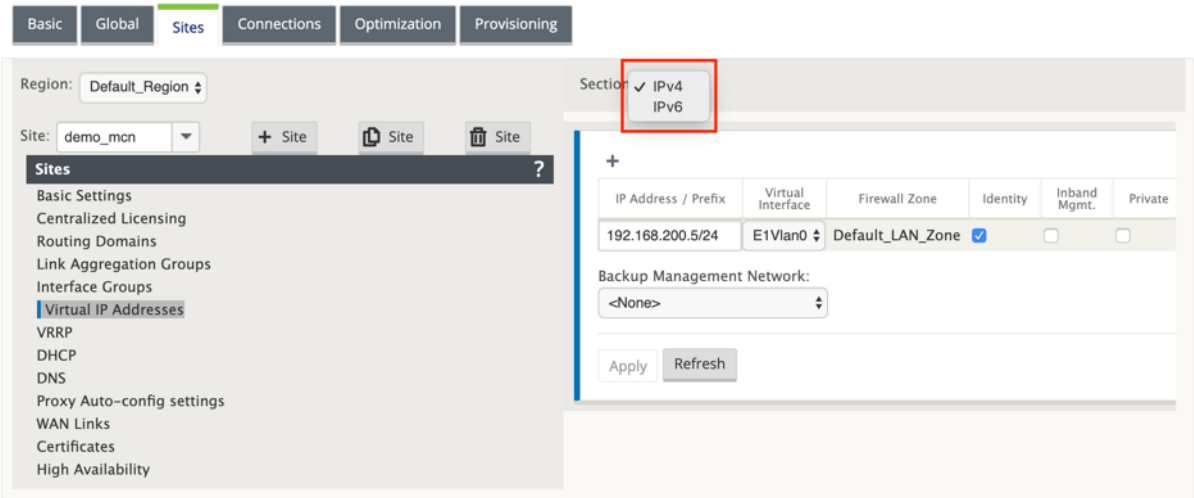
6. Wählen Sie eine virtuelle IP als **Backup-Management-Netzwerk** aus. Auf diese Weise können Sie die virtuelle IP-Adresse für die Verwaltung verwenden, wenn der Verwaltungsport nicht mit einem Standard-Gateway konfiguriert ist.



7. Klicken Sie auf **Apply**. Dadurch werden die Adressinformationen zur Site hinzugefügt und in die Tabelle **Virtuelle IP-Adressen** der Site 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-** 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.

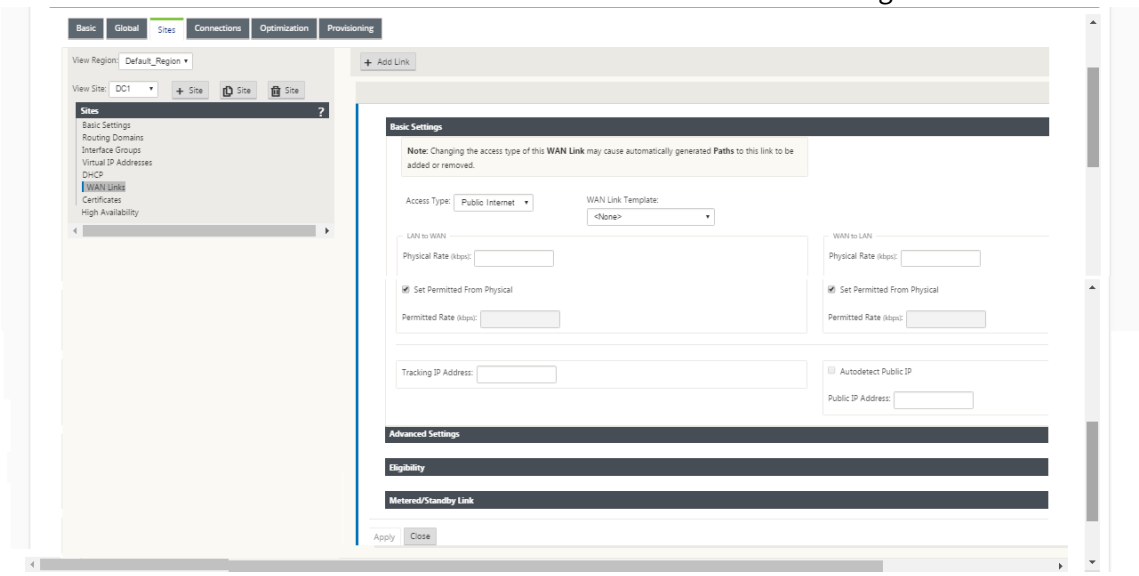
> **HINWEIS:**
> Neighbor Discovery Protocol (NDP) wird von IPv6 unterstützt.

Wenn sowohl IPv4- als auch IPv6-Access Interfaces für die lokale und die Remotesite definiert sind, wird der Pfad nur mit IPv6-Adresse geformt.

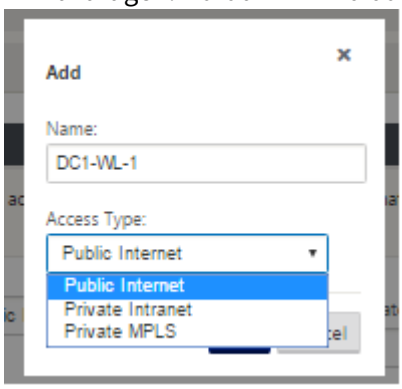
So konfigurieren Sie WAN-Links für den MCN

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** .



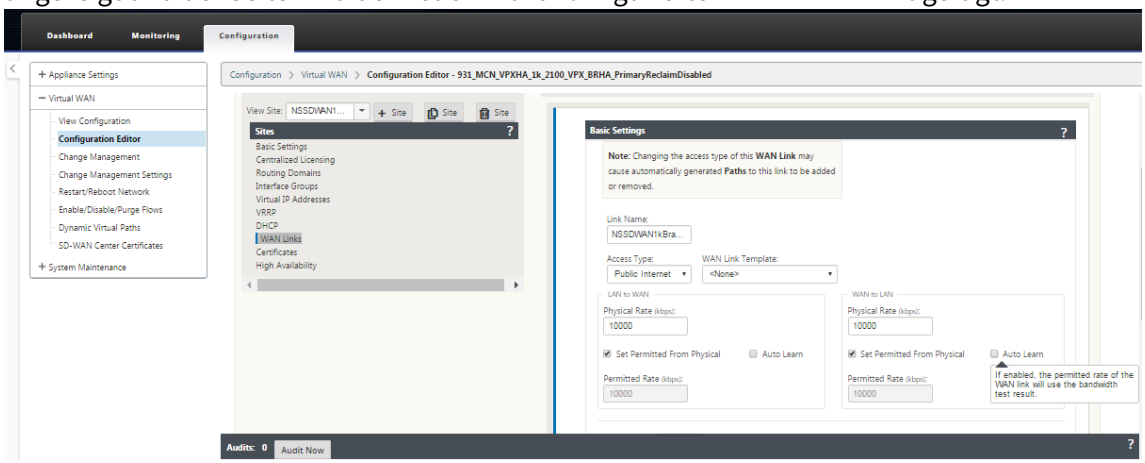
2. Klicken Sie rechts neben den **WAN-Links** auf **Link hinzufügen**, um eine neue WAN-Verbindung hinzuzufügen. Daraufhin wird das Dialogfeld **Hinzufügen** geöffnet.



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.

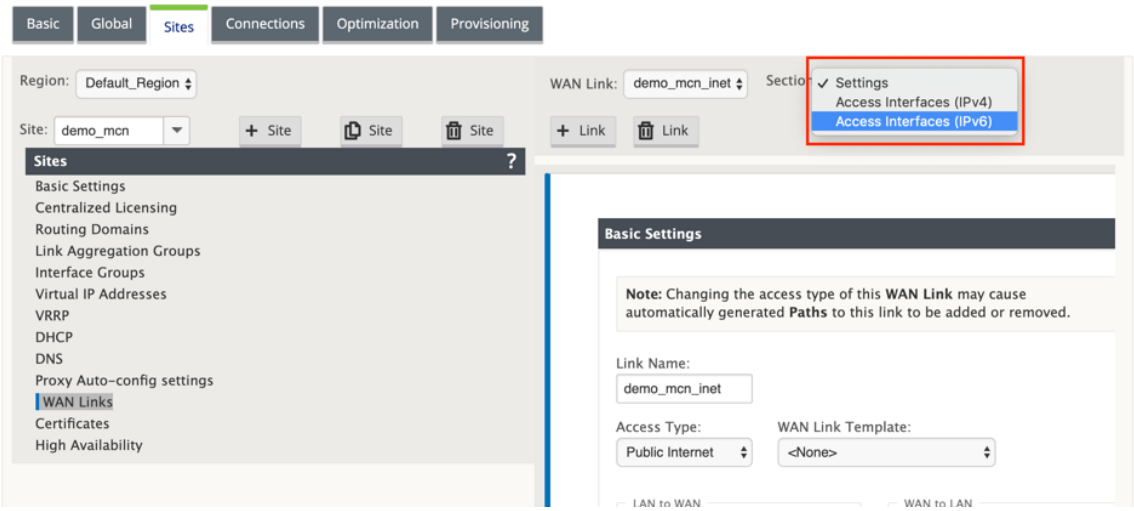
4. Wählen Sie den **Zugriffstyp** aus dem Dropdownmenü aus. Die Optionen sind **Public Internet, Private Intranet** oder **Private MPLS.**

5. 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.

1. Wählen Sie im Dropdownmenü **Einstellung** die Option **Access Interfaces (IPv6)** aus.

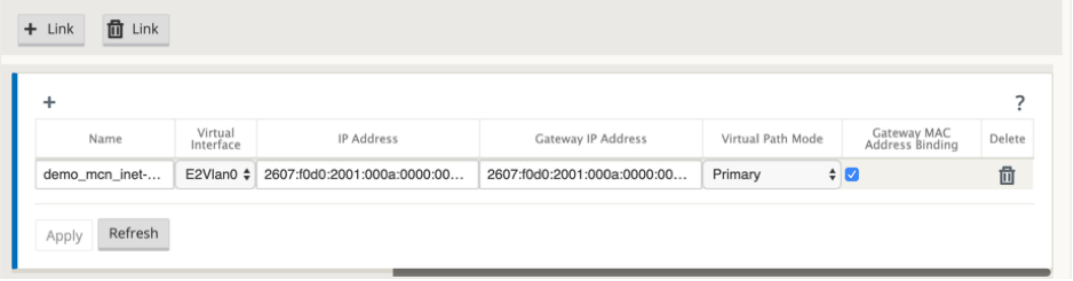


2. Definieren Sie die folgenden Felder:

   - **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 Dropdownmenü 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 Dropdownmenü 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.



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

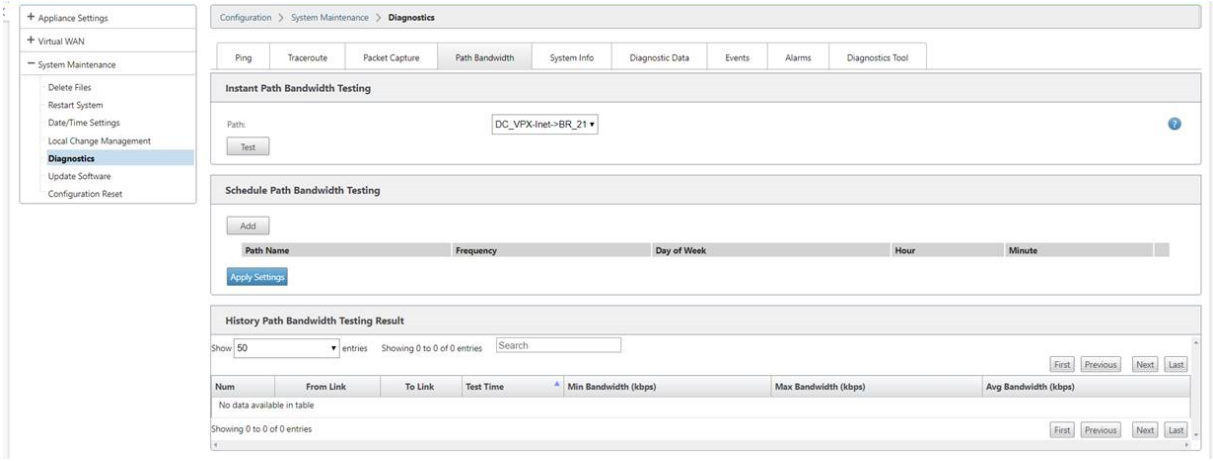
Auto Learn läuft beim Systemstart und wiederholt sich alle fünf Minuten, bis ein erfolgreiches Ergebnis beobachtet wird. Auto learn wird auch ausgeführt, nachdem Änderungen der WAN-Verbindungskonfiguration im Konfigurationseditor vorgenommen wurden.

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**

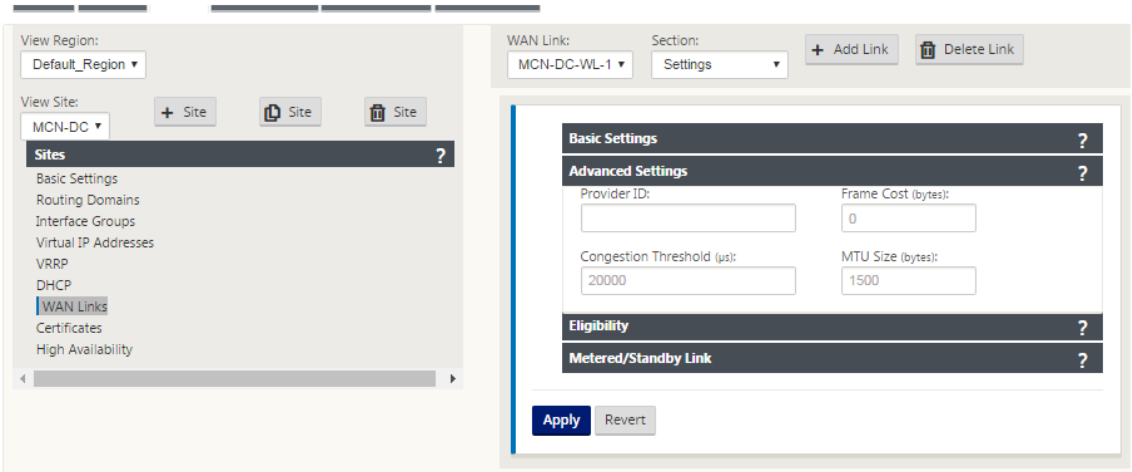
> Automatische Erkennung der WAN Link-Bandbreite, gilt nur für Zweige und nicht für MCN/RCN.



1. Geben Sie die Linkdetails für den neuen WAN-Link ein. Konfigurieren Sie die Einstellungen von LAN zu WAN, WAN zu **LAN**. Einige Richtlinien lauten wie folgt:

   - Einige Internetlinks könnten asymmetrisch sein.
   - Eine Fehlkonfiguration der zulässigen Geschwindigkeit kann die Leistung für diese Verbindung beeinträchtigen
   - Vermeiden Sie die Verwendung von Burstgeschwindigkeiten, die die festgeschriebene Rate übertreffen.
   - Fügen Sie für Internet-WAN-Verbindungen unbedingt die öffentliche IP-Adresse hinzu.

2. Klicken Sie auf die graue Bereichsleiste **Erweiterte Einstellungen**. Dadurch wird das Formular **Erweiterte Einstellungen** für den Link geöffnet.



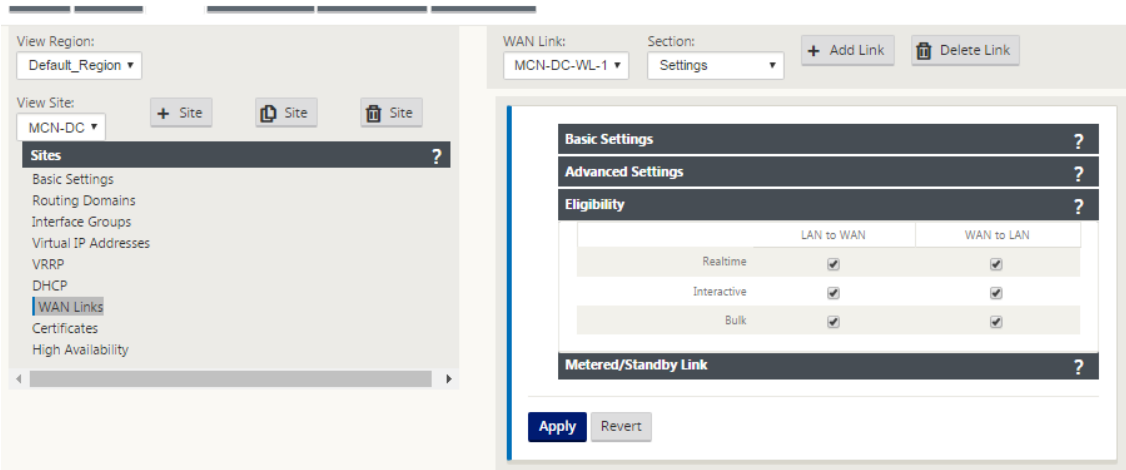
3. Geben Sie die **erweiterten Einstellungen** für den Link ein:

   - Anbieter-**ID** —(Optional) Geben Sie eine eindeutige ID-Nummer 1—100 ein, um WAN-Verbindungen zu kennzeichnen, die mit demselben Dienstanbieter verbunden sind.

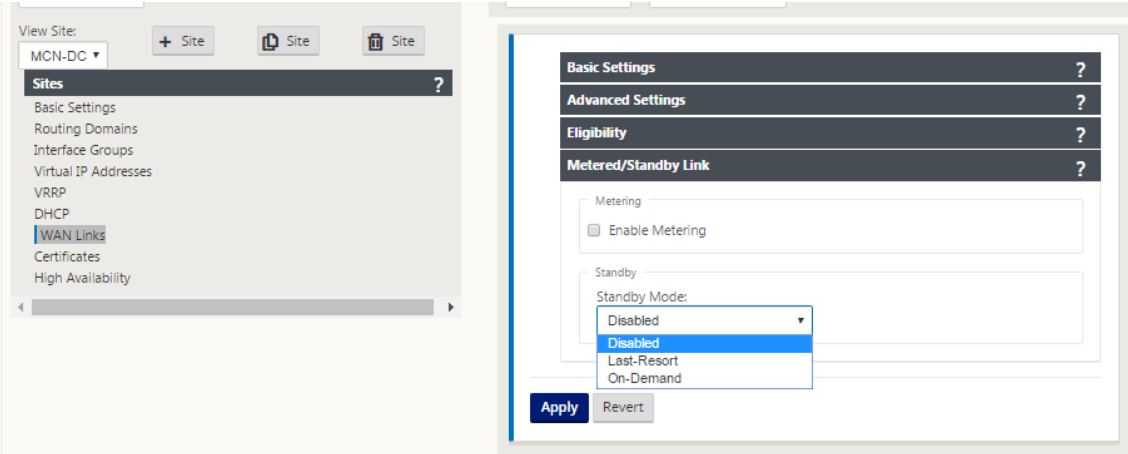
Virtual WAN verwendet die Provider-ID, um Pfade beim Senden doppelter Pakete zu unterscheiden.

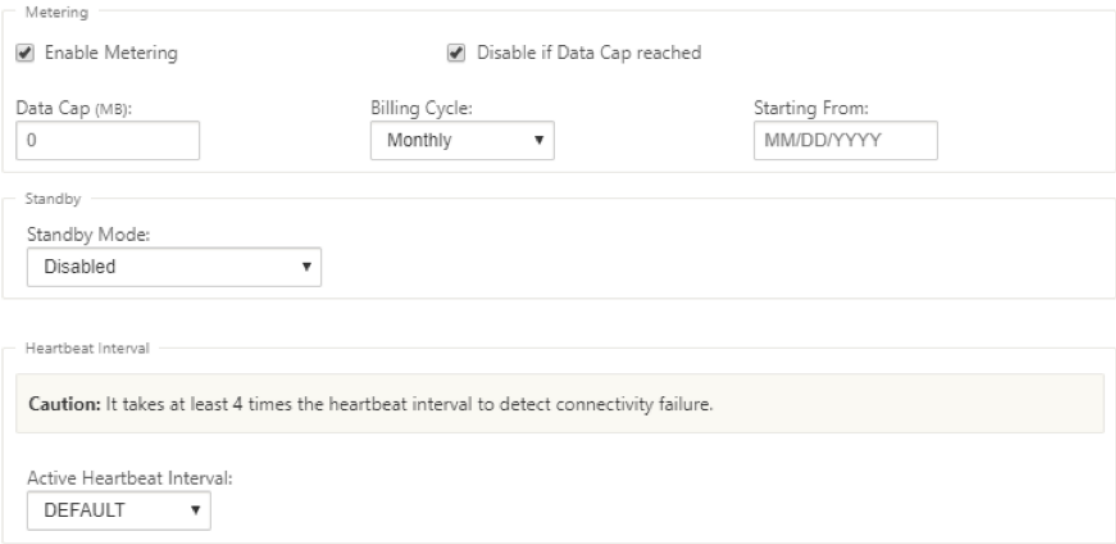
- **Framekosten (Byte)** —Geben Sie die Größe (in Byte) des Headers/Trailers ein, der jedem Paket hinzugefügt wurde. Zum Beispiel die Größe der hinzugefügten Ethernet-IPG- oder AAL5-Anhänger in Bytes.
- **Überlastungsschwelle** —Geben Sie den Überlastungsschwellenwert (in Mikrosekunden) ein, nach dem die WAN-Verbindung die Paketübertragung drosselt, um eine weitere Überlastung zu vermeiden.
- **MTU-Größe (Byte)** —Geben Sie die größte Rohpaketgröße (in Byte) ein, ohne die Framekosten.

4. Klicken Sie auf die graue Teilleiste **Berechtigung**. Dadurch wird das Formular **Berechtigungseinstellungen** für den Link geöffnet.
5. Wählen Sie die **Berechtigungseinstellungen** für den Link aus.



6. Klicken Sie auf die graue Abschnittleiste mit **Metered Link**. Dadurch wird das Einstellungsformular für **Metered Link** für den Link geöffnet.
7. (Optional) Wählen Sie **Metering aktivieren** aus, um die Messung für diesen Link zu aktivieren. Daraufhin werden die Felder **Metering-Einstellungen aktivieren** angezeigt.





8. Konfigurieren Sie die Messeinstellungen für den Link. Geben Sie Folgendes ein:

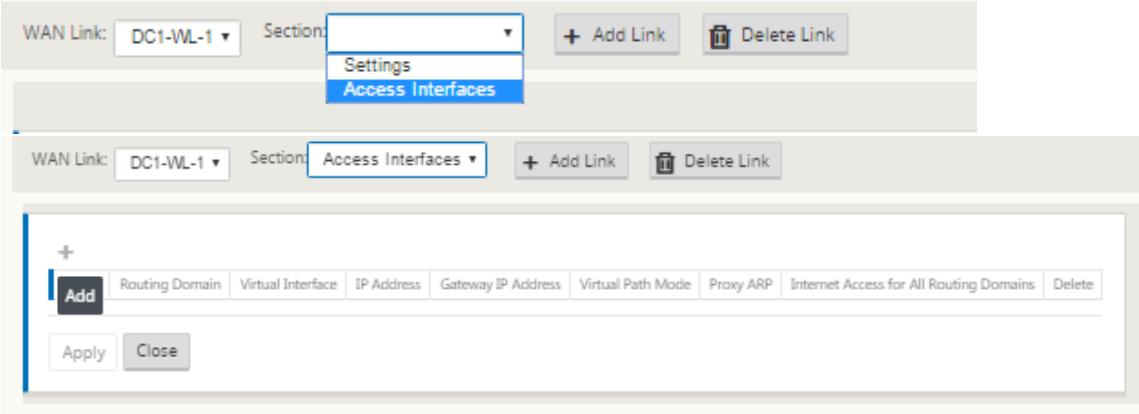
- **Datenobergrenze (MB)** —Geben Sie die Daten-Cap-Zuweisung für den Link in Megabyte ein.
- **Abrechnungszeitraum** —Wählen Sie entweder **Monatlich oder Wöchentlich** aus dem Dropdownmenü aus.
- Beginnend **von** —Geben Sie das Startdatum des Abrechnungszyklus ein.
- **Last Resort** —Wählen Sie diese Option aus, um diesen Link als Link der letzten Instanz zu aktivieren, falls alle anderen verfügbaren Links ausfallen. Unter normalen WAN-Bedingungen sendet Virtual WAN nur minimalen Datenverkehr über gemessene Verbindungen, um den Verbindungsstatus zu überprüfen. Im Falle eines Ausfalls kann SD-WAN jedoch aktive dosierte Verbindungen als letzten Ausweg für die Weiterleitung des Produktionsverkehrs verwenden.

Klicken Sie auf **Apply**. Dies wendet Ihre angegebenen Einstellungen auf die neue WAN-Verbindung an.

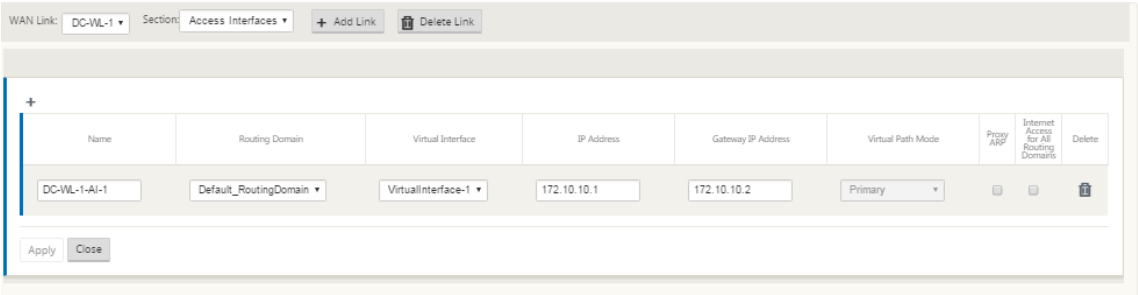
Der nächste Schritt besteht darin, die Access Interfaces für die neue WAN-Verbindung zu konfigurieren. Ein Access Interface besteht aus einer virtuellen Schnittstelle, einer WAN-Endpunkt-IP-Adresse, einer Gateway-IP-Adresse und einem virtuellen Pfadmodus, die gemeinsam als Schnittstelle für eine bestimmte WAN-Verbindung definiert sind. Jede WAN-Verbindung muss mindestens ein Access Interface haben.

So konfigurieren Sie die Zugriffsschnittstelle:

1. Wählen Sie auf der Seite WAN-Link-Konfiguration für den Link **Zugriffsschnittstellen** aus. Dadurch wird die Ansicht **Access Interfaces** für die Site geöffnet.



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, unter dem auf dieses Access Interface verwiesen wird. Geben Sie einen Namen für das neue Access Interface ein, oder übernehmen Sie die Standardeinstellung. Die Standardeinstellung verwendet die folgende Namenskonvention:
  WAN_Link_Name-AI-Number: Wobei *WAN_Link_Name* der Name des WAN-Links ist, den Sie dieser Schnittstelle zuordnen, und Nummer die Anzahl der derzeit für diese Verbindung konfigurierten Zugriffsschnittstellen ist, 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.

- **Virtuelles Interface** —Dies ist das virtuelle Interface, das dieses Access Interface verwendet. Wählen Sie einen Eintrag aus dem Dropdownmenü der Virtuellen Schnittstellen aus, die für diesen Zweigstandort konfiguriert sind.
- **Routing-Domäne** —Die Routing-Domäne, die Sie für das Access Interface 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** —Dies gibt die Priorität für den Virtual Path-Verkehr 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 **Apply**.

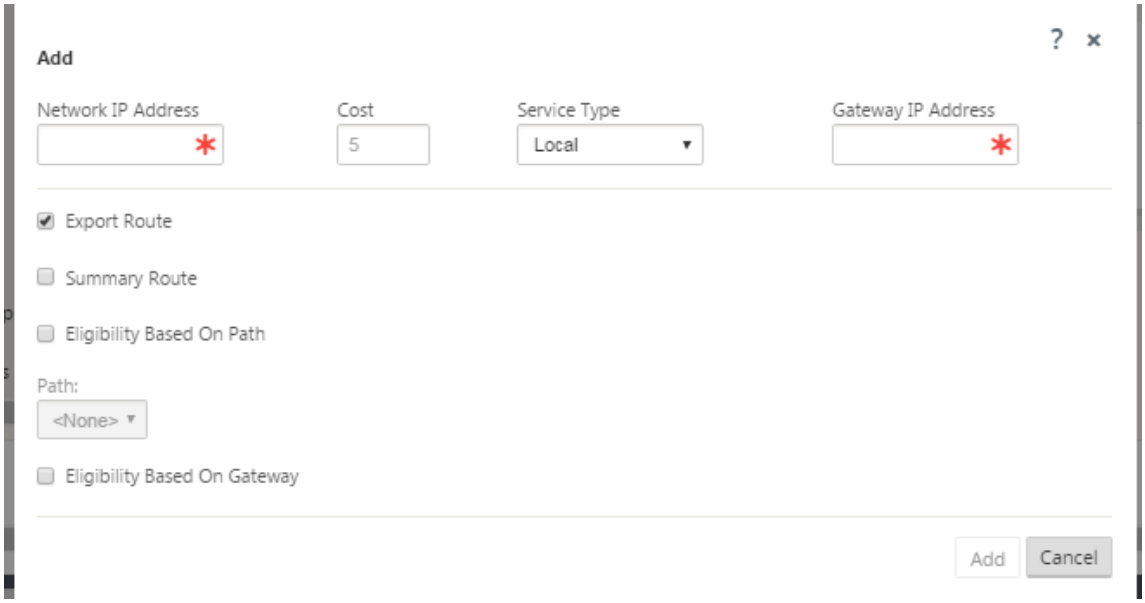
Sie haben nun die Konfiguration der neuen WAN-Verbindung abgeschlossen. Wiederholen Sie diese Schritte, um weitere WAN-Links für die Site hinzuzufügen und zu konfigurieren.

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 den neuen MCN-Standort und wählen Sie **Routen**aus. Dadurch wird die Ansicht **Routen** für die Site angezeigt.
2. Klicken Sie rechts neben **Routes** auf **+**, um eine Route hinzuzufügen. Daraufhin wird das Dialogfeld **Routen** zur Bearbeitung geöffnet.



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 ein Gewicht von 1 bis 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 erreicht, indem ständig gemessen und an sich ändernde Anwendungsanforderungen und WAN-Bedingungen angepasst werden. 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 Verkehr zwischen einer Enterprise-Site und Websites im öffentlichen Internet. Verkehr dieser Art ist nicht gekapselt. In Zeiten der Überlastung verwaltet das SD-WAN aktiv die Bandbreite, indem es den Internetverkehr relativ zum virtuellen Pfad und den Intranet-Verkehr gemäß der vom Administrator festgelegten SD-WAN-Konfiguration begrenzt.
  - **Intranet** —Dieser Dienst verwaltet Enterprise Intranet-Verkehr, 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, kann Datenverkehr, der normalerweise über einen virtuellen Pfad übertragen wird, stattdessen als Intranet-Verkehr behandelt werden, um die Netzwerkzuverlässigkeit aufrechtzuerhalten.

- **Passthrough** —Dieser Dienst verwaltet den Datenverkehr, der durch das virtuelle WAN geleitet werden soll. Der an den Passthrough-Dienst gerichtete Datenverkehr umfasst Broadcasts, ARPs und anderen Nicht-IPv4-Verkehr sowie Datenverkehr im lokalen Subnetz der Virtual WAN Appliance, konfigurierten Subnetzen oder Regeln, die vom Netzwerkadministrator angewendet werden. Dieser Verkehr wird vom SD-WAN nicht verzögert, geformt oder modifiziert. 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-Verkehr 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-Verkehr, der für einen GRE-Tunnel bestimmt ist, und entspricht dem am Standort konfigurierten LAN GRE-Tunnel. Mit der GRE-Tunnel-Funktion können Sie SD-WAN-Appliances konfigurieren, um GRE-Tunnel im LAN zu beenden. 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.

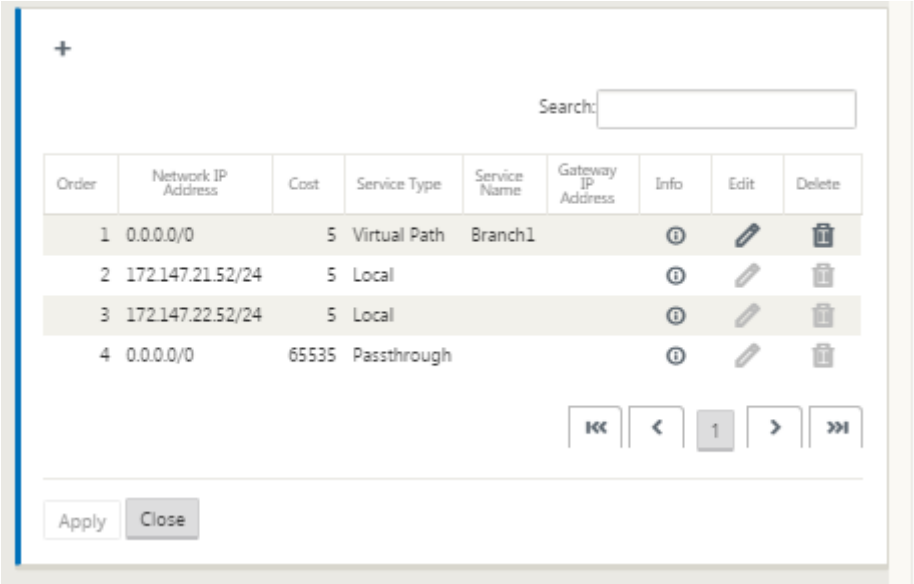
Je nach Servicetyp werden folgende Einstellungen angezeigt:

Servicetyp	Einstellungen für den Servicetyp
Virtueller Pfad	Next Hop Site —Dies gibt den Remotestandort an, an den Virtual Path-Pakete geleitet werden.

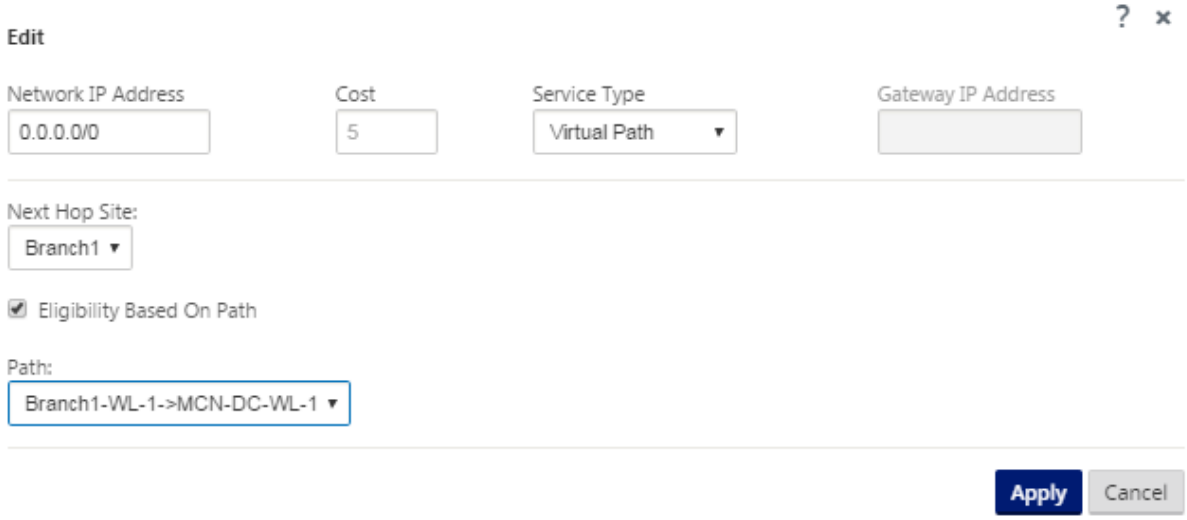
Servicetyp	Einstellungen für den Servicetyp
Internet	Route exportieren: Aktivieren/Deaktivieren, um Routen zu anderen verbundenen Standorten zu exportieren, Berechtigung basierend auf Pfad
Intranet	Route exportieren, Intranetdienst, Berechtigung basierend auf Pfad, Berechtigung basierend auf Tunnel
Passthrough	Berechtigung basierend auf Pfad
Lokal	Route exportieren, Übersichtsroute, 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, Übersichtsroute
Inter-Routing	Inter-Routingdomänendienst

1. Klicken Sie auf **Apply**.

> **Hinweis**
>
> Nachdem Sie auf **Übernehmen**geklickt haben, werden möglicherweise Audit-Warnungen angezeigt, die darauf hinweisen, dass weitere Maßnahmen erforderlich sind. Ein Roter-Punkt- oder Goldenrod-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 konfigurierte Routen auch wie folgt bearbeiten.



Um weitere Routen für die Site hinzuzufügen, klicken Sie rechts neben dem Zweig **Routen** auf **+**, und fahren Sie wie oben beschrieben fort.

Sie haben jetzt die primären Konfigurationsinformationen für den neuen MCN-Site eingegeben. Die folgenden beiden Abschnitte enthalten Anweisungen für weitere optionale Schritte:

- Konfigurieren von Hochverfügbarkeit (HA) für den MCN-Site (optional).
- Aktivieren und Konfigurieren von Virtual WAN-Sicherheit und Verschlüsselung (optional).

Wenn Sie diese Funktionen jetzt nicht konfigurieren möchten, können Sie direkt mit dem Abschnitt Benennen, Speichern und Sichern der MCN-Site-Konfiguration fortfahren.

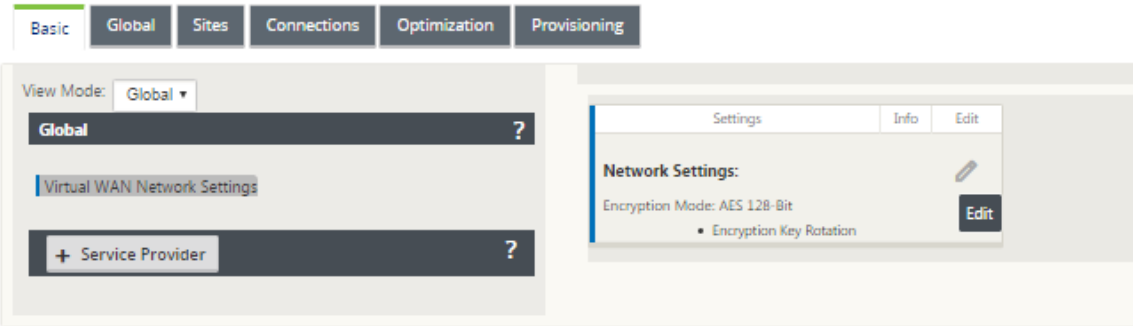
Aktivieren und Konfigurieren von Virtual WAN-Sicherheit und Verschlüsselung (optional)

October 28, 2021

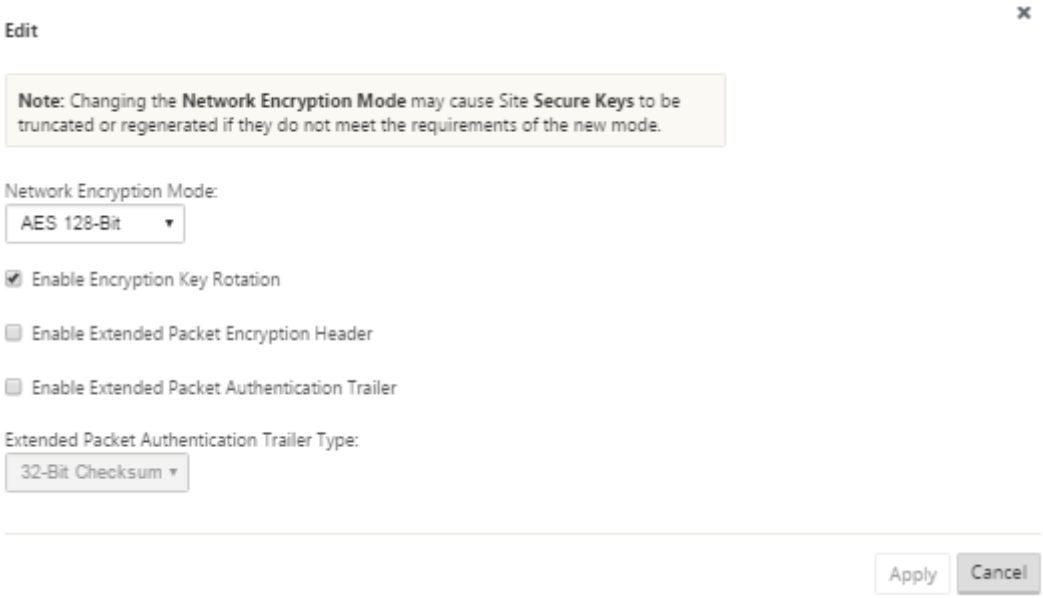
Gehen Sie wie folgt vor, um die Sicherheit und Verschlüsselung von Virtual WAN zu aktivieren und zu konfigurieren:

> **Hinweis**
>
> Die Aktivierung von Virtual WAN-Sicherheit und Verschlüsselung ist optional.

1. Navigieren Sie im **Konfigurationseditor** zur Registerkarte **Basic**, wählen Sie **Global** für den **Anzeigemodus**. Das Konfigurationsformular für virtuelle Netzwerkeinstellungen wird angezeigt.



2. Klicken Sie auf **Bearbeiten** (Stiftsymbol), um die Bearbeitung des Formulars zu ermöglichen.



3. Geben Sie Ihre globalen Sicherheitseinstellungen ein. Die folgenden Optionen stehen zur Auswahl:

   - **Netzwerkverschlüsselungsmodus** —Dies ist der Verschlüsselungsalgorithmus für verschlüsselte Pfade. Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü: **AES 128 Bit** oder **AES 256 Bit**.
   - **Enable Encryption Key Rotation**: Wenn diese Option aktiviert ist, werden Verschlüsselungsschlüssel in Intervallen von 10—15 Minuten gedreht.
   - **Extended Packet Encryption Header aktivieren**: Wenn diese Option aktiviert ist, wird ein 16-Byte-verschlüsselter Zähler dem verschlüsselten Datenverkehr vorangestellt, um als Initialisierungsvektor zu dienen und die Paketverschlüsselung zufällig zu machen.
   - **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 zugestellt wird.
   - **Trailertyp für erweiterte Paketauthentifizierung**: Dies ist der Anhängertyp, der zur Validierung des Paketinhalts verwendet wird. Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü: **32-Bit-Prüfsumme** oder **SHA-256**.

4. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen auf die Konfiguration zu übernehmen.

Damit ist die Konfiguration der MCN-Site abgeschlossen. Der nächste Schritt besteht darin, die neue MCN-Site-Konfiguration 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.

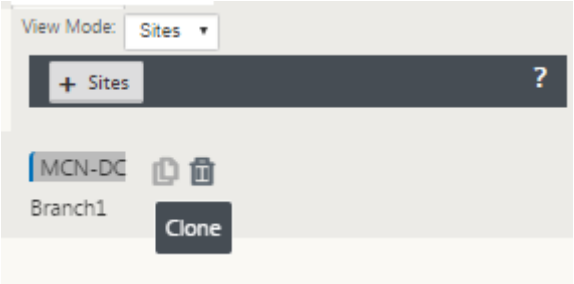
Die primäre Umschaltung von MCN zu sekundärem MCN erfolgt nach 15 Sekunden, wenn der primäre MCN inaktiv ist. Sie können den primären Rückgewinn für sekundären MCN nicht konfigurieren, die primäre Rückgewinnung erfolgt automatisch, nachdem das primäre Gerät wieder eingeschaltet ist und der Haltezeitgeber 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.

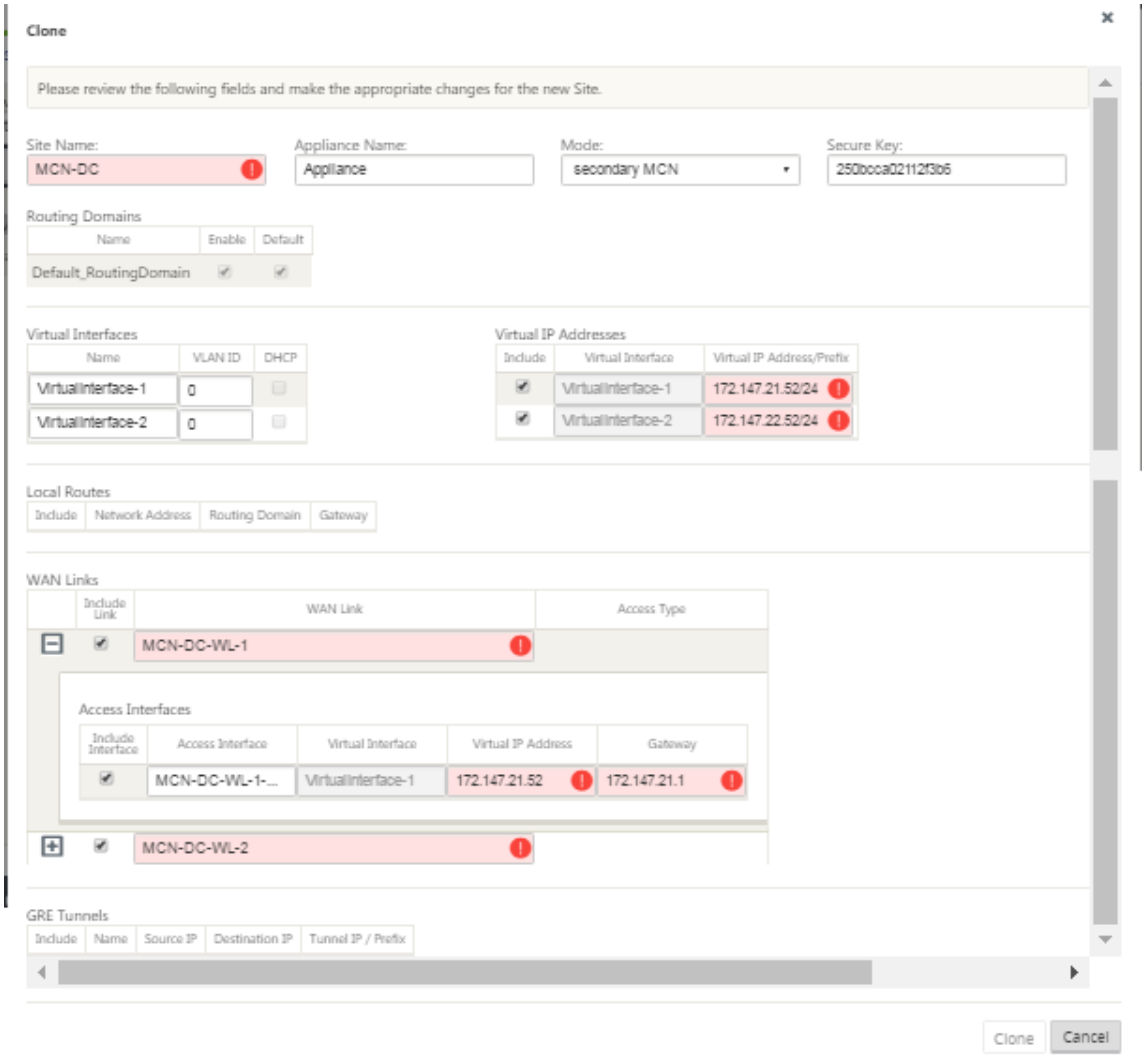
> **Hinweis**
>
> Sie können einen MCN klonen, um einen sekundären MCN oder Zweigstandorte zu erstellen. Sie können nur einen sekundären MCN konfigurieren.

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.



> **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

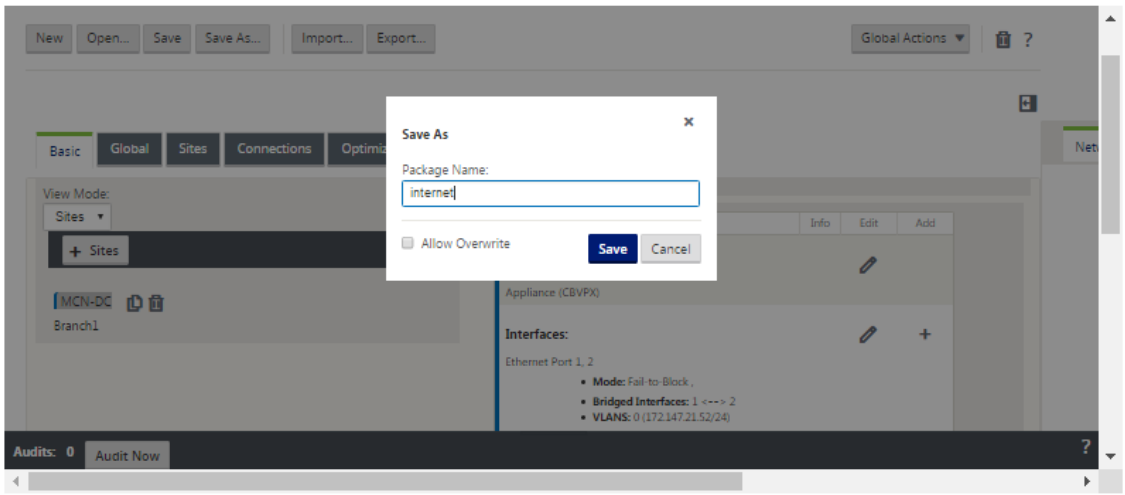
MCN-Konfiguration verwalten

October 28, 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 vom Management Webinterface ab und setzen den Konfigurationsvorgang 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 auftritt oder Sie sich vor dem Speichern Ihrer 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 wird empfohlen, Speichern unter anstelle von Speichern zu verwenden, um zu vermeiden, dass das falsche Konfigurationspaket überschrieben wird.

1. Klicken Sie auf **Speichern** unter (oben im mittleren Bereich des **Konfigurationseditors**). Das Dialogfeld **Speichern** unter wird geöffnet.



2. Geben Sie den Namen des Konfigurationspakets ein.

> **Hinweis**
>
> Wenn Sie die Konfiguration in einem vorhandenen Konfigurationspaket speichern, wählen Sie vor dem Speichern unbedingt **Überschreiben zulassen** aus.

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 Konfigurationseditor.

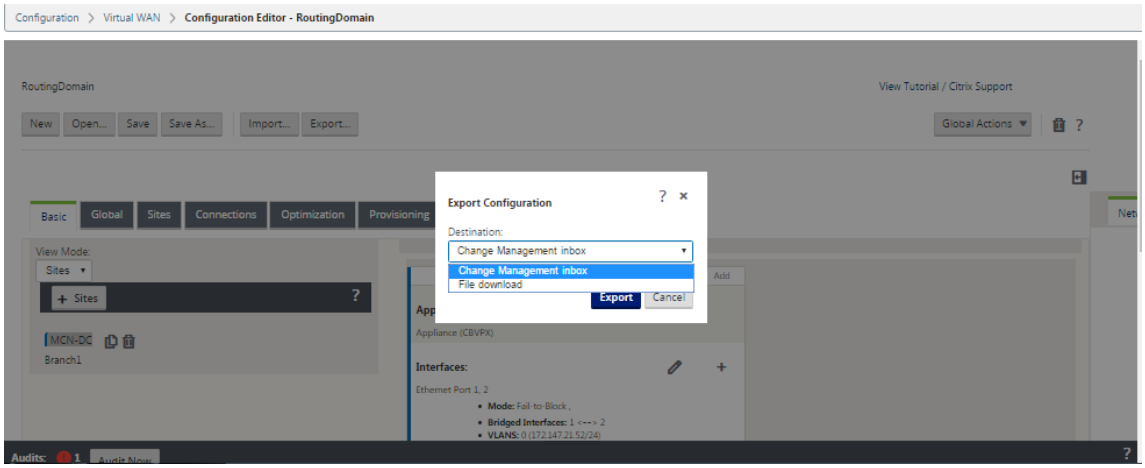
Sie haben nun die MCN-Standortkonfiguration abgeschlossen und ein neues SD-WAN-Konfigurationspaket erstellt. Sie können nun die Zweig-Sites hinzufügen und konfigurieren. Anweisungen finden Sie unter Setup Branch Sites](/en-us/citrix-sd-wan/current-release/configuration/setup-branch-nodes.html).

Exportieren eines Backups des Konfigurationspakets

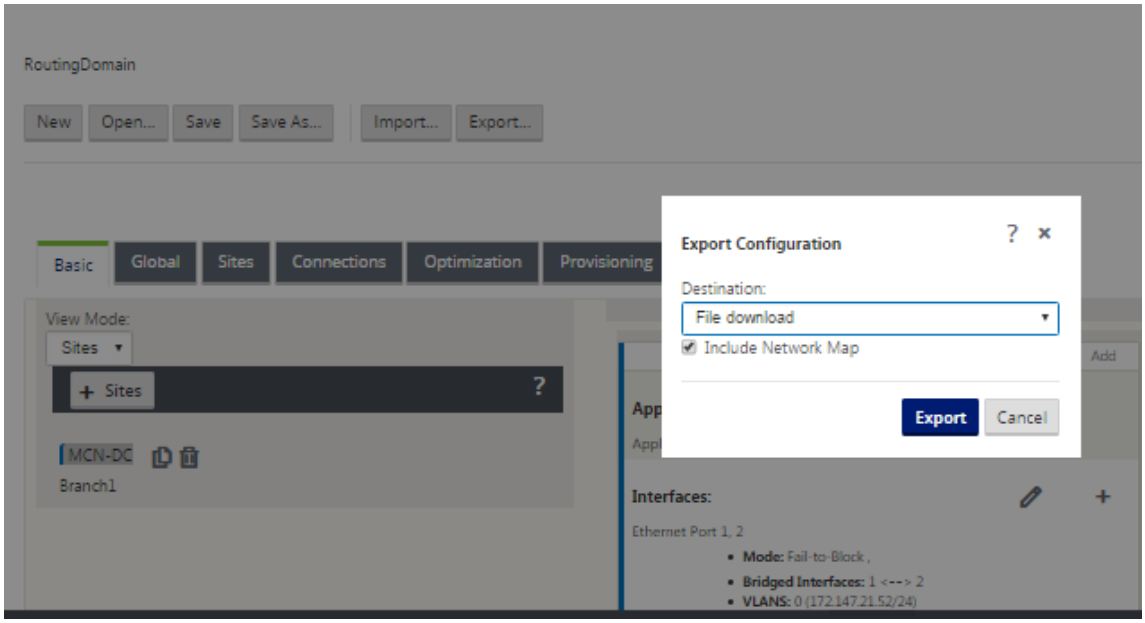
Zusätzlich zum Speichern der laufenden Konfiguration in Ihrem Appliance-Workspace wird empfohlen, die Konfiguration regelmäßig auf Ihrem lokalen PC zu sichern.

Gehen Sie wie folgt vor, um das aktuelle Konfigurationspaket auf Ihren PC zu exportieren:

1. Klicken Sie auf **Exportieren**. Dadurch wird das Dialogfeld **Konfiguration exportieren** angezeigt.



2. Wählen Sie im Dropdownmenü “**Ziel:** “die Option “**Dateidownload**”. Dadurch wird die Option **Netzwerkzuordnung einschließen** angezeigt, die standardmäßig ausgewählt ist.



3. Akzeptieren 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 zum Speichern der Konfiguration.
4. Navigieren Sie zum Speicherort auf Ihrem PC und klicken Sie auf **Speichern**. Dadurch wird das Konfigurationspaket auf Ihrem PC gespeichert.

> **Hinweis**
>
> Um ein gesicherte Konfigurationspaket wiederherzustellen, können Sie einen **Importvorgang** verwenden, um das Paket von Ihrem PC zu importieren und in den **Konfigurationseditor**zu laden. Sie können das importierte Paket dann zur zukünftigen Verwendung in Ihrem Management-Webinterface-Arbeitsbereich speichern.

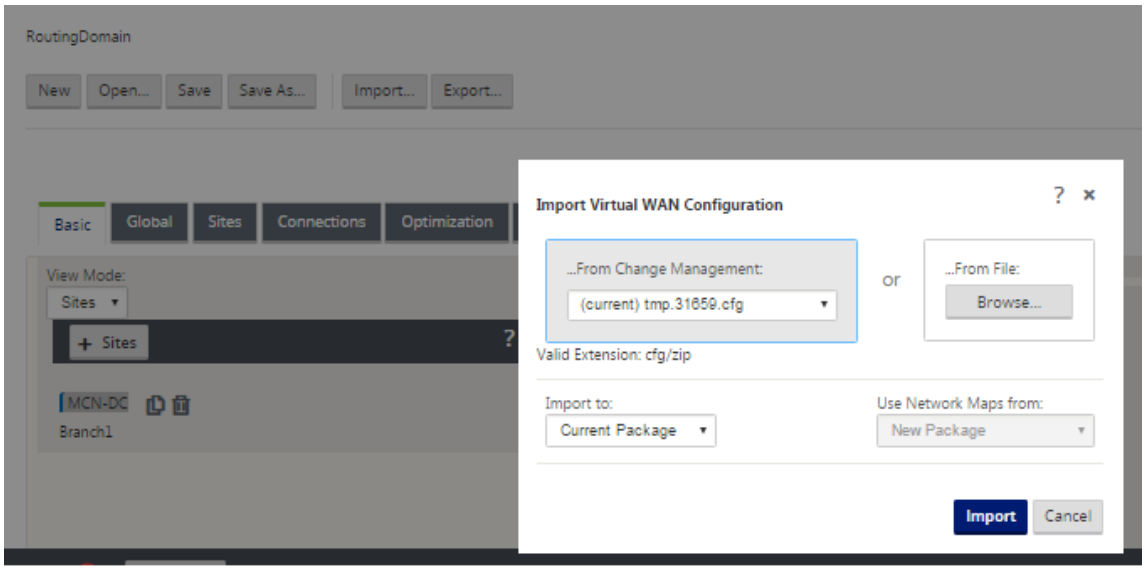
Import gesichertes Konfigurationspaket

Manchmal möchten Sie möglicherweise zu einer früheren Version eines Konfigurationspakets zurückkehren. Wenn Sie eine Kopie der früheren Version auf Ihrem lokalen PC gespeichert haben, können Sie sie wieder in den Konfigurationseditor importieren und dann zur Bearbeitung öffnen. Wenn dies keine Erstbereitstellung ist, können Sie auch ein vorhandenes Konfigurationspaket aus dem globalen Change Management-Posteingang auf dem aktuellen MCN importieren. Anweisungen für diese beiden Verfahren sind nachstehend aufgeführt.

Gehen Sie wie folgt vor, um ein Konfigurationspaket zu importieren:

1. Öffnen Sie den **Konfigurationseditor**.
2. Klicken Sie in der Menüleiste des **Konfigurationseditors** auf **Importieren**.

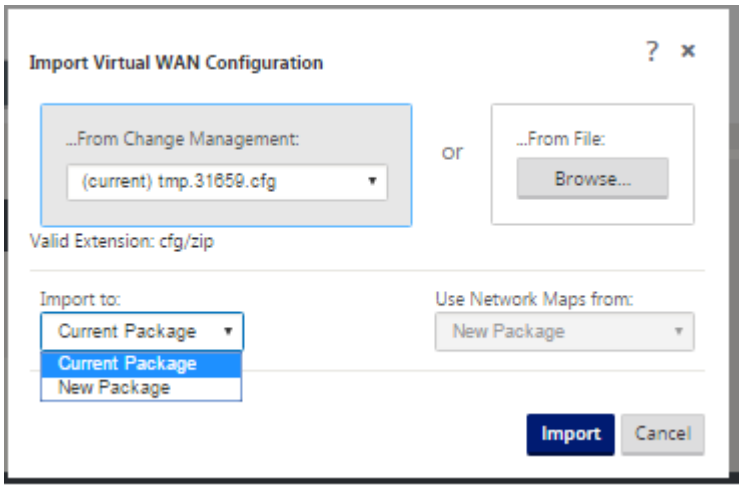
Das Dialogfeld **Virtuelle WAN-Konfiguration importieren** wird angezeigt.



3. Wählen Sie den Ort aus, von dem das Paket importiert werden soll.

   - So importieren Sie ein Konfigurationspaket aus Change Management: Wählen Sie das Paket **aus dem Dropdownmenü Aus Change Management** aus (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 aus (falls zutreffend). Wenn ein Konfigurationspaket bereits im **Konfigurationseditor geöffnet ist,** ist das Dropdownmenü **Importieren nach:** verfügbar.



Wählen Sie eine der folgenden Optionen:

Aktuelles Paket —Wählen Sie diese Option, 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 ermöglichen.

- **Neues Paket** —Wählen Sie diese Option aus, um ein neues, leeres Konfigurationspaket zu öffnen und mit dem Inhalt des importierten Pakets zu füllen. Das neue Paket hat automatisch denselben Namen wie das importierte Paket.

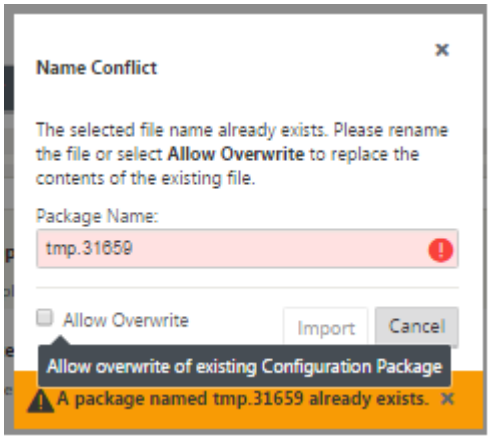
5. Geben Sie an, welche Netzwerkzuordnungen enthalten sind (falls zutreffend) Wenn ein Konfigurationspaket bereits im **Konfigurationseditor**geöffnet ist, ist das Dropdownmenü **Netzwerkzuordnungen verwenden von:** verfügbar.

Wählen Sie eine der folgenden Optionen:

- Aktuelles Paket —Hierbei werden die Netzwerkzuordnungen beibehalten, die derzeit im Paket konfiguriert sind, das jetzt im Konfigurationseditor verfügbar ist, und alle Netzwerkzuordnungen aus dem importierten Paket werden verworfen.
- Neues Paket —Dies ersetzt die derzeit im aktuell geöffneten Paket konfigurierten Netzwerkzuordnungen durch die Netzwerkzuordnungen (falls vorhanden) aus dem importierten Paket.
- Beide **Pakete** —Dies schließt alle Netzwerkzuordnungen sowohl des aktuellen als auch des importierten Pakets ein.

6. Klicken Sie auf **Importieren**. Die importierte Datei wird gemäß Ihren Vorgaben in den **Konfigurationseditor**geladen.

> **Hinweis**
>
> Wenn ein Paket mit demselben Namen in Ihrem Workspace vorhanden ist, wird das Dialogfeld **Namenskonflikt** angezeigt.



Um den Namen anzugeben, der für das importierte Paket verwendet werden soll, führen Sie einen der folgenden Schritte aus:

- Geben Sie einen anderen Namen in das Feld **Paketname** ein, um das neue Paket umzubenennen und die Schaltfläche **Importieren** zu aktivieren. Das importierte Paket wird mit dem angegebenen Namen in den **Konfigurationseditor** geladen. Der Paketname wird jetzt in Ihrem Workspace gespeichert, aber der Paketinhalt wird 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 ermöglichen 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 Import abzuschließen.

Gesichertes Konfigurationspaket

Um die Arbeit an einem gespeicherten Konfigurationspaket fortzusetzen, müssen Sie zuerst das Paket öffnen und in den **Konfigurationseditor laden.**

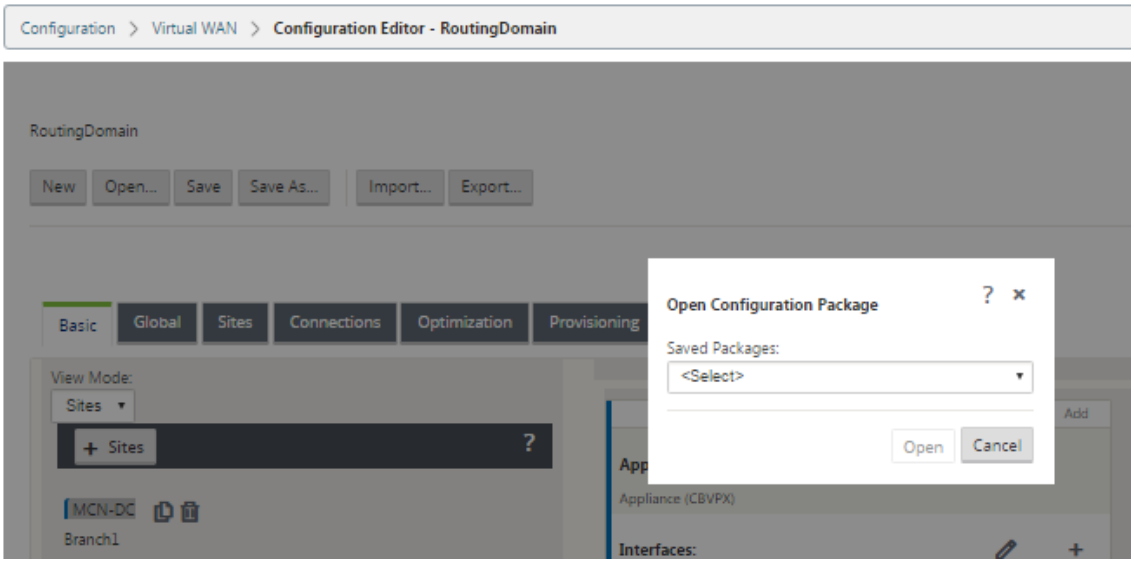
Gehen Sie wie folgt vor, um ein gespeichertes Konfigurationspaket zu laden:

1. Melden Sie sich wieder beim Management-Webinterface an und navigieren Sie zum **Konfigurationseditor**. Dadurch wird die Hauptseite des **Konfigurationseditors** für eine neue Sitzung geöffnet.

   Wenn Sie sich wieder beim Management-Webinterface angemeldet haben, wird der **Konfigurationseditor** zunächst für eine neue Sitzung geöffnet, ohne dass ein Konfigurationspaket geladen ist. Sie können eine neue Konfiguration starten (**neu**), eine vorhandene gespeicherte

Konfiguration öffnen (**Öffnen**) oder importieren (Importieren**)** und dann eine Konfiguration öffnen **(Öffnen**), die zuvor auf Ihrem lokalen PC gesichert wurde.

2. Klicken Sie auf **Öffnen**. Das Dialogfeld "**Konfigurationspaket öffnen** "wird angezeigt.



3. Wählen Sie im Dropdownmenü **Gespeicherte Pakete** das zu öffnende Paket aus.

> **Hinweis**
>
> Wenn Sie den **Konfigurationseditor**geöffnet haben, kann es je nach Anzahl der Konfigurationen, die Sie in Ihrem Workspace **gespeichert haben, einige Sekunden, eine Minute oder zwei Minuten dauern, bis das Menü Gespeicherte Pakete** gefüllt ist. Wenn ja, zeigt das Menüfeld **Gespeicherte Pakete** in der Zwischenzeit möglicherweise die Meldung **Keine gespeicherten Paketen**an. In diesem Fall klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, einige Augenblicke zu warten und erneut auf **Öffnen** zu klicken, um das Dialogfeld erneut zu öffnen.

4. Klicken Sie auf **Öffnen**.

> **Hinweis**
>
> Dadurch wird das angegebene Konfigurationspaket geöffnet und nur zur Bearbeitung in den **Konfigurationseditor** geladen. Dadurch wird für die ausgewählte Konfiguration für die lokale Appliance kein Staging oder Aktivieren durchführt.

Umbenennen von Sites

Wenn Sie den Namen der MCN-Site im Konfigurationseditor ändern, müssen Sie die Konfiguration mit der umbenannten Site auf das MCN- und SD-WAN-Netzwerk anwenden. Abhängig von der MCN-

Rolle und ob Hochverfügbarkeit aktiviert oder deaktiviert ist, gelten die folgenden Szenarien für die SD-WAN-Netzwerkkonfiguration 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 **Local Change Management** des MCN.
   a) Laden Sie das zuvor heruntergeladene Paket hoch.
   b) Klicken Sie nach Abschluss der Verarbeitung auf **Weiter**.
   c) Klicken Sie auf **Aktivieren**.

> **Hinweis**
>
> Nachdem Schritt 3 (c) abgeschlossen ist, aktiviert der Change-Management-Prozess automatisch die gestagte Software für Appliances (Knoten) im Netzwerk.

Umbenennen von MCN-Site mit hoher Verfügbarkeit

Nach dem Umbenennen des MCN, 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 **Local Change Management** 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 Änderungsmanagementprozess automatisch die gestagte Software für Appliances im Netzwerk.

GEO-Site umbenennen

So laden Sie eine neue Konfiguration für eine umbenannte GEO-Site hoch:

1. Vom MCN, Stagingnetzwerk 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 auf dem **MCN** die Option **Activate Staged** für das Netzwerk 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 einer GEO-Site mit hoher Verfügbarkeit

So laden Sie eine neue Konfiguration mit einer umbenannten GEO-Site hoch, die mit hoher Verfügbarkeit aktiviert ist:

1. Vom MCN, Stagingnetzwerk mit neuer Konfiguration, die die umbenannte GEO-Site enthält.
2. Laden Sie vom MCN das Staging-Konfigurationspaket für die aktiven und hochverfügbaren Appliances mit der umbenannten GEO-Site herunter.
3. Wählen Sie auf dem **MCNAktivieren Sie Staged** für das Netzwerk aus. Dadurch wird die umbenannte Site deaktiviert, und die Site wird nicht mehr verfügbar.
4. Navigieren Sie zur aktiven GEO-Appliance.
   a) Rufen Sie die Seite Local Change Management auf.
   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 das Standby-Gerät.

RCN-Site umbenennen

So laden Sie eine neue Konfiguration mit umbenannter RCN-Site hoch:

1. Aus dem MCN das Netzwerk mit einer neuen Konfiguration, die den umbenannten RCN-Site enthält.
2. Laden Sie vom MCN das Staging-Paket für die umbenannte RCN-Site herunter.
3. Wählen Sie auf dem **MCN** die Option **Activate Staged** für das Netzwerk 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 Local Change Management 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**
   >
   > Es dauert einige Zeit, bis die Niederlassungen in der Region verfügbar sind, da die Regionsbereitstellung erst erfolgt, nachdem Schritt 4 (c) abgeschlossen ist. Der Change-Management-Prozess des RCN verwaltet das Staging der Region.

Umbenennen von RCN-Site mit hoher Verfügbarkeit

Hochladen einer neuen Konfiguration mit umbenannter RCN-Site, die mit hoher Verfügbarkeit aktiviert ist.

1. Aus dem MCN das Netzwerk mit einer neuen Konfiguration, die den umbenannten RCN-Site enthält.
2. Laden Sie vom MCN das Staging-Paket für die aktiven und hochverfügbaren 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 auf dem **MCN** die Option **Activate Staged** für das Netzwerk aus.
4. Deaktivieren Sie den Dienst auf der Standby-RCN-Appliance.
5. Navigieren Sie zur Seite **Local Change Management** 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-Appliance.
6. Aktivieren Sie den Dienst auf der Standby-RCN-Appliance.

Umbenennen der GEO RCN-Site

So laden Sie eine neue Konfiguration mit umbenannter 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 Staging-Paket für die umbenannte GEO RCN-Site herunter.
3. Wählen Sie auf dem **MCN** die Option **Activate Staged** für das Netzwerk 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** von 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 vom MCN das Staging-Paket für die aktive und hochverfügbare Appliance für die umbenannte GEO RCN-Site herunter.
3. Wählen Sie auf dem **MCN** die Option **Activate Staged** für das Netzwerk 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 aktiven Seite “**Lokales Änderungsmanagement** “von 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

October 28, 2021

Dieses Kapitel enthält Anweisungen zum Hinzufügen und Konfigurieren der Zweigstandorte. Das Verfahren zum Hinzufügen eines Zweigstandorts ist dem Erstellen und Konfigurieren des MCN-Standorts sehr ähnlich. Einige Konfigurationsschritte und -einstellungen unterscheiden sich jedoch geringfügig für einen Zweigstandort. Sobald Sie einen ersten Zweigstandort hinzugefügt haben, können Sie außerdem für Standorte mit demselben Appliance-Modell die Funktion **Klonen** (Duplizieren) verwenden, um den Prozess des Hinzufügens und Konfigurierens dieser Sites zu optimieren.

Wie beim Erstellen des MCN-Standorts zum Einrichten eines Zweigstandorts müssen Sie den **Konfigurationseditor** im Management-Webinterface auf der MCN-Appliance verwenden. Der **Konfigurationseditor** ist nur verfügbar, wenn die Schnittstelle auf den **MCN-Konsolenmodus** eingestellt ist.

Zusätzliche Informationen zur Bereitstellung von Zweigstellen

Zusätzlich zu diesem Leitfaden werden die folgenden Knowledge Base-Supportartikel empfohlen:

- Bereitstellungsschritte im virtuellen WAN PBR-Modus (CTX201577)

  http://support.citrix.com/article/CTX201577

- Bereitstellungsschritte für den virtuellen WAN-Gatewaymodus (CTX201576)

  http://support.citrix.com/article/CTX201576

Übersicht über die Konfigurationsprozeduren für Zweigstandort

Die Schritte zum Abschließen dieses Vorgangs lauten wie folgt:

1. Fügen Sie die Niederlassung 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 Modelle der virtuellen WAN-Appliance müssen sowohl für die ursprüngliche als auch für die geklonten Sites identisch sein. Sie können das angegebene Einheitenmodell für einen Klon nicht ändern. Wenn das Appliance-Modell für einen Standort anders ist, müssen Sie die Site manuell hinzufügen.

9. Beheben Sie alle Konfigurations-Audit-Warnungen.
10. Speichern Sie die abgeschlossene Konfiguration.

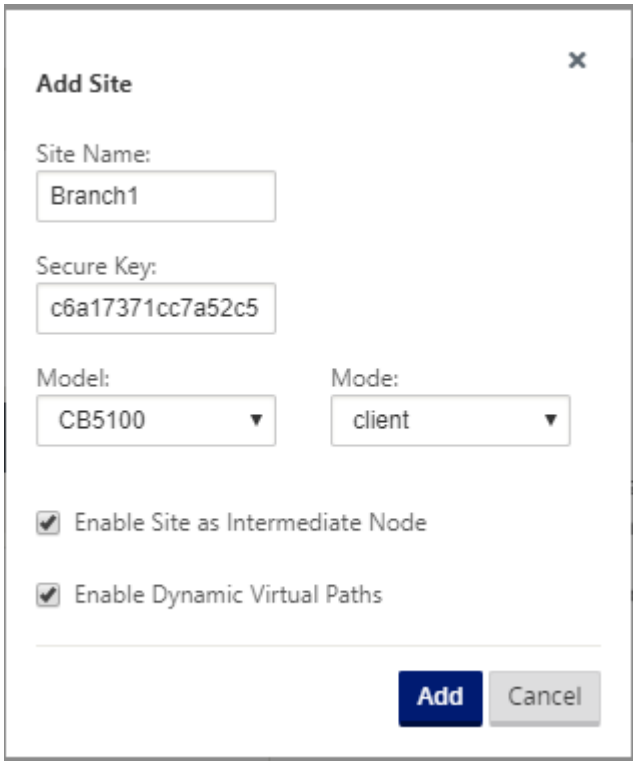
Zweigknoten konfigurieren

October 28, 2021

Gehen Sie wie folgt 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 **Konfigurationseditors** (oben im Seitenbereich) auf **Öffnen**. Daraufhin wird ein Dialogfeld zur Auswahl der Konfiguration angezeigt, die Sie ändern möchten.

1. Klicken Sie im **Konfigurationseditor**in der **Sites-Leiste** auf **Hinzufügen**, um mit dem Hinzufügen und Konfigurieren des neuen Zweigstandorts zu beginnen. Das Dialogfeld **Site hinzufügen** wird angezeigt.

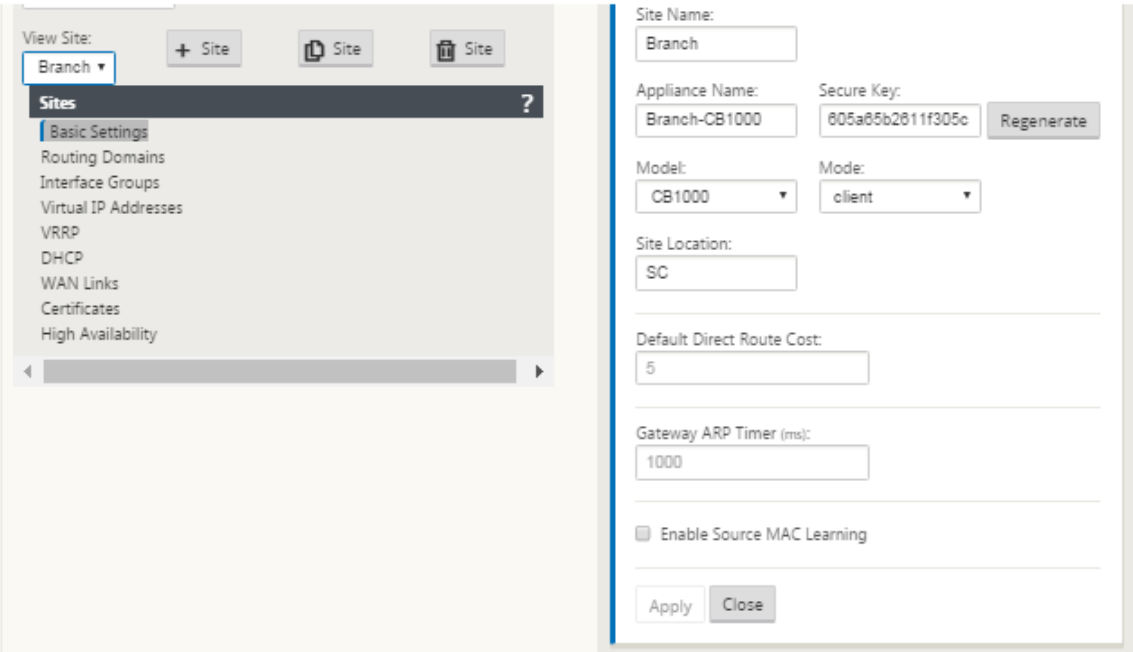


2. Geben Sie die folgenden Siteinformationen ein.

> **Hinweis**
>
> Einträge dürfen keine Leerzeichen enthalten und müssen im Linux-Format vorliegen.

- **Site-Name** —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—32 Ziffern, der zur Verschlüsselung und Überprüfung der Mitgliedschaft in der SD-WAN-Appliance verwendet wird. Standardmäßig ist dieses Feld mit einem automatisch generierten Sicherheitsschlüssel vorgefüllt. Akzeptieren Sie die Standardeinstellung oder geben Sie ein benutzerdefiniertes Hexadezimalformat ein.
- **Modell** —Wählen Sie das Einheitenmodell 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.



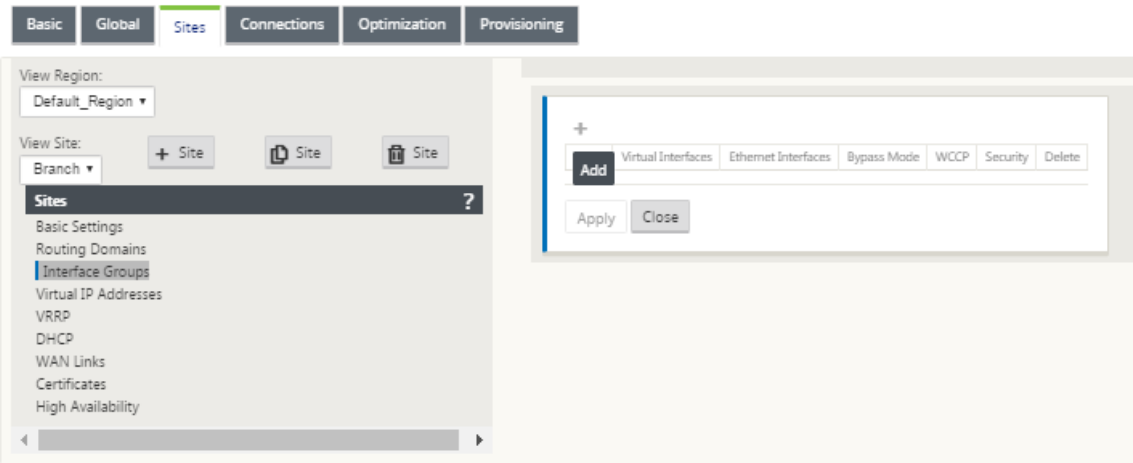
4. Geben Sie die Grundeinstellungen für die Website ein, und klicken Sie auf **Übernehmen**.

   Der nächste Schritt besteht darin, die Schnittstellengruppen für den neuen Zweigstandort hinzuzufügen und zu konfigurieren.

So konfigurieren Sie Schnittstellengruppen für den Zweig

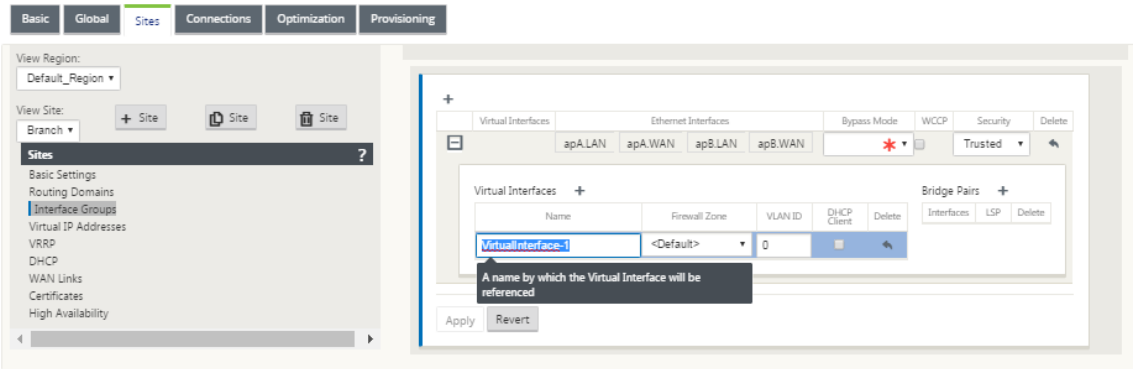
Gehen Sie folgendermaßen vor, um der neuen Zweigstellensite eine Schnittstellengruppe hinzuzufügen:

1. Wenn Sie in der **Sites-Ansicht** des **Konfigurationseditors**fortfahren, wählen Sie die Zweigstelle aus dem Dropdownmenü **Site** aus. Dadurch wird die Konfigurationsansicht für den ausgewählten Standort geöffnet.



2. Klicken Sie auf **+**, um die **Gruppe der virtuellen Schnittstelle** hinzuzufügen. Ein neuer leerer Gruppeneintrag für virtuelle Schnittstellen wird der Tabelle 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 einzuschließen/auszuschließen. Sie können beliebig viele Schnittstellen auswählen, die in die Gruppe aufgenommen werden sollen.

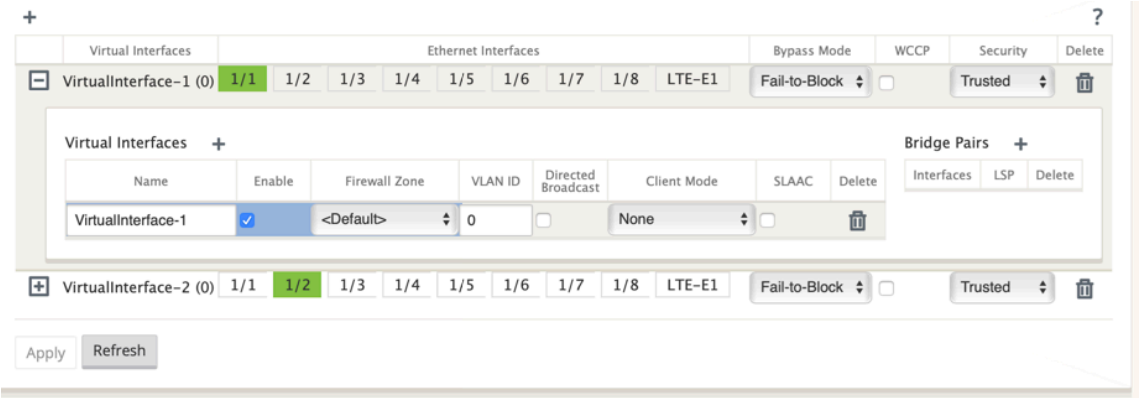
5. Wählen Sie im Dropdownmenü den **Umgehungsmodus** (keine Standardeinstellung).

   Der **Bypass-Modus** legt das Verhalten von Bridge-gekoppelten Schnittstellen in der virtuellen Schnittstellengruppe im Falle eines Ausfalls oder Neustarts einer Appliance oder eines Dienstes fest. Die Optionen sind: **Fail-to-Wire** oder **Fail-to-Block**.

6. Wählen Sie im Dropdownmenü die **Sicherheitsstufe** aus.

   Dies gibt die Sicherheitsstufe für das Netzwerksegment der Virtual Interface Group an. Die Optionen sind: **Vertrauenswürdig** oder **Nicht vertrauenswürdig**. Vertrauenswürdige Segmente sind durch eine Firewall geschützt (Standard ist Trusted).

7. Klicken Sie am linken Rand des virtuellen Interface, das Sie hinzugefügt haben, auf **+**. Daraufhin wird die Tabelle **Virtuelle Schnittstellen** angezeigt.



8. Klicken Sie rechts neben **Virtuelle Schnittstellen** auf **+**. Die IDs **Name, Firewallzone** 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.
   - **Aktivieren** - Standardmäßig ist das Kontrollkästchen **Aktivieren** für alle virtuellen Schnittstellen aktiviert. Wenn Sie die virtuelle Schnittstelle deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Aktivieren**.

     > **Hinweis**
     >
     > – Die Option zum Deaktivieren einer virtuellen Schnittstelle ist nur verfügbar, wenn sie nicht von einem WAN Link Access Interface verwendet wird. Wenn die virtuelle Schnittstelle von einem WAN-Link-Zugriffsschnittstelle verwendet wird, ist das Kontrollkästchen schreibgeschützt und standardmäßig aktiviert.
     > – Bei der Konfiguration anderer Funktionen zusammen mit aktivierten virtuellen Schnittstellen werden auch die deaktivierten virtuellen Schnittstellen aufgelistet, mit Ausnahme von **Access Interfaces** for a **WAN-Link**. Selbst wenn Sie eine deaktivierte virtuelle Schnittstelle auswählen, wird die virtuelle Schnittstelle nicht berücksichtigt und hat keine Auswirkungen auf die Netzwerkkonfiguration.

   - **Firewall-Zone** - Wählen Sie eine Firewall-Zone aus dem Dropdownmenü aus.
   - **VLAN-ID** —Die ID zum Identifizieren und Markieren des Datenverkehrs zur 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 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 Pairs**.

12. Klicken Sie auf **Apply**. 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 gehen Sie wie oben vor.

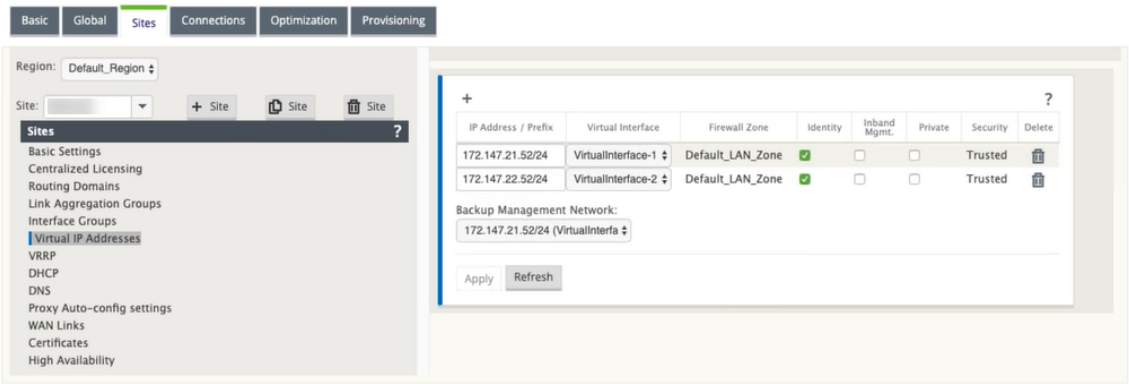
So konfigurieren Sie die virtuelle IP-Adresse für den Zweigstandort

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 die neue Site angezeigt.
2. Klicken Sie auf **+** rechts neben **Virtuelle IP-Adressen**, 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. Firewallzone, Identität, Privat und Sicherheit.
5. Wählen Sie **Inband Mgmt** aus, damit die virtuelle IP-Adresse eine Verbindung zu Verwaltungsdiensten wie Web UI und SSH herstellen kann.

    > **Hinweis:**
    >
    > Die Schnittstelle muss vom Sicherheitstyp **Trusted** und **Identity** aktiviert sein.

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.

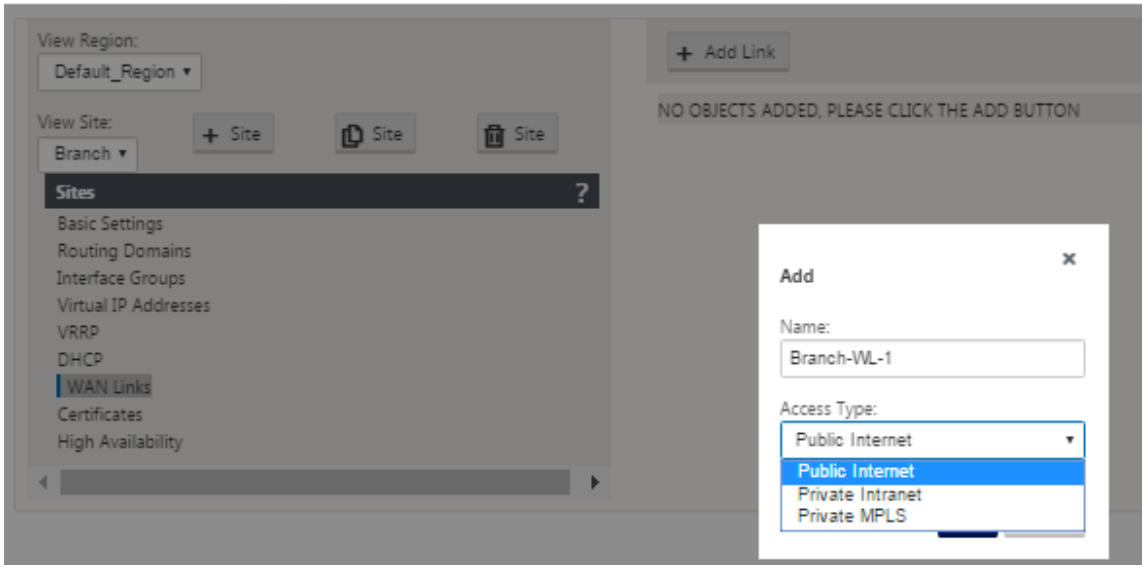


7. Klicken Sie auf **Apply**. Die Adressinformationen zur Site werden hinzugefügt und in die Tabelle **Virtuelle IP-Adressen** des Standorts aufgenommen.
8. Um weitere virtuelle IP-Adressen hinzuzufügen, klicken Sie rechts neben den **Virtuellen IP-Adressen** auf **+**, und fahren Sie wie oben beschrieben 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 das Label **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:

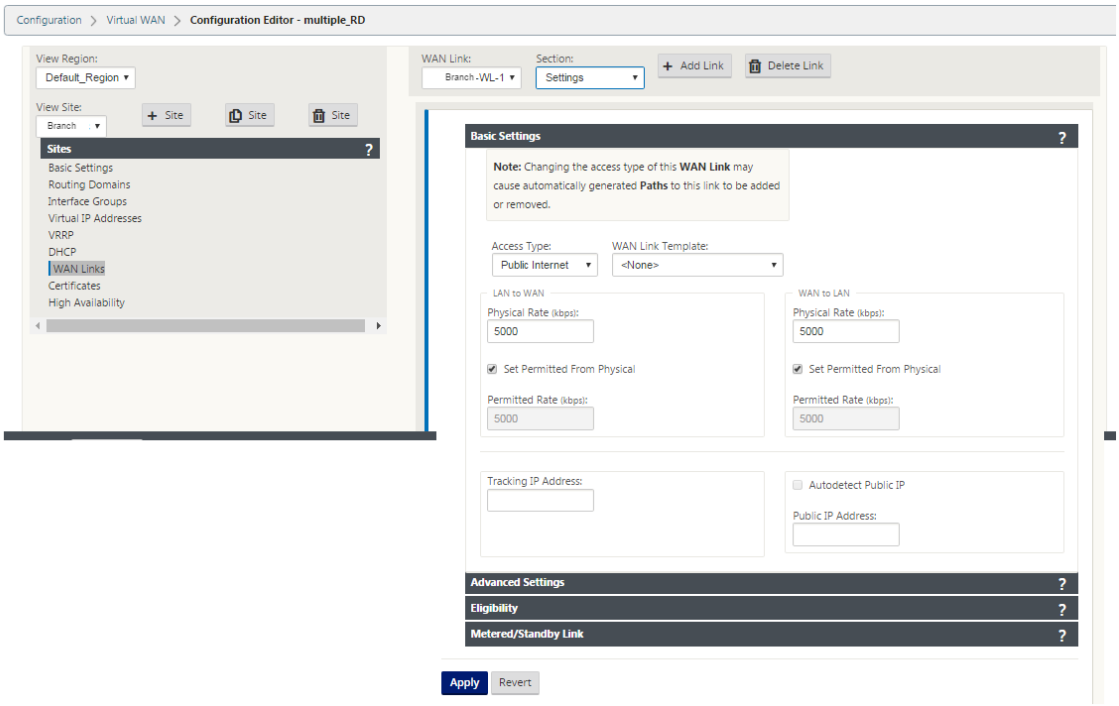
-WL- <number>

Wo <number>ist die Anzahl der WAN-Links für diese Site, erhöht um eins.

4. Wählen Sie den **Zugriffstyp** aus dem Dropdownmenü aus.

   Die Optionen sind **Public Internet, Private Intranet** oder **Private Multiprotocol Label Switching.**

5. Klicken Sie auf **Hinzufügen**. Die Konfigurationsseite für **WAN-Links-Grundeinstellungen** wird angezeigt und fügt der Seite den neuen nicht konfigurierten WAN-Link hinzu.

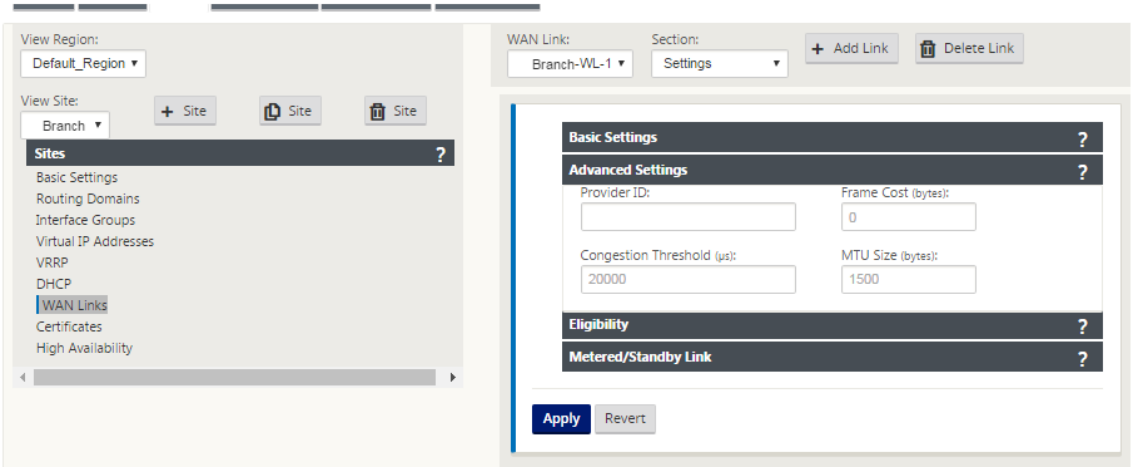


6. Geben Sie die Verknüpfungsdetails für die neue WAN-Verbindung ein. Konfigurieren Sie die Einstellungen von LAN zu WAN, WAN zu **LAN**.

   Einige Richtlinien lauten wie folgt:

   - Einige Internetlinks könnten asymmetrisch sein. Eine Fehlkonfiguration der zulässigen Geschwindigkeit kann die Leistung für diese Verbindung beeinträchtigen.
   - Vermeiden Sie die Verwendung von Burstgeschwindigkeiten, die die festgeschriebene Rate übertreffen.
   - Fügen Sie für Internet-WAN-Verbindungen unbedingt die öffentliche IP-Adresse hinzu.

7. Klicken Sie auf die graue Bereichsleiste **Erweiterte Einstellungen**. Dadurch wird das Formular **Erweiterte Einstellungen** für den Link geöffnet.

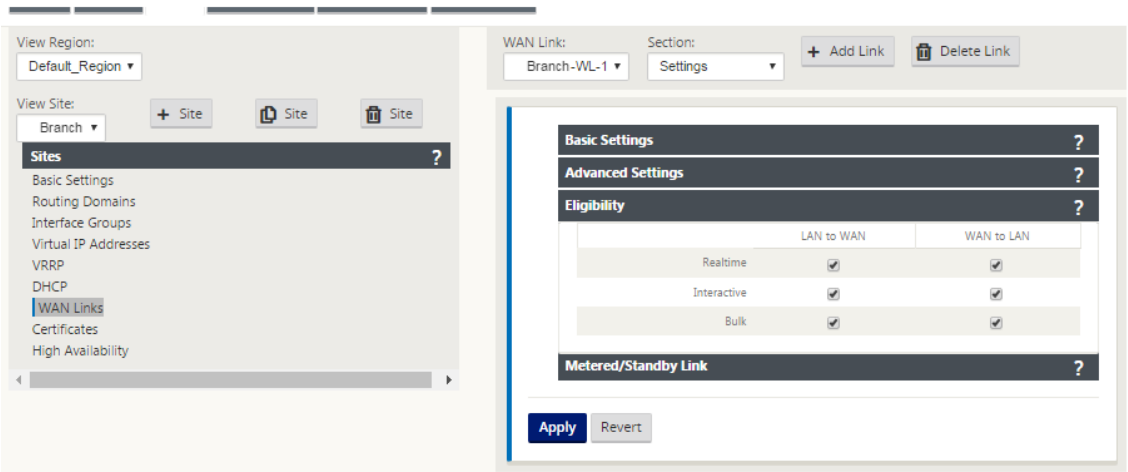


8. Geben Sie die **erweiterten Einstellungen** für den Link ein.

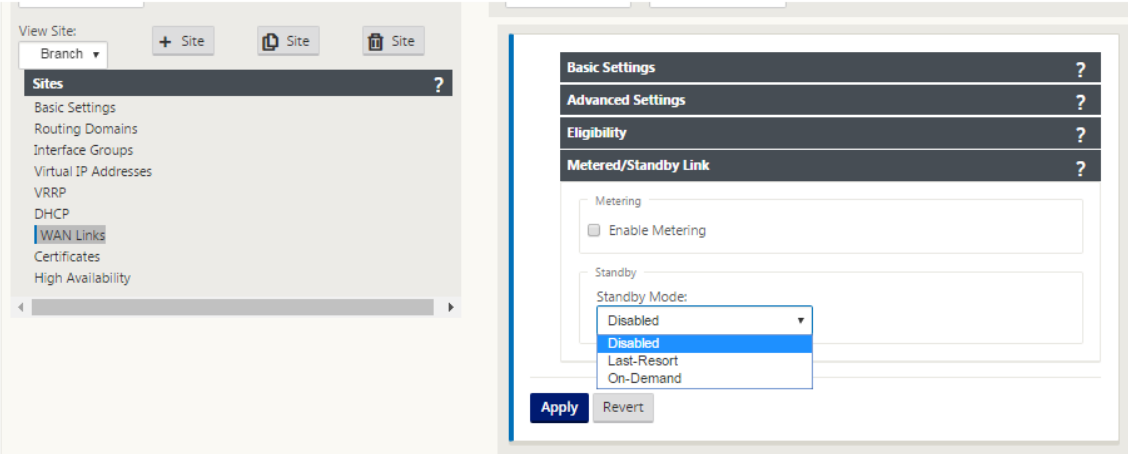
   - **Anbieter-ID** —(Optional) Geben Sie eine eindeutige ID-Nummer 1—100 ein, um WAN-Verbindungen zu kennzeichnen, die mit demselben Dienstanbieter verbunden sind. Virtual WAN verwendet die Provider-ID, um Pfade beim Senden doppelter Pakete zu unterscheiden.
   - **Framekosten (Byte)** —Geben Sie die Größe (in Byte) des Headers/Trailers ein, der jedem Paket hinzugefügt wurde. Zum Beispiel die Größe der hinzugefügten Ethernet-IPG- oder AAL5-Anhänger in Bytes.
   - **Überlastungsschwelle** —Geben Sie den Überlastungsschwellenwert (in Mikrosekunden) ein, nach dem die WAN-Verbindung die Paketübertragung drosselt, um eine weitere Überlastung zu vermeiden.
   - **MTU-Größe (Byte)** —Geben Sie die größte Rohpaketgröße (in Byte) ein, ohne die Framekosten.

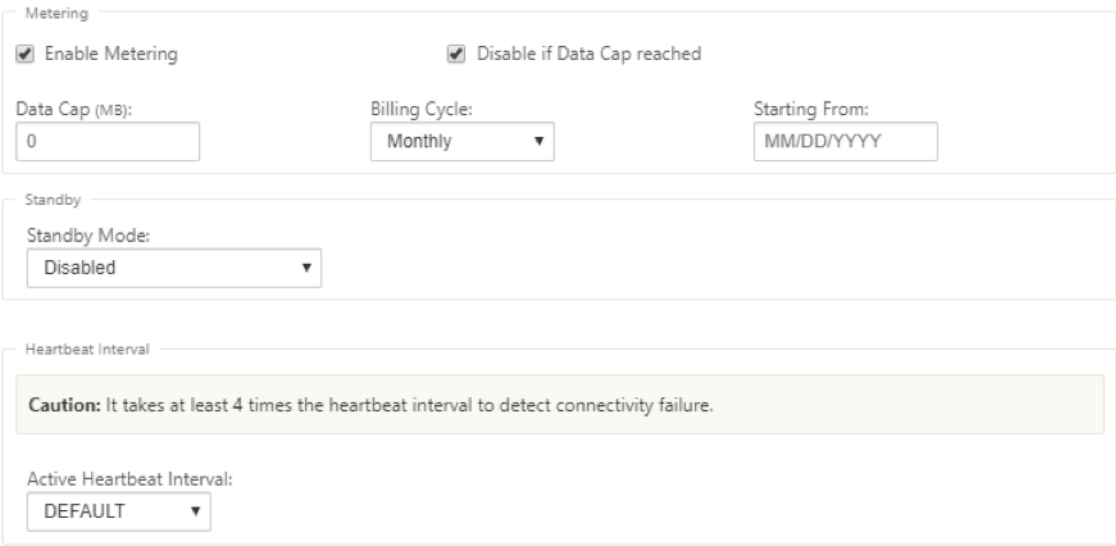
9. Klicken Sie auf die graue Teilleiste **Berechtigung**. Dadurch wird das Formular **Berechtigungseinstellungen** für den Link geöffnet.

10. Wählen Sie die **Berechtigungseinstellungen** für den Link aus.



11. Klicken Sie auf die graue Abschnittleiste mit **Metered Link**. Dadurch wird das Einstellungsformular für **Metered Link** für den Link geöffnet.
12. (Optional) Wählen Sie **Metering aktivieren** aus, um die Messung für diesen Link zu aktivieren. Daraufhin werden die Felder **Metering-Einstellungen aktivieren** angezeigt.





13. Konfigurieren Sie die Messeinstellungen für den Link. Geben Sie Folgendes ein:

    - **Datenobergrenze (MB)** —Geben Sie die Daten-Cap-Zuweisung für die Verbindung in MB ein.
    - **Abrechnungszyklus** —Wählen Sie entweder **monatlich oder wöchentlich** aus dem Dropdownmenü aus.
    - **Beginnend von** —geben Sie das Startdatum des Abrechnungszyklus ein.
    - **Last Resort** —Wählen Sie diese Option aus, um diesen Link als Link der letzten Instanz zu aktivieren, falls alle anderen verfügbaren Links ausfallen. Unter normalen WAN-Bedingungen sendet Virtual WAN nur minimalen Datenverkehr über gemessene Verbindungen, um den Verbindungsstatus zu überprüfen. Im Falle eines Ausfalls kann SD-WAN jedoch aktive dosierte Verbindungen als letzten Ausweg für die Weiterleitung des Produktionsverkehrs verwenden.

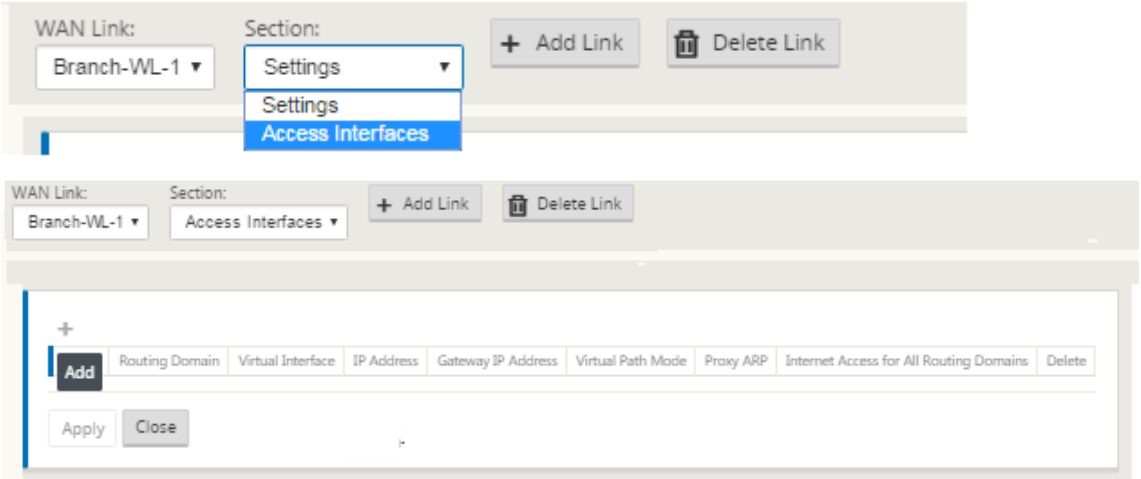
14. Klicken Sie auf **Apply**. Dies wendet Ihre angegebenen Einstellungen auf die neue WAN-Verbindung an.

    Der nächste Schritt besteht darin, die Access Interfaces für die neue WAN-Verbindung zu konfigurieren. Ein Access Interface 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 mindestens ein Access Interface haben.

    > **Hinweis**
    >
    > Eine Option zur automatischen Bereitstellung von Freigaben unter Berücksichtigung der Remotebandbreite wird hinzugefügt, um WAN-Verbindungen zu konfigurieren. Mit der Option "Provisioning mit Remote-Bandbreite festlegen"können Benutzer mit großen Netzw-

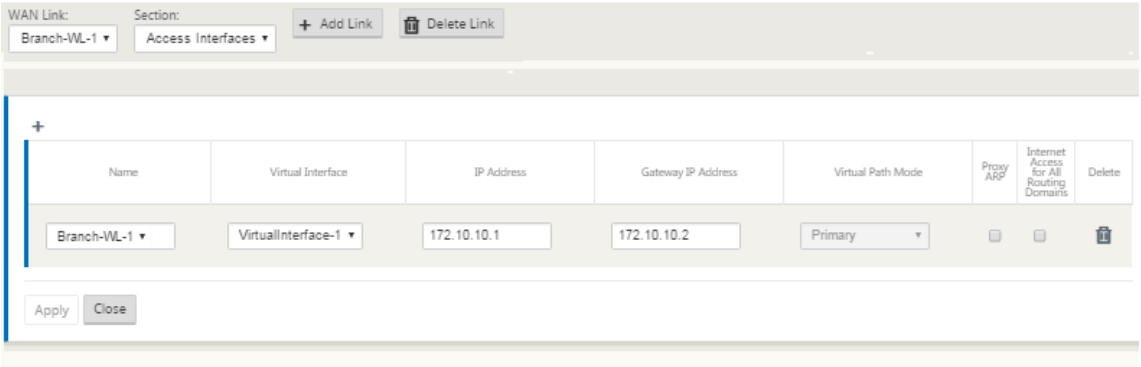
> erken und unterschiedlichen Bandbreitenkonfigurationen die Bandbreitenbereitstellung für Rechenzentrumsstandorte dynamisch verwalten.

15. Wählen Sie auf der Seite WAN-Link-Konfiguration für den Link **Zugriffsschnittstellen** aus. Dadurch wird die Ansicht **Access Interfaces** für die Site geöffnet.



16. Klicken Sie auf **+**, um eine Schnittstelle hinzuzufügen. Ein leerer Eintrag zur Tabelle wird hinzugefügt und zur Bearbeitung geöffnet. Geben Sie die Einstellungen für **Zugriffsschnittstellen** für den Link ein.

> **Hinweis**
>
> Jede WAN-Verbindung muss mindestens ein Access Interface haben.



17. Geben Sie Folgendes ein:

    - **Name**: Dies ist der Name, unter dem auf dieses Access Interface verwiesen wird. Geben Sie einen Namen für das neue Access Interface ein, oder übernehmen Sie die Standardeinstellung. Die Standardeinstellung 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 die Nummer ist die Anzahl der Access Interfaces, die derzeit für diesen Link konfiguriert sind, 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.

- **Virtuelles Interface** —Das virtuelle Interface, das dieses Access Interface verwendet. 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 Virtual Path-Verkehr 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 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.

18. Klicken Sie auf **Apply**.

    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 die Zweigstelle

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 Ansicht **Routen** für die Site angezeigt.
2. Klicken Sie rechts neben **Routes** auf **+**, um eine Route hinzuzufügen. Daraufhin wird das Dialogfeld **Routen** zur Bearbeitung geöffnet.

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 von 1 bis 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 ständiges Messen und Anpassen an sich ändernde 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 Verkehr zwischen einer Enterprise-Site und Websites im öffentlichen Internet. Verkehr dieser Art ist nicht gekapselt. In Zeiten der Überlastung verwaltet das SD-WAN aktiv die Bandbreite, indem es den Internetverkehr relativ zum virtuellen Pfad und den Intranet-Verkehr gemäß der vom Administrator festgelegten SD-WAN-Konfiguration begrenzt.
     - **Intranet** —Dieser Dienst verwaltet Enterprise Intranet-Verkehr, der nicht für die Übertragung über einen virtuellen Pfad definiert wurde. Wie beim Internetverkehr bleibt er

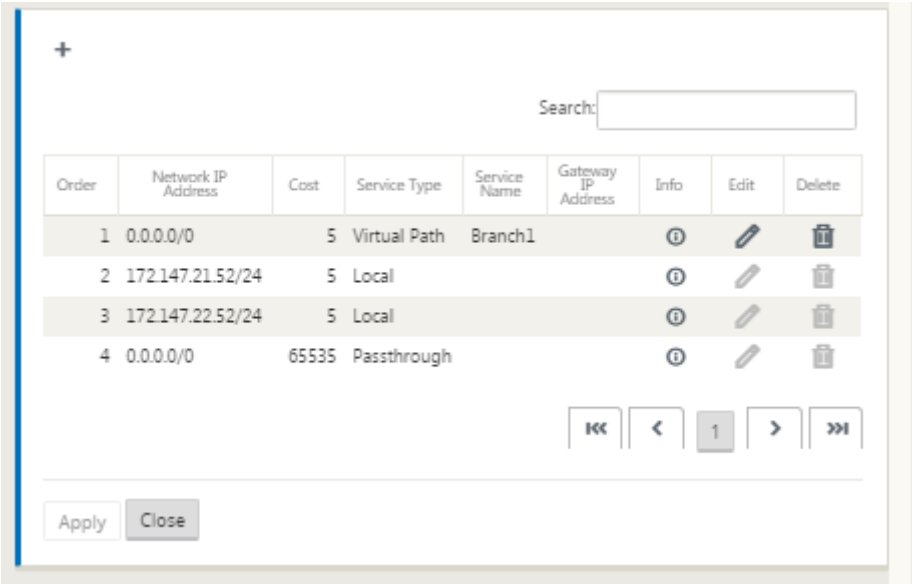
ungekapselt, und das SD-WAN verwaltet die Bandbreite, indem dieser Datenverkehr im Verhältnis zu anderen Diensttypen während der Staus begrenzt wird. Unter bestimmten Bedingungen und wenn für Intranet-Fallback auf dem virtuellen Pfad konfiguriert, kann Datenverkehr, der normalerweise mit einem virtuellen Pfad übertragen wird, stattdessen als Intranet-Verkehr behandelt werden, um die Netzwerkzuverlässigkeit aufrechtzuerhalten.

- **Passthrough** —Dieser Dienst verwaltet den Datenverkehr, der durch das virtuelle WAN geleitet werden soll. Der an den Passthrough-Dienst gerichtete Datenverkehr umfasst Broadcasts, ARPs und anderen Nicht-IPv4-Verkehr sowie Datenverkehr im lokalen Subnetz der Virtual WAN Appliance, konfigurierten Subnetzen oder Regeln, die vom Netzwerkadministrator angewendet werden. Dieser Verkehr wird vom SD-WAN nicht verzögert, geformt oder verändert. 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-Verkehr 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-Verkehr, der für einen GRE-Tunnel bestimmt ist, und entspricht dem am Standort konfigurierten LAN GRE-Tunnel. Mit der GRE-Tunnel-Funktion können Sie SD-WAN-Appliances konfigurieren, um GRE-Tunnel im LAN zu beenden. 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.

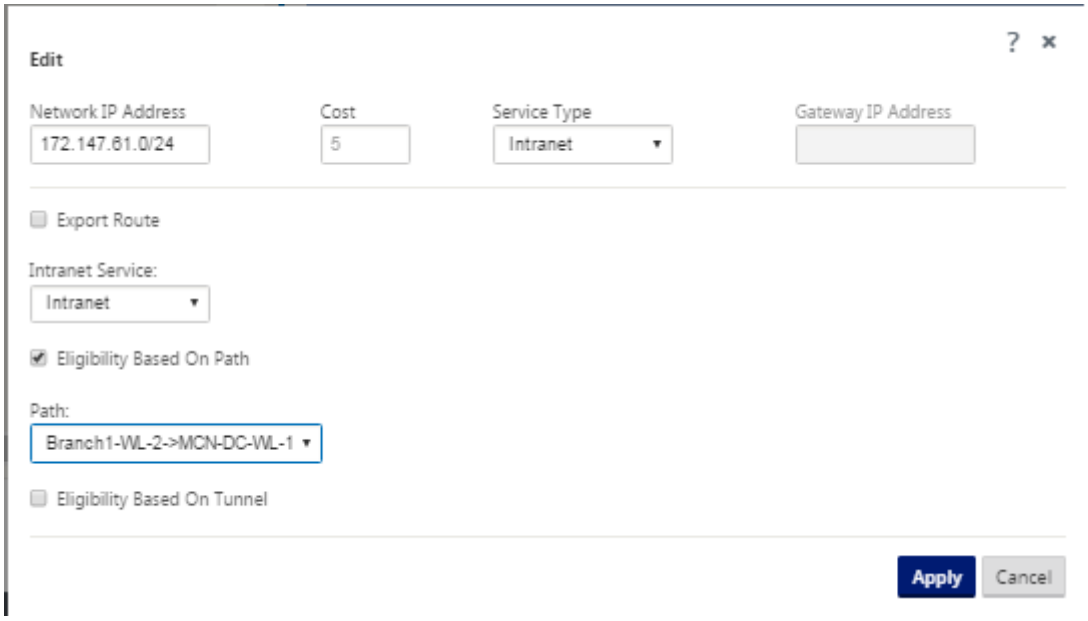
- **Gateway IP Addres**s —Geben Sie die Gateway-IP-Adresse für diese Route ein.
- **Berechtigung basierend auf Pfad** (Kontrollkästchen) —(Optional) —(Optional) Wenn diese Option aktiviert ist, erhält die Route keinen Traffic, wenn der ausgewählte Pfad ausgefallen ist.
- **Pfad** —Dies gibt den Pfad an, der zum Bestimmen der Routenberechtigung verwendet werden soll.

4. Klicken Sie auf **Apply**.

> **Hinweis**
>
> Nachdem Sie auf **Übernehmen**geklickt haben, werden möglicherweise Audit-Warnungen angezeigt, die darauf hinweisen, dass weitere Maßnahmen erforderlich sind. Ein Roter-Punkt- oder Goldenrod-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.



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 der Vorbereitung der SD-WAN-Appliance-Pakete auf dem MCN fortfahren.

Die optionalen Schritte sind wie folgt:

- **Konfigurieren von Hochverfügbarkeit** —Hochverfügbarkeit ist eine Konfiguration, bei der zwei virtuelle WAN-Appliances an einem Standort in einer Active/Standby-Partnerschaftskapazität für Redundanzzwecke dienen. Wenn Sie Hochverfügbarkeit für diese Site nicht implementieren, können Sie diesen Schritt überspringen. Anweisungen finden Sie unter Konfigurieren von Hochverfügbarkeit (Hochverfügbarkeit) für den Zweigstandort (optional).
- **Klonen des neuen Zweigstandorts** —Sie haben die Möglichkeit, den von Ihnen konfigurierten Zweigstandort zu klonen und diesen als Vorlage für das Hinzufügen einer weiteren Site zu verwenden. Die Appliance-Modelle für die Original-Site und den Klon müssen identisch sein. Anweisungen finden Sie unter Klonen der Zweigstelle (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 **Konfigurationseditor**ausfüllen und die geänderte Konfiguration speichern.

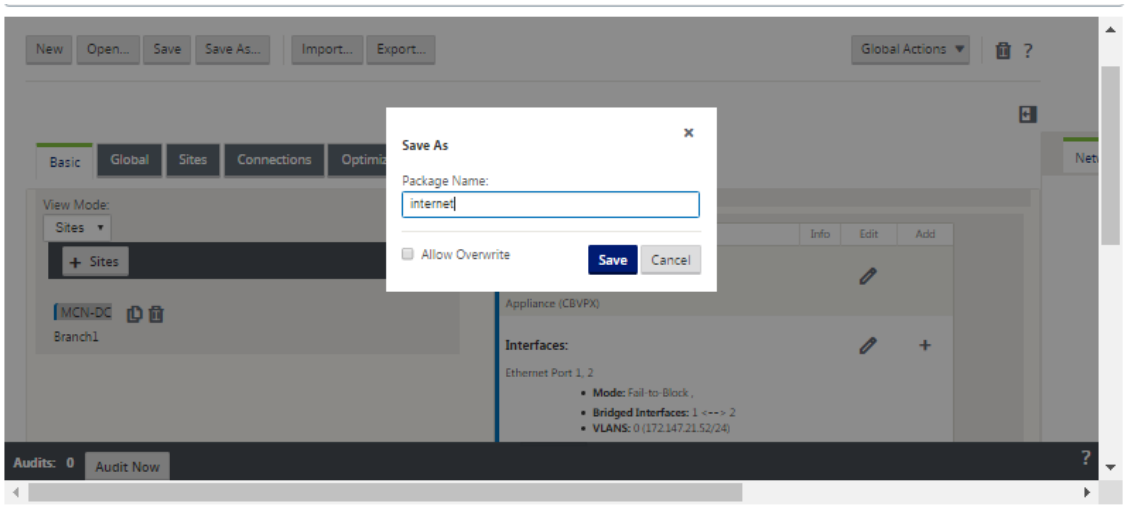
Konfiguration speichern

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 auftritt oder Sie sich vor dem Speichern Ihrer 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, Speichern unter anstelle von**Speichern**zu verwenden, um zu vermeiden, dass das falsche Konfigurationspaket überschrieben wird.**
>
> Nach dem Speichern der Konfigurationsdatei haben Sie die Möglichkeit, sich vom Management-Webinterface abzumelden und den Konfigurationsprozess 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 Konfigurationseditor.

Gehen Sie folgendermaßen vor, um das aktuelle Konfigurationspaket zu speichern:

1. Klicken Sie auf **Speichern** unter (oben im mittleren Bereich des **Konfigurationseditors**). 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, wählen Sie vor dem Speichern unbedingt **Überschreiben zulassen** aus.

Der nächste Schritt besteht darin, die virtuellen Pfade und den Virtual Path Service zwischen dem MCN und den Clientsites zu konfigurieren. Anweisungen finden Sie im Konfigurieren des virtuellen Pfaddienstes zwischen dem MCN und den Client-Sites.

Zweigstandort umbenennen

Nach dem Umbenennen der Zweigstelle 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 Staging-Paket für den umbenannten Zweigstandort herunter.
3. Wählen Sie auf dem **MCNStaged network aktivieren** aus. Dadurch wird die umbenannte Site deaktiviert, und die Site wird nicht mehr verfügbar.
4. Navigieren Sie zur Seite **Local Change Management** der Zweigstelle.
5. Laden Sie das zuvor heruntergeladene Paket hoch. Klicken Sie auf **Weiter** und dann auf **Activate**.

Umbenennen von Zweigstandort mit hoher Verfügbarkeit

So laden Sie eine neue Konfiguration nach dem Umbenennen einer Zweigstelle mit hoher Verfügbarkeit hoch:

1. Stationieren Sie im MCN das Netzwerk mit einer neuen Konfiguration, die den umbenannten Zweigstandort enthält.
2. Laden Sie das Staging-Paket für die aktive und die Hochverfügbarkeits-Appliance mit umbenannter Zweigstelle herunter
3. Wählen Sie auf dem **MCN** die Option **Activate Staged** für das Netzwerk 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 **Activate**.

6. Wiederholen Sie die Schritte 4 (a) und 4 (b) für die Standby-Appliance.

Klonen eines Zweigstandorts (optional)

October 28, 2021

Dieser Abschnitt enthält Anweisungen zum Klonen des neuen Zweigstandorts zur Verwendung als Teilvorlage für das Hinzufügen weiterer Zweigstandorte.

> **Hinweis**
>
> Das Klonen der Site ist optional. Die Modelle der virtuellen WAN-Appliance müssen sowohl für die ursprüngliche als auch für die geklonten Sites identisch sein. Sie können das angegebene Einheitenmodell für einen Klon nicht ändern. Wenn das Appliance-Modell für einen Standort anders ist, müssen Sie den Standort manuell hinzufügen, wie in den vorherigen Abschnitten beschrieben.

Das Klonen einer Site rationalisiert den Prozess des Hinzufügens und Konfigurierens 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 Site ändern. Einige der ursprünglichen Einstellungen können gegebenenfalls beibehalten werden. Die meisten Einstellungen müssen jedoch für jede Site eindeutig sein.

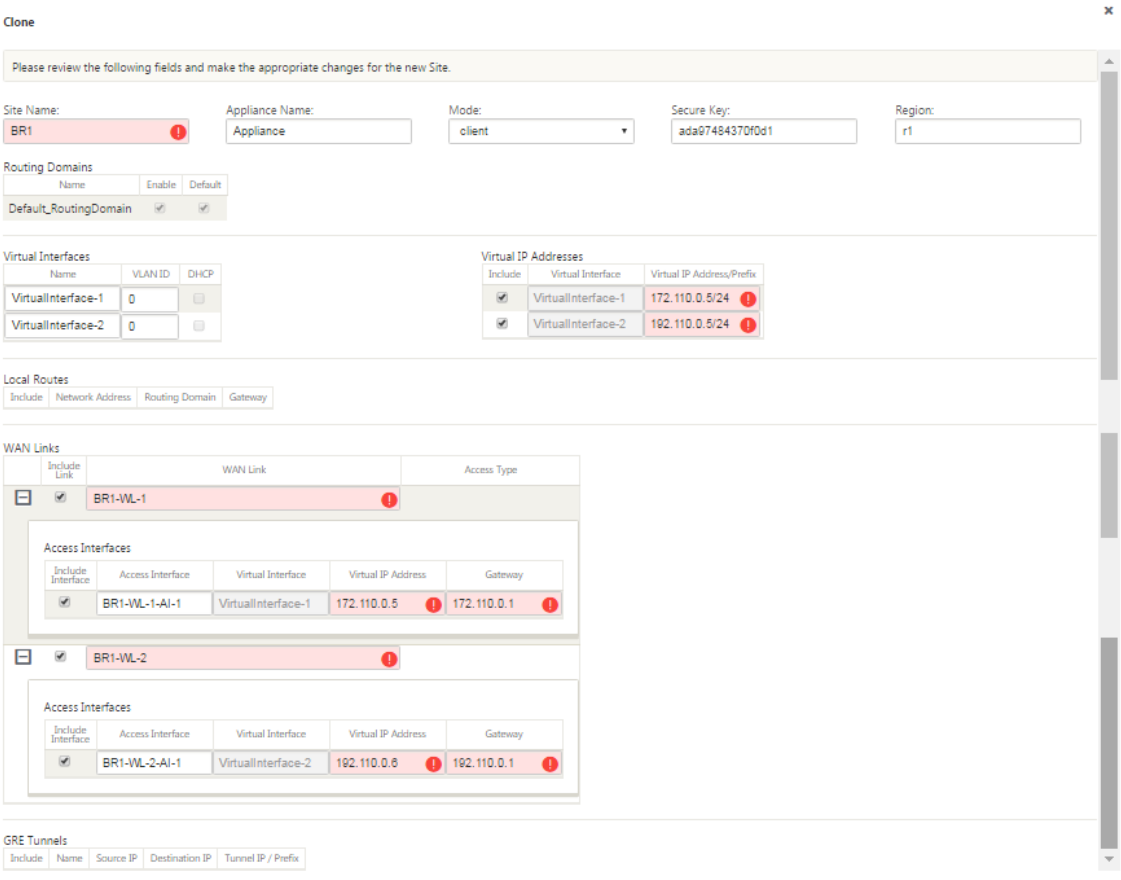
Gehen Sie wie folgt vor, um eine Site zu klonen:

1. Klicken Sie in der Baumstruktur **Sites** (mittlerer Bereich) des **Konfigurationseditors**auf den Zweigstandort, den Sie duplizieren möchten.

   Dadurch wird dieser Site-Zweig im **Sites-Baum** geöffnet und die Schaltfläche **Klonen** (Doppelseiten-Symbol) und die Schaltfläche “Löschen”(Mülleimer-Symbol) angezeigt.

2. Klicken Sie auf das Symbol **Klonen** rechts neben dem Namen der Zweigstelle im Baum.

   Dadurch wird die **Seite Konfiguration der Klon-Site** geöffnet.



3. Geben Sie die Konfigurationsparametereinstellungen für den neuen Standort ein.

   Ein rosafarbenes Feld mit einem Audit-Warnsymbol (roter Punkt) zeigt eine erforderliche Parametereinstellung an, die einen anderen Wert als die Einstellung für die ursprüngliche geklonte Site haben muss. Normalerweise muss dieser Wert eindeutig sein.

   > **Tipp**
   >
   > Um den Klonvorgang weiter zu rationalisieren, verwenden Sie beim Benennen der Klone eine konsistente, vordefinierte Namenskonvention.

4. Beheben Sie alle Audit-Warnungen.

   Um einen Fehler zu diagnostizieren, bewegen Sie den Mauszeiger über das **Audit-Alarm-Symbol** (roter Punkt oder Goldrutendelta), um die Blasenhilfe für diese bestimmte Warnung anzuzeigen.

5. Klicken Sie auf **Klonen** (ganz rechts), um die Site zu erstellen und zur Tabelle **Sites** hinzuzufügen.

> **Hinweis**
>
> Die Schaltfläche **Klonen** bleibt nicht verfügbar, bis Sie alle erforderlichen Werte eingegeben haben und die neue Site-Konfiguration 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.** Achten Sie darauf, vor dem Speichern in einer vorhandenen Konfiguration **Überschreiben zulassen** zu wählen, sonst werden Ihre Änderungen 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

October 28, 2021

Ein Audit-Warnsymbol (ein roter Punkt oder ein Goldrutendelta) neben einem Element weist auf einen Konfigurationsfehler oder fehlende Parameterinformationen für diesen Artikel hin. Eine Zahl neben dem Symbol gibt die Anzahl der zugehörigen Fehler für diese Warnung an. Um die Blasenhilfe für eine bestimmte Warnung anzuzeigen, bewegen Sie den Mauszeiger über das Warnsymbol. Daraufhin wird eine kurze Beschreibung der spezifischen Fehler angezeigt, die von dieser Warnung gekennzeichnet wurden. Sie müssen alle Audit-Warnungen in der Konfiguration auflösen, sonst können Sie das Konfigurationspaket später im Bereitstellungsprozess nicht überprüfen, ein Staging durchführen und aktivieren.

Durch das Auflösen aller Audit-Warnungen (falls vorhanden) wird die **Sites-Phase** der Konfiguration abgeschlossen. Der nächste Schritt besteht darin, die abgeschlossene **Sites** Konfiguration zu speichern.

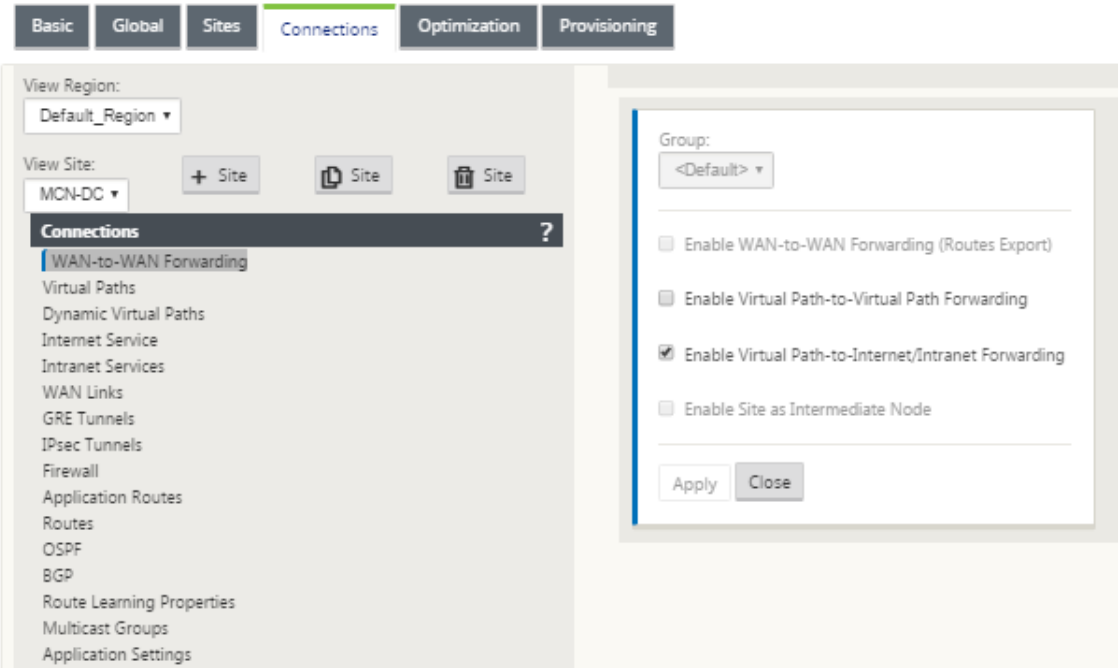
Konfigurieren des virtuellen Pfaddienstes zwischen MCN und Clientsites

October 28, 2021

Der nächste Schritt besteht darin, den Virtual Path Service zwischen dem MCN und jedem der Clientsites (Zweigstellen) zu konfigurieren. Dazu verwenden Sie die Konfigurationsformulare und -einstellungen, die in der Konfigurationsstruktur des Abschnitts **Verbindungen** des **Konfigurationseditors**verfügbar sind.

Gehen Sie wie folgt vor, um den Virtual Path Service zwischen dem MCN und einer Client-Site zu konfigurieren:

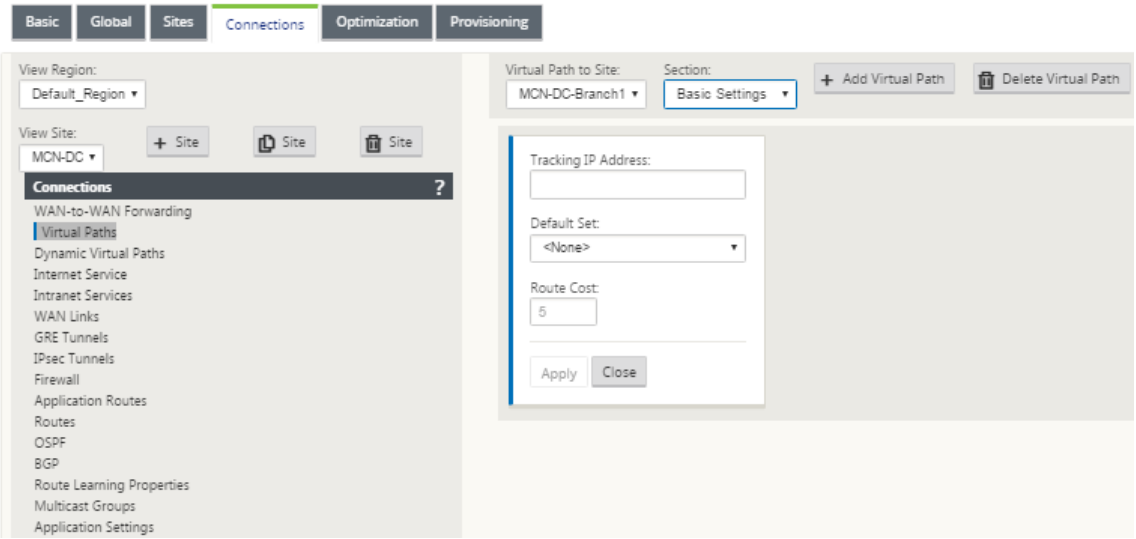
1. Klicken Sie im **Konfigurationseditor** auf die Registerkarte **Verbindungen**. Dadurch wird die Konfigurationsstruktur des Abschnitts **Verbindungen** angezeigt.
2. Wählen Sie den **MCN** aus dem Dropdownmenü **Site anzeigen** auf der Seite **Verbindungen** aus. Dadurch wird der MCN-Site in der Konfiguration **Connections** geöffnet.



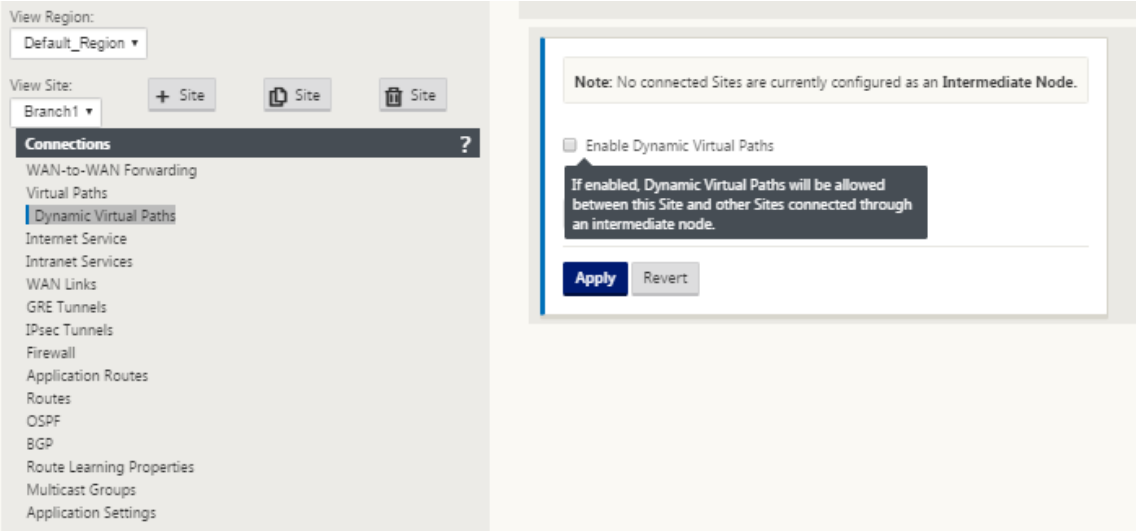
> **Hinweis**
>
> WAN-zu-WAN-Weiterleitungsgruppen werden nur innerhalb einer Region und nicht über Regionen hinweg unterstützt. Sie können Regionen verwenden, um Netzwerke zu trennen, anstatt sich auf WAN-zu-WAN-Weiterleitungsgruppen zu verlassen.

3. Klicken Sie auf **Virtuelle Wege**. 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 der Virtual WAN-Client-Sites. Die folgende Abbildung zeigt ein Beispiel für virtuelle Pfade für eine MCN-Site.



Die folgende Abbildung zeigt ein Beispiel für **dynamische virtuelle Pfade** für einen Zweigstandort.



Im Abschnitt **Dynamic Virtual Paths** 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 basierend auf einem konfigurierten Schwellenwert direkt zwischen Standorten eingerichtet werden. Der Schwellenwert basiert in der Regel auf dem Umfang des Datenverkehrs zwischen diesen Sites. Dynamische virtuelle Pfade sind erst betriebsbereit, wenn der angegebene Schwellenwert erreicht wurde. Dynamische virtuelle Pfade sind für den normalen Betrieb nicht erforderlich, daher ist die Konfiguration dieses Ab-

schnitts optional.

- **<MCN_Site_Name_<Branch_Site_Name>** —Das System fügt zunächst automatisch einen statischen virtuellen Pfad zwischen dem MCN und einem Clientstandort hinzu, da dieser virtuelle Pfad erforderlich ist. Der Name für den Pfad verwendet das folgende Formular:

  <MCN_Site_Name>_<Branch_Site_Name>

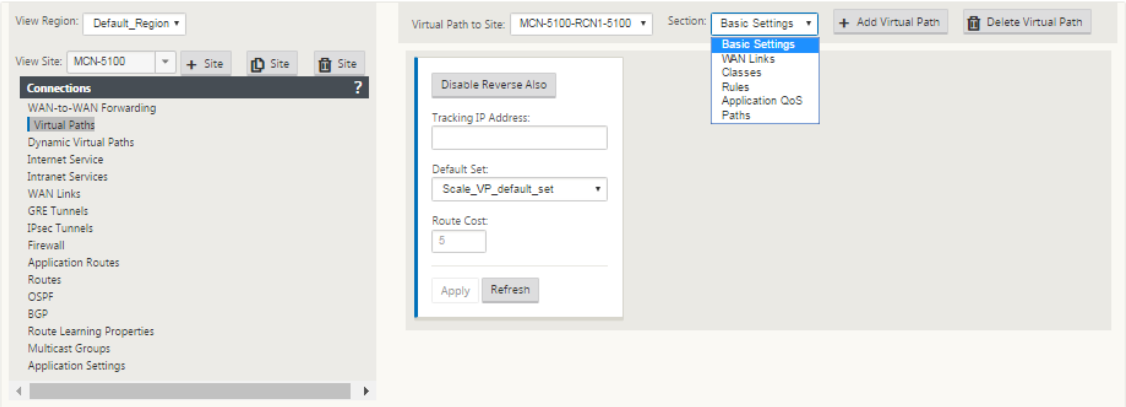
  Wobei:

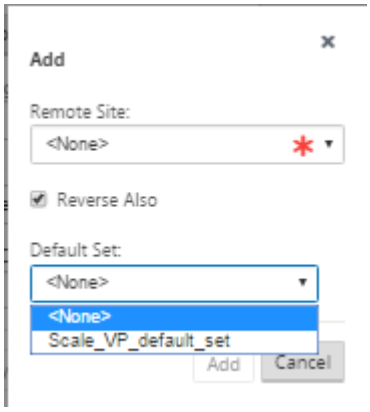
  MCN_Site_Name ist der Name des MCN für dieses virtuelle WAN.

  Branch_Site_Name ist der Name einer Client-Site, der im aktuellen Konfigurationspaket angegeben ist.

Vom Benutzer konfigurierbare Standardeinstellungen werden anfänglich auf den statischen virtuellen Pfad angewendet, wie im Abschnitt **Virtueller Pfad > Standardsätze** der **Verbindungskonfiguration** definiert. Sie können jedoch die definierten **Standardsätze**anpassen oder zu diesen hinzufügen sowie die Konfiguration für eine bestimmte Site und einen bestimmten virtuellen Pfad anpassen.

> **Hinweis**
>
> Um statischere virtuelle Pfade für eine Site hinzuzufügen, müssen Sie dies manuell tun. Anweisungen zum manuellen Hinzufügen eines statischen virtuellen Pfades sind in den Schritten wie folgt enthalten.



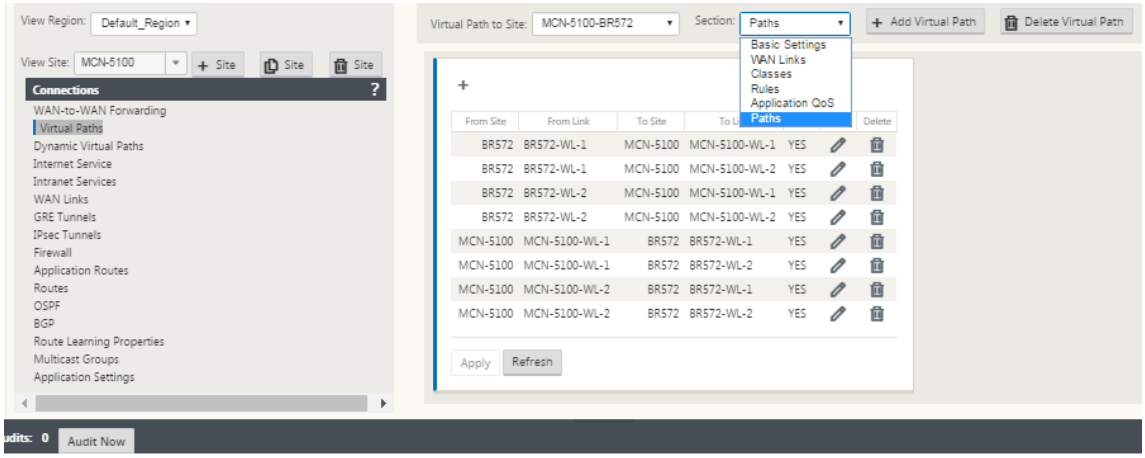


4. Klicken Sie im Abschnitt **Virtuelle Pfade** neben dem Namen des statischen virtuellen Pfades auf **+ Virtuellen Pfad hinzufügen**. Dies zeigt mehr Konfiguration für den statischen virtuellen Pfad:

   a) **Remotesite** —In diesem Abschnitt können Sie die Einstellungen für den **virtuellen Pfad** aus der Perspektive einer Remotesite 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 Remotesite hinzufügen.
   b) **Reverse Also -** Wenn diese Option aktiviert ist, werden Klassen und Regeln auf beiden Sites den virtuellen 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.

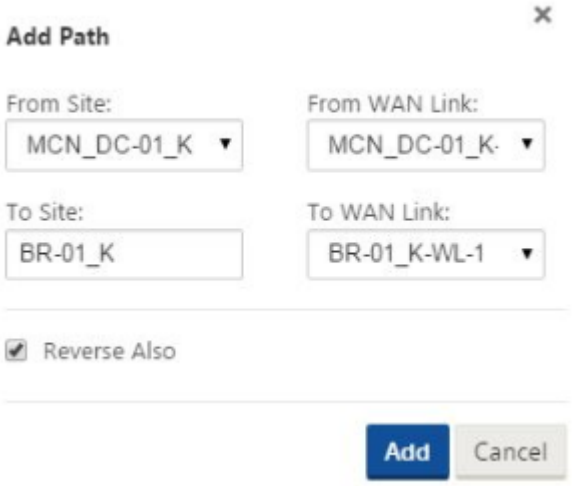
   Die folgende Abbildung zeigt ein Beispiel für statische MCN-Zweige mit Virtual Path und untergeordnete Zweige.

5. Wählen Sie **Pfade** aus dem Dropdownmenü **Abschnitt** aus.



6. Klicken Sie über der Tabelle **Pfade** auf **+** (Hinzufügen).

   Dadurch wird das Dialogfeld **Pfad hinzufügen** (Konfigurationsformular) angezeigt.

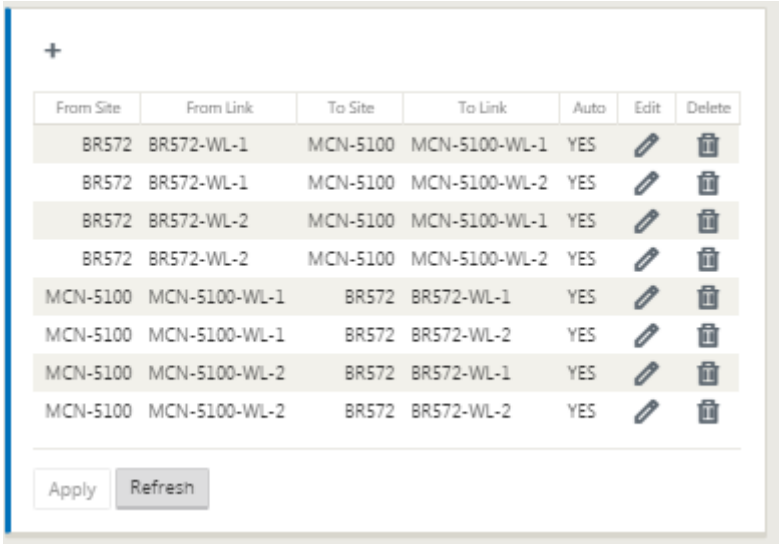


7. Geben Sie die Quell- und Zielsiteinformationen für den neuen virtuellen Pfad an.
8. Geben Sie in den verfügbaren Dropdownmenüs Folgendes an:

> **Hinweis**
>
> Abhängig davon, wie die WAN-Verbindungen für die Sites konfiguriert sind, sind einige Felder schreibgeschützt. Konfigurierbare Felder bieten ein Dropdownmenü mit den verfügbaren Auswahlen.

   - **Von Site** —Dies ist die Quell-Site 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.
   - **Zur Site** —Dies ist die Ziel-Site für den virtuellen Pfad.
   - **Zu WAN-Link** - Dies ist die Ziel-WAN-Verbindung für den virtuellen Pfad.
9. Klicken Sie auf **Hinzufügen**.

   Dadurch wird der konfigurierte virtuelle Pfad sowohl zum MCN als auch zur zugehörigen Client-Site in der Struktur **Verbindungen > Virtuelle Pfade** hinzugefügt. Dadurch wird auch automatisch das Konfigurationsformular für **Pfadeinstellungen** für die **Von Site** für den virtuellen Pfad (in diesem Fall der MCN) geöffnet.



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 akzeptieren Sie die Standardeinstellungen.

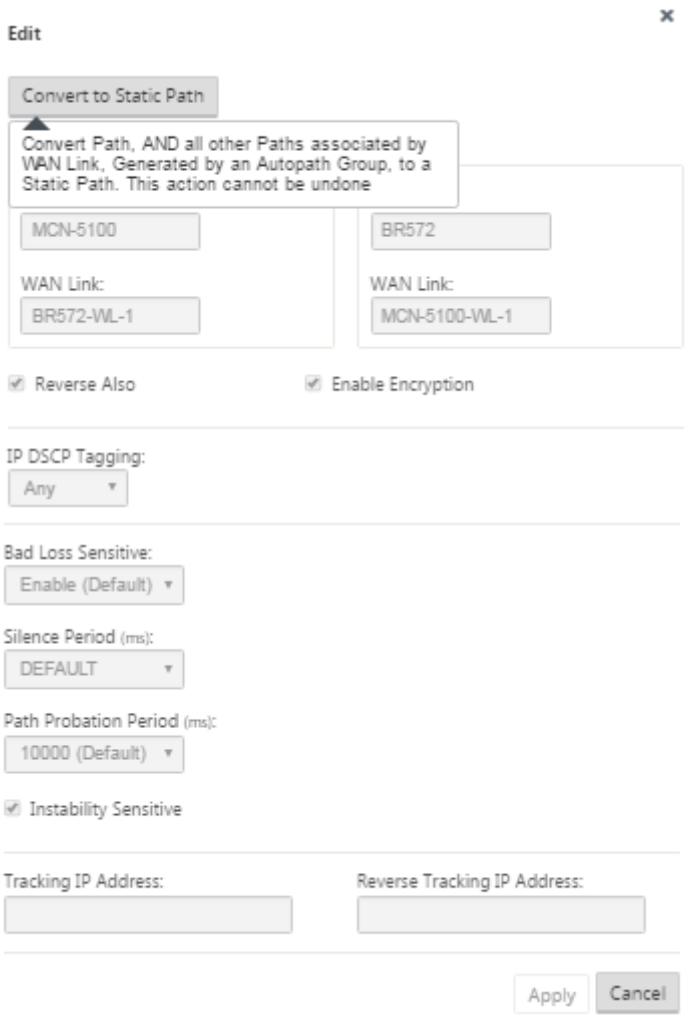
    Das **Paths-Konfigurationsformular** enthält die folgenden Einstellungen:

    - **Aus dem Abschnitt Site** :
      - **Site** —Dies ist die Quell-Site 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.
    - **Zum Abschnitt Site** :
      - **Site** —Dies ist die Ziel-Site für den virtuellen Pfad.
      - **WAN-Link** —Dies ist die Ziel-WAN-Verbindung für den virtuellen Pfad.
    - **Umkehren auch** - Aktivieren Sie dieses Kontrollkästchen, um Reverse Also für diesen virtuellen Pfad zu aktivieren. Wenn diese Option aktiviert ist, erstellt das System automatisch einen virtuellen Pfad in die entgegengesetzte Richtung des konfigurierten Pfads, wobei dieselben WAN-Verbindungen verwendet werden, die für den ursprünglichen Pfad konfiguriert wurden.
    - **IP-DSCP-Tagging** —Wählen Sie ein Tag aus dem Dropdownmenü aus. Dies gibt das DSCP-Tag an, das im IP-Header für den Datenverkehr über diesen virtuellen Pfad festgelegt werden soll.
    - **Verschlüsselung aktivieren** —Aktivieren Sie dieses Kontrollkästchen, um die Verschlüsselung von Paketen zu aktivieren, die über diesen virtuellen Pfad gesendet werden.

- **Sensitiv gegen schlechten Verlust** —Wählen Sie eine Einstellung aus dem Dropdownmenü aus. Es gibt folgende Optionen:
  - **Aktivieren**—(Standard) Wenn diese Option aktiviert ist, werden Pfade aufgrund eines Verlusts als **BAD** markiert und es wird eine Strafe für die Pfadbewertung erhoben.
  - **Deaktivieren** —Das Deaktivieren von **Bad Loss Sensitive** kann nützlich sein, wenn der Verlust an Bandbreite unerträglich ist.
  - **Benutzerdefiniert** —Wählen Sie Benutzerdefiniert aus, um den Prozentsatz des Verlusts im Zeitverlauf anzugeben, der erforderlich ist, um einen Pfad als BAD Bei Auswahl dieser Option werden die folgenden weiteren Einstellungen angezeigt:
    * **Prozentualer Verlust (%)** - Dies gibt den Prozentsatz der Verlustschwelle an, bevor ein Pfad als BAD markiert wird, gemessen über die angegebene Zeit. Standardmäßig basiert der Prozentsatz auf den letzten 200 empfangenen Paketen.
    * **Im Laufe der 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.
  - **Stille Periode (ms)** —Dies gibt die Dauer (in Millisekunden) vor dem Übergang des Pfadstatus von **GOOD** nach **BAD** an.

  Der Standardwert beträgt 150 Millisekunden. Wählen Sie im Dropdownmenü für dieses Feld eine Option zwischen 150 und 1000 aus.
  - **Pfad Probezeit (ms)** - Dies gibt die Wartezeit (in Millisekunden) an, bevor ein Pfad von BAD zu GOOD wechselt. Wählen Sie im Dropdownmenü für dieses Feld eine Option zwischen 500 und 60000 aus. Der Standardwert beträgt 10,000 Millisekunden.
  - **Instabilitätssensitiv** —Aktivieren Sie dieses Kontrollkästchen, um zu aktivieren. Wenn diese Option aktiviert ist, werden Latenzstrafen aufgrund eines Pfadstatus von **BAD** und anderen Latenzspitzen im Pfad-Scoring-Algorithmus berücksichtigt.
  - **Tracking-IP-Adresse** —Geben Sie im virtuellen Pfad eine virtuelle IP-Adresse ein, die angepingt werden kann, um den Status des Pfades zu bestimmen.
  - **Reverse-Tracking-IP-Adresse** —Wenn **Reverse Also** für den virtuellen Pfad aktiviert ist, geben Sie eine virtuelle IP-Adresse in den Pfad ein, die angepingt werden kann, um den Status des umgekehrten Pfads zu bestimmen.

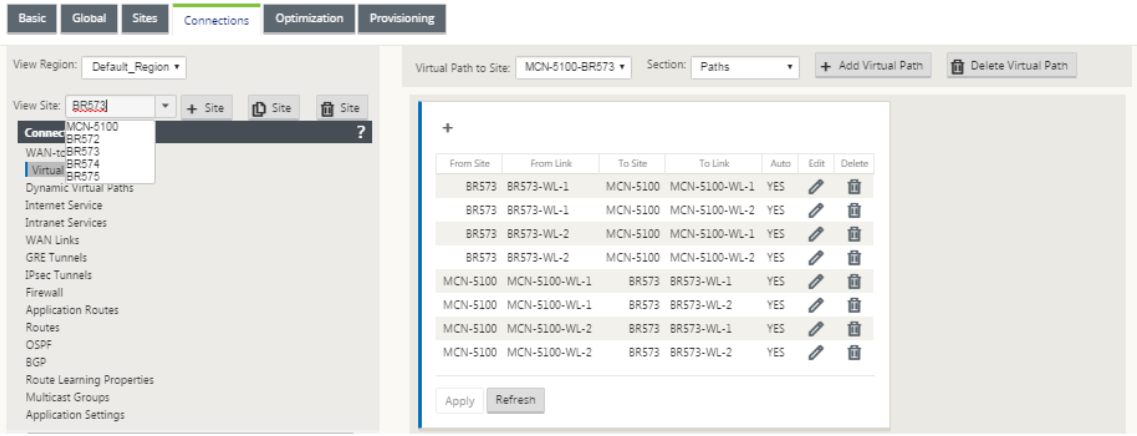
12. Klicken Sie auf **Apply**. Dies zeigt, dass die beiden neuen virtuellen Pfade **From Site** und **To Site** zwischen dem MCN und der Client-Site zur Tabelle Paths hinzugefügt wurden.



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 Clientsites 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 Clientstandort-Zweig in der **Verbindungsstruktur** wird geöffnet.

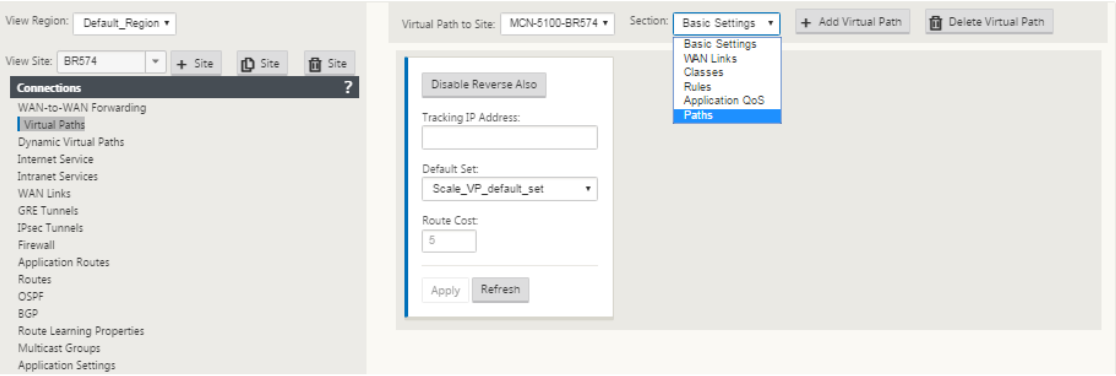


15. Navigieren Sie zum Konfigurationsformular für **Pfadeinstellungen** für jeden virtuellen Pfad der Client-Site, den Sie konfigurieren möchten.

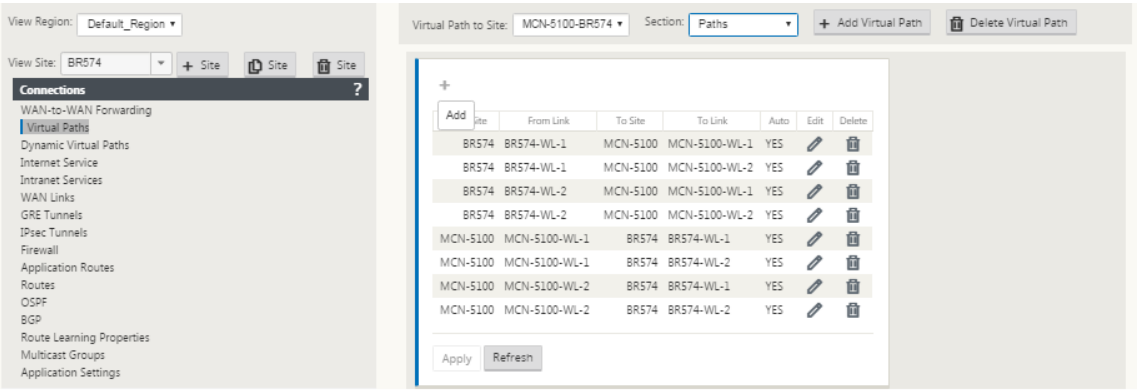
    Gehen Sie wie folgt vor, um zum Formular **Pfadeinstellungen** für die Client-Site zu navigieren:

16. Wählen Sie **Pfade** auf der Registerkarte **Abschnitt** der Verzweigungsseite für die Client-Site aus.

    Die folgende Abbildung zeigt ein Beispielformular 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. Befolgen Sie dieselben Schritte wie beim Konfigurieren der virtuellen Pfade für die MCN-Site.



Damit ist die Grundkonfiguration der virtuellen Pfade zwischen den Clientstandorten und dem MCN abgeschlossen.

> **Hinweis**
>
> Informationen zum Konfigurieren weiterer Einstellungen in den Abschnitten **Verbindungen** oder **Provisioning** des **Konfigurationseditors**finden Sie in der Online-Hilfe des Management-Webinterface für diese Abschnitte. Wenn Sie diese Einstellungen derzeit nicht konfigurieren möchten, können Sie mit dem entsprechenden 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 bitte mit dem Thema Aktivieren und Konfigurieren der WAN-Optimierung fort. Andernfalls können Sie direkt mit der Installation der SD-WAN-Appliance-Pakete auf den Clients fortfahren.
- **SD-WAN Edition** — Diese Edition enthält keine WAN-Optimierungsfunktionen. Sie können jetzt direkt mit der Installation der SD-WAN-Appliance-Pakete auf den Clients fortfahren.

MCN-Konfiguration bereitstellen

October 28, 2021

Der nächste Schritt besteht darin, die SD-WAN-Appliance-Pakete für die Verteilung an die Clientknoten vorzubereiten. Dies beinhaltet die folgenden zwei Verfahren:

1. Exportieren Sie das Konfigurationspaket nach Change Management.

   Bevor Sie die Appliance-Pakete generieren können, müssen Sie zuerst das fertige Konfigurationspaket aus dem **Konfigurationseditor** 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 zum **Change Management-Posteingang** hinzugefügt haben, können Sie die Appliance-Pakete generieren und ein Staging durchführen. Dazu verwenden Sie den **Änderungsmanagement-Assistenten** im Management-Webinterface auf dem MCN. Anweisungen finden Sie im Abschnitt Konfiguration für Zweige bereitstellen.

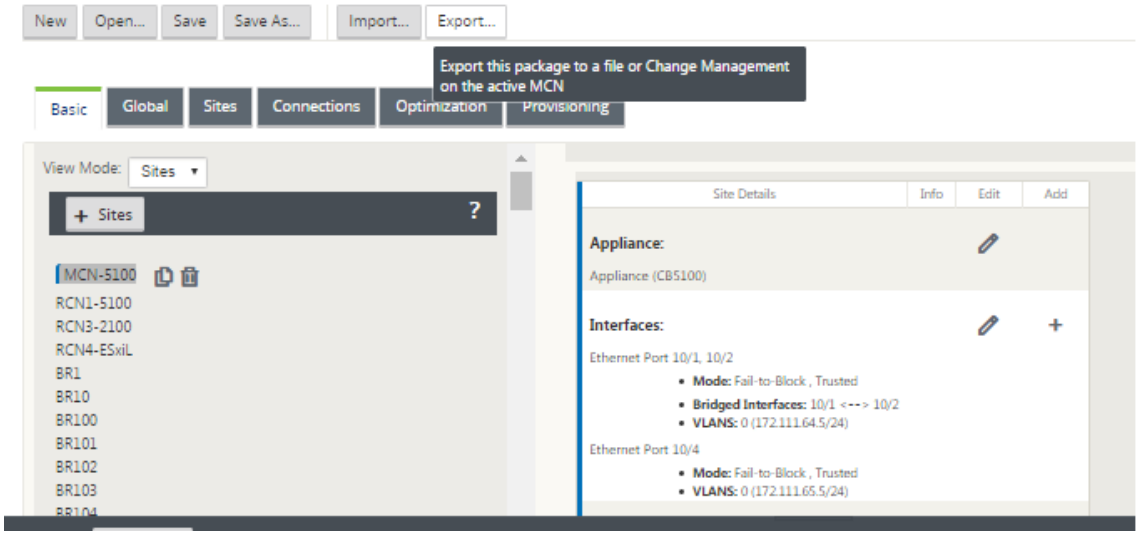
MCN Change Management durchführen

October 28, 2021

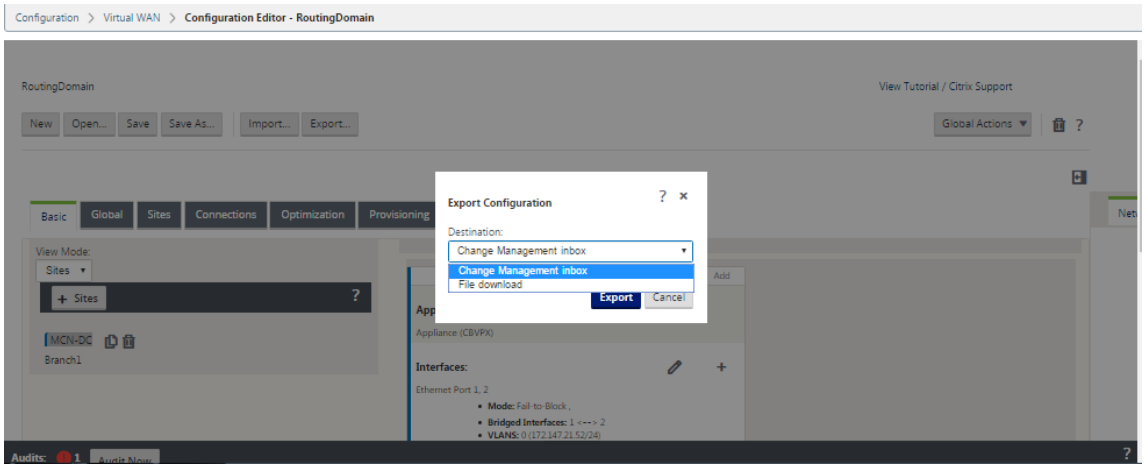
Bevor Sie die Appliance-Pakete generieren können, müssen Sie zuerst das fertige Konfigurationspaket in das Management Webinterface **Change Management-System** exportieren.

Gehen Sie wie folgt vor, um das Konfigurationspaket nach **Change Management**zu exportieren:

1. Klicken Sie auf der Seite **Konfigurationseditor** auf **Exportieren** (oben auf der Seite).



Dadurch wird das Dialogfeld **Konfiguration exportieren** geöffnet.



2. Wählen Sie **Change Management-Posteingang** als Exportziel aus. Verwenden Sie das Dropdownmenü im Feld **Ziel**, um Ihre Auswahl zu treffen.

3. Klicken Sie auf **Exportieren.**

Wenn der Exportvorgang abgeschlossen ist, wird oben auf der Seite eine grüne Erfolgsmeldung angezeigt.

> **Tipp**
>
> Sie können in der Erfolgsmeldung auf den blauen Link **Änderungsmanagement** klicken, um direkt zur Seite **Änderungsvorbereitung** —**Dateien hochladen und überprüfen** (zweite Seite) des **Änderungsverwaltungs-Assistenten** zu gelangen. Sie müssen zu dieser Seite navigieren, um den nächsten Schritt im Konfigurationsprozess auszuführen. Die Erfolgsmeldung wird jedoch nur wenige Sekunden lang angezeigt. Danach müssen Sie den Navigationsbaum verwenden, um den Assistenten zu öffnen und dann zu dieser Seite zu gelangen. 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

October 28, 2021

Nachdem Sie die Konfiguration mithilfe des Konfigurationseditors vorbereitet und das Konfigurationspaket in den Posteingang für das Änderungsmanagement exportiert haben, müssen Sie im nächsten Schritt die SD-WAN-Appliance-Pakete für die Verteilung an die Clientknoten vorbereiten. Verwenden Sie den **Änderungsmanagement-Assistenten** 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, gebündelt mit dem Konfigurationspaket, das Sie bereitstellen möchten. Daher muss für jedes Appliance-Modell in Ihrem Netzwerk ein anderes Appliance-Paket vorbereitet und generiert werden.

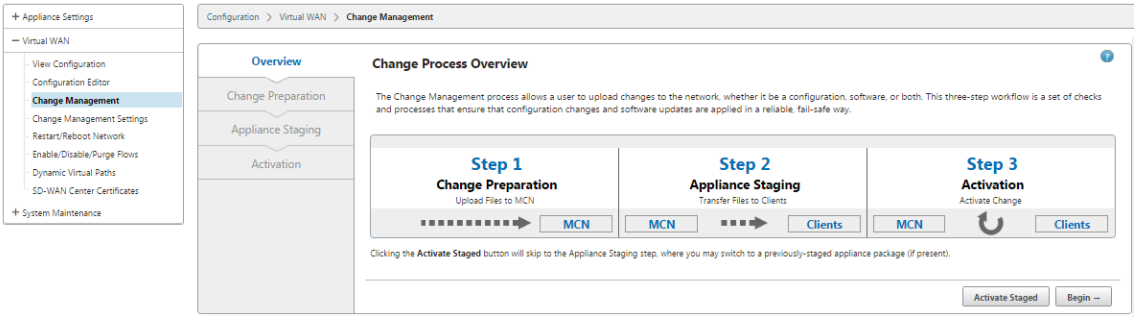
> **Hinweis**
>
> Wenn Sie die erforderlichen SD-WAN-Softwarepakete noch nicht auf einen PC heruntergeladen haben, der mit Ihrem Netzwerk verbunden ist, können Sie dies jetzt tun. Informationen zum Erwerb und Herunterladen der Software finden Sie im Abschnitt Erwerb der SD-WAN-Softwarepakete

Gehen Sie folgendermaßen vor, um das Paket und die Konfiguration in den MCN hochzuladen und zu installieren:

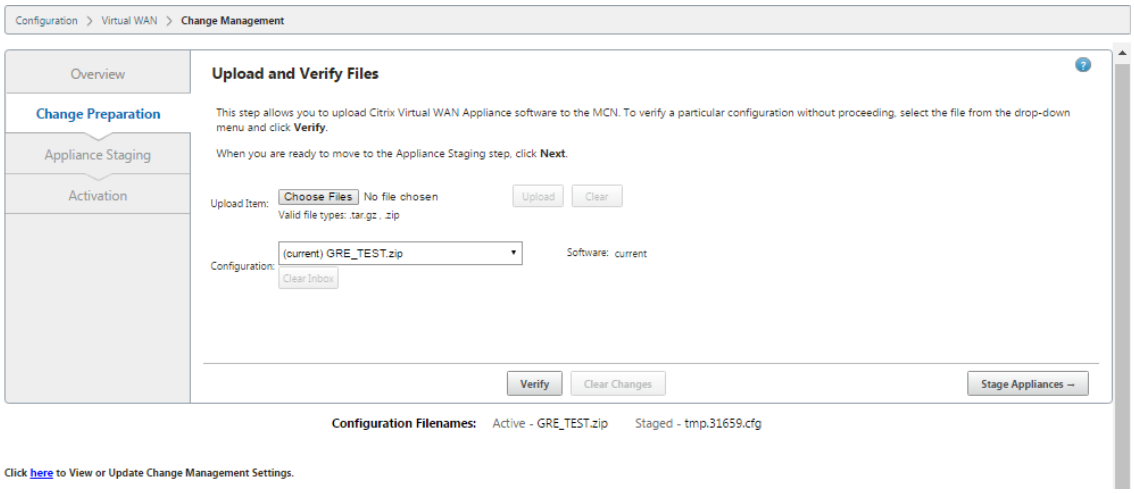
1. Melden Sie sich beim Management-Webinterface auf der MCN-Appliance an.

> **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 **Virtual WAN** und wählen Sie **Change Management**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) Click **Choose File** next to the **Upload Item** field. This opens a file browser for selecting an SD-WAN software package to upload.

   b) Select an SD-WAN software package, and click **OK**.

c) Navigate to the SD-WAN software packages you downloaded earlier to the local PC, and select the package to upload.

d) Click **Upload**.

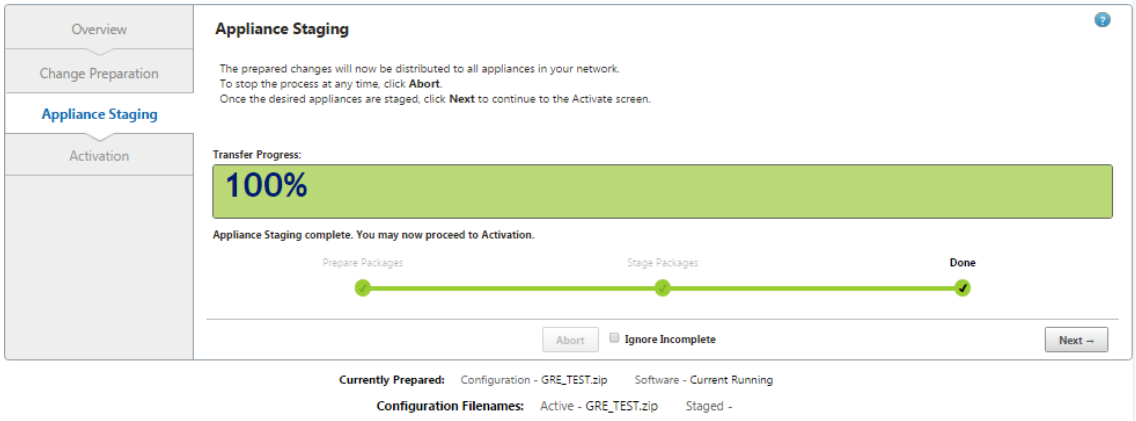
e) Repeat steps (i) through (iii) for each of the SD-WAN software packages required for your network.

6. Wählen Sie im Dropdownmenü **Konfiguration** das neue Konfigurationspaket aus, das Sie gerade nach **Change Management**exportiert haben.

7. Klicken Sie auf **Stage-Gerät**. Das Appliance-Staging leitet die folgenden Aktionen ein:

   - Überträgt das ausgewählte Softwarepaket und die Konfiguration an den MCN.
   - Generiert ein Appliance-Paket für jedes in der ausgewählten Konfiguration identifizierte Appliance-Modell.
   - Fügt die neuen Appliance-Pakete zur Liste der verfügbaren Pakete in der Site-Appliance-Tabelle hinzu.
   - Stufenweise die neue Konfiguration und das entsprechende Softwarepaket auf dem MCN.

8. Klicken Sie auf **Weiter**. Daraufhin wird die Seite **Appliance-Staging** fortgesetzt.

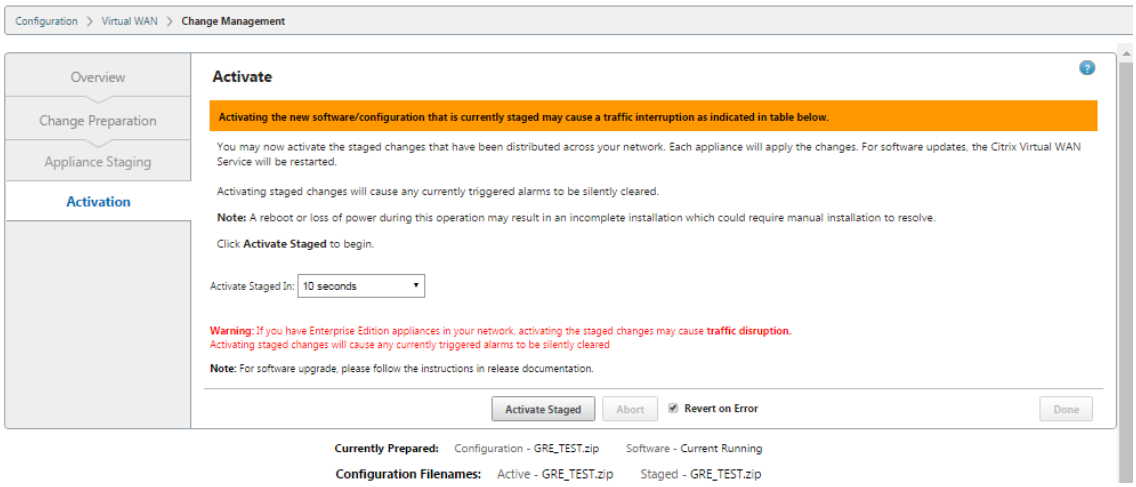


Wenn der Staging-Vorgang abgeschlossen ist, wird die **Tabelle Site-Appliance mit den neu bereitgestellten Appliance-Paketinformationen gefüllt.

> **Hinweis**
>
> Wenn dies eine erste Bereitstellung ist, wird jetzt nur der MCN aktualisiert und bereitgestellt. Wenn Sie eine vorhandene Bereitstellung aktualisieren und die virtuellen Pfade bereits zwischen den bereitgestellten Standorten funktionieren, verteilt dies auch die entsprechenden Appliance-Pakete an die bereitgestellten Clientknoten und initiiert das Staging auf diesen Knoten. Wenn Sie jedoch neue Clientknoten zu einer vorhandenen Virtual WAN-Bereitstellung hinzufügen, müssen Sie das entsprechende Appliance-Paket

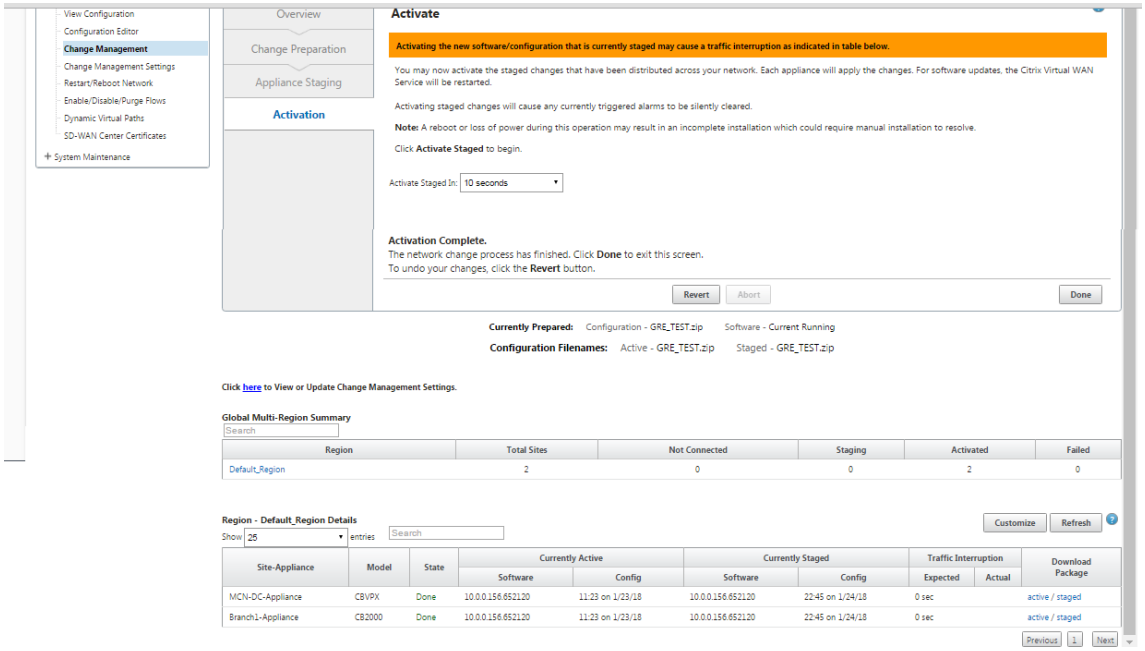
> auf jedem neuen Client manuell hochladen, bereitstellen und aktivieren, wie in den übrigen Schritten in diesem Verfahren beschrieben.
>
> Wenn die Site auf der Änderungsverwaltungsseite als **nicht verbunden** angezeigt wird, wird sie während des Staging-Vorgangs als fehlgeschlagen markiert und der Fortschrittsbalken wird auf 100% abgeschlossen. Sobald die **nicht verbundene** Website wieder online und verbunden ist, korrigiert MCN sie automatisch.

9. Wählen Sie **Bei Fehler wiederherstellen** aus, um bei Auftreten eines Fehlers zum vorherigen Anwendungspaket zurückzukehren. Weitere Informationen finden Sie unter Konfigurations-Rollback.
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.



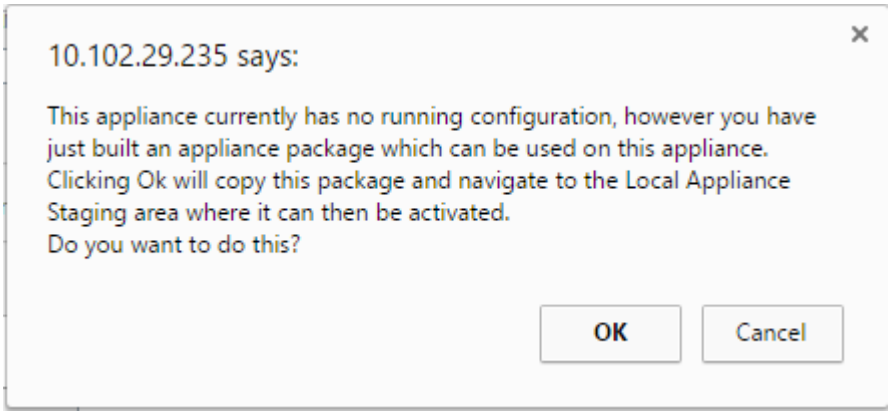
Wenn die Aktivierung abgeschlossen ist, wird eine Statusmeldung **Aktivierung abgeschlossen** angezeigt, und die Schaltfläche **Fertig** ist aktiviert. Darüber hinaus zeigt die Statuszeile für **Konfigurationsdateinamen** (über der Tabelle) jetzt den Namen des neu aktivierten Pakets im Feld **Aktiv** 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 der Aktivierung des virtuellen WAN-Dienstesfortfahren.
    - Wenn Sie Ihrem SD-WAN neue Clientknoten hinzufügen möchten, fahren Sie mit Verbinden der Client-Appliances mit Ihrem Netzwerk.
    - If you are activating an initial configuration, the new configuration package is not activated at this point, and there are more steps you must perform. The next step is to copy the configuration package to the Local Appliance Staging area, in preparation for staging and activating the configuration package on the MCN.

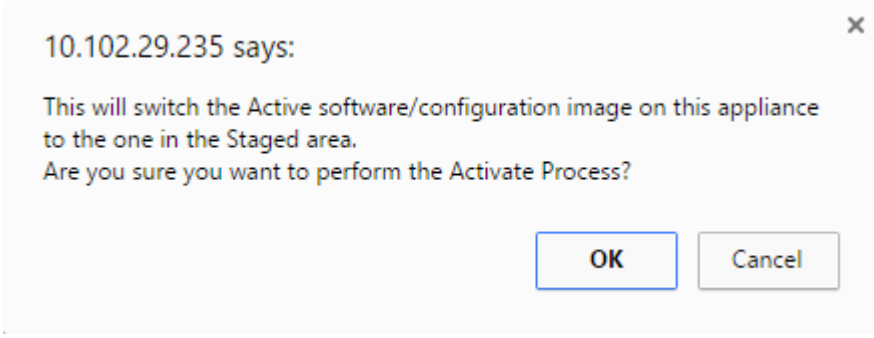
    Do the following:

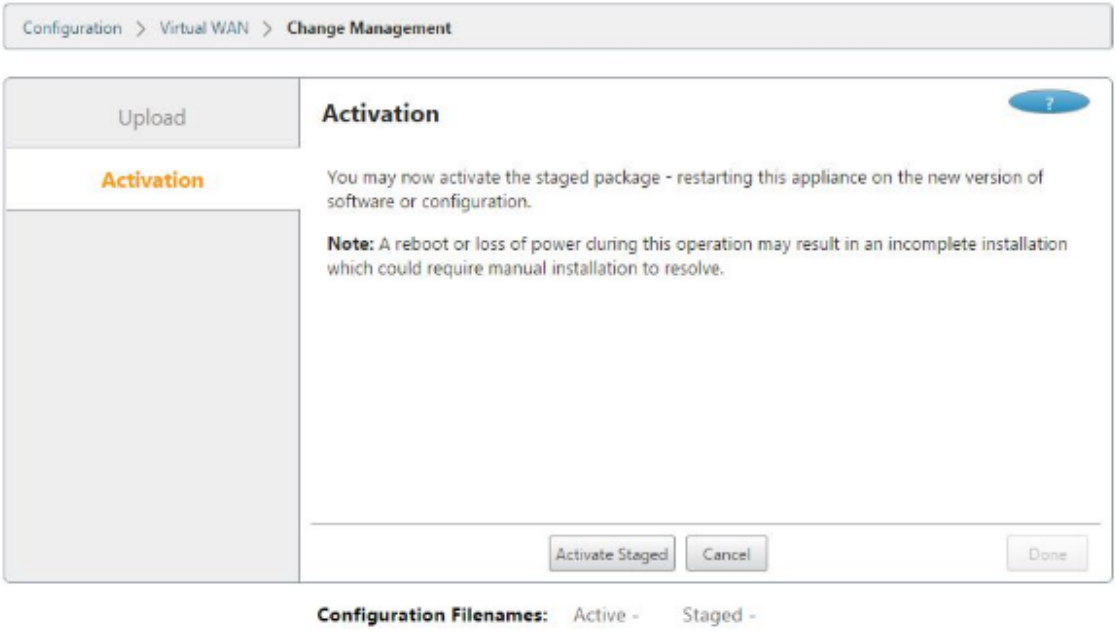
12. Sobald Sie auf **Staged aktivieren** geklickt haben, wird die folgende Meldung angezeigt.



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**.

Dies initiiert die Aktivierung des gestagten Konfigurationspakets. Dieser Vorgang dauert mehrere Sekunden, während der eine Statusmeldung angezeigt wird.

Wenn die Aktivierung abgeschlossen ist, wird eine Statusmeldung angezeigt, die besagt, dass die Aktivierung abgeschlossen ist, und die Schaltfläche **Fertig** ist aktiviert.

16. Klicken Sie auf **Fertig**. Dadurch wird die Seite Management Web Interface **Dashboard** weitergeleitet, auf der Sie die Aktivierungsergebnisse anzeigen können.

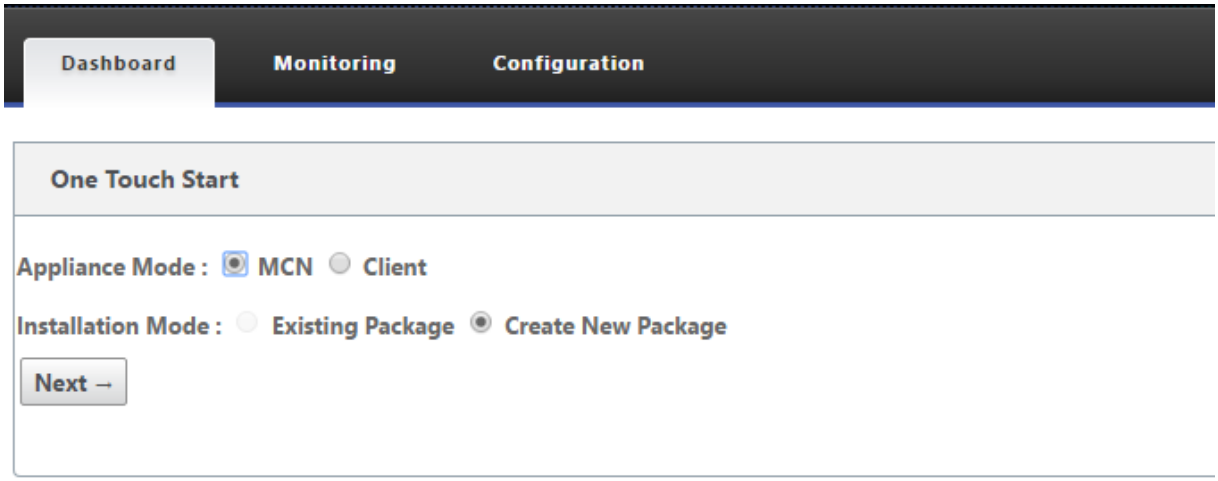
Sie haben nun die Vorbereitung der SD-WAN Appliance-Pakete auf dem MCN abgeschlossen. Fahren Sie mit (/en-us/citrix-sd-wan/current-release/configuration/connecting-client-appliances-to-network.html) fort, um die Clientgeräte mit Ihrem Netzwerk zu verbinden.

> **Tipp**
>
> Mit dem **Änderungsverwaltungsassistenten** können Sie die Site-Appliance-Tabelle durchsuchen. Auf diese Weise können Sie Websites in einem großen Netzwerk mit mehreren Standorten nachschlagen und die erforderliche Stagingkonfiguration herunterladen. Sie können auch nach Fehlerzuständen suchen, zum Beispiel: "Fehlgeschlagen"oder "Nicht verbunden". Dadurch erhalten Sie eine Liste aller Sites in diesem Status.

One-Touch-Start

October 28, 2021

Nach dem Touchstart können Sie Ihre SD-WAN-Appliance beim ersten Start einfach und schnell als Client konfigurieren.
Die One-Touch-Startoption wird angezeigt, wenn Ihr Gerät zum ersten Mal hochfährt.



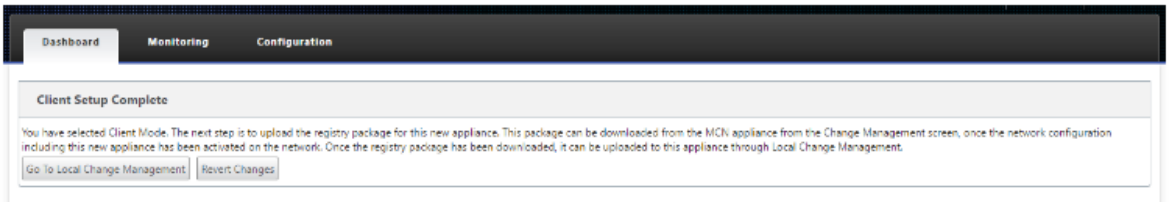
> **Hinweis**
>
> Um die SD-WAN-Appliance als MCN zu konfigurieren, erstellen Sie eine Konfiguration oder importieren Sie eine vorhandene Konfiguration mit dem **Konfigurationseditor**. Weitere Informationen finden Sie unter Vorbereiten der SD-WAN-Appliance-Pakete auf dem MCN

So konfigurieren Sie Ihre SD-WAN-Appliance als Client mithilfe einer vorhandenen Konfigurationsdatei:

1. Wählen Sie **Client** als Appliance-Modus aus.
2. Wählen Sie den Installationsmodus **vorhandenes Paket**. Der Administrator muss die Konfiguration des MCN regelmäßig speichern, um ein vorhandenes Paket des MCN nutzen zu können.
3. Klicken Sie auf **Datei auswählen**, um das Konfigurationspaket von Ihrem lokalen Computer auszuwählen.
4. Klicken Sie auf **Upload and Install**.

So konfigurieren Sie Ihre SD-WAN-Appliance mithilfe von Local Change Management 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 über den Bildschirm Änderungsverwaltung heruntergeladen werden.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Gehe zu Local Change Management.**



Befolgen Sie die Anweisungen im Thema Installieren der SD-WAN-Appliance-Pakete auf den Clients.

Verbinden der Client-Appliances mit dem Netzwerk

October 28, 2021

Bei einer Erstbereitstellung oder wenn Sie einem vorhandenen SD-WAN Client-Knoten hinzufügen, besteht der nächste Schritt darin, dass die Administratoren der Zweigstellen die Client-Appliances an ihren jeweiligen Zweigstellen mit dem Netzwerk verbinden. Dies ist in Vorbereitung auf das

Hochladen und Aktivieren der entsprechenden SD-WAN-Appliance-Pakete auf die Clients. Verbinden Sie jeden Zweigstandortadministrator, um diese Verfahren zu initiieren und zu koordinieren.

Um die Site-Appliances mit dem SD-WAN zu verbinden, sollten Site-Administratoren Folgendes tun:

1. Wenn Sie dies noch nicht getan haben, richten Sie die Client-Appliances ein.

   Gehen Sie für jede Appliance, die Sie zu Ihrem SD-WAN hinzufügen möchten, wie folgt 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. Stellen Sie den Timeout-Schwellenwert für die Konsolensitzung auf einen hohen oder den Maximalwert ein.
   d) Laden Sie die Softwarelizenzdatei hoch und installieren Sie sie auf der Appliance.

2. Verbinden Sie das Gerät mit dem LAN der Zweigstelle. Verbinden Sie ein Ende eines Ethernet-Kabels mit einem für LAN konfigurierten Port auf der SD-WAN-Appliance. Verbinden Sie dann das andere Ende des Kabels mit dem LAN-Switch.

3. Verbinden Sie das Gerät mit dem WAN. Verbinden Sie ein Ende eines Ethernet-Kabels mit einem für WAN konfigurierten Port auf der SD-WAN-Appliance. 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

October 28, 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 WAN verbunden haben, besteht der nächste Schritt darin, das entsprechende SD-WAN-Appliance-Paket auf jedem Client hochzuladen und zu aktivieren. Der Änderungsmanagement-Assistent führt Sie durch diesen Prozess.

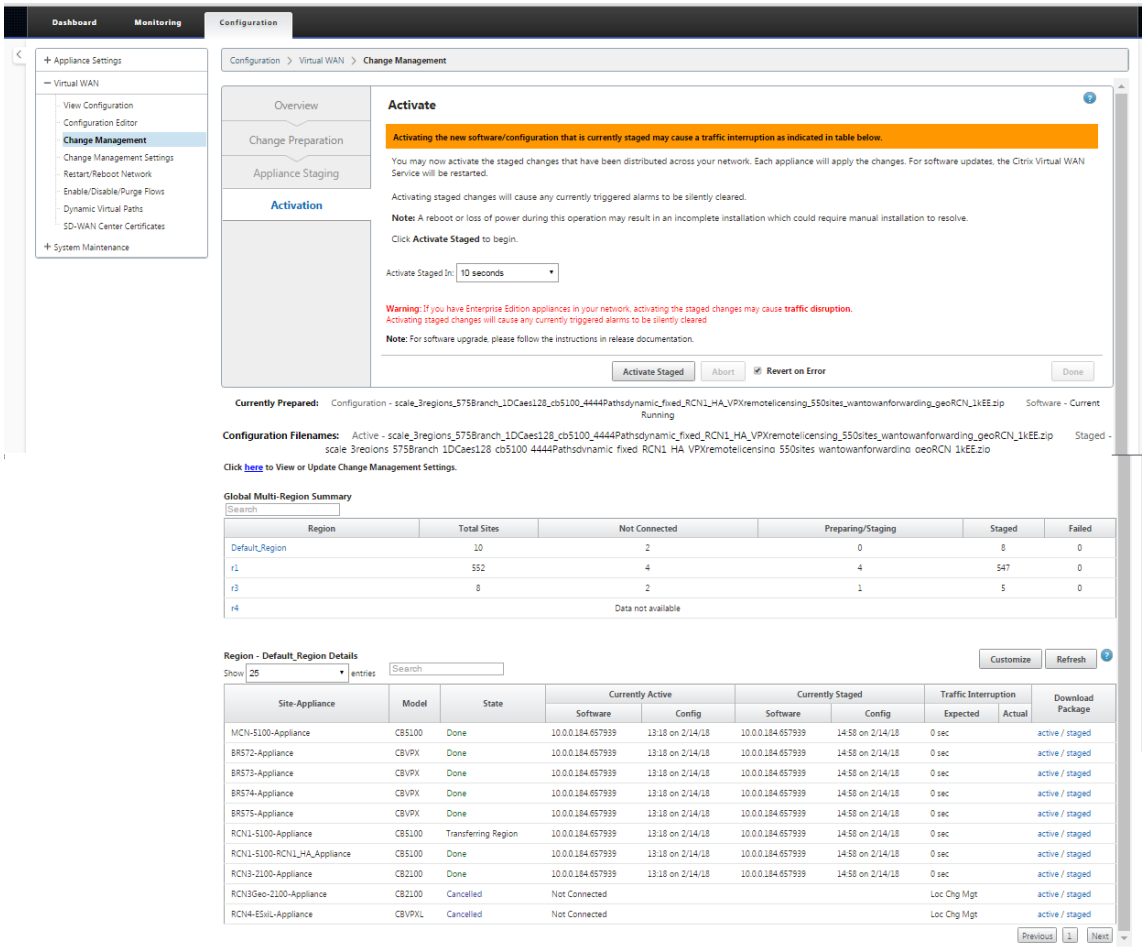
Gehen Sie wie folgt vor, um die Software und Konfiguration auf einer Client-Appliance zu installieren und zu aktivieren

1. Öffnen Sie auf einem angeschlossenen PC einen Browser und melden Sie sich am MCN-Appliance-Management-Webinterface an.

Geben Sie die Management-IP-Adresse für den MCN in das Adressfeld des Browsers ein. Dadurch wird die Seite Management Web Interface **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 **Change Process Overview** (die erste Seite des **Change Management-Assistenten**) angezeigt.



Unten auf dieser Seite sehen Sie eine Tabelle mit den einzelnen Websites und Appliances. Ganz rechts in der Tabelle in der Spalte **Paket herunterladen** befinden sich Links für die Pakete **Aktiv** (falls verfügbar) und **Staged appliance**.

Hinweis

> Wenn es sich um eine Erstinstallation handelt, sind die **Active-Links** noch nicht verfügbar und werden durch eine Nur-Text-Markierung **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 Site-Appliance und klicken Sie auf den Link **Staged** in der Spalte **Paket herunterladen** dieses Eintrags. Ein Dateibrowser zur Auswahl des Download-Speicherorts (auf dem lokalen PC) wird angezeigt.

4. Wählen Sie den Download-Ort und klicken Sie auf **OK.**

5. (Optional.) Melden Sie sich nach Abschluss des Downloads vom MCN Management Webinterface ab.

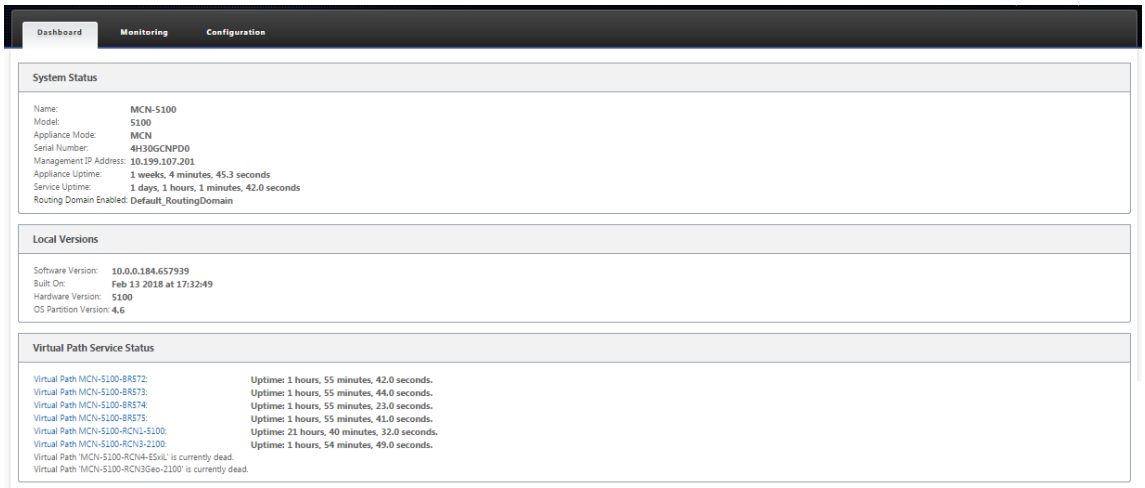
6. Öffnen Sie einen Browser und geben Sie die IP-Adresse des Clients ein, auf den Sie die ZIP-Datei des Appliance-Pakets hochladen möchten.

   > **Hinweis**
   >
   > Bitte ignorieren Sie alle Warnungen zu Browserzertifikaten für das Management-Webinterface.

   Dadurch wird das Anmeldebildschirm für das Citrix SD-WAN Management Webinterface auf der Client-Appliance geöffnet.

7. Geben Sie den Benutzernamen und das Kennwort des Administrators ein und klicken Sie auf **Anmelden** Der standardmäßige Administrator-Benutzername lautet *admin*. Das Standardkennwort ist *Kennwort*.

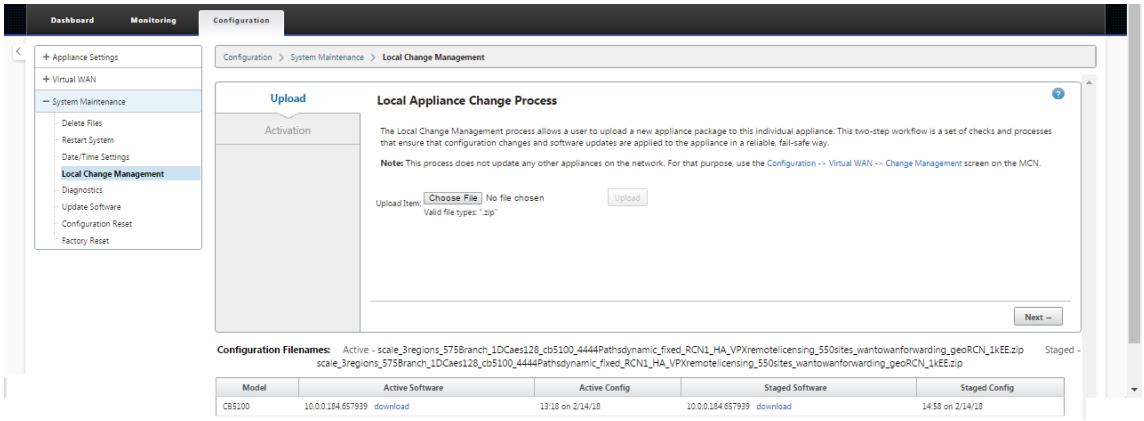
   Dadurch wird die Seite Management Web Interface **Dashboard** für die Client-Appliance angezeigt.



> **Hinweis**
>
> Wenn es sich um eine Erstinstallation handelt oder wenn Sie den virtuellen WAN-Dienst auf dieser Appliance vorübergehend deaktiviert haben, wird ein Symbol für Goldenrod Audit Alert mit einer Statusmeldung angezeigt, die darauf hinweist, dass der Virtual WAN-Dienst inaktiv oder deaktiviert ist. Sie können diese Warnung vorerst ignorieren. Die Warnung bleibt auf der Seite **Dashboard**, 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 **Lokales Änderungsmanagement**aus.

   Dadurch wird die Seite **Upload des lokalen Appliance-Änderungsprozesses** zum Hochladen eines Appliance-Pakets angezeigt.



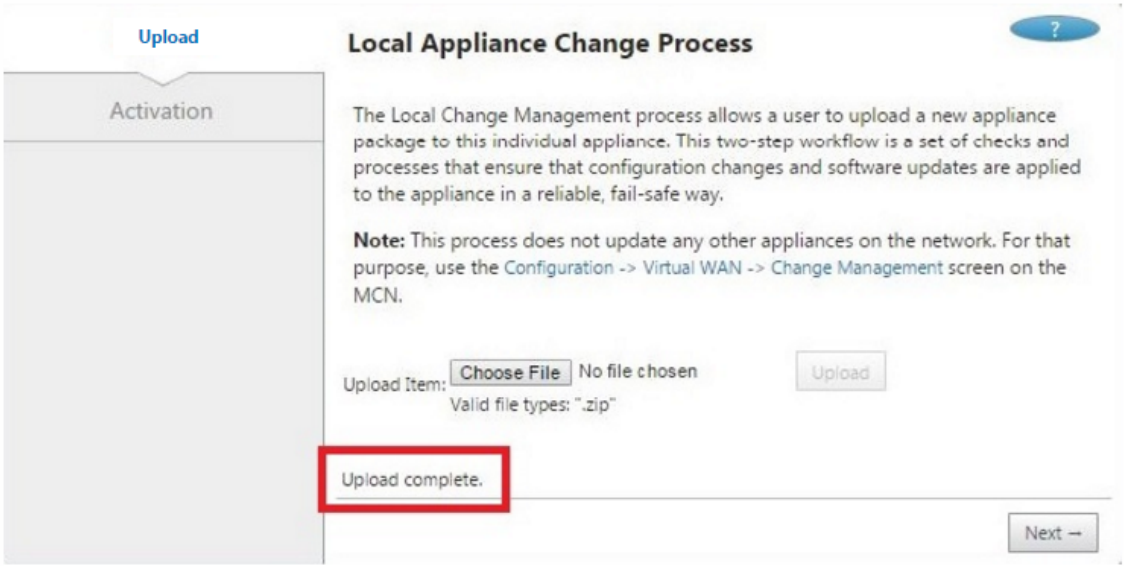
10. Klicken Sie neben dem Label **Element hochladen** auf **Datei auswählen**.

    Dadurch wird ein Dateibrowser für die Auswahl des Appliance-Pakets geöffnet, das Sie auf den Client hochladen möchten.

11. Navigieren Sie zur Zip-Datei des SD-WAN-Appliance-Pakets, die Sie gerade vom MCN heruntergeladen haben, wählen Sie sie aus und klicken Sie auf **OK**.

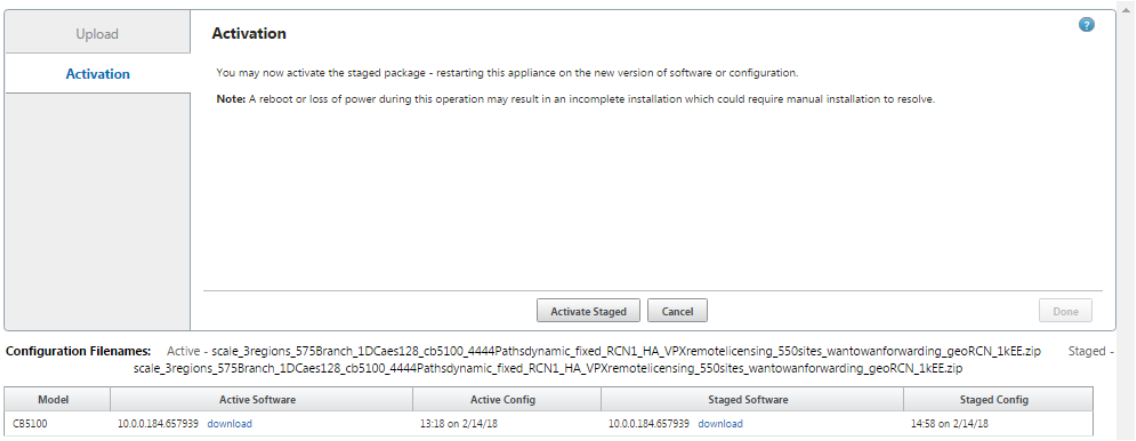
12. Klicken Sie auf **Upload**.

    Der Upload-Vorgang dauert einige Sekunden. Nach Abschluss wird eine Statusmeldung (linke Mitte der Seite) mit der Meldung **Upload abgeschlossen angezeigt.**



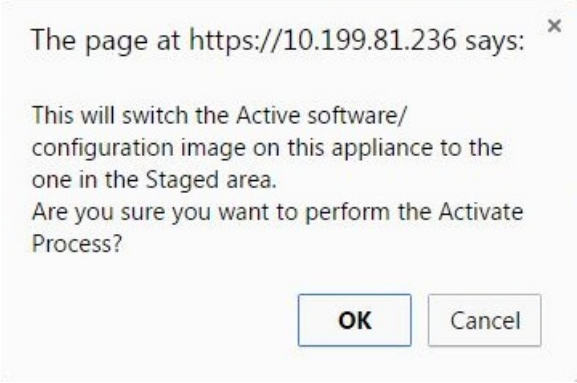
13. Klicken Sie auf **Weiter**.

    Dadurch wird das angegebene Softwarepaket hochgeladen und die Seite "Lokale Change **Management-Aktivierung** "angezeigt.



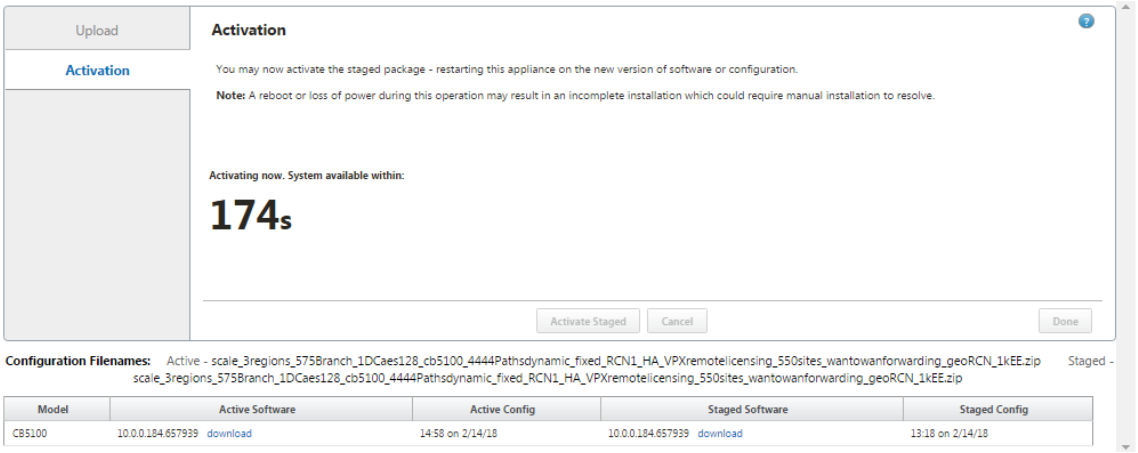
14. Klicken Sie auf **Activate Staged**.

    Daraufhin wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, den Aktivierungsvorgang zu bestätigen.

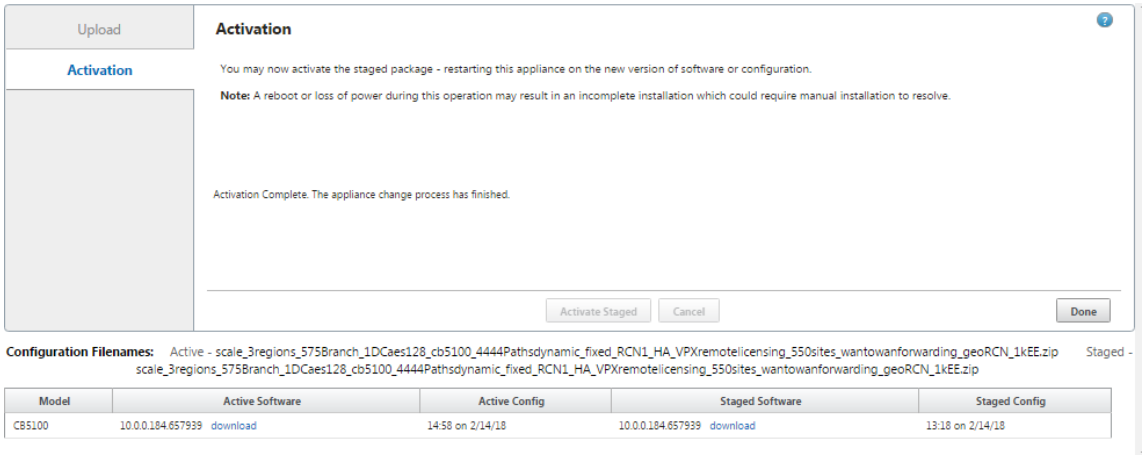


15. Klicken Sie auf **OK**.

    Dadurch wird das neu installierte Paket aktiviert und, falls es sich nicht um eine Erstbereitstellung handelt, wird der virtuelle 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 angezeigt, die besagt, dass die **Aktivierung abgeschlossen**ist, und die Schaltfläche **Fertig** wird verfügbar.

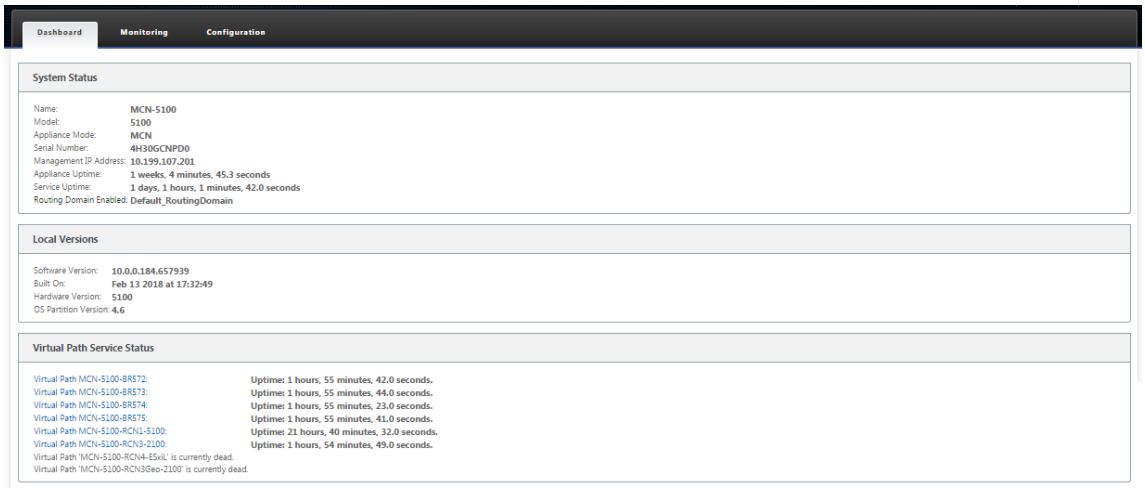


16. Klicken Sie auf **Fertig**, um den Assistenten zu beenden und die Aktivierungsergebnisse anzuzeigen.

    Nachdem die Aktivierung abgeschlossen ist, klicken Sie auf der Seite **Aktivierung** auf **Fertig**, um zur Seite Management Web Interface **Dashboard** zurückzukehren.

    Wenn es sich nicht um eine Erstbereitstellung handelt, sollte diese Seite jetzt aktualisierte Informationen für die derzeit aktive Version des Softwarepakets, die Betriebssystempartition und den Status des virtuellen Pfads anzeigen. Wenn es sich um eine Erstinstallation handelt, wird ein Goldrud-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 Aktivieren des virtuellen WAN-Dienstesbeschrieben.

    Die folgende Abbildung zeigt eine Beispielseite des **Client-Dashboards**, 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-Dienstes.

Bereitstellen von Citrix SD-WAN Standard Edition in OpenStack mit CloudInit

October 28, 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.

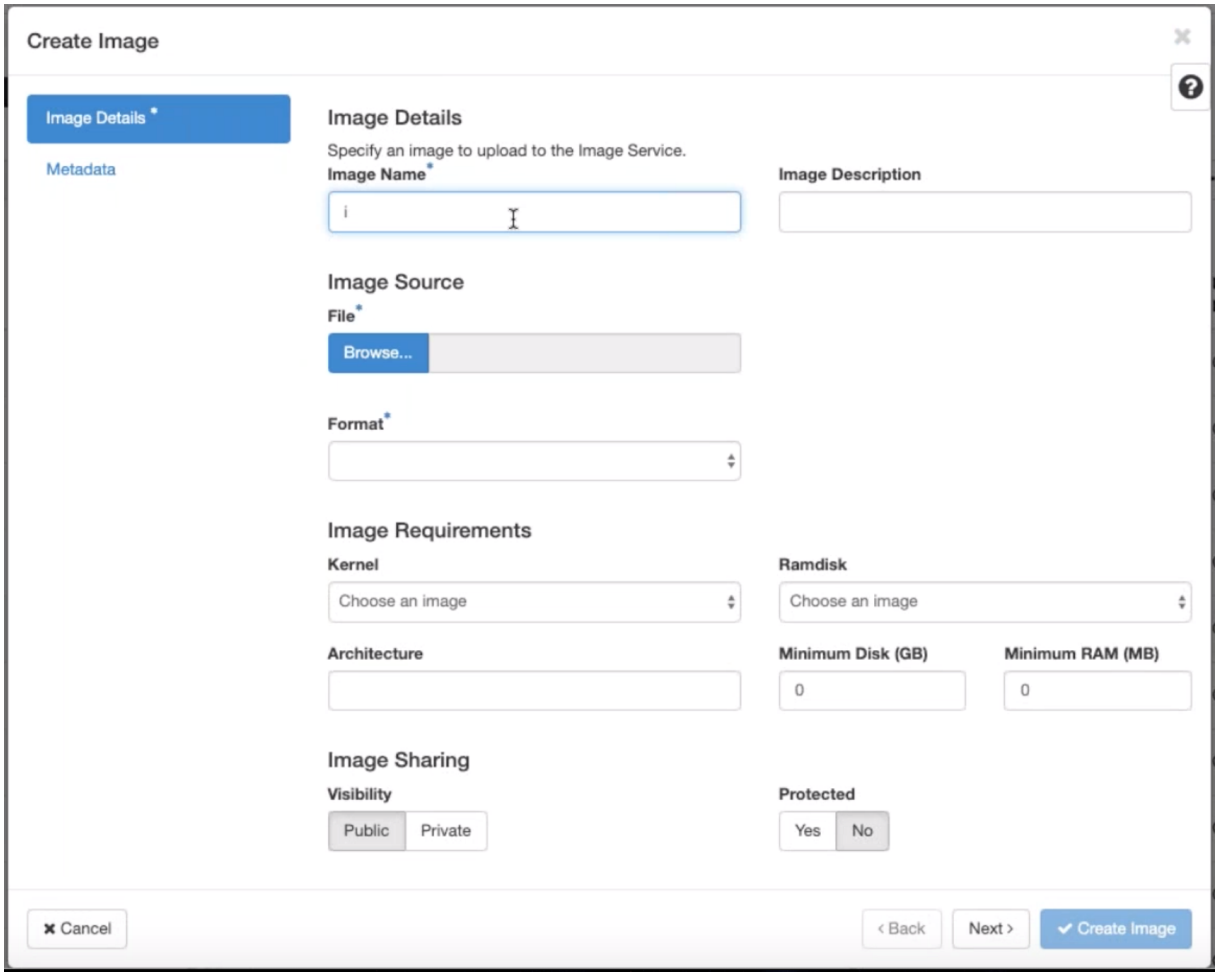
Für eine SD-WAN-Instanz in OpenStack sind die Eingaben für Management IP, DNS und Seriennummer der Benutzer erforderlich. Das Cloudinit-Skript analysiert diese Eingaben und stellt der Instanz die angegebenen Informationen zur Verfügung.

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**.



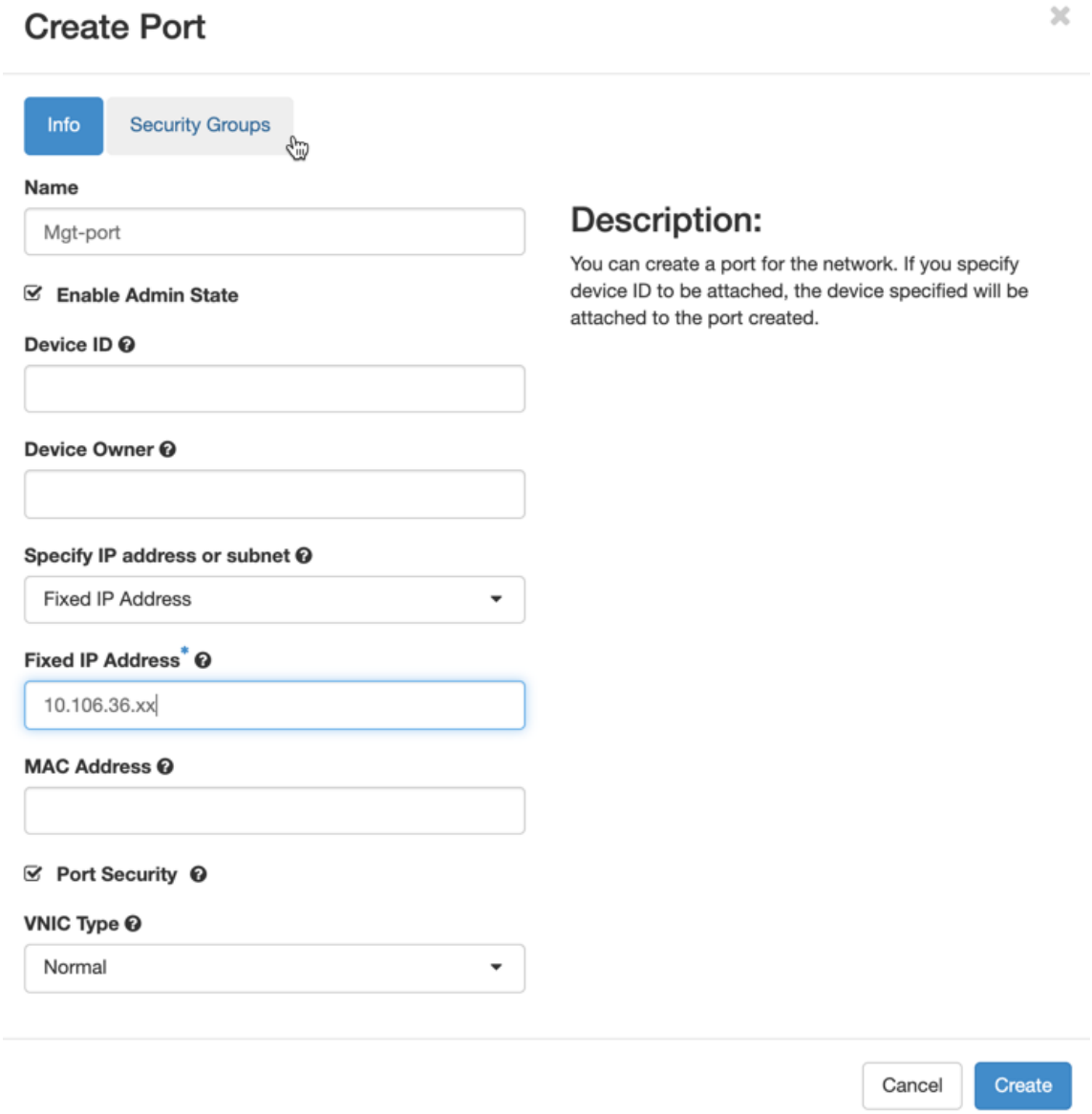
- **Imagename** - Geben Sie den Imagenamen an.
- **Imagebeschreibung** —Fügen Sie eine Bildbeschreibung hinzu.
- **Datei** - Suchen Sie von Ihrem lokalen Laufwerk nach der kvm.qcow2-Imagedatei und wählen Sie sie aus.

- **Format** —Wählen Sie das Datenträgerformat QCOW2 —QEMU Emulator aus der Dropdownliste aus.

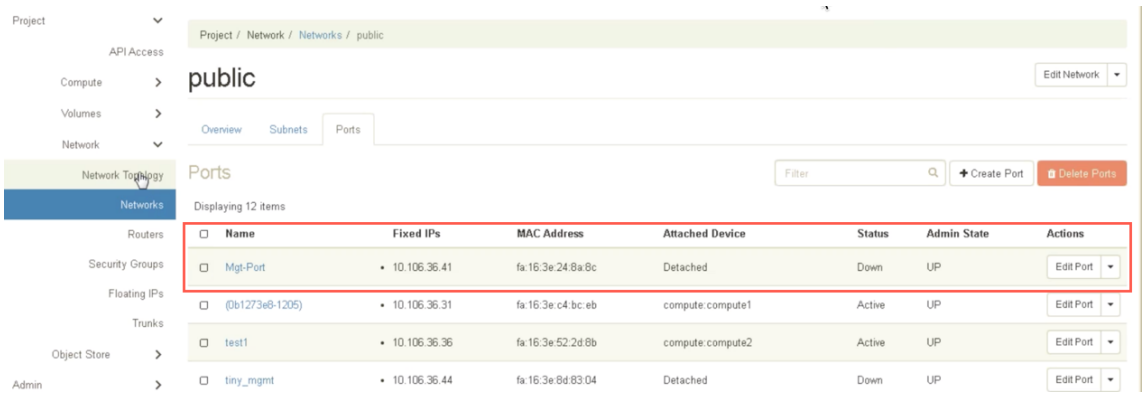
Klicken Sie auf **Image erstellen**.

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.



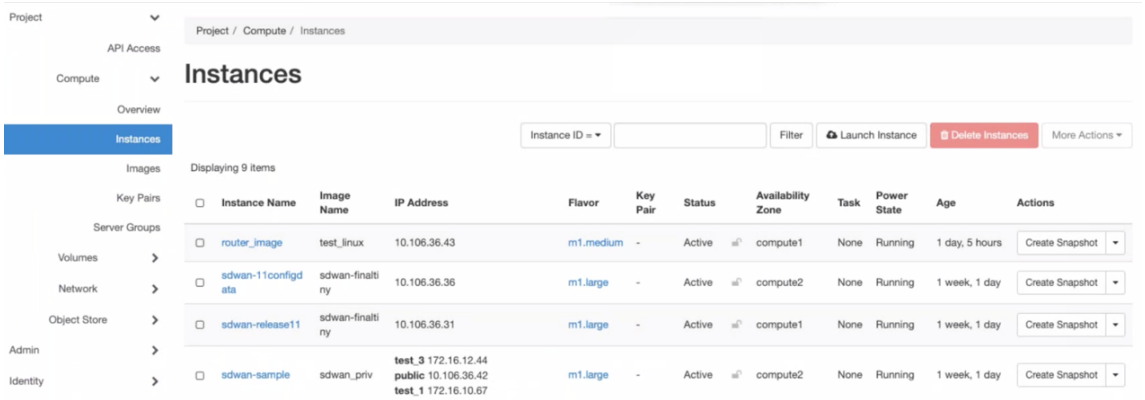
Wenn Sie **Feste IP-Adresse**auswählen, müssen Sie die Subnetz-IP-Adresse für den neuen Port angeben.



Der Port wird erstellt und da er nicht an ein Gerät angeschlossen ist, wird der aktuelle Status als Detached angezeigt.

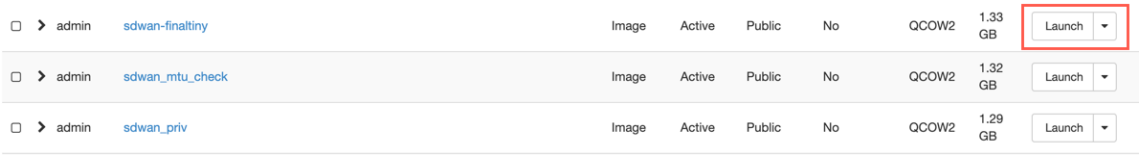
Erstellen Sie OpenStack-Instanz, um config-drive zu aktivieren und die user_data zu übergeben.

3. Melden Sie sich bei OpenStack an und konfigurieren Sie Instanzen.



4. Laden Sie die **kvm.qcow2.gz-Datei** herunter und entpacken Sie sie.
5. Gehen Sie zu **Instances** und klicken Sie auf **Launch Instance**

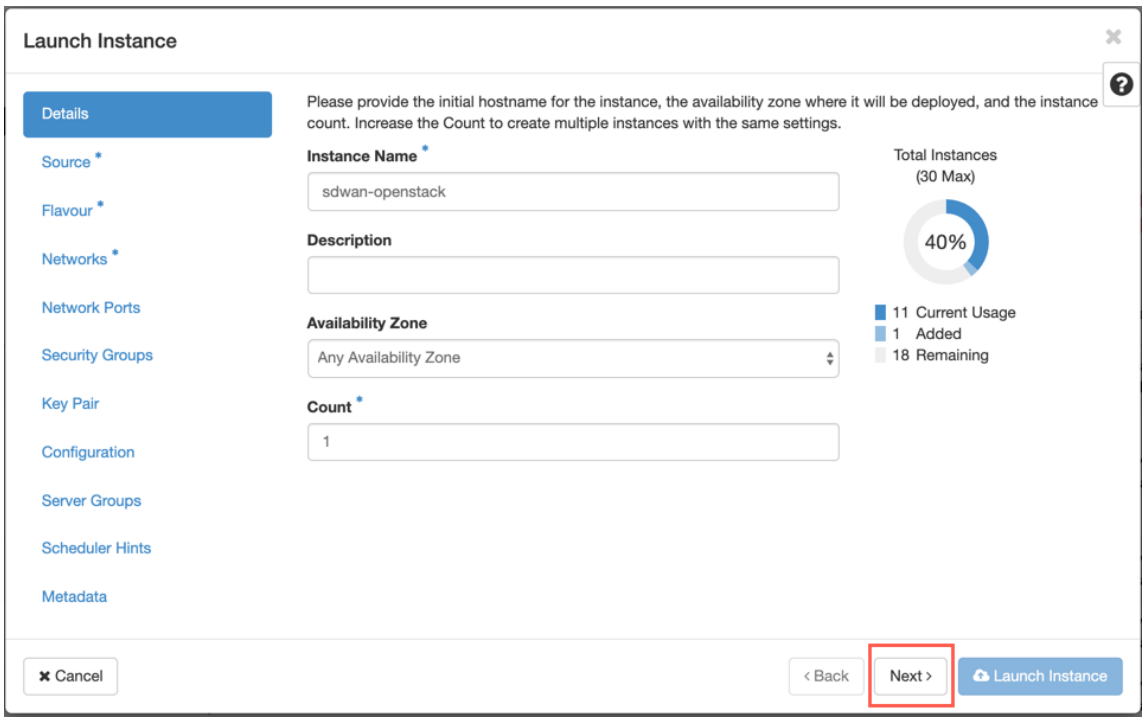
> **HINWEIS**
>
> Sie können zu **Instances** zurückkehren und auf **Launch Instance** klicken oder im Bildschirm Images auf **Launch** klicken, sobald das Image erstellt wurde.



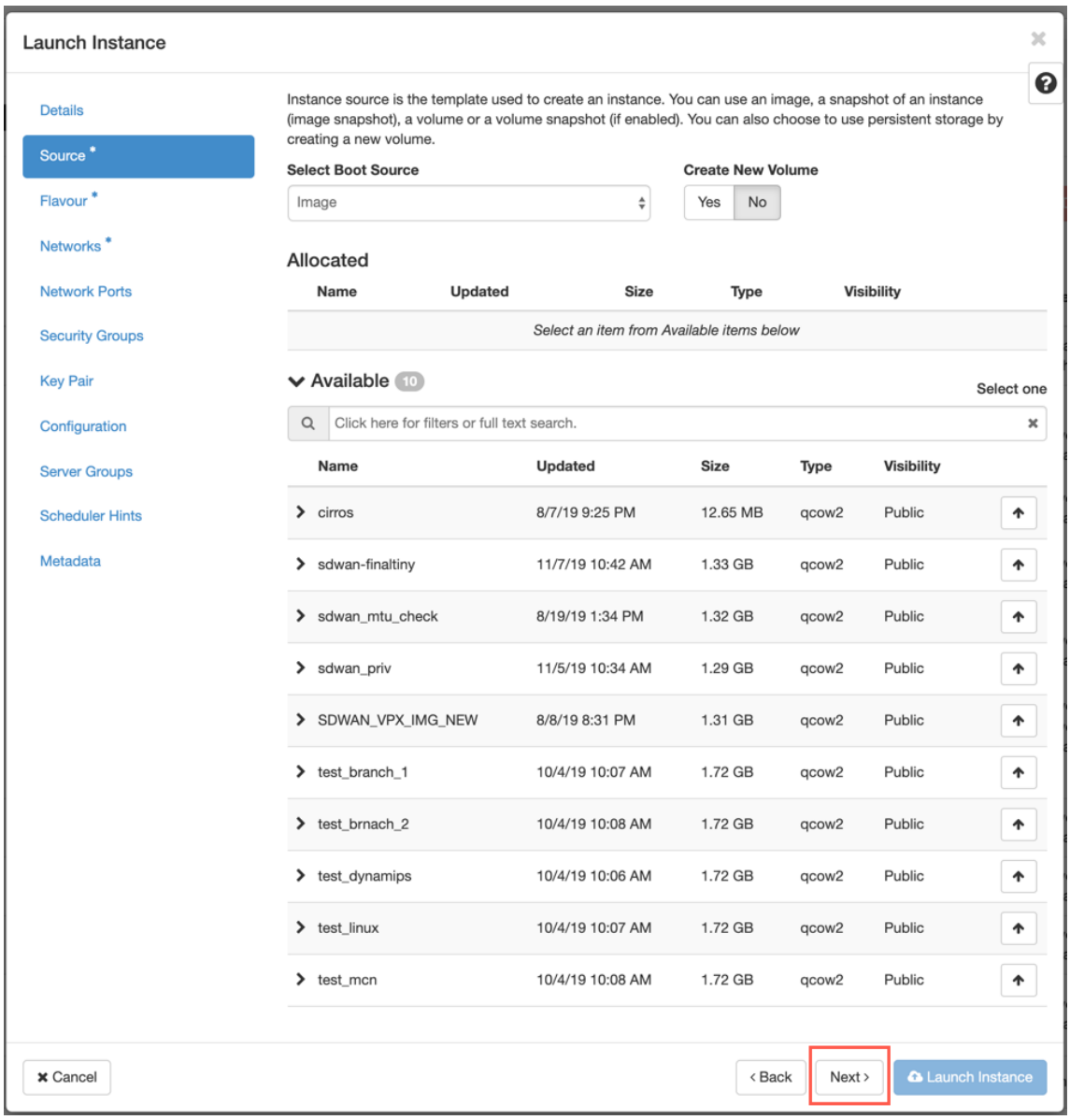
6. Geben Sie auf der Registerkarte **Details** die folgenden Informationen an:

   - **Instanzname** —Geben Sie den Hostnamen für die Instanz an.
   - **Beschreibung** —Fügt eine Beschreibung für die Instanz hinzu.

- **Availability Zone** —Wählen Sie die Availability Zone aus der Dropdownliste 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**.



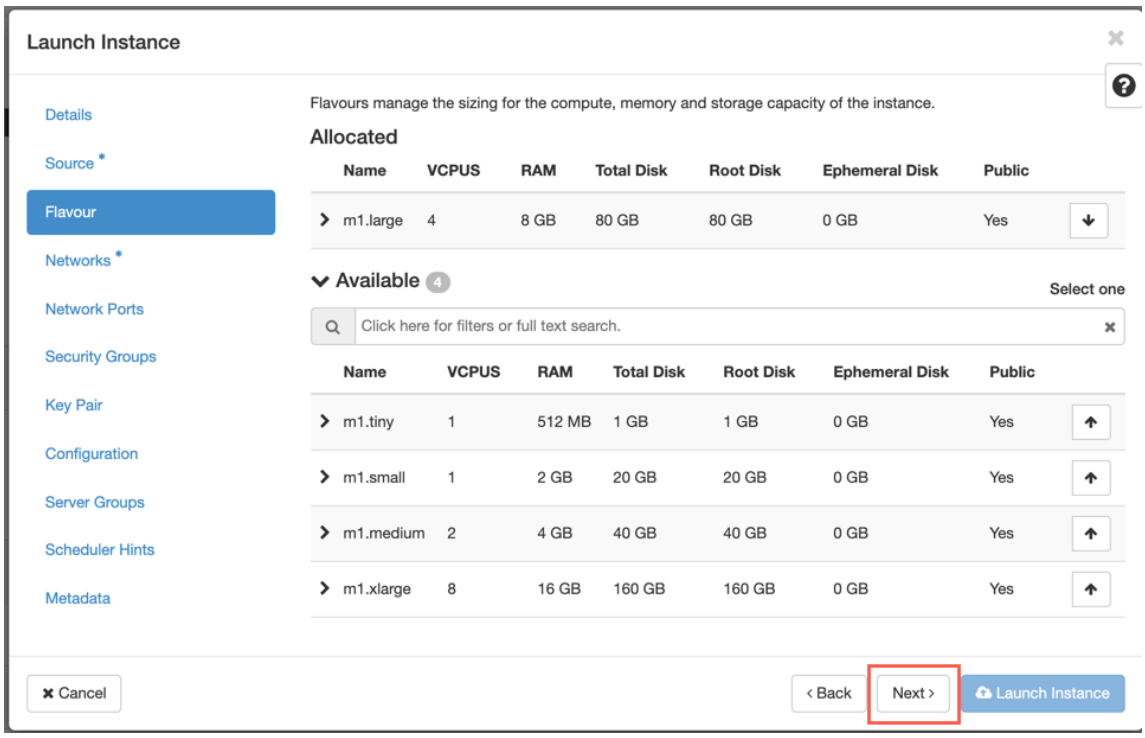
7. Wählen Sie auf der Registerkarte **Quelle** unter **Neues Volume erstellen** die Option **Nein** aus und klicken Sie auf**Weiter**. Instanzquelle ist die Vorlage, die zum Erstellen einer Instanz verwendet wird.



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.

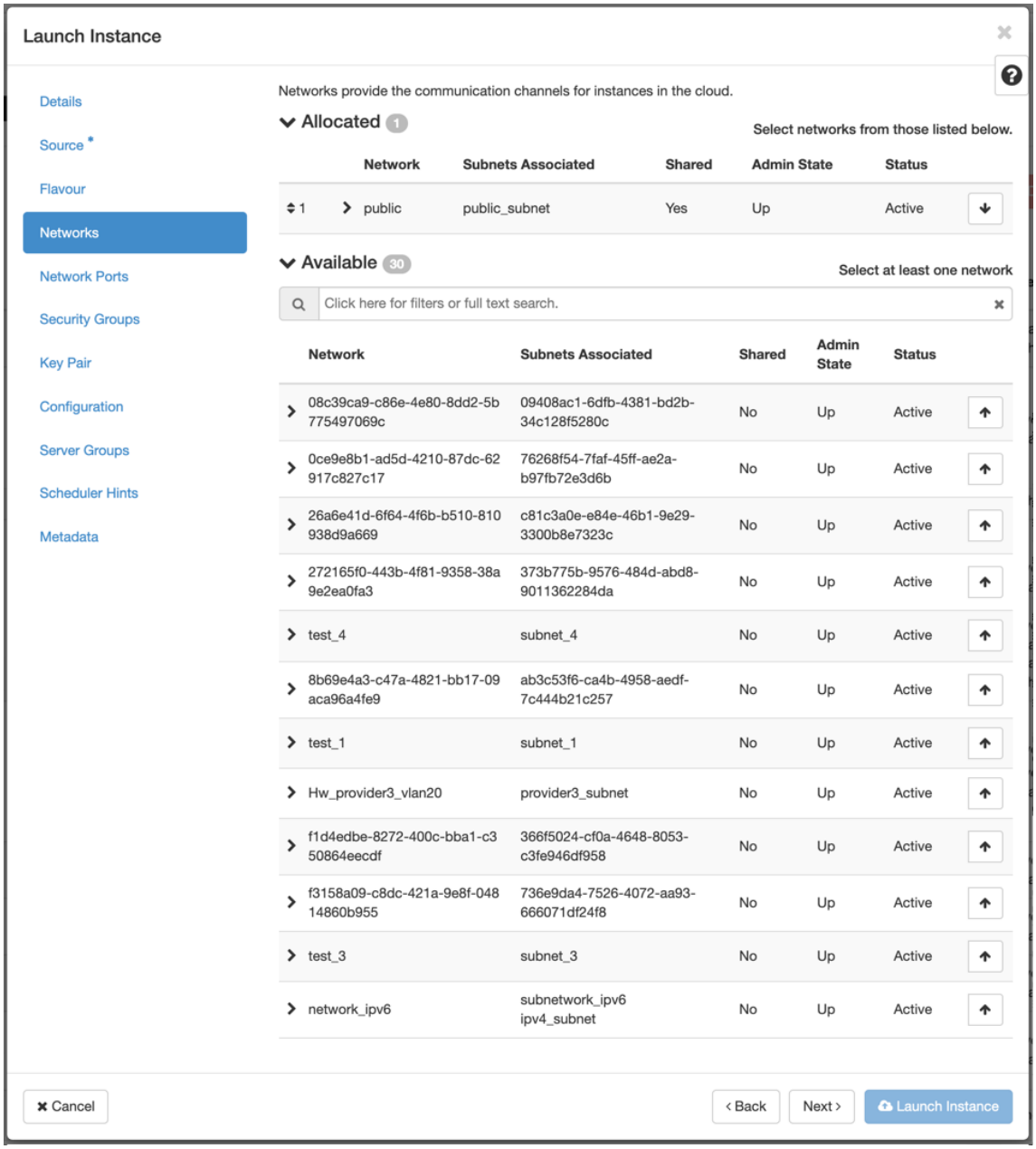
> **HINWEIS:**
>
> Dem ausgewählten Flavour müssen genügend Ressourcen zugewiesen sein, um den Instanztyp zu unterstützen, den Sie erstellen möchten. Flavours, die nicht genügend Ressourcen für Ihre Instanz bereitstellen, werden in der verfügbaren Tabelle mit einem gelben Warnsymbol gekennzeichnet.

Administratoren sind für die Erstellung und Verwaltung von Geschmacksrichtungen verantwortlich. Klicken Sie auf den Pfeil (rechts), den Sie zuweisen möchten.



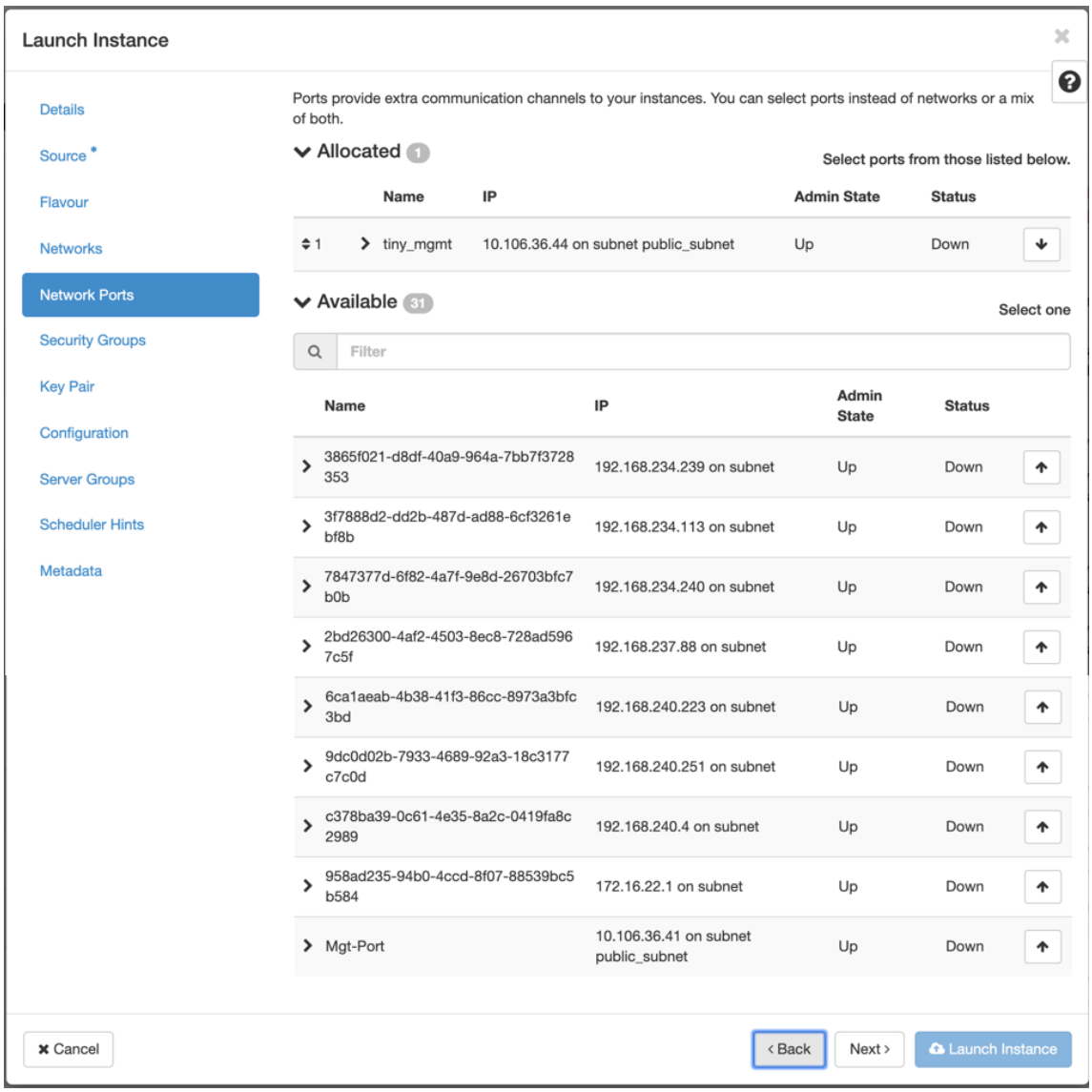
9. Wählen Sie das Netzwerk aus und klicken Sie auf **Weiter**. Netzwerke stellen die Kommunikationskanäle für Instanzen bereit.

> **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.



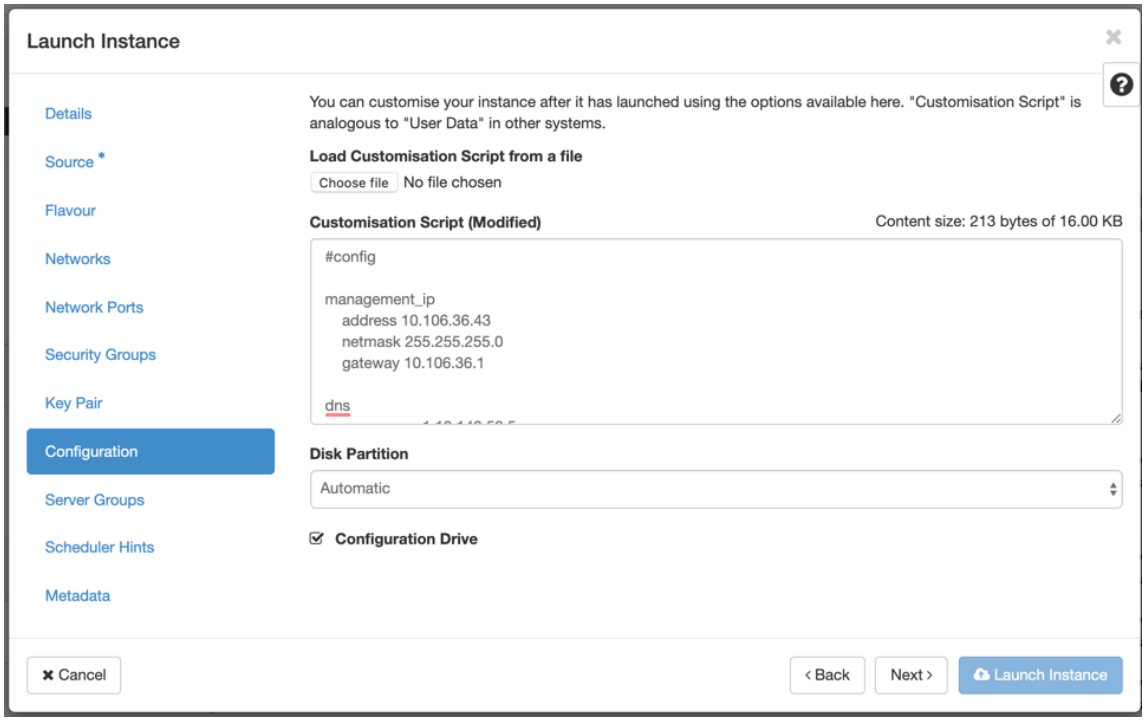
10. Wählen Sie einen Netzwerkport für die Instanz und klicken Sie auf **Weiter**. Netzwerkports stellen zusätzliche Kommunikationskanäle für die Instanzen bereit.

> **HINWEIS:**
>
> Sie können Ports anstelle von Netzwerken oder eine Mischung aus beiden auswählen.



11. Gehen Sie zu **Configuration** und klicken Sie auf **Choose file** Markieren Sie die Datei user_data. 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.



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.

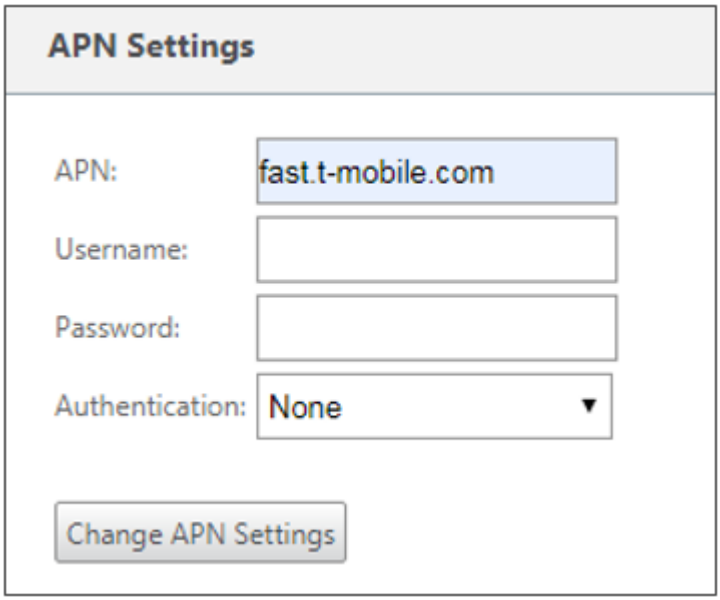
   > **Hinweis:**
   > Es wird nur eine Standard- oder 2FF-SIM-Karte (15x25 mm) unterstützt.

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**.

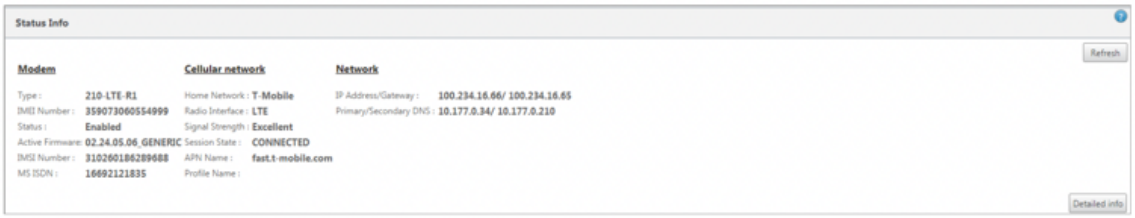
4. Konfigurieren Sie die APN-Einstellungen. Navigieren Sie in der SD-WAN GUI zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband > APN-Einstellungen**.

> **Hinweis:**
> Rufen Sie die APN-Informationen vom Anbieter ab.



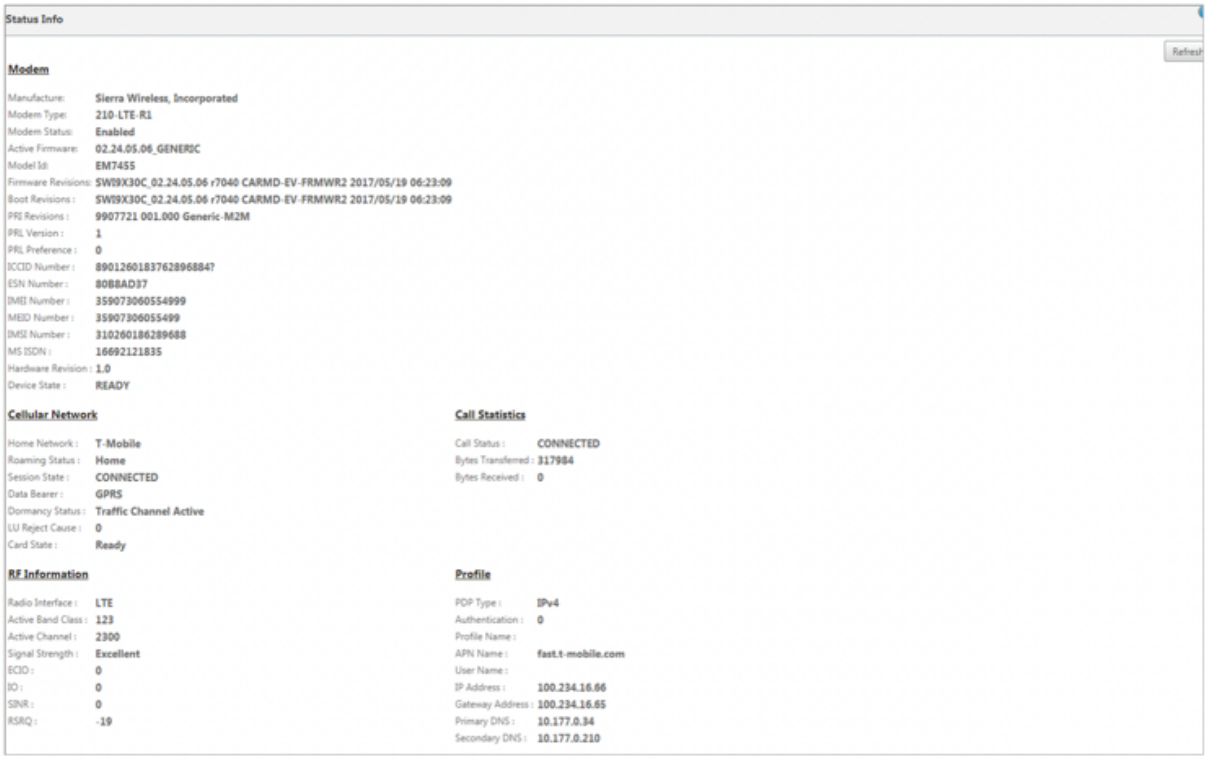
5. Geben Sie den **APN**, den **Benutzernamen**, **das Kennwort**und die **Authentifizierung** ein, die vom Anbieter bereitgestellt werden. Sie können zwischen PAP, CHAP, PAPCHAP Authentifizierungsprotokollen wählen. Wenn der Anbieter keinen Authentifizierungstyp angegeben hat, setzen Sie ihn auf **Keine**.
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:

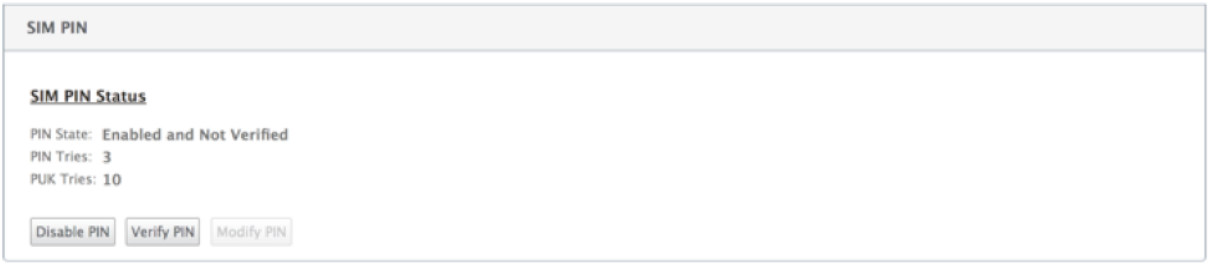
- **Betriebsart**: Zeigt den Modemstatus an.
- **Aktive SIM**: Zu einem bestimmten Zeitpunkt kann nur eine SIM aktiv sein. Die aktuell aktive SIM wird angezeigt.
- **Kartenstatus**: Vorhanden zeigt an, dass die SIM ordnungsgemäß eingelegt ist.
- **Signalstärke**: Qualität der Signalstärke - ausgezeichnet, 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.



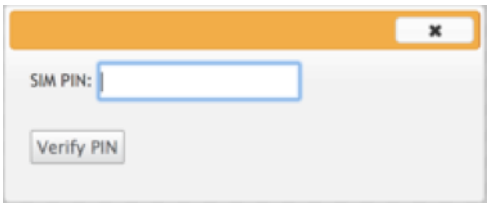
SIM-PIN

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.

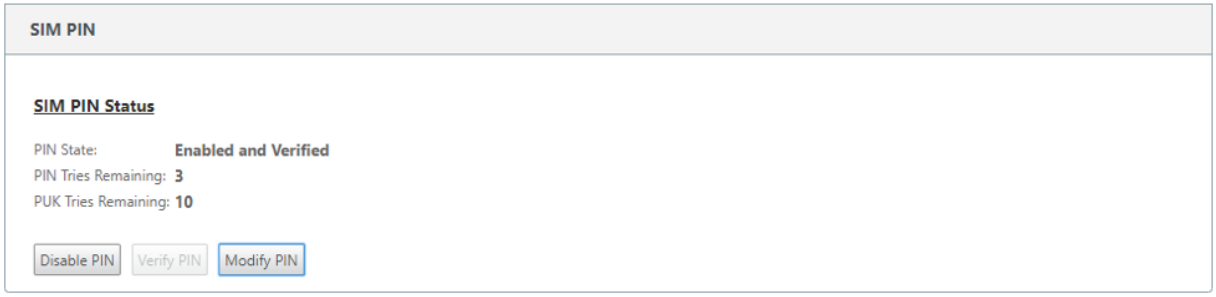
Um SIM-PIN-Vorgänge durchzuführen, navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Mobiles Breitband > SIM-PIN**.



Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.

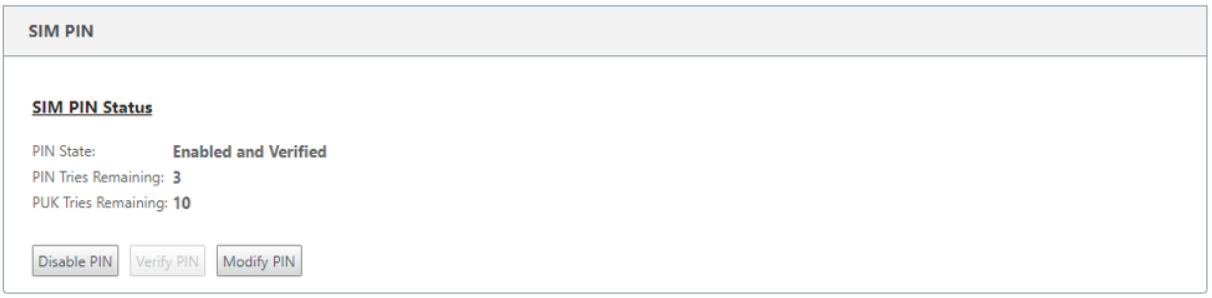


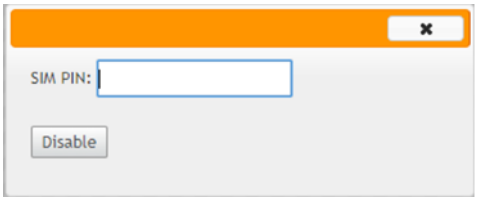
Der Status ändert sich in **Aktiviert und Verifiziert**.



SIM-PIN deaktivieren

Sie können die SIM-PIN-Funktionalität für eine SIM-Karte deaktivieren, für die SIM-PIN aktiviert und verifiziert ist.

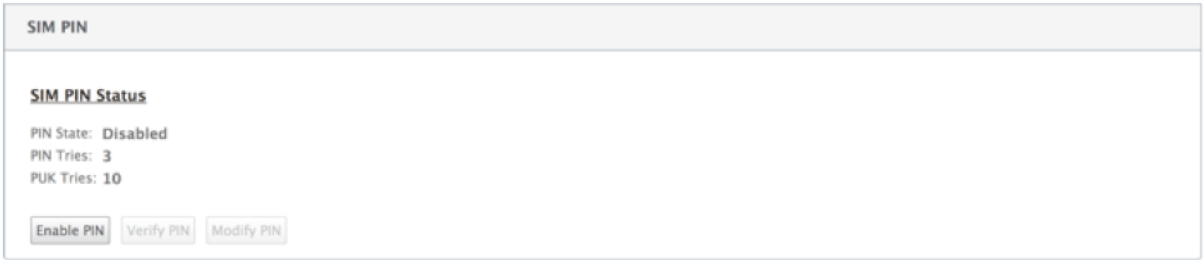




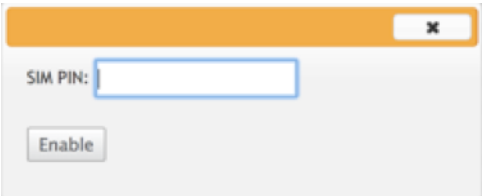
Klicken Sie auf **PIN deaktivieren**. Gib die **SIM-PIN** ein und klicke auf **Deaktivieren**

SIM-PIN aktivieren

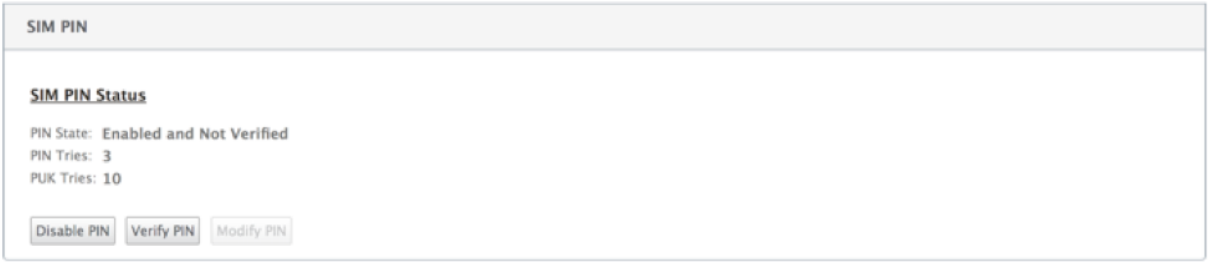
Die SIM-PIN kann für die SIM aktiviert werden, für die sie deaktiviert ist.



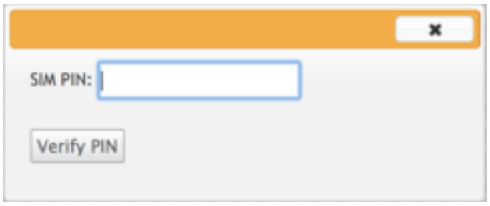
Klicken Sie auf **PIN aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**.



Wenn sich der SIM-PIN-Status in **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.



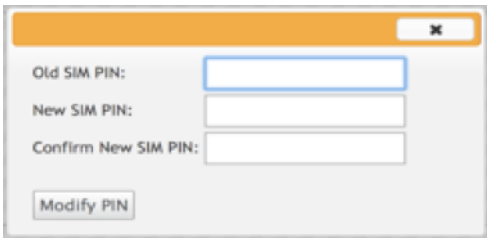
Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.



SIM-PIN ändern

Sobald die PIN im Status **Aktiviert und Verifiziert** ist, können Sie die PIN ändern.

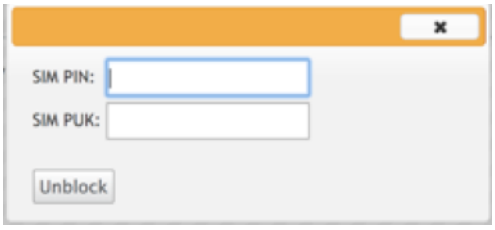
Klicken Sie auf **PIN ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **PIN ändern**.



SIM aufheben

Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe der vom Träger erhaltenen SIM-PUK zurücksetzen.

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**.



> **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.

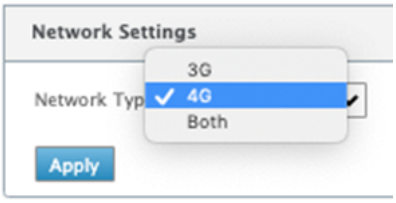
Firmware verwalten

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.

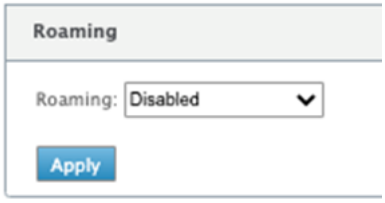
Netzwerkeinstellungen

Sie können das Mobilfunknetz auf 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

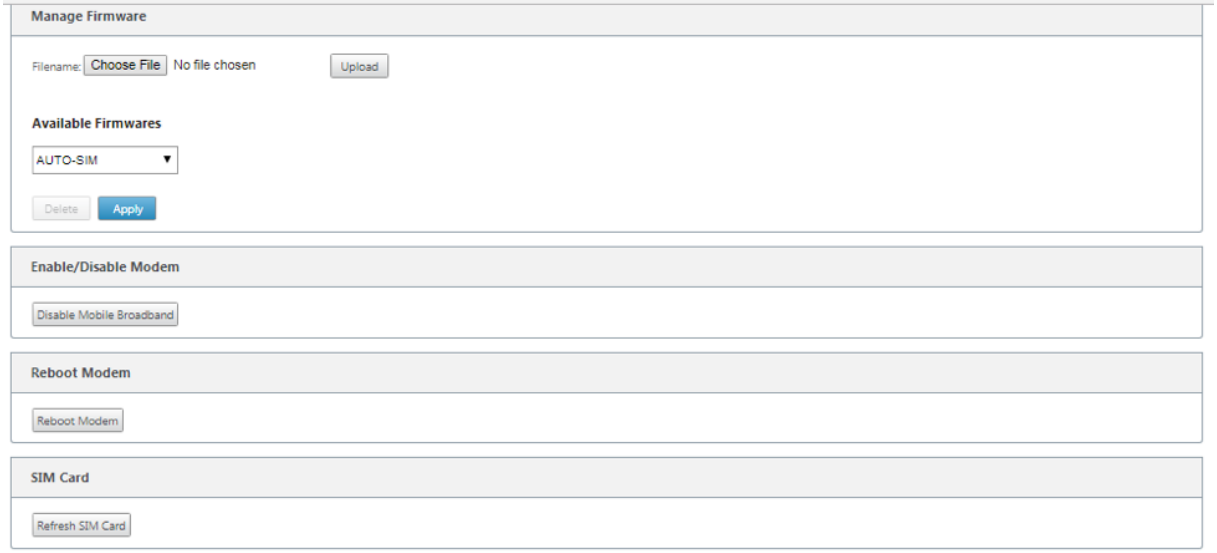
Aktivieren/deaktivieren Sie das Modem abhängig von Ihrer Absicht, die LTE-Funktionalität zu verwenden. Standardmäßig ist das LTE-Modem aktiviert.

Modem neu starten

Startet das Modem neu. Es kann bis zu 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.



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 <unblock> <sim puk> <sim pin>   # Unblock SIM card PIN
reboot                                  # Reboot modem
ping                                    # Check if modem manager ready
list-fw                                 # List available firmware
apply-fw <fw>                           # Apply the specified firmware
```


In der folgenden Tabelle sind die Beschreibungen des **LTE**-Befehls aufgeführt.

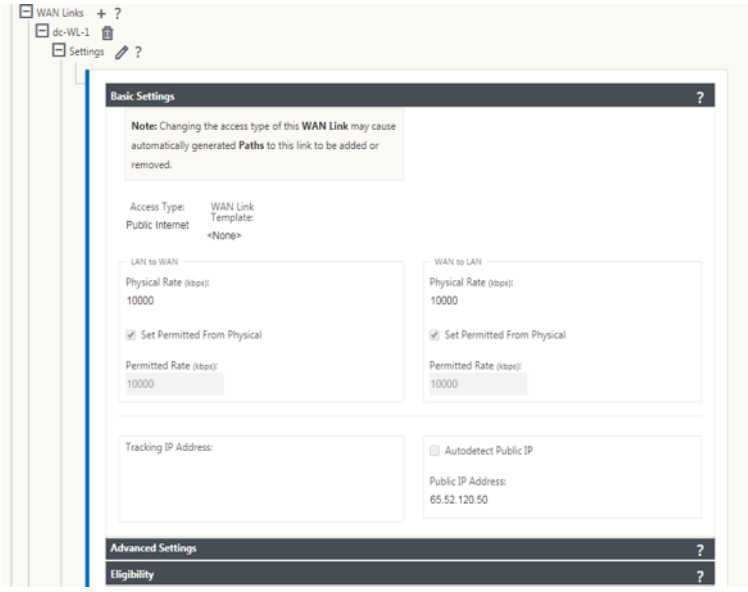
Command	Beschreibung
Help {lte>help}	Listet die verfügbaren LTE-Befehle und -Parameter auf
Status {lte>status}	Zeigt den LTE-Konnektivitätsstatus an
Show {lte>show}	Zeigt LTE-Einstellungen an
Disable {lte>disable}	Deaktiviert das LTE-Modem
Aktiviere {lte>enable}	Aktiviert LTE-Modem
Apn {lte>apn}	Konfiguriert 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.

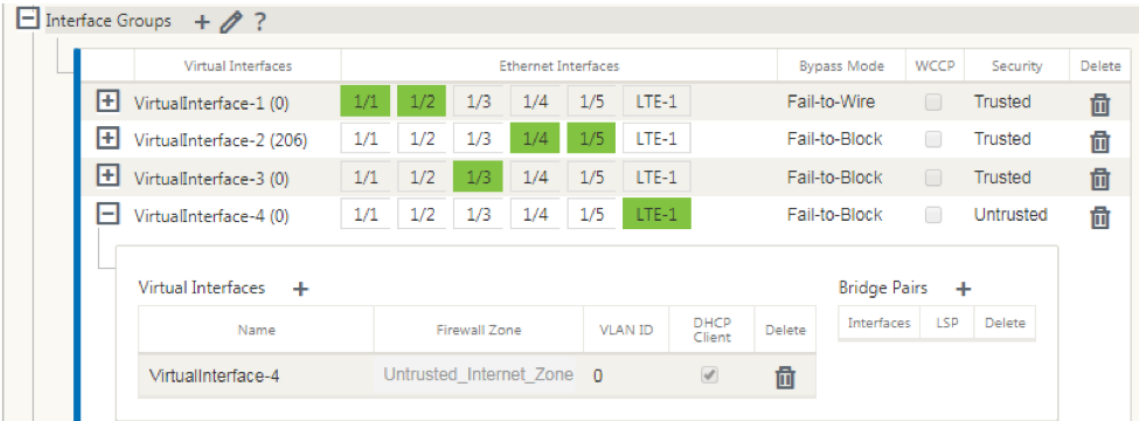


Zweig für LTE konfigurieren

So konfigurieren Sie die 210-SE LTE-Appliance als Zweigstelle:

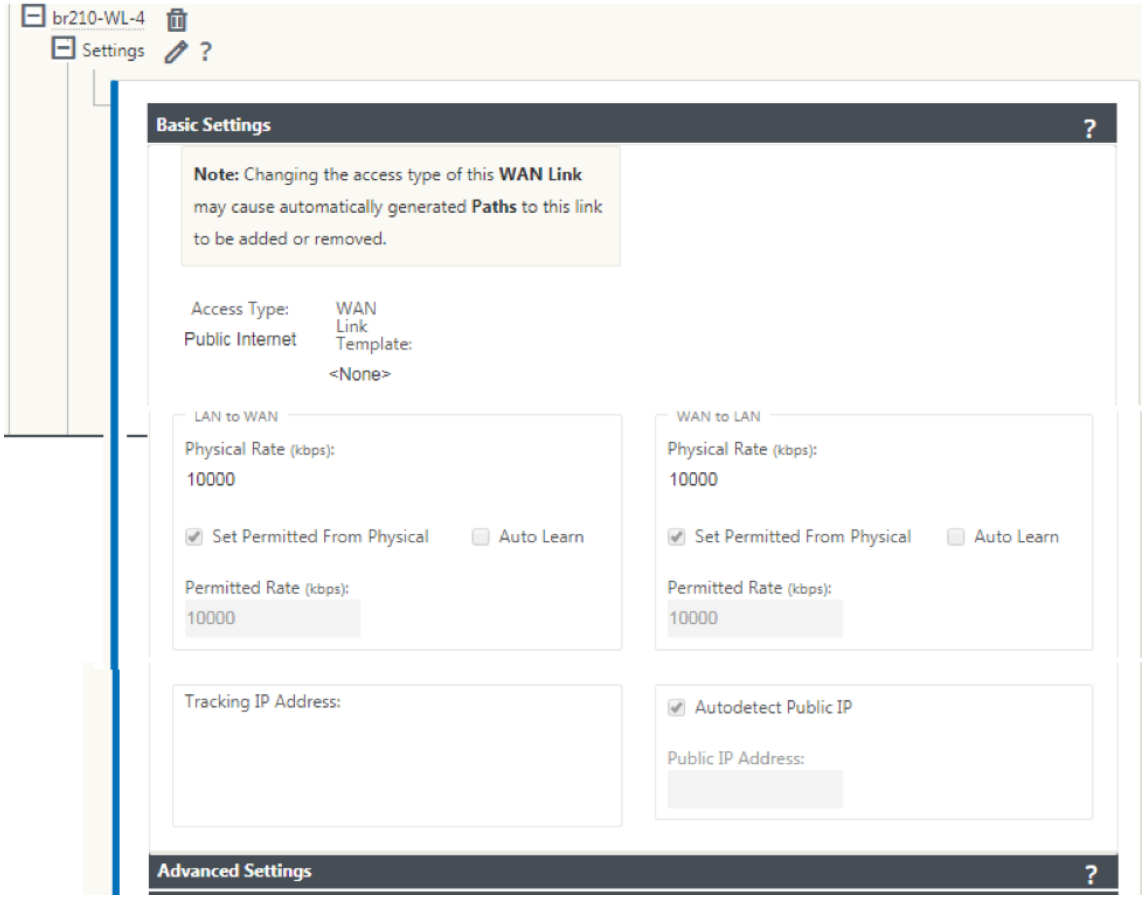
1. Wechseln Sie in der Benutzeroberfläche der SD-WAN-Appliance zum Konfigurationseditor. Siehe Zweig konfigurieren.

   - 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)

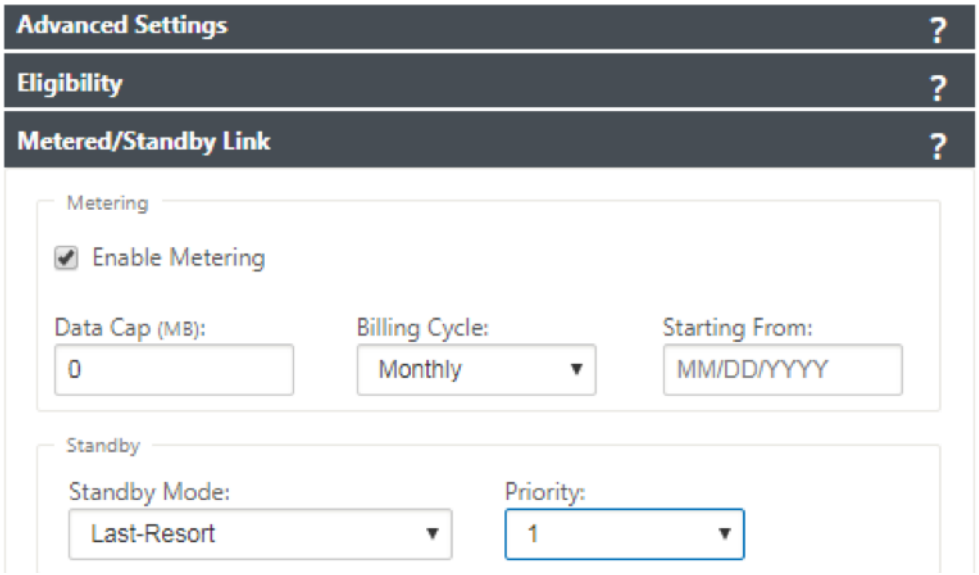


2. Aktivieren Sie die **AutoDetect Public IP** für WAN-Verbindungskonfiguration, wenn Sie die WAN-Verbindung mithilfe der für die LTE-Schnittstelle erstellten virtuellen Schnittstelle

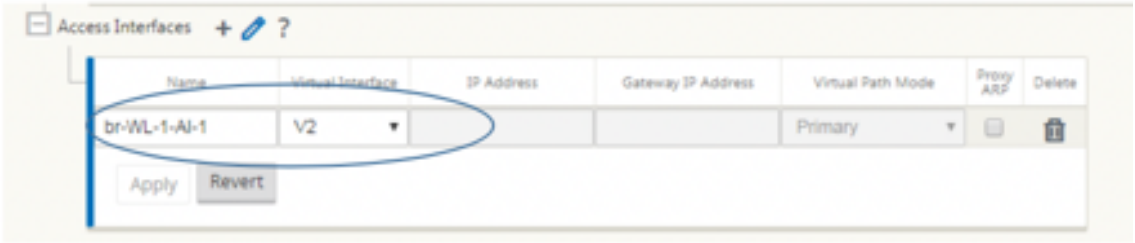
konfigurieren.



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.



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.

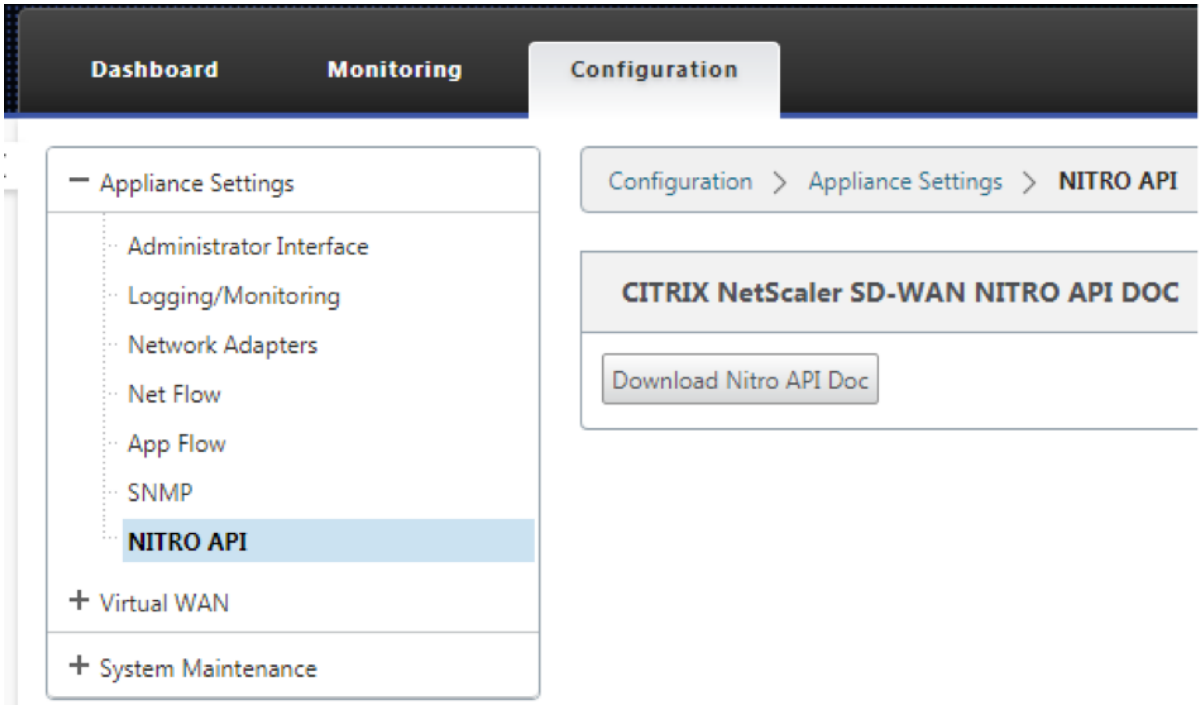
Weitere Informationen zur Bereitstellung und Konfiguration der 210-SE LTE-Appliance mit SD-WAN Center finden Sie im Zero-Touch-Bereitstellungsverfahren.

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**.

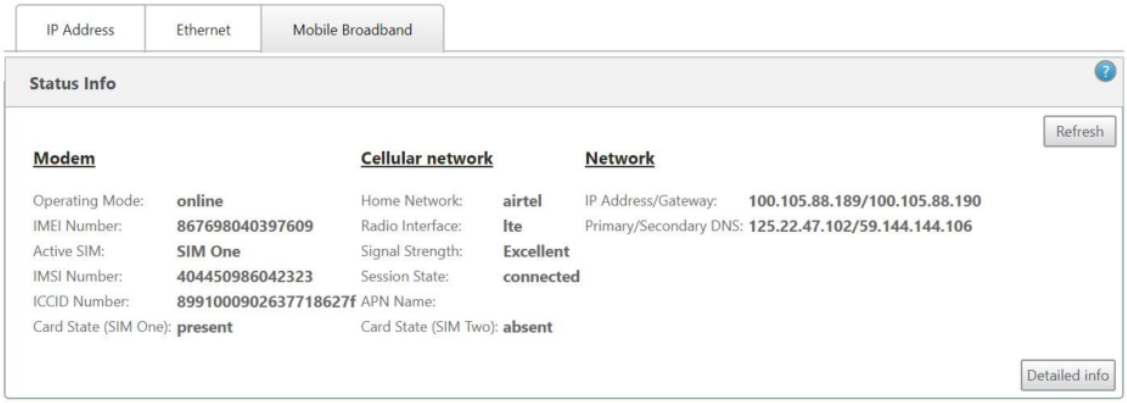
   > **Hinweis**
   >
   > Rufen Sie die APN-Informationen vom Mobilfunkanbieter ab.

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.



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.

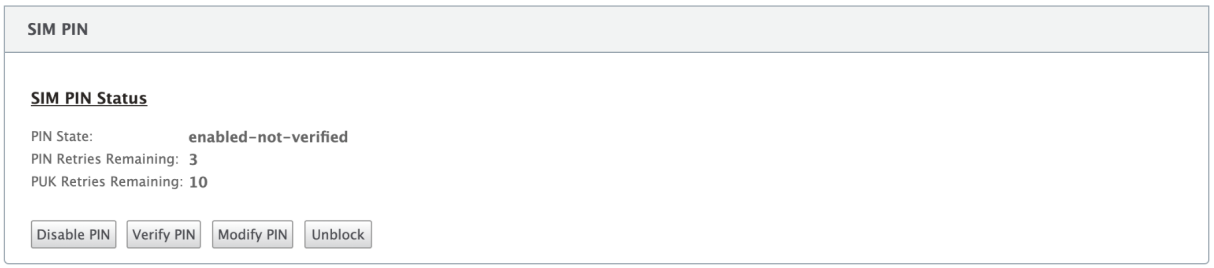
- **SIM Two bevorzugt**: Wenn zwei SIMs eingelegt sind, verwendet das LTE-Modem beim Hochfahren SIM Two, falls verfügbar. Wenn das LTE-Modem eingeschaltet ist und läuft, verwendet es die SIM (SIM One oder SIM Two), die in diesem Moment verwendet werden kann. Es wird weiterhin verwendet, bis die SIM aktiv 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.

SIM-PIN

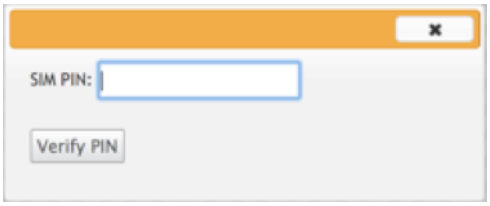
Wenn Sie eine SIM-Karte eingelegt haben, die mit einer PIN gesperrt ist, ist der SIM-Status **aktiviert und nicht überprüft**. Sie können die SIM-Karte erst verwenden, wenn sie mit der SIM-PIN verifiziert wurde. Sie können die SIM-PIN vom Anbieter erhalten.

> **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**.



Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.

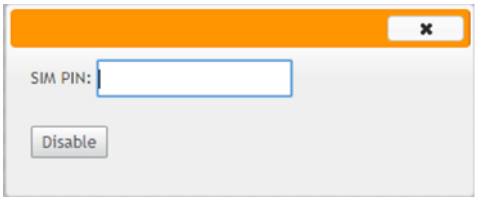


Der Status ändert sich in “**Aktiviert-verified**”.

SIM-PIN deaktivieren

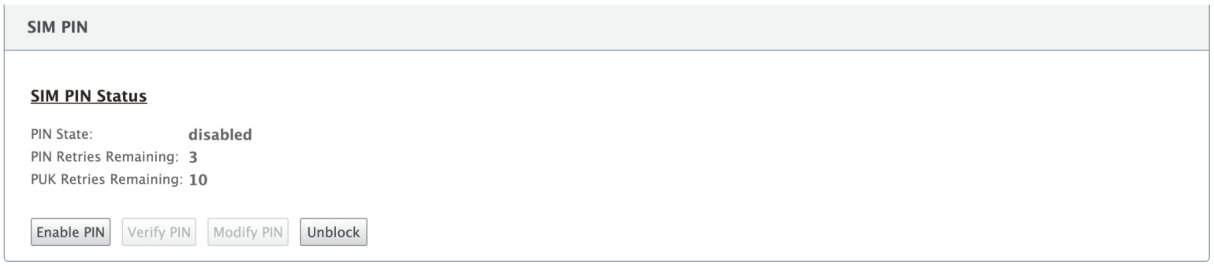
Sie können die SIM-PIN-Funktionalität für eine SIM-Karte deaktivieren, für die SIM-PIN aktiviert und verifiziert ist.

Klicken Sie auf **PIN deaktivieren**. Gib die **SIM-PIN** ein und klicke auf **Deaktivieren**

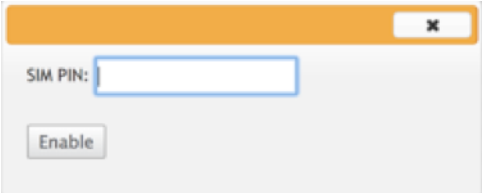


SIM-PIN aktivieren

Die SIM-PIN kann für die SIM aktiviert werden, für die sie deaktiviert ist.

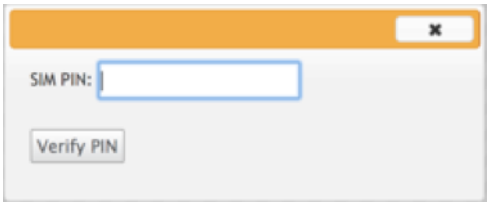


Klicken Sie auf **PIN aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**.



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.

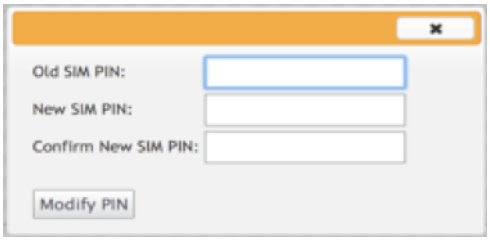
Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.



SIM-PIN ändern

Sobald sich die PIN im Status "**Aktiviert**" befindet, können Sie die PIN ändern.

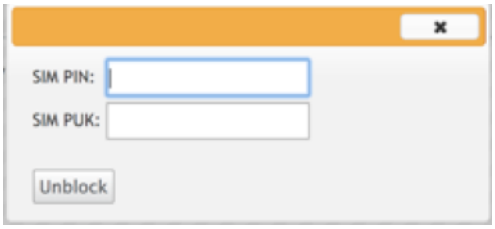
Klicken Sie auf **PIN ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **PIN ändern**.



SIM aufheben

Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe der vom Träger erhaltenen SIM-PUK zurücksetzen.

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**.



> **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.

Netzwerkeinstellungen

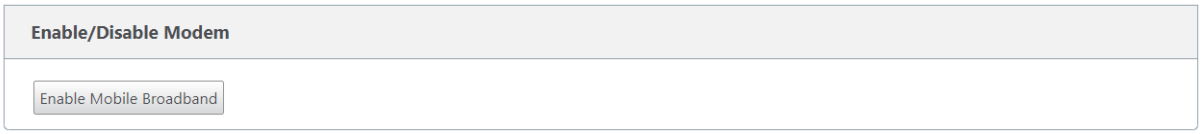
Sie können das Mobilfunknetz auf den Citrix SD-WAN Appliances auswählen, die internes LTE-Modem unterstützen. Die unterstützten Netzwerke sind 3G, 4G oder beides.

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.

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

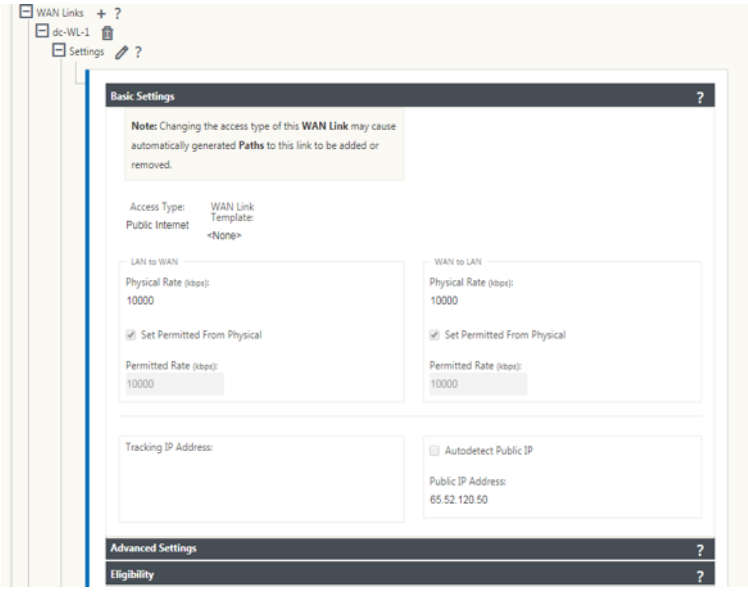
> **Hinweis**
>
> Die Firmware-Vorgänge werden von der 110-LTE-WiFi-Appliance nicht unterstützt.

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.

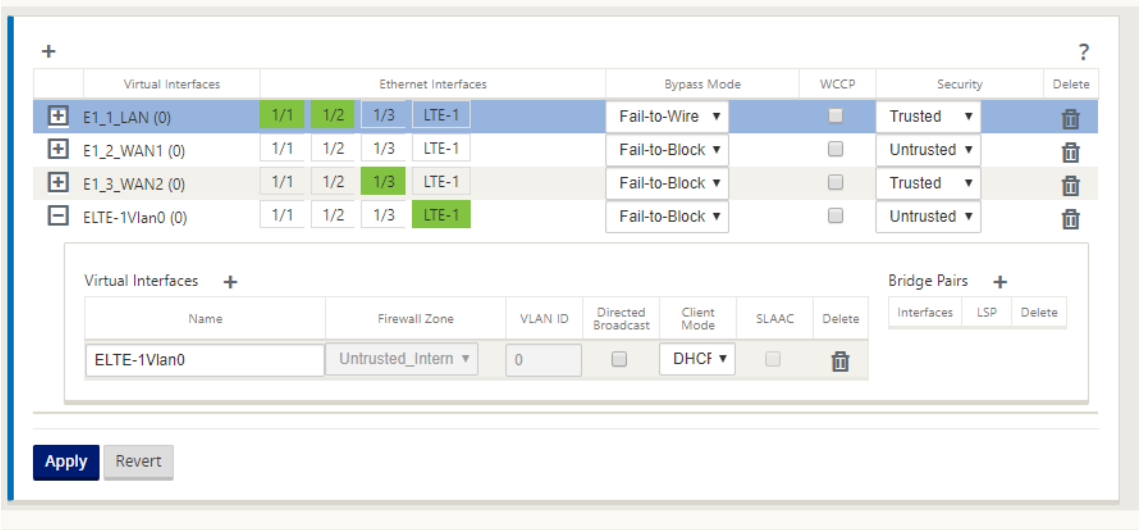


Zweig für LTE konfigurieren

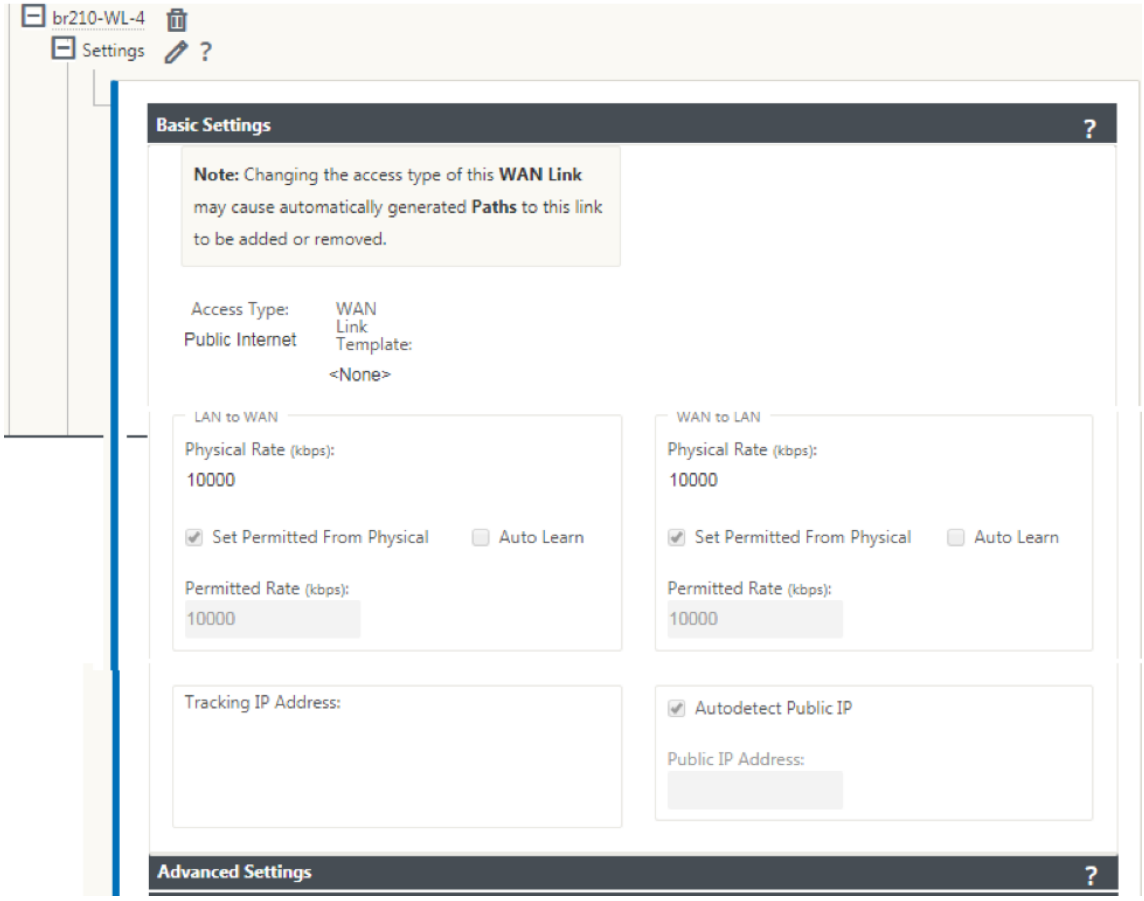
So konfigurieren Sie die 110-LTE-WiFi-Einheit als Zweigstandort:

1. Wechseln Sie in der Benutzeroberfläche der SD-WAN-Appliance zum Konfigurationseditor. Siehe Zweig konfigurieren.

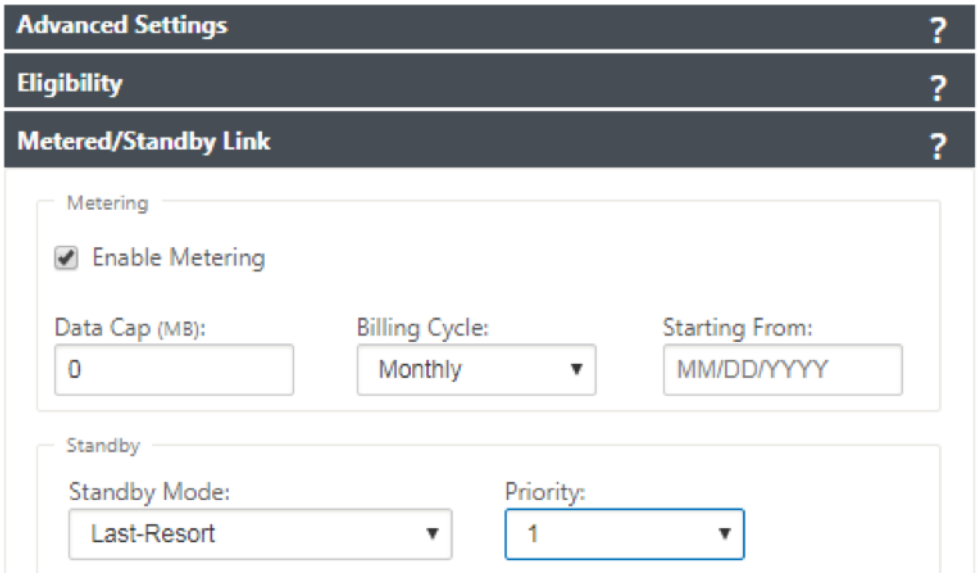
   - Erstellen Sie Schnittstellengruppen.
   - Erstellen Sie bis zu eine virtuelle Schnittstelle und eine Schnittstellengruppe für den LTE-Adapter, um die WAN-Verbindung zu konfigurieren, indem Sie Folgendes auswählen:
     - Ethernet-Schnittstelle —LTE 1
     - Sicherheit —nicht vertrauenswürdig (Standard)
     - DHCP-Client —Aktiviert (Standard)



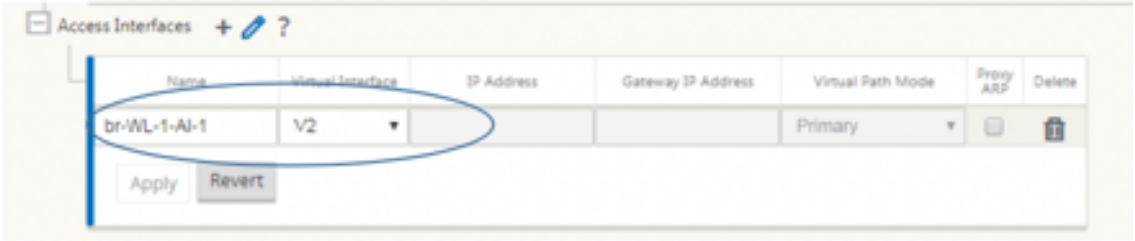
2. Aktivieren Sie die **AutoDetect Public IP** für WAN-Verbindungskonfiguration, wenn Sie die WAN-Verbindung mithilfe der für die LTE-Schnittstelle erstellten virtuellen Schnittstelle konfigurieren.



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.



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. Vervollständigen Sie den Rest der erforderlichen Branch-Konfiguration für die 110-LTE-WiFi-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

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:

1. Installieren Sie die Antenne, schalten Sie das Gerät ein und legen Sie die SIM-Karte ein.
2. 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.

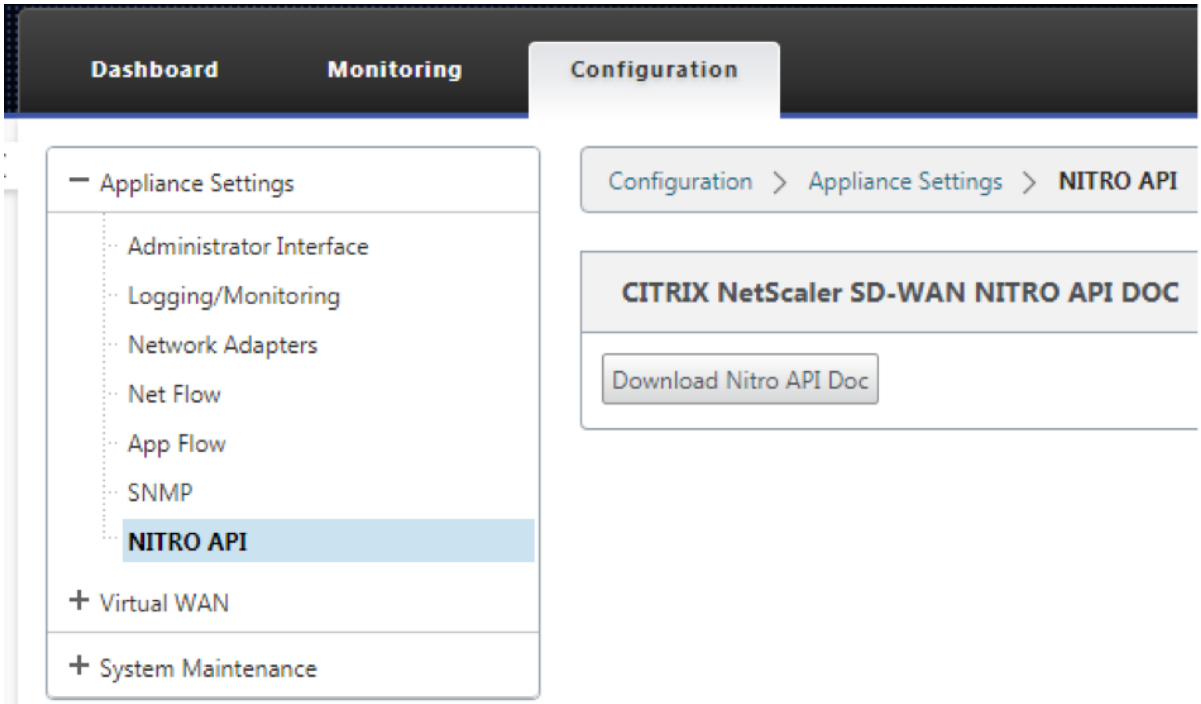
Weitere Informationen zum Bereitstellen und Konfigurieren von 110-LTE-WiFi-Appliance mit SD-WAN Center finden Sie im Zero-Touch-Bereitstellungsverfahren.

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 / AE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 Wi-Fi SE
- Citrix SD-WAN 110 LTE Wi-Fi SE
- Citrix SD-WAN 1100 SE / PE / AE
- Citrix SD-WAN 2100 SE / PE

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 und das Aktivieren/Deaktivieren des Modems auf MBIM- und NCM-USB-Modems konfigurieren. Mobile Breitbandvorgänge werden auf CDC Ethernet USB-Modems nicht unterstützt.

Anschließen des USB-Modems

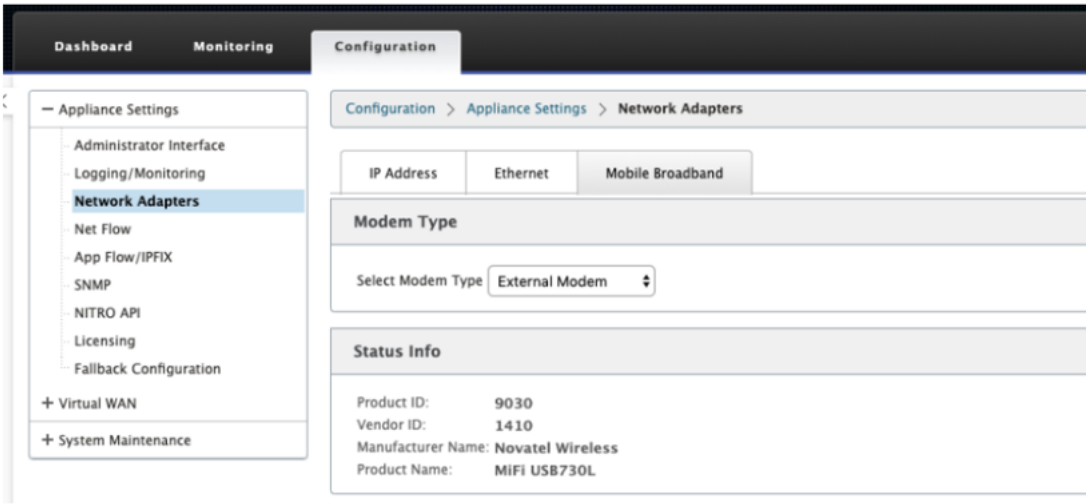
Aktivieren und testen Sie das USB-Modem gemäß den Richtlinien Ihres Mobilfunkanbieters.

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 Modellnummer des LTE USB-Dongle wird im Abschnitt "**Statusinformationen** "nicht angezeigt.

Mobiler Breitbandbetrieb

Vorgänge, die von externen CDC-Ethernet- und MBIM-/NCM-Modems unterstützt werden:

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

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 -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. Der Kunde kontrolliert das Update der Modem-Firmware. 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

August 29, 2022

Im Folgenden sind einige der Anwendungsfallszenarien aufgeführt, 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
- Statische WAN-Pfade
- 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 einer einzelnen Region
- Bereitstellung mit mehreren Regionen
- Hohe Verfügbarkeit

Checkliste und Bereitstellung

October 28, 2021

Es wird dringend empfohlen, vor Beginn der Installation zuerst das Citrix Virtual WAN Deployment Planning Guide durchzulesen. In diesem Artikel werden die wesentlichen Konzepte und Funktionen von Virtual WAN erläutert und Richtlinien für die Planung Ihrer 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.

Informationen zum Anzeigen einiger Anwendungsfälle für die Bereitstellung finden Sie unter Bereitstellungen.

1. Sammeln Sie Ihre Citrix SD-WAN-Bereitstellungsinformationen.
2. Richten Sie die Citrix SD-WAN Appliances ein.
    - Für jede Hardware-Appliance, die Sie zu 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) Stellen Sie das **Timeout-Intervall** der Konsolensitzung auf einen hohen oder maximalen Wert ein.
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 auszubringende Appliance:
  - Management-IP-Adresse
  - Virtuelle IP-Adressen
  - Sitename
  - Gerätename (einer pro Standort)
  - SD-WAN Appliance-Modell (für jede einzusetzende Appliance)
  - Bereitstellungsmodus (MCN oder Client)
  - Topologie
  - Gateway-MPLS
  - Informationen zum GRE-Tunnel
  - 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 Verkehrsblackhole 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 Netzwerkknoten 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).

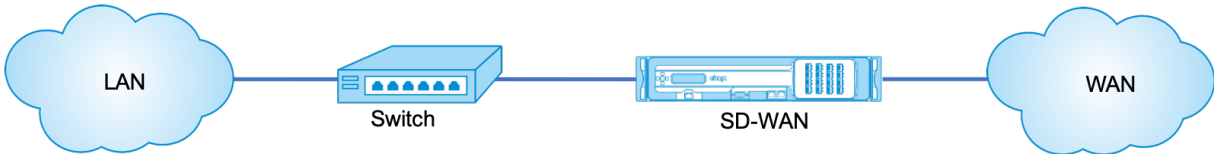
- Richtige Entwurfsüberlegungen sind zu berücksichtigen, um zu wissen, ob der gesamte Datenverkehr über SD-WAN oder nur bestimmten Datenverkehr umgeleitet wird.
- Das bedeutet, dass SD-WAN einen Teil der Bandbreite ausschließlich für sich selbst dediziert sein muss, der auf den Schnittstellen so eingestellt 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

October 28, 2021

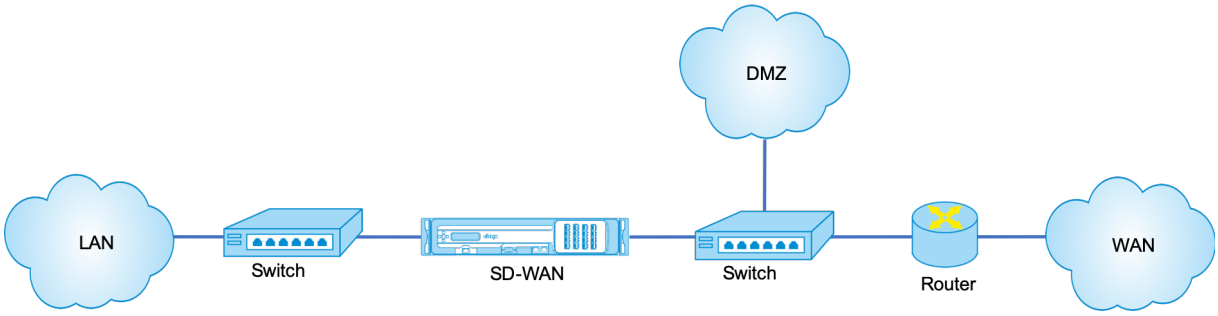
Gateway -Modus platziert die SD-WAN-Appliance physisch in den Pfad (Zwei-Arm-Bereitstellung) und erfordert Änderungen in der vorhandenen Netzwerkinfrastruktur, damit die SD-WAN-Appliance zum Standard-Gateway für das gesamte LAN-Netzwerk für diesen Standort wird. Gateway-Modus für neue Netzwerke und Routerersatz. 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-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. Inline-Modus für die Integration in bereits definierte Netzwerke.

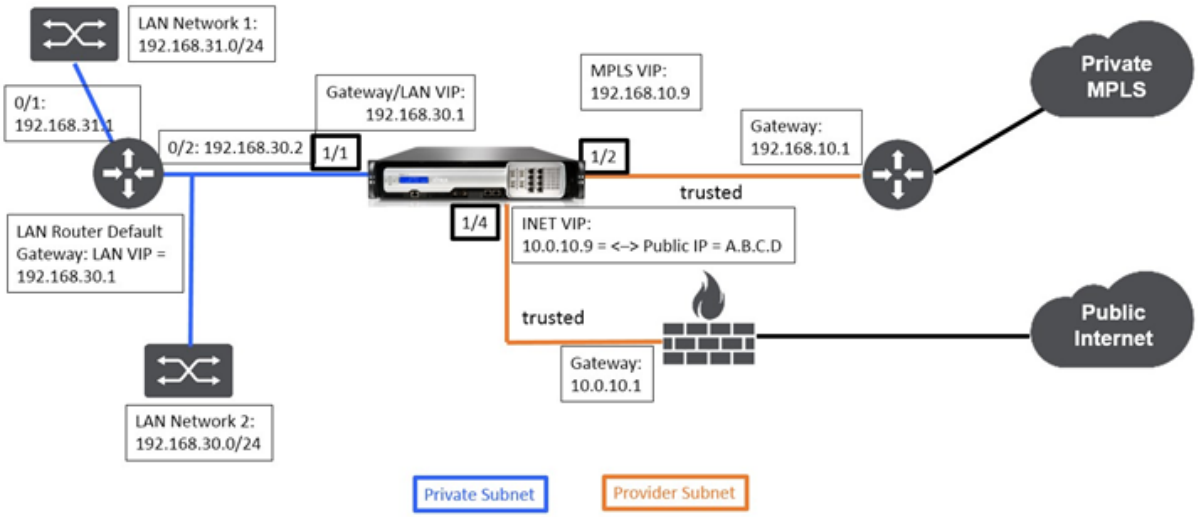


Dieser Artikel enthält schrittweise Verfahren zum Konfigurieren einer SD-WAN-Appliance im Gateway-Modus in einem Beispielnetzwerk-Setup. Die Inline-Bereitstellung wird auch für die Zweigseite beschrieben, um die Konfiguration abzuschließen. Ein Netzwerk kann weiterhin funktionieren, wenn ein Inline-Gerät entfernt wird, verliert jedoch jeglichen Zugriff, wenn das Gateway-Gerät entfernt wird.

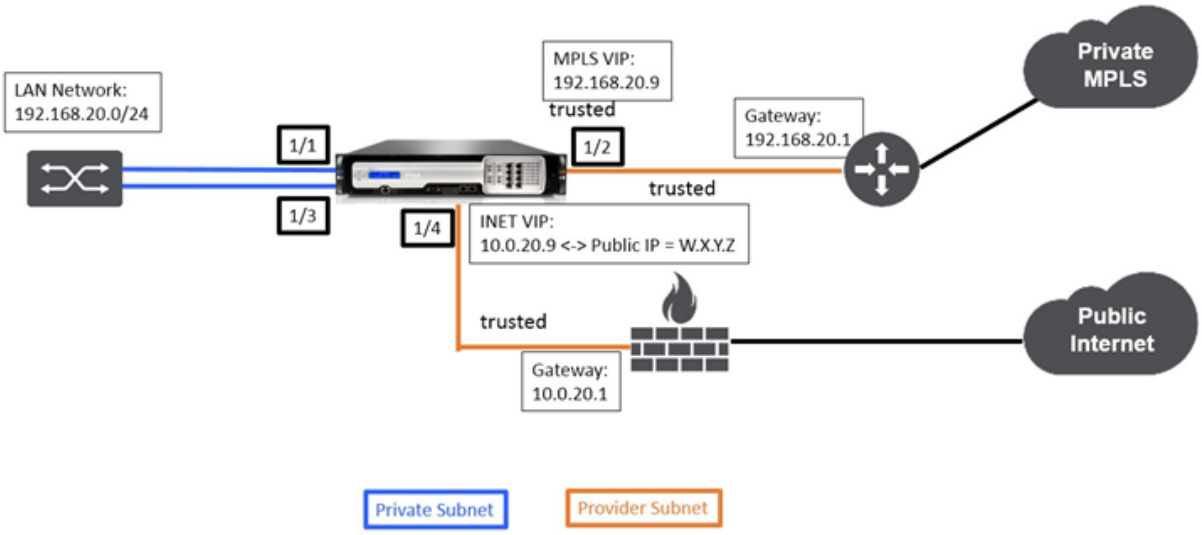
Topologie

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

Die Bereitstellungsanforderungen und zugehörige Informationen werden nachstehend beschrieben, um Sie beim Erstellen der Konfiguration zu unterstützen.

Sitename	Rechenzentrums-Standort	Niederlassungsstandort
Appliance-Name	A_DC1	A_BR1
Management-IP	172.30.2.10/24	172.30.2.20/24
Sicherheits-Schlüssel	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 (öffentliche IP —A.B.C.D), 192.168.30.1/24 - LAN	192.168.20.9/24 - MPLS, 10.0.20.9/24 —Internet (öffentliche 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-Webverwaltungsoberfläche zu **Konfiguration** > **Appliance-Einstellungen** > **Administratorschnittstelle** > **Registerkarte Verschiedenes** > **Switch-Konsole**.

> **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** > **Konfigurationseditor** navigieren. Klicken Sie auf **Neu**, um mit der Konfiguration zu beginnen.

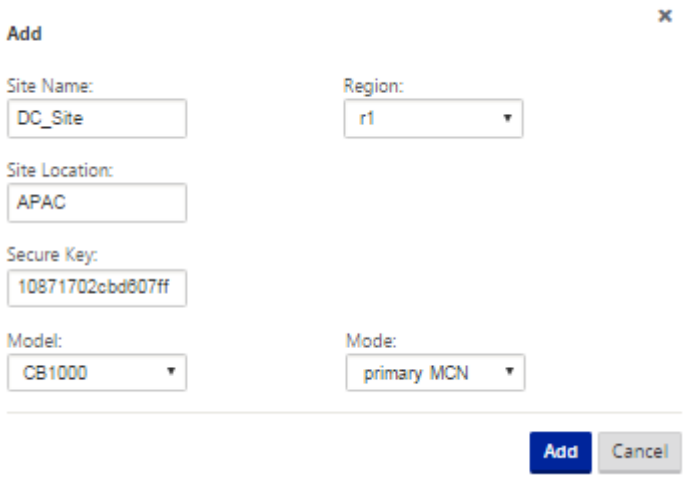
Konfiguration des Sitegatewaymodus für Rechenzentren

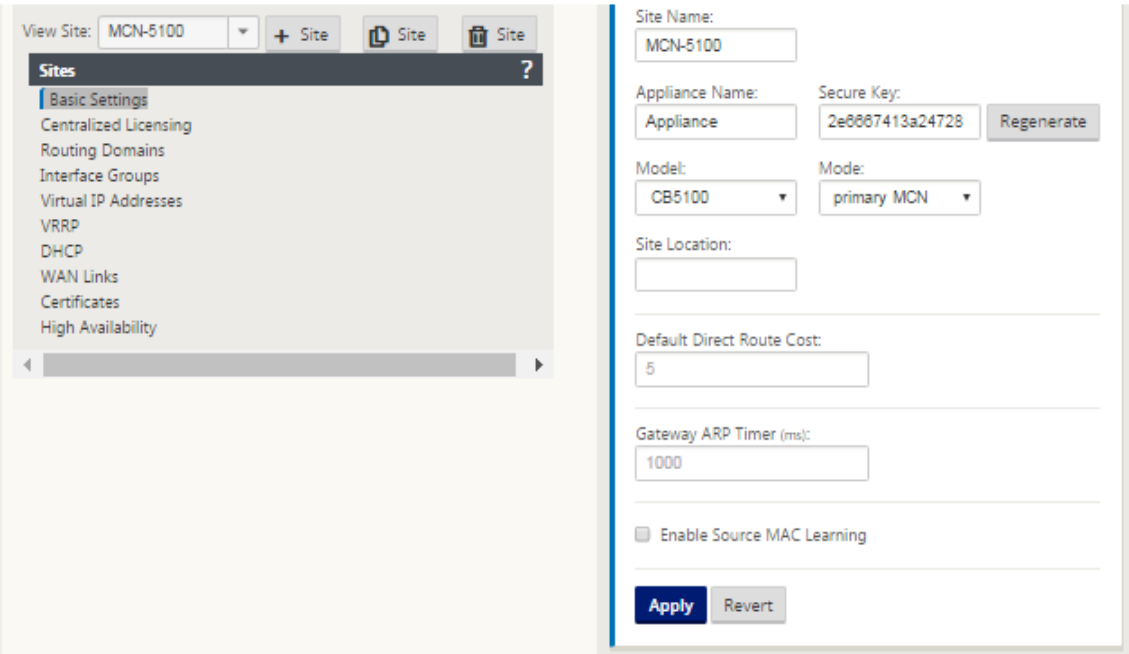
Im Folgenden werden die Konfigurationsschritte auf hoher Ebene zum Konfigurieren der Gateway-Bereitstellung des Rechenzentrums beschrieben:

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

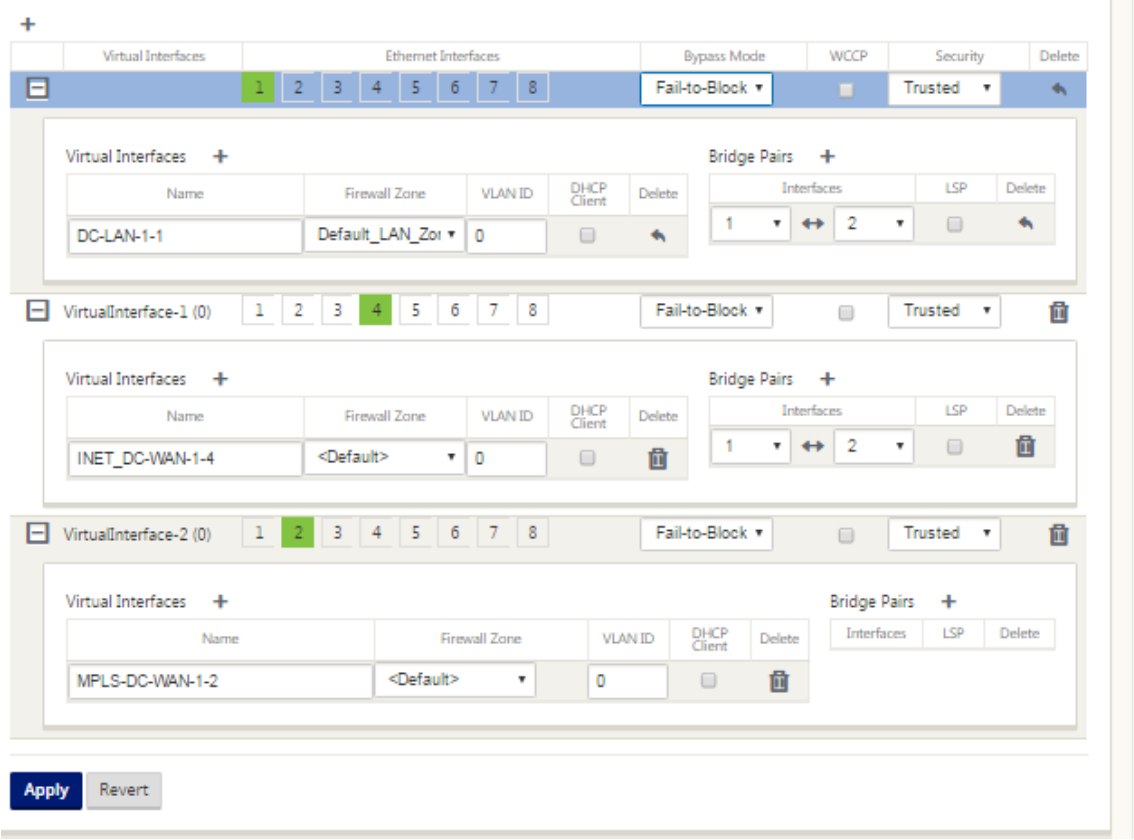
1. Navigieren Sie zu **Konfigurationseditor** > **Sites**und klicken Sie auf die Schaltfläche **+ Hinzufügen**.
2. Füllen Sie die Felder wie unten gezeigt.
3. Behalten Sie die Standardeinstellungen bei, wenn Sie nicht dazu aufgefordert werden.





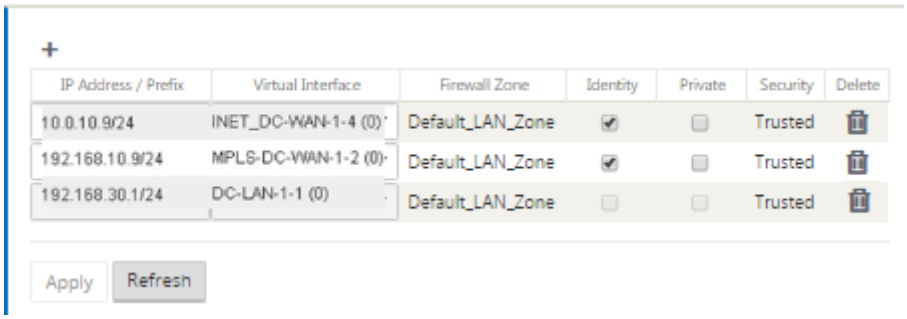
So konfigurieren Sie Schnittstellengruppen basierend auf verbundenen Ethernet-Schnittstellen

1. Navigieren Sie im **Konfigurationseditor**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.



So erstellen Sie VIP-Adresse (Virtual IP) für jede virtuelle Schnittstelle

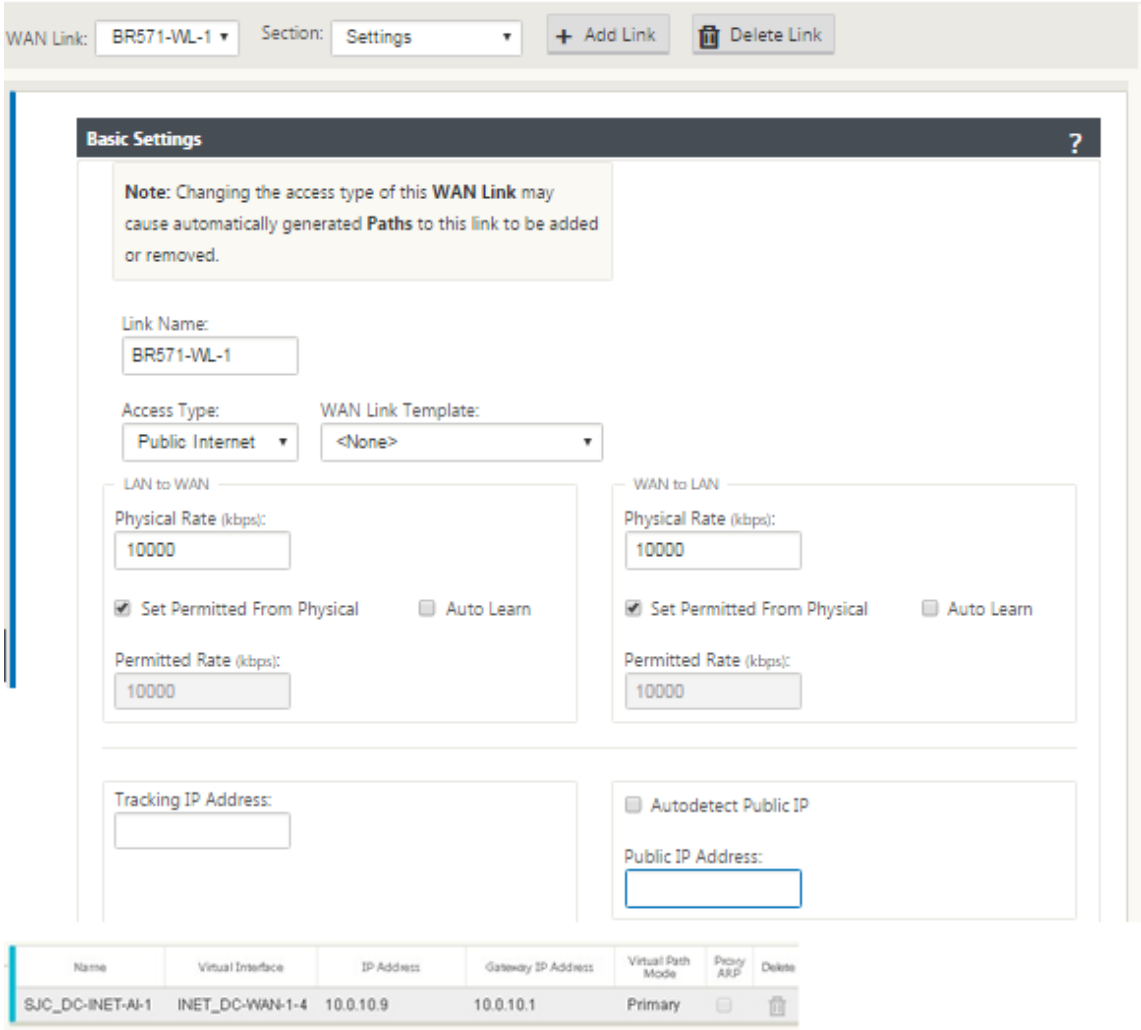
1. Erstellen Sie für jeden WAN-Link im entsprechenden Subnetz eine VIP. VIPs werden für die Kommunikation zwischen zwei SD-WAN-Appliances in der virtuellen WAN-Umgebung verwendet.
2. Erstellen Sie eine virtuelle IP-Adresse, die als Gateway-Adresse für das LAN-Netzwerk verwendet werden soll.



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.

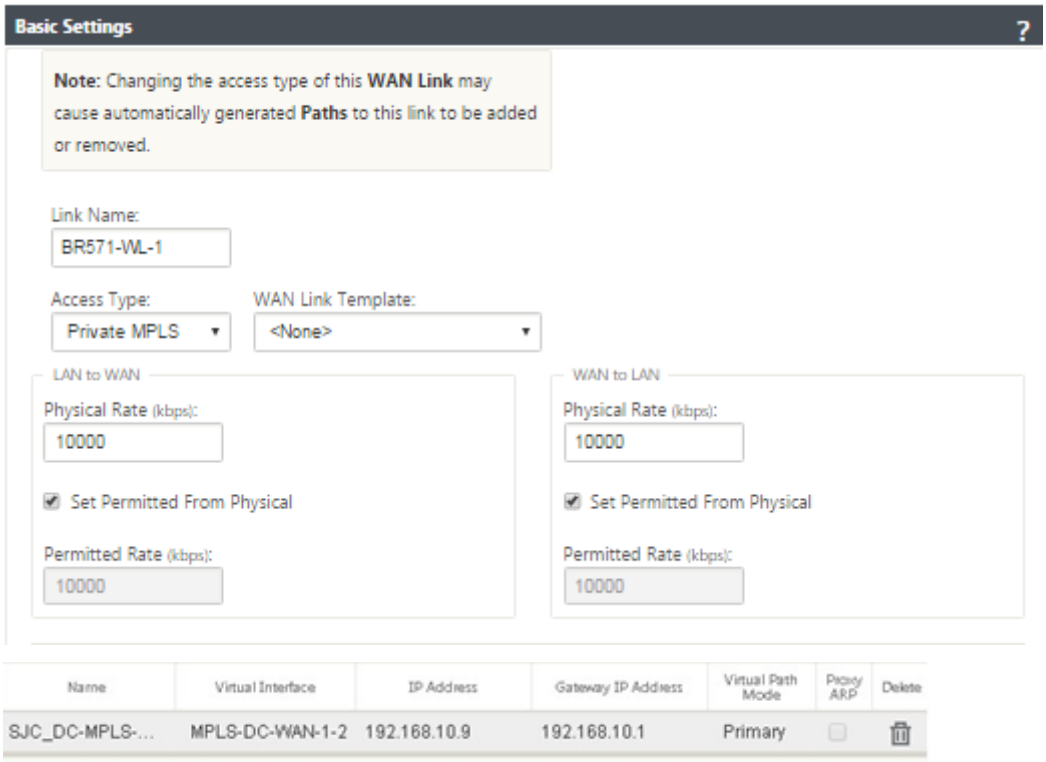
2. Geben Sie Informationen zum Internetlink ein, einschließlich der angegebenen öffentlichen IP-Adresse, wie unten dargestellt. AutoDetect **Public IP** kann nicht für SD-WAN-Appliance ausgewählt werden, die als MCN konfiguriert ist.
3. Navigieren Sie im Dropdownmenü des Abschnitts zu **Access Interfaces**und 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.



So erstellen Sie eine MPLS-Verbindung

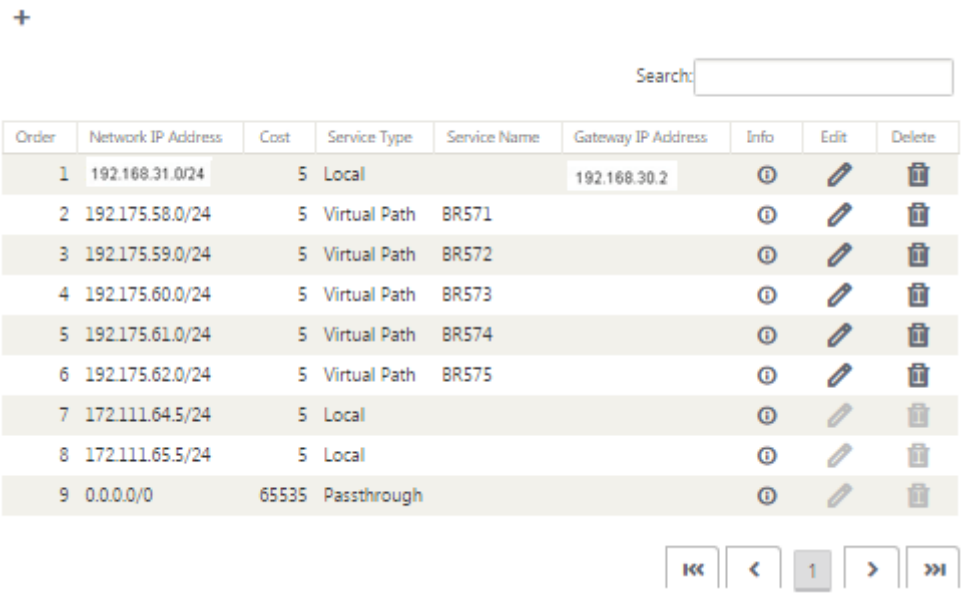
1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+**, um einen WAN-Link für den MPLS-Link hinzuzufügen.
2. Füllen Sie MPLS-Link-Details wie unten gezeigt.

3. Navigieren Sie zu **Access Interfaces**, klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den MPLS-Link hinzuzufügen.
4. Füllen Sie das Access Interface für IP- und Gateway Adressen wie unten dargestellt aus.



So füllen Sie Routen aus

Routen werden basierend auf der obigen Konfiguration automatisch erstellt. Die oben gezeigte DC-LAN-Beispieltopologie hat 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.



Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	192.168.31.0/24	5	Local		192.168.30.2			
2	192.175.58.0/24	5	Virtual Path	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5	Local					
9	0.0.0.0/0	65535	Passthrough					

1

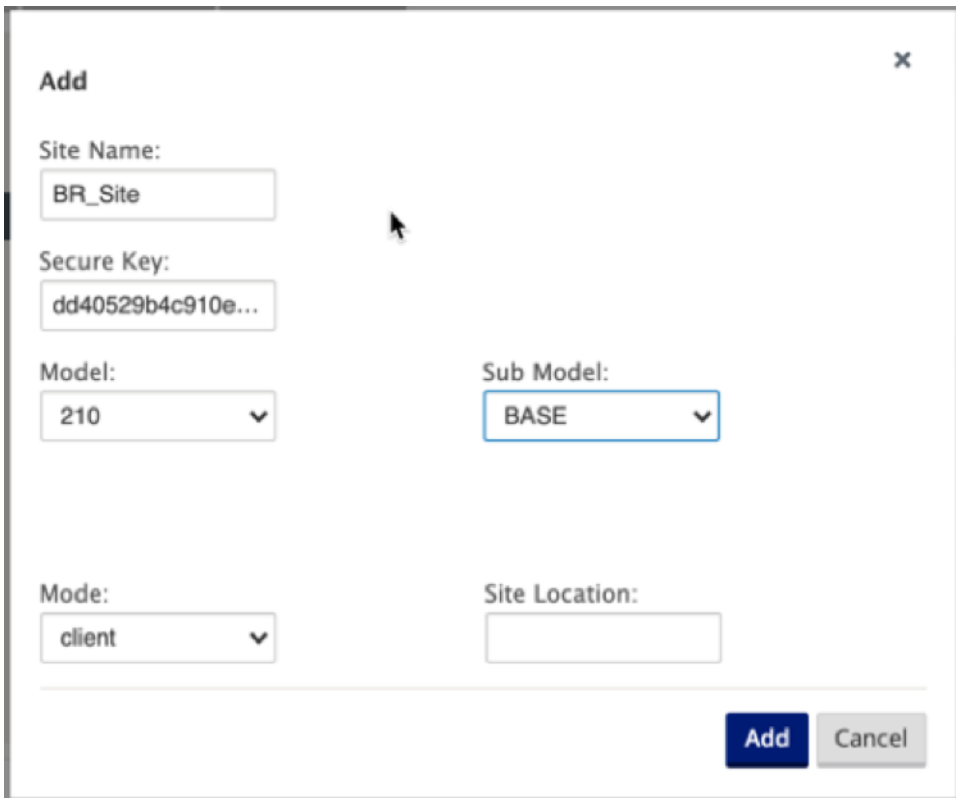
Konfiguration der Inline-Bereitstellung von Zweigstandort

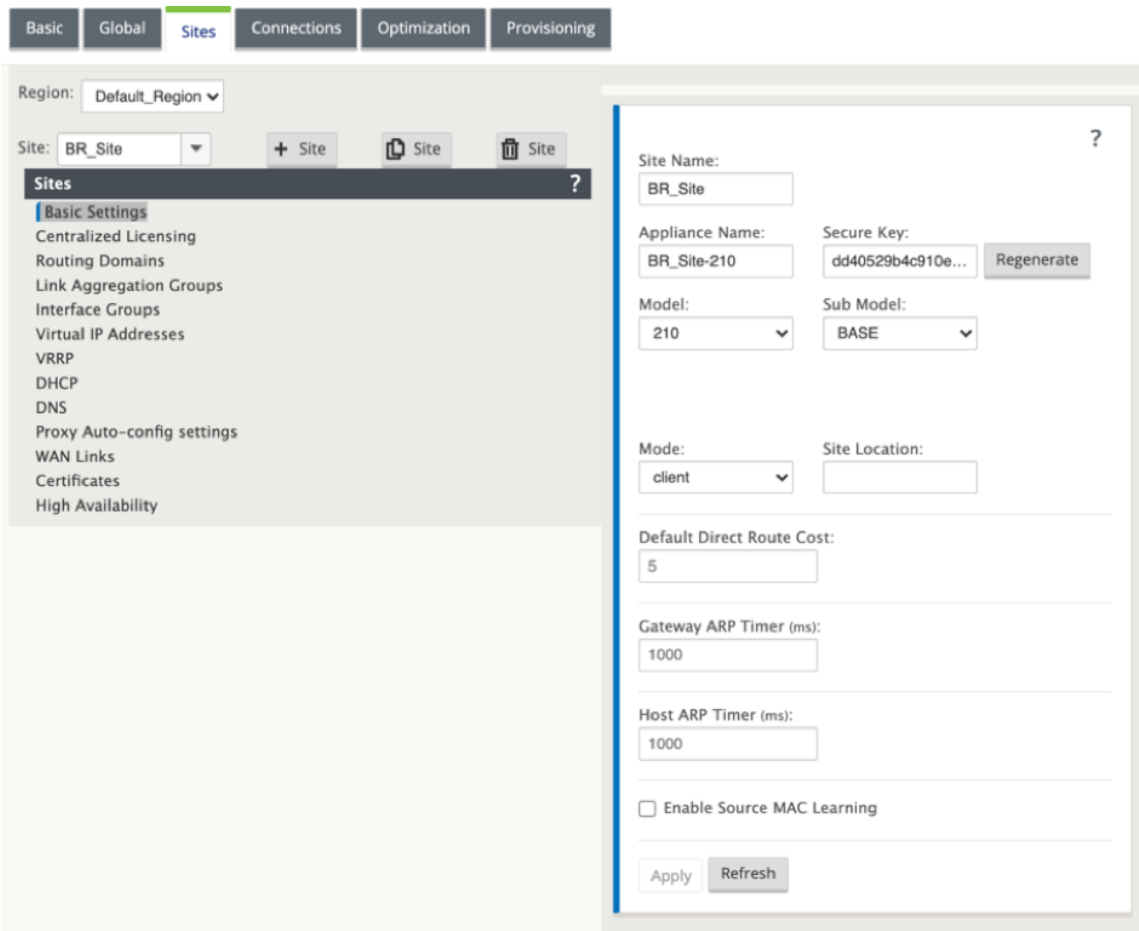
Im Folgenden sind die Konfigurationsschritte auf hoher Ebene zum Konfigurieren des Zweigstandorts für die Inline-Bereitstellung aufgeführt

1. Erstellen Sie eine Zweigsite.
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

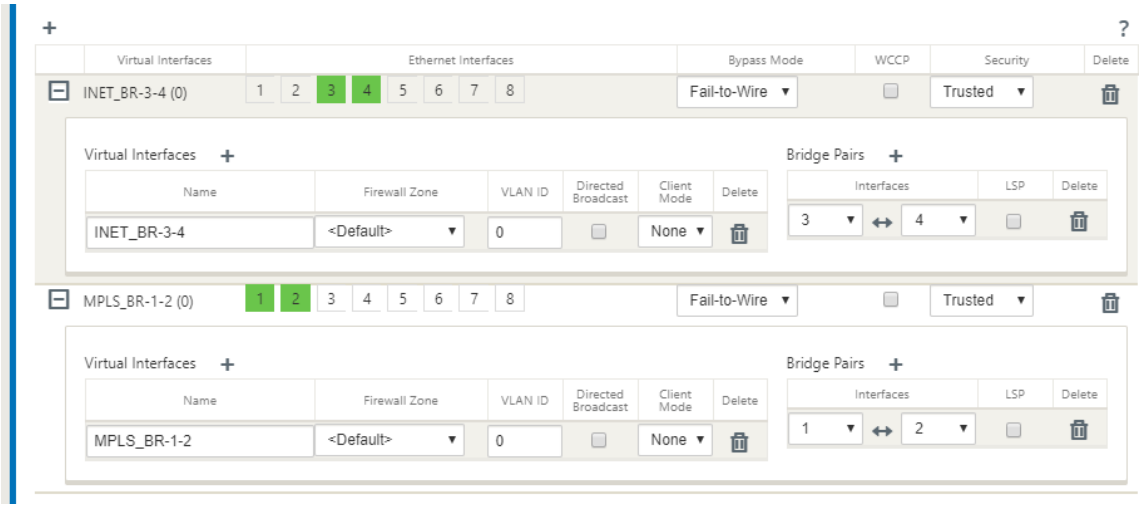
1. Navigieren Sie zu **Konfigurationseditor** > **Sites**und klicken Sie auf die Schaltfläche “**+**” **Hinzufügen**.
2. Füllen Sie die Felder wie unten gezeigt.
3. Behalten Sie die Standardeinstellungen bei, wenn Sie nicht dazu aufgefordert werden.





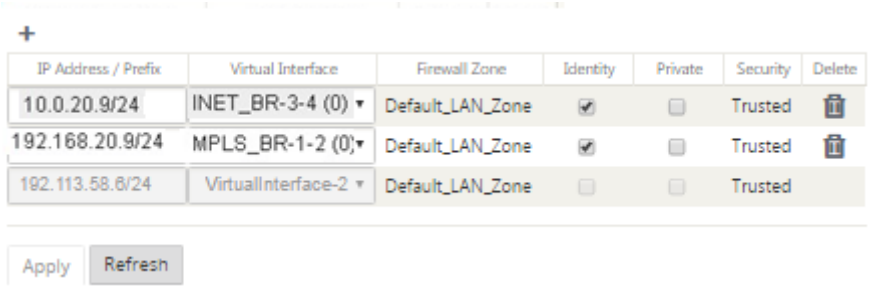
So füllen Sie Schnittstellengruppen basierend auf angeschlossenen Ethernet-Schnittstellen aus

1. Navigieren Sie im **Konfigurationseditor**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.



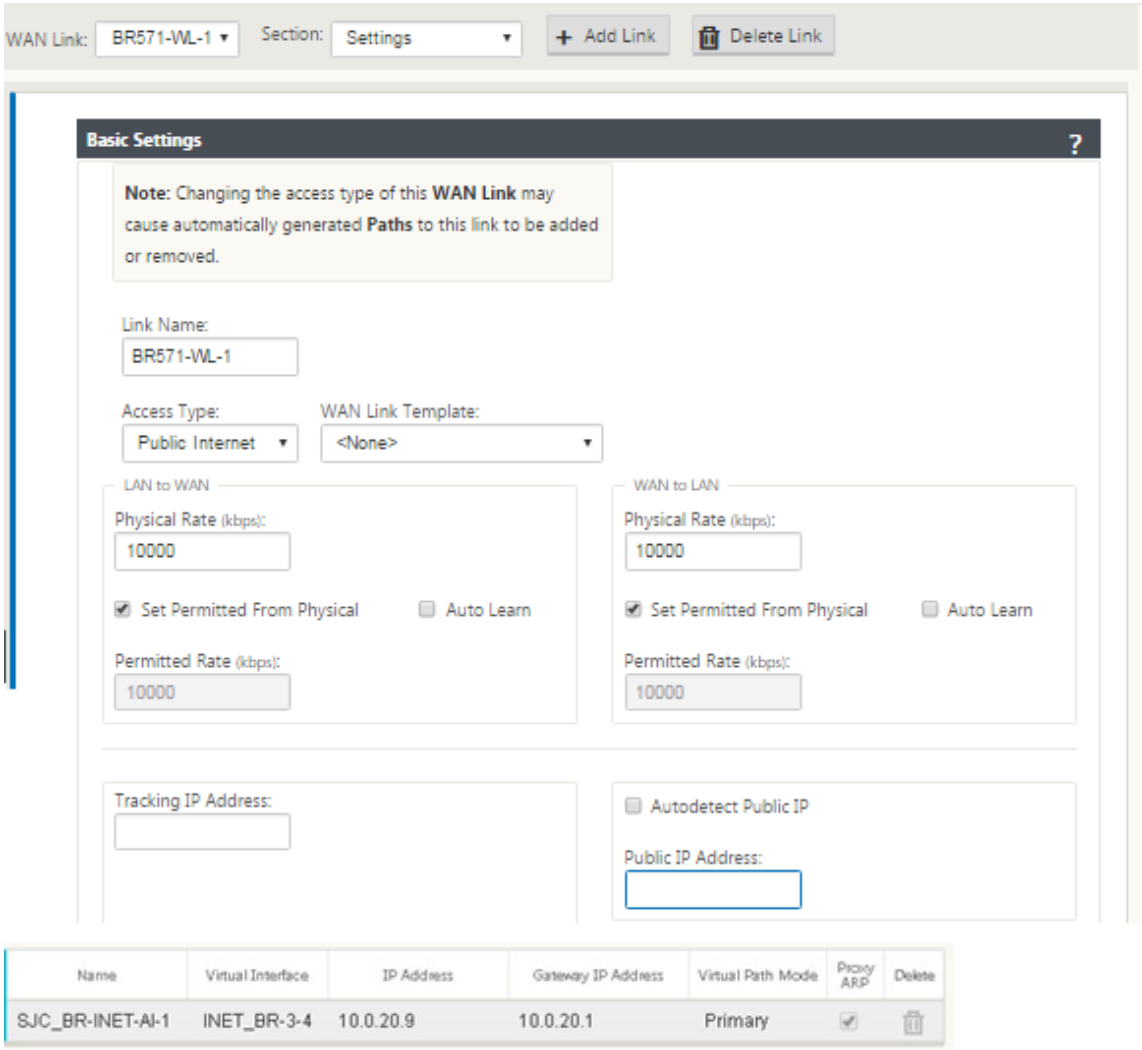
So erstellen Sie VIP-Adresse (Virtual IP) für jede virtuelle Schnittstelle

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.



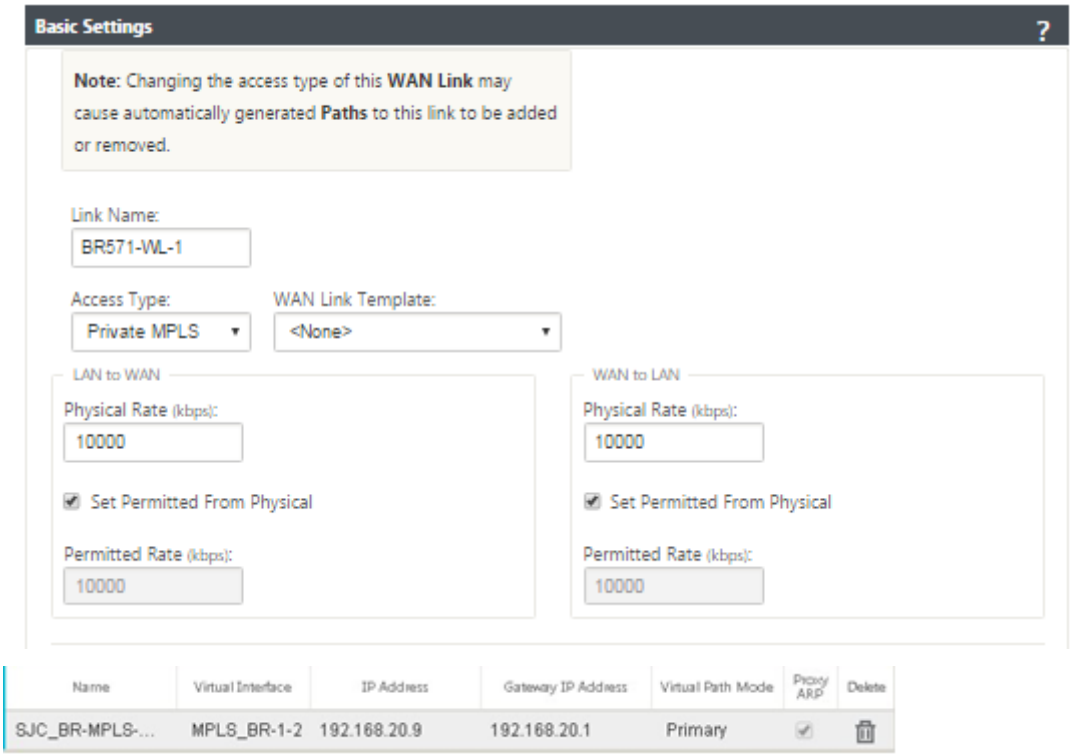
So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten mithilfe des Internetlinks aus:

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.



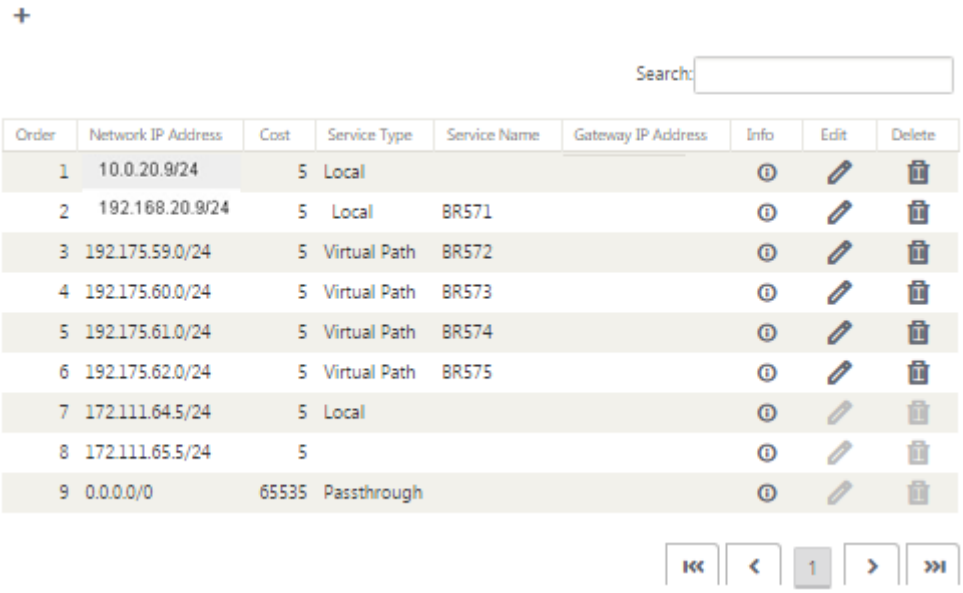
So erstellen Sie MPLS-Verknüpfung

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.



So füllen Sie Routen aus

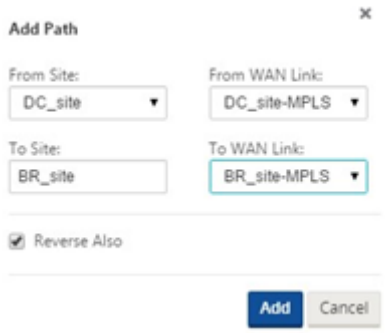
Routen werden automatisch basierend auf der obigen Konfiguration erstellt. Falls es mehr Subnetze für diese Remote-Zweigstelle gibt, müssen bestimmte Routen hinzugefügt werden, die angeben, welches Gateway den Datenverkehr leitet, um diese Back-End-Subnetze zu erreichen.



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.



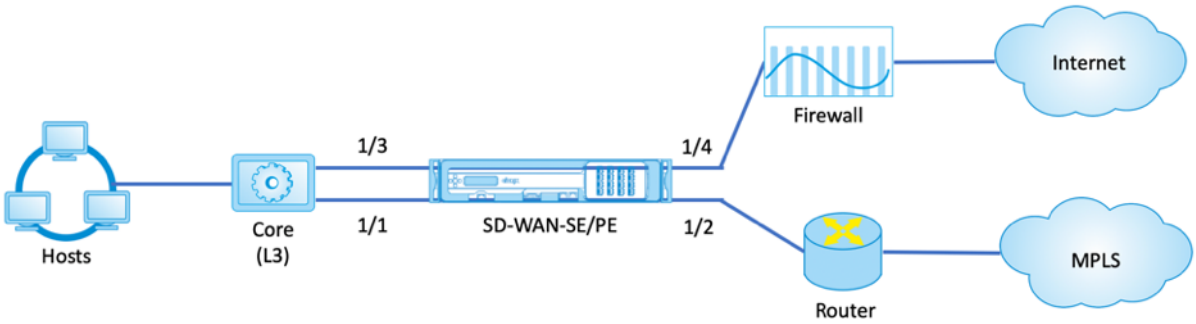
Nachdem Sie alle oben genannten Schritte ausgeführt haben, fahren Sie mit Vorbereiten der SD-WAN-Appliance-Paketefort.

Inlinemodus

October 28, 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.



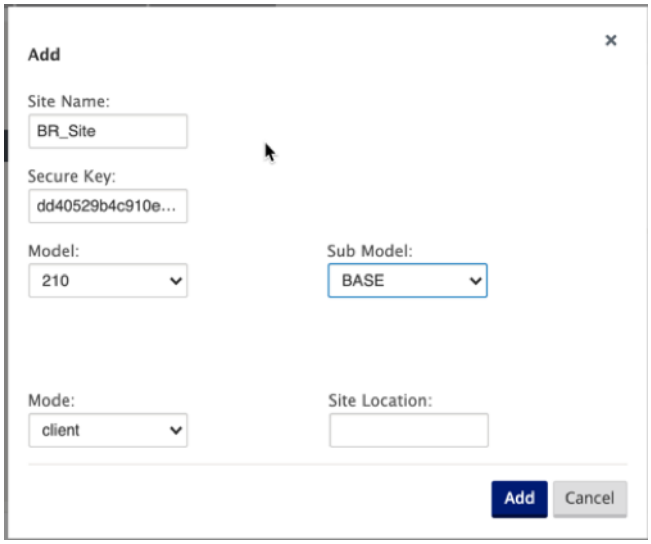
Konfiguration der Inline-Bereitstellung von Zweigstandort

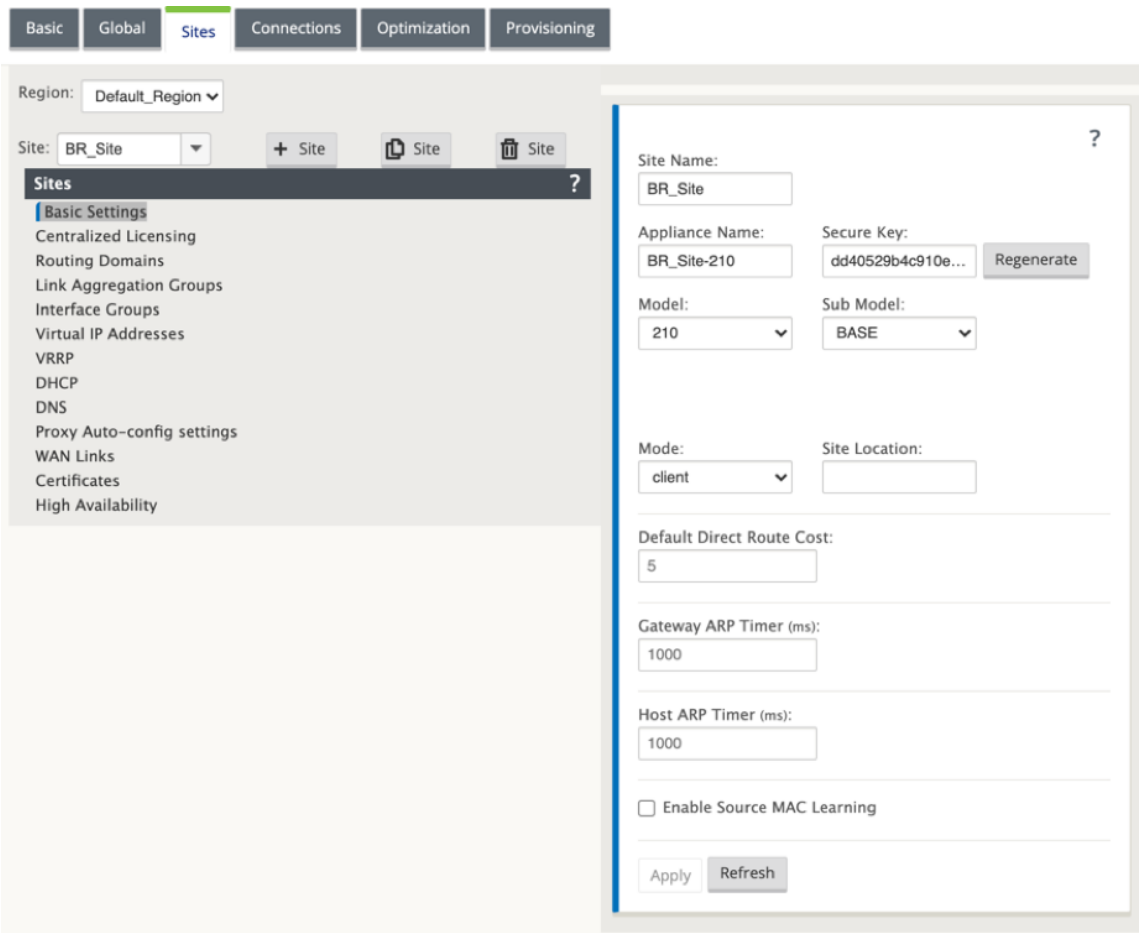
Im Folgenden sind die Konfigurationsschritte auf hoher Ebene zum Konfigurieren des Zweigstandorts für die Inline-Bereitstellung aufgeführt

1. Erstellen Sie eine Zweigsite.
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

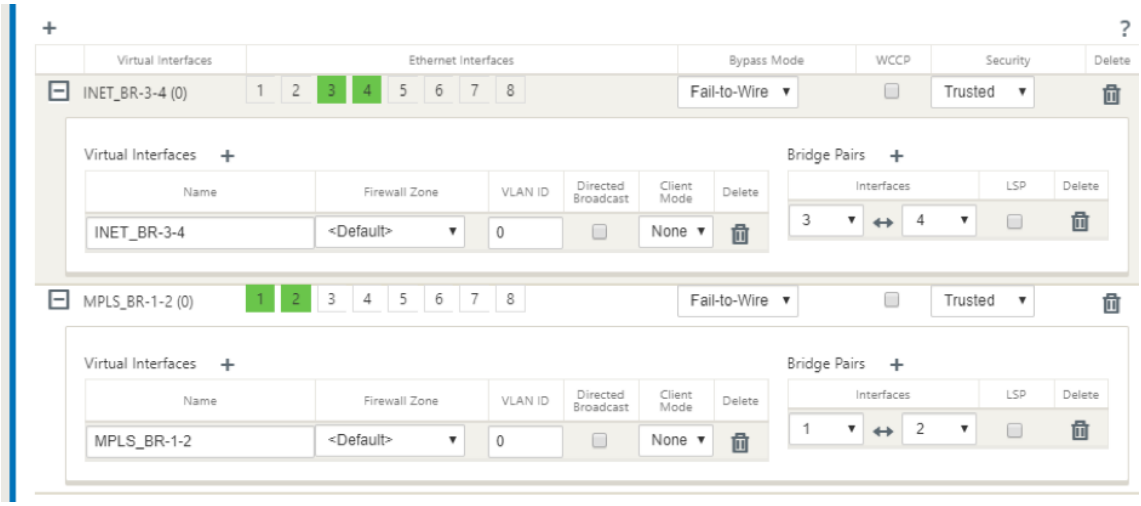
1. Navigieren Sie zu **Konfigurationseditor > Sites** und klicken Sie auf **+ Hinzufügen**.
2. Behalten Sie die Standardeinstellungen bei, wenn Sie nicht dazu aufgefordert werden.





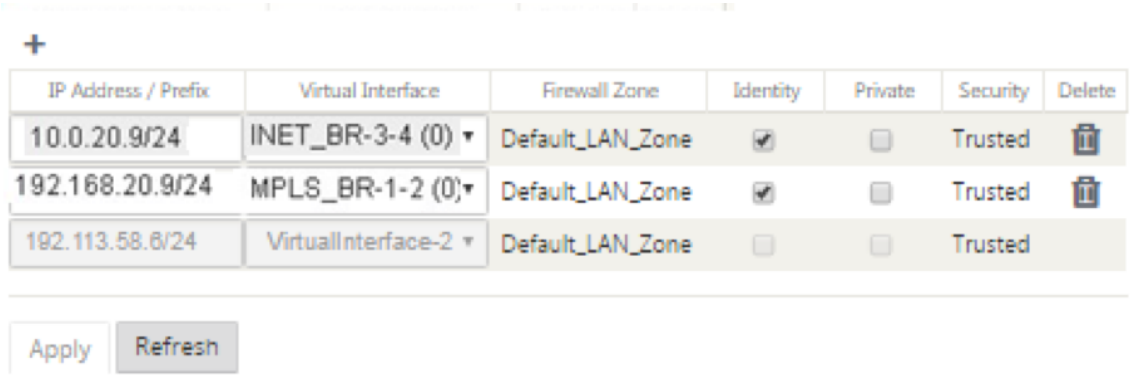
So füllen Sie Schnittstellengruppen basierend auf angeschlossenen Ethernet-Schnittstellen aus

1. Navigieren Sie im Konfigurationseditor 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.



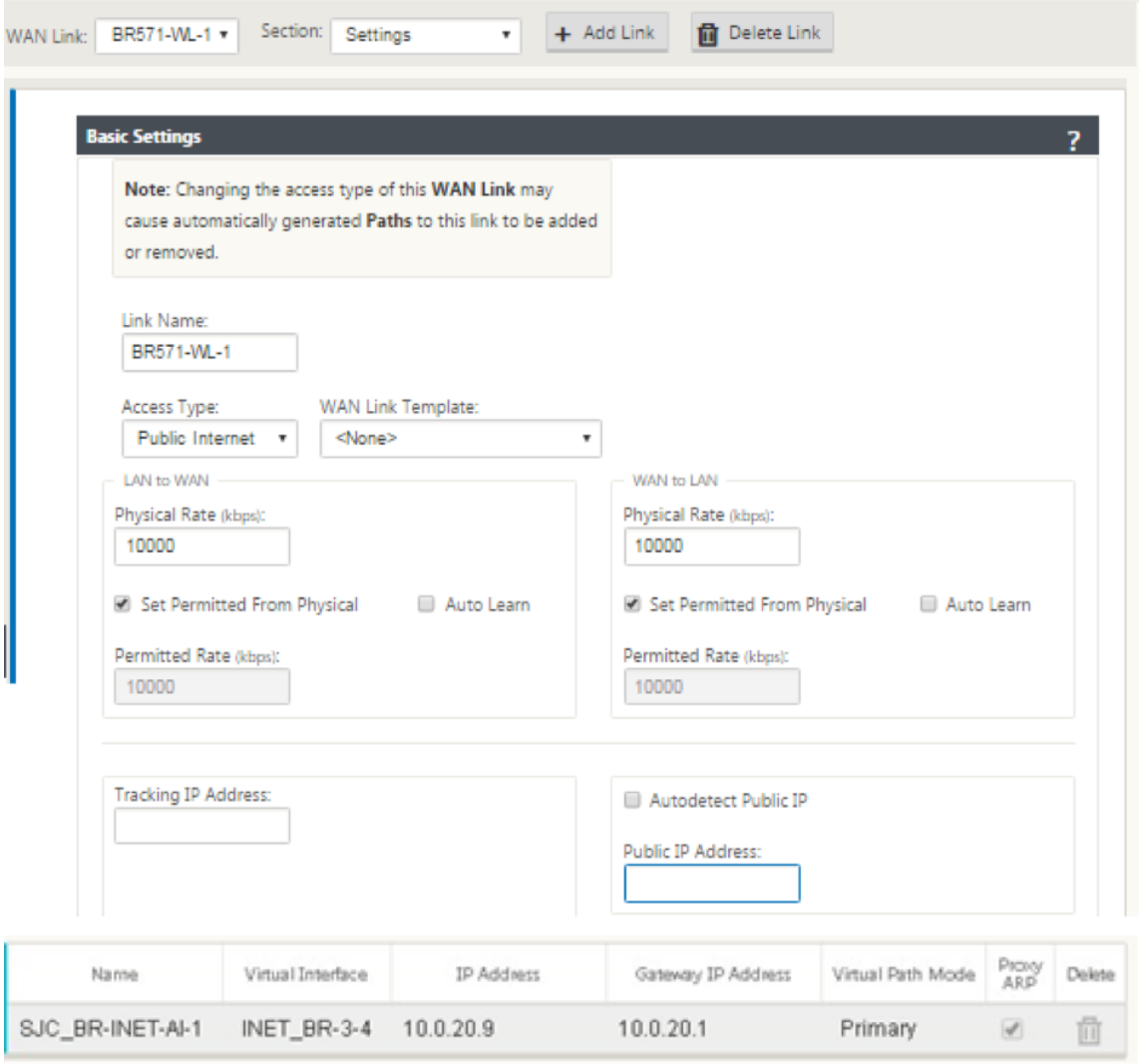
So erstellen Sie VIP-Adresse (Virtual IP) für jede virtuelle Schnittstelle

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.



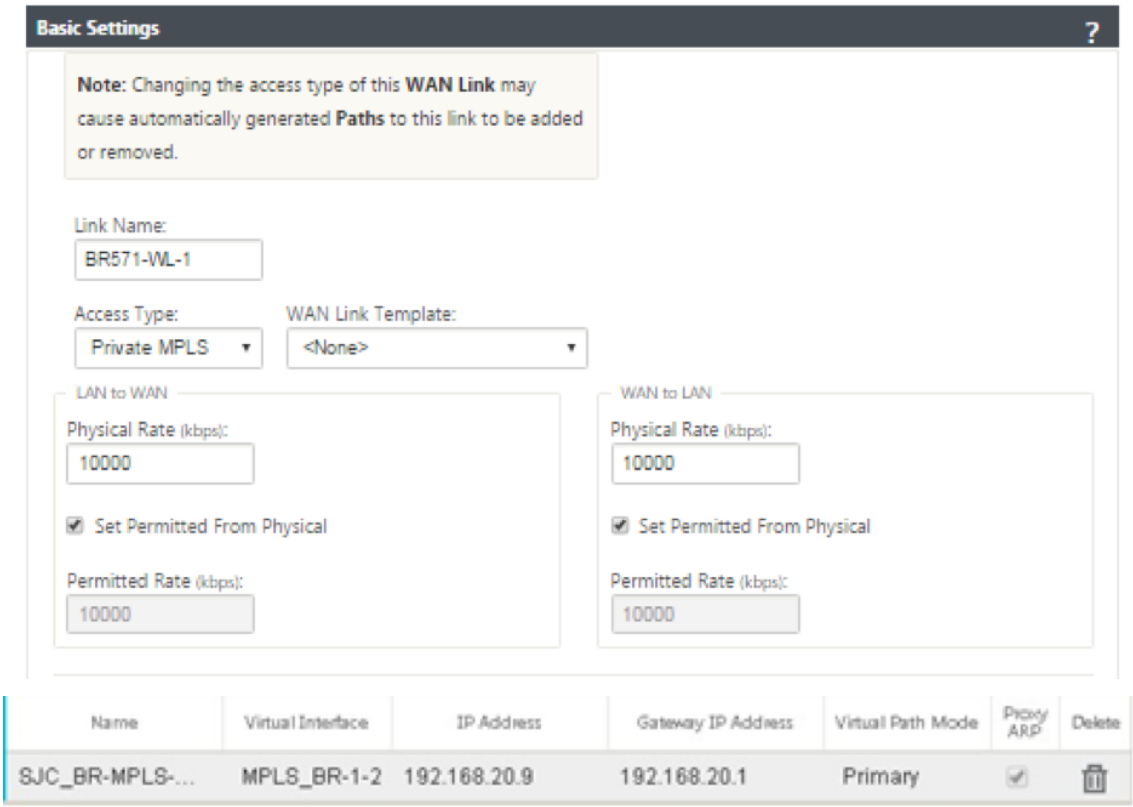
So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten über Internetlinks aus

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.



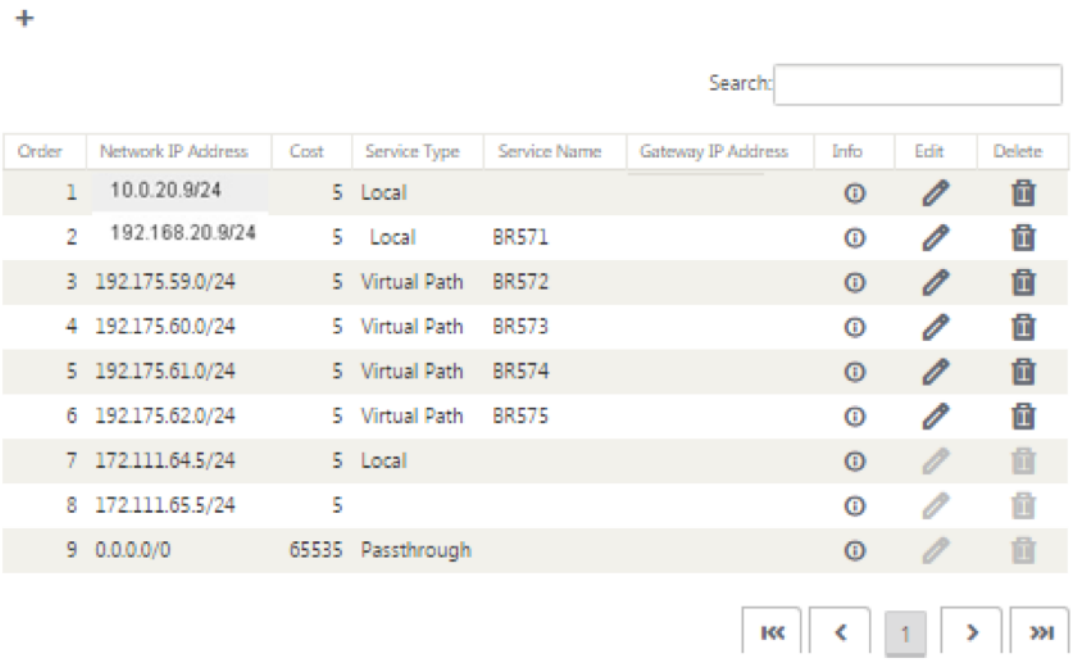
So erstellen Sie MPLS-Verknüpfung

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.



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.



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 (einarmige 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.

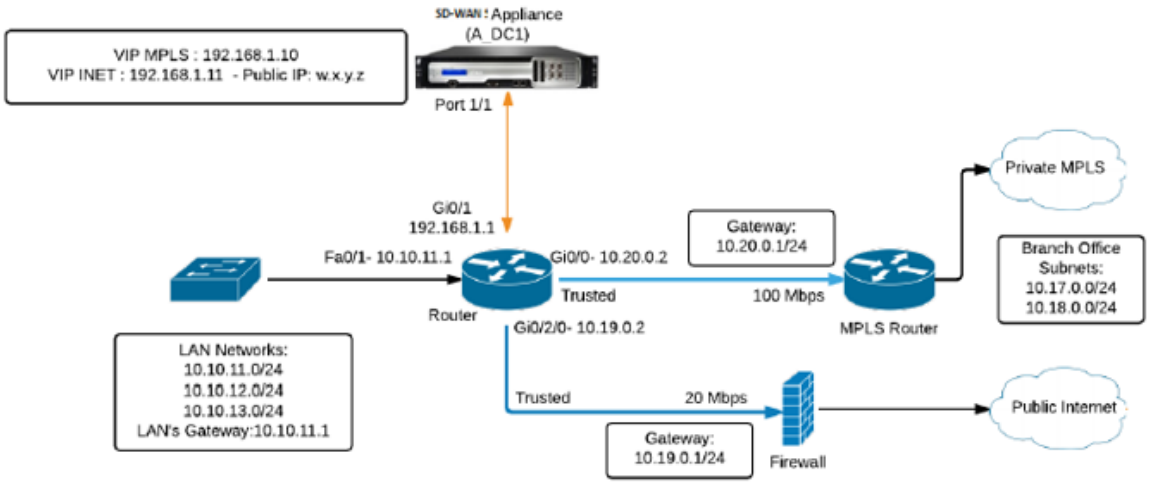
Sammeln Sie Informationen

Sammeln Sie die folgenden Informationen, die für die Konfiguration des virtuellen Inlinemodus erforderlich sind:

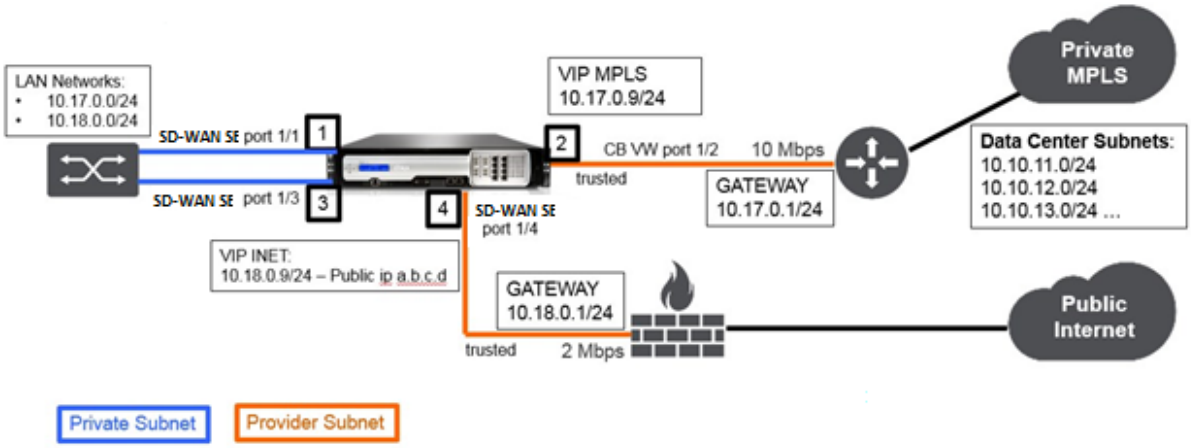
- Genaues Netzwerkschema Ihrer lokalen und Remotestandorte, einschließlich:
  - Lokale und Remote-WAN-Verbindungen und ihre Bandbreiten in beide Richtungen, ihre Subnetze, virtuellen IP-Adressen und Gateways von jeder Verbindung, Routen und VLANs.
- Tabelle für die Bereitstellung

Das Folgende ist ein Beispiel für ein Netzwerkschema und eine Bereitstellungstabelle:

Rechenzentrumtopologie —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

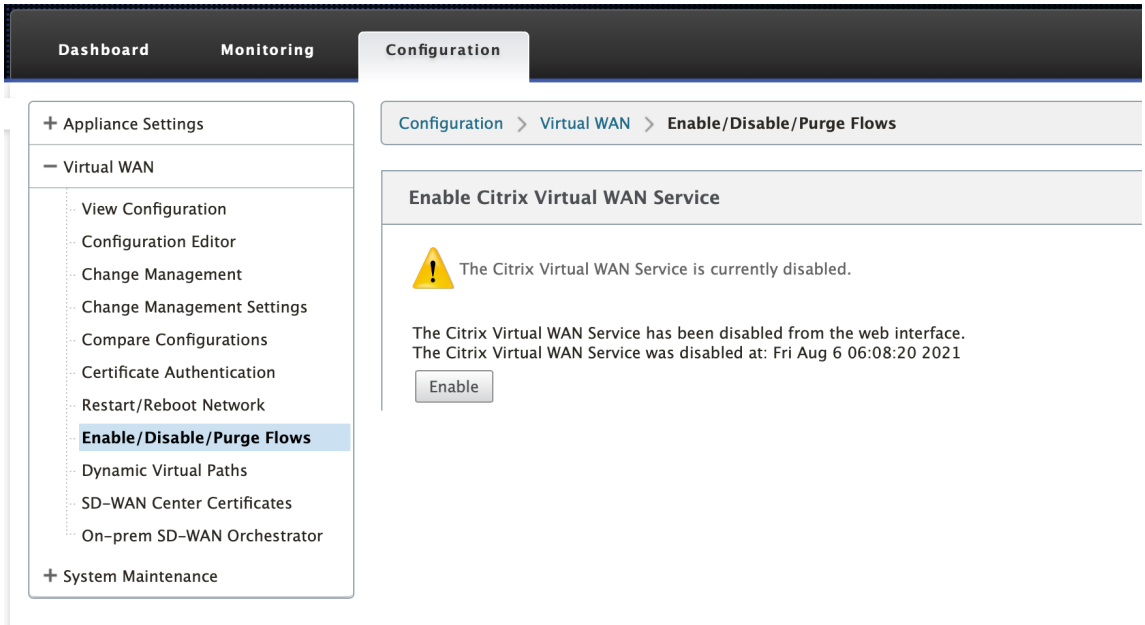
Sitename	Rechenzentrums-Standort	Niederlassungsstandort
Route	Sie müssen eine Route auf der SD-WAN SE Appliance hinzufügen, wie Sie die LAN-Subnetze (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24 usw.) über eine der physischen Schnittstellen erreichen: Gi0/1 - 192.168.1.1, **Konfiguration > Virtuelles 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

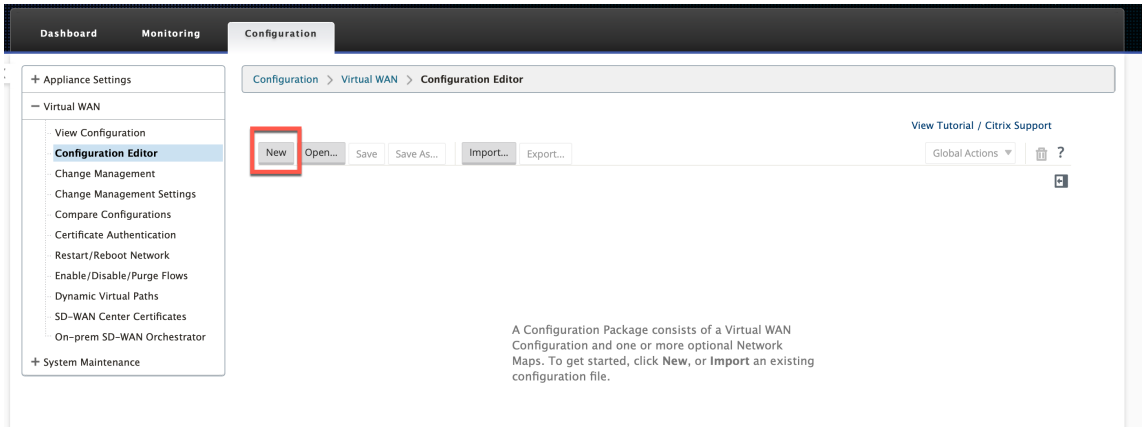
1. Navigieren Sie in der Webverwaltungsoberfläche der SD-WAN-Appliance zu **Konfiguration > Appliance-Einstellungen > Administratorschnittstelle > Verschiedenes und klicken** Sie auf **Switch-Konsole**.

   > **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**.



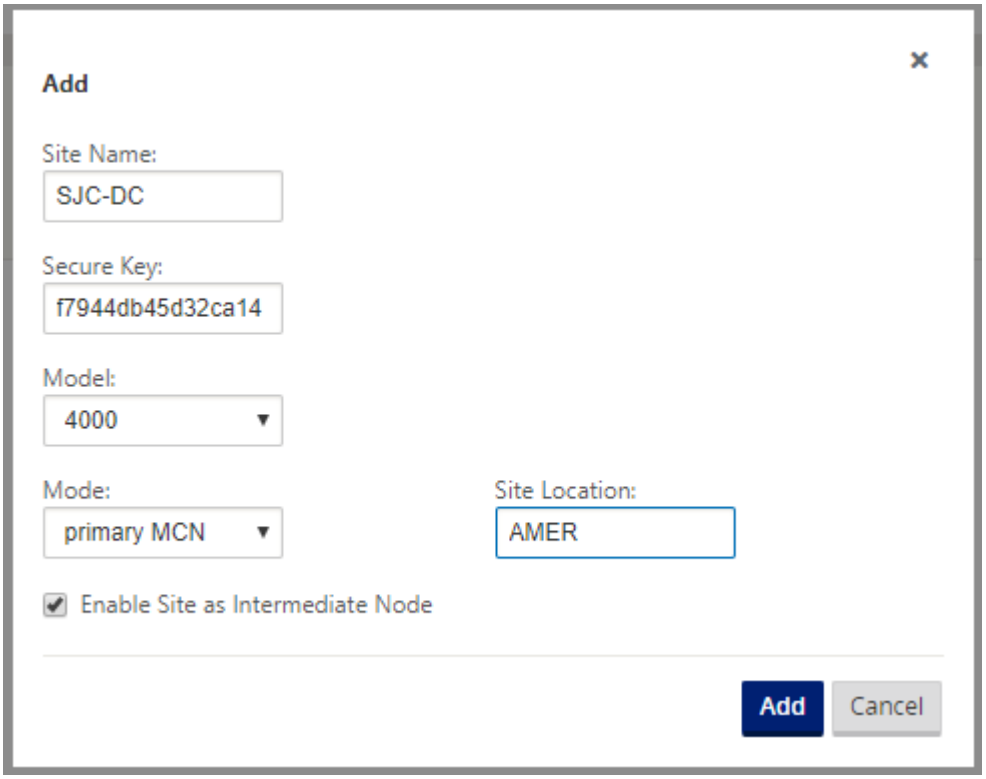
3. Starten Sie Konfiguration, indem Sie zu **Konfiguration > Virtuelles WAN > Konfigurationsed-itor**navigieren. Klicken Sie auf **Neu**, um mit der Konfiguration zu beginnen. Durch Klicken auf **Neu** wird eine anfängliche Konfigurationsdatei mit **Untitled_1** als Dateinamen erstellt. Sie können die Datei später [optional] mit der Schaltfläche **Speichern** unter umbenennen.



Rechenzentrumsstandort —Konfiguration des virtuellen Inlinemodus

Erstellen eines Rechenzentrumsstandorts

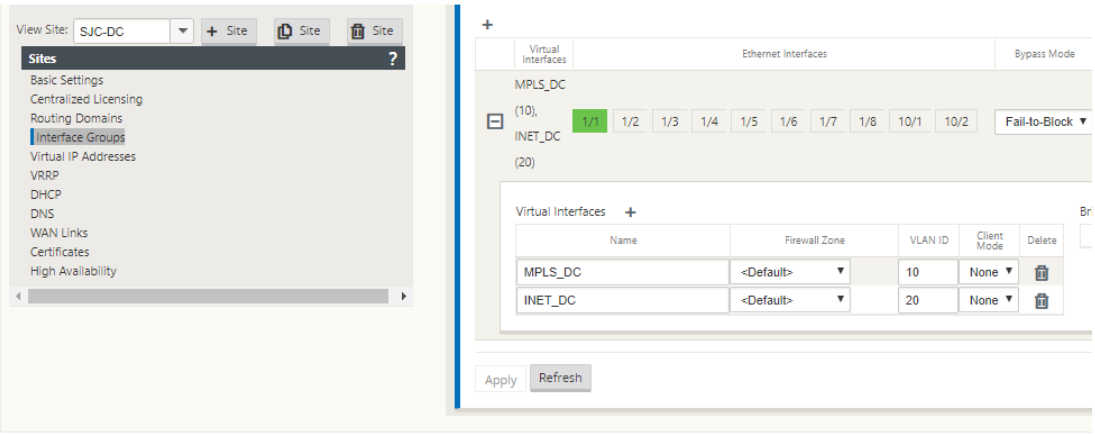
1. Navigieren Sie zu **Konfiguration > Virtual WAN > Konfigurationseditor > Sites** und klicken Sie auf **+ Site**.
2. Geben Sie den Site-Namen und den Standort ein. Wählen Sie das **Appliance-Modell** aus der Dropdownliste Modell und **Primärer MCN** aus der Dropdownliste **Modus** aus.
3. Klicken Sie auf **Hinzufügen**.



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.

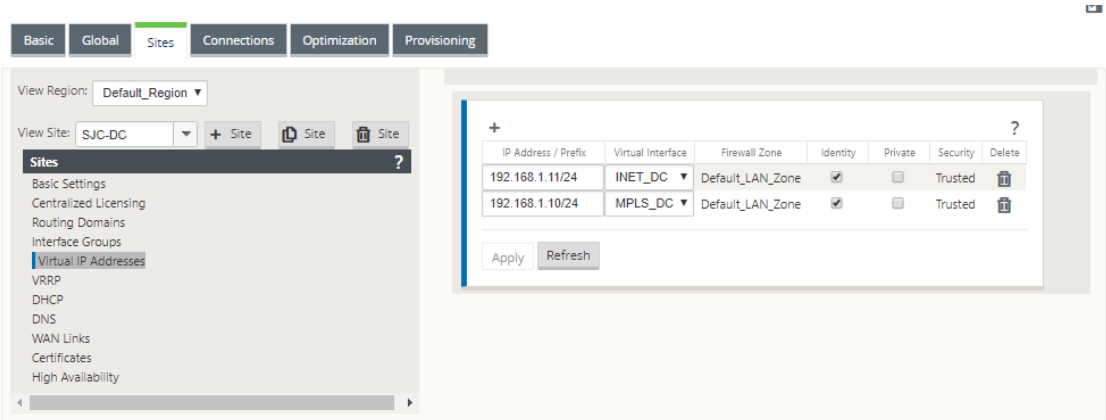
1. Navigieren Sie im **Konfigurationseditor**zu **Sites > [Site-Name] > Schnittstellengruppen**. Klicken Sie auf **+**, um Schnittstellen hinzuzufügen, die verwendet werden sollen.
2. Wählen Sie die Ethernet-Schnittstelle aus, die mit dem Upstream-Router verbunden wird, und klicken Sie neben Virtuelle 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.

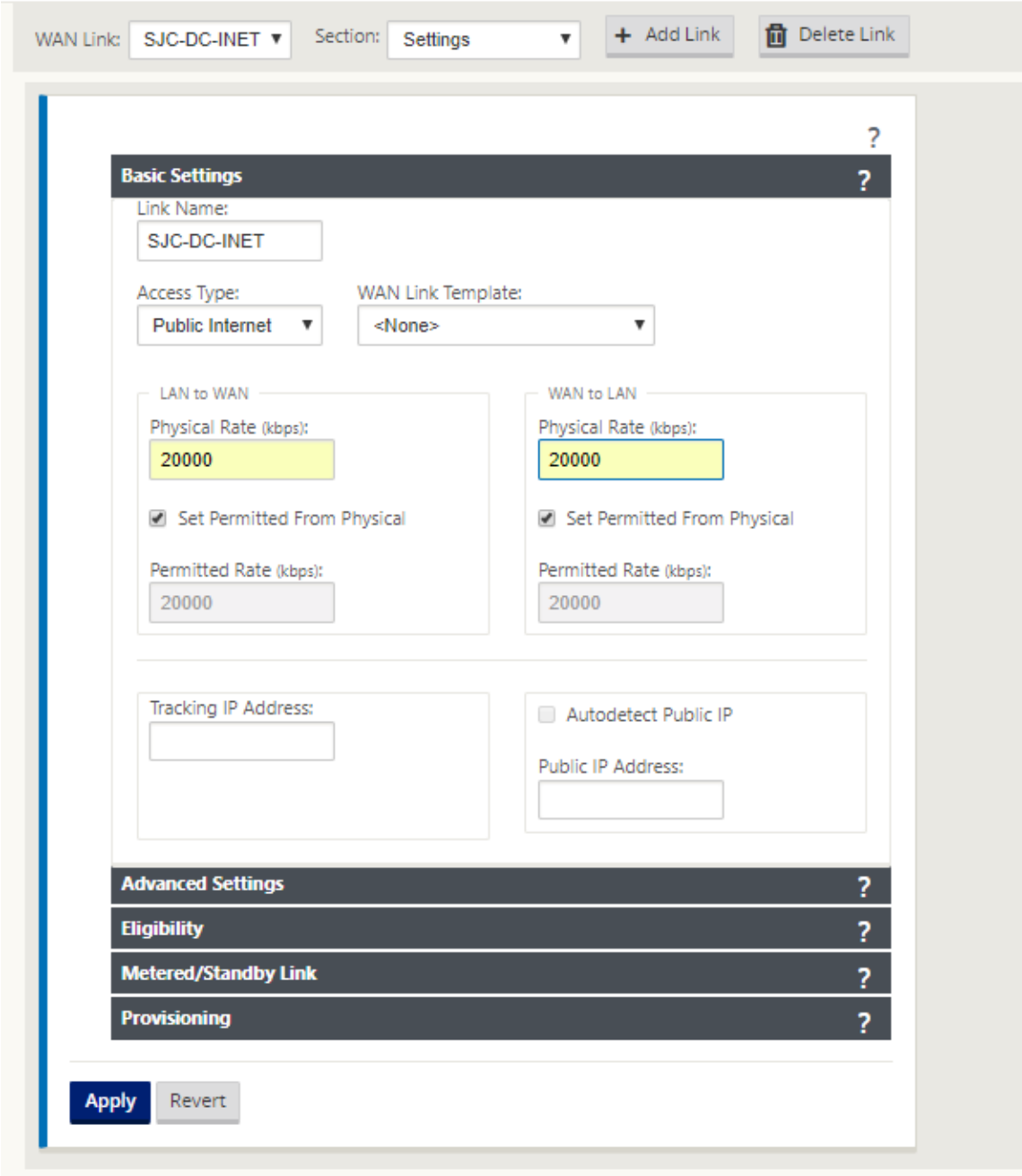
1. Navigieren Sie im **Konfigurationseditor**zu **Sites >[Site-Name] > Virtuelle IP-Adressen**. Klicken Sie auf **+**, um VIPs zu erstellen.
2. Geben Sie die IP-Adresse/das Präfix ein und wählen Sie die entsprechende virtuelle Schnittstelle für MPLS und Internet aus.
3. Klicken Sie auf **Apply**.



Internet-WAN-Link erstellen

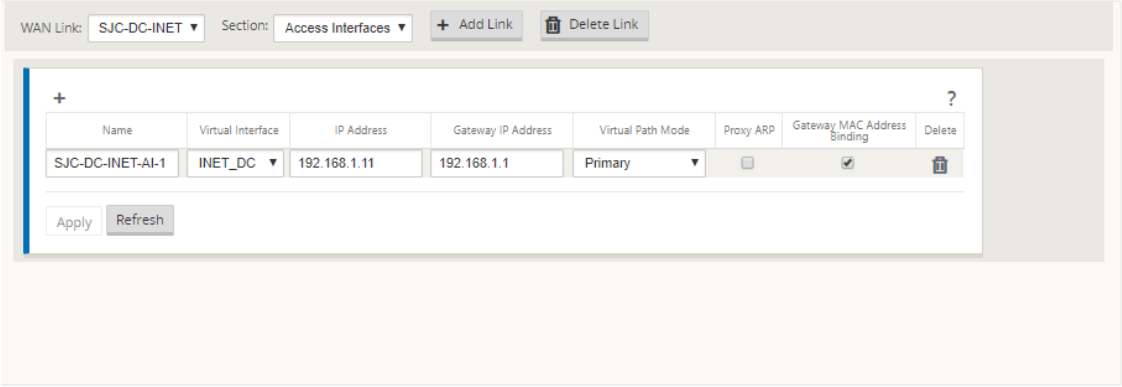
Erstellen Sie eine Internet-WAN-Verbindung basierend auf der physischen Rate und nicht auf Burst-Geschwindigkeiten.

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.



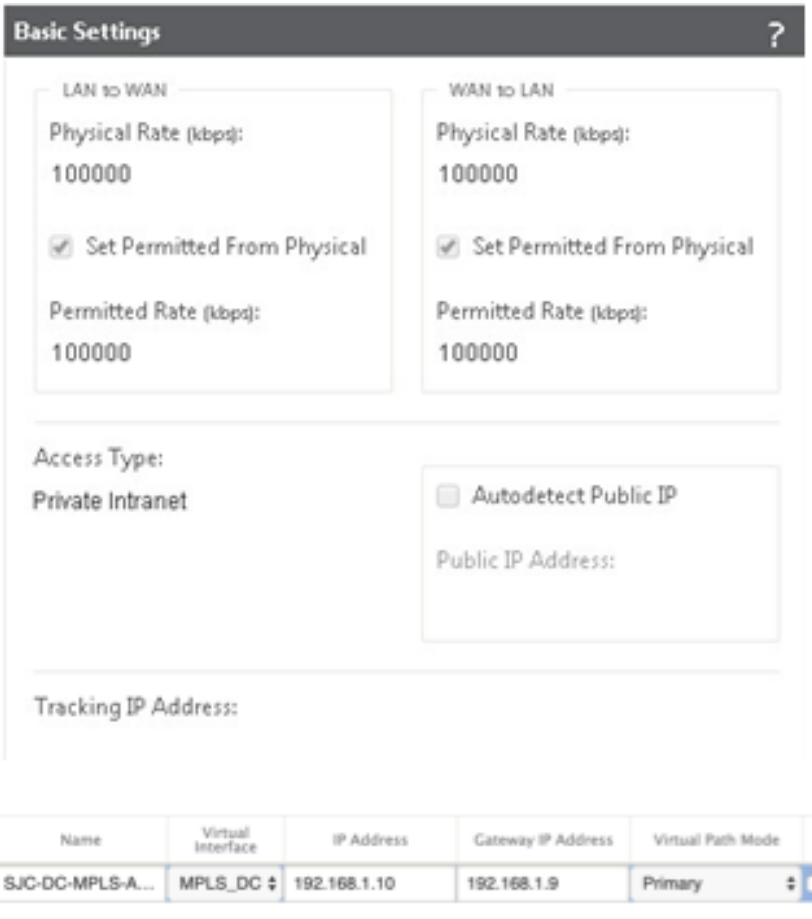
3. Wählen Sie in der Dropdownliste **Abschnitt** die Option **Zugriffsschnittstellen** aus und klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den Internetlink hinzuzufügen.

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**.

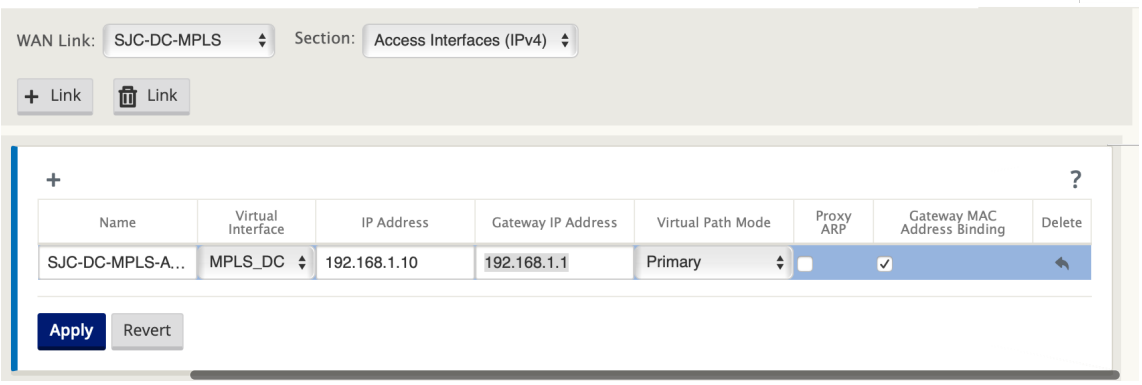


Erstellen Sie einen MPLS-Link

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**.



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**.



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.

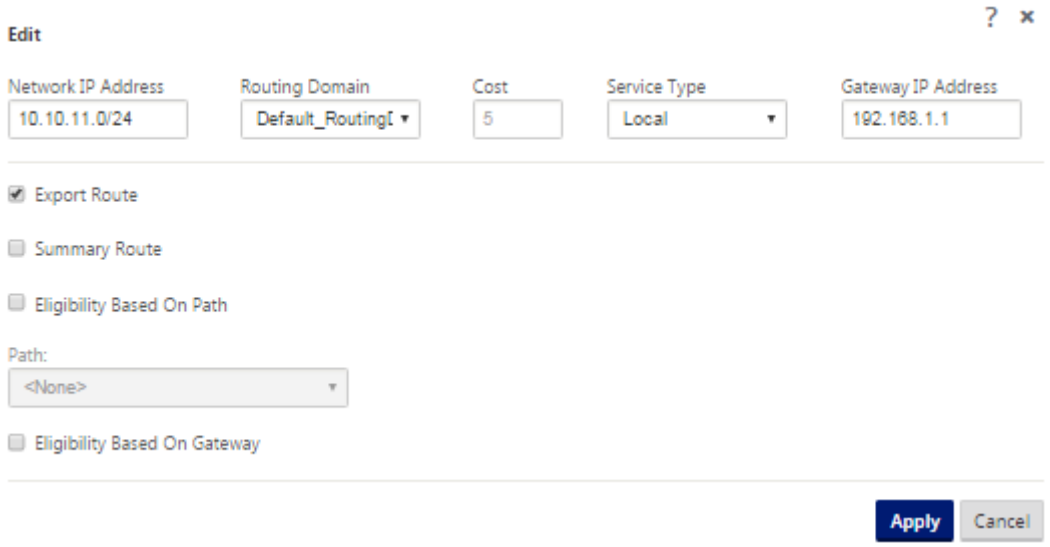
0/1/0.1 —192.168.1.1 auf VLAN 10

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**.

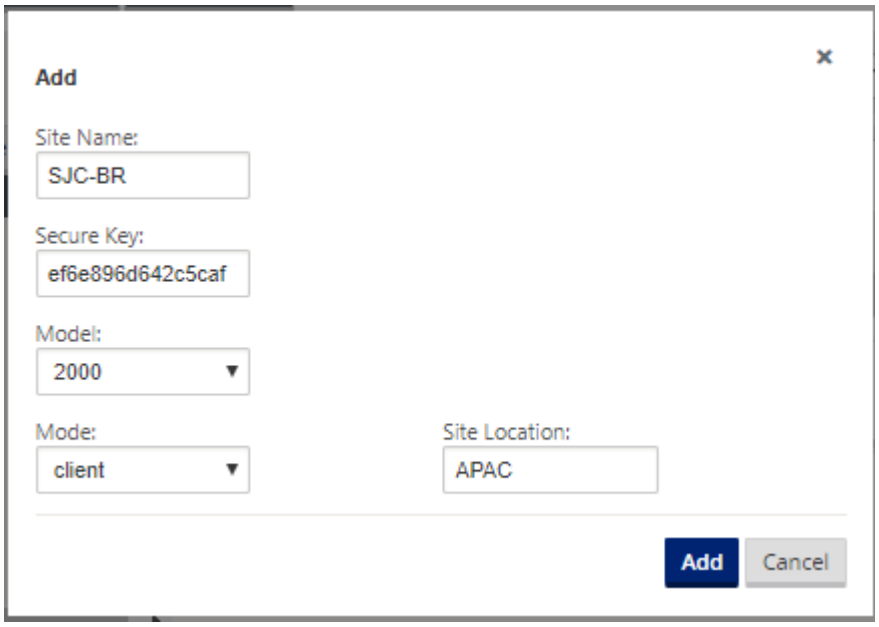


Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.10.13.0/24	5	Local		192.168.1.1			
2	10.10.12.0/24	5	Local	BR571	192.168.1.1			
3	10.10.11.0/24	5	Local	BR572	192.168.1.1			
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					

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**.

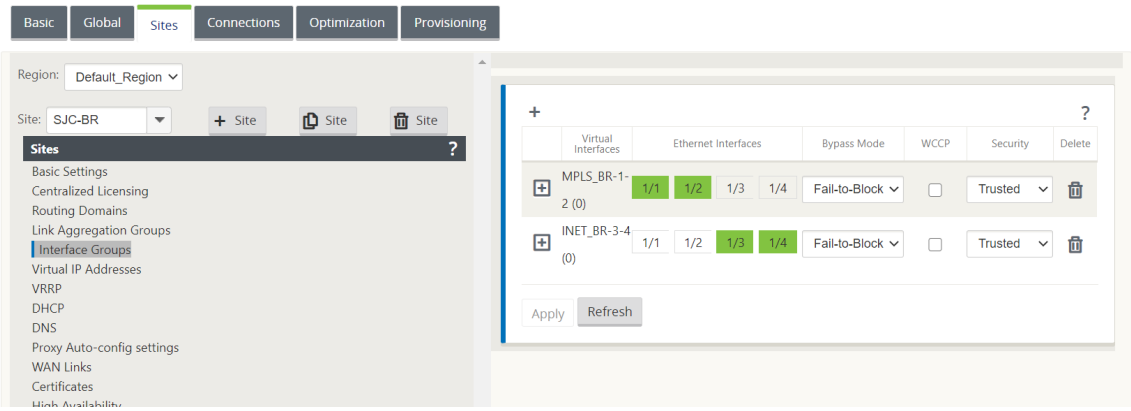


Konfigurieren von Schnittstellengruppen basierend auf verbundenen Ethernet-Schnittstellen

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.

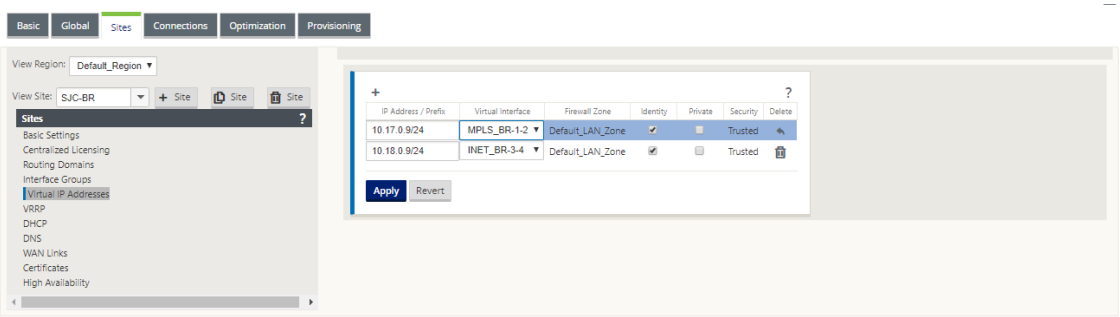
   Lesen Sie das Diagramm **Zweigtopologie** —**Inline-Modus-Topologie** im Abschnitt Voraussetzungen, und füllen Sie die Schnittstellengruppen aus.



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.

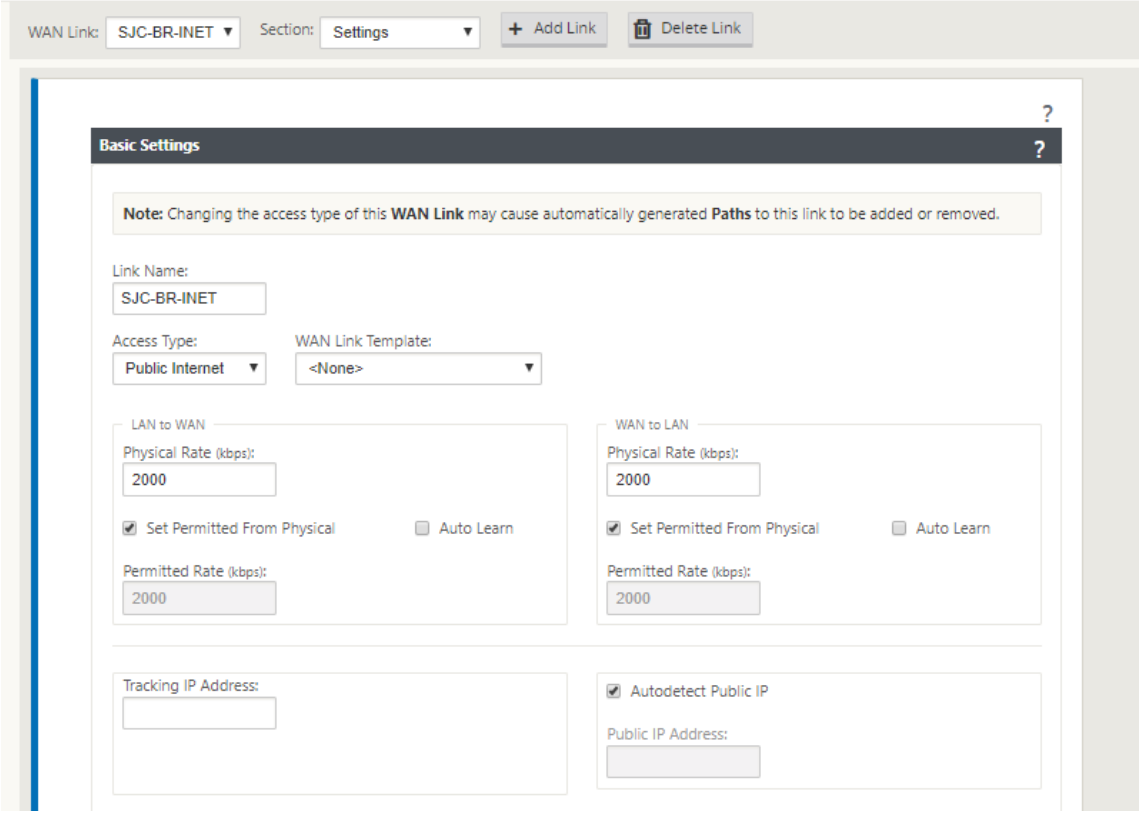
1. Navigieren Sie im **Konfigurationseditor**zu **Sites >[Site-Name] > Virtuelle IP-Adressen**. Klicken Sie auf **+**, um VIPs zu erstellen.
2. Geben Sie die IP-Adresse/das Präfix ein und wählen Sie die entsprechende virtuelle Schnittstelle für MPLS und Internet aus.
3. Klicken Sie auf **Apply**.

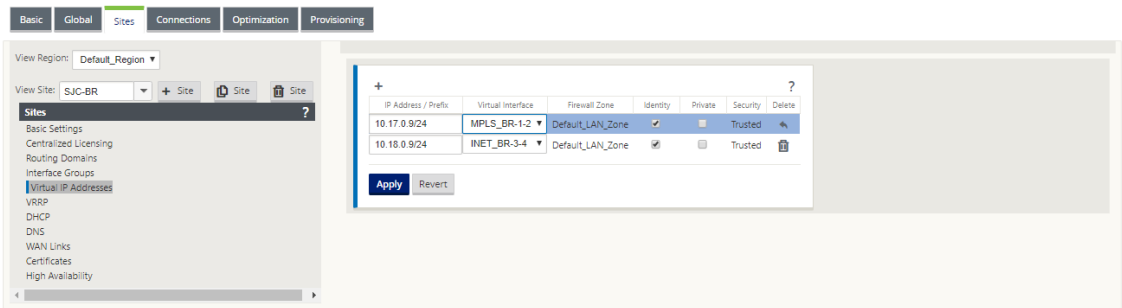


Internet-WAN-Link erstellen

So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten über Internetlinks aus

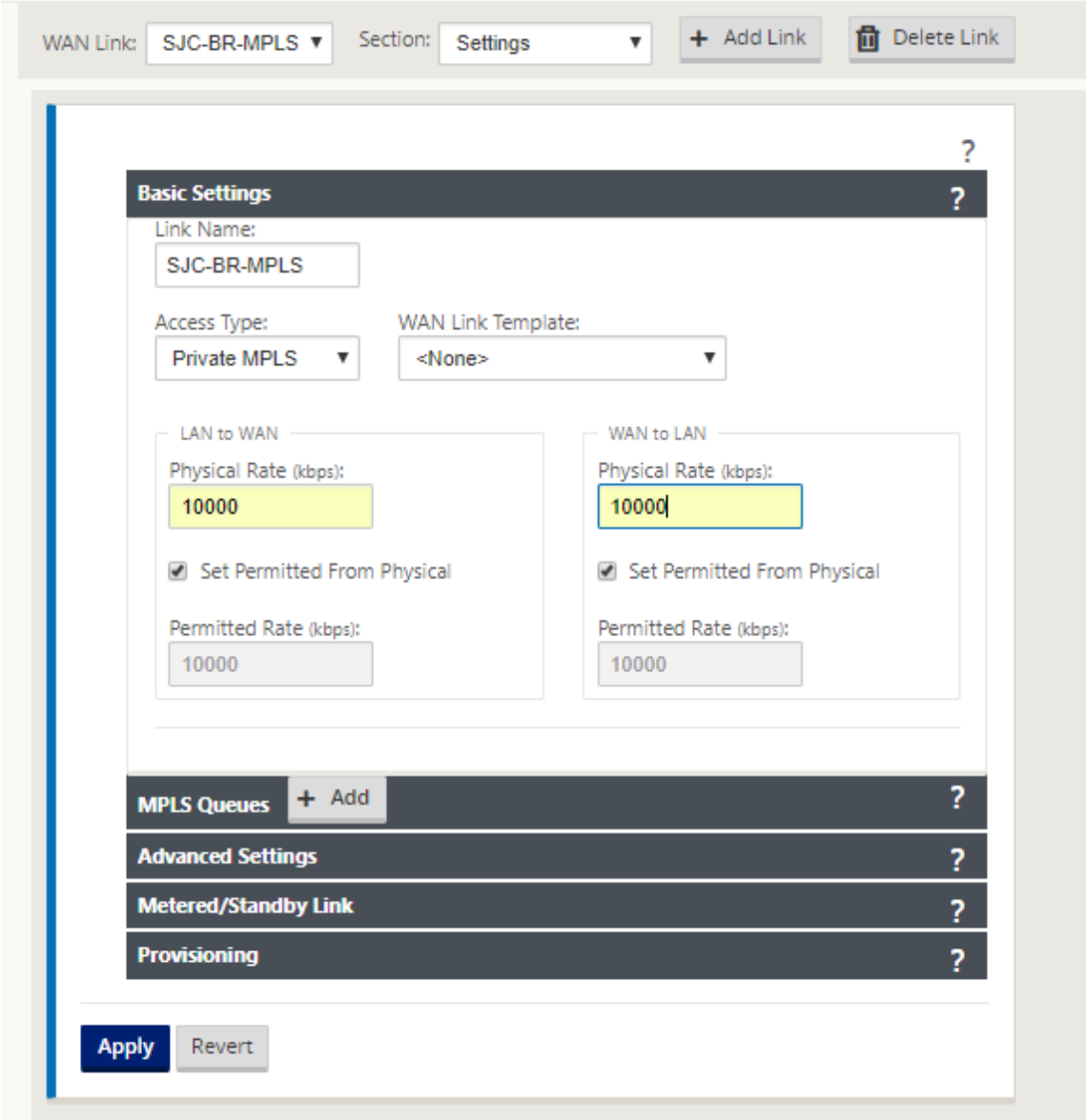
1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+ Link**, um einen WAN-Link für den Internetlink hinzuzufügen. Geben Sie einen Namen ein und wählen Sie **Zugriffstyp** als **öffentliches Internet**. Klicken Sie auf **Hinzufügen**.
2. Füllen Sie die Internetverbindungsdetails aus 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.



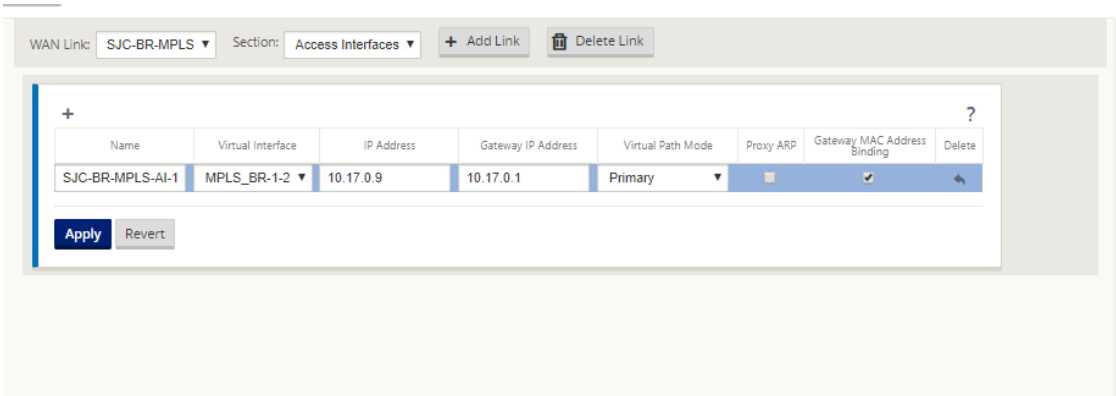


Erstellen Sie eine MPLS-WAN-Verbindung

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.



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.

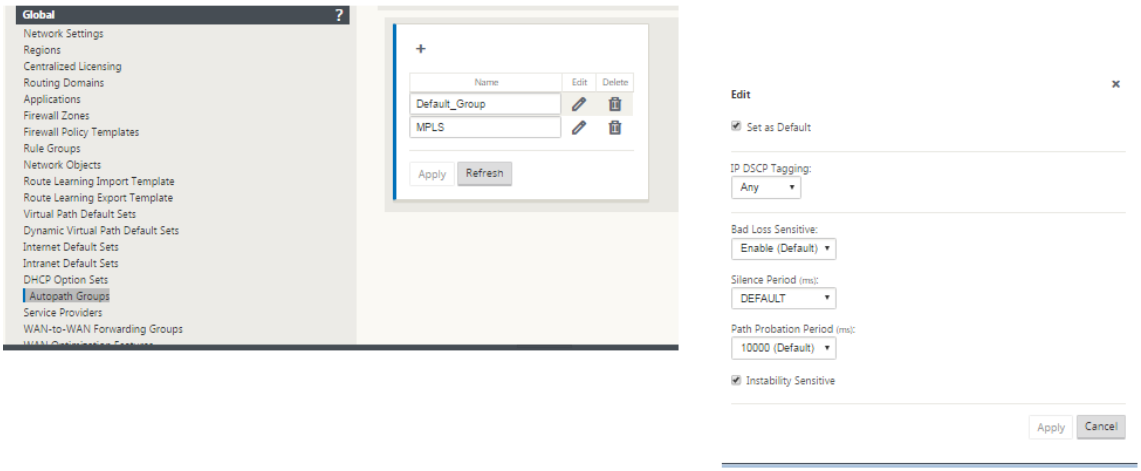


Routen auffüllen

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**.



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.

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-Paketefort.

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

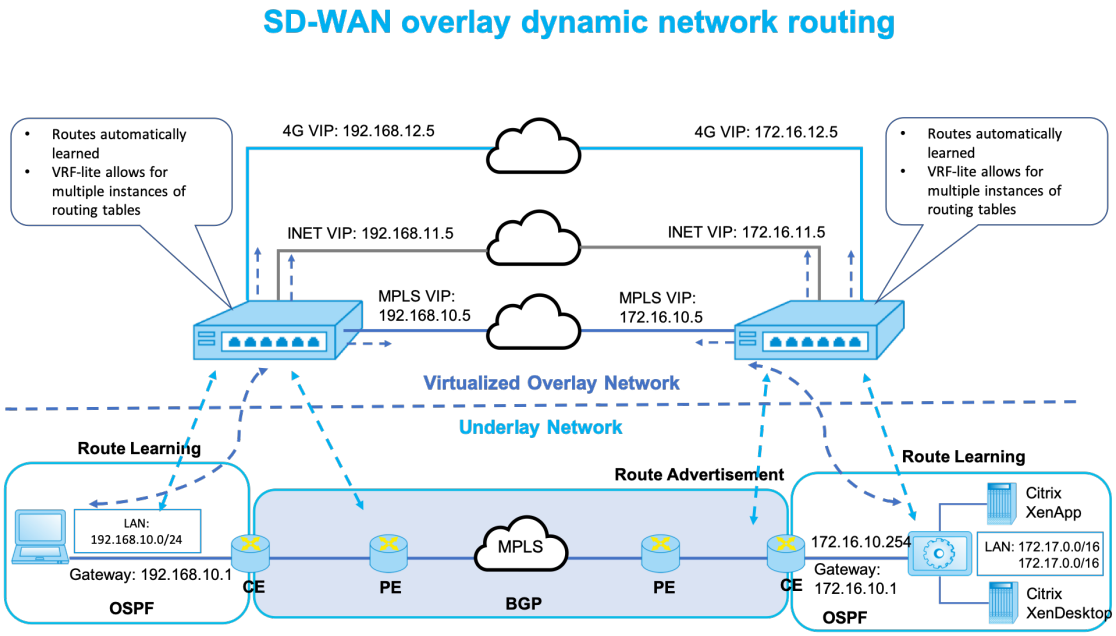
October 28, 2021

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 unter Verwendung des SD-WAN-Overlay-Netzwerks anstelle der vorhandenen Unterlage durchqueren können, die am wenigsten intelligent und kosteneffizient ist.

SD-WAN-Routingkomponenten und Netzwerktopologie

- Lokal —Subnetz befindet sich an dieser Site (in der SD-WAN-Umgebung beworben)
- Virtueller Pfad —wird über den virtualisierten Pfad zur ausgewählten Site-Appliance gesendet
- Intranet —Standorte ohne SD-WAN-Appliance
- Internet —Internet-gebundener Verkehr
- Pass-Through —unberührter Verkehr, in einer Brückenschnittstelle aus dem 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.



WAN-Optimierung nur mit Premium (Enterprise) Edition

October 28, 2021

Die SD-WAN Premium (Enterprise) Edition-Appliances enthalten zusätzlich zur WAN-Virtualisierung voll ausgestattete 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 (physisch oder virtuell) am DC-Standort als MCN konfigurieren. Die SD-WAN-Appliance verwaltet die gesamte Konfiguration des Netzwerks. Ein virtueller Pfad wird zwischen dem Niederlassungsstandort und MCN am DC-Standort eingerichtet. Dieser virtuelle Pfad wird nur zum Senden von Steuerdatenverkehr zwischen den Appliances verwendet. In der Zweigstelle wird der Datenverkehr als Intranetdienst verarbeitet. Der Intranet-Verkehr ist nicht gekapselt und überquert die vorhandene WAN-Verbindung, um den DC-Standort zu erreichen. Eine WANOP-Appliance am DC-Standort sollte sich im Verkehrspfad befinden, um eine End-to-End-Verkehrsoptimierung 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 Router eines Drittanbieters 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 zwingend erforderlich.

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 der PBR-Bereitstellung:

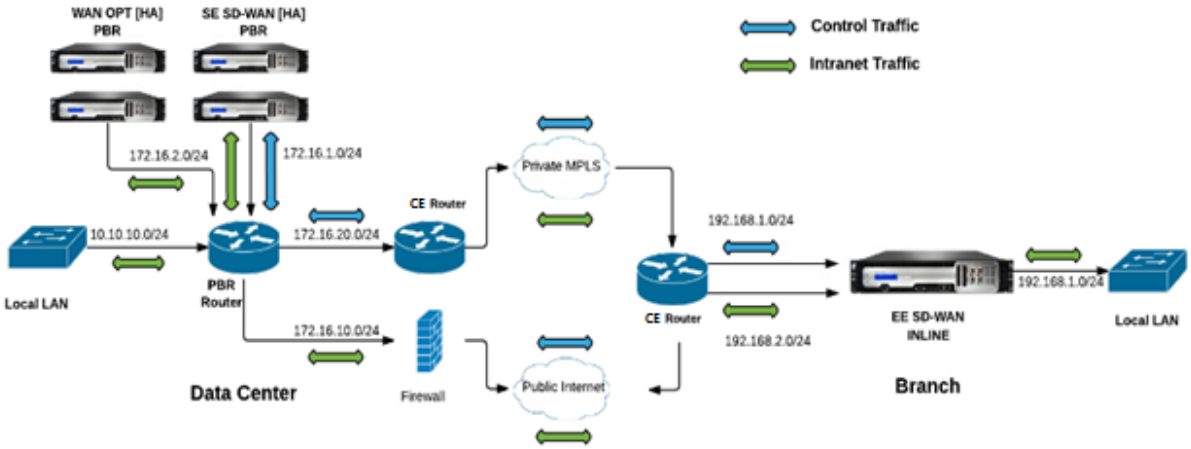
In der folgenden Abbildung werden sowohl die SD-WAN SE- als auch die WAN OP-Appliances am DC-Standort im Einarmmodus eingesetzt. Die SD-WAN-Appliance unterstützt die PBR-Bereitstellung, während die WANOP-Appliance sowohl PBR als auch WCCP unterstützt. Der vom WAN am DC-Standort empfangene Steuerdatenverkehr (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 (Kunden-Edge) -Router -> PBR-Router -> SD-WAN -> PBR-Router -> LAN

- CE (Kunden-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 in der Inline-Bereitstellung:

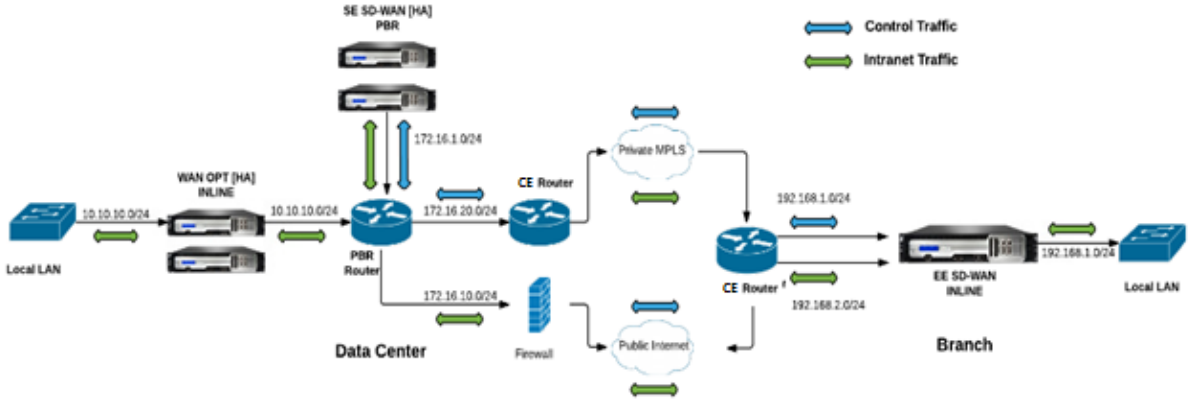
In der folgenden Abbildung wird die SD-WAN-Appliance am DC-Standort im Einarmmodus bereitgestellt, während die WANOP-Appliance im Inline-Modus bereitgestellt wird.

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 (Kunden-Edge) -Router -> PBR-Router -> SD-WAN -> PBR-Router -> LAN
- CE (Kunden-Edge) Router -> PBR-Router -> WAN OPT -> LAN

Der gleiche Verkehrsfluss wird in umgekehrter Richtung verfolgt.



Konfigurationsschritte

1. Konfigurieren Sie die SD-WAN Appliance bei DC [MCN], um virtuelle Pfade zwischen DC- und Zweigstandorten einzurichten.

   Siehe Konfigurieren des virtuellen Pfaddienstes zwischen MCN und Clients.

2. Konfigurieren Sie den Intranetdienst am DC-Standort.

   a) Wechseln Sie auf dem MCN (DC-Standort) zu **Konfiguration > Virtuelles WAN > Konfigurationseditor > Verbindungen > Standort (DC) > Intranetdienste**. Klicken Sie auf das **[+-Zeichen]**, um einen Intranetdienst hinzuzufügen.

   b) Wählen Sie einen oder mehrere WAN-Links für den **Intranetdienst**aus, und klicken Sie dann auf **Übernehmen**.

   c) Navigieren Sie zu Routen unter demselben **Standort (DC)**, klicken Sie auf das **[+-Zeichen]**-Zeichen, um das Remotenetzwerk mit Kosten unter 5 hinzuzufügen, und klicken 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 weniger als 5 betragen, damit die Intranetroute Vorrang hat.

3. Konfigurieren Sie den Intranetdienst am Standort der Zweigstelle.

   a) Wiederholen Sie die Teilschritte a bis c aus **Schritt 2** oben auf dem Zweigstandort.

      Beispiel: - Geben Sie **172.16.1.0/24** in das Feld Netzwerk-IP-Adresse mit Kosten 4 ein und wählen Sie **Servicetyp** als **Intranet**aus.

4. Führen Sie **das Änderungsmanagement** durch, um die Konfiguration hochzuladen und auf den Zweigstandort

   Siehe Konfigurationspaket exportieren und Änderungsmanagement

   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 zur Konfiguration der WAN-Optimierung finden Sie unter: Enabling-Configuring-WAN-Optimierung.

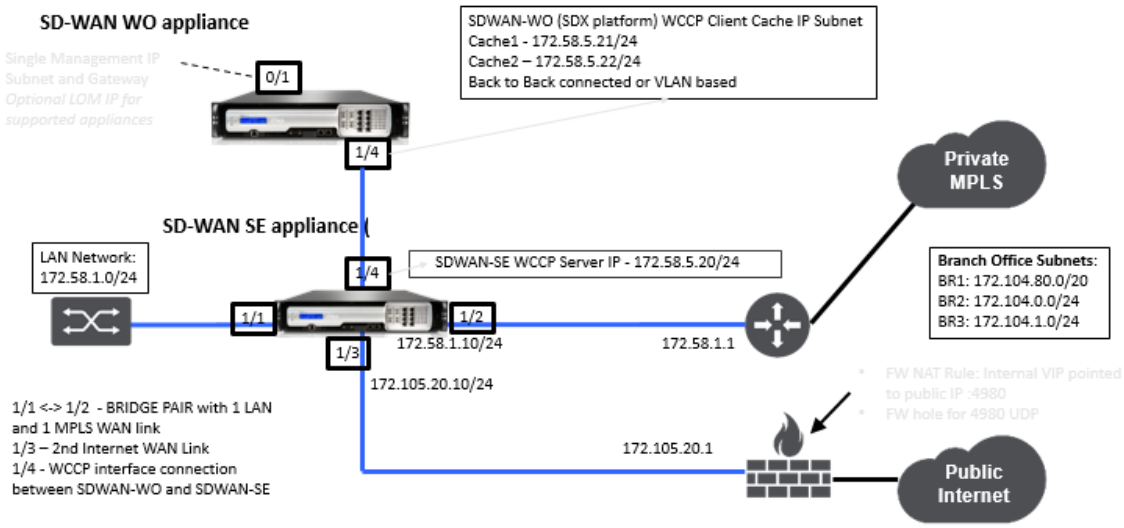
Zwei-Box-Modus

October 28, 2021

Der Zwei-Box-Modus ist eine einarmige WCCP-Bereitstellung, bei der die SD-WAN SE-Appliance als WCCP-Router fungiert und die SDWAN-WANOP (4000/5000) -Appliances als WCCP-Clients fungieren und zur Herstellung der WCCP-Konvergenz beitragen. Auf diese Weise werden alle virtuellen Pfad/Intranet-Service-orientierten TCP-Pakete, die die SD-WAN SE-Appliance erreichen, zur Optimierung an die SDWAN-WANOP-Appliance umgeleitet, indem sowohl SD-WAN SE- als auch WANOP-Vorteile für den Kundenverkehr bereitgestellt werden.

Der Zwei-Box-Modus wird nur bei den folgenden Gerätemodellen unterstützt:

- SD-WAN SE-Geräte —4000, 4100 und 5100
- SD-WAN WANOP-Geräte —4000, 4100, 5000 und 5100



> **Hinweis**
>
> Hochverfügbarkeit und WCCP-Bereitstellungsmodi sind nicht verfügbar, wenn der Zwei-Box-Modus aktiviert ist. Diese Bereitstellungsmodi stehen dem Benutzer jedoch zur Verwaltung zur Verfügung.
>
> **Wichtig**
>
> - Obwohl die alte WCCP-Bereitstellung deaktiviert ist, wenn der Zwei-Box-Modus aktiviert ist, kann die Konvergenz der Dienstgruppe nur auf der WCCP-Überwachungsseite überprüft werden. Unter dem Überwachungsabschnitt für den Zwei-Box-Modus gibt es keine separate GUI-Seite.
> - Wenn der WCCP-Prozess, der auf der Standard Edition-Appliance ausgeführt wird, inner-

halb eines kurzen Zeitraums mehrmals neu gestartet wird, z. B. dreimal in einer Minute, wird die Service Group automatisch heruntergefahren. Um in einem solchen Szenario die WCCP-Konvergenz auf der WANOP-Appliance zu erhalten, aktivieren Sie die WCCP-Funktion in der Web-GUI der WANOP-Appliance erneut.

- Wenn sich die WCCP-Konfiguration oder 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 Konfigurationseditors, gefolgt vom Change Management-Prozess, aktivieren/deaktivieren, startet auch die WANOP-Appliance neu.

Hinweis

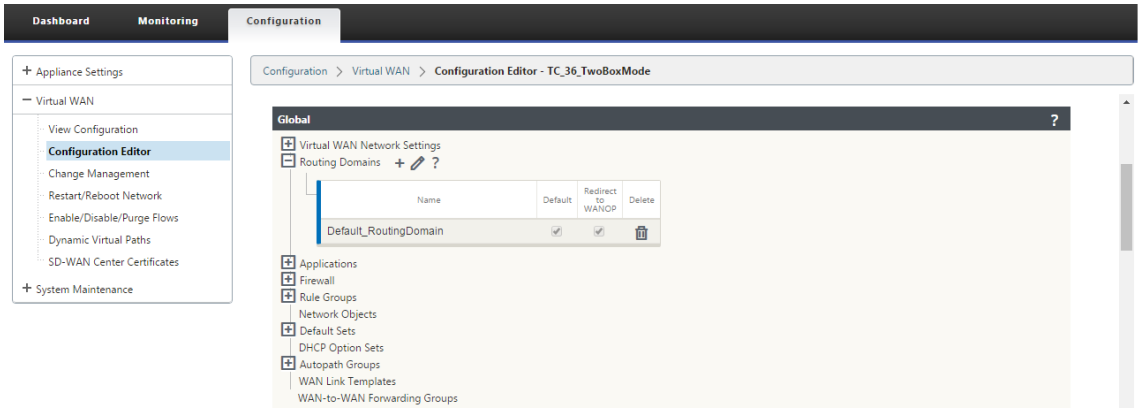
Beachten Sie außerdem die folgenden Punkte, die bei der Implementierung des Zwei-Box-Modus zu beachten sind:

- Wenn eine Routingdomäne aus dem Konfigurationseditor 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. Zum 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-fähige Schnittstellengruppe die Routingdomäne konfiguriert hat, reicht es nicht aus, den End-to-End-Verkehr zu übertragen, der mit Vorteilen der WAN-Optimierung fließt.

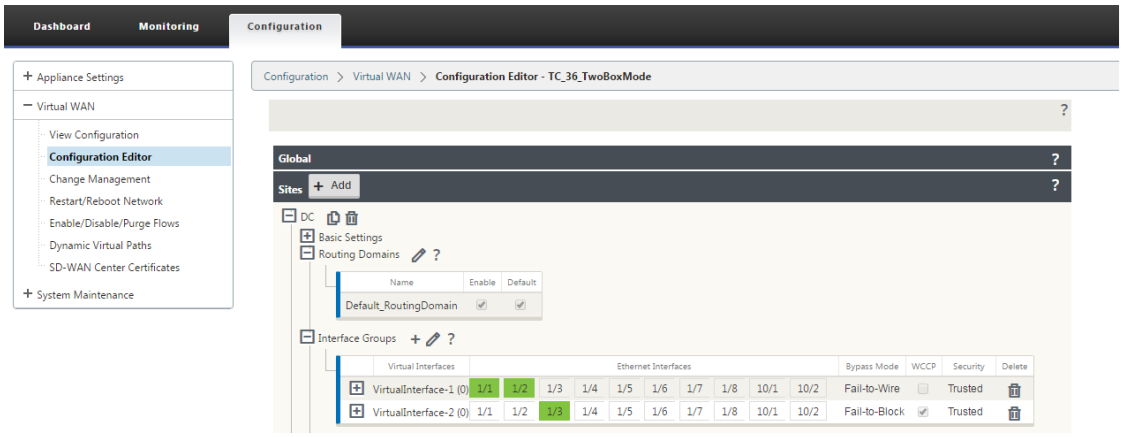
Citrix SD-WAN Standardausgabe

So konfigurieren Sie die Lösung im Zwei-Box-Modus in der Standard Edition-Appliance am DC- oder Zweigstandort:

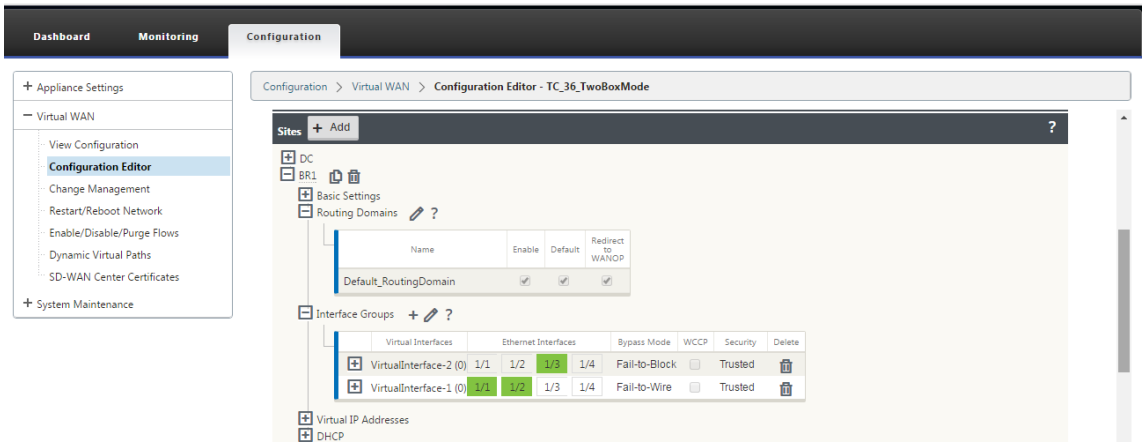
1. Wechseln Sie in der SD-WAN SE-Webverwaltungsoberfläche zu **Konfiguration** > **Virtuelles WAN** > **Konfigurationseditor**. Öffnen Sie ein vorhandenes Konfigurationspaket oder erstellen Sie ein Paket.
2. Wechseln Sie im ausgewählten Konfigurationspaket zur Registerkarte **Erweitert**, um die Konfigurationsdetails anzuzeigen.
3. Öffnen Sie **Globale** Einstellungen und erweitern Sie **Routing Domains**, um anzuzeigen, dass das Kontrollkästchen **Zu WANOP umleiten** aktiviert ist.



4. Erweitern Sie DC, um **WCCP** für die **virtuelle**Schnittstelle unter Schnittstellengruppeneinstellungen** zu aktivieren, die angeben, für welche virtuelle Netzwerkschnittstelle die Appliance aktiviert ist.



5. Erweitern Sie **Sites+ Hinzufügen**, um die Einstellungen für Zweigroutingdomäne und Schnittstellengruppen anzuzeigen. Unter dem Zweigstandort ist das Kontrollkästchen **Weiterleitung zu WANOP** für Routingdomänen aktiviert.

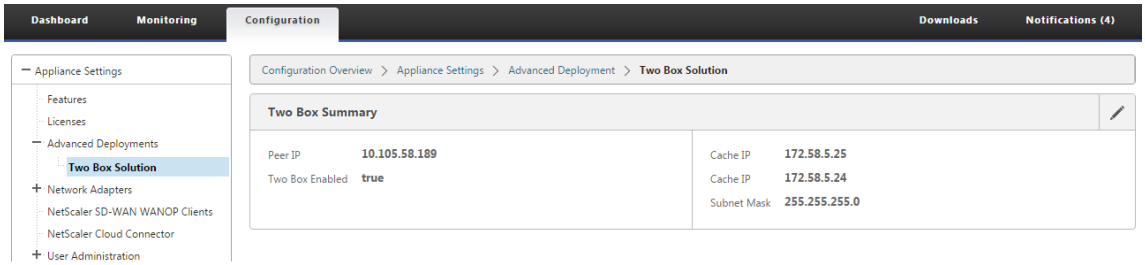


> **Hinweis**
>
> Der WCCP-Listener sollte nur für die virtuellen Netzwerkschnittstellen aktiviert werden, für die nur EINE Ethernet-Schnittstelle konfiguriert ist. Aktivieren Sie den WCCP-Listener nicht für ein BRIDGED-Paar. Es soll auf der ONE-ARM-Schnittstelle zwischen den SD-WAN SE und SD-WAN WANOP-Einheiten aktiviert werden.

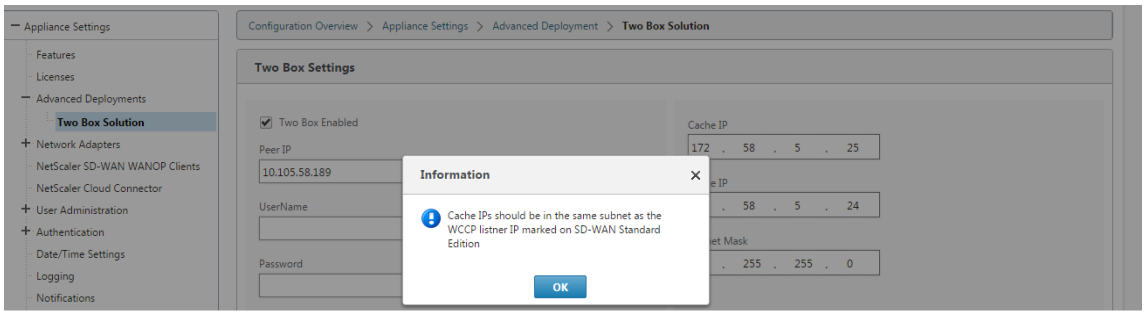
Citrix SD-WAN WANOP-Konfiguration

So konfigurieren Sie den Zwei-Box-Bereitstellungsmodus in der Web-GUI der SD-WAN WANOP Appliance:

1. Wechseln Sie in der SD-WAN WANOP-Webverwaltungsoberfläche zu **Konfiguration** > **Appliance-Einstellungen** > **Erweiterte Bereitstellungen** > **Zwei-Box-Lösung**.



2. Klicken Sie auf das Symbol **Bearbeiten**, um die beiden Box-Modus-Einstellungen zu bearbeiten. Das Informationsdialogfeld 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 Benutzeranmeldedaten ein und klicken Sie auf **Übernehmen**.

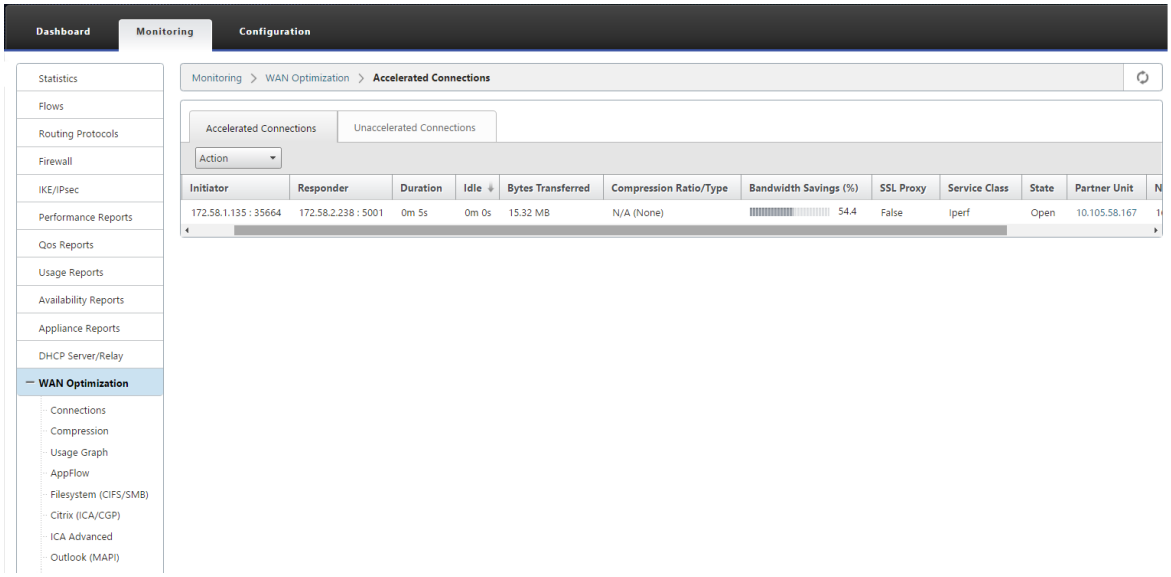
Konfiguration und Verwaltbarkeit im Zwei-Box-Modus

Im Folgenden sind einige der beiden Konfigurations- und Verwaltbarkeitspunkte im Box-Modus aufgeführt, die für die Bereitstellung zu berücksichtigen sind

- Die unten genannten SD-WAN WANOP-Konfigurationen können über den SD-WAN SE-Konfigurationseditor als einheitlicher Bereich konfiguriert werden
  - SERVICE CLASS
  - APPLICATION CLASSIFIER
  - FEATURES
  - SYSTEM TUNING

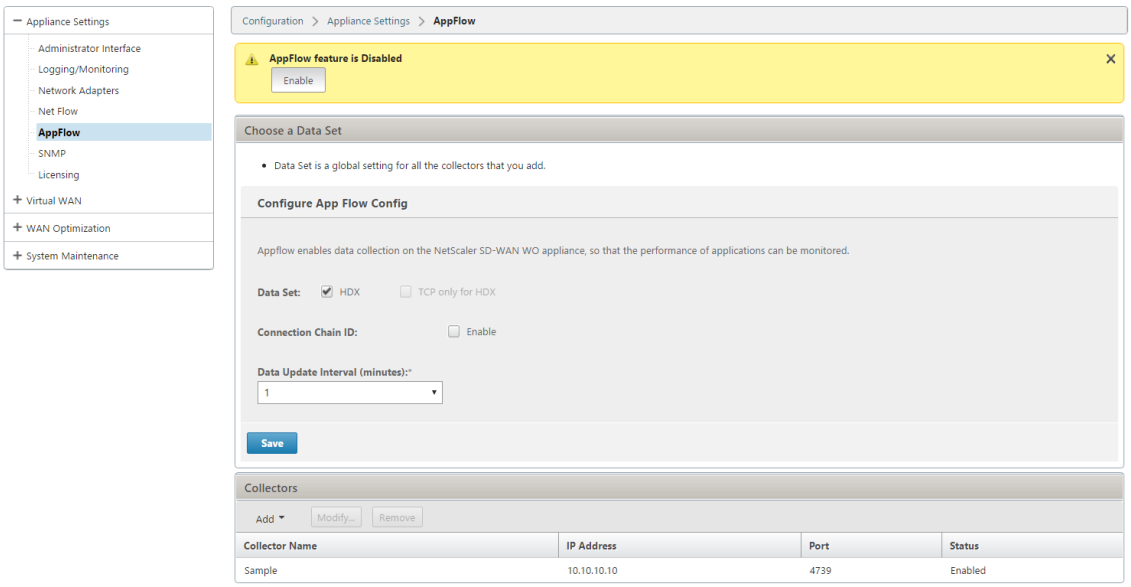
Überwachen

Sie können den SD-WAN WANOP-Verkehr direkt über die Überwachungsseite der Web-UI 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, die Details des sicheren Partners usw. unter dem Knoten WAN-Optimierung in der SDWAN-SE-Benutzeroberfläche anzeigen.



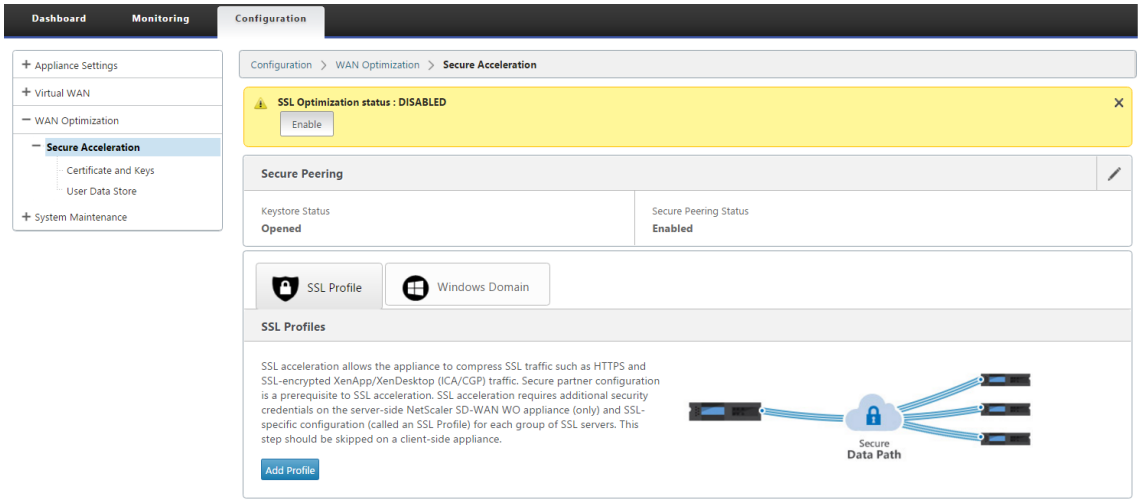
Konfiguration

Sie können APPFLOW direkt von der SDWAN-SE-**Konfigurationsseite** unter dem **APPFLOW**-Knoten konfigurieren. Auf diese Weise kann SDWAN-SE als ein einziger Bereich für die Konfiguration von APPFLOW und anderen Datenverarbeitungskonfigurationsattributen wie Service Class, Application Classifiers fungieren. Die Konfiguration auf dem SDWAN-SE spiegelt die SDWAN-WO-Konfiguration wider und behält die nahtlose Unterstützung der APPFLOW-Funktionalität bei.



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 Verkehrsverarbeitung 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 bei der Aufrechterhaltung eines einzigen Konfigurationsbereichs von Konfigurationen wie Domain Join oder Secure Acceleration/SSL-Profilerstellung für erweiterte Optimierungen oder SSL-Proxy.



- Die Lizenzierung sollte für jede SD-WAN SE- und SD-WAN WANOP-Appliance separat verwaltet werden.
- Das Software-Upgrade sollte für jede der SD-WAN SE- und SD-WAN WANOP-Appliances mit den jeweiligen Softwarepaketen separat verwaltet werden. Zum Beispiel tar.gz für SD-WAN SE und Upgrade-Upg für SD-WAN WANOP.
- Die Datenpfadintegration sollte zwischen SD-WAN SE und externen WANOP-Appliances über den WCCP-Bereitstellungsmodus konfiguriert werden.
  - Auf Datenpfadebene 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

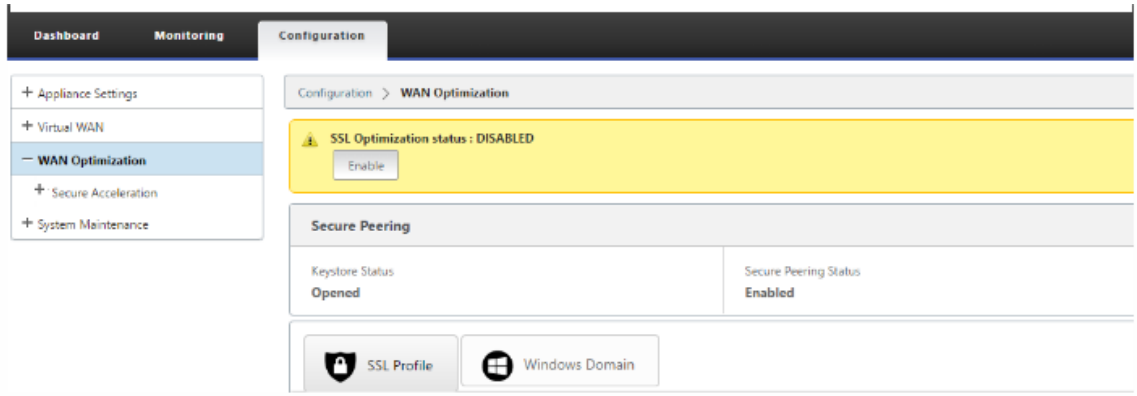
Wenn Sie den Zwei-Box-Modus mit SD-WAN SE und SDWAN-WANOP-Appliances aktivieren, können Sie die Konfiguration in der SD-WAN SE-Appliance ähnlich anzeigen, wie Sie zwei Box-Konfigurationen mit der SD-WAN-EE-Appliance anzeigen können.

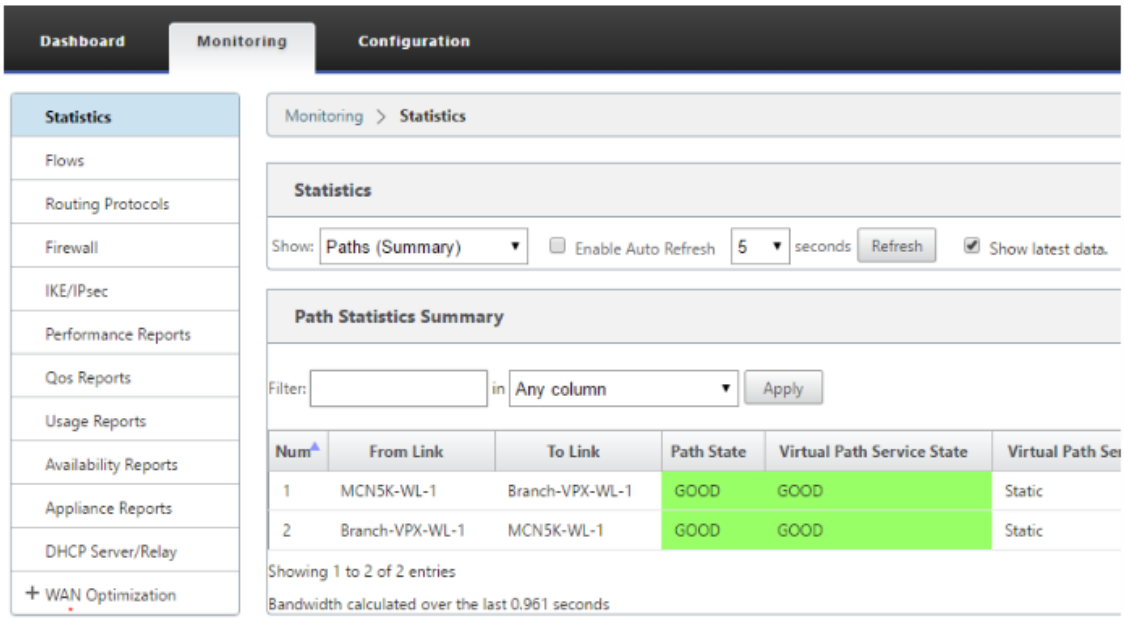
1. Gehe zu **Konfiguration** > **Virtuelles WAN** > **WAN-Optimierung**
2. Appflow-Knoten unter **Konfiguration** > **Appliance-Einstellungen**
3. WAN-Optimierungsknoten unter Konfiguration.

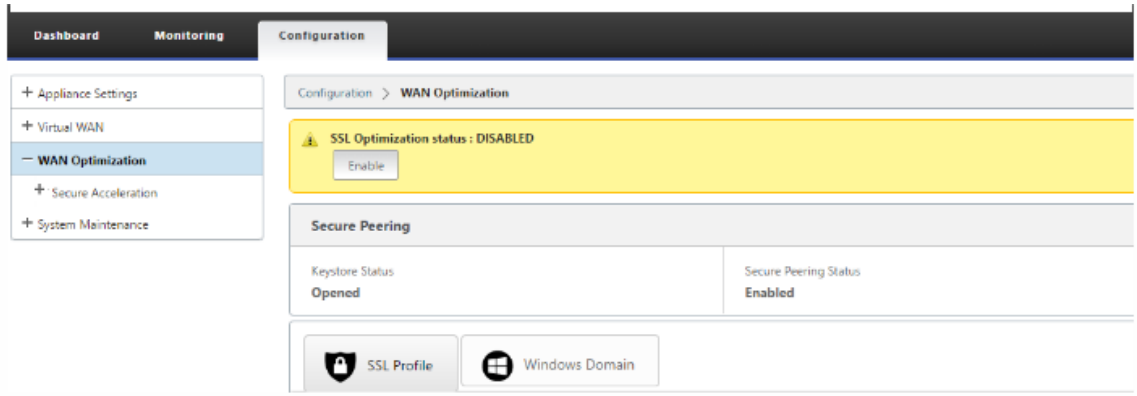
Diese Informationen werden von der SD-WAN WANOP-Appliance umgeleitet, die sich mit der SD-WAN SE-Appliance im Zwei-Box-Modus befindet.

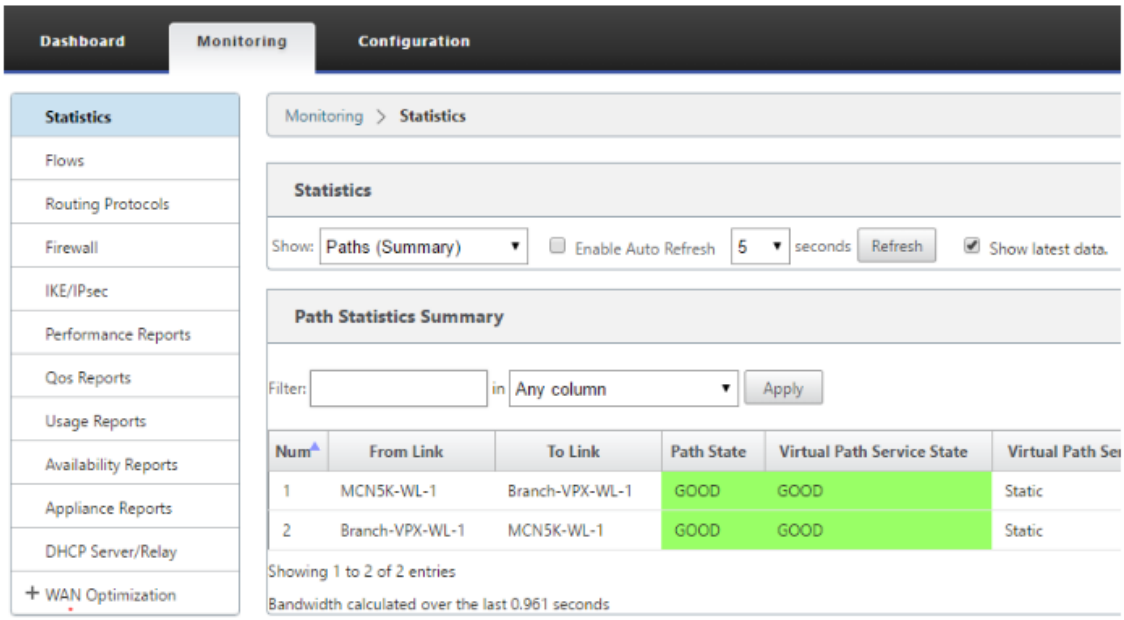
Konfigurationen im Zusammenhang mit WANOP, wie SSL Acceleration und AppFlow können nun von der SD-WAN SE Web-GUI durchgeführt werden.

Verkehrsbezogene Statistiken wie Verbindungen, Komprimierung, CIFS/SMB, ICA Advanced, MAPI und Partner können jetzt über die SD-WAN SE-Web-GUI unter **Überwachung** > **WAN-Optimierung** überwacht werden, ähnlich der SD-WAN Premium (Enterprise) Edition-Appliance.









Änderung der Verwaltungs-IP-Adresse für 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 auf den Seiten der URL-Umleitung angezeigt.

Die Management-IP-Adresse wird für die Konfiguration von Peer-IP-Adressen verwendet.

Deaktivieren Sie den Zwei-Box-Modus auf SD-WAN WANOP-Einheit

So deaktivieren oder entkoppeln Sie die SD-WAN WANOP- und SD-WAN SE-Appliances vom 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_sync*aus.

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**:

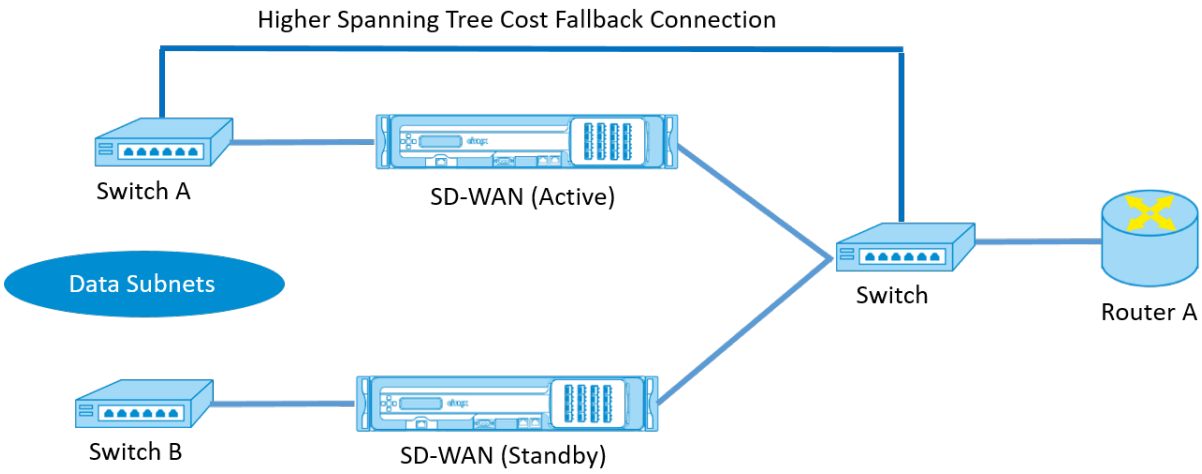
  Der aktive Datenverkehr fließt auch dann, wenn der virtuelle Pfad ausgefallen ist, solange eine der SD-WAN-Appliances aktiv ist. Die SD-WAN-Appliance leitet den Datenverkehr als Intranetverkehr zurück an den Router um. Wenn jedoch beide aktive/Standby-SD-WAN-Appliances inaktiv werden, versucht der Router, 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:

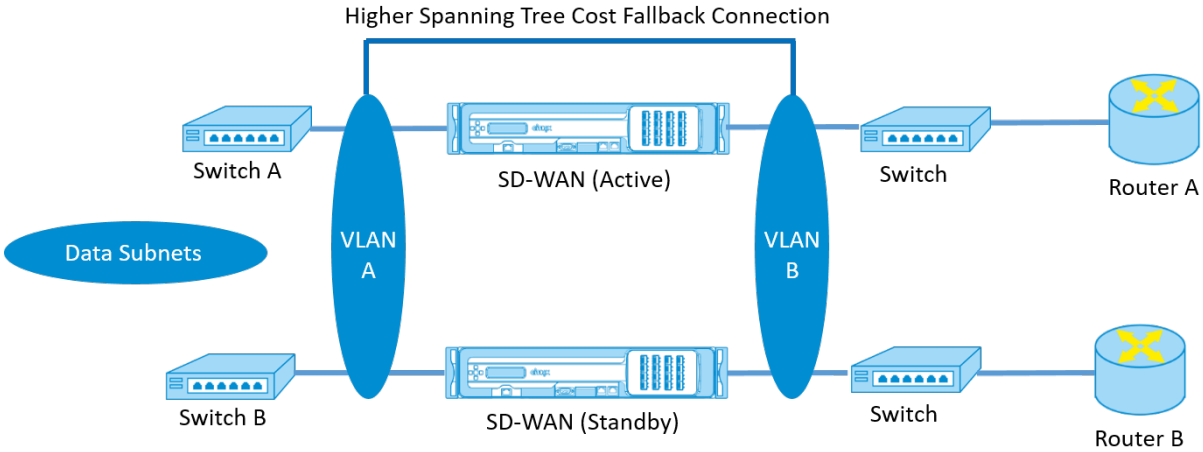
Im parallelen Inline-Hochverfügbarkeitsmodus werden die SD-WAN-Appliances inline mit dem Datenpfad nebeneinander bereitgestellt. Es wird nur ein Pfad durch die Active Appliance verwendet. Es ist wichtig zu beachten, dass Bypass-Schnittstellengruppen so konfiguriert sind, dass sie Failto-Block sind, um 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:

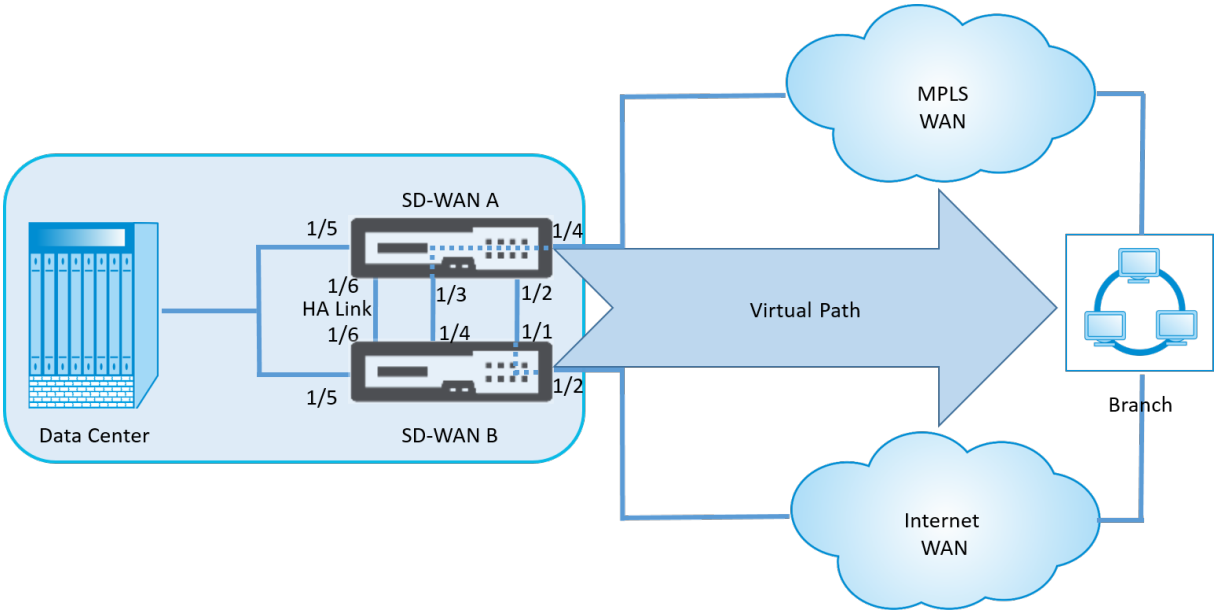
Im Fail-to-Wire-Modus befinden sich die SD-WAN-Appliances im selben Datenpfad. Die Bypass-Schnittstellengruppen müssen sich im Fail-to-Wire-Modus befinden, wobei sich die Standby-Appliance im Passthrough- oder Bypass-Status befindet. Für die hochverfügbare Schnittstellengruppe muss eine direkte Verbindung 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.



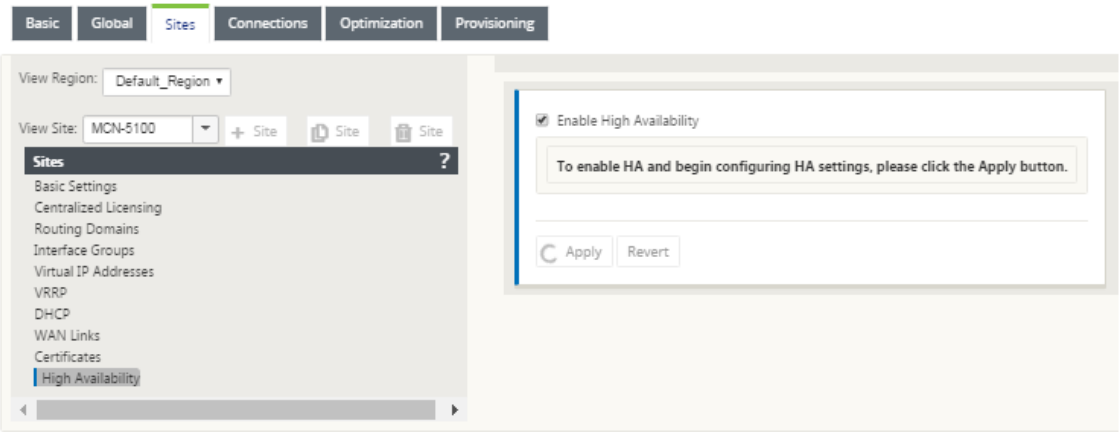
Die Einarm-Hochverfügbarkeitskonfiguration oder die Parallele Inline-Hochverfügbarkeitskonfiguration wird für Rechenzentren oder Sites empfohlen, die ein hohes Datenvolumen weiterleiten, um Unterbrechungen während des Failovers zu minimieren.

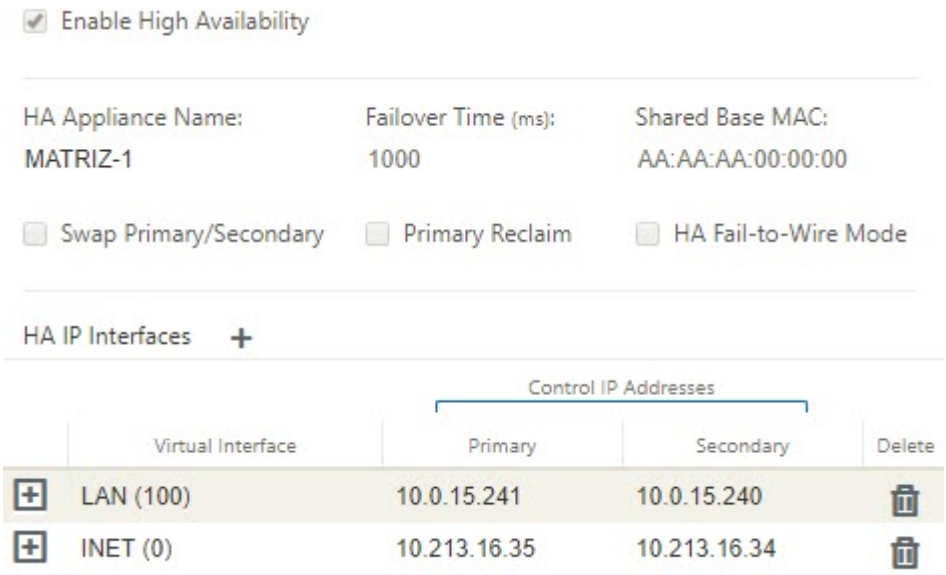
Wenn während eines Failovers ein minimaler Service-Verlust akzeptabel ist, ist der Fail-to-Wire-Hochverfügbarkeitsmodus eine bessere Lösung. Der Fail-to-Wire-Hochverfügbarkeitsmodus schützt vor Ausfällen der Appliance und die parallele Inline-Hochverfügbarkeit schützt vor allen Ausfällen. In allen Szenarien 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**.





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

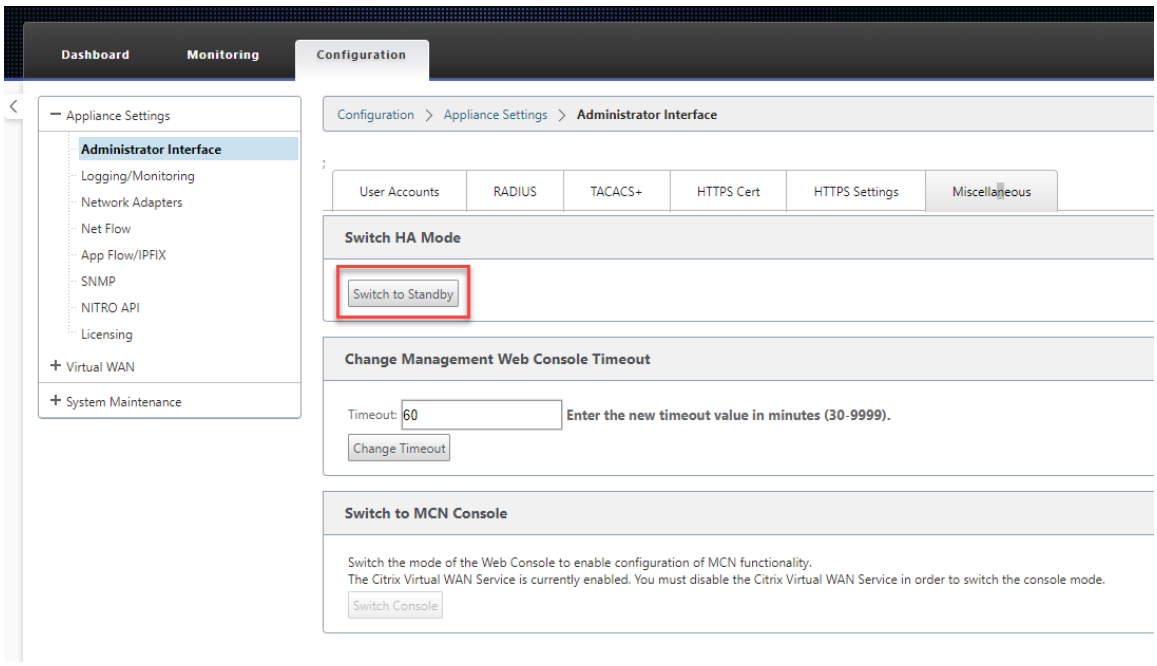
> **Hinweis**
>
> Für Hypervisor- und Cloud-basierte Plattformen wählen Sie die Option **Shared Base MAC** deaktivieren, um die gemeinsam genutzte virtuelle MAC-Adresse zu deaktivieren.
>
> Stellen Siefür Hypervisor basierte Plattformen sicher, dass der Promiscuous-Modus auf den Hypervisoren aktiviert 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**.

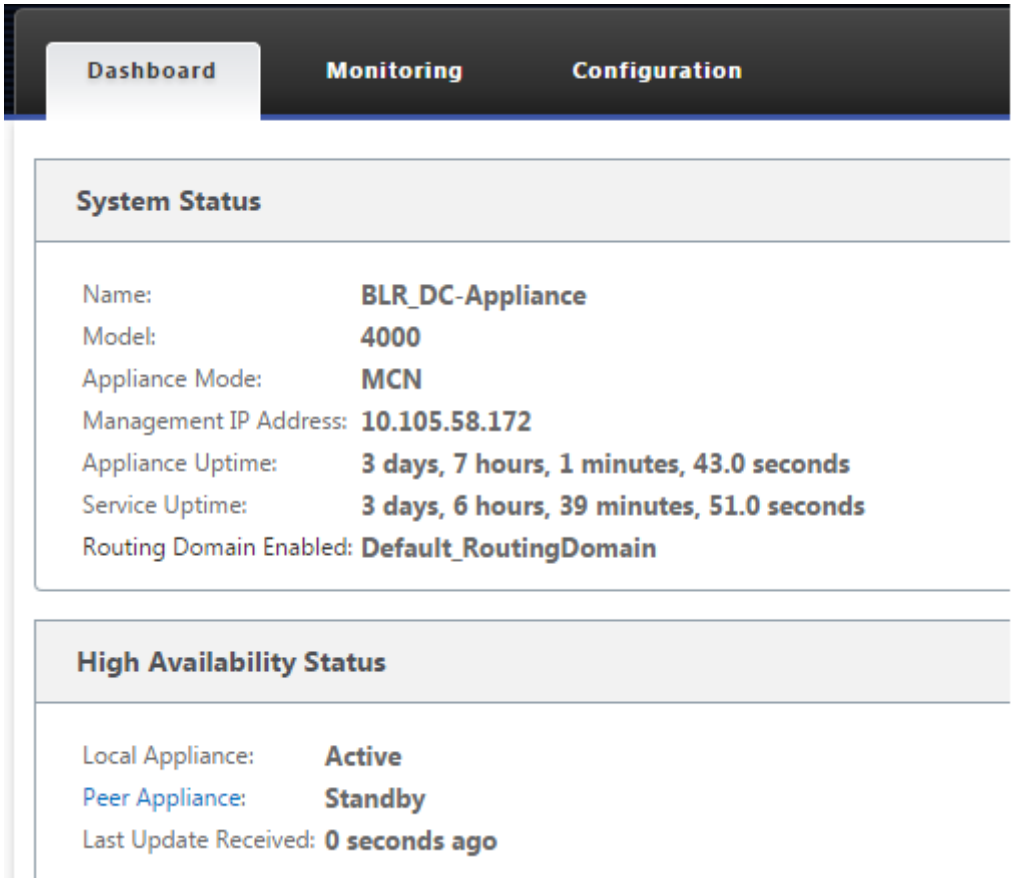
> **Hinweis:**
>
> Sie können eine HA-Umschaltung auch manuell von der Appliance aus auslösen. Navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Administratorschnittstelle** > **Verschiedenes**. Klicken Sie im Abschnitt HA-Modus **wechseln je nach HA-Appliance auf In Standbywechseln oder Zu Aktiv** wechseln.

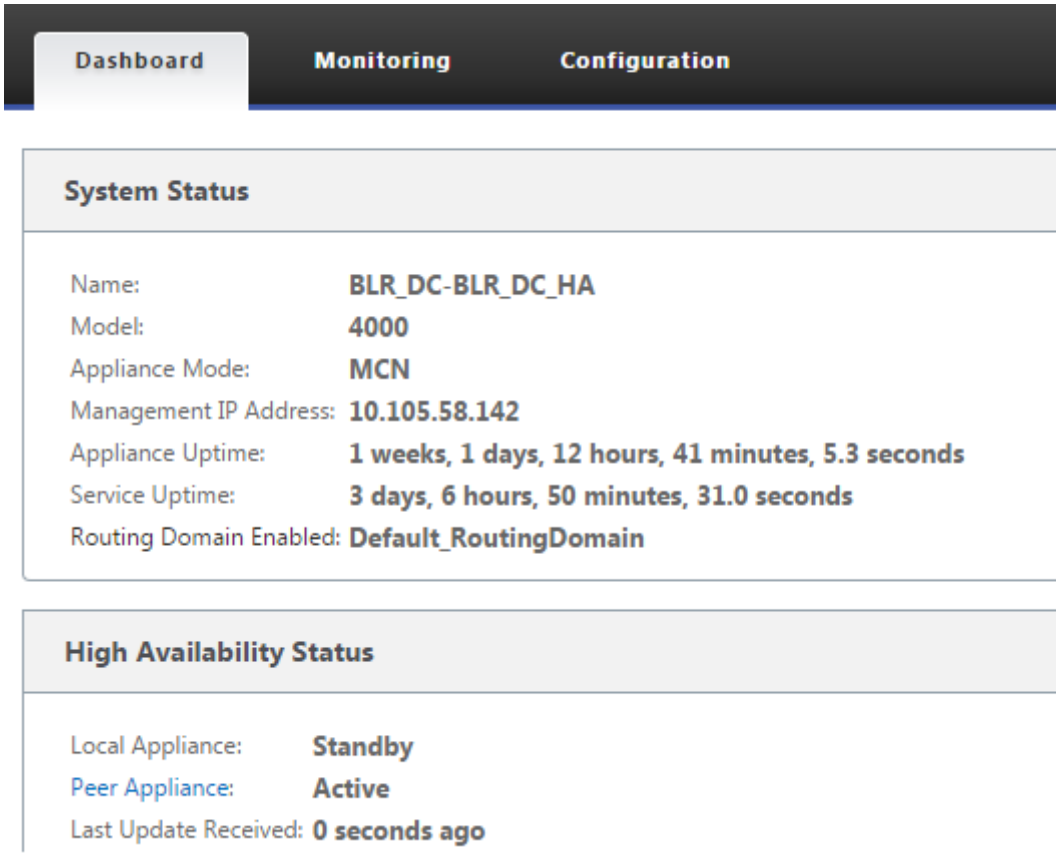


Überwachen

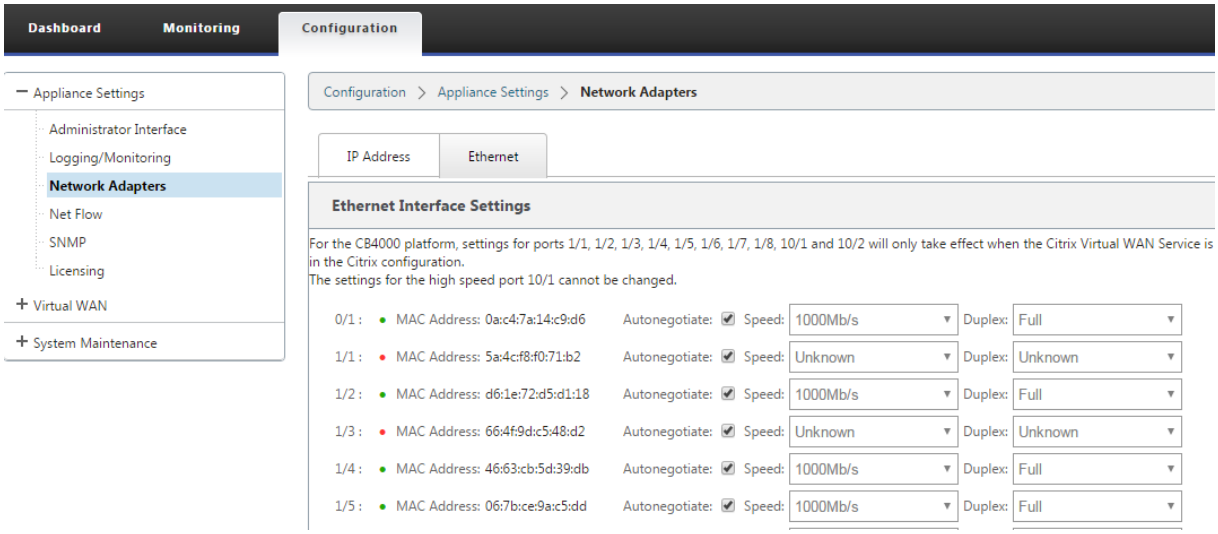
So überwachen Sie die Konfiguration mit hoher Verfügbarkeit:

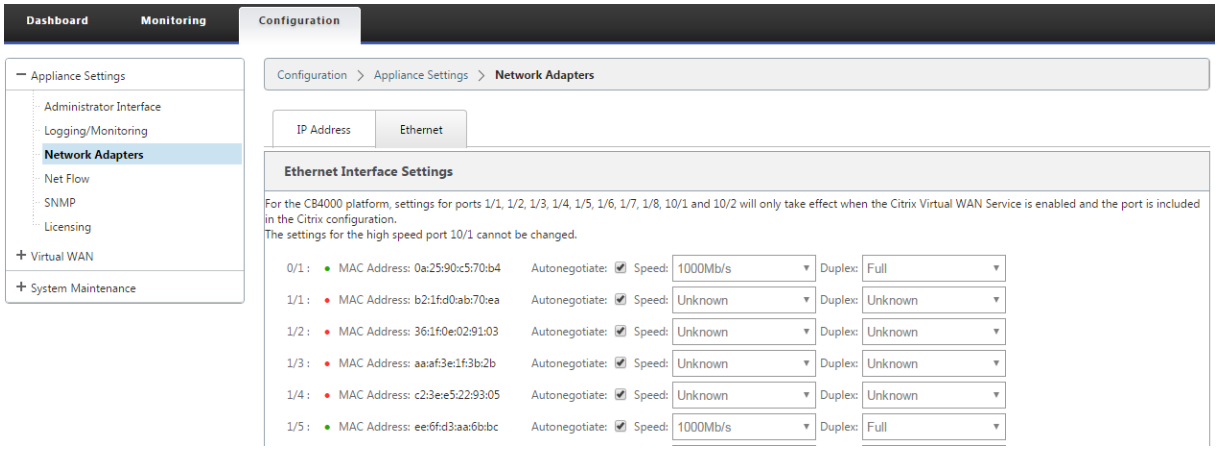
Melden Sie sich bei der SD-WAN-Webverwaltungsschnittstelle für die Active und Standby-Appliance an, für die eine hohe Verfügbarkeit implementiert ist. Zeigen Sie den Status der hohen Verfügbarkeit auf der Registerkarte **Dashboard** an.





Informationen zu Netzwerkadaptern zu Active und Standby-Hochverfügbarkeits-Appliances finden Sie unter **Konfiguration** > **Einheiteneinstellungen** > **Netzwerkadapter** > **Ethernet**.





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 **racp**protokolliert.

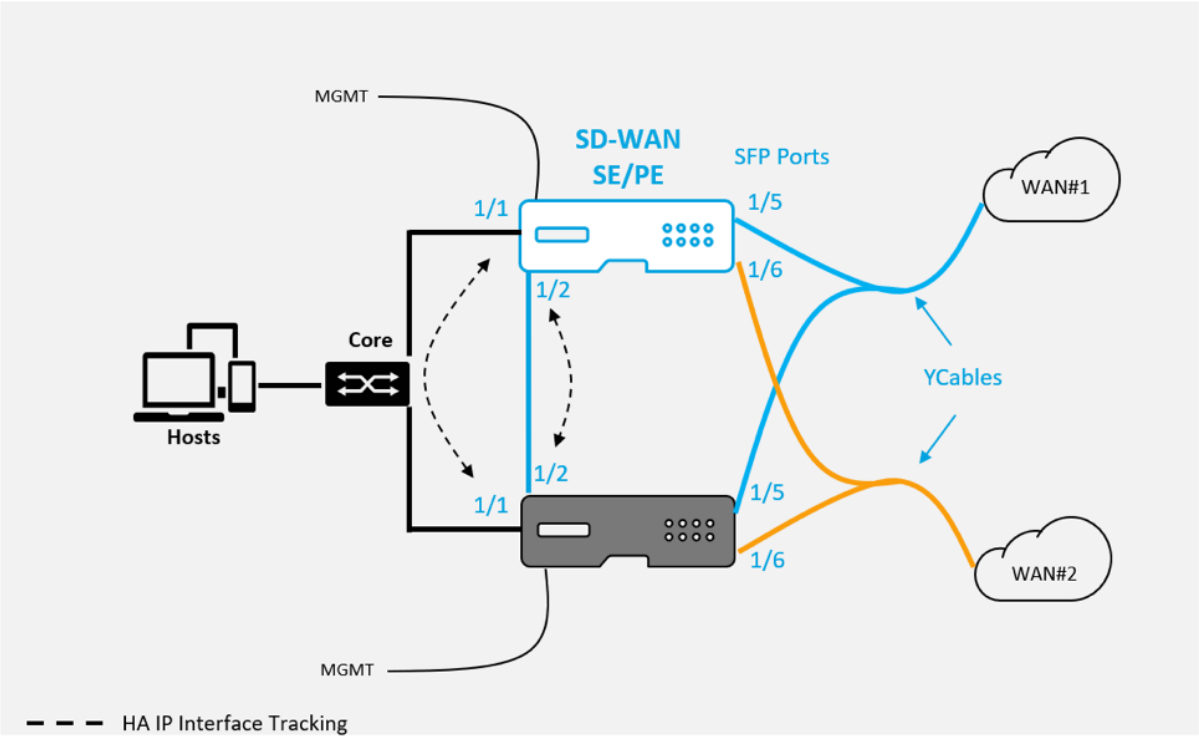
3. Sie können die portbezogenen Ereignisse in der Datei **SDWAN_common.log** überprüfen (z. B. gehen die HA-fähigen Ports aus oder nach oben).
4. Bei jeder HA-Statusänderung wird ein SD-WAN-Ereignis protokolliert. Wenn also die Protokolle überrollt werden, können Sie die Ereignisprotokolle überprüfen, 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 Funktion nur für die 1100 SE/PE-Appliance anwendbar.

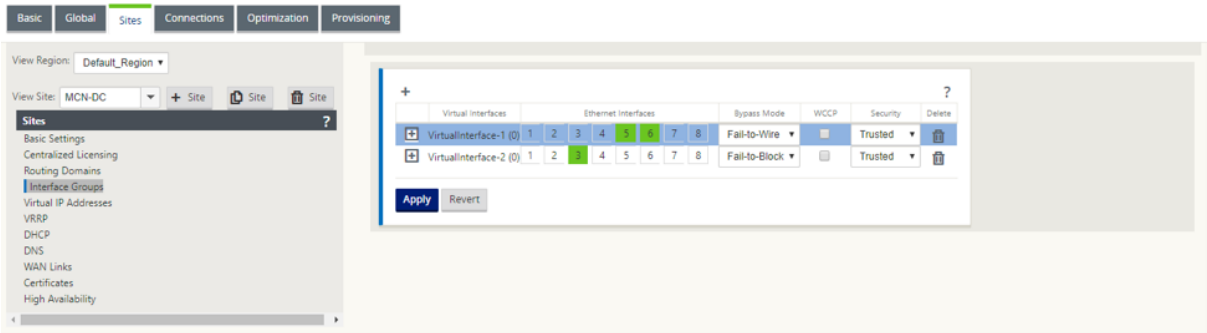
Das folgende Verfahren beschreibt die Schritte zum Aktivieren von Hochverfügbarkeit (HA) auf 1100 SE/PE-Appliances, die im Edge-Modus bereitgestellt werden, wobei die Übergaben der WAN-Verbindungsdienstanbieter Glasfaser sind.
Die verfügbaren Small Form-Factor Pluggable (SFP) -Ports an 1100-Geräten können mit Glasfaser-Y-Kabeln verwendet werden, um eine Hochverfügbarkeitsfunktion für die Bereitstellung im Edge-Modus zu ermöglichen.
Auf der 1100 SE/PE-Einheit verbindet das Splitterkabel mit Glasfaseranschlüssen von zwei 1100 Einheiten, die im HA-Paar konfiguriert sind.
Das Glasfaser-Y-Kabel hat drei Enden. Ein Ende ist mit der Glasfaserübergabe des Anbieters verbunden, 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 aufzuteilen.



Voraussetzungen:

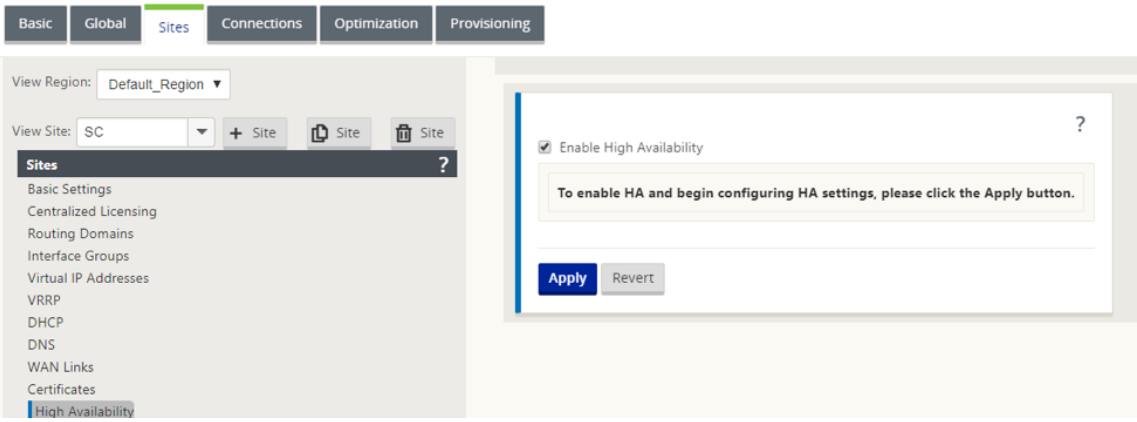
1. Auf der 1100 SE/PE-Appliance sind die Ports 1/5 und 1/6 SFP-Ports. Verbinden Sie die Splitterenden des Y-Kabels mit einem dieser Ports an beiden Geräten im HA-Paar, siehe 1100 SE für weitere Informationen.
2. Fügen Sie der SD-WAN-Appliance-Konfiguration SFP-Ports hinzu. Die Konfiguration der SFP-Ports 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.

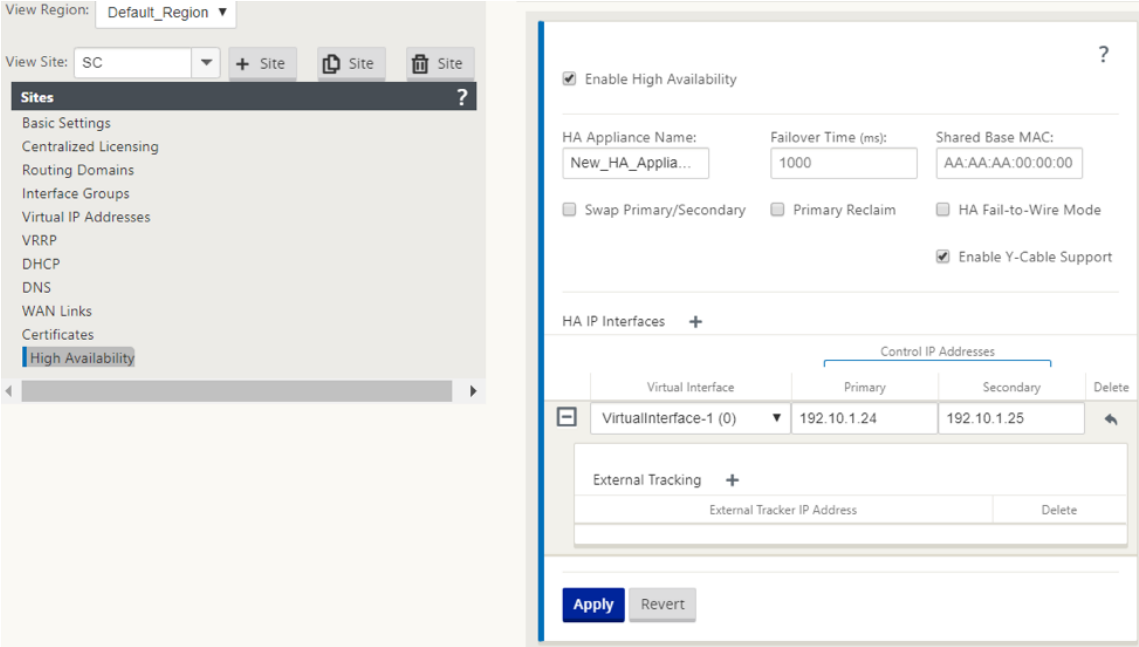


So aktivieren Sie Hochverfügbarkeit mit Y-Kabel:

1. Navigieren Sie in der GUI der 1100 SE/PE-Einheit zu **Konfiguration > Virtuelles WAN > Konfigurationseditor > Sites**. Klicken Sie auf **Hochverfügbarkeit aktivieren**.



2. Klicken Sie auf **Y-Kabelunterstützung aktivieren**.
3. Fügen Sie HA-IP-Schnittstellen hinzu, die neben den an die Y-Kabel angeschlossenen Schnittstellen eine andere Schnittstelle verwenden (z. B. 1/1 LAN-Schnittstelle oder 1/2 direkt angeschlossene Schnittstellen). 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:

- Die Konfiguration des HA-Fail-to-Wire-Modus 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 cloudbasierter 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. Der Zugriff auf den Cloud-Dienst für die Zero-Touch-Bereitstellung erfolgt über das SSL-Protokoll (Secure Socket Layer).

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 alle Zero Touch-Bereitstellungsanfragen zu authentifizieren und die Zuordnung zwischen dem Kundenkonto und den Seriennummern von Citrix SD-WAN-Appliances ordnungsgemäß zu überprüfen.

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.)

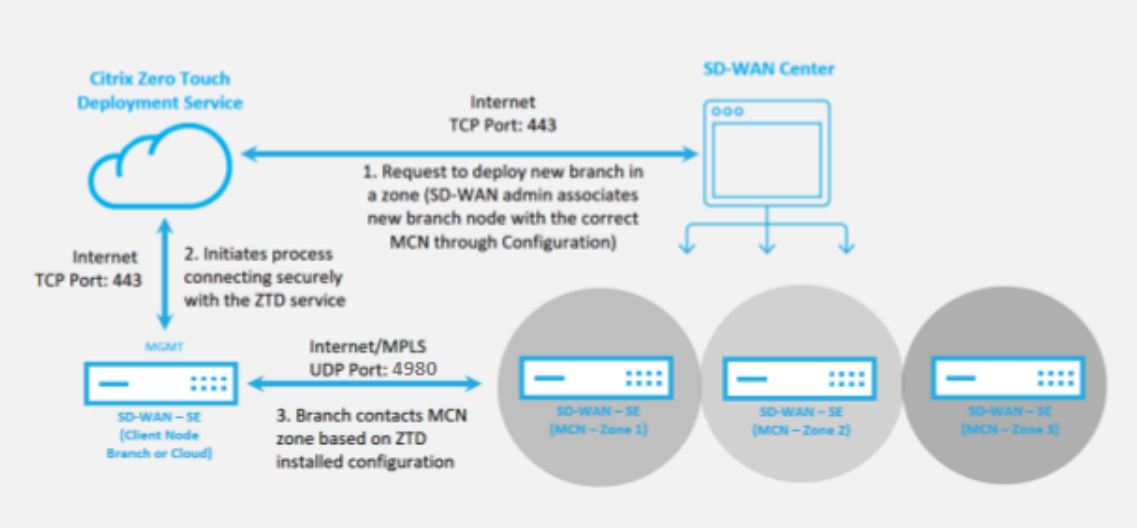
- Konfigurieren Sie ggf. Firewalls für die ausgehende Kommunikation mit dem FQDN ***sd-wanzt.citrixnetworkapi.net*** vom SD-WAN Center.

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.

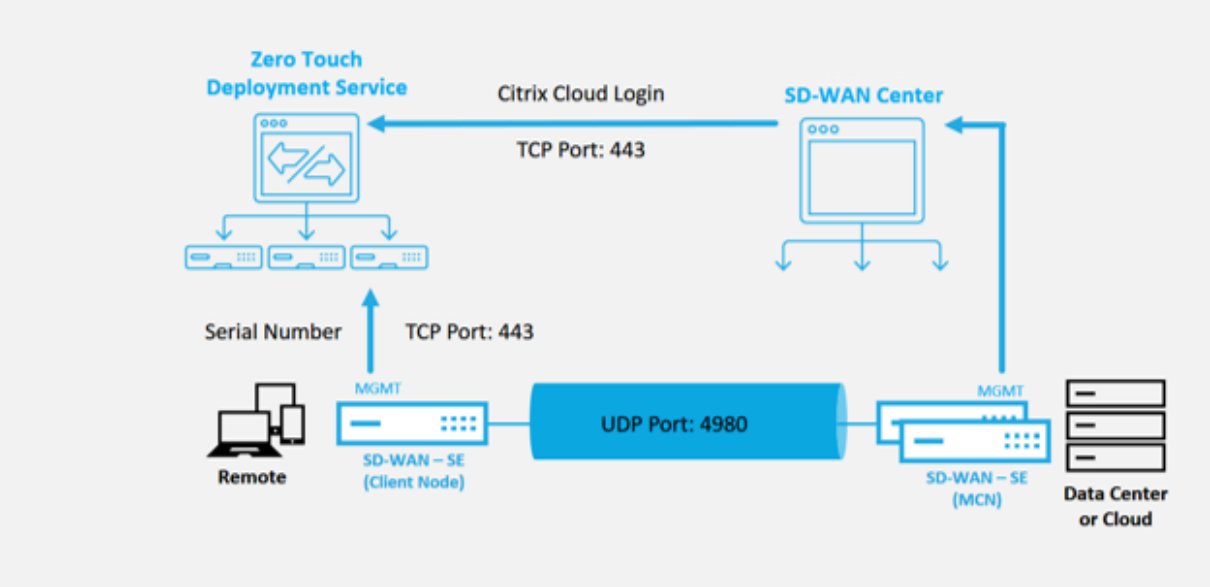


Die folgenden Voraussetzungen sind erforderlich, bevor Sie einen Zero Touch-Bereitstellungsdienst starten:

- 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).

- Verwaltungsnetzwerkkonnektivität (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 Unterlagernetzwerk 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, haben Sie die Möglichkeit, die für die Zero-Touch-Bereitstellung zu verwendende Appliance vorab zu authentifizieren, indem Sie die Seriennummer vorab ausfüllen und die E-Mail-Kommunikation mit dem Installationsprogramm vor Ort initiieren, 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.

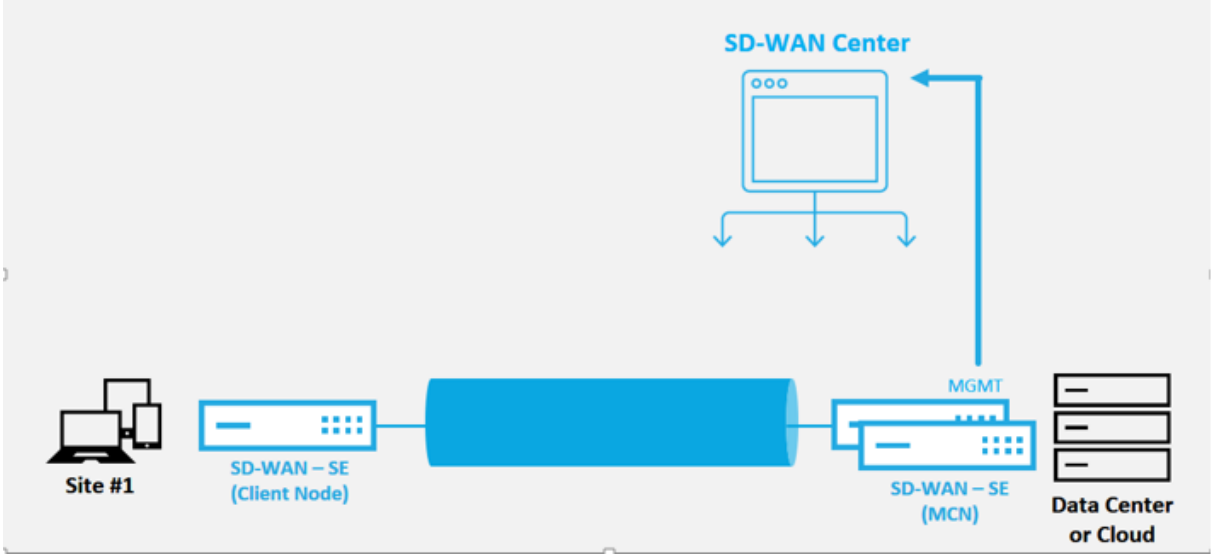
- Schieben Sie alle fehlenden SD-WAN-Softwarekomponenten oder erforderlichen Updates auf die Zweigeinheit.
- Push einer temporären 10-Mbit/s-Lizenzdatei zum Bestätigen der Herstellung virtueller Pfade zur Zweigstellenappliance.
- Aktivieren Sie den SD-WAN-Dienst auf der Zweigeinheit.

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-Bereitstellungsgeräteverfahren

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

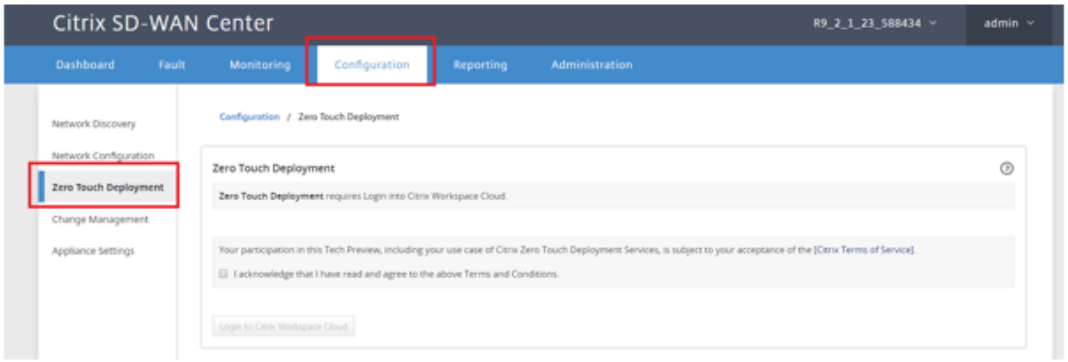
Das SD-WAN-Center verfügt über die Funktionalität, um Anforderungen von neu verbundenen Appliances zu akzeptieren, um dem SD-WAN Enterprise-Netzwerk beizutreten. Die Anforderung wird über den Zero-Touch-Bereitstellungsdienst an das Webinterface weitergeleitet. Sobald die Appliance eine Verbindung zum Dienst herstellt, werden Konfigurations- und Software-Upgrade-Pakete heruntergeladen.

Konfigurations-Workflow:

- Öffnen Sie **SD-WAN Center** > **Neue Standortkonfiguration erstellen** oder vorhandene Konfiguration importieren 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**.

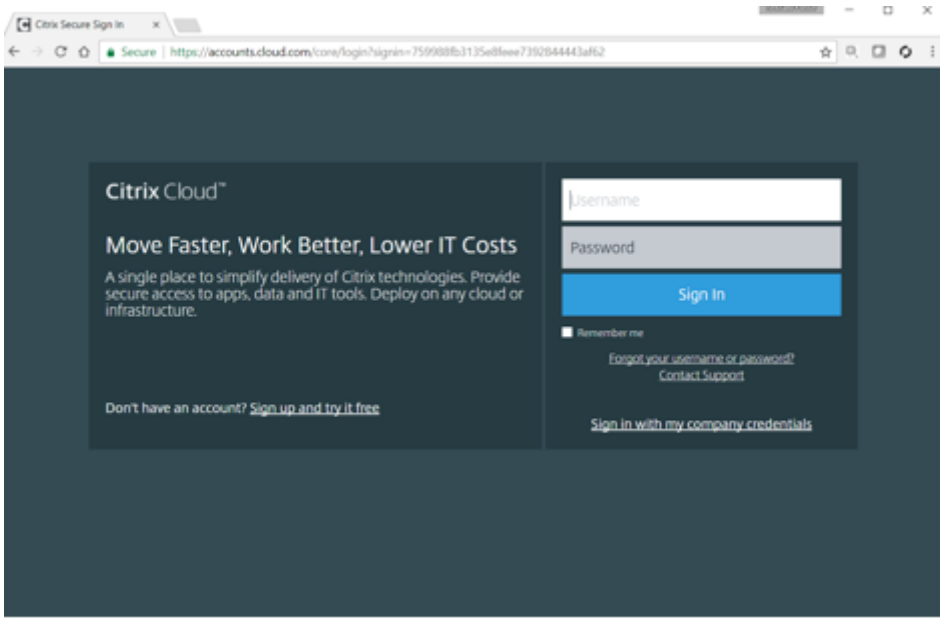
f) Klicken Sie auf die Schaltfläche Bei **Citrix Workspace Cloud anmelden**, wenn bereits ein Citrix Cloud-Konto erstellt wurde.

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)

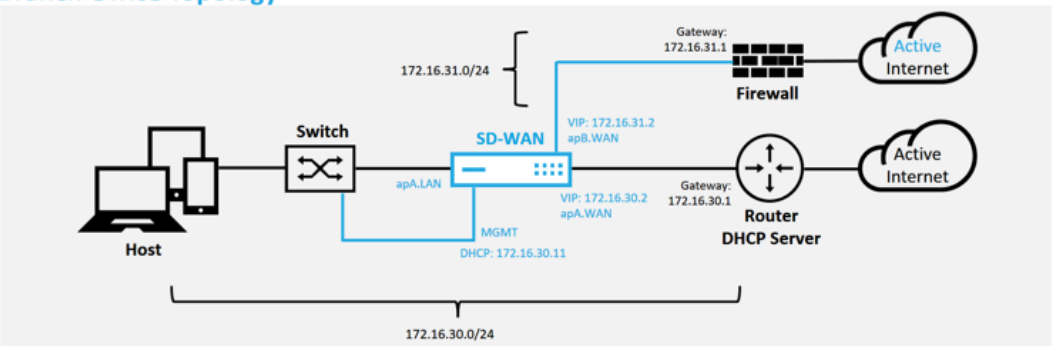
6. Aktualisieren Sie die Konfiguration, um einen **neuen Remote-** Standort mit einer **ZTD-fähigen SD-WAN-Appliance** mithilfe der SD-WAN-Center-Netzwerkkonfiguration hinzuzufügen.

   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 Schnittstellengruppen, 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

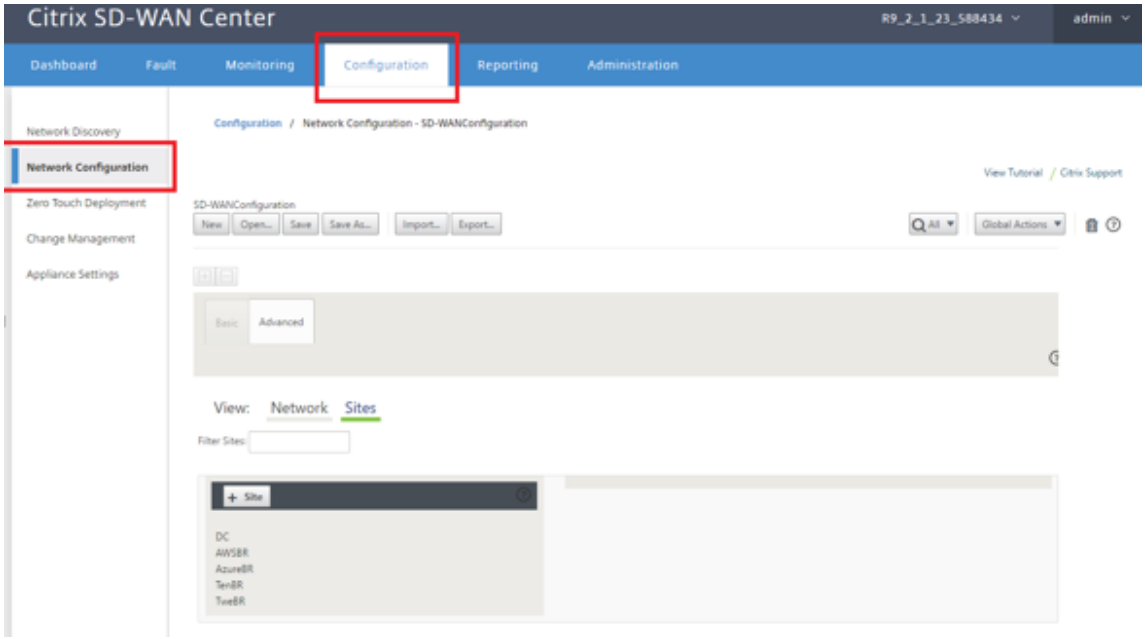
   Branch Office Topology

Dies ist eine Beispielbereitstellung eines Zweigstellenstandorts, die SD-WAN-Appliance wird physisch auf dem Pfad der vorhandenen MPLS-WAN-Verbindung über ein 172.16.30.0/24-Netzwerk bereitgestellt und verwendet eine vorhandene Backup-Verbindung, indem sie in einen aktiven Zustand versetzt und diese zweite WAN-Verbindung direkt in das SD-WAN beendet wird Appliance in einem anderen Subnetz 172.16.31.0/24.

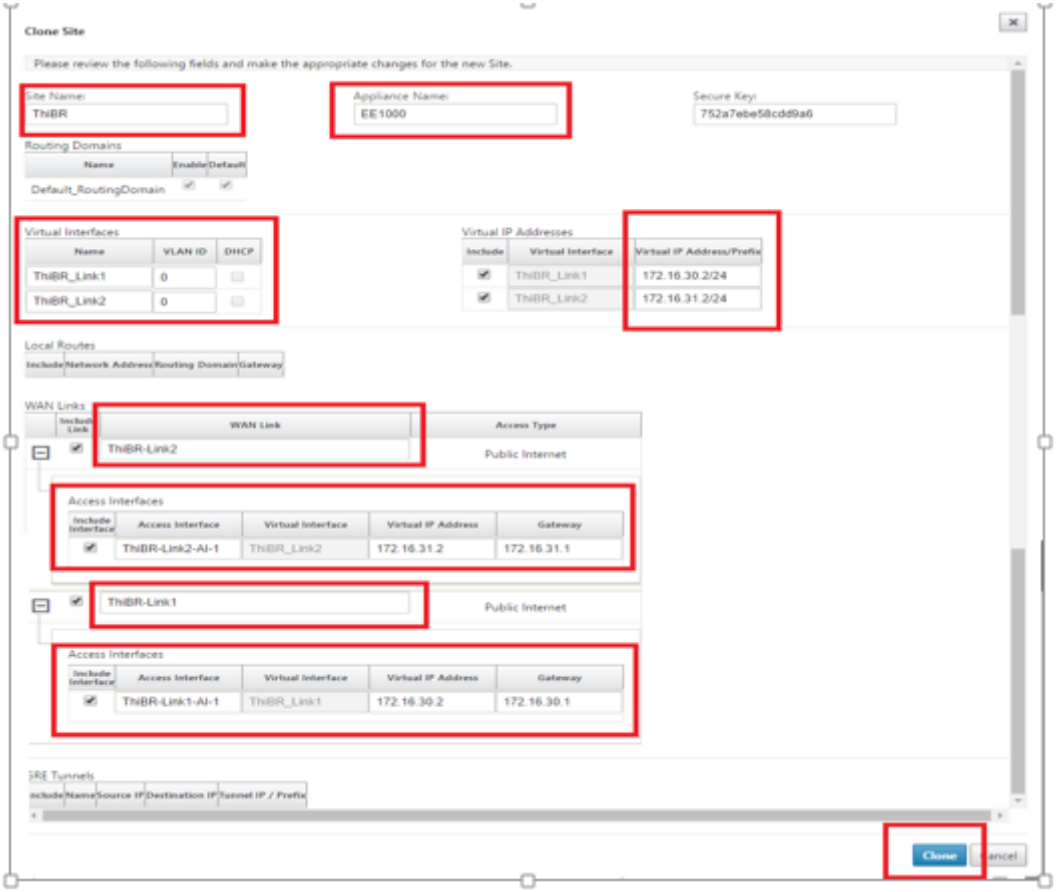
> **Hinweis**
>
> Die SD-WAN-Appliances weisen automatisch eine Standard-IP-Adresse 192.168.100.1/16 zu. Wenn DHCP standardmäßig aktiviert ist, stellt der DHCP-Server im Netzwerk der Appliance möglicherweise eine zweite IP-Adresse in einem Subnetz bereit, das den Standardwert überlappt. Dies kann möglicherweise 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**.

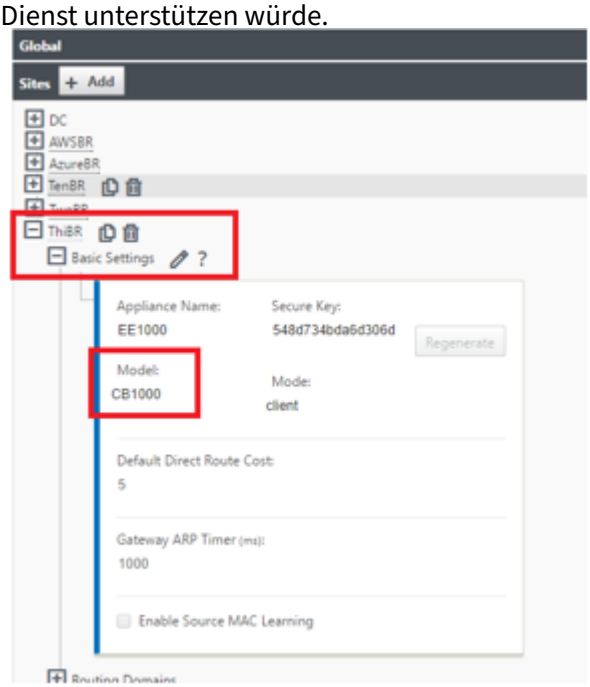


8. Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration vom MCN.
9. Navigieren Sie zur Registerkarte Erweitert, um eine Site zu erstellen.
10. Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.
11. Erstellte 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



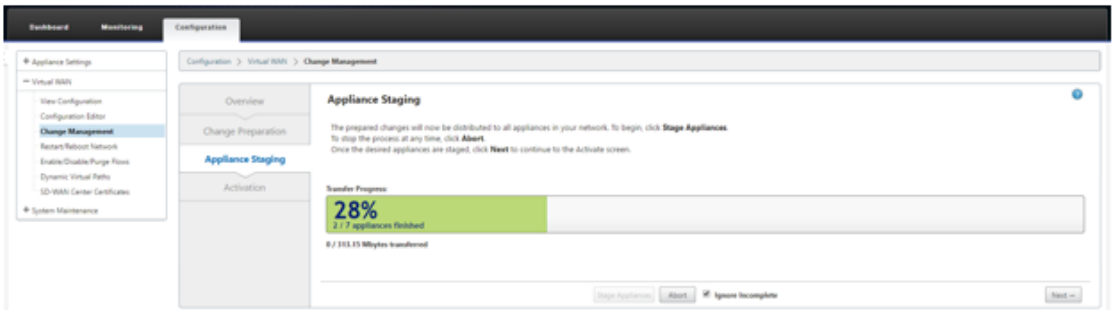
13. Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen**der Site und vergewissern Sie sich, dass das SD-WAN-Modell korrekt ausgewählt ist, das den Zero-Touch-Dienst unterstützen würde.



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.

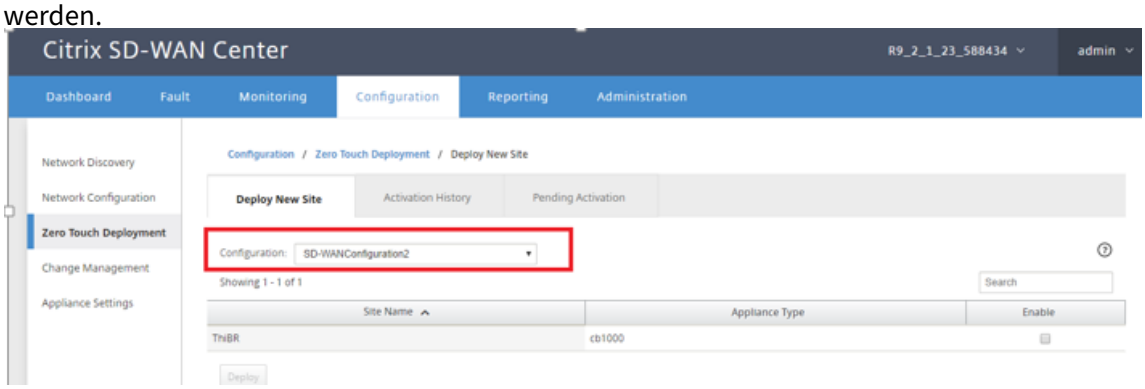
15. Folgen Sie dem Änderungsverwaltungsverfahren, um für die neue Konfiguration ordnungsgemäß ein Staging durchzuführen, wodurch die vorhandenen SD-WAN-Geräte auf die neue Site aufmerksam gemacht werden, die per Zero Touch bereitgestellt werden soll. Sie müssen die Option "Unvollständig ignorieren"verwenden, um den Versuch zu überspringen, die Konfiguration auf die neue Site zu übertragen, die noch den Zero-Touch-Bereitstellungs-Workflow durchlaufen muss.



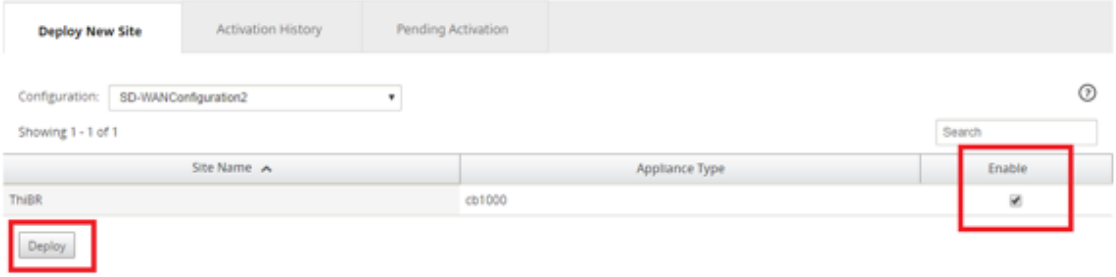
16. Navigieren Sie zurück zur Seite "Zero Touch Deployment"von SD-WAN Center, und wenn die neue aktive Konfiguration ausgeführt wird, steht die neue Site für die Bereitstellung zur Verfügung.

17. Wählen Sie auf der Seite "Zero Touch Deployment"auf der Registerkarte **Neue Site bereitstellen** die laufende Netzwerkkonfigurationsdatei aus

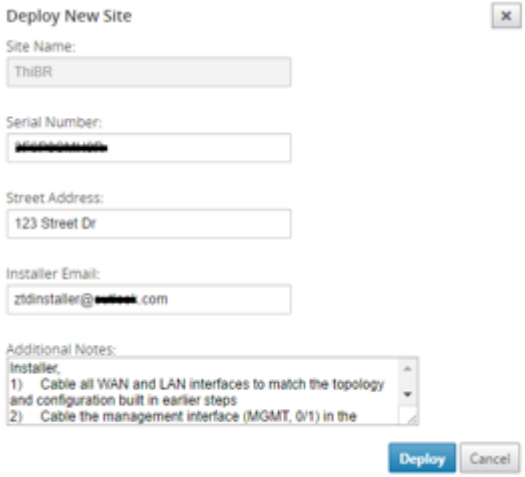
18. Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit nicht bereitgestellten SD-WAN-Geräten angezeigt, die für keine Berührung unterstützt werden.



19. Wählen Sie die Zweigstellen aus, die Sie für den Zero Touch-Dienst konfigurieren möchten, klicken Sie auf **Aktivieren**und dann auf **Bereitstellen**.



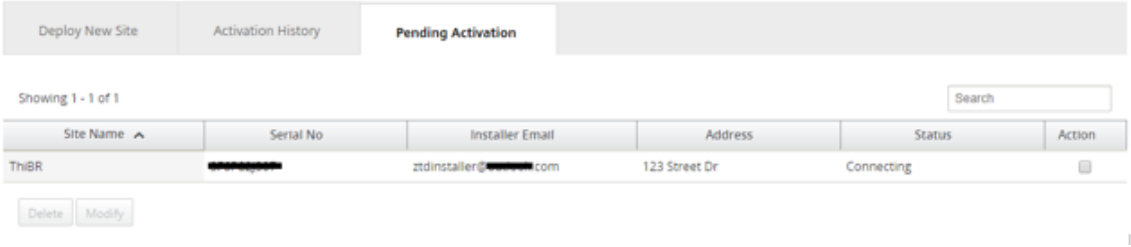
20. Es wird ein Popupfenster Neue Site bereitstellen angezeigt, in dem der Administrator bei Bedarf die Seriennummer, die Straßenadresse der Zweigstelle, die E-Mail-Adresse des Installers und weitere Hinweise angeben kann.



> **Hinweis**
>
> Das Eingabefeld Seriennummer ist optional und führt je nachdem, ob es ausgefüllt ist oder nicht, zu einer Änderung der Vor-Ort-Aktivitäten, für die der Installer 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.

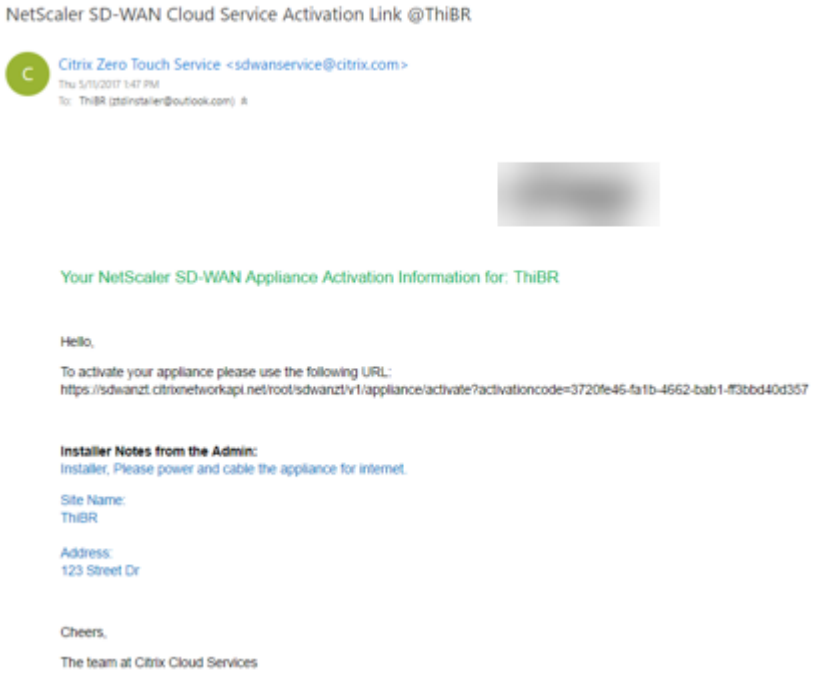
22. Navigieren Sie zur Registerkarte Ausstehende Aktivierung, um zu bestätigen, dass die Informationen der Zweigstandsite-Site erfolgreich ausgefüllt wurden und in den Status der ausstehenden Installationsaktivität versetzt wurden.



> **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.

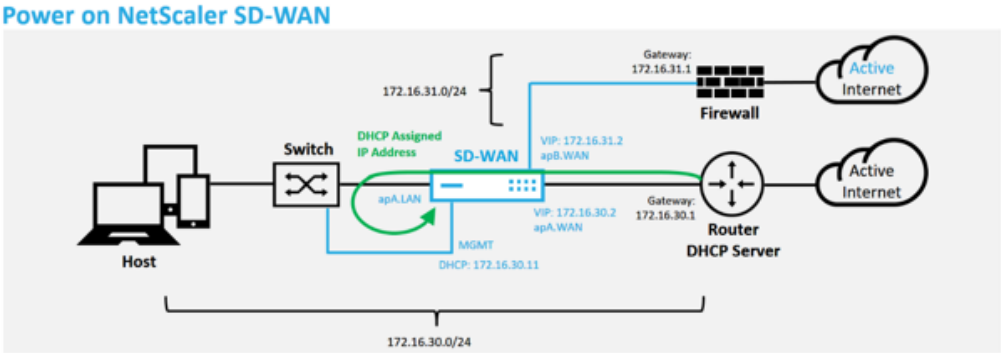
> **Hinweis**
>
> Die meisten Appliances schaltet sich automatisch ein, wenn das Netzkabel angeschlossen ist. Einige Appliance muss möglicherweise über den Netzschalter an der Vorderseite der Appliance eingeschaltet werden, andere haben möglicherweise den Netzschalter auf der Rückseite der Appliance. 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 Zweigeinheit 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.

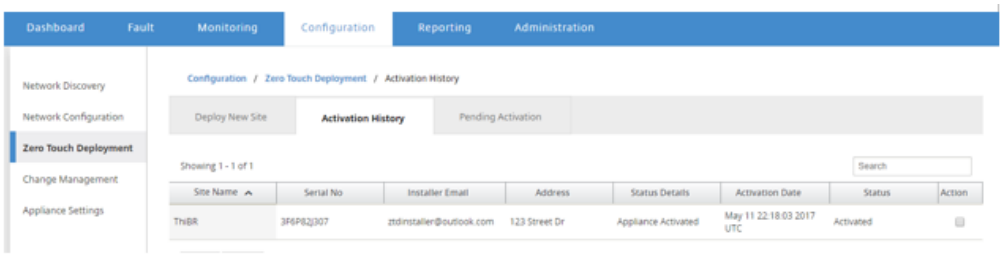
      

      b) Wenn die Appliance die Webverwaltung und die DNS-IP-Adressen vom DHCP-Server des Unterlay-Netzwerkes abruft, initiiert die Appliance den Zero Touch-Bereitstellungsdienst und lädt alle Softwareupdates für die Null-Touch-Bereitstellung herunter.

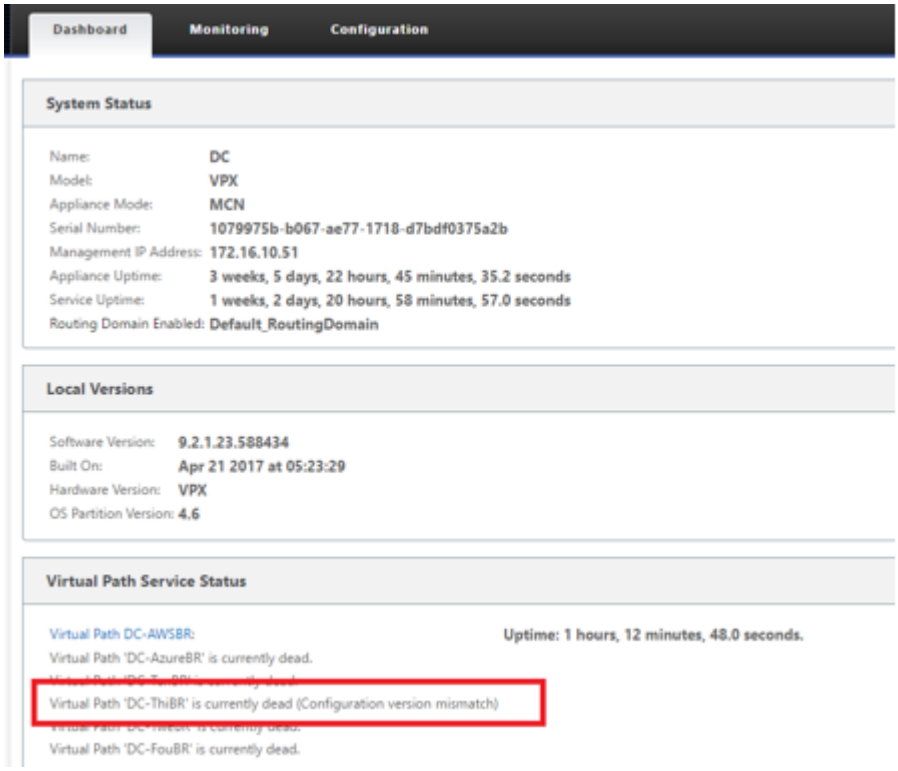
      c) Bei erfolgreicher Konnektivität mit dem Cloud Service für die Zero-Touch-Bereitstellung führt der Bereitstellungsprozess automatisch Folgendes aus:

         - 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**.

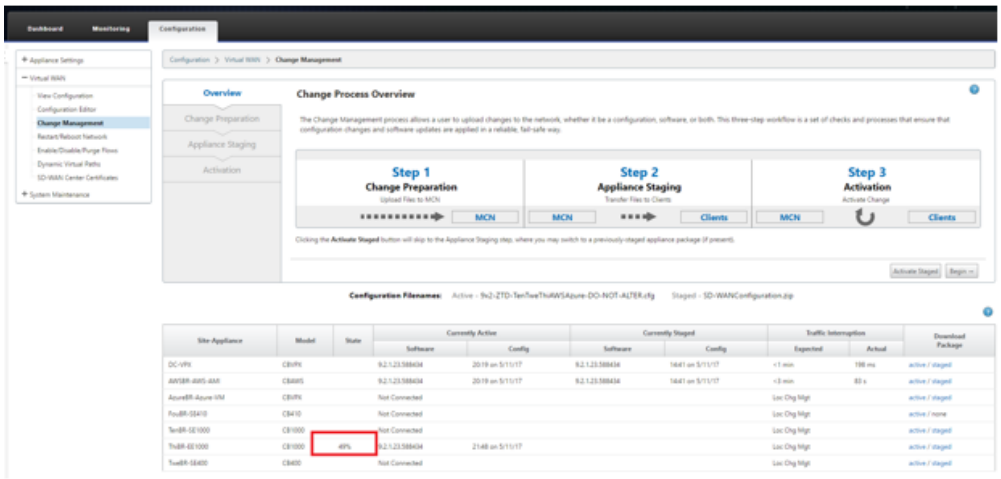


e) Die virtuellen Pfade werden möglicherweise nicht sofort in einem verbundenen Zustand angezeigt, da das MCN der Konfiguration, die vom Clouddienst für die Zero-Touch-Bereitstellung übergeben wurde, nicht vertraut und meldet “Konfigurationsversion nicht übereinstimmen”im MCN-Dashboard.

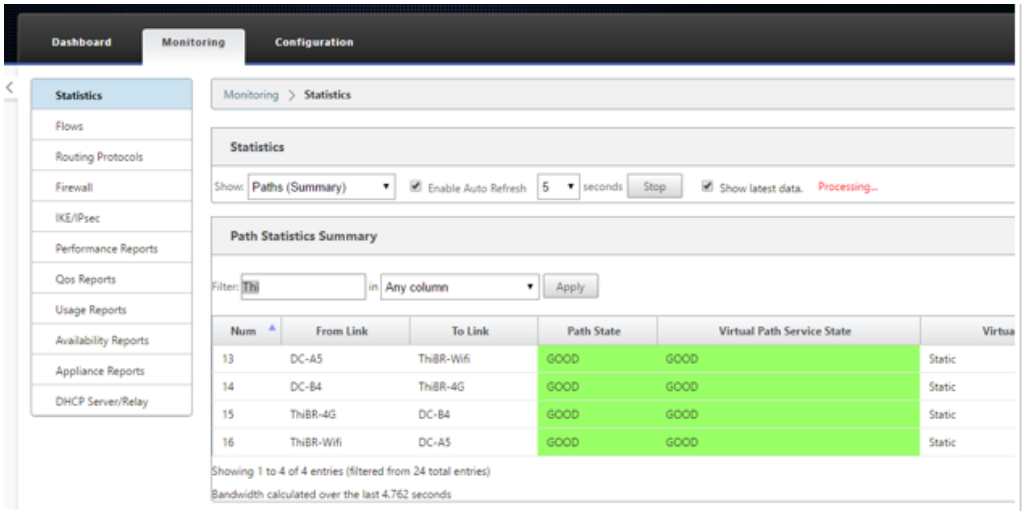


f) Die Konfiguration wird erneut an die neu installierte Zweigstelleneinheit übermit-

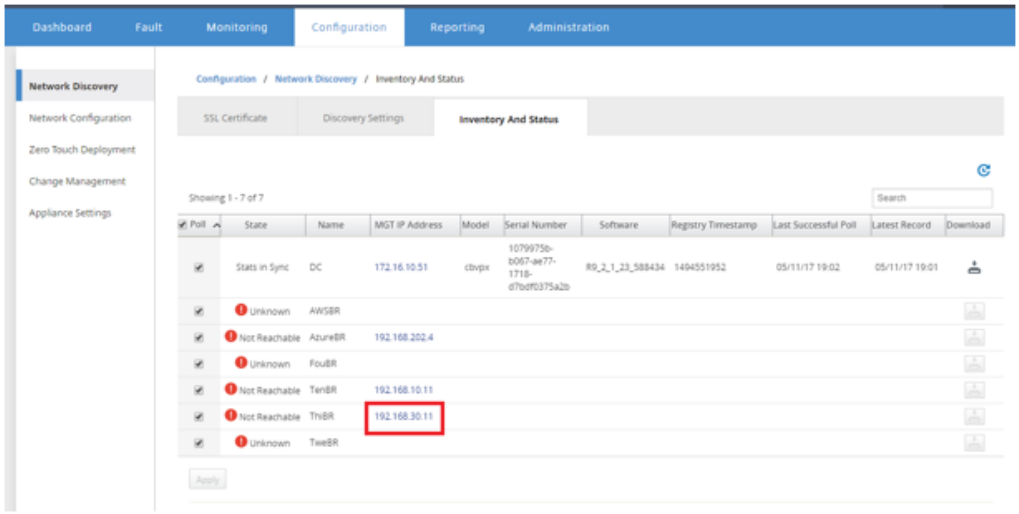
telt und der Status wird auf der Seite **MCN** > **Konfiguration** > **Virtuelles WAN** > **Änderungsverwaltung** überwacht (dieser Vorgang kann einige Minuten dauern).



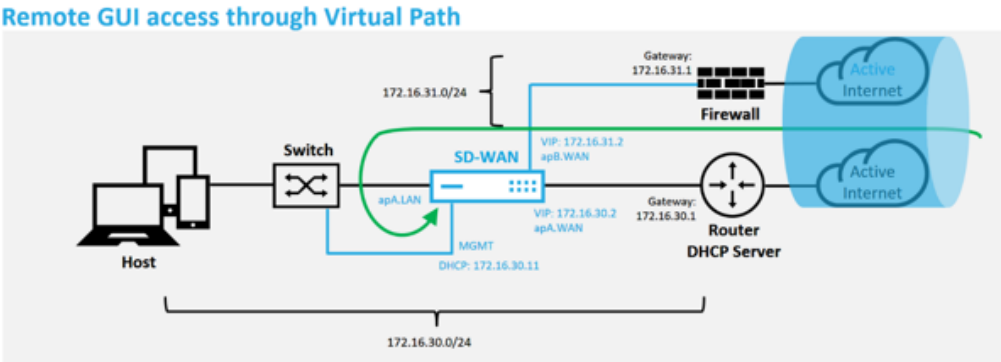
g) Der SD-WAN-Administrator kann die Head-End-MCN-Webverwaltungsseite für die etablierten virtuellen Pfade der Remotesite überwachen.



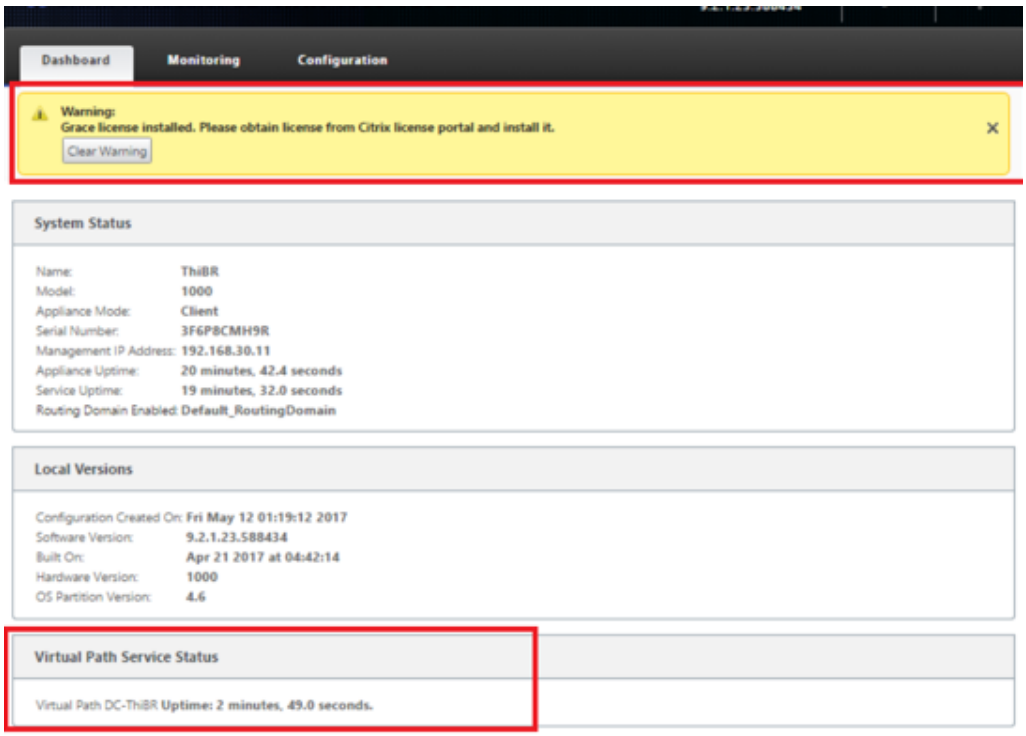
h) SD-WAN Center kann auch verwendet werden, um die DHCP-zugewiesene IP-Adresse der Vor-Ort-Appliance auf der Seite **Konfiguration** > **Netzwerkerkennung** > **Inventar und Status** zu identifizieren.



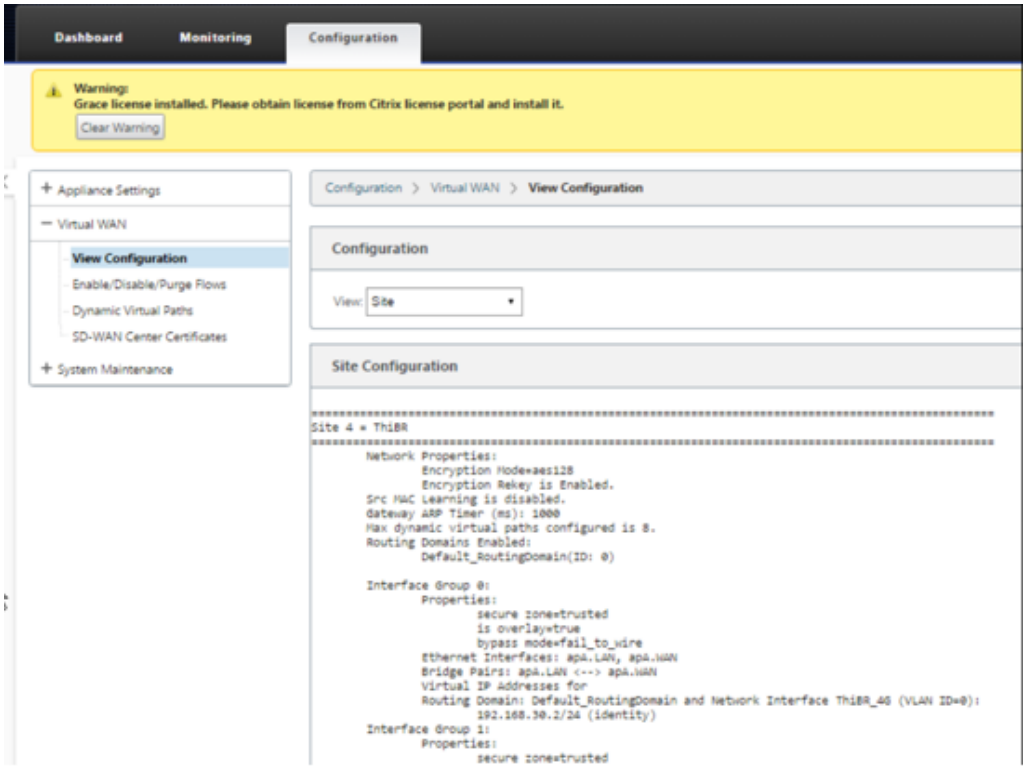
i) Zu diesem Zeitpunkt kann der SD-WAN-Netzwerkadministrator mithilfe des SD-WAN-Overlay-Netzwerks auf die Appliance vor Ort Zugriff auf die Appliance vor Ort erhalten.



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.

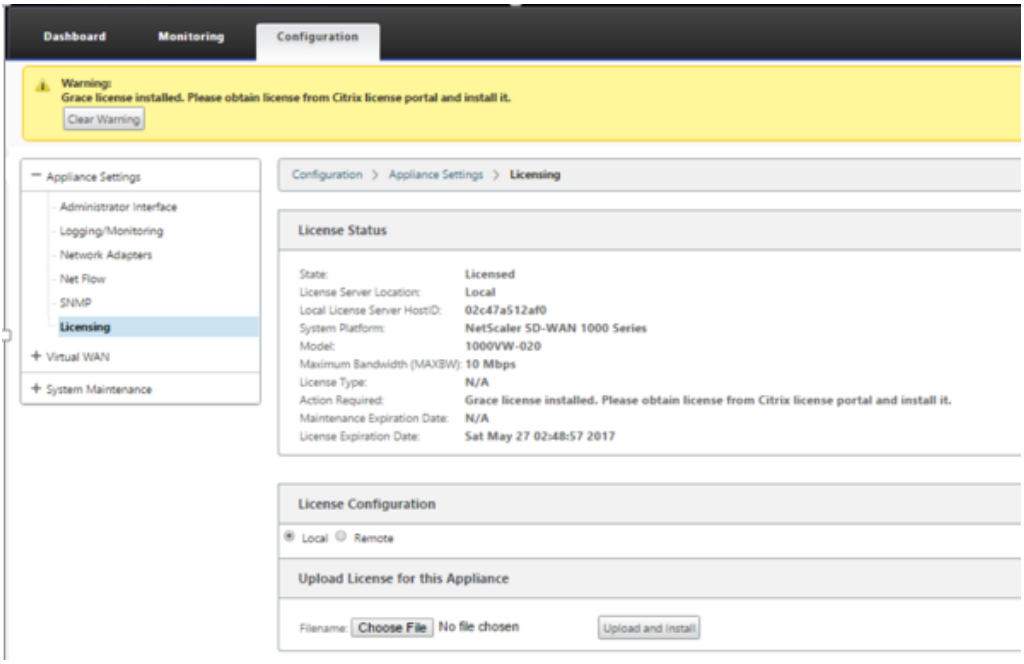


k) Die Appliance-Konfiguration kann über die Seite **Konfiguration** > **Virtuelles WAN** > **Konfiguration anzeigen** validiert werden.



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

October 28, 2021

Anweisungen zum Bereitstellen einer SD-WAN-Appliance mit Zero Touch Service finden Sie im Thema; Konfigurieren des Zero Touch-Bereitstellungsdienstes.

AWS

October 28, 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 zur Bereitstellung des Zero Touch-Bereitstellungsprozesses für vier

Cloud-Instanzen unterscheidet sich geringfügig von der Appliance-Bereitstellung für den Zero-Touch-Dienst.

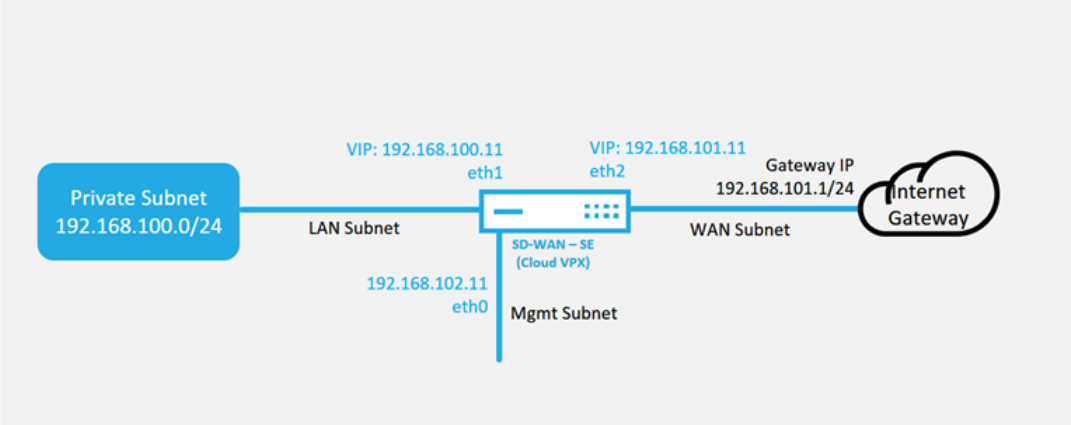
1. Aktualisieren Sie die Konfiguration, um mithilfe der SD-WAN-Center-Netzwerkkonfiguration einen neuen Remotestandort mit einem ZTD-fähigen SD-WAN-Cloud-Gerät hinzuzufügen.

   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 auf eine Zero-Touch-Bereitstellung ausgerichtet 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 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 Cloud-Vorlagen für SD-WAN VPX sind derzeit schwer darauf eingestellt, die #.#.#.#.#.11 IP-Adresse der verfügbaren Subnetze in der VPC zu erhalten.

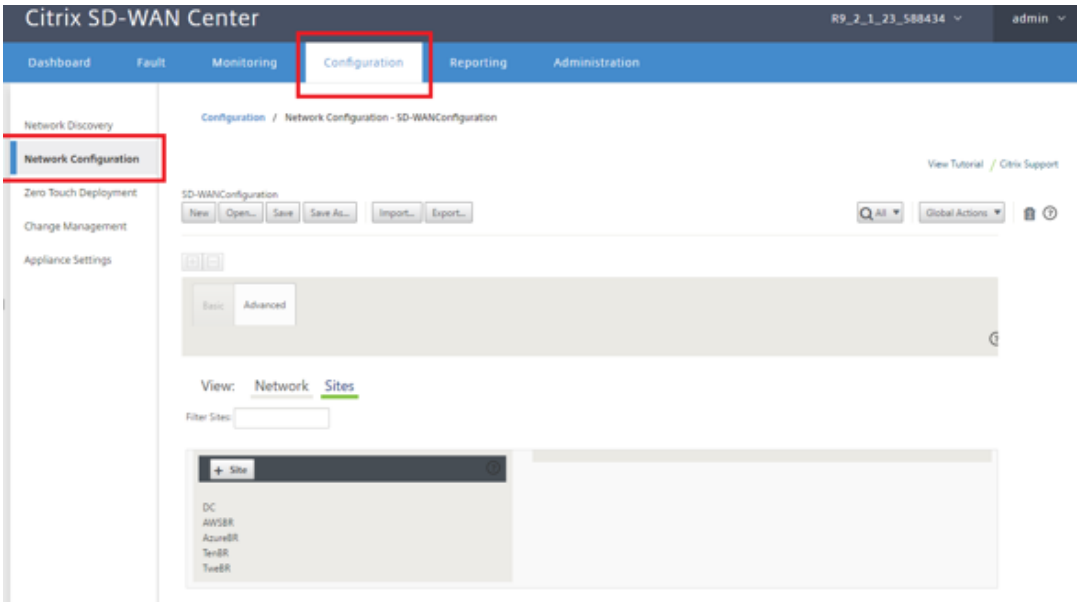
   Cloud Topology with NetScaler SD-WAN

   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. Remotestandorte können mehrere ver-

schiedene Internet-WAN-Verbindungen nutzen, die sich mit demselben Internet-Gateway für die Cloud verbinden, wodurch Ausfallsicherheit und aggregierte Bandbreitenkonnektivität von jedem SD-WAN-Bereitstellungsstandort zur Cloud-Infrastruktur bereitgestellt werden. Dies bietet eine 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**.

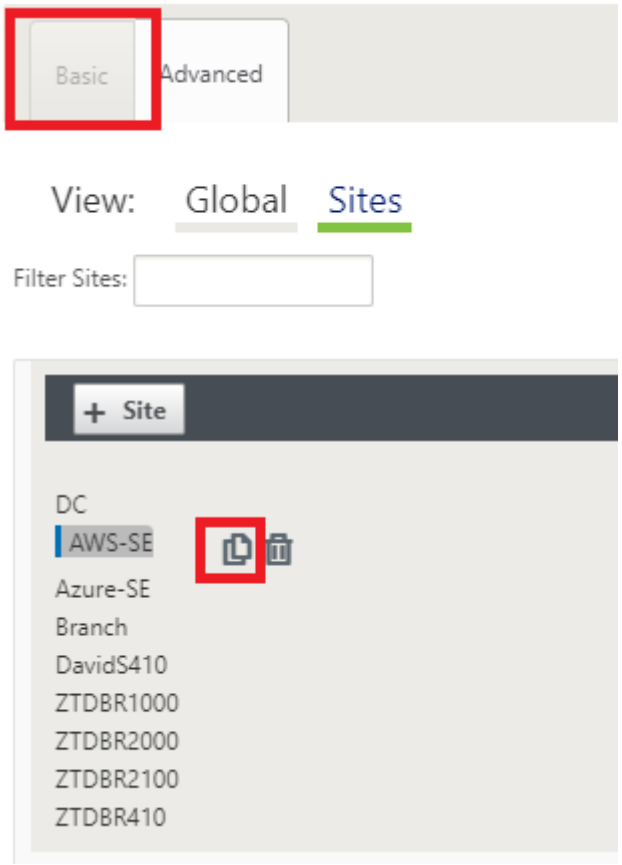


c) Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration aus dem MCN.

d) Navigieren Sie zur Registerkarte Basic, um eine neue Site zu erstellen.

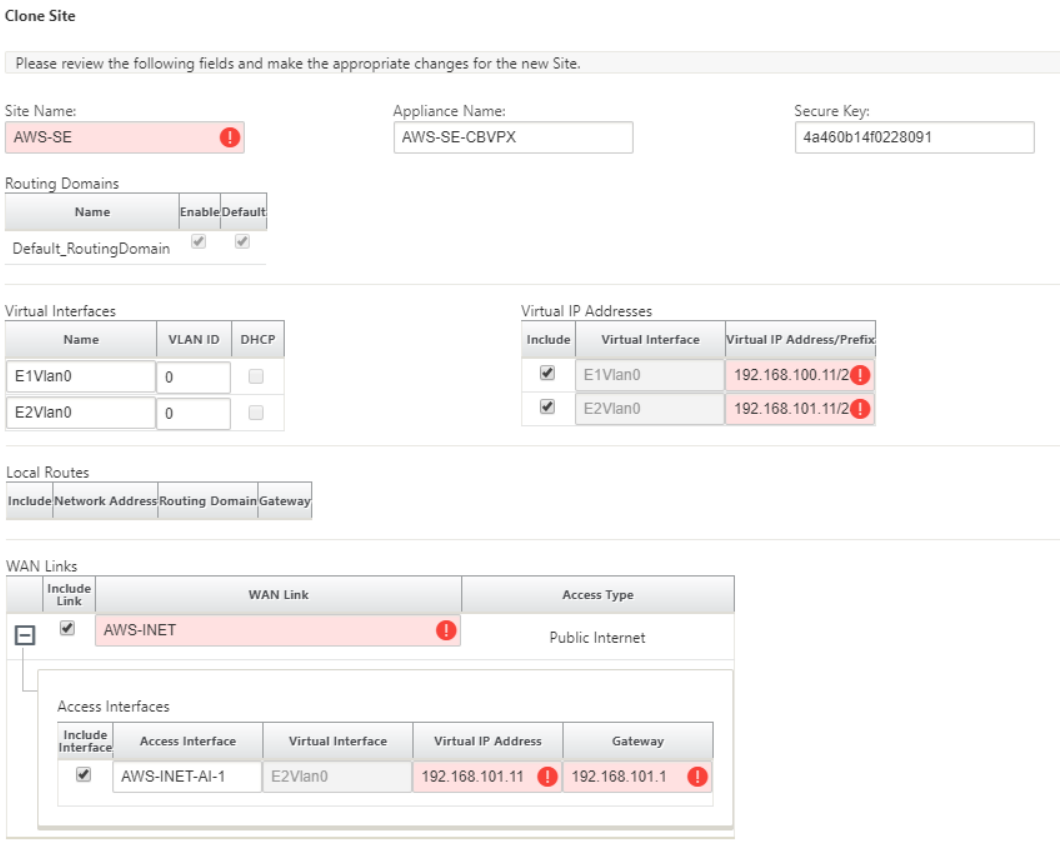
e) Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.

f) Erstellen Sie schnell die Konfiguration für die neue Cloud-Site, indem Sie die Klonfunktion einer vorhandenen Site nutzen oder manuell eine neue Site erstellen.

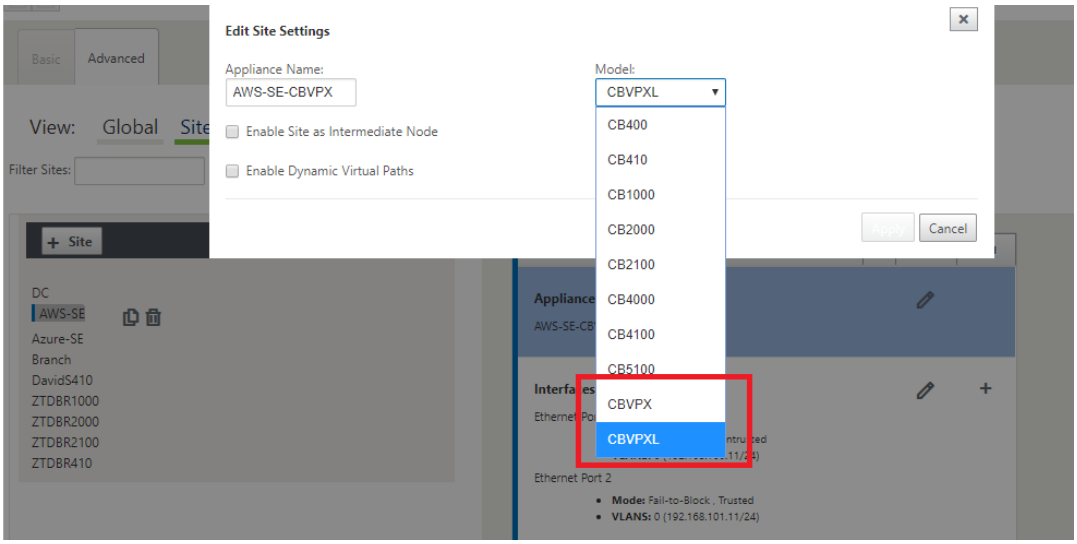


g) Füllen Sie alle erforderlichen Felder aus der zuvor für diese neue Cloud-Site entwickelten Topologie aus.

Beachten Sie, dass die für Cloud-ZTD-Bereitstellungen verfügbare Vorlage fest festgelegt ist, um die #.#.#.11-IP-Adresse für die Mgmt-, LAN- und WAN-Subnetze zu verwenden. Wenn die Konfiguration nicht so eingestellt ist, dass sie mit der erwarteten Host-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.

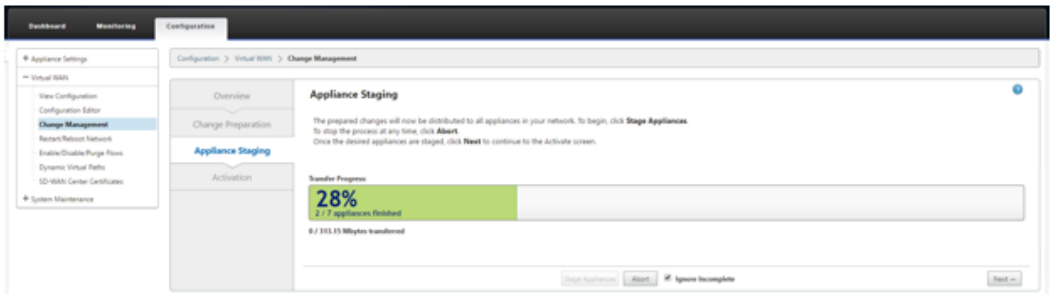


h) Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen**der Site, und überprüfen Sie, ob das SD-WAN-Modell korrekt ausgewählt ist, was den Null-Touch-Dienst unterstützen würde.



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.

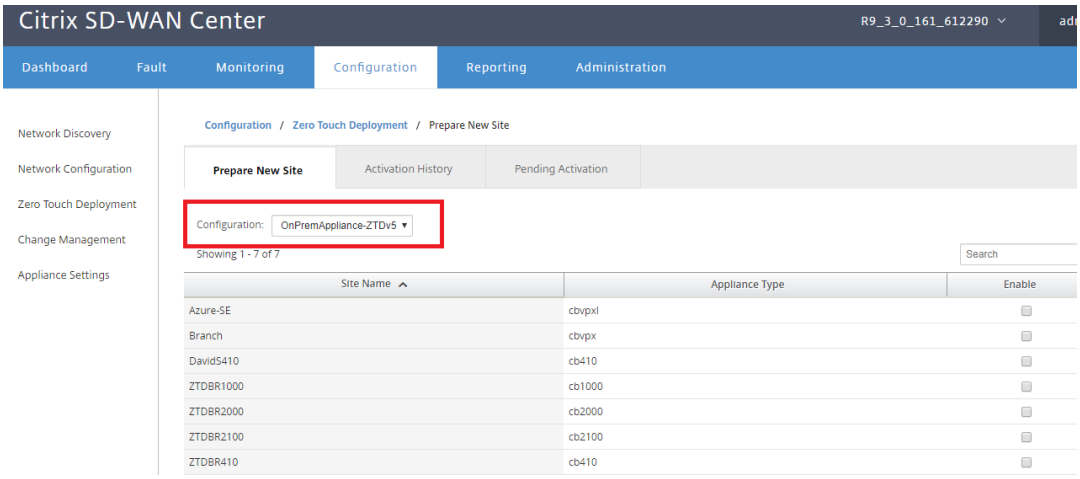
j) Befolgen Sie das Change Management-Verfahren, um für die neue Konfiguration das Staging richtig durchzuführen, wodurch die vorhandenen SD-WAN-Geräte über den neuen Standort informiert werden, der per Zero Touch bereitgestellt werden soll. Sie müssen die Option *Unvollständig ignorieren* verwenden, um den Versuch zu überspringen, die Konfiguration an die neue Site zu übertragen, die muss immer noch den ZTD-Workflow durchlaufen.



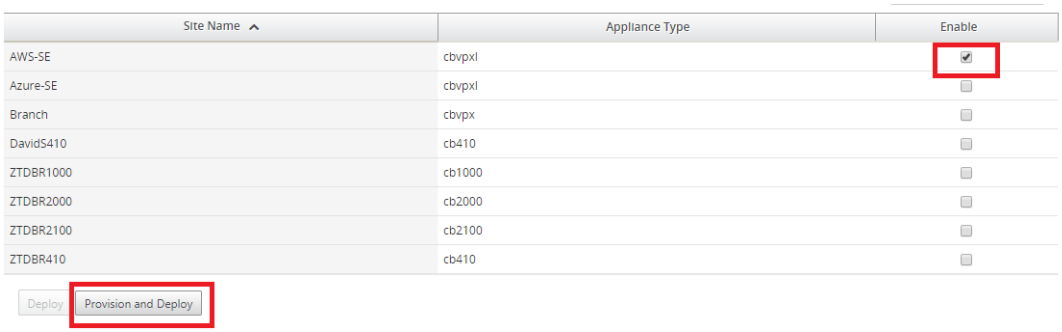
2. Navigieren Sie zurück zur Seite “Zero Touch Deployment”von SD-WAN Center. Wenn die neue aktive Konfiguration ausgeführt wird, steht die neue Site für die Bereitstellung zur Verfügung.

a) Wählen Sie auf der Seite “Zero Touch Deployment”auf der Registerkarte **Neue Site bereitstellen** die laufende Netzwerkkonfigurationsdatei aus.

b) Nachdem die laufende Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit nicht bereitgestellten Citrix SD-WAN-Geräten angezeigt, die für Zero Touch unterstützt werden.

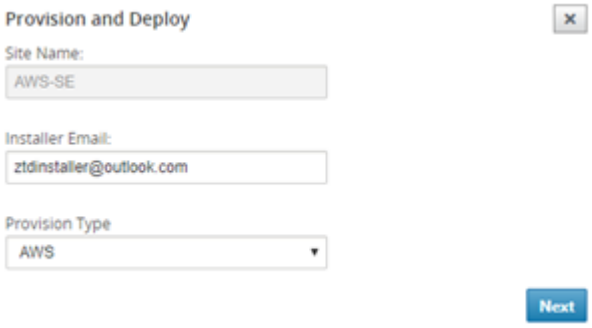


c) Wählen Sie die Ziel-Cloud-Site aus, die Sie mithilfe des Zero Touch-Dienstes bereitstellen möchten, klicken Sie auf **Aktivieren**und dann auf **Bereitstellen und Bereitstellen**.

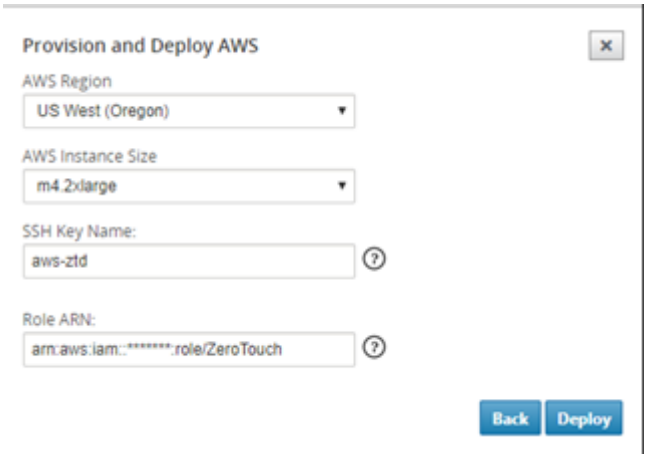


d) Es erscheint ein Popup-Fenster, in dem der Citrix SD-WAN Admin die Bereitstellung für Zero Touch initiieren kann.

Füllen Sie eine E-Mail-Adresse aus, an die die Aktivierungs-URL zugestellt werden kann, und wählen Sie die **Bereitstellungsart** für die gewünschte Cloud aus.



e) Nachdem Sie auf **Weiter**geklickt haben, wählen Sie die entsprechende Region, Instanzgröße, füllen Sie die Felder SSH-Schlüsselname und Rolle ARN entsprechend aus.

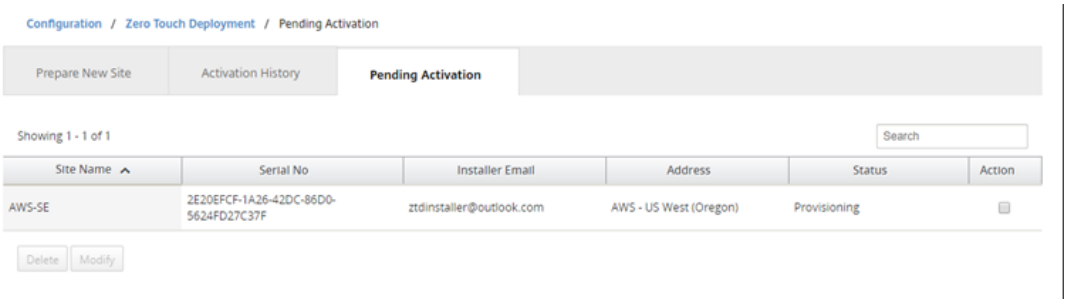


> **Hinweis**
>
> Nutzen Sie die Hilfe-Links, um Anleitungen zum Einrichten des SSH-Schlüssels und der Rollen-ARN für das Cloud-Konto zu erhalten. Stellen Sie außerdem sicher, dass die ausgewählte Region mit dem übereinstimmt, was auf dem Konto verfügbar ist,

> und dass die ausgewählte Instanzgröße mit VPX oder VPXL als dem ausgewählten Modell in der SD-WAN-Konfiguration übereinstimmt.

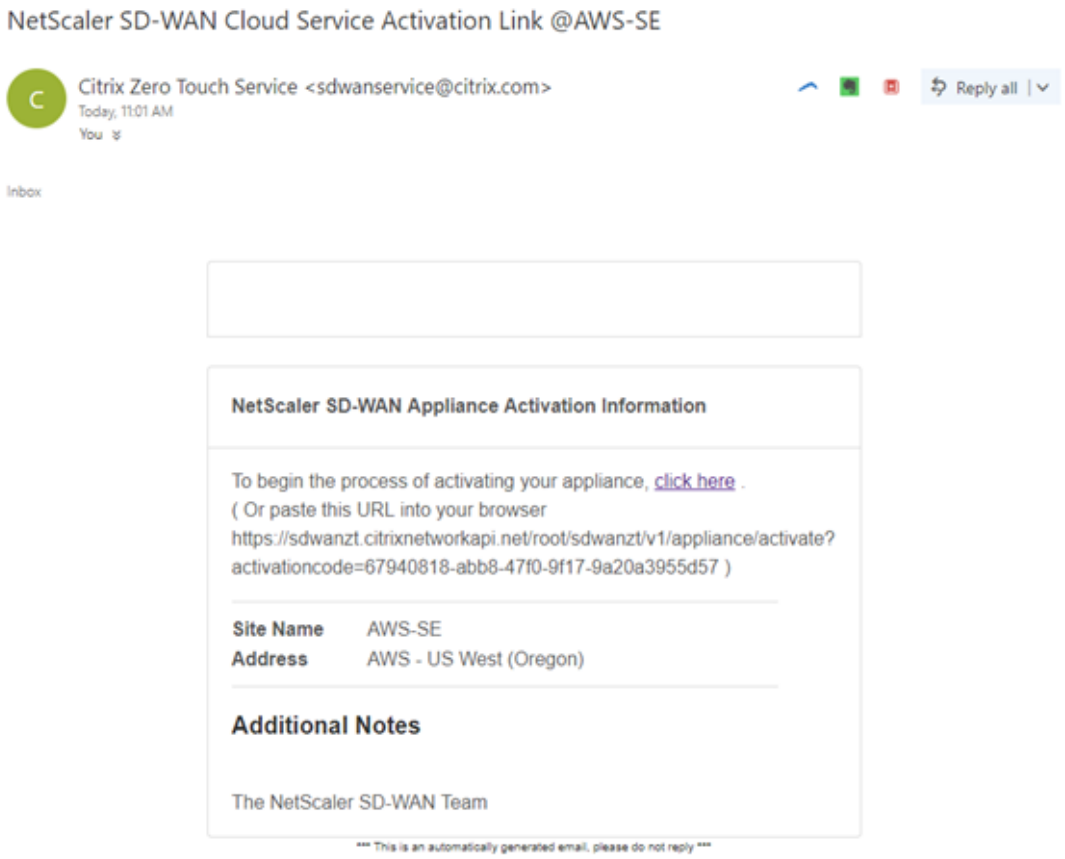
f) Klicken Sie auf **Bereitstellen**, um das SD-WAN Center auszulösen, das zuvor beim ZTD Cloud Service registriert war, um die Konfiguration dieser Site für die zeitliche Speicherung im ZTD-Cloud-Dienst freizugeben.

g) Navigieren Sie zur Registerkarte **Ausstehende Aktivierung**, um zu bestätigen, dass die Site-Informationen erfolgreich ausgefüllt und in einen Provisioning-Status versetzt wurden.



3. Starten Sie den Zero Touch Deployment Prozess als Cloud-Admin.

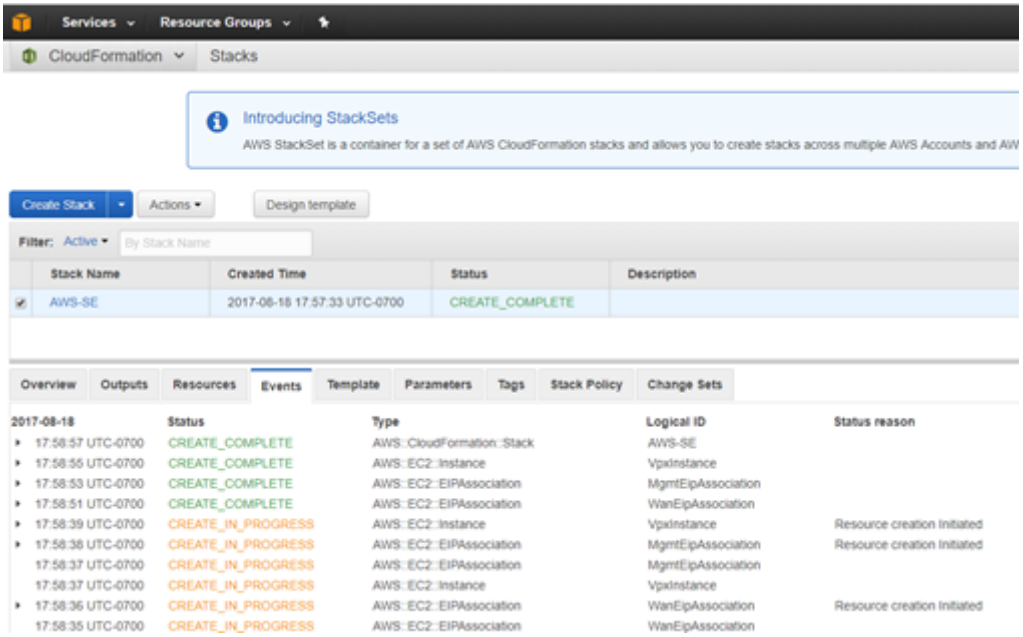
   a) Das Installationsprogramm muss das Postfach der E-Mail-Adresse überprüfen, die der SD-WAN-Administrator bei der Bereitstellung der Site verwendet hat.



b) Öffnen Sie die Aktivierungs-URL in der E-Mail in einem Internetbrowser-Fenster (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.

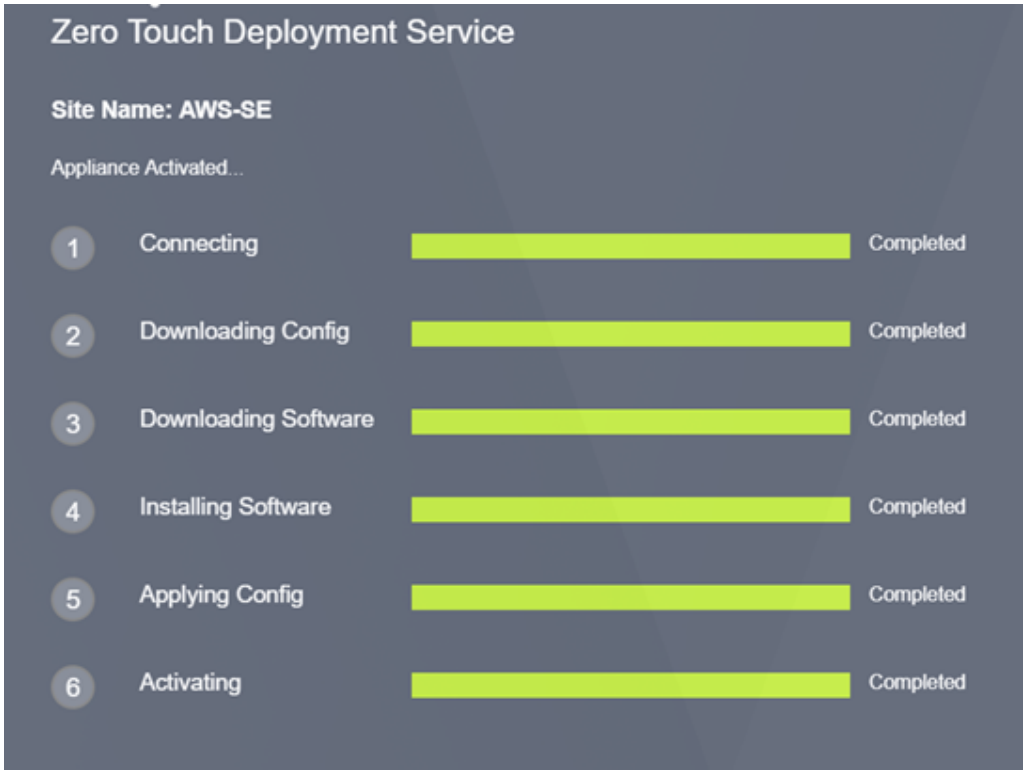
d) Zur zusätzlichen Fehlerbehebung auf der AWS-Konsole kann der Cloud Formation Service verwendet werden, um alle Ereignisse abzufangen, die während des Bereitstellungsvorgangs auftreten.



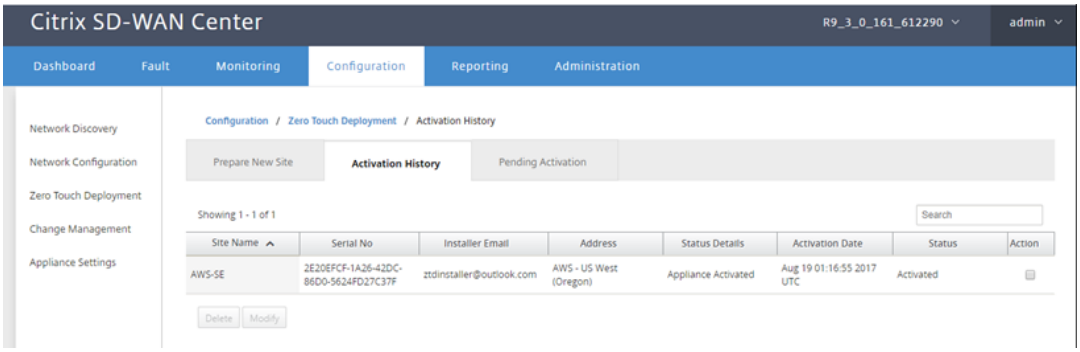
e) Lassen Sie den Bereitstellungsvorgang ~8-10 Minuten und die Aktivierung weitere ~3-5 Minuten einhalten, um vollständig abzuschließen.

f) Bei erfolgreicher Konnektivität der SD-WAN-Cloud-Instanz mit dem ZTD-Cloud-Dienst führt der Dienst automatisch Folgendes aus:

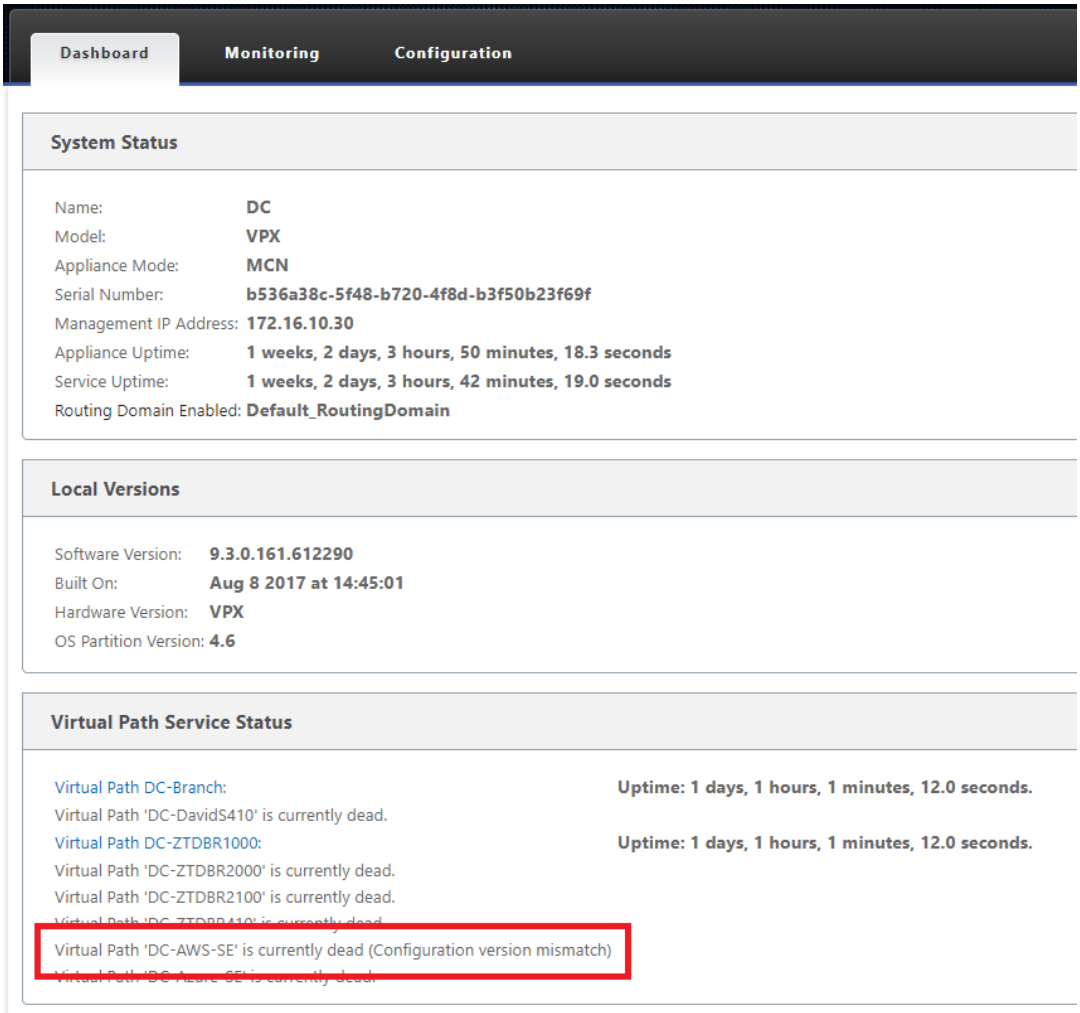
- Laden Sie die standortspezifische Konfigurationsdatei herunter, die zuvor vom SD-WAN Center gespeichert wurde
- Anwenden der Konfiguration auf die lokale Instanz
- Laden Sie eine temporäre Lizenzdatei mit 10 MB herunter und installieren Sie sie
- Laden Sie bei Bedarf Softwareupdates herunter und installieren Sie sie
- Aktivieren Sie den SD-WAN-Dienst



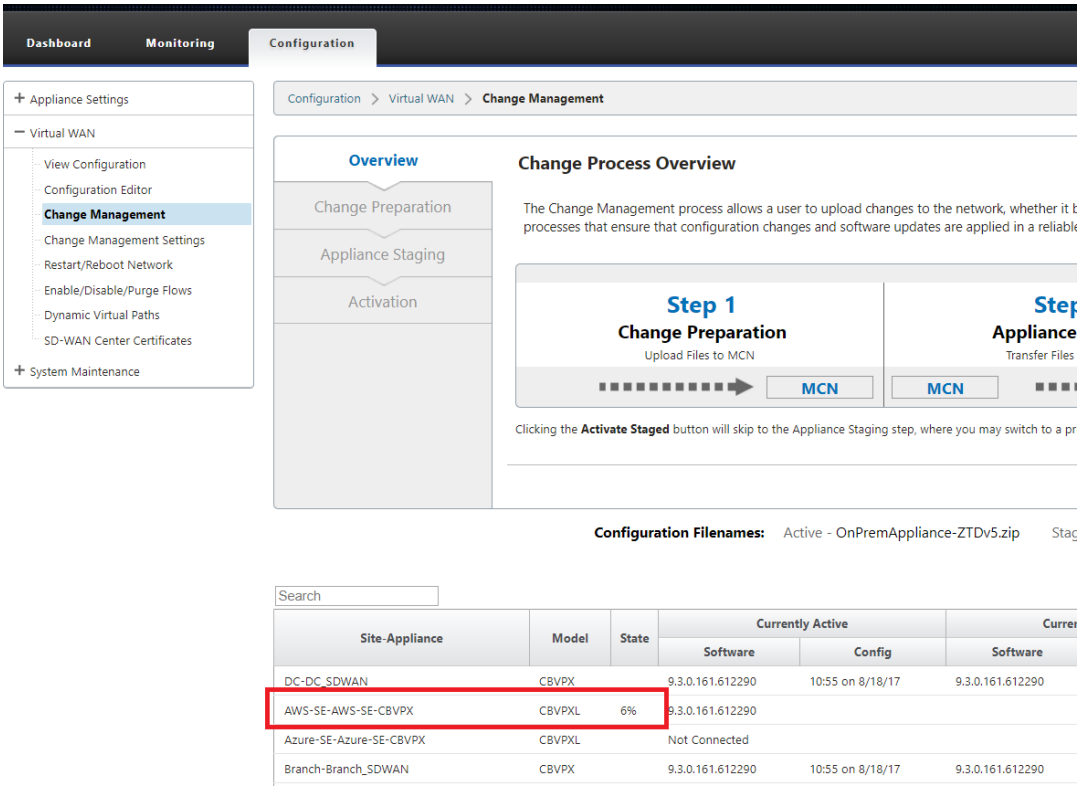
g) Eine weitere Bestätigung kann in der Webverwaltungsoberfläche des SD-WAN Center erfolgen. Das Zero Touch-Bereitstellungsmenü zeigt erfolgreich aktivierte Appliances auf der Registerkarte **Aktivierungsverlauf** an.



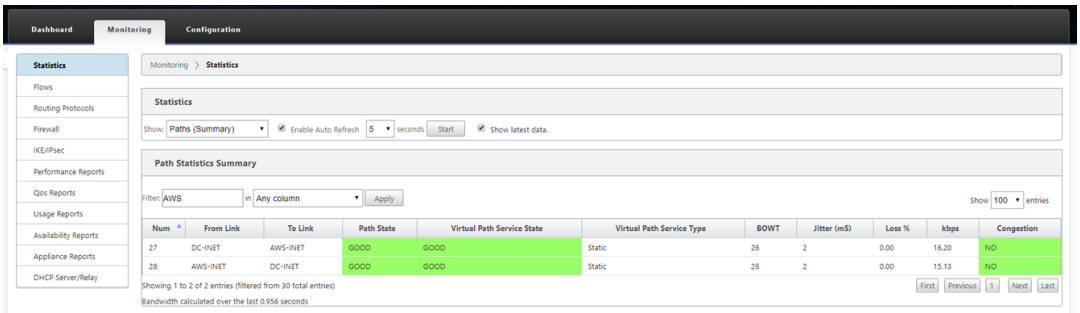
h) Die virtuellen Pfade werden möglicherweise nicht sofort in einem verbundenen Zustand angezeigt. Dies liegt daran, dass der MCN der vom ZTD-Cloud-Dienst übermittelten Konfiguration möglicherweise nicht vertraut und eine *Nichtübereinstimmung der Konfigurationsversion* im MCN-Dashboard meldet.



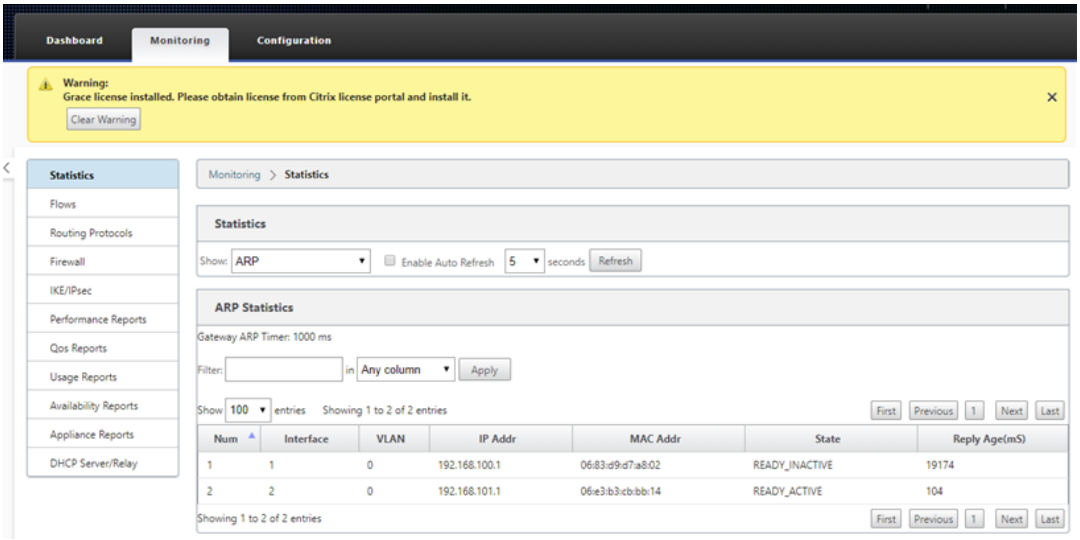
i) Die Konfiguration wird automatisch an die neu installierte Zweigstelleneinheit weitergegeben. Der Status kann auf der Seite **MCN** > **Konfiguration** > **Virtuelles WAN** > **Änderungsmanagement** überwacht werden (je nach Konnektivität kann dieser Prozess Nehmen Sie sich einige Minuten Zeit, um abzuschließen).



j) Der SD-WAN-Administrator kann die Head-End-MCN-Webverwaltungsseite für die etablierten virtuellen Pfade der neu hinzugefügten Cloud-Site überwachen.



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

October 28, 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 Remotesite mit einem ZTD-fähigen SD-WAN-Cloud-Gerät mit SD-WAN Center-Netzwerkkonfiguration hinzuzufügen

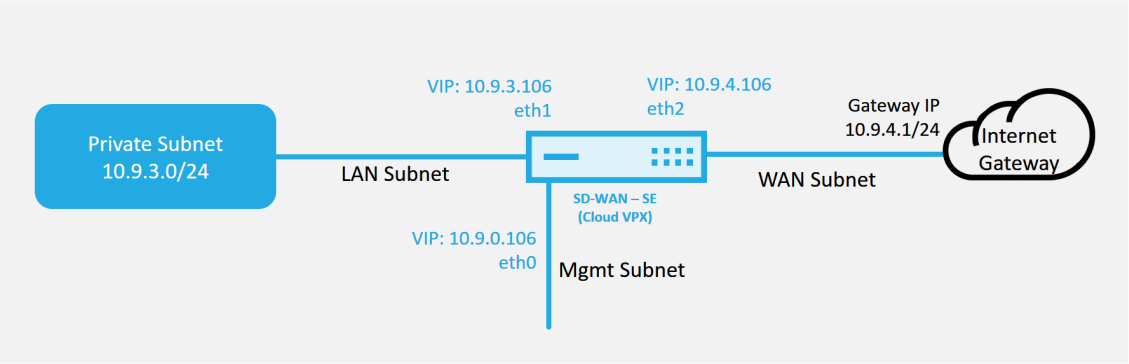
Wenn die SD-WAN-Konfiguration nicht mit der SD-WAN-Center-Netzwerkkonfiguration erstellt wurde, importieren Sie die aktive Konfiguration aus dem MCN und beginnen Sie mit der Änderung der Konfiguration mit dem SD-WAN Center. Für die Zero Touch-Bereitstellung muss der SD-WAN-Administrator die Konfiguration mithilfe des SD-WAN-Centers erstellen. Das folgende Verfahren sollte verwendet werden, um einen neuen Cloud-Knoten hinzuzufügen, der auf eine Zero-Touch-Bereitstellung ausgerichtet 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).

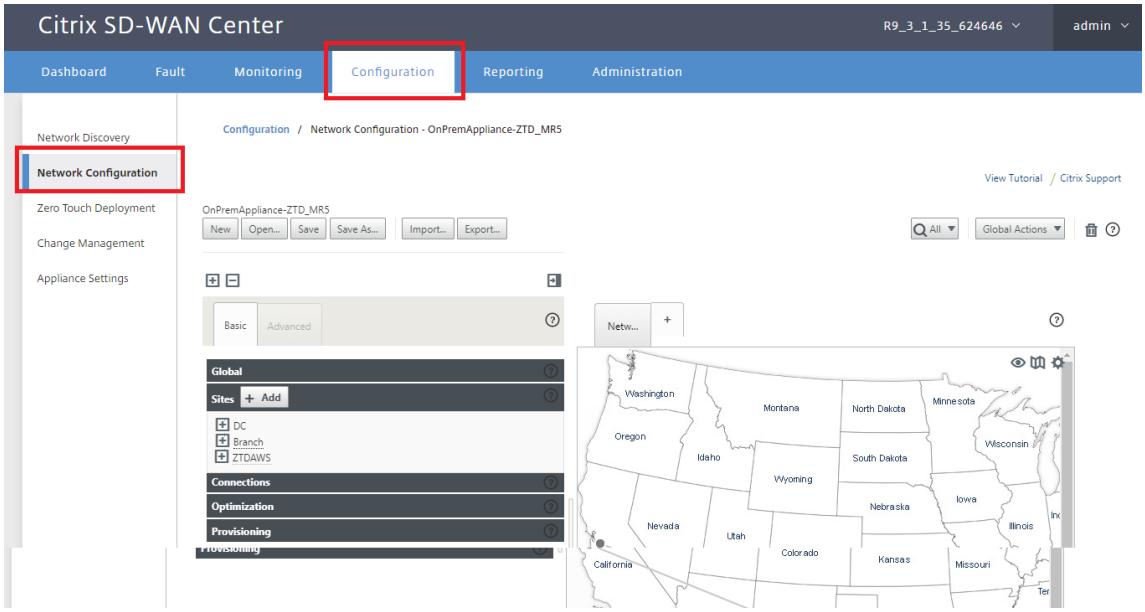
> - Die verfügbaren Azure-Cloudvorlagen für SD-WAN VPX sind derzeit hart festgelegt, um die 10.9.4.106 IP für das WAN, 10.9.3.106 IP für das LAN und 10.9.0.16 IP für die Verwaltungsadresse zu erhalten. Die SD-WAN-Konfiguration für den Azure-Knoten, der auf Zero Touch ausgerichtet ist, muss diesem Layout entsprechen.
> - Der Azure-Site-Name in der Konfiguration muss alle Kleinbuchstaben ohne Sonderzeichen enthalten (z. B. ztdazure).

Azure Cloud Topology with NetScaler SD-WAN

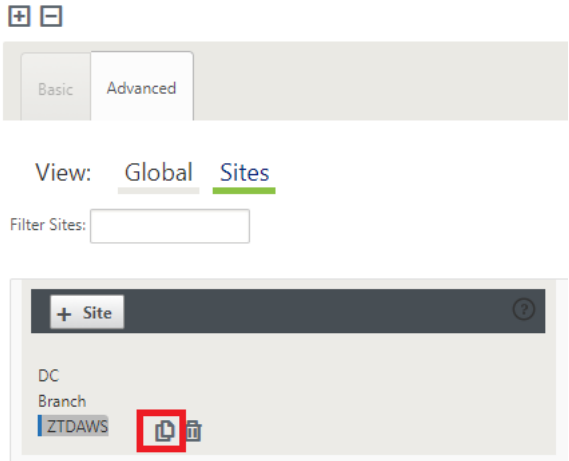


Dies ist ein Beispiel für die Bereitstellung einer SD-WAN-Cloud bereitgestellten Site. Das Citrix SD-WAN Gerät wird als Edge-Gerät bereitgestellt, das eine einzelne Internet-WAN-Verbindung in diesem Cloud-Netzwerk bedient. Remotestandorte können mehrere verschiedene Internet-WAN-Verbindungen nutzen, die sich mit demselben Internet-Gateway für die Cloud verbinden, wodurch Ausfallsicherheit und aggregierte Bandbreitenkonnektivität von jedem SD-WAN-Bereitstellungsstandort zur Cloud-Infrastruktur bereitgestellt werden. Dies bietet eine 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 Site 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 Klonfunktion einer vorhandenen Site nutzen oder manuell eine neue Site erstellen.

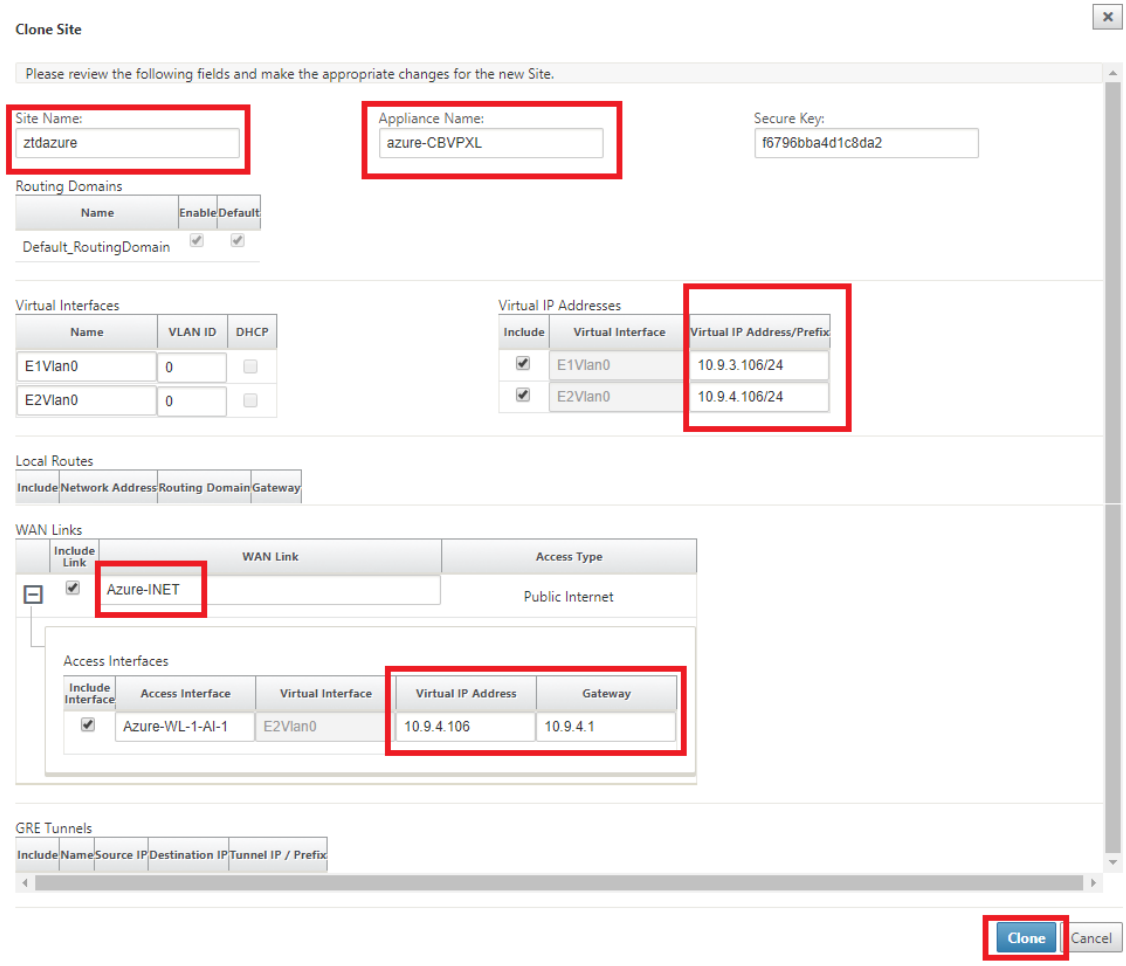


7. Füllen Sie alle erforderlichen Felder aus der zuvor für diese neue Cloud-Site entworfenen Topologie aus.

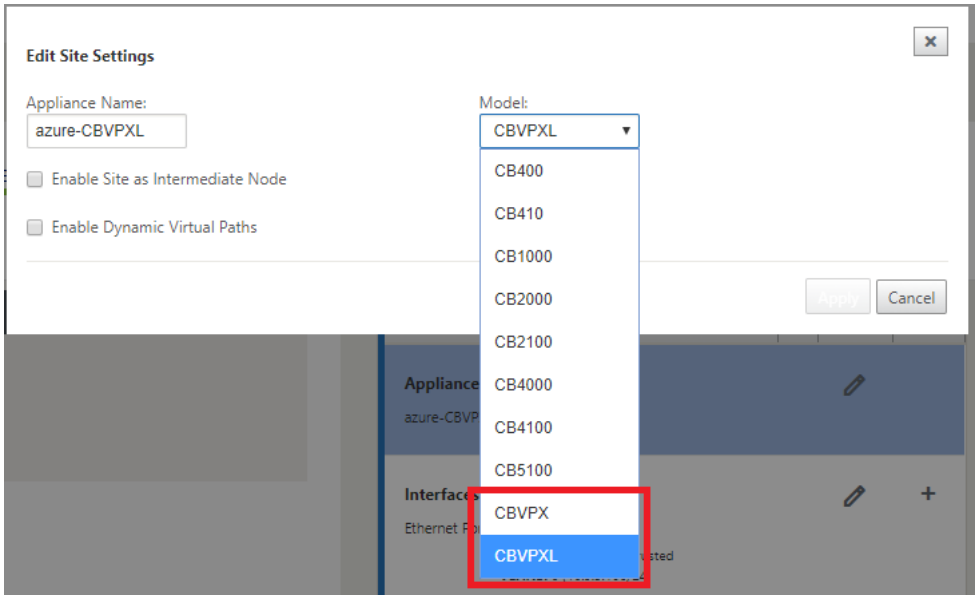
   Beachten Sie, dass die für Azure Cloud ZTD-Bereitstellungen verfügbare Vorlage derzeit fest festgelegt ist, um die 10.9.4.106 IP für das WAN, 10.9.3.106 IP für das LAN und 10.9.0.16 IP für die Verwaltungsadresse zu erhalten. Wenn die Konfiguration nicht so eingestellt ist, dass sie der erwarteten VIP-Adresse für jede Schnittstelle entspricht, kann das Gerät ARP nicht ordnungs-

gemäß für die Cloud-Umgebungsgateways und IP-Konnektivität zum virtuellen Pfad des MCN einrichten.

Es wird importiert, dass der Sitename mit dem übereinstimmt, was Azure erwartet. Der Site-Name muss in Kleinbuchstaben enthalten sein, mindestens 6 Zeichen, ohne Sonderzeichen, er muss mit dem folgenden regulären Ausdruck **^ [a-z] [a-z0-9-] {1,61} [a-z0-9] $ bestätigen.**

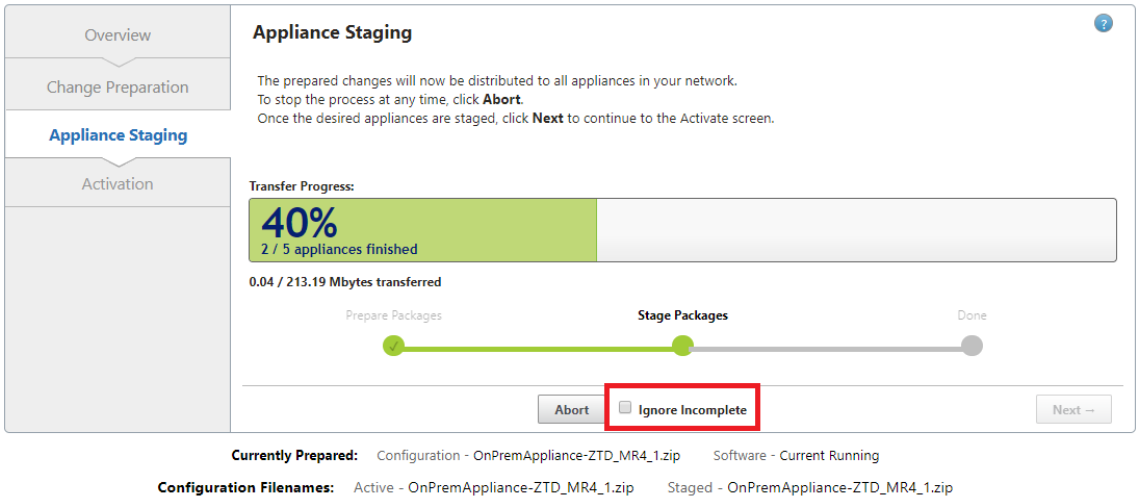


8. Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen**der Site, und überprüfen Sie, ob das SD-WAN-Modell korrekt ausgewählt ist, was den Null-Touch-Dienst unterstützen würde.



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.

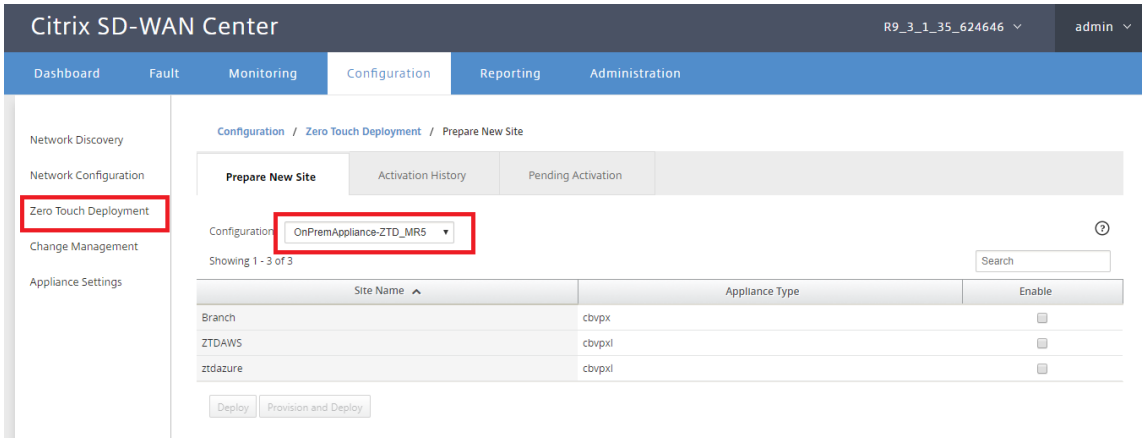
10. Befolgen Sie das Change Management-Verfahren, um für die neue Konfiguration das Staging richtig durchzuführen, wodurch die vorhandenen SD-WAN-Geräte über den neuen Standort informiert werden, der per Zero Touch bereitgestellt werden soll. Sie müssen die Option *Unvollständig ignorieren* verwenden, um den Versuch zu überspringen, die Konfiguration an die neue Site zu übertragen, die muss immer noch den ZTD-Workflow durchlaufen.



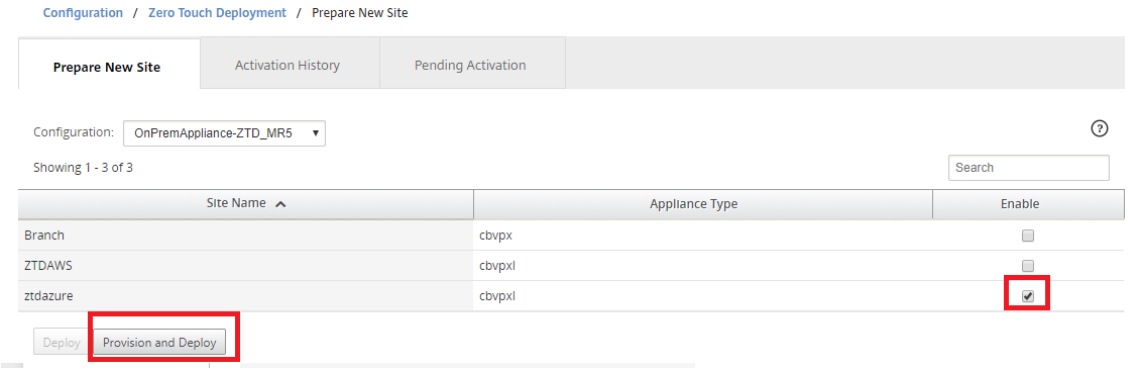
Navigieren Sie zur Zero Touch-Bereitstellungsseite des SD-WAN Centers, und wenn die neue aktive Konfiguration ausgeführt wird, wird die neue Site für SD-WAN Center Provisioning und Deploy Azure verfügbar sein (Schritt 1 von 2)

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 laufende Netzwerkkonfigurationsdatei aus.

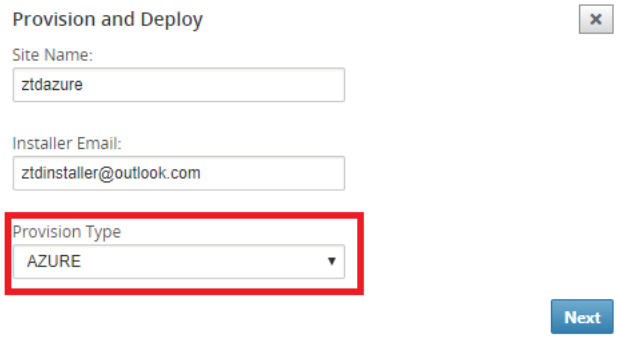
2. Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit ZTD-fähigen Citrix SD-WAN Geräten angezeigt.



3. Wählen Sie die Ziel-Cloud-Site aus, die Sie mithilfe des Zero Touch-Dienstes bereitstellen möchten, klicken Sie auf **Aktivieren**und dann auf **Bereitstellen und Bereitstellen**.

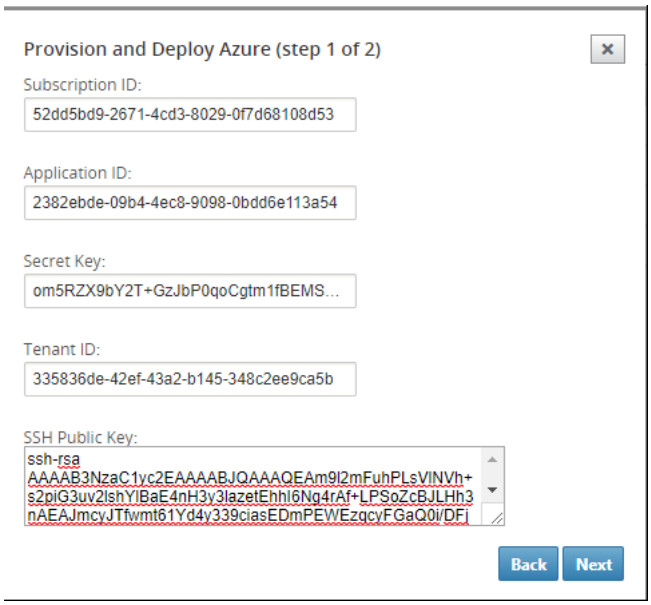


4. Es erscheint ein Popup-Fenster, in dem der Citrix SD-WAN Admin die Bereitstellung für Zero Touch initiieren kann. Stellen Sie sicher, dass der Site-Name den Anforderungen für Azure entspricht (Kleinbuchstaben ohne Sonderzeichen). Geben Sie eine E-Mail-Adresse auf, an die die Aktivierungs-URL bereitgestellt werden kann, und wählen Sie Azure als **Bereitstellungstyp** für die gewünschte Cloud aus, bevor Sie auf **Weiter**klicken.

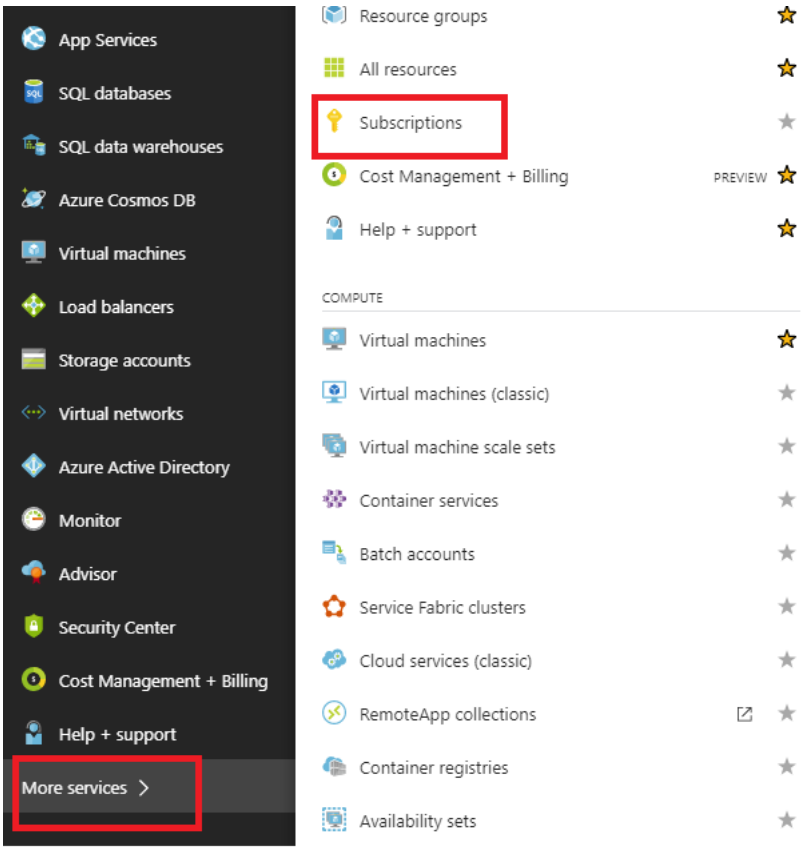


5. Nachdem Sie auf **Weiter**geklickt haben, erfordert das Fenster Bereitstellung und Bereitstellung von Azure (Schritt 1 von 2) die Eingabe der vom Azure-Konto erhaltenen Daten.

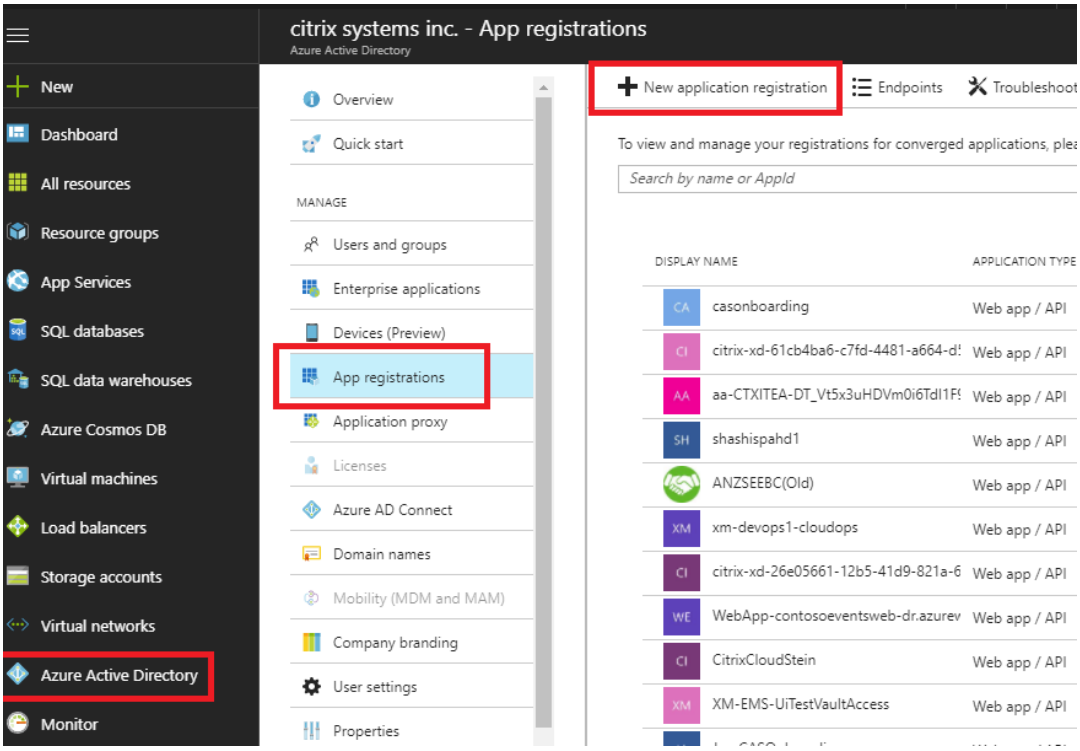
   Kopieren Sie alle erforderlichen Felder, nachdem Sie die Informationen von Ihrem Azure-Konto erhalten haben, und fügen Sie sie ein. In den folgenden Schritten wird beschrieben, wie Sie die erforderliche Abonnement-ID, Anwendungs-ID, den geheimen Schlüssel und die Mandanten-ID von Ihrem Azure-Konto erhalten und dann auf **Weiter**klicken.



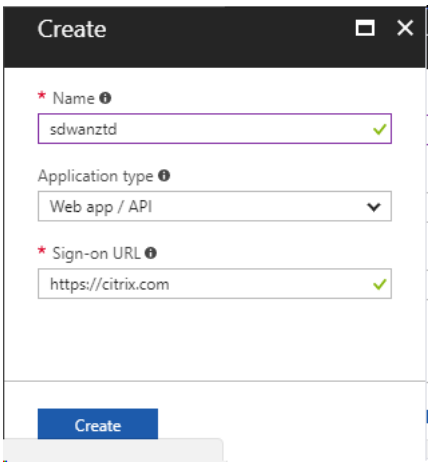
   a) Auf dem Azure-Konto können wir die erforderliche **Abonnement-ID** identifizieren, indem wir zu “Weitere Dienste”navigieren und **Abonnements auswählen.**



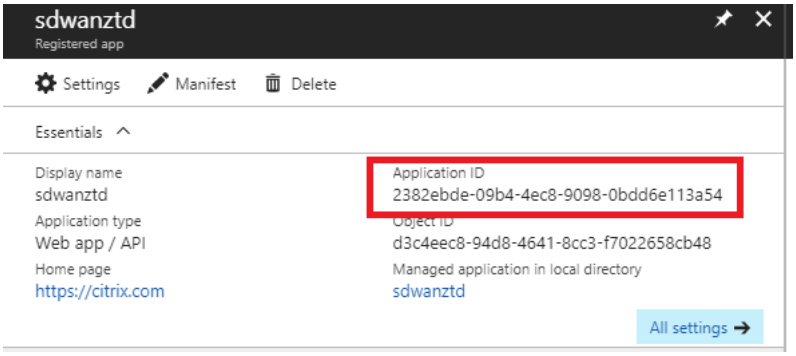
b) Um die erforderliche ***Application ID zu identifizieren**, navigieren Sie zu Azure Active Directory, Anwendungsregistrierungen und klicken Sie auf **Neue Anwendungsregistrierung.**



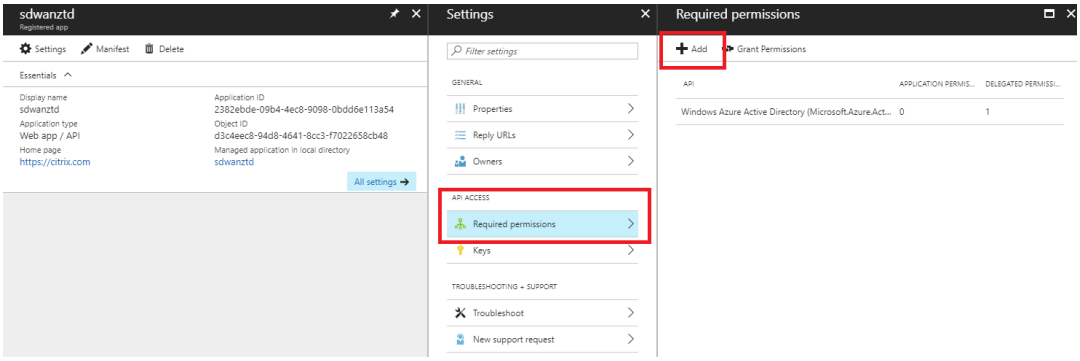
c) Geben Sie im Menü zum Erstellen der App-Registrierung einen Namen und eine Anmelde-URL ein (dies kann eine beliebige URL sein, die einzige Voraussetzung ist, dass sie gültig sein muss) und klicken Sie dann auf **Erstellen**.



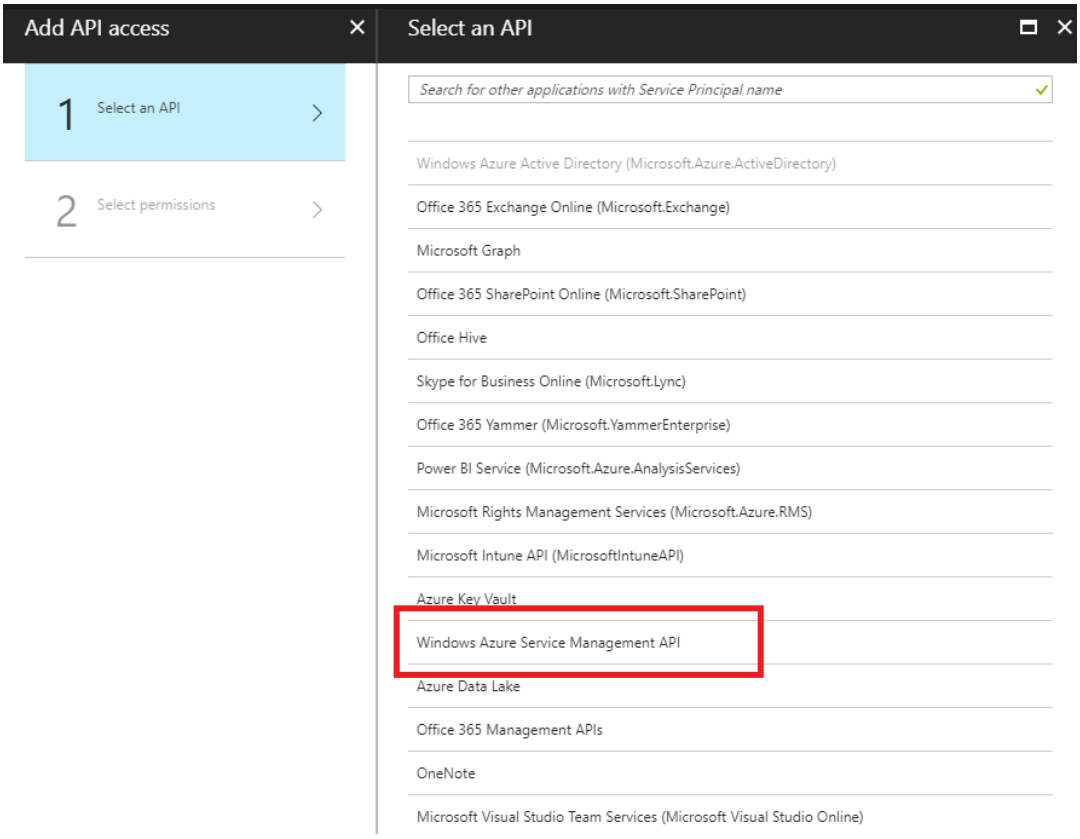
d) Suchen und öffnen Sie die neu erstellte registrierte App und notieren Sie sich die Anwendungs-ID.



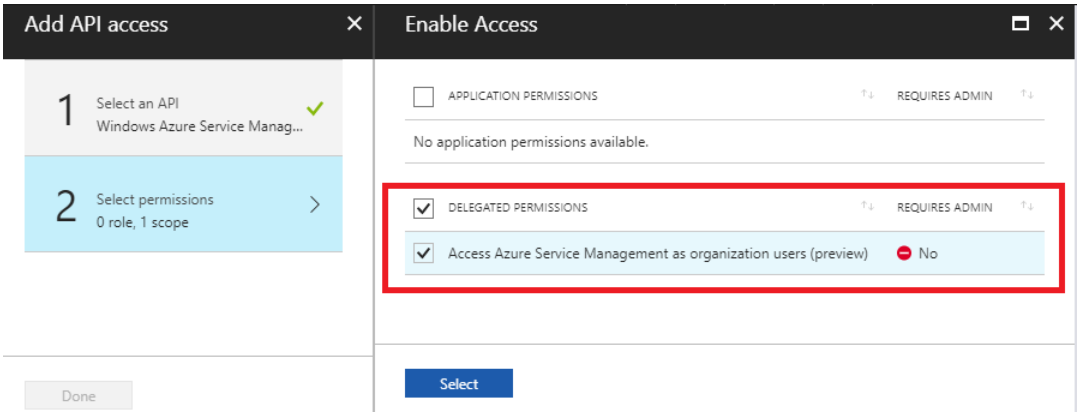
e) Öffnen Sie erneut die neu erstellte Registrierungs-App, und um den erforderlichen *Sicherheitsschlüssel*zu identifizieren, wählen Sie unter API-Zugriff die Option **Erforderliche Berechtigungen aus,** damit ein Dritter bereitstellen und instanzieren kann. Wählen Sie dann **Add**.



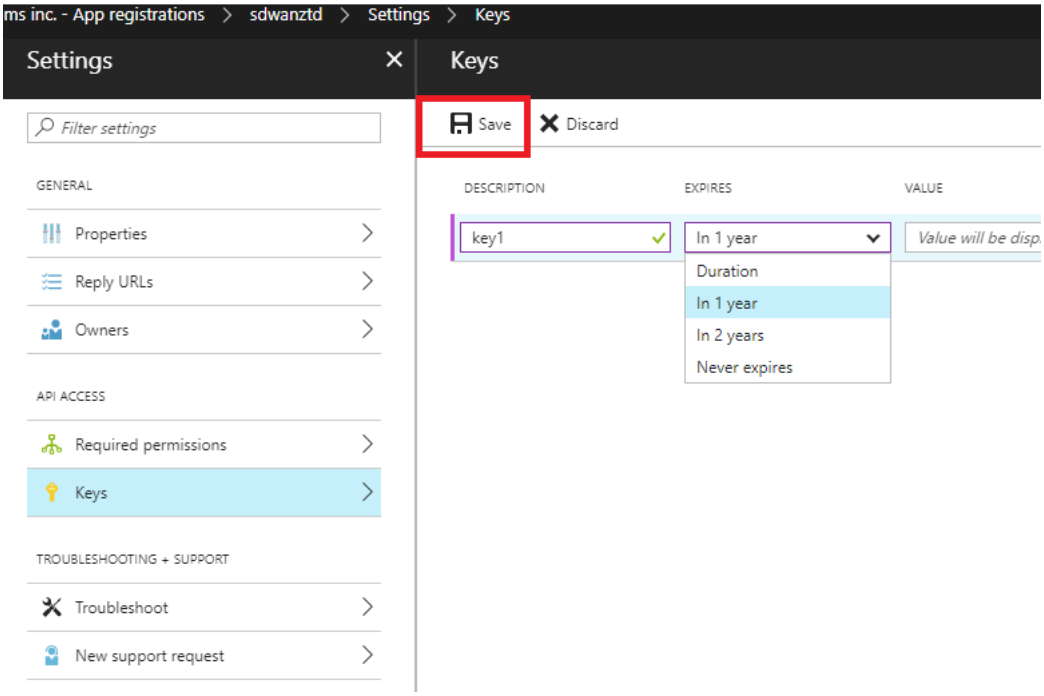
f) Wenn Sie die erforderlichen Berechtigungen hinzufügen, **wählen Sie eine API** aus und markieren Sie dann die **Windows Azure Service Management-API.**



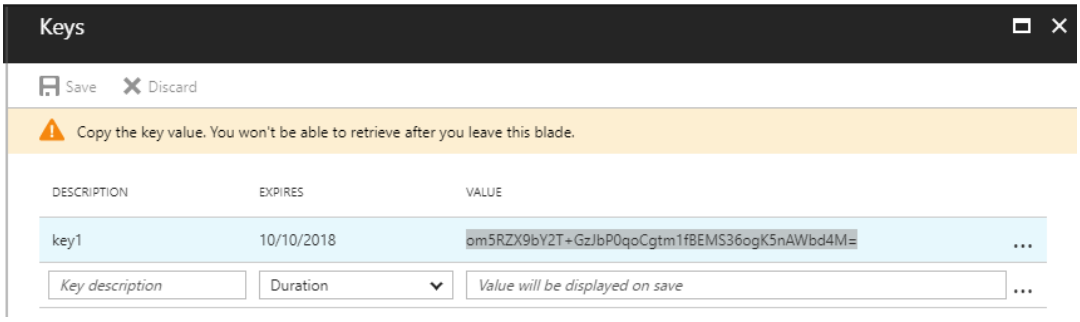
g) Aktivieren Sie **Delegate-Berechtigungen**, um Instanzen bereitzustellen, und klicken Sie dann auf **Auswählen** und **Fertig**.



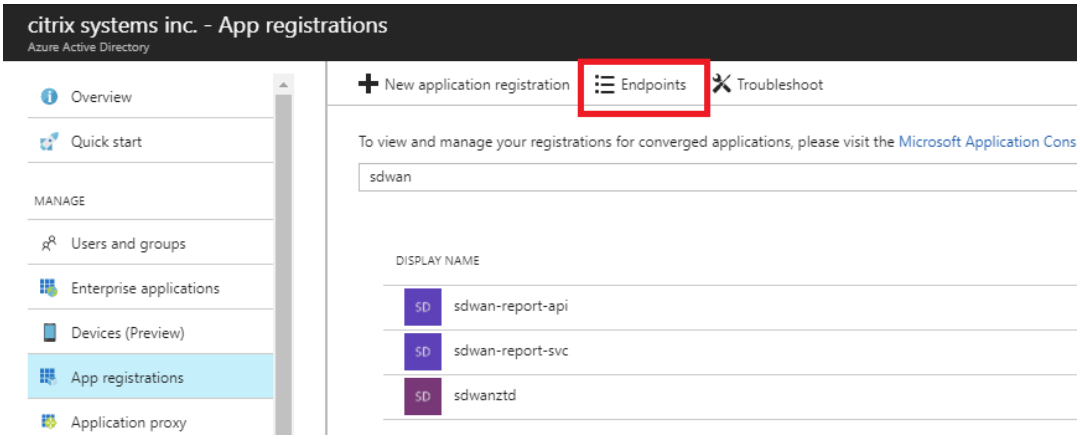
h) Wählen Sie für diese registrierte App unter API-Zugriff **Schlüssel** aus und erstellen Sie eine geheime **Schlüsselbeschreibung** und die gewünschte **Dauer**, bis der Schlüssel gültig ist. Klicken Sie dann auf **Speichern**, wodurch ein **geheimer Schlüssel** erzeugt wird (der Schlüssel ist nur für den Bereitstellungsprozess erforderlich, er kann gelöscht werden, nachdem die Instanz verfügbar gemacht wurde).



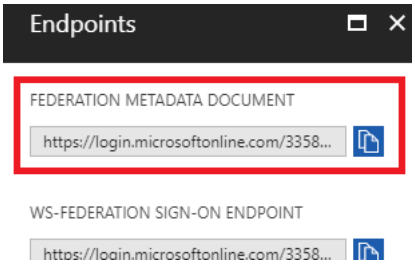
i) Kopieren und speichern Sie den geheimen Schlüssel (beachten Sie, dass Sie diesen später nicht mehr abrufen können).



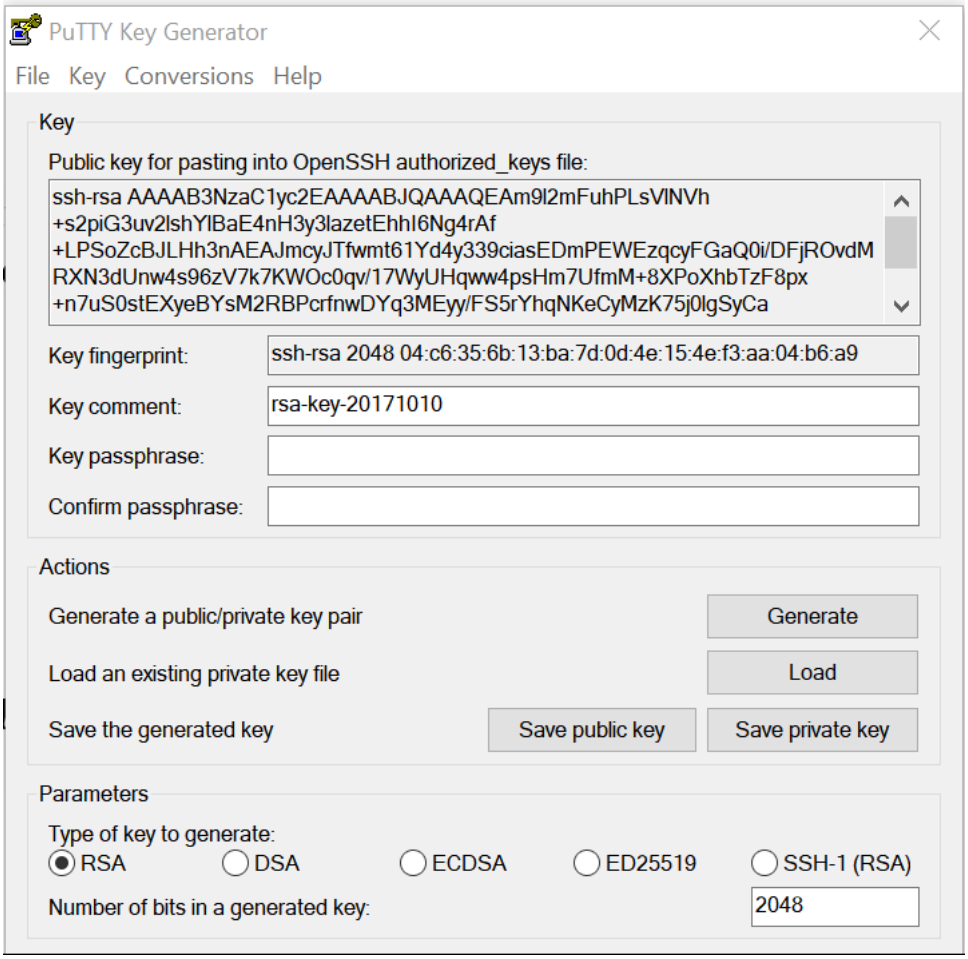
j) Um die erforderliche ***Mandanten-ID***zu identifizieren, navigieren Sie zurück zum App-Registrierungsbereich und wählen Sie **Endpoints**aus.



k) Kopieren Sie das **Federation-Metadaten-Dokument**, um Ihre Mandanten-ID zu identifizieren (beachten Sie, dass die Mandanten-ID aus einer 36-stelligen Zeichenfolge besteht, die zwischen `online.com/` und `/federation` in der URL steht).

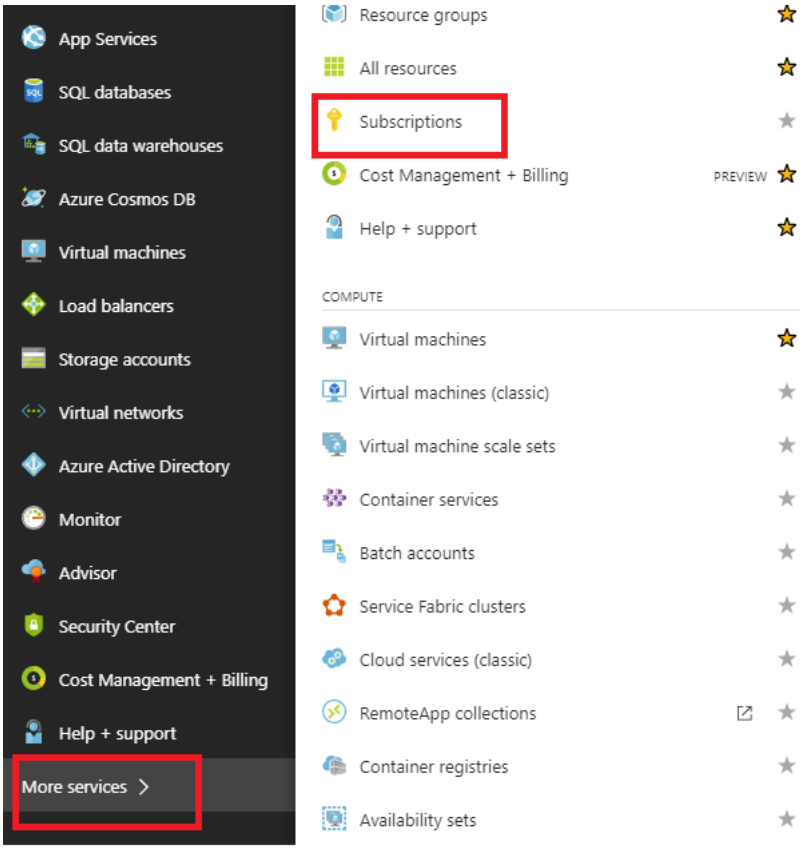


l) Der letzte erforderliche Punkt ist der ***öffentliche SSH-Schlüssel***. Dies kann mit Putty Key Generator oder ssh-keygen erstellt werden und wird für die Authentifizierung verwendet, sodass keine Passwörter für die Anmeldung erforderlich sind. Der öffentliche SSH-Schlüssel kann kopiert werden (einschließlich der Überschrift ssh-rsa und nachfolgender rsa-Schlüsselzeichenfolgen). Dieser öffentliche Schlüssel wird durch SD-WAN Center-Eingabe für den Citrix Zero Touch Deployment Service freigegeben.

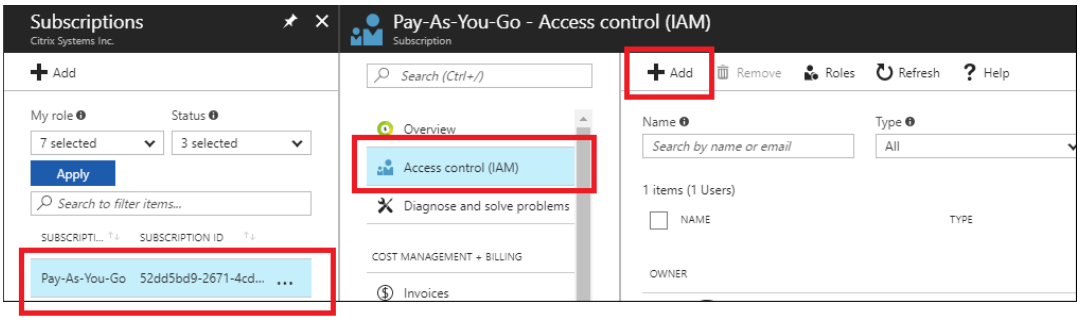


m) Zusätzliche Schritte sind erforderlich, um der Anwendung eine Rolle zuzuweisen.

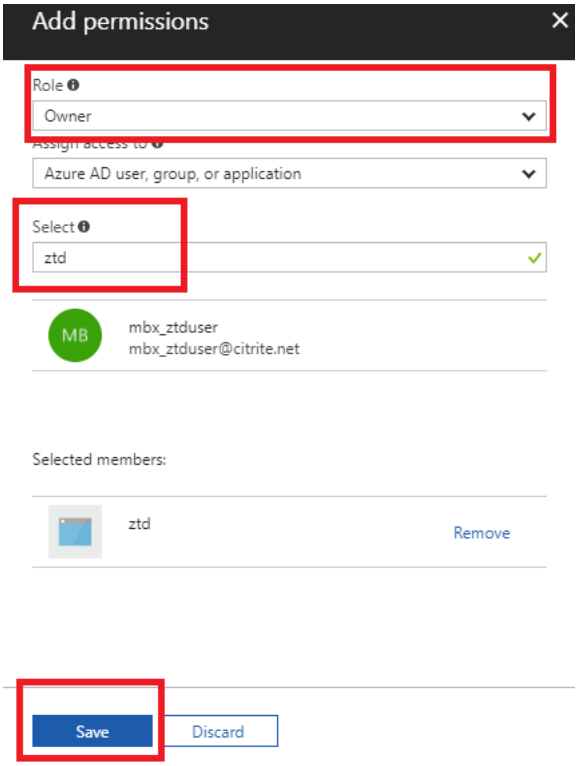
Navigieren Sie zurück zu Weitere Dienste und dann zu Abonnements.



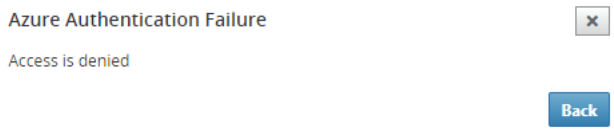
n) Wählen Sie das aktive Abonnement aus, dann **Zugriffssteuerung (AIM)**und klicken Sie anschließend auf **Hinzufügen.**



o) Wählen Sie im Bereich Berechtigungen hinzufügen die Rolle **Besitzer** aus, weisen Sie **Azure AD-Benutzern, Gruppen oder Anwendungen** Zugriff zu und suchen Sie im **Feld Auswählen** nach der registrierten App, damit der Zero Touch Deployment Cloud Service die Instanz im Azure-Abonnement erstellen und konfigurieren kann. Sobald die App identifiziert wurde, wählen Sie sie aus und stellen Sie sicher, dass sie als ausgewähltes Mitglied ausgefüllt wird, bevor Sie auf **Speichern**klicken.

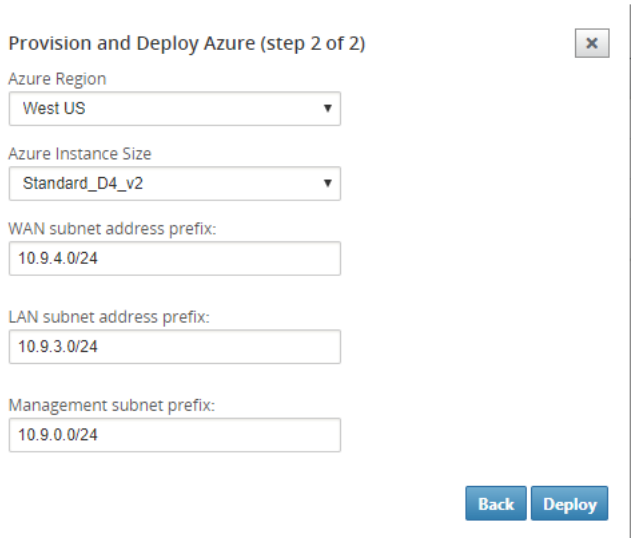


p) Nachdem Sie die erforderlichen Eingaben gesammelt und in das SD-WAN Center eingegeben haben, klicken Sie auf **Weiter**. Wenn die Eingaben nicht korrekt sind, tritt ein Authentifizierungsfehler auf.

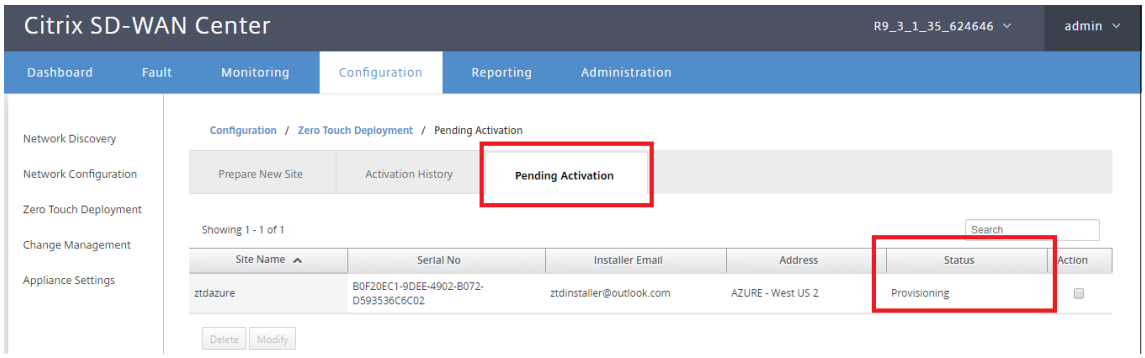


SD-WAN-Center Bereitstellung und Bereitstellung von Azure (Schritt 2 von 2)

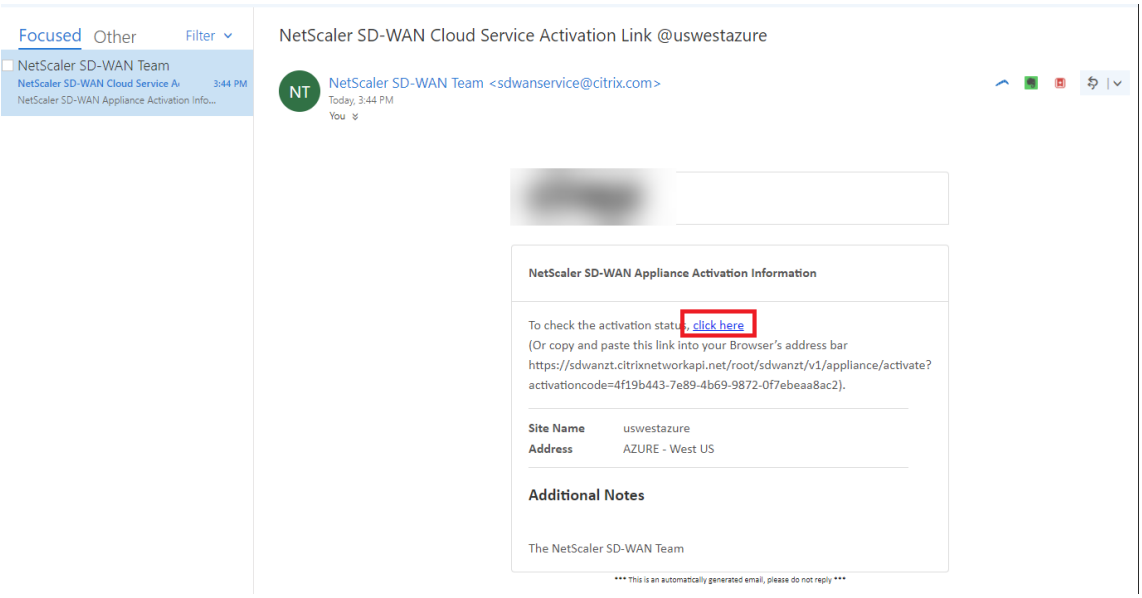
1. Füllen Sie nach erfolgreicher Azure-Authentifizierung die entsprechenden Felder aus, um die gewünschte Azure-Region und die entsprechende Instanzgröße auszuwählen, und klicken Sie dann auf **Bereitstellen**.



2. Wenn Sie im SD-WAN Center zur Registerkarte "**Ausstehende Aktivierung** "navigieren, können Sie den aktuellen Status der Bereitstellung verfolgen.

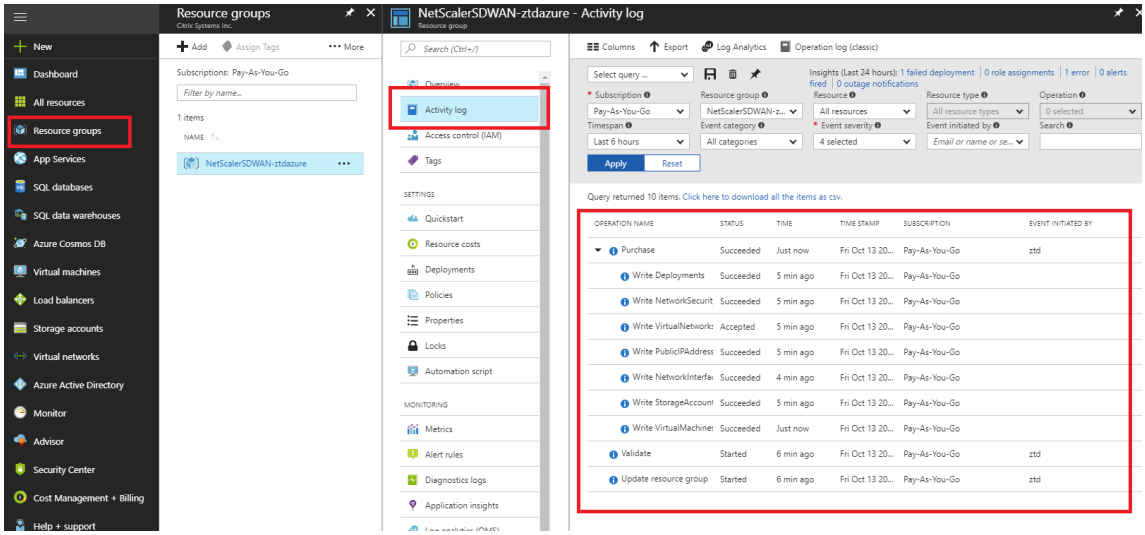


3. Eine E-Mail mit einem Aktivierungscode wird an die in Schritt 1 eingegebene E-Mail-Adresse gesendet, die E-Mail abgerufen und die **Aktivierungs-URL** geöffnet, um den Prozess auszulösen und den Aktivierungsstatus zu überprüfen.

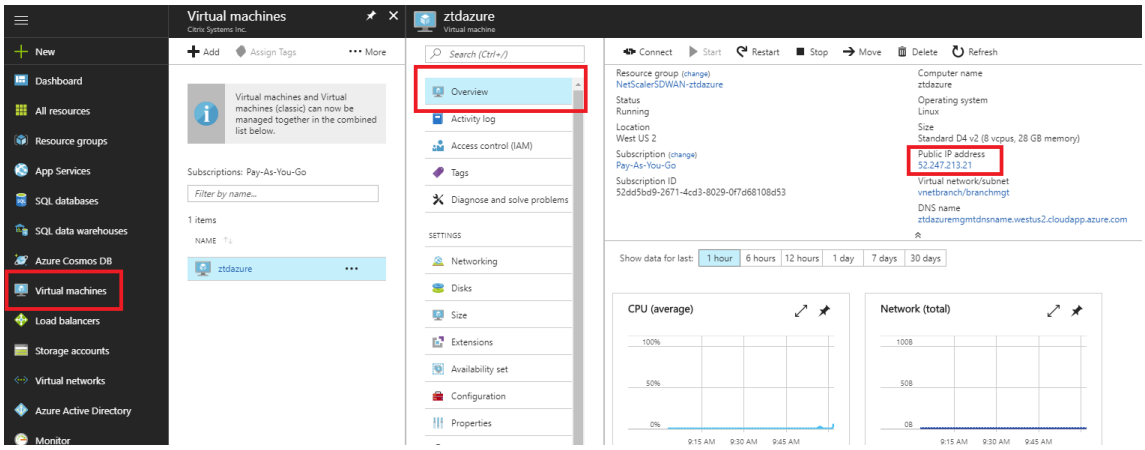


4. Eine E-Mail mit einer Aktivierungs-URL wird an die in Schritt 1 eingegebene E-Mail-Adresse gesendet. Rufen Sie die E-Mail ab und öffnen Sie die **Aktivierungs-URL**, um den Prozess auszulösen und den Aktivierungsstatus zu überprüfen.

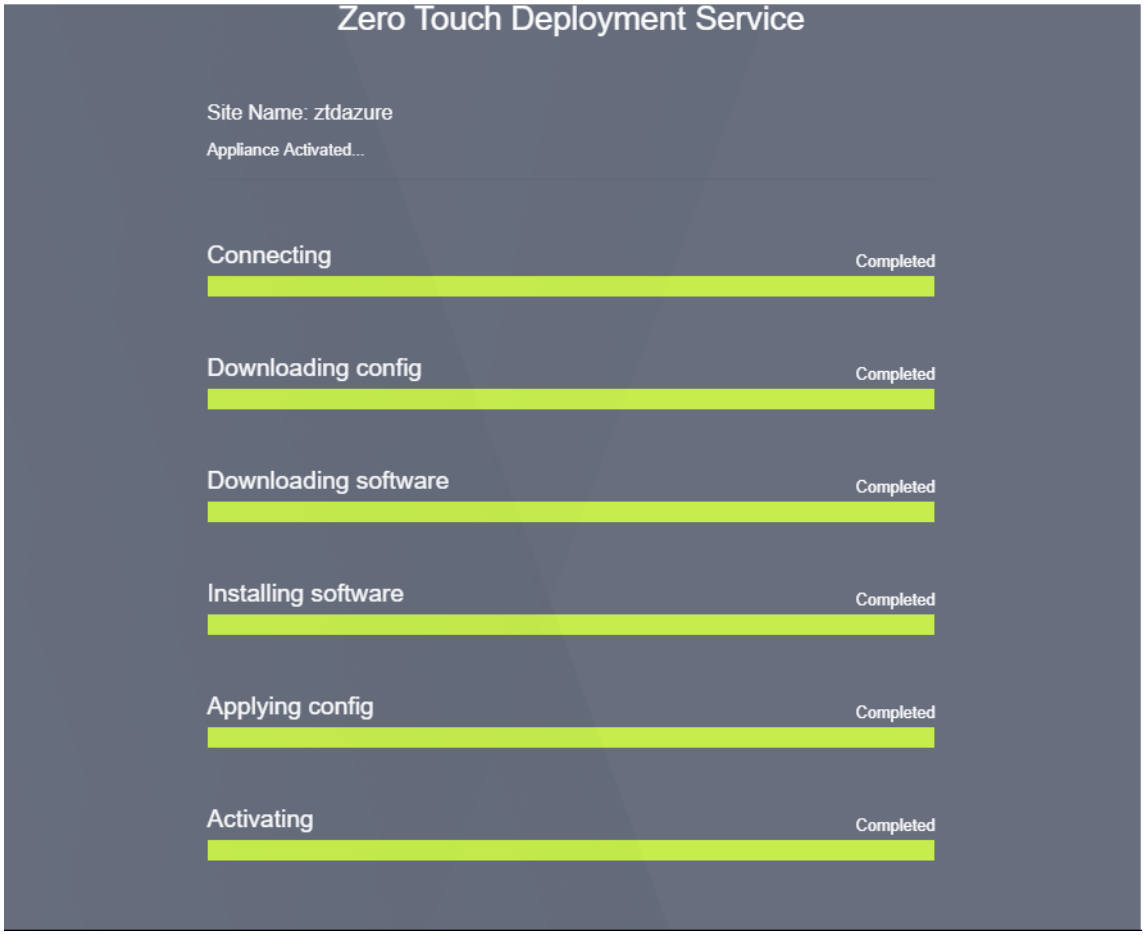
5. Es dauert einige Minuten, bis die Instanz vom SD-WAN Cloud Service bereitgestellt wird. Sie können die Aktivität im Azure-Portal unter **Aktivitätsprotokoll** für die **Ressourcengruppe** überwachen, die automatisch erstellt wird. Alle Probleme oder Fehler bei der Bereitstellung werden hier aufgefüllt und im Aktivierungsstatus auf SD-WAN Center repliziert.



6. Im Azure-Portal wird die erfolgreich gestartete Instanz unter **Virtuelle Maschinen verfügbar sein.** Um die zugewiesene öffentliche IP zu erhalten, navigieren Sie zur Übersicht für die Instanz.

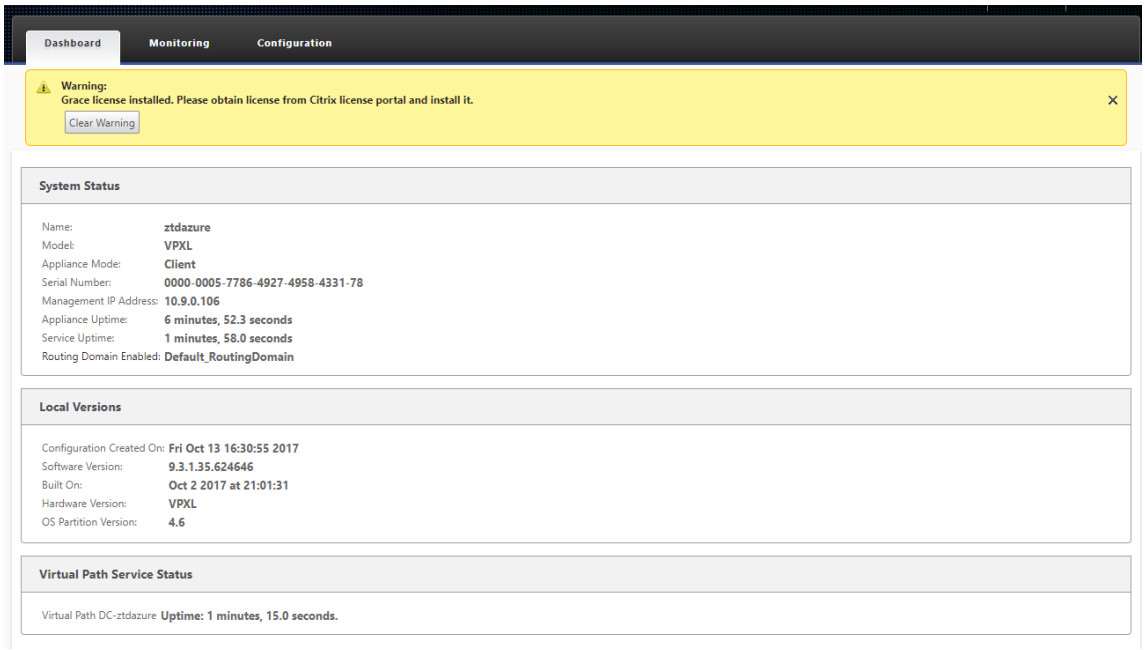


7. Nachdem sich die VM in einem laufenden Zustand befindet, geben Sie ihr eine Minute Zeit, bevor der Dienst Kontakt aufnimmt und mit dem Herunterladen der Konfiguration, Software und Lizenz beginnt.

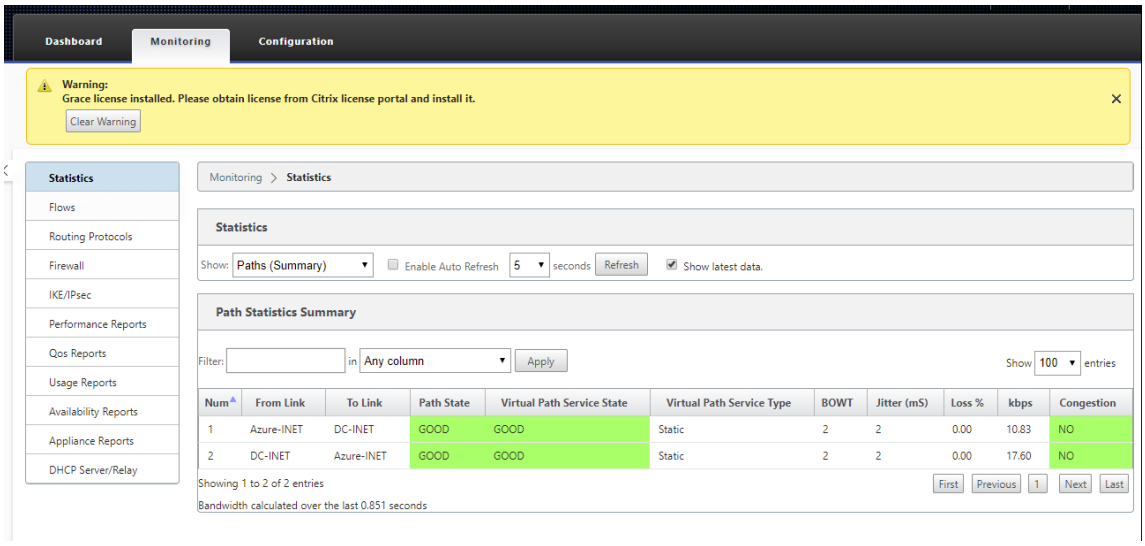


8. Nachdem die einzelnen SD-WAN-Cloud-Dienstschritte automatisch kompliziert sind, melden

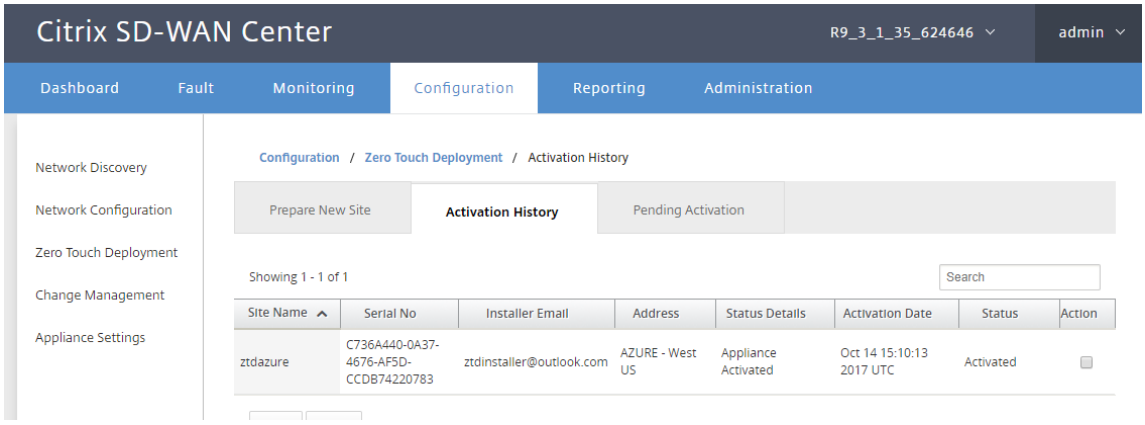
Sie sich bei der Webschnittstelle von SD-WAN-Instanzen mit der öffentlichen IP-Adresse an, die vom Azure-Portal abgerufen wurde.



9. Auf der Seite Citrix SD-WAN Monitoring Statistics wird die erfolgreiche Konnektivität vom MCN zur SD-WAN-Instanz in Azure identifiziert.



10. Darüber hinaus wird der erfolgreiche (oder erfolglose) Bereitstellungsversuch auf der Seite Aktivierungsverlauf des SD-WAN Centers protokolliert.



Bereitstellung in einer Region

October 28, 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 Standardregion.

Statische und dynamische virtuelle Pfade sind zwischen Regionen nicht zulässig. RCNs verwalten den Datenverkehr zwischen Regionen.

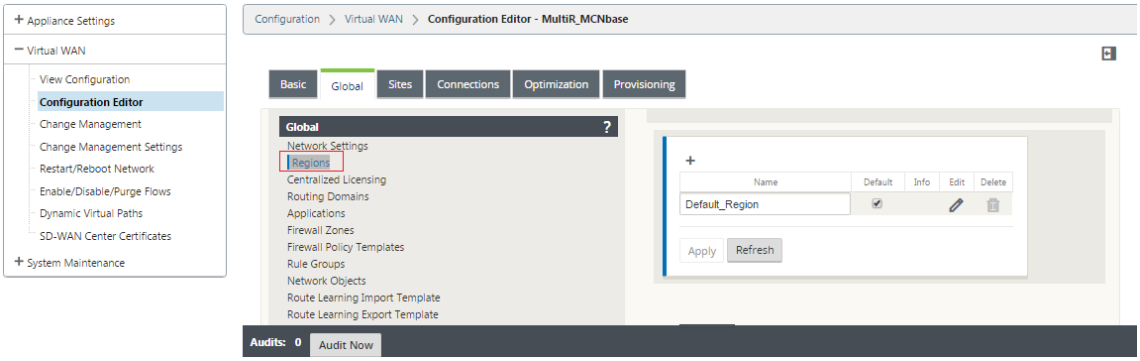
Eine Bereitstellung in einer Region in einem SD-WAN-Netzwerk kann Netzwerkstandorte mit weniger als 550 unterstützen.

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.

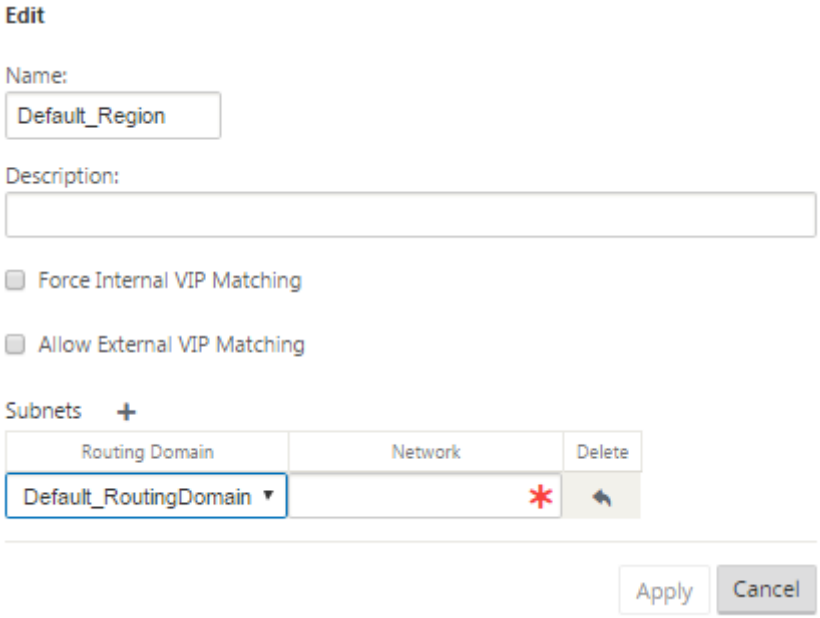
So konfigurieren Sie die Bereitstellung einer einzelnen Region:

1. Navigieren Sie im Konfigurationseditor zur Registerkarte **Global**. Wählen Sie **Regionen**aus. Die standardmäßigen Region-Konfigurationsoptionen 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.
   - Zulässiges externes 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.



5. Wählen Sie eine **Routingdomäne** aus, geben Sie die **Netzwerkadresse** ein. Klicken Sie auf **Apply**. Die Netzwerkadresse ist die IP-Adresse und die Maske für das Subnetz.

Bereitstellung in mehreren Regionen

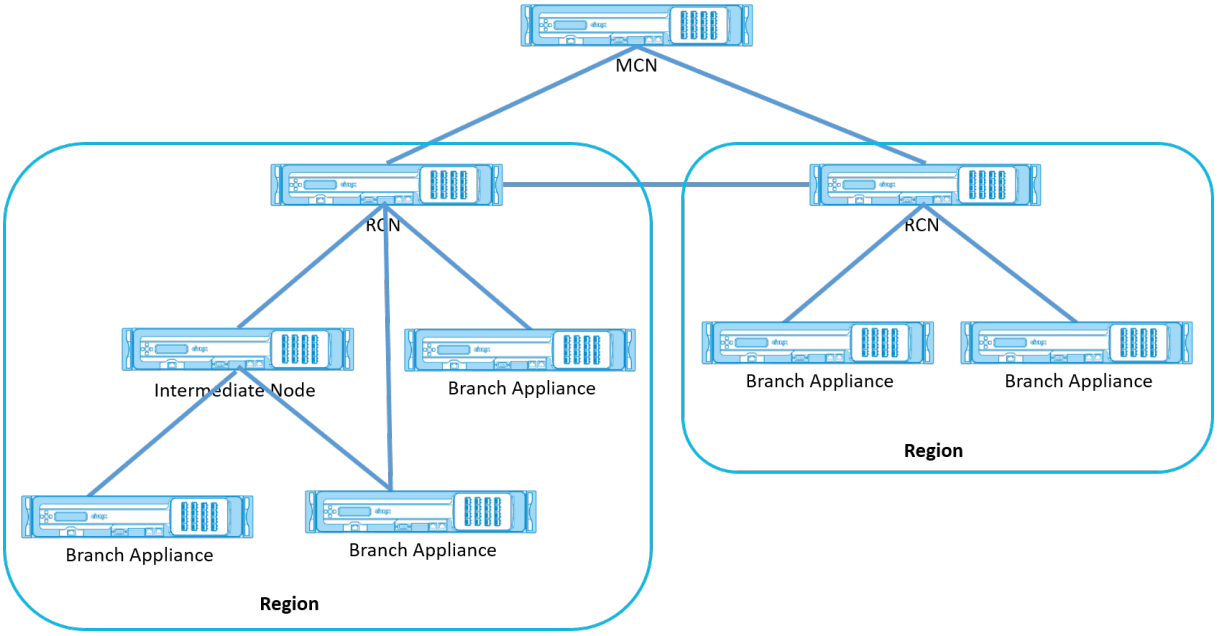
October 28, 2021

Eine SD-WAN-Appliance, die als Master Control Node (MCN) konfiguriert ist, unterstützt die Bereitstellung mehrerer Regionen. Der MCN verwaltet mehrere regionale Kontrollknoten (RCNs). Jeder RCN wiederum verwaltet mehrere Clientsites. 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.

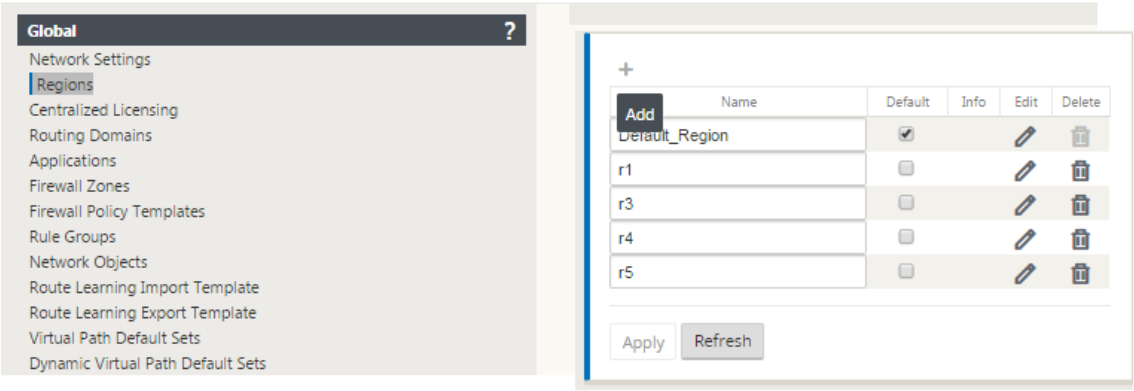
Plattform-Edition	Primär-/Sekundär-MCN	Primär/Sekundär-RCN
110-SE	Nein	Nein
210-SE	Ja	Ja
400-SE	Ja	Nein
410-SE	Ja	Nein
1000-SE, 1000-PE	Ja	Nein
1100-SE, 1100-PE	Ja	Ja
VPX-SE, VPXL-SE	Ja	Ja
2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE	Ja	Ja

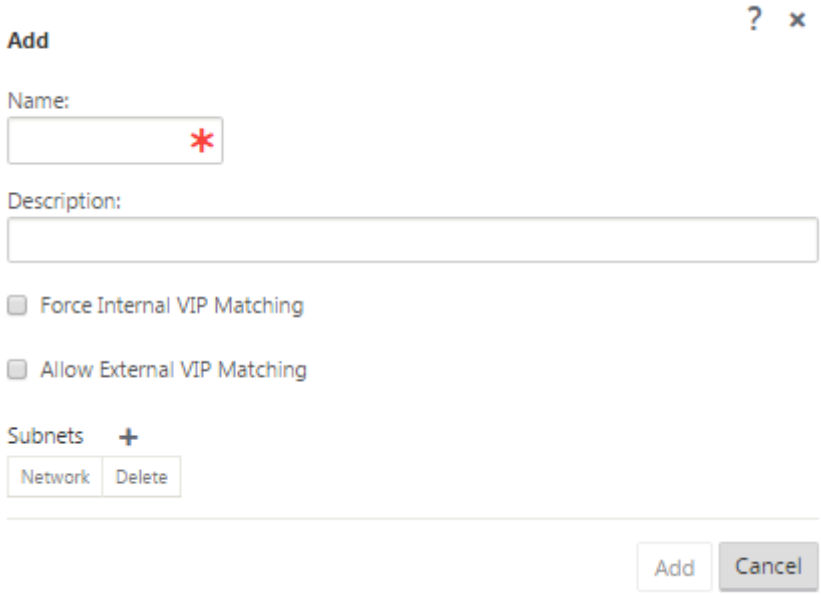
So konfigurieren Sie die Bereitstellung mit mehreren Regionen für ein SD-WAN-Netzwerk:

1. Navigieren Sie im Konfigurationseditor zur Registerkarte **Global**. Wählen Sie **Regionen**aus. Die standardmäßigen Region-Konfigurationsoptionen werden angezeigt.

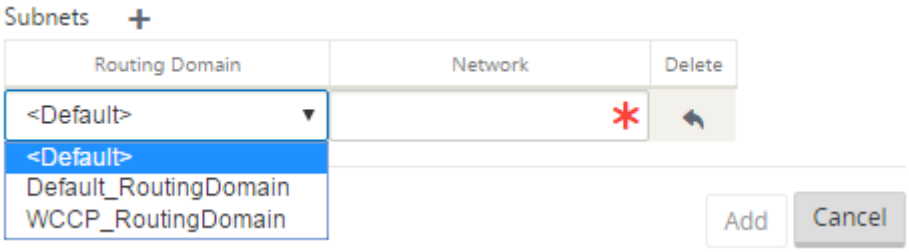
   Sie können den Namen und die Beschreibung für den Standardbereich ändern, indem Sie ihn bearbeiten.

2. Klicken Sie auf **+ Hinzufügen**, um eine neue Region hinzuzufügen.



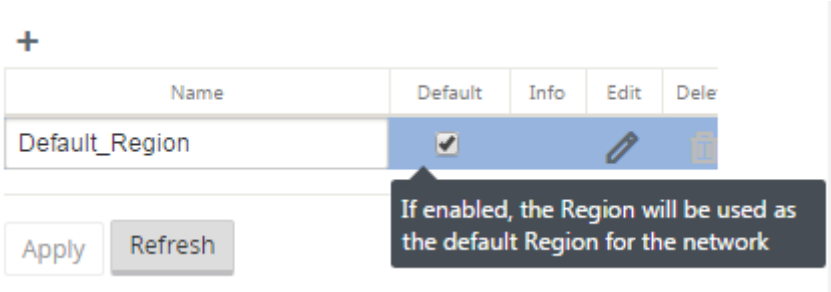


3. Geben Sie einen Namen und eine Beschreibung für den Teilsektor ein.
4. Aktivieren Sie den internen VIP-Abgleich je nachdem, ob Sie einen **erzwungenen internen VIP-Abgleich** oder **einen externen VIP-Abgleich zulassen** möchten
   - Erzwungene interne VIP: Wenn diese Option aktiviert ist, müssen alle nicht-privaten virtuellen IP-Adressen in der Region mit den konfigurierten Subnetzen übereinstimmen.
   - Zulässiges externes 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.



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 Clientsite klonen.

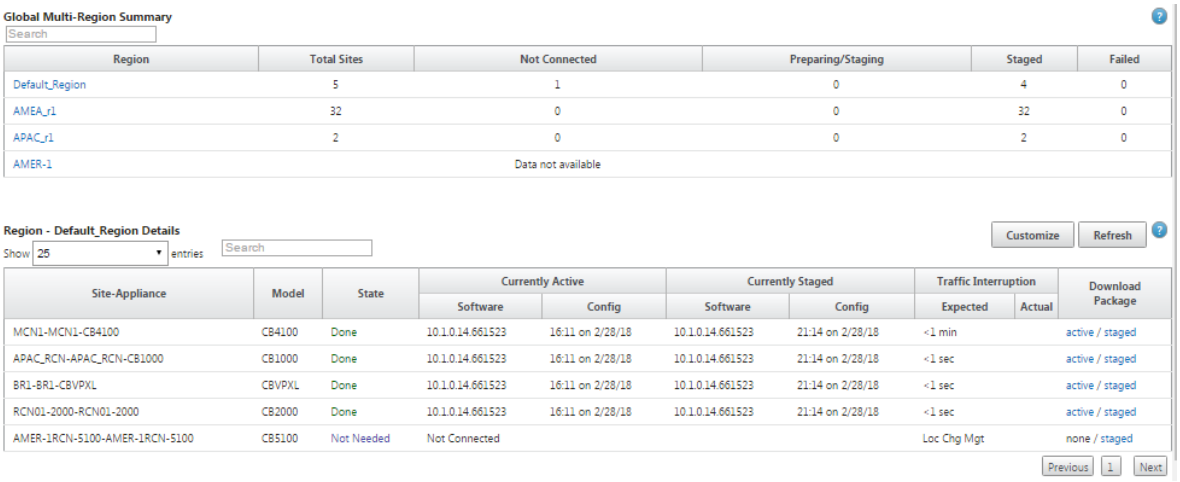
Das SD-WAN Center unterstützt die Bereitstellung mehrerer Regionen. Weitere Informationen finden Sie unter SD-WAN Center Multi-Region-Bereitstellung und Berichterstattung.

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

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

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

Show 25 entries Search

Customize Refresh

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

Previous 1 2 Next

> **Hinweis**
>
> In einigen Fällen ist der in der Tabelle **Globale Multi-Region-Übersicht** angezeigte Wert für die **Gesamtzahl der Sites** geringer 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 s-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 im 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

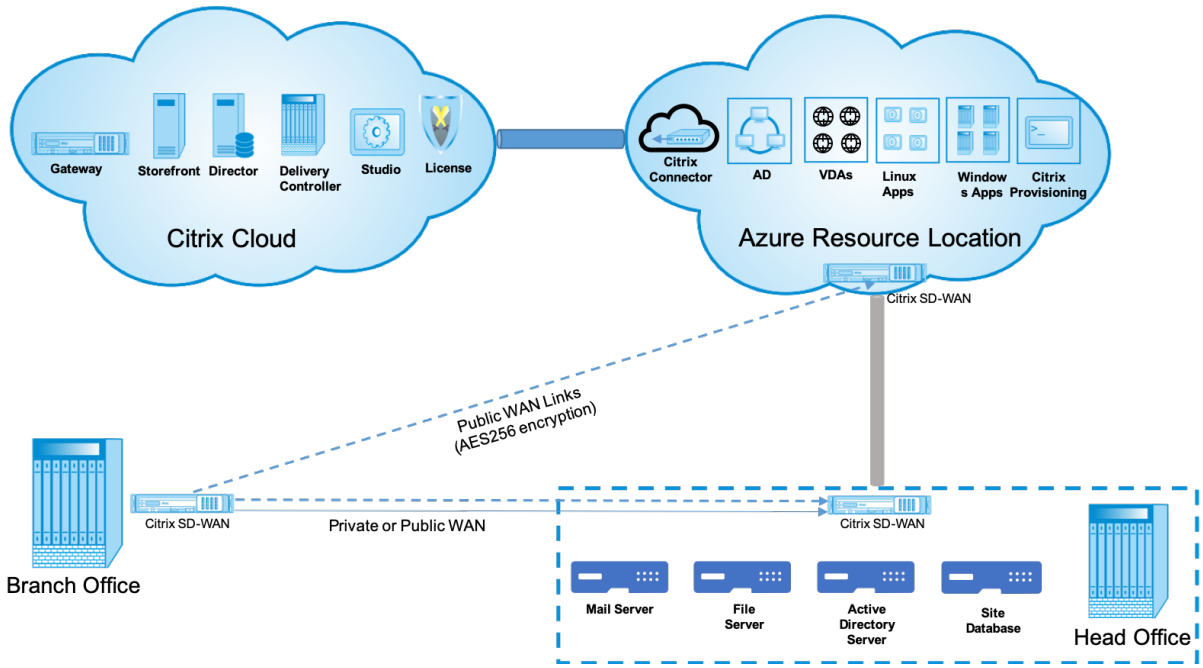
Voraussetzungen

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 Rechenzentrumsumgebung), 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 und entweder im Zweigmodus 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.

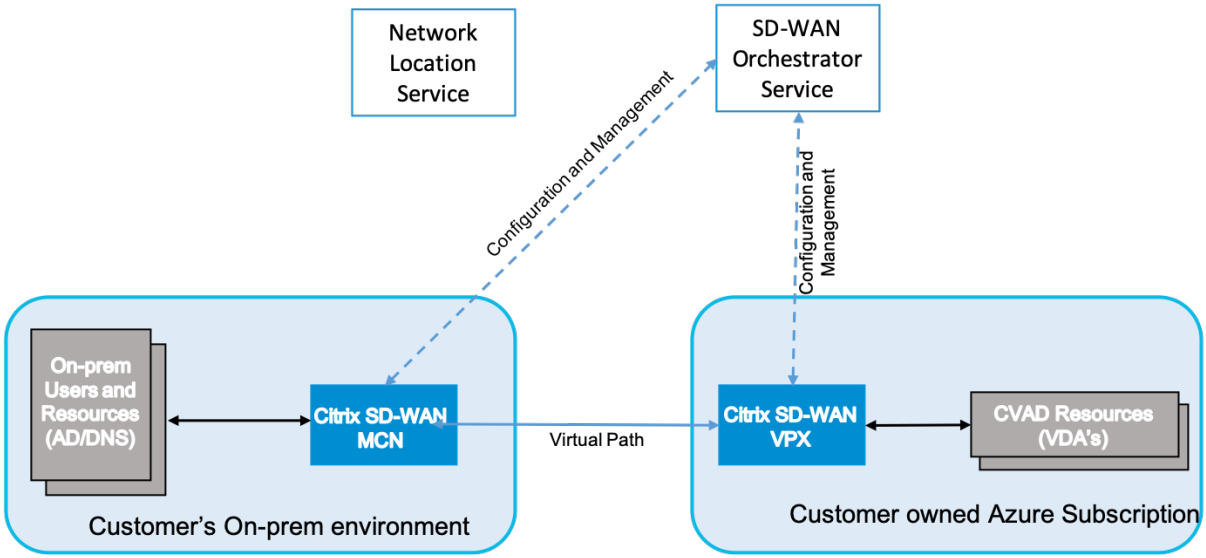
  Mit dem Citrix Virtual Apps and Desktops s-Dienst können Sie sichere virtuelle Apps und Desktops auf jedem Gerät bereitstellen und den Großteil der Produktinstallation, Setup, Konfiguration, Upgrades und Überwachung von Citrix überlassen. Sie behalten die vollständige Kontrolle über Anwendungen, Richtlinien 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 SD-WAN Orchestrator verwenden, um mehrere Kunden mit einem einzigen Fensterbereich 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 (im Falle einer HA-Bereitstellung) erstellt, indem diese Instanzen über 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.

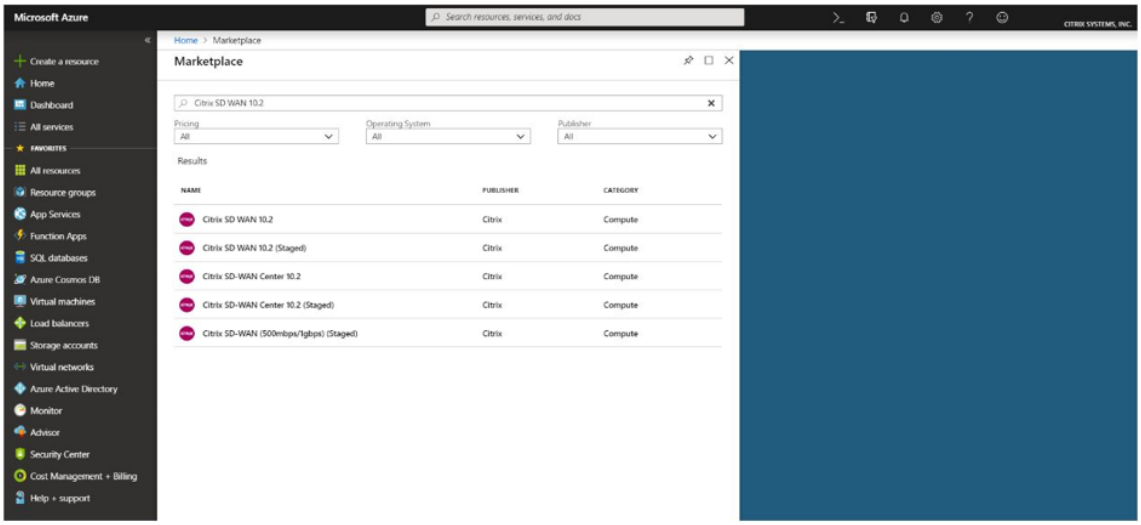
Die dritte Komponente dieser Integration ist der **Network Location Service (NLS)**, der es internen Benutzern ermöglicht, das Gateway zu Bypass und sich direkt mit den VDAs zu verbinden, wodurch die Latenz für den internen Netzwerkverkehr reduziert wird. Sie können NLS manuell oder über Citrix SD-WAN 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. Gehen Sie in einem Webbrowser zum 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.

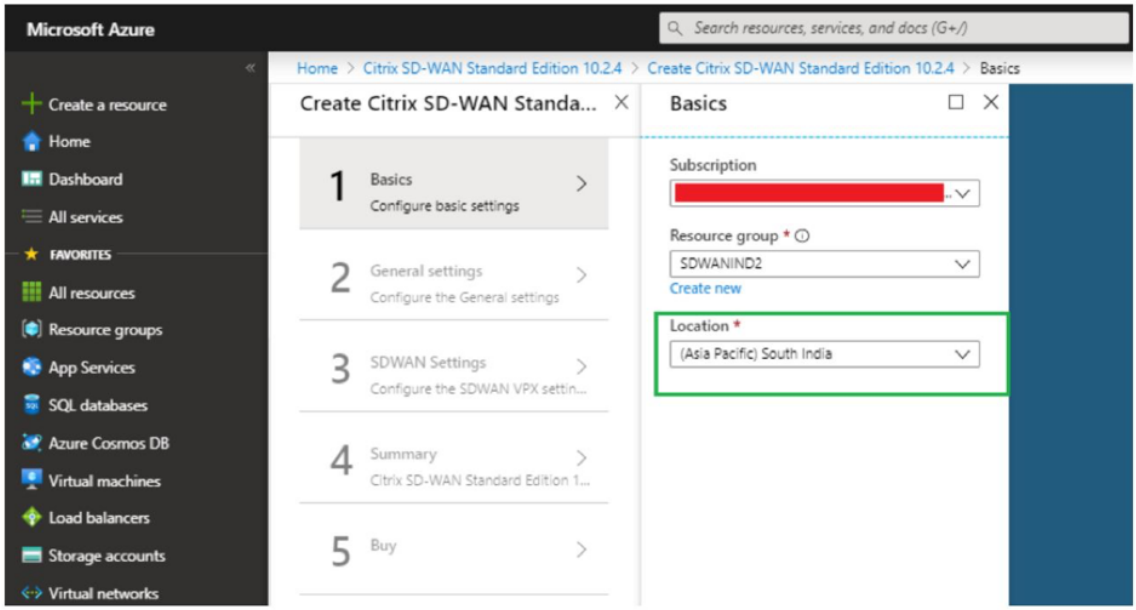


   Klicken Sie auf **Erstellen**, einen Assistenten, der mit den erforderlichen Details zum Erstellen der virtuellen Maschine auffordert.

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.

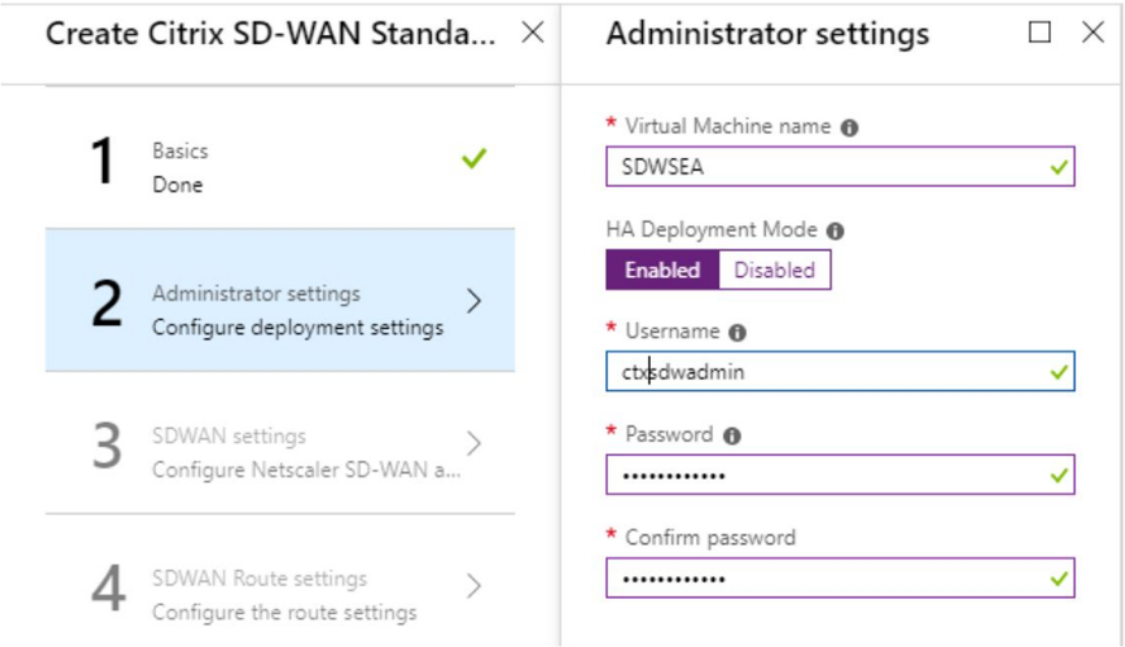
   Für Citrix SD-WAN wird empfohlen, dass die ausgewählte Ressourcengruppe leer sein muss. Wählen Sie in ähnlicher Weise die Azure-Region aus, in der Sie die SD-WAN-Instanz bereitstellen möchten. Die Region muss mit der Region identisch sein, in der Ihre Citrix Virtual Apps and Desktops Ressourcen bereitgestellt 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**.

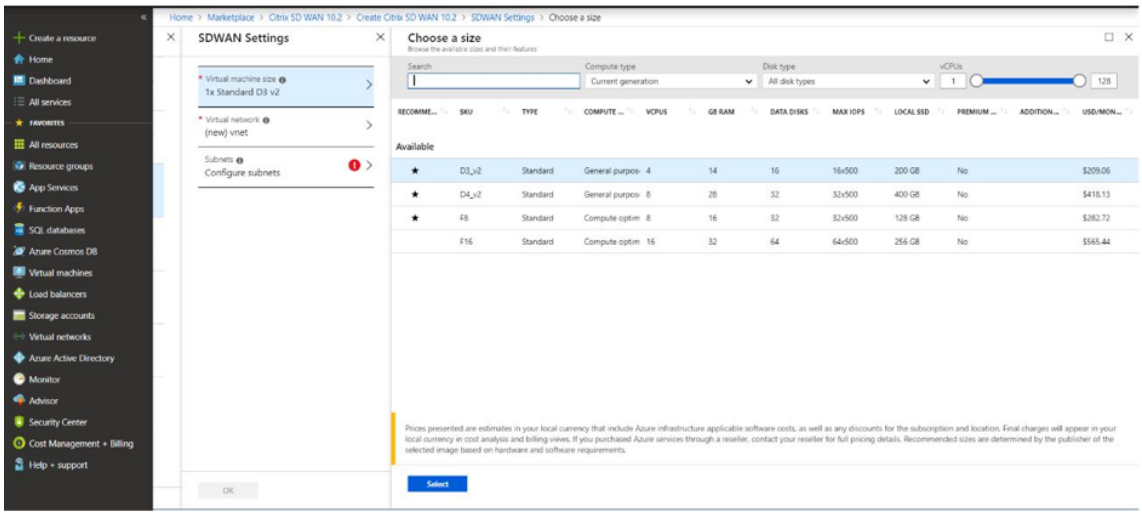
   Dieses Kennwort ist erforderlich, um sich als Gastbenutzer an der Verwaltungsoberfläche der Instanz anzumelden. Um Admin-Zugriff auf die Instanz zu erhalten, verwenden Sie admin als Benutzernamen und das Kennwort, das während der Provisioning der Instanz erstellt wurde. Wenn Sie den Benutzernamen verwenden, 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.

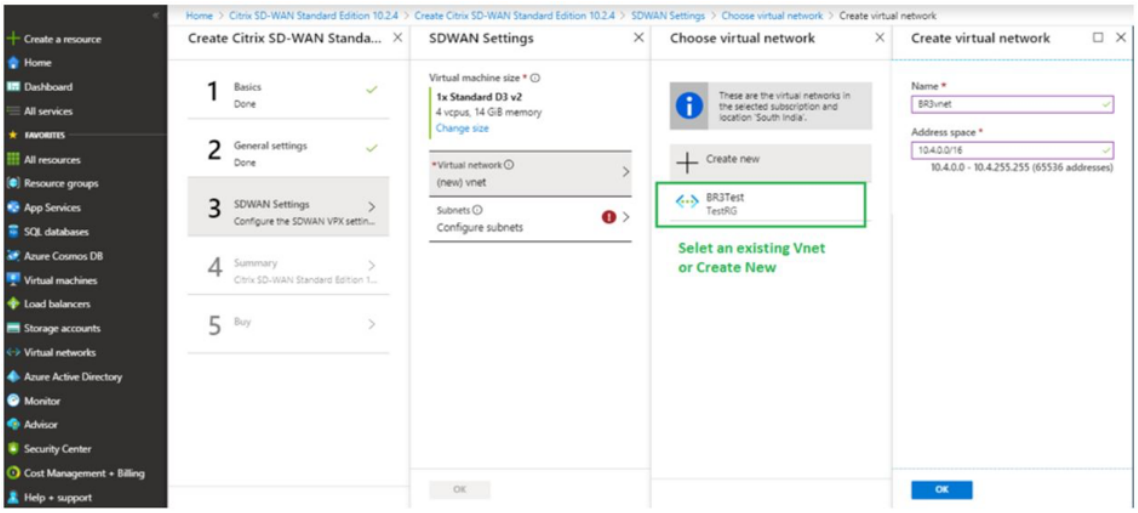


5. Wählen Sie auf der **SD-WAN-Einstellungsseite** die Instanz aus, in der Sie das Image ausführen möchten. Wählen Sie den folgenden Instanz-Typ gemäß Ihrer Anforderung:

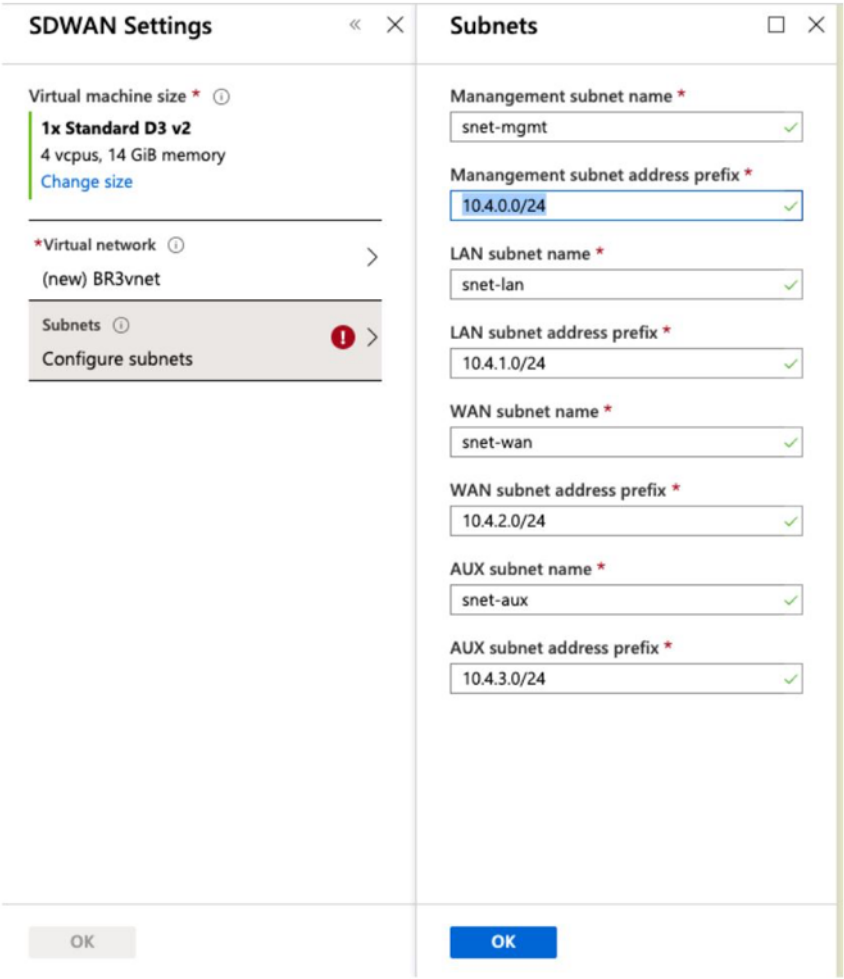
   - Instanztyp D3_V2 für maximalen unidirektionalen Durchsatz von 200 Mbit/s mit direkter Konnektivität zu maximal 16 Zweigen.
   - Instanztyp D4_V2 für maximalen unidirektionalen Durchsatz von 500 Mbit/s mit direkter Konnektivität zu maximal 16 Zweigen.
   - Instanztyp F8 Standard für maximalen unidirektionalen 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.



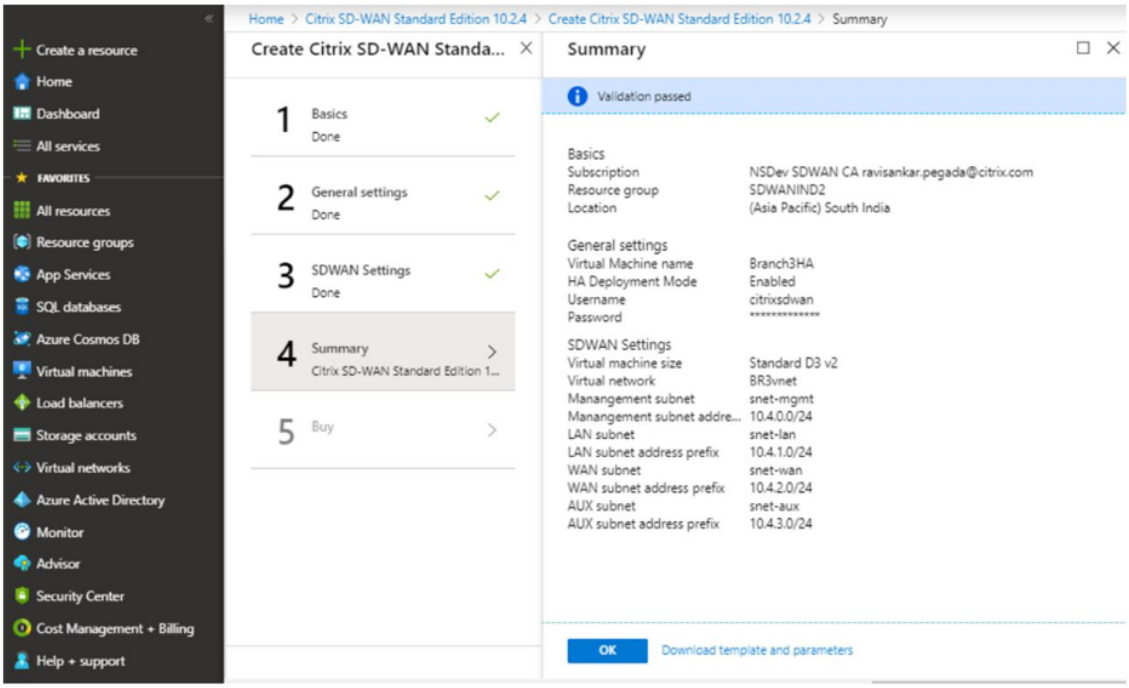
6. Erstellen Sie ein neues virtuelles Netzwerk (VNet) oder verwenden Sie ein vorhandenes VNet. Dies ist der wichtigste Schritt für die Bereitstellung, da in diesem Schritt die Subnetze ausgewählt werden, die den Schnittstellen der SD-WAN VPX-VM zugewiesen werden sollen.



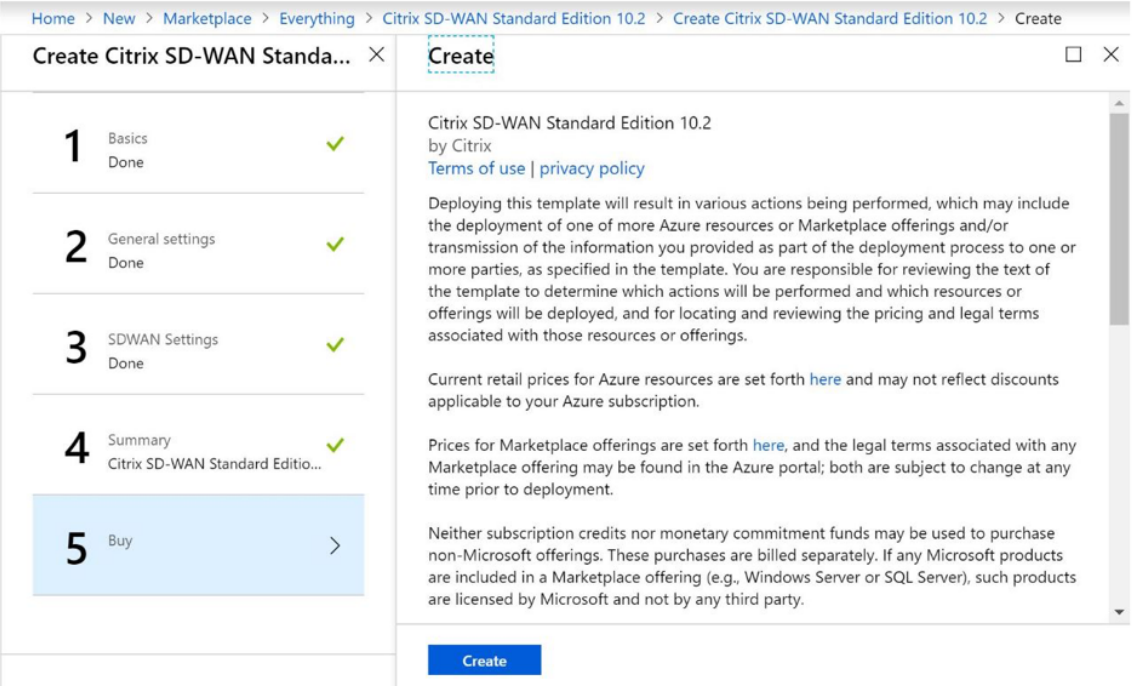
Das Aux-Subnetz wird nur benötigt, wenn Sie die Instanzen im HA-Modus bereitstellen. Stellen Sie sicher, dass die SD-WAN-Instanz im selben VNet wie Ihre Citrix Virtual Apps and Desktops-Ressourcen bereitgestellt wird und sich im selben Subnetz wie die LAN-Schnittstelle der SD-WAN VPX-Appliance befindet.



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.

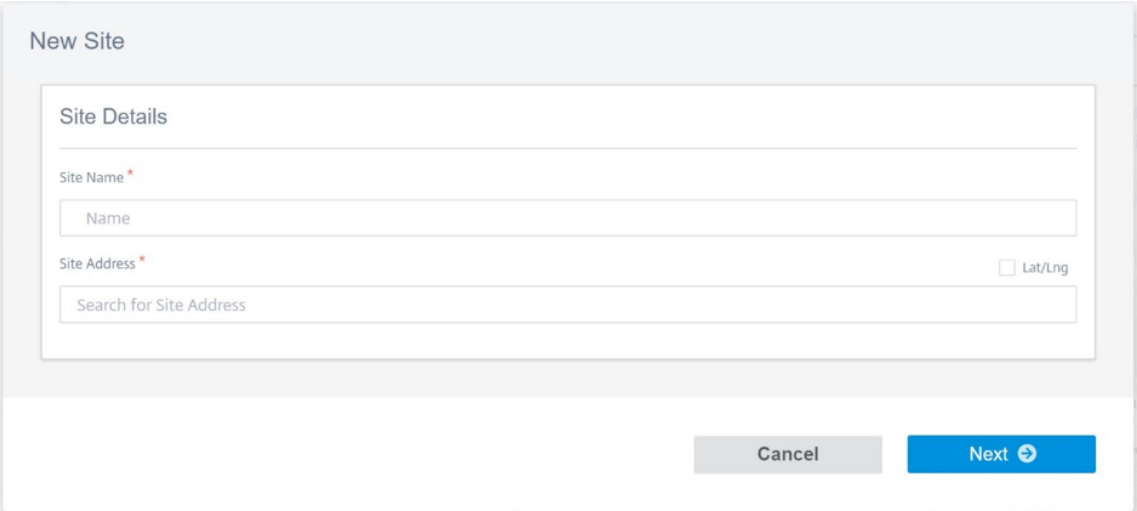


Nachdem die Instanz erfolgreich erstellt wurde, rufen Sie die öffentliche IP ab, die der Verwaltungsschnittstelle der SD-WAN-Instanz zugewiesen ist. Sie finden sie unter dem Netzwerkab-

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, verweisen Sie auf Citrix SD-WAN Orchestrator Onboarding.
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).

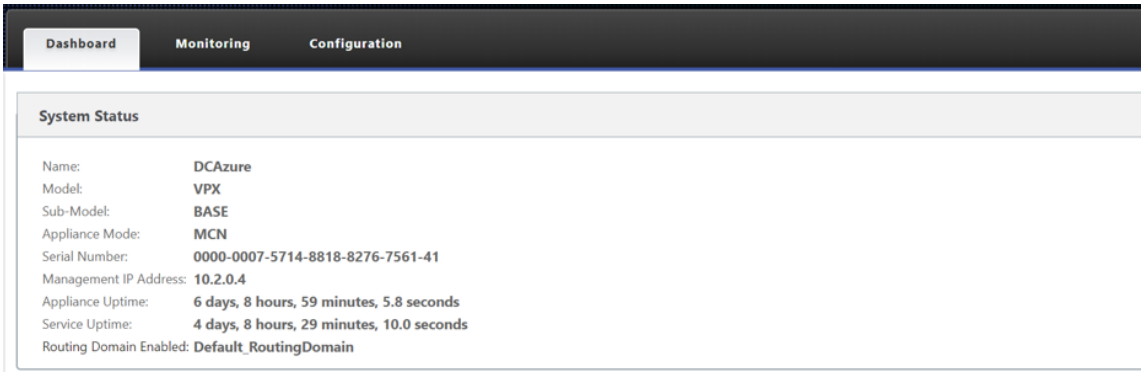


12. Geben Sie einen eindeutigen Site-Namen an, und geben Sie die Adresse basierend auf der Region ein, in der Sie das Image Provisioning. Informationen zum Einrichten der Instanz in Azure finden Sie unter Grundeinstellungen.

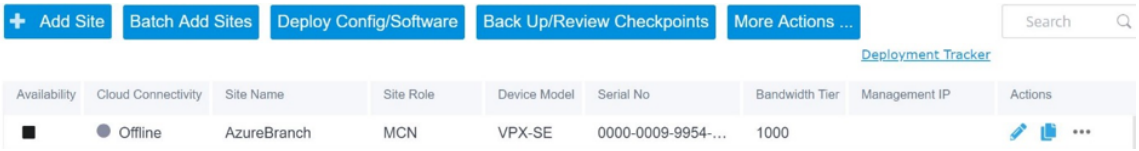
> **Hinweis**
>
> Um die Seriennummer der Instanz in Azure abzurufen, melden Sie sich über die Public Management IP bei der Instanz an. Sie können die Seriennummer auf dem Dashboard-Bildschirm sehen. Wenn Sie Instanzen in HA konfigurieren, müssen beide Seriennummern erfasst werden. Stellen Sie außerdem 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 Home**navigieren.

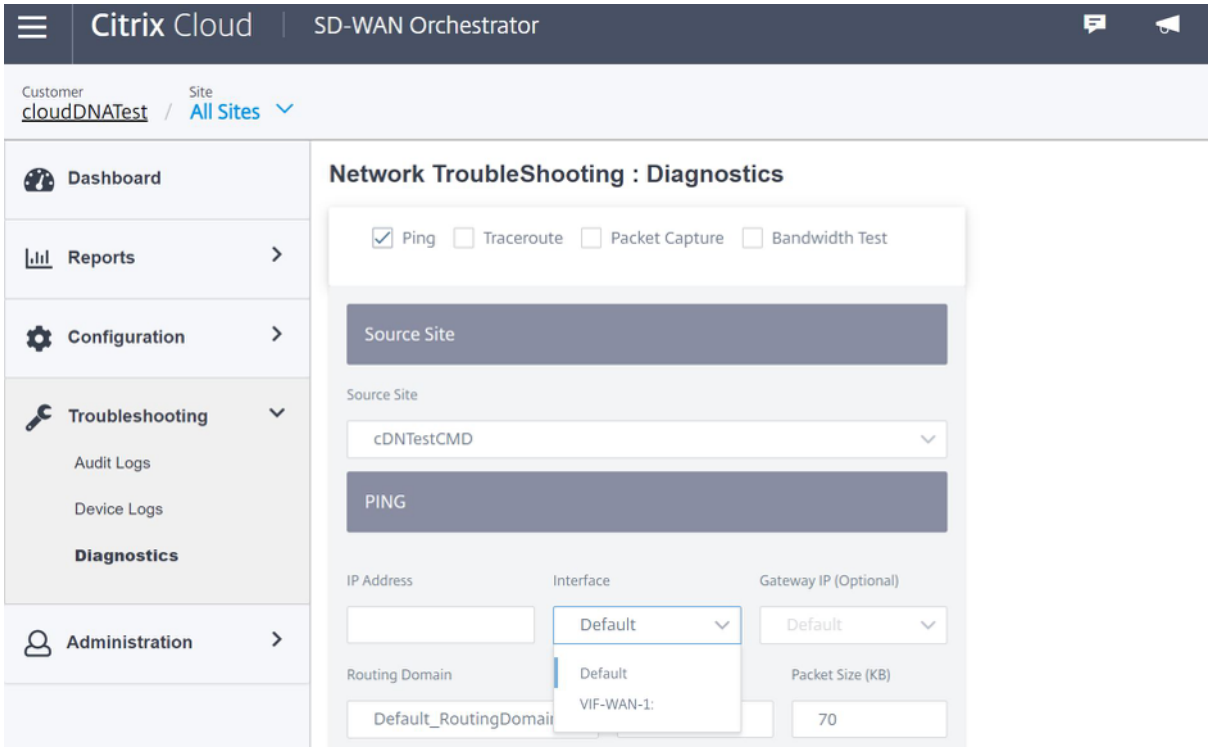


15. Wenn es keine Probleme gibt und die Konfiguration korrekt ist, müssen Sie die virtuellen Pfade zwischen der Instanz in Azure und Ihrem MCN haben, sobald die Konfigurationsbereitstellung ausgeführt wurde.

Konfiguration von Citrix Virtual Apps and Desktops

Wie im Abschnitt Bereitstellung und Konfiguration hervorgehoben, befindet sich das AD/DNS on-premises Standort, der als DC fungiert, und in einer Bereitstellung mit SD-WAN, die sich hinter dem SD-WAN befindet, das sich im LAN-Netzwerk befindet. 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 > Diagnose**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.



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**: Ausführliche Informationen zur Konfiguration von NLS mit Citrix SD-WAN Orchestrator finden Sie unter Netzwerkstandortdienst.
- **Netzwerkstandortdienst PowerShell-Modul, das Citrix bereitstellt**: Ausführliche Informationen zur Konfiguration von NLS mithilfe des PowerShell-Moduls 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

October 28, 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.

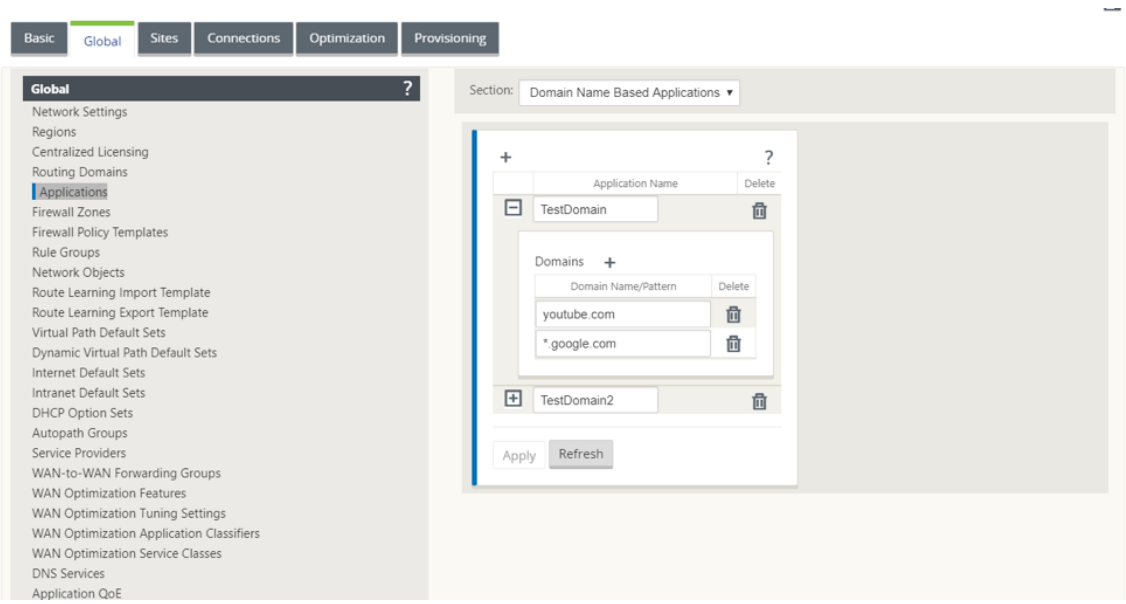
DNS-Proxy

Sie können einen Proxy mit mehreren Weiterleitungen konfigurieren, mit denen DNS-Anfragen basierend auf Anwendungsdomänennamen gesteuert werden können. Die DNS-Weiterleitung funktioniert für die Anfragen, die über UDP-Verbindungen empfangen werden.

So konfigurieren Sie SD-WAN als DNS-Proxy:

1. Definieren Sie die auf Domainnamen basierenden Anwendungen. Navigieren Sie im Konfigurationseditor zu **Global > Anwendungen > Domänennamen-basierte Anwendungen**.

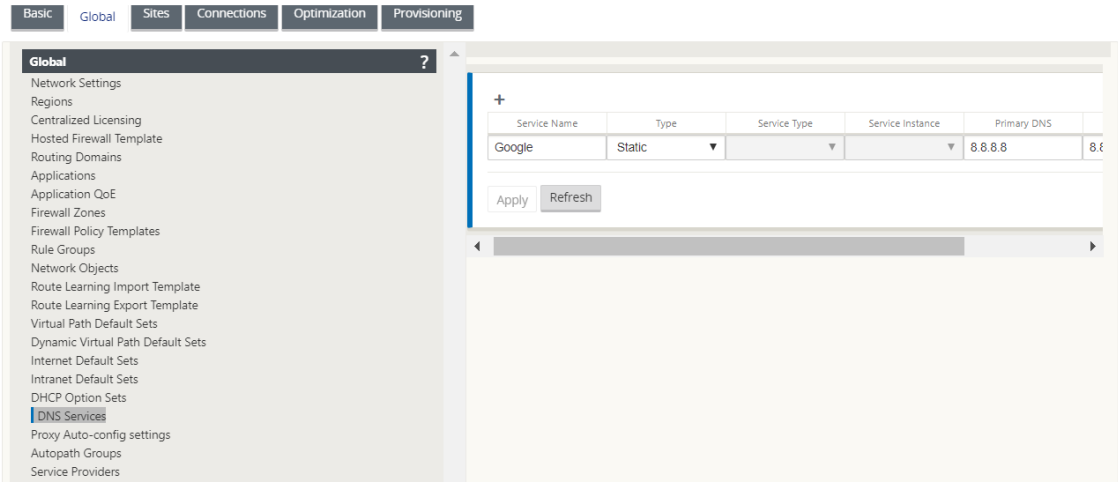
   Geben Sie den Anwendungsnamen und die erforderlichen Domainnamen oder -muster ein. Sie können mehrere Domainnamen als Anwendung gruppieren. Sie können entweder den vollständigen Domainnamen eingeben oder am Anfang Wildcards verwenden. Zum Beispiel - *.google.com



2. Definieren Sie die erforderlichen DNS-Dienste. Sie können statischen oder dynamischen DNS-Dienst definieren.

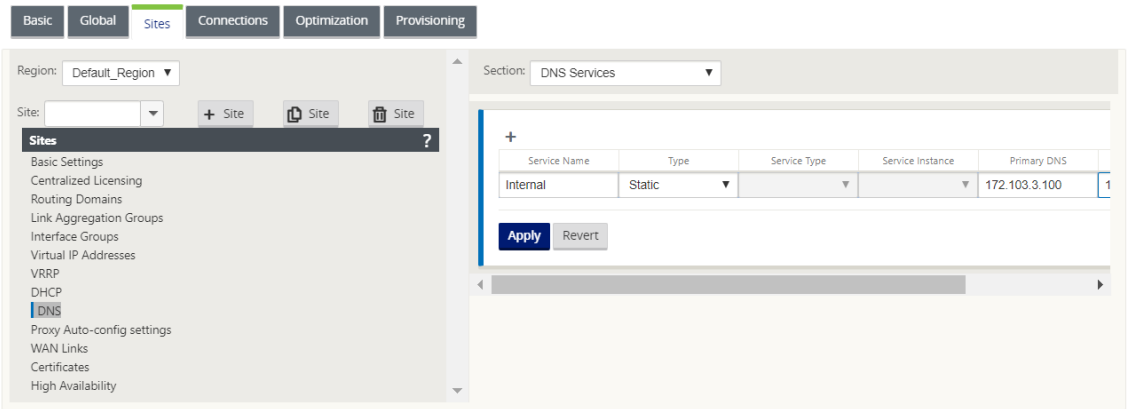
   Um einen statischen DNS-Dienst zu konfigurieren, navigieren Sie zu **Global** > **DNS Service**und

wählen Sie den **Typ** als **Statisch**aus. Geben Sie den **Dienstnamen** und ein Paar primäre und sekundäre DNS-Server-IP-Adressen ein.



> **Hinweis**
>
> Wenn Sie Office 365-Breakout-Richtlinie konfiguriert haben, wird automatisch ein Quad9-DNS-Dienst erstellt. Weitere Informationen finden Sie unter Office 365-Optimierung.

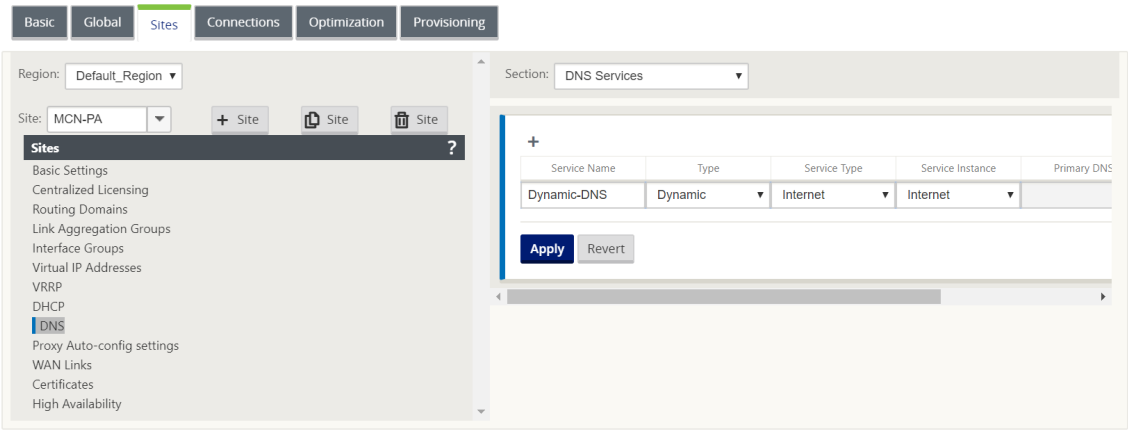
Alternativ können Sie die statischen DNS-Dienste auch auf individueller Standortebene definieren. Die Konfiguration des DNS-Dienstes auf Standortebene überschreibt die globale Konfiguration. Um den standortspezifischen statischen DNS-Dienst zu konfigurieren, navigieren Sie zu **Sites** > **DNS** > **DNS Services** und wählen Sie den **Typ** als **Statisch**aus.



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.

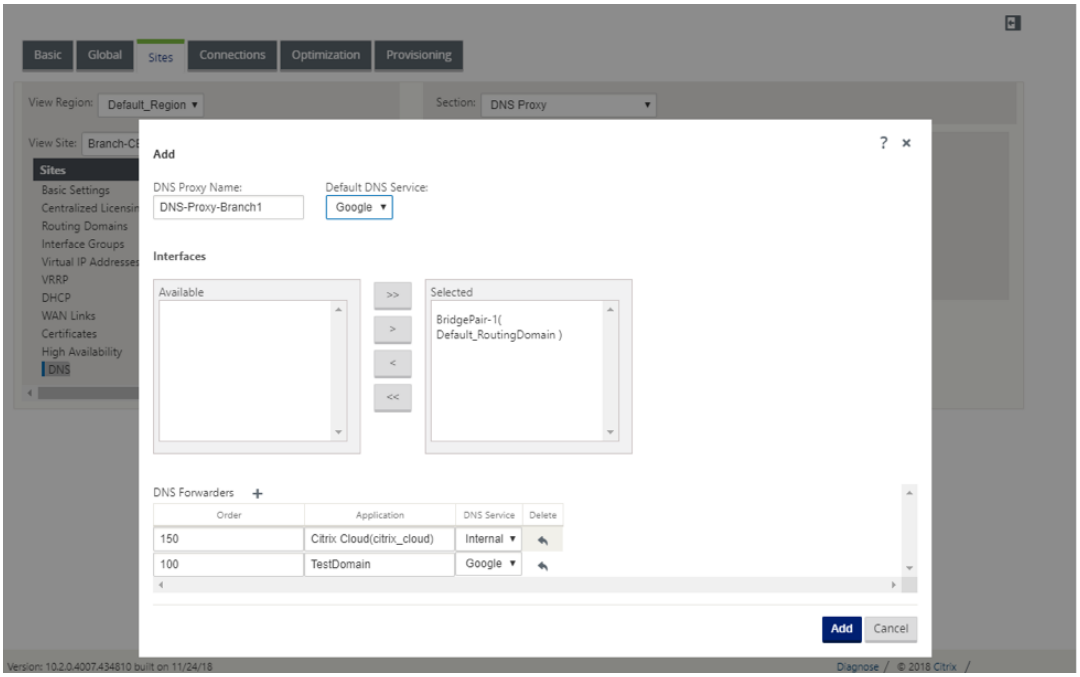
> **Hinweis**

> 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-Proxy-Name**: Name des DNS-Proxys.
   - **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-Forwarder**: Liste der DNS-Forwarder.
     - **Auftrag**: Die Priorität des Spediteurs.
     - **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.

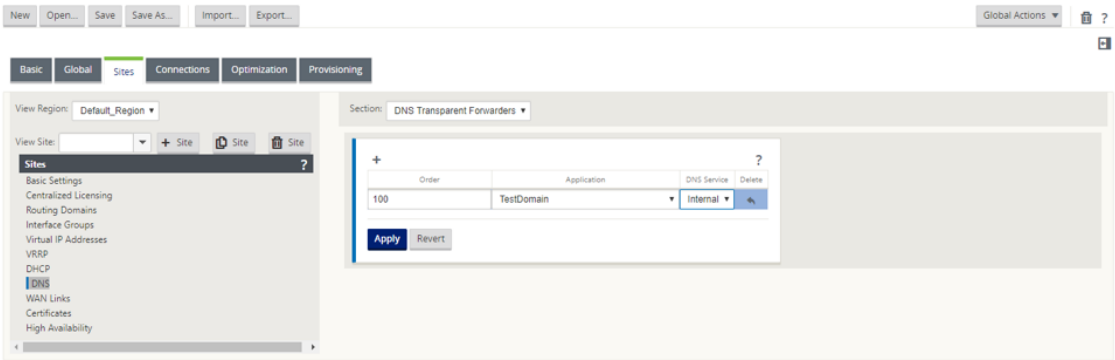


Transparente DNS-Weiterleitung

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 Anfragen unterstützt, die über UDP-Verbindungen kommen.

So konfigurieren Sie SD-WAN als transparenten DNS-Forwarder:

1. Navigieren Sie zu **Sites > DNS > DNS Transparente Forwarders**. Klicken Sie auf **+**.
2. Geben Sie Werte für die folgenden Parameter ein:
   - **Auftrag**: Die Priorität des Spediteurs.
   - **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.

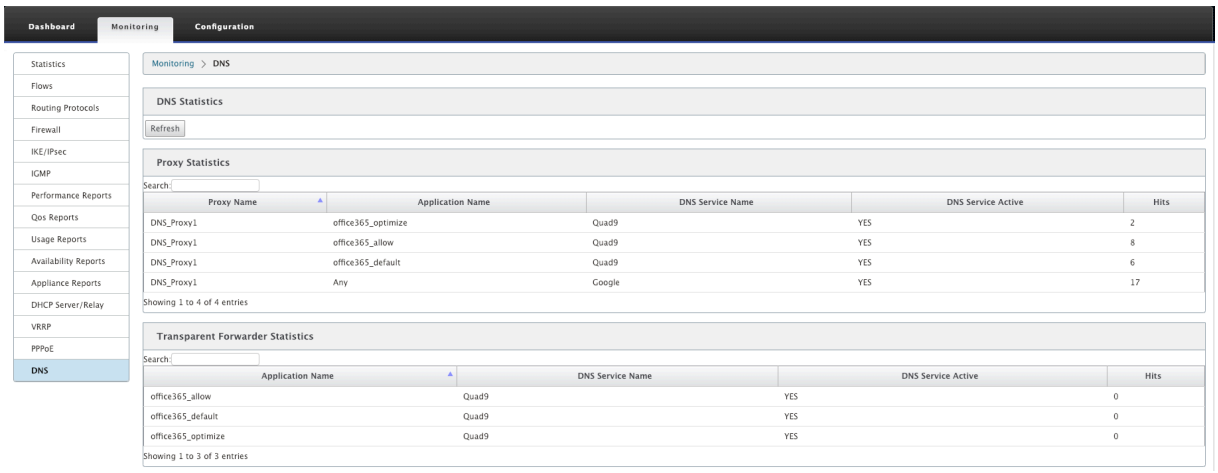
3. Klicken Sie auf **Apply**.

Überwachen

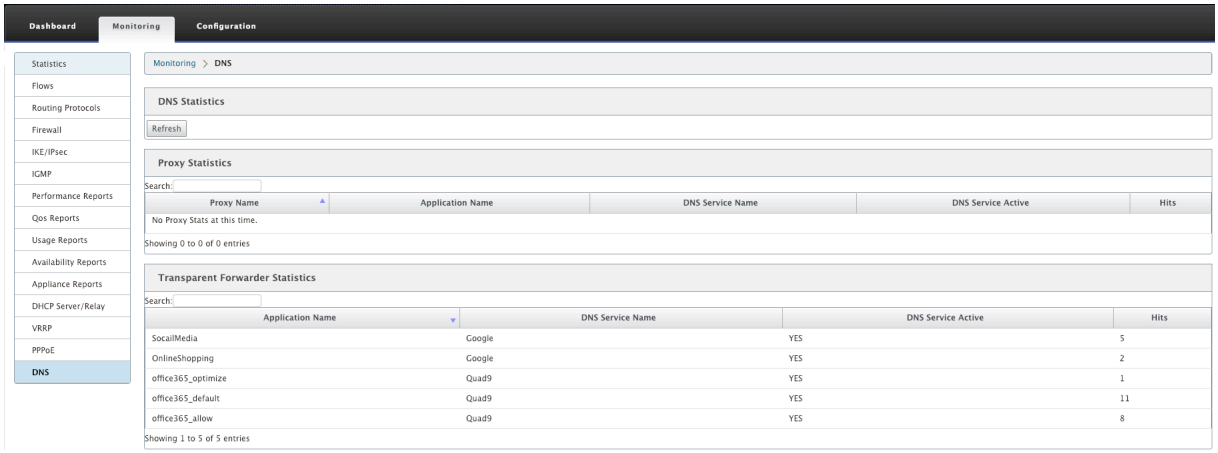
Um Proxy-Statistiken und transparente Forwarder-Statistiken anzuzeigen, navigieren Sie zu **Überwachung > DNS**.

Sie können den Anwendungsnamen, den DNS-Dienstnamen, den DNS-Dienststatus und die Anzahl der Treffer für den DNS-Dienst anzeigen.

Proxystatistik



Transparente Weiterleitungsstatistiken



DHCP-Server und DHCP-Relay

October 28, 2021

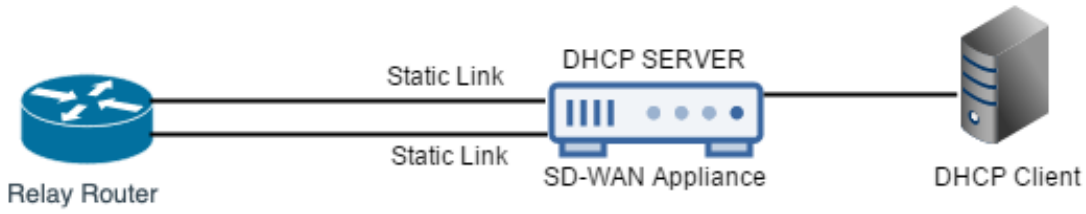
Citrix SD-WAN bietet die Möglichkeit, Standard- oder Premium Edition-Appliances entweder als DHCP-Server oder DHCP-Relay-Agenten zu verwenden. Mit der DHCP-Serverfunktion können Geräte im gleichen Netzwerk wie die LAN/WAN -Schnittstelle der SD-WAN-Appliance ihre IP-Konfiguration von der SD-WAN-Appliance 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 des DHCP-Servers und der DHCP-Relay-Funktionen aufgeführt:

- Reduzieren Sie die Menge an Ausrüstung am Standort des Kunden.
- Ersetzen Sie den Router am Clientstandort (einfache Bereitstellung von Edge-Router-Diensten).
- Vereinfachen Sie das Client-Site-Netzwerk.
- Konfiguration des Routers ohne CLI-Befehle.
- Reduzieren Sie die manuelle Konfiguration auf einfachen Clientsites.

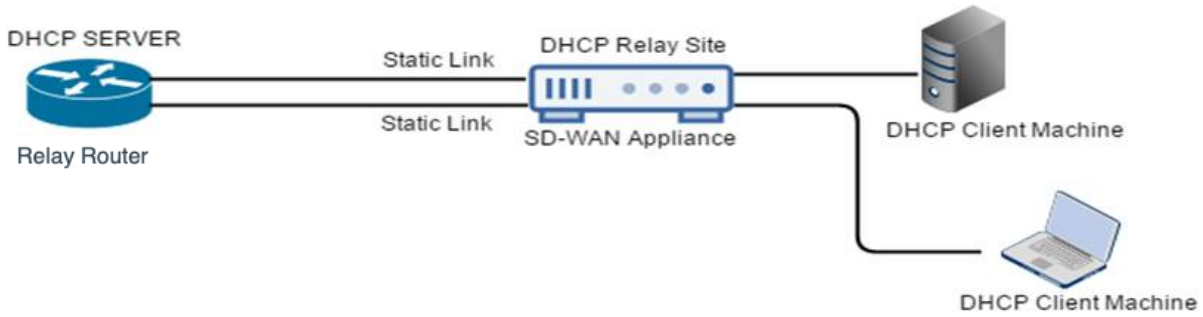
DHCP-Server

Citrix SD-WAN-Appliances können als DHCP-Server konfiguriert werden. Es kann IP-Adressen aus bestimmten Adresspools innerhalb des Netzwerks DHCP-Clients zuweisen und verwalten. Der DHCP-Server kann so konfiguriert werden, dass er weitere Parameter wie die IP-Adresse des Domain Name System (DNS) -Servers und den Standard-Router zuweist. 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 Remote-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

October 28, 2021

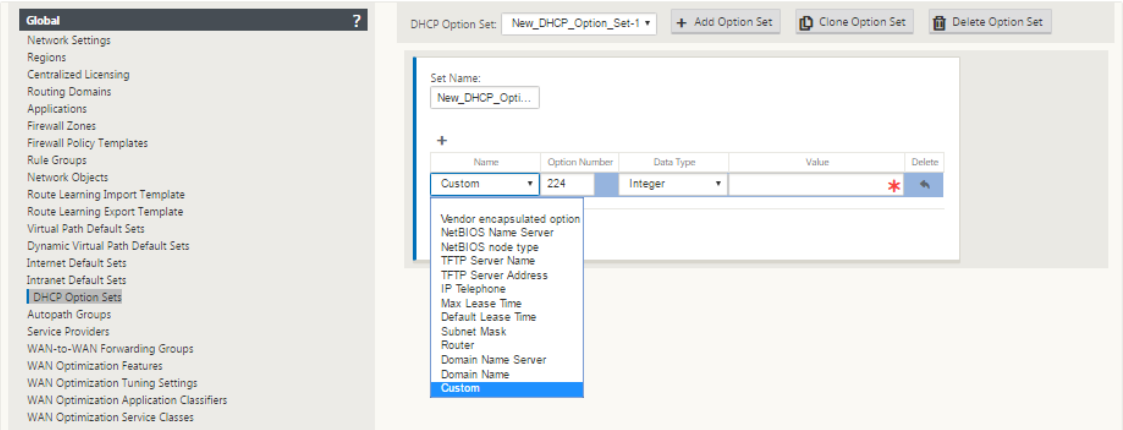
Konfigurieren von DHCP Server und DHCP Relay mithilfe des Konfigurationseditors

Sie können die DHCP-Server- und DHCP-Relay-Einstellungen für die Appliances im Netzwerk mithilfe des Konfigurationseditors 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 **Konfigurationseditor** > **Sites**[> Site-Name] > DHCP > **Serversubnetze**. Klicken Sie auf **+**.
2. Wählen Sie eine konfigurierte Routingdomäne aus, wenn mehrere Domänen vorhanden sind.
3. Wählen Sie die **virtuelle Schnittstelle** aus, die für den Empfang der DHCP-Anfragen verwendet werden soll. Das IP-Subnetz, das vom DHCP-Server zur Verfügung gestellt wird, um Adressen für zu liefern, wird automatisch ausgefüllt.
4. Geben Sie den **Domainnamen**, das **primäre DNS**und das **sekundäre 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 Anfangs- 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.



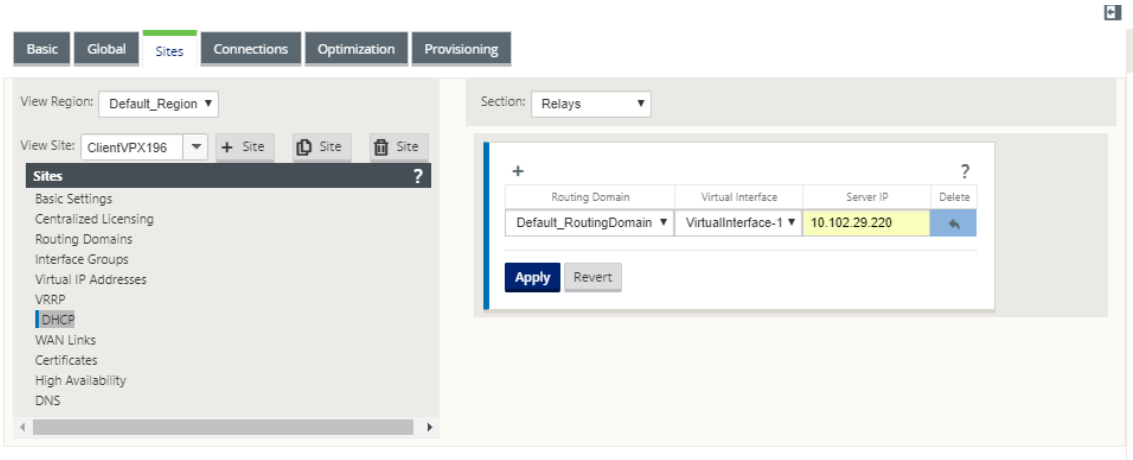
7. Konfigurieren Sie einzelne Hosts, für die eine feste IP-Adresse basierend auf der MAC-Adresse erforderlich ist. Wählen Sie die **feste IP-Adresse**, die **MAC-Adresse**und den **Optionssatz aus**.

So konfigurieren Sie einen Standort mit dem Konfigurationseditor als DHCP-Relay:

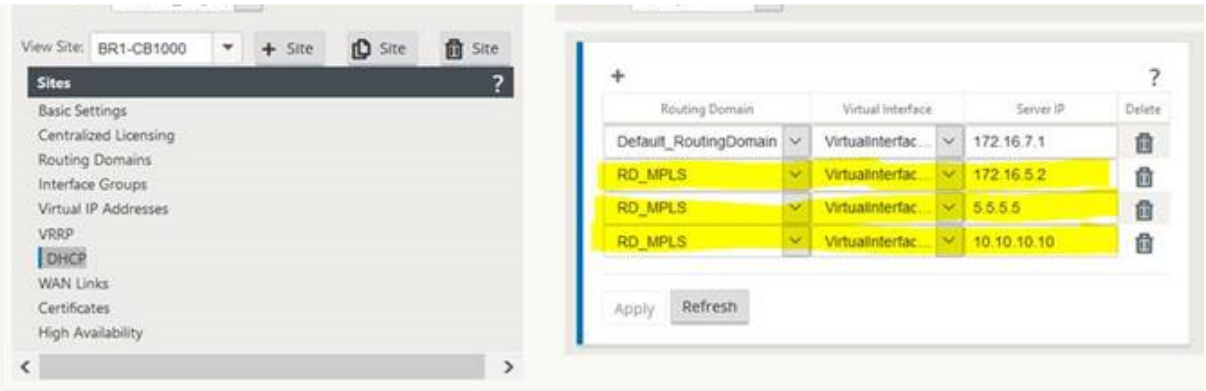
1. Navigieren Sie zu **Konfigurationseditor** > **StandorteSite Name[> Site-Name]** > > **DHCP** > **Relays** . Klicken Sie auf **+**.

   > **Hinweis:**
   >
   > Sie können maximal 16 DHCP-Relays konfigurieren.

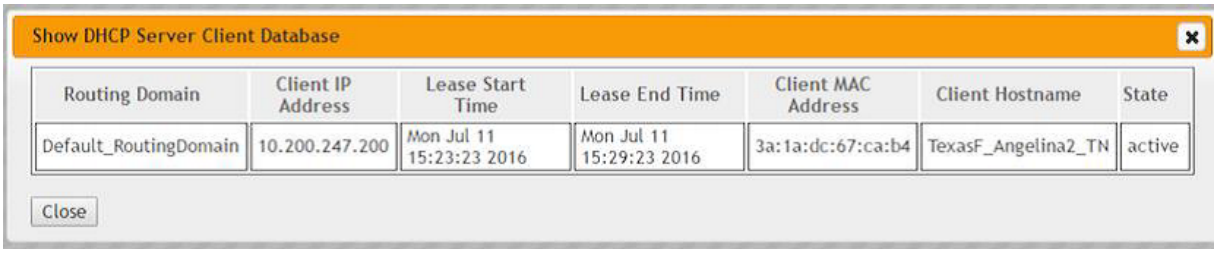
2. Wählen Sie eine konfigurierte Routingdomäne aus, wenn mehrere Domänen vorhanden sind.
3. Wählen Sie ein virtuelles Interface aus, das mit einem Remote-DHCP-Server kommuniziert.
4. Geben Sie die DHCP-Server-IP ein, mit der das Relay die Anforderung und Antwort von den Clients weiterleitet.



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** .



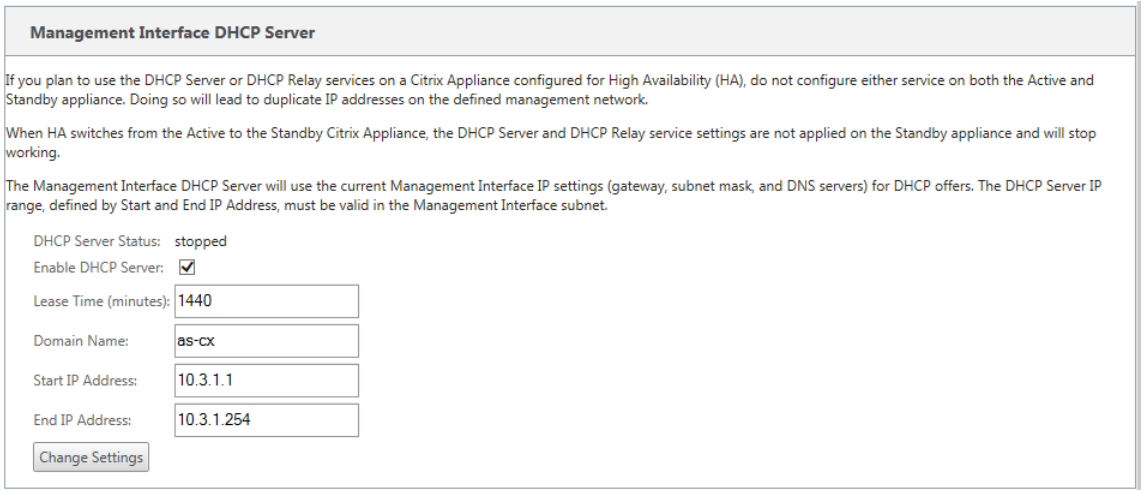
Konfigurieren einer SD-WAN-Appliance als DHCP-Server oder DHCP-Relay mithilfe von Appliance-Einstellungen

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 **Domänennamen** 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.



3. Klicken Sie auf **Einstellungen ändern**, um die Konfiguration des DHCP-Servers abzuschließen.

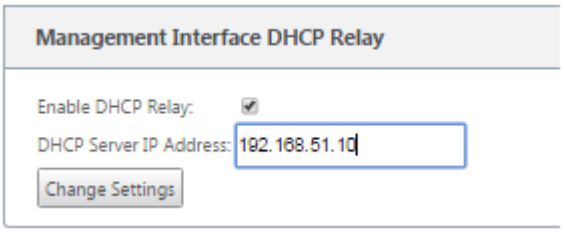
> **Hinweis**
>
> Wenn Sie DHCP-Server auf einer für Hochverfügbarkeit (High Availability) konfigurierten SD-WAN-Appliance verwenden möchten, konfigurieren Sie den Dienst nicht sowohl auf der aktiven als auch auf der Standby-Appliance. Dies führt zu doppelten IP-Adressen im definierten Verwaltungsnetzwerk.

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 **Management Interface DHCP-Relay**.
2. Klicken Sie auf das Kontrollkästchen **DHCP-Relay** aktivieren, um den Dienst zu aktivieren. Geben Sie die **DHCP-Server-IP-Adresse** 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

October 28, 2021

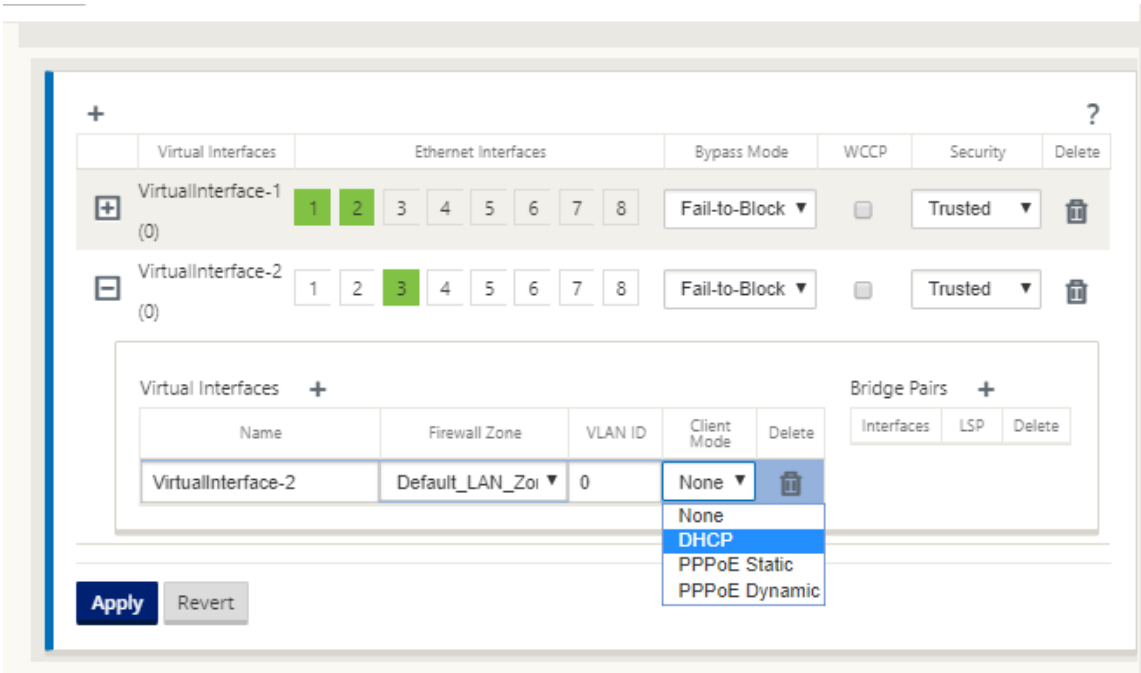
Citrix SD-WAN-Appliances unterstützen das Erlernen von WAN-Link-IP-Adressen durch DHCP-Clients. Diese Funktionalität reduziert den Umfang der manuellen Konfiguration, die für die Bereitstellung von SD-WAN-Appliances erforderlich ist, und senkt die ISP-Kosten, da keine statischen IP-Adressen gekauft werden 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.
> - Der DHCP-Client und der Datenport können nur auf MCN/RCN aktiviert werden, wenn die öffentliche IP-Adresse konfiguriert ist.
> - 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 **Konfigurationseditor**zu **Sites > [Site-Name]** > **Schnittstellengruppen** > **Virtuelle Schnittstellen**.

   > **Hinweis**
   >
   > Die physische Schnittstelle in der Schnittstellengruppe muss ein nicht überbrücktes Paar auf einer einzigen Schnittstelle sein.

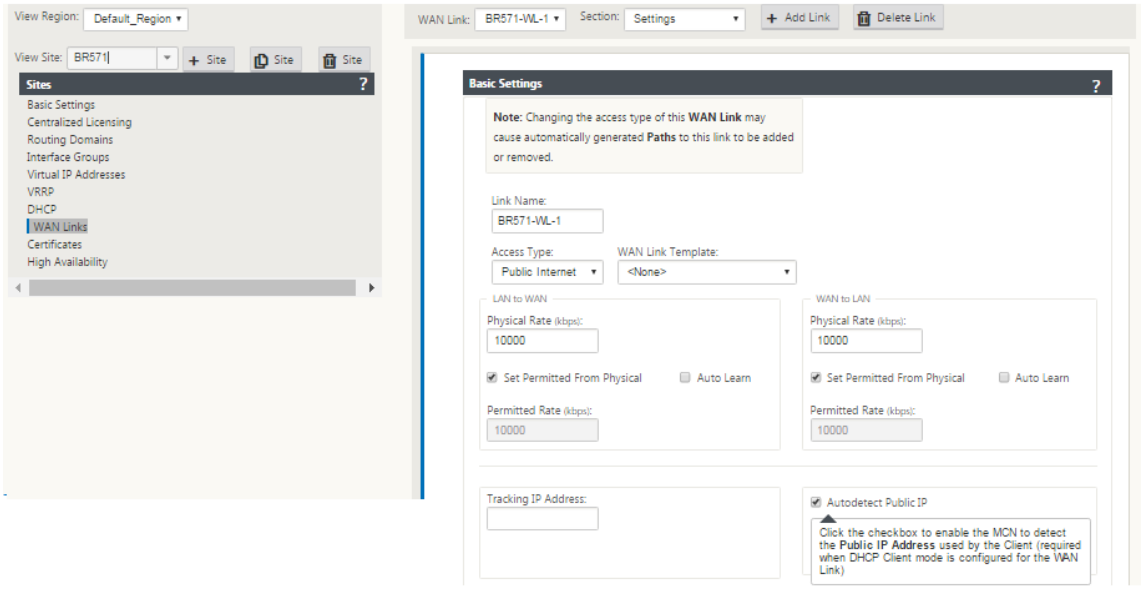


2. Wählen Sie eine der folgenden Optionen als **Client-Modus**aus:

   - Nur DHCP IPv4
   - Nur DHCP IPv6
   - DHCP IPv4 IPv6

Wenn sowohl SLAAC als auch entweder DHCP IPv6 oder DHCP IPv4 IPv6 aktiviert ist, funktioniert DHCPv6 im statusfreien Modus.

1. Navigieren Sie zu **WAN-Links** > **[WAN-Linkname]** > **Einstellungen** > **Grundeinstellungen** .
2. 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.

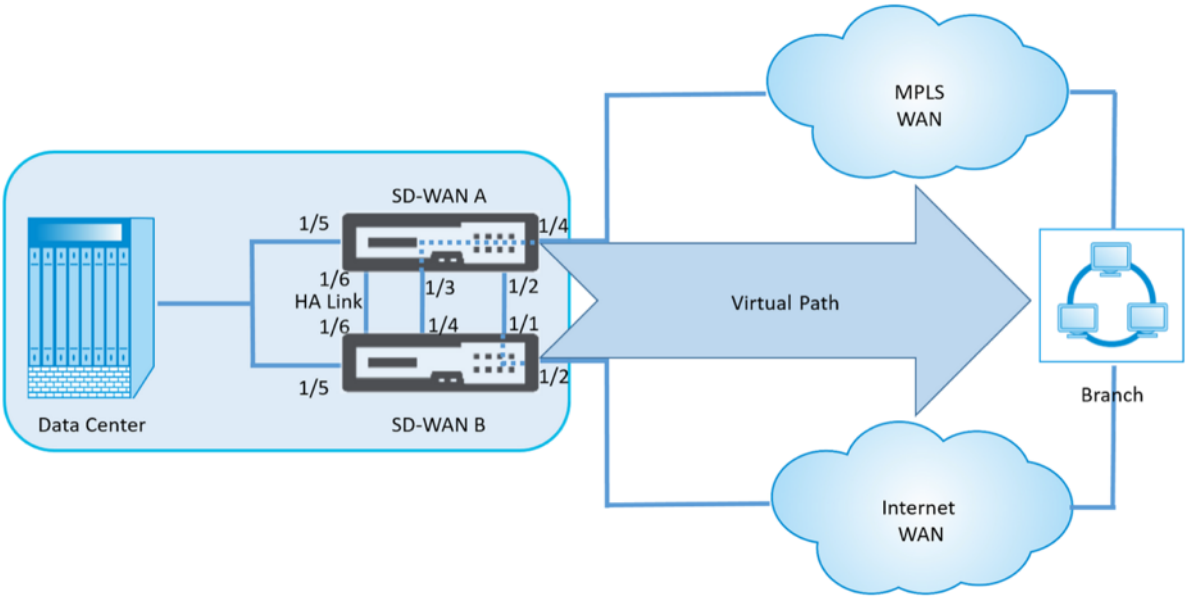


DHCP-Unterstützung für Fail-to-Wire-Port

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:

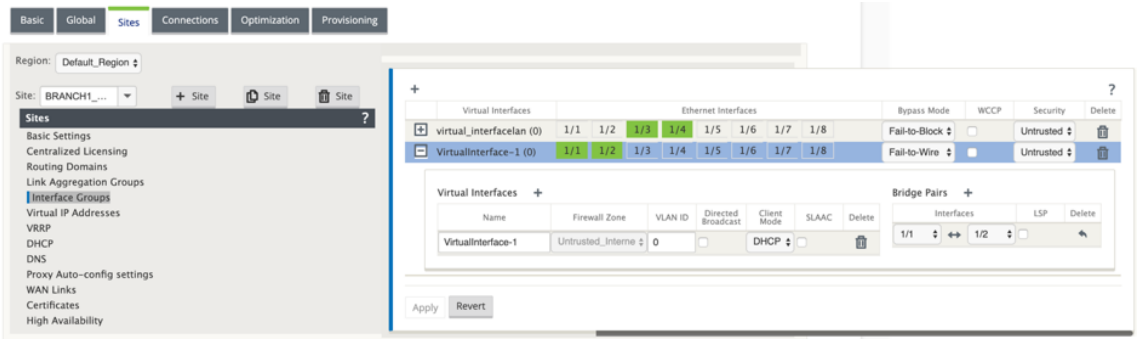
- Ermöglicht die DHCP-Clientkonfiguration für nicht vertrauenswürdige Schnittstellengruppe, die über Fail-to-Wire-Bridge-Paare und serielle HA-Bereitstellungen verfügt
- Ermöglicht die Auswahl von DHCP-Schnittstellen als Teil von **privaten Intranet-WAN-Verbindungen**.

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 **Konfigurationseditor** zu **Sites > [Site-Name] > Schnittstellengruppen > Virtuelle Schnittstellen**.

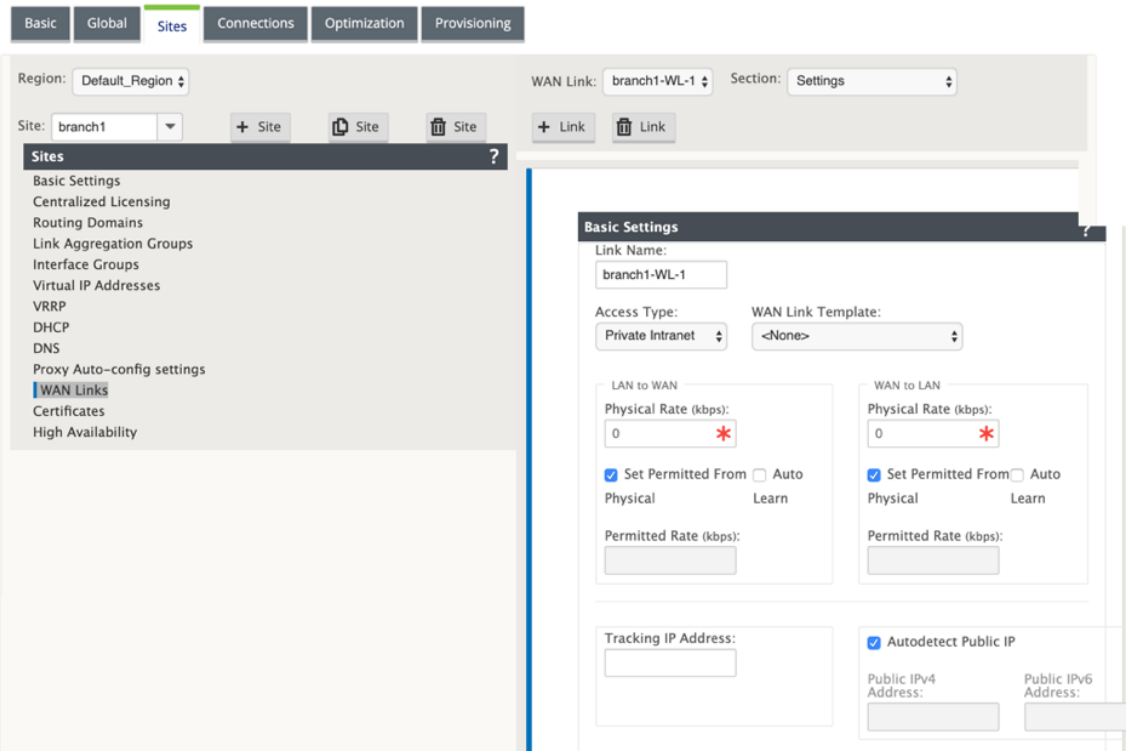


2. Wählen Sie eine der folgenden Optionen als **Client-Modus** aus und fügen Sie dann **Bridge-Paare**hinzu:

   - Nur DHCP IPv4
   - Nur DHCP IPv6
   - DHCP IPv4 IPv6

3. Gehen Sie zu **WAN-Links** klicken Sie auf **+** wählen Sie **WAN-Link-Name** aus der Dropdownliste > 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 Einstellungen für virtuelle IP-Adresse, Subnetzmaske und Gateway zur Laufzeit werden in einer Protokolldatei mit dem Namen *SDWANVW_ip_learned.log protokolliert und 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 IP-Adressen 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 WAN-Verbindungen von 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 **Release Renew**wählen, das eine neue IP-Adresse oder die gleiche IP-Adresse mit einem neuen Leasing 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	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

Dynamische PAC-Dateianpassung

October 28, 2021

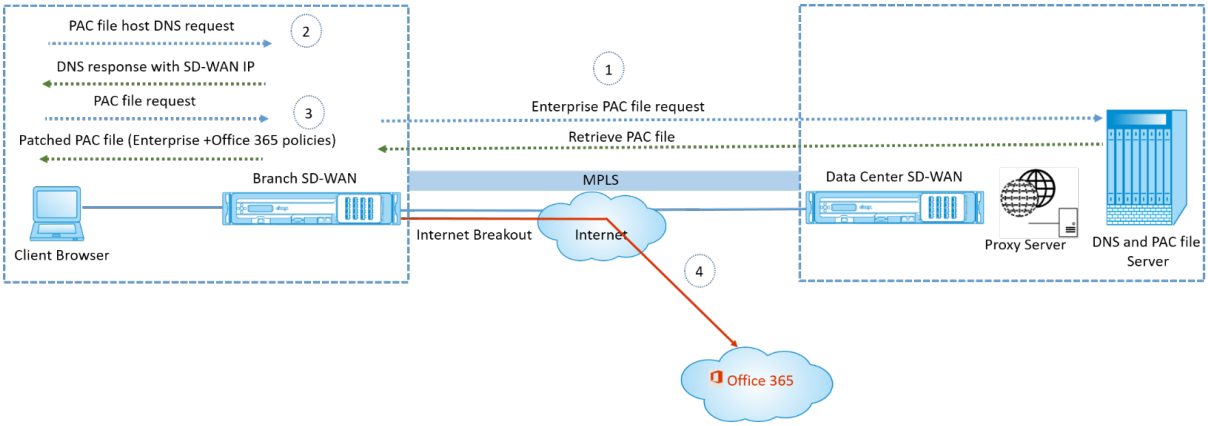
Mit der zunehmenden Akzeptanz geschäftskritischer SaaS-Anwendungen und verteilter Belegschaft in Unternehmen wird es äußerst wichtig, Latenz und Überlastung zu reduzieren. Latenz und Überlastung sind traditionellen Methoden zum Backhauling des Datenverkehrs durch das Rechenzentrum inhärent. Citrix SD-WAN 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 Webproxy gelenkt, was die Klassifizierung und das direkte Internetbreakout erschwert. Die Lösung besteht darin, den SaaS-Anwendungsverkehr vom Proxy auszuschließen, indem die Unternehmens-PAC-Datei (Proxy Auto-Config) angepasst wird.

Citrix SD-WAN 11.0 ermöglicht Proxy-Umgehung und lokale Internetausbrüche für Office 365-Anwendungsdatenverkehr, indem benutzerdefinierte PAC-Dateien dynamisch generiert und bereitgestellt werden. Die PAC-Datei ist eine JavaScript-Funktion, die definiert, ob Webbrowseranfragen direkt an das Ziel oder an einen Webproxyserver gesendet werden.

So funktioniert die Anpassung von PAC-Dateien

Idealerweise werden die PAC-Datei des Unternehmensnetzwerks Host auf dem internen Webserver, diese Proxyeinstellungen über Gruppenrichtlinien verteilt. Der Client-Browser fordert vom Unternehmens-Webserver nach PAC-Dateien. Die Citrix SD-WAN Appliance stellt die benutzerdefinierten PAC-Dateien für Sites bereit, auf denen Office 365-Breakout aktiviert ist.



1. Citrix SD-WAN fordert regelmäßig die neueste Kopie der Enterprise-PAC-Datei vom Unternehmens-Webserver an und ruft sie ab. Die Citrix SD-WAN-Appliance patcht Office 365-URLs an die PAC-Datei des Unternehmens. Es wird erwartet, dass die Unternehmens-PAC-Datei einen Platzhalter (SD-WAN-spezifisches Tag) enthält, in dem die Office 365-URLs nahtlos gepatcht werden.
2. Der Client-Browser stellt eine DNS-Anforderung für den PAC-Dateihost des Unternehmens. Citrix SD-WAN fängt die Anforderung für die Proxy-Konfigurationsdatei FQDN ab und antwortet mit dem Citrix SD-WAN VIP.
3. Der Client-Browser fordert die PAC-Datei an. Die Citrix SD-WAN Appliance stellt die gepatchte PAC-Datei lokal bereit. Die PAC-Datei enthält die Unternehmensproxy-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

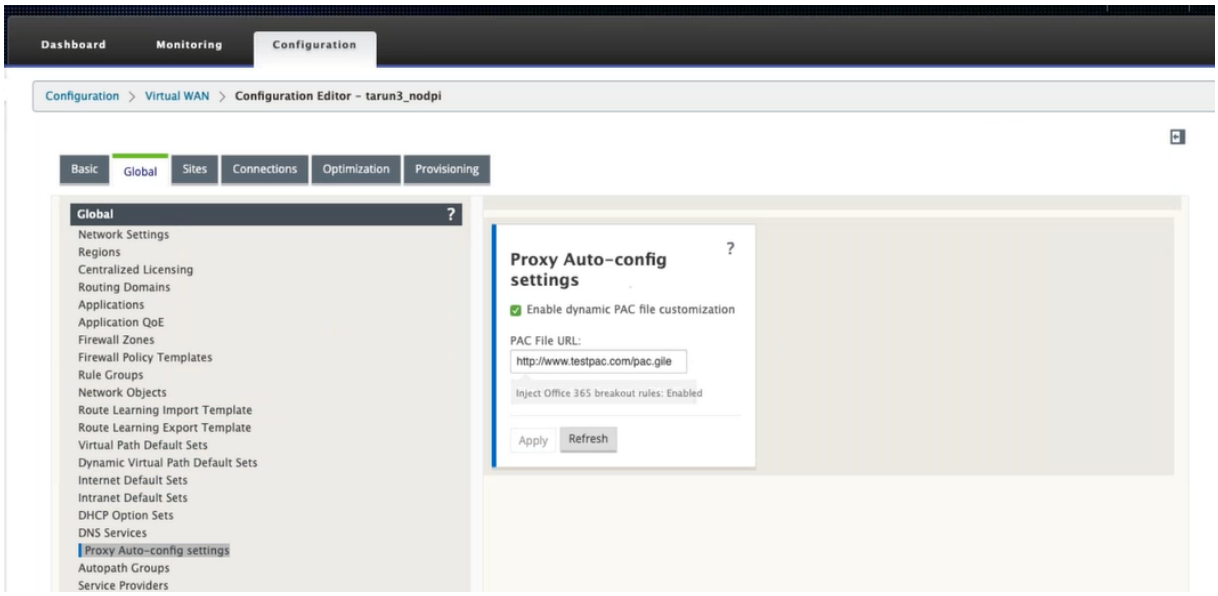
1. Die Unternehmen sollten eine PAC-Datei gehostet haben.
2. Die PAC-Datei sollte einen Platzhalter *SDWAN_TAG* oder ein Vorkommen der *findproxyforurl-Funktion* zum Patchen von Office 365-URLs haben.
3. Die PAC-Datei-URL sollte domänenbasiert und nicht IP-basiert sein.
4. Die PAC-Datei wird nur über die vertrauenswürdigen Identitäts-VIPs bereitgestellt.
5. Die Citrix SD-WAN Appliance sollte die Enterprise-PAC-Dateien über die Verwaltungsschnittstelle herunterladen können.

Konfigurieren der Anpassung von PAC-Dateien

Sie können die PAC-Dateianpassung global oder auf Standortebene aktivieren.

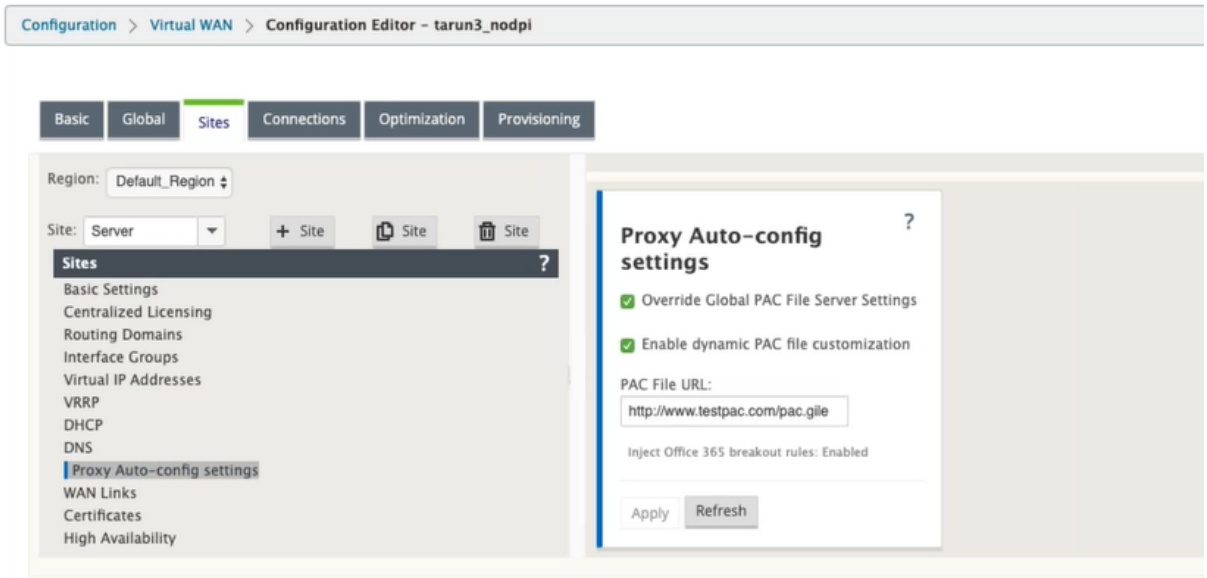
> **Hinweis**
>
> Die Office 365-Breakout-Option muss für die dynamische Anpassung von PAC-Dateien aktiviert sein. Informationen zum Aktivieren des Office 365-Breakout finden Sie unter Office 365-Optimierung.

Um die dynamische PAC-Dateianpassung global für alle Sites zu konfigurieren, navigieren Sie im Konfigurationseditor zu **Global** > **Proxy Auto-config-Einstellungen**.



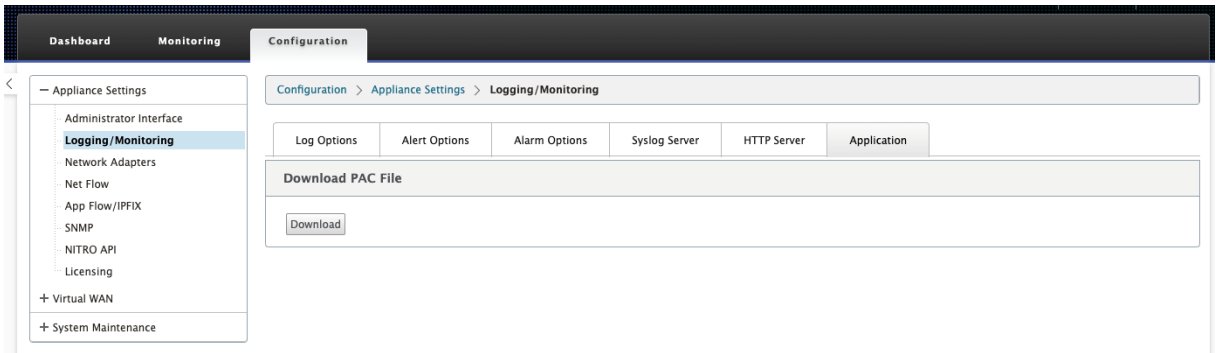
Wählen Sie **Dynamische PAC-Dateianpassung aktivieren**. Geben Sie im Feld **PAC-Datei-URL** die URL des PAC-Dateiservers für Unternehmen ein. Die Office 365-Breakoutregeln werden dynamisch in die Enterprise-PAC-Datei gepatcht.

Um die dynamische PAC-Dateianpassung für eine Site zu konfigurieren, navigieren Sie zu **Sites** > [Site] > **Proxy-Auto-Config-Einstellungen**. Sie können auch globale PAC-Dateiserver-Einstellungen außer Kraft setzen und eine andere PAC-Dateiserver-URL angeben.

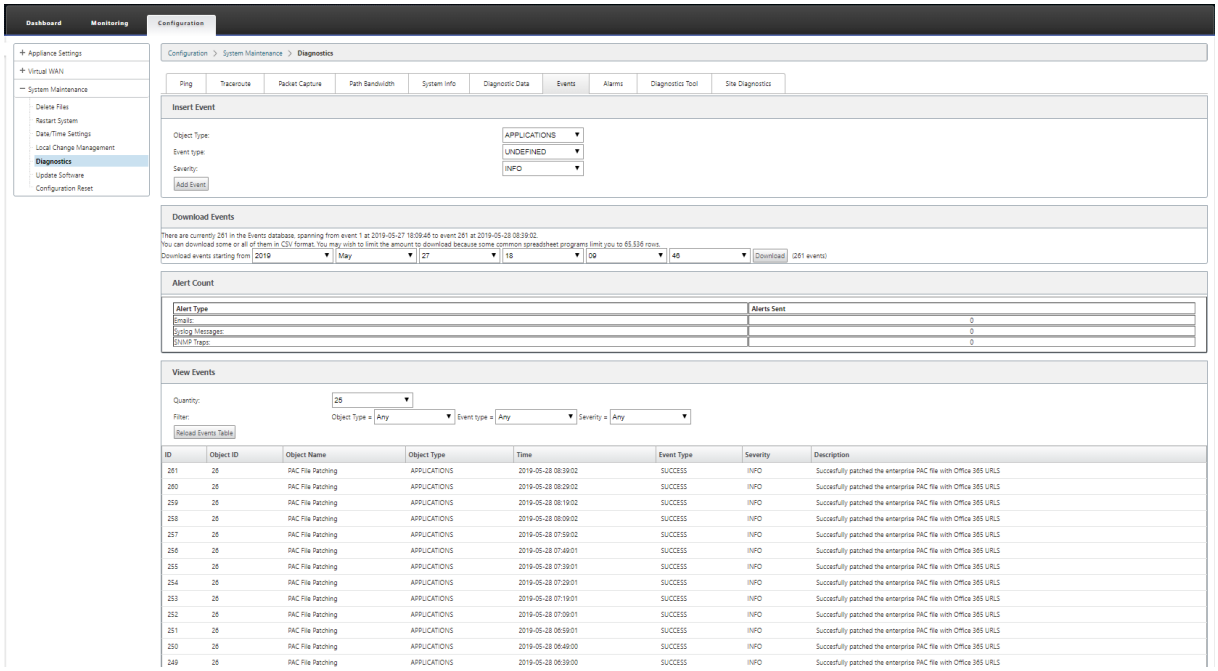


Problembehandlung

Sie können die angepasste PAC-Datei zur Fehlerbehebung von der Citrix SD-WAN Appliance herunterladen. Navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Protokollierung/Überwachung** > **Anwendung und klicken Sie auf Herunterladen**.



Sie können den Patch-Status für PAC-Dateien auch im Abschnitt **Ereignisse** anzeigen, zu **Konfiguration** > **Systemwartung** > **Diagnose**navigieren und auf die Registerkarte **Ereignisse** klicken.



Einschränkungen

- HTTPS PAC-Dateiserver-Anfragen 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

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 den Standort nicht als GRE-Tunnel-Abschlussknoten konfigurieren möchten, können Sie diesen Schritt überspringen und mit dem Abschnitt Konfigurieren der WAN-Links für den MCN-Sitefortfahren.

So konfigurieren Sie einen GRE Tunnel:

Klicken Sie in der Ansicht **Sites** für die neue MCN-Website auf **+** links neben dem Label **GRE Tunnels** . Der **GRE-Tunnels-Tisch** für den neuen Standort wird geöffnet. Weitere Informationen finden Sie in den GRE-Themen.

Konfigurieren von GRE-Tunneln der MCN-Site.

Konfigurieren von GRE-Tunneln für den Zweigstandort.

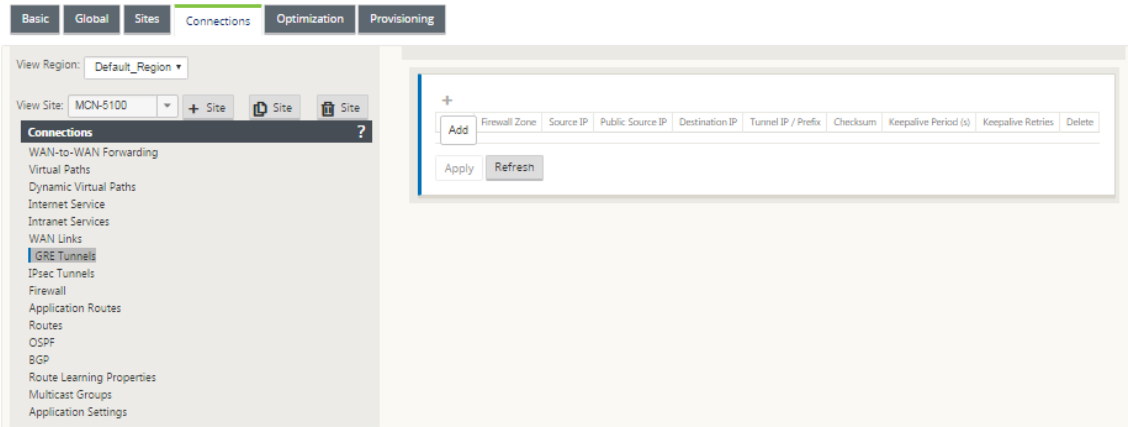
GRE-Tunnel für den MCN-Standort konfigurieren (optional)

October 28, 2021

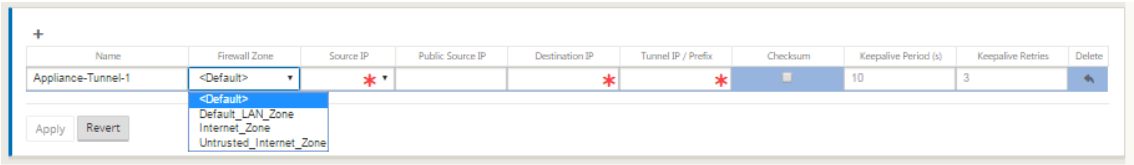
Mit der GRE-Tunnelfunktion können Sie Citrix SD-WAN Appliances so konfigurieren, dass GRE-Tunnel im LAN oder Intranet beendet werden. Wenn Sie diesen Standort nicht als GRE-Tunnel-Abschlussknoten konfigurieren möchten, können Sie diesen Schritt überspringen und mit dem Abschnitt Konfigurieren der WAN-Links für den MCN-Sitefortfahren.

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.



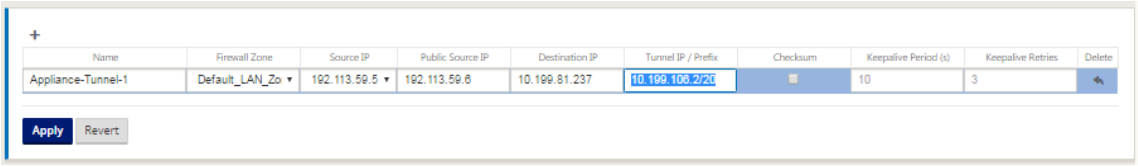
3. Konfigurieren Sie die GRE Tunneleinstellungen.

   Geben Sie Folgendes ein:

   - **Servicetyp** - Wählen Sie den Diensttyp entweder Intranet oder LAN aus der Dropdownliste aus.

- **Bezeichnung**:
  - Wenn der Diensttyp Intranet ist, wählen Sie aus der Liste der konfigurierten Intranetdienste 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.
- **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.



5. 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-Sitezu konfigurieren.

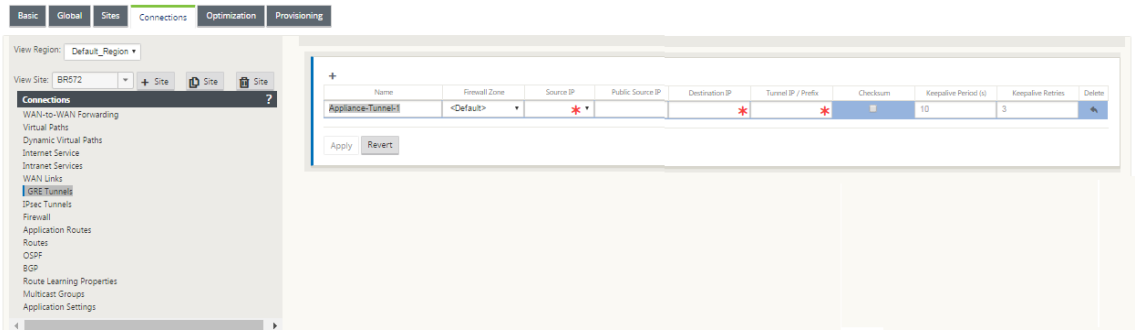
GRE-Tunnel für einen Zweigstandort konfigurieren

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 Zweigstandortfortfahren.

So konfigurieren Sie einen LAN-GRE-Tunnel für den Zweigstandort:

1. Klicken Sie in der Ansicht Verbindungen für den neuen Zweigstandort auf **GRE-Tunnel**. Die **GRE-Tunnels-Ansicht**für den neuen Standort wird 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.

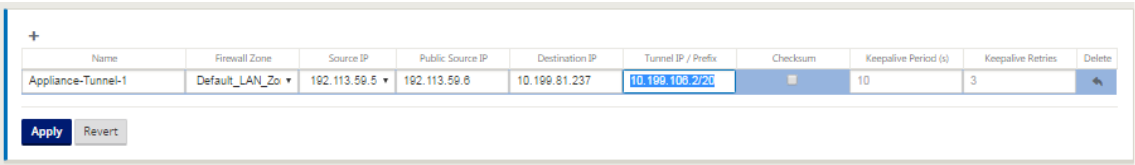


3. Konfigurieren Sie die GRE Tunneleinstellungen. Geben Sie Folgendes ein:
   - **Servicetyp** - Wählen Sie den Diensttyp entweder Intranet oder LAN aus der Dropdownliste aus.
   - **Bezeichnung**:
     - Wenn der Diensttyp Intranet ist, wählen Sie aus der Liste der konfigurierten Intranet-dienste im 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.



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 Zweigstandortzu konfigurieren.

In-Band- und Backup-Management

October 28, 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.

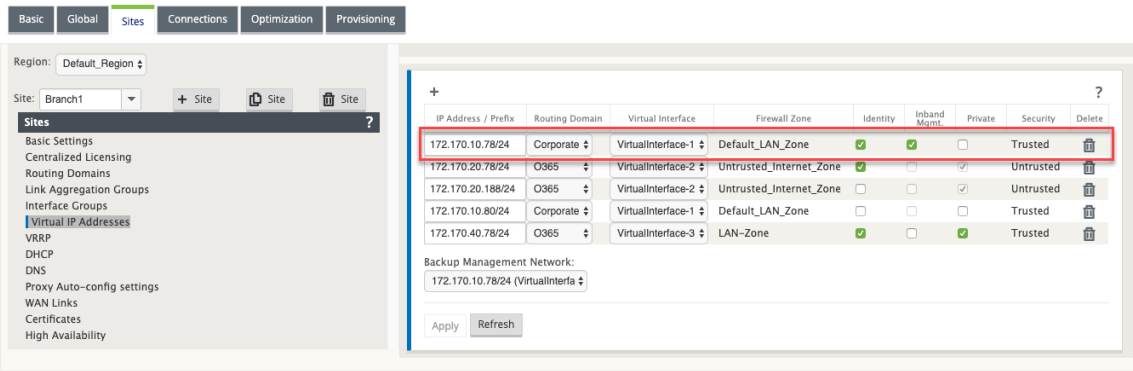
Durch die In-Band-Verwaltung können virtuelle IP-Adressen mit Verwaltungsdiensten wie Web-UI und SSH verbunden werden. Sie können die In-Band-Verwaltung auf mehreren vertrauenswürdigen Schnittstellen aktivieren, die für die Verwendung für IP-Dienste aktiviert sind. Sie können auf die Web-UI und SSH über die Management-IP und virtuelle In-Band-IPs zugreifen.

> **Hinweis**
>
> - Citrix SD-WAN Center unterstützt keine Konnektivität mit der High Availability Appliance durch In-Band-Management.
> - Sie können den **Diensttyp** nur mit dem MCN-Konfigurationseditor als **Any** konfigurieren. Der Citrix SD-WAN Orchestrator-Dienst lässt die Konfiguration des **Diensttyps** als **Any** für Ziel-NAT-Richtlinien nicht zu.
> - Vermeiden Sie es, den Dienst zu deaktivieren, wenn die einzige Verwaltungskonnektivität In-Band-HA ist.
> Sie können sich aus der Appliance ausschließen, wenn Sie den Dienst deaktivieren.

So aktivieren Sie die In-Band-Verwaltung auf einer virtuellen IP:

1. Navigieren Sie im Konfigurationseditor zu **Sites** > **Virtuelle IP-Adressen**.
2. Wählen Sie **Inband Mgmt** für die virtuellen IPs aus, für die Sie das In-Band-Management 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 virtueller IP-Adressen finden Sie unter How to configure virtual ip.

Ab Citrix SD-WAN 11.3.1 unterstützt die In-Band-Verwaltung High-Availability Appliance-Paare. Die Kommunikation zwischen den primären und sekundären Appliances erfolgt über die virtuellen Schnittstellen mit NAT.

Die folgenden Ports ermöglichen die Kommunikation mit Verwaltungsdiensten auf den HA-Appliances:

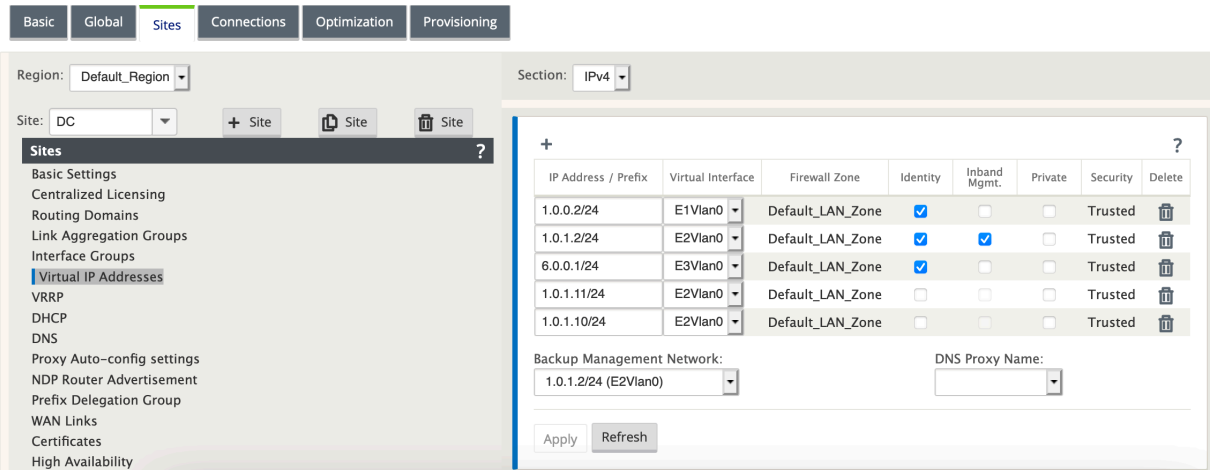
- HTTPS
  - 443 - Verbindet sich mit der HA aktiv
  - 444 - Leitet auf die HA-Primär um
  - 445 - Weiterleitungen zur HA-Sekundär
- SSH
  - 22 - Verbindet sich mit der HA aktiv
  - 23 - Leitet auf HA-Primär um
  - 24 - Leitet auf HA-Sekundär um
- SNMP
  - 161 - Verbindet sich mit der HA aktiv
  - 162 - Leitet auf HA-Primär um
  - 163 - Weiterleitungen zur HA-Sekundär

Verwenden Sie Ziel-NAT-Richtlinien, um IP-Adressen zu erstellen, die eine Konnektivität mit In-Band-HA ermöglichen, ohne einen Port eingeben zu müssen.

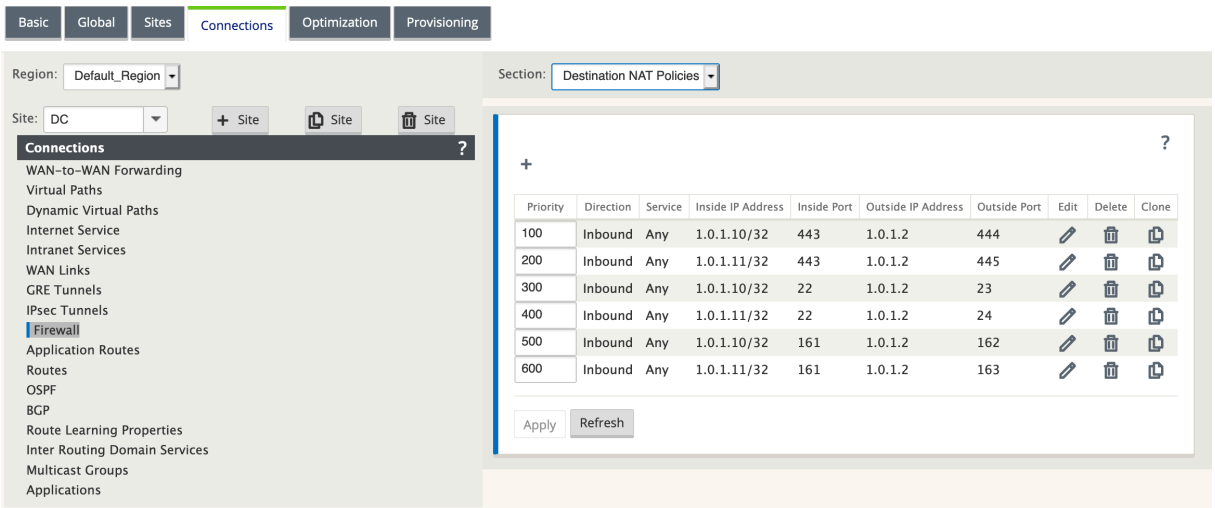
Beispielsweise werden die folgenden Inband-IP-Adressen für den Zugriff auf die Appliances verwendet:

- Aktive Appliance - 1.0.1.2
- Primäre Appliance - 1.0.1.10
- Sekundäre Appliance - 1.0.1.11

Erstellen Sie zwei neue virtuelle IP-Adressen, die sich im selben Netzwerk wie die der virtuellen IP-Adresse der In-Band-Verwaltung befinden. In diesem Beispiel sind 1.0.1.2/24 die virtuellen IP-Adressen im In-Band-Management und 1.0.1.2/24 wird als Backup-Netzwerk ausgewählt. 1.0.1.10 und 1.0.1.11 sind die neuen virtuellen IP-Adressen, die erstellt werden. 1.0.1.10 wird für den Zugriff auf die primäre Appliance verwendet und 1.0.1.11 wird für den Zugriff auf die sekundäre Appliance verwendet.



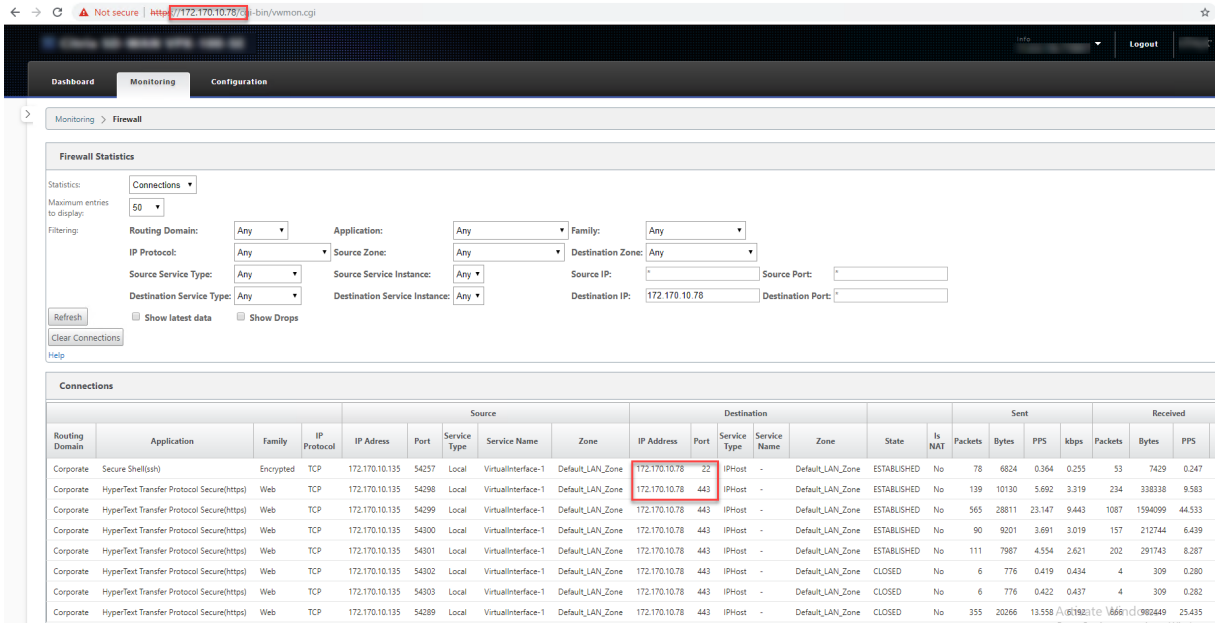
Erstellen Sie NAT-Ziel-Richtlinien. Die sechs DNAT-Richtlinien leiten die Basisports für Dienste auf den entsprechenden In-Band-HA-Port um. Nach der Anwendung der Konfiguration können Sie direkt mit den internen IP-Adressen auf die primären und sekundären Appliances zugreifen.



Überwachung der In-Band-Verwaltung

Im vorangegangenen Beispiel haben wir die In-Band-Verwaltung auf 172.170.10.78 virtueller IP aktiviert. Sie können diese IP verwenden, um auf die Webbenutzeroberfläche und SSH zuzugreifen.

Navigieren Sie in der Web-Benutzeroberfläche zu **Monitoring** > **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 zusammen mit der In-Band-Verwaltungsfunktion ermöglicht die Provisioning und Konfigurationsverwaltung über bestimmte Datenports. Die Zero-Touch-Bereitstellung wird jetzt auf den ausgewiesenen Datenports unterstützt und es ist nicht erforderlich, einen separaten Verwaltungsport für die Zero-Touch-Bereitstellung 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 SD-WAN Center finden Sie unter Zero Touch-Bereitstellung. Informationen zur Zero-Touch-Bereitstellung über SD-WAN Orchestrator finden Sie unter Zero Touch Deployment.

Hinweis: Für die Day-0-Bereitstellung von SD-WAN-Appliances über die Daten-Ports muss 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

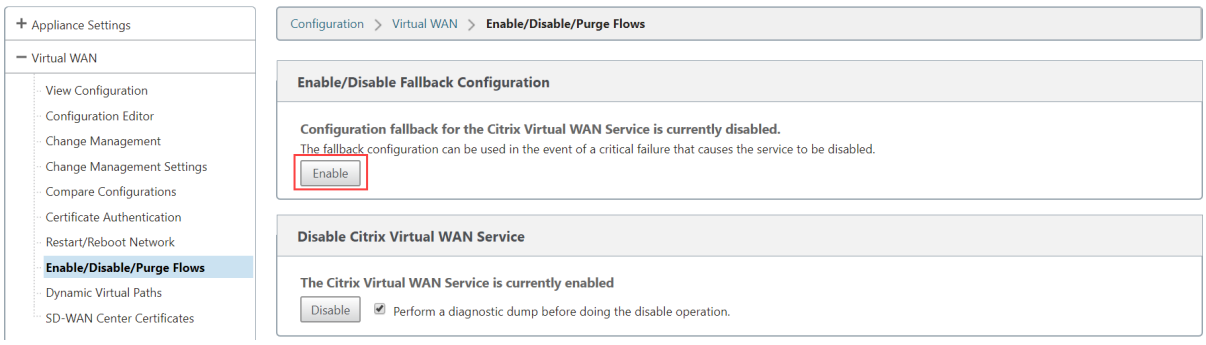
eine Appliance-Lizenz oder eine Kulanzlizenz abläuft, wird die Standardkonfiguration aktiviert, um sicherzustellen, dass die Appliance weiterhin mit dem Zero-Touch-Bereitstellungsdienst verbunden bleibt und Lizenzen erhält, die über eine Zero-Touch-Bereitstellung verwaltet werden.

Default-/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** > **Appliance-Einstellungen** > **Standard-/Fallback-Konfiguration** navigieren > auf **Aktivieren**klicken.



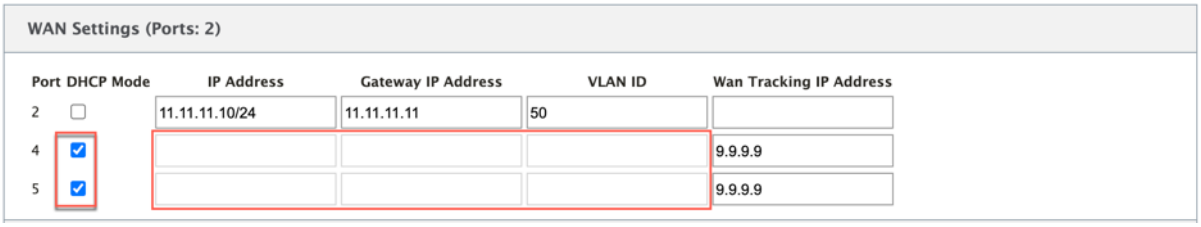
Die folgende Tabelle enthält die Details der vordefinierten WAN- und LAN-Ports für die Fallbackkonfiguration auf verschiedenen Plattformen:

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)

Ab Citrix SD-WAN 11.3.1 sind die WAN-Port-Einstellungen konfigurierbar. WAN-Ports können mit dem DHCP-Client als unabhängige WAN-Verbindungen konfiguriert werden und überwachen den Quad9 DNS-Dienst, um die WAN-Konnektivität zu bestimmen. Sie können WAN-IPs/Statische IPs für die WAN-Ports ohne DHCP konfigurieren, um das In-Band-Management für die anfängliche Provisioning zu verwenden.

> **Hinweis:**
>
> Sie können die Ethernet-Ports nur mit den statischen IPs konfigurieren. Die statischen IPs sind nicht mit LTE-1- und LTE-E1-Ports konfigurierbar. Obwohl Sie den LTE-1 und LTE-E1-Port als WAN hinzufügen können, bleiben die Konfigurationsfelder nicht editierbar.

Wenn Sie einen WAN-Port hinzufügen, wird er im Abschnitt **WAN-Einstellungen (Port: 2)** hinzugefügt, wobei das standardmäßig aktivierte Kontrollkästchen **DHCP-Modus** aktiviert ist. Wenn das Kontrollkästchen **DHCP-Modus** aktiviert ist, sind die Textfelder **IP-Adresse, Gateway-IP-Adresse** und **VLAN-ID** ausgegraut. Deaktivieren Sie das Kontrollkästchen **DHCP-Modus**, wenn Sie die statische IP konfigurieren möchten.



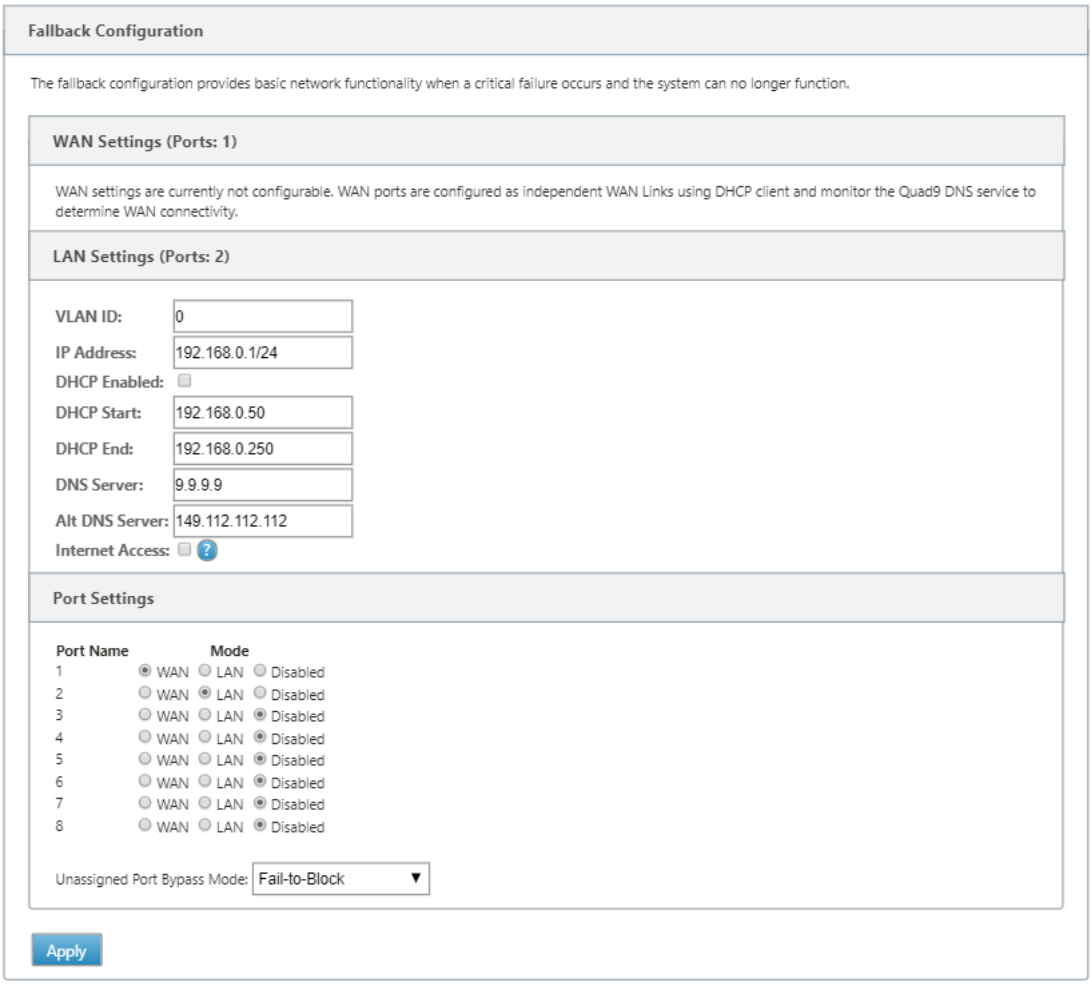
Standardmäßig wird das Feld **WAN-Tracking-IP-Adresse** automatisch mit 9.9.9.9 gefüllt. Sie können die Adresse nach Bedarf ändern.

> **Hinweis**
>
> Wenn Sie das Kontrollkästchen **Dynamic DNS Servers** aktivieren, müssen Sie mindestens einen WAN-Port mit ausgewähltem **DHCP-Modus** hinzufügen/konfigurieren.

So passen Sie die Fallbackkonfiguration gemäß Ihrem LAN-Netzwerk an:

1. Navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Default/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.



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

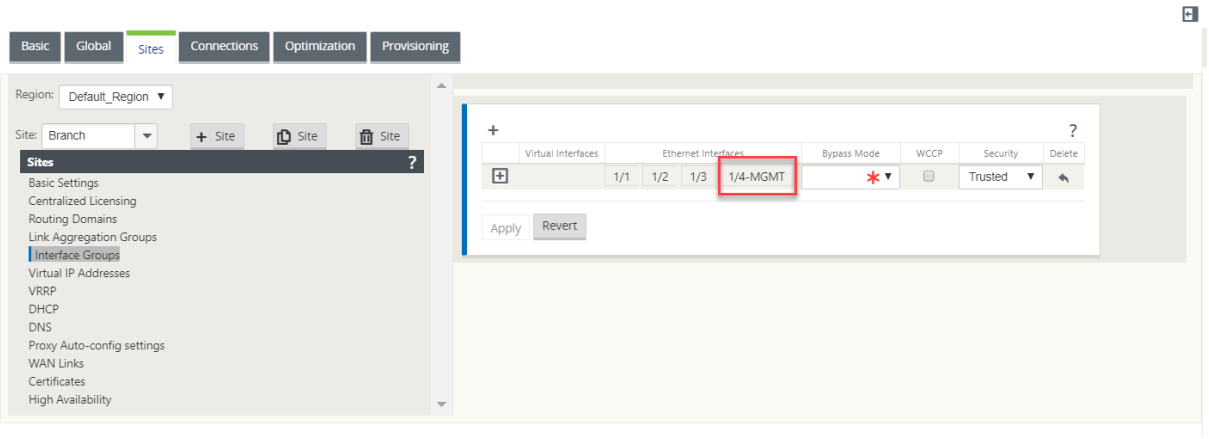
der Management-Port auf den Low-End-Appliances, die bereits eine geringe Portdichte aufweisen, ungenutzt. Mit Citrix SD-WAN können Sie den Verwaltungsport so konfigurieren, dass er entweder als Datenport oder als Verwaltungsport verwendet wird.

> **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.

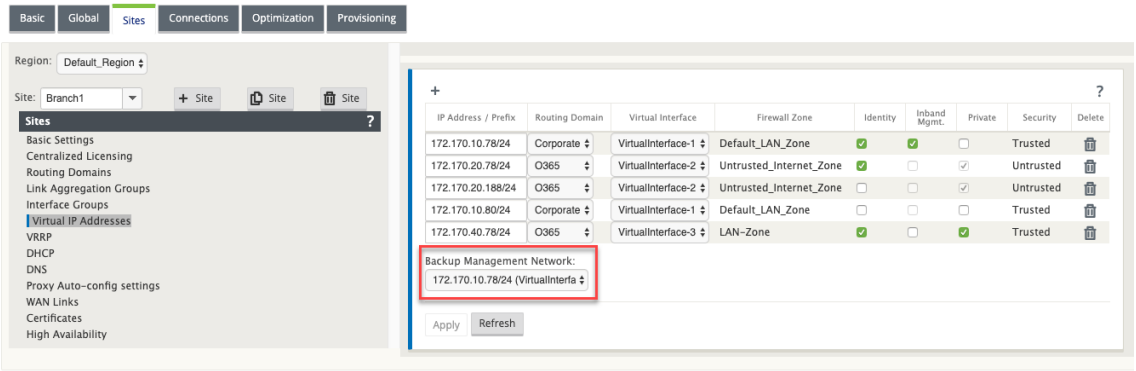
Backup-Management-Netzwerk

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 Backupverwaltungsnetzwerk ausgewählt.

So wählen Sie eine virtuelle IP als Backupverwaltungsnetzwerk aus:

1. Navigieren Sie im Konfigurationseditor zu **Sites** > **Virtuelle IP-Adressen**.
2. Wählen Sie eine virtuelle IP-Adresse als Backupverwaltungsnetzwerk 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 Backupverwaltungsnetzwerk für eine virtuelle IP aktiviert sind.

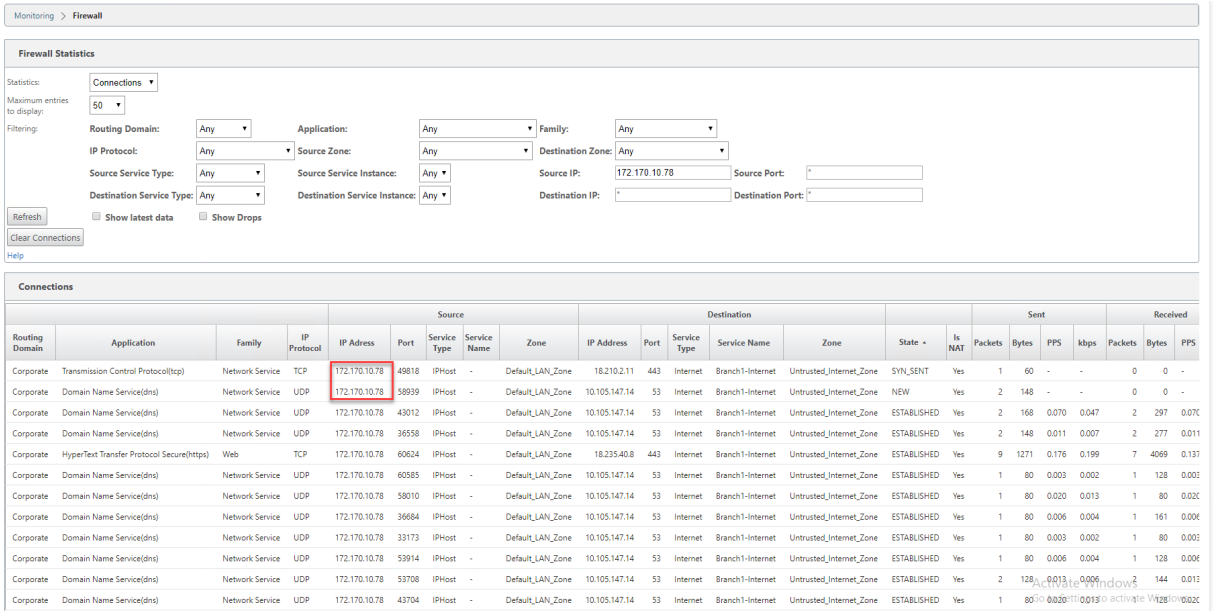
4. Klicken Sie auf **Apply**.

Ausführliche Vorgehensweise zum Konfigurieren einer virtuellen IP-Adresse finden Sie unter So konfigurieren Sie virtuelle IP-Adresse

Überwachung der Backupverwaltung

Im vorangegangenen Beispiel haben wir 172.170.10.78 virtuelle IP als Backupverwaltungsnetzwerk ausgewählt. Wenn die Management-IP-Adresse nicht mit einem Standard-Gateway konfiguriert ist, können Sie diese IP verwenden, um auf die Webbenutzeroberfläche und SSH zuzugreifen.

Navigieren Sie in der Web-Benutzeroberfläche zu **Monitoring** > **Firewall**. Sie können diese virtuelle IP-Adresse als Quell-IP-Adresse für SSH- und Web-UI-Zugriff sehen.



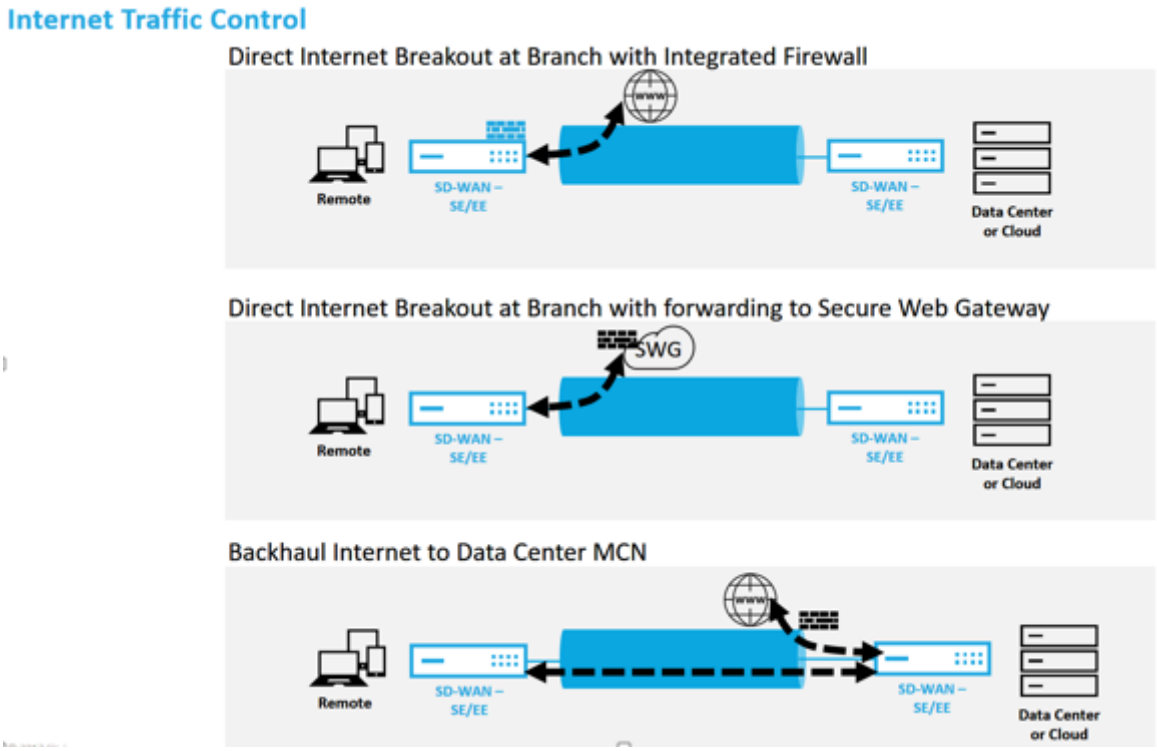
Internetzugriff

October 28, 2021

Der Internetdienst wird für den Datenverkehr zwischen einer Endbenutzer-Website und Websites im öffentlichen Internet verwendet. Der Internetdienstverkehr ist nicht von SD-WAN gekapselt und verfügt nicht über die gleichen Fähigkeiten wie der 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 die WAN-Verbindungsbandbreite aktiv verwalten kann, indem der Internetverkehr im Verhältnis zum Datenverkehr, der über den virtuellen Pfad und den Intranet-Verkehr gemäß der vom Administrator festgelegten Konfiguration geliefert wird, begrenzt wird. Zusätzlich zu den Funktionen zur Provisioning der Bandbreite bietet SD-WAN die zusätzliche Möglichkeit, den über den Internetdienst bereitgestellten Datenverkehr mit mehreren Internet-WAN-Verbindungen auszugleichen oder optional die Internet-WAN-Verbindungen in einer primären oder sekundären Konfiguration zu nutzen.

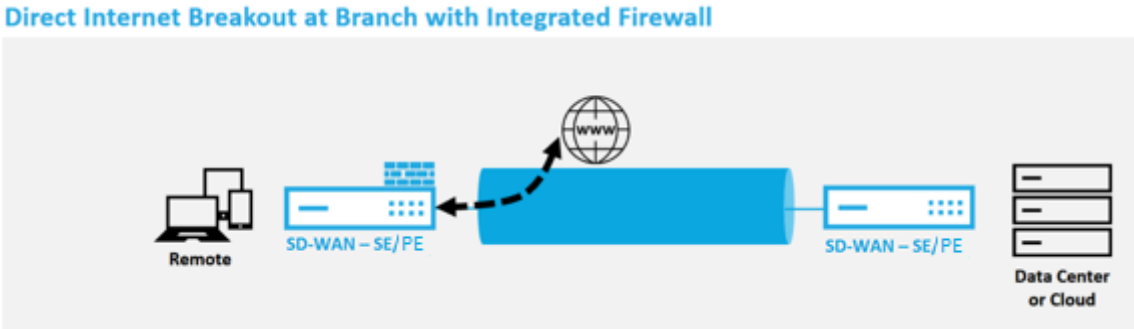
Die Steuerung des Internetverkehrs über den Internetdienst auf SD-WAN-Appliances kann in den folgenden Bereitstellungsmodi konfiguriert werden:

- Direktes Internetbreakout in Branch mit integrierter Firewall
- Direktes Internetbreakout bei Zweigweiterleitung an Secure Web Gateway
- Backhaul Internet zum Rechenzentrum MCN



Direktes Internetbreakout in Branch mit integrierter Firewall

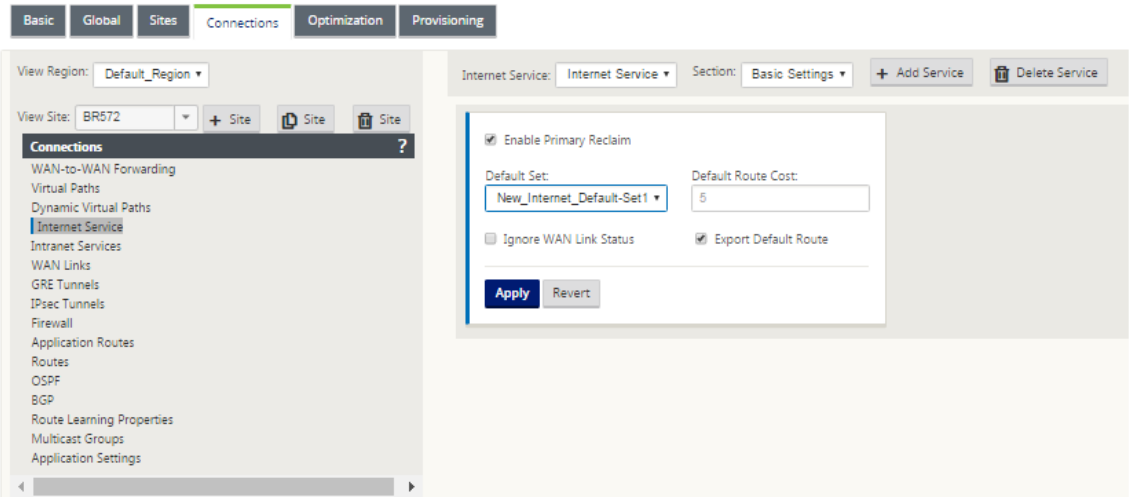
October 28, 2021



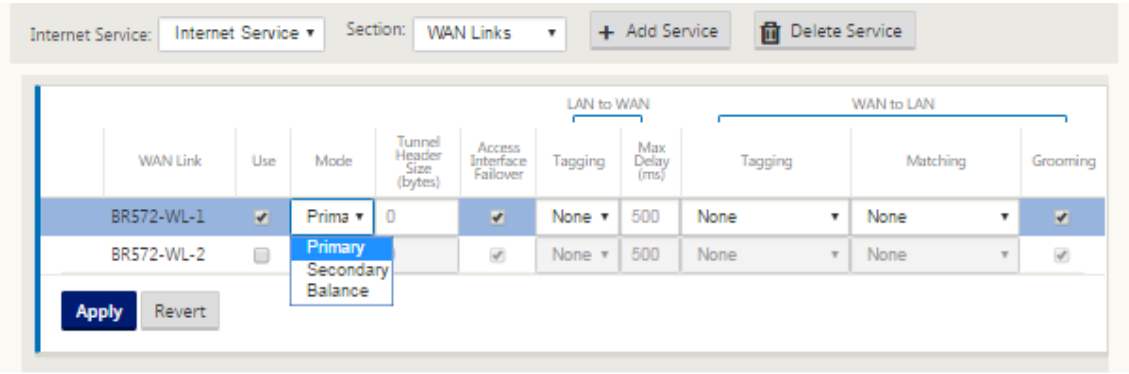
Führen Sie die folgenden Schritte aus, um den Internetdienst für jeden Standort (Client-Knoten oder MCN) zu aktivieren:

1. Navigieren Sie im **Konfigurationseditor** 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 Möglichkeiten, wie sich der Internetdienst bei Nichtverfügbarkeit von WAN-Verbindungen verhalten soll. Ein Internet-

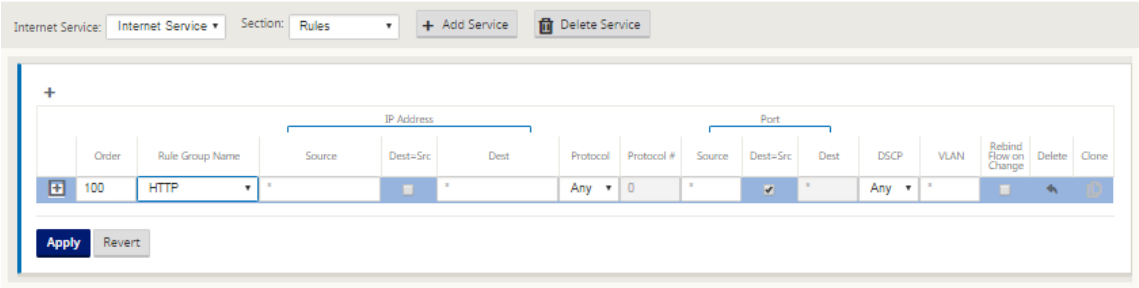
Standardset kann in der globalen Kachel mit einer Reihe von Regeln definiert werden, die auf jeden Knoten in der Konfiguration angewendet werden können, für den Internetdienst aktiviert ist, und bietet eine zentrale Steuerung für die Internetdienstverwaltung, ohne jeden Knoten separat konfigurieren zu müssen.



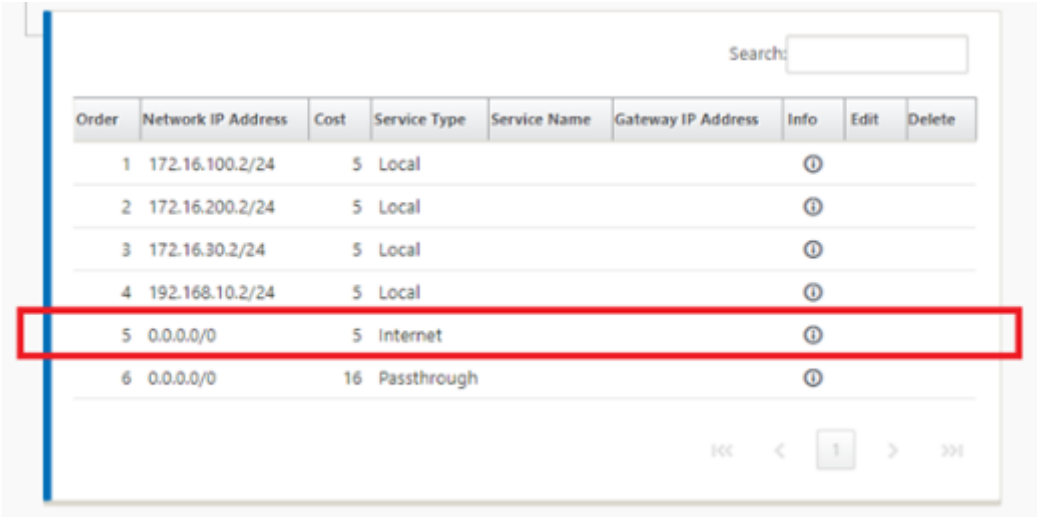
3. Im Knoten Internetdienst-WAN-Links werden die in der Site-Kachel eingebauten WAN-Links zur Verfügung gestellt, um auszuwählen, welche WAN-Verbindung Sie für den Internetverkehr verwenden möchten. Zusätzlich zu anderen Optionen sind die verfügbaren Modi Primär, Sekundär und Ausgewogen, sodass der Administrator die verfügbaren WAN-Verbindungen gleichzeitig oder in einer aktiven/passiven Rolle verwenden kann.



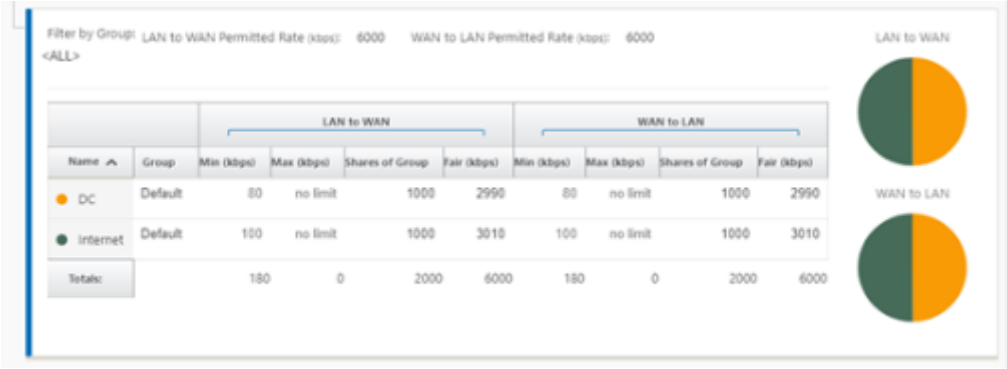
4. Es sind standortknotenspezifische Regeln verfügbar, die die Anpassung jeder Site ermöglichen, alle allgemeinen Einstellungen, die im globalen Standardsatz konfiguriert sind, eindeutig außer Kraft zu setzen. Zu den Modi gehört die gewünschte Bereitstellung über eine bestimmte WAN-Verbindung oder als Override-Dienst, der das Durchleiten oder Verwerfen des gefilterten Datenverkehrs ermöglicht.



Wenn ein Internetdienst für einen Knoten erstellt wird, wird die Routentabelle für diesen bestimmten Knoten automatisch mit einer 0.0.0.0/0-Route für den Diensttyp gleich Internet und einer Routenkosten von 5 aktualisiert, andernfalls würde die Standardroute mit Kosten 16 mit Passthrough als Diensttyp festgelegt werden, und der Internetverkehr würde zur Route an das Unterlagennetzwerk übergeben werden.



Wenn der Internetdienst für einen Standortknoten aktiviert ist, wird die Provisioning-Kachel zur Verfügung gestellt, um die bidirektionale Verteilung der Bandbreite für eine WAN-Verbindung zwischen den verschiedenen Diensten zu ermöglichen, die die WAN-Verbindung verwenden. Im Abschnitt Dienste können Benutzer die Bandbreitenzuweisung weiter optimieren. Darüber hinaus kann Fair Share aktiviert werden, sodass alle Dienste ihre reservierte Mindestbandbreite erhalten können, 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 vorhandenen 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 geliefert 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 es 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.

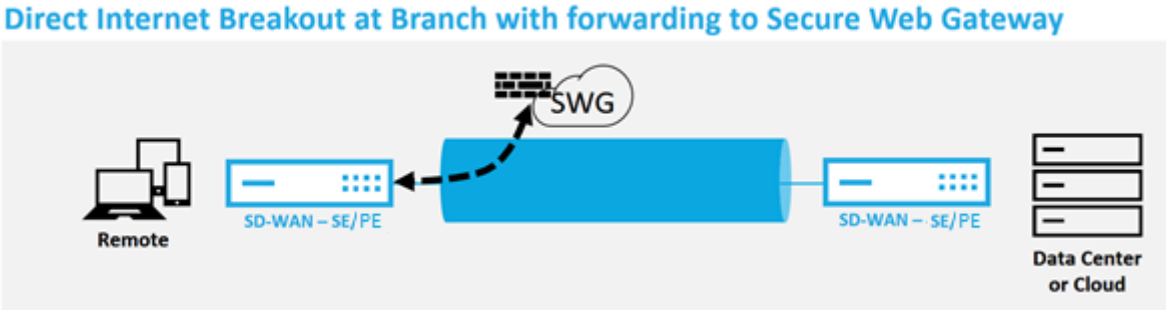
Direkter Internetzugang mit Secure Web Gateway

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.



Citrix SD-WAN unterstützt die folgenden Secure Web Gateway-Lösungen von Drittanbietern:

- Z-Scaler
- Forcepoint
- Palo Alto
- Citrix Secure Internet Access

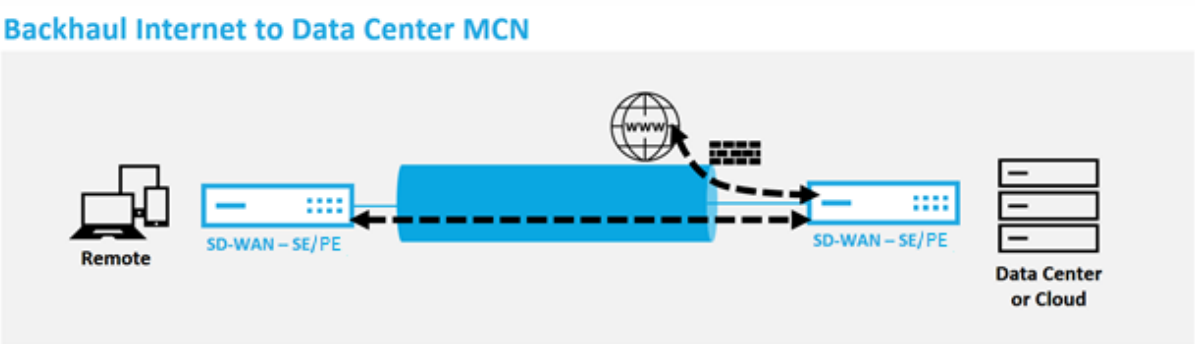
Backhaul Internet

October 28, 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 Remotestandort, 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.



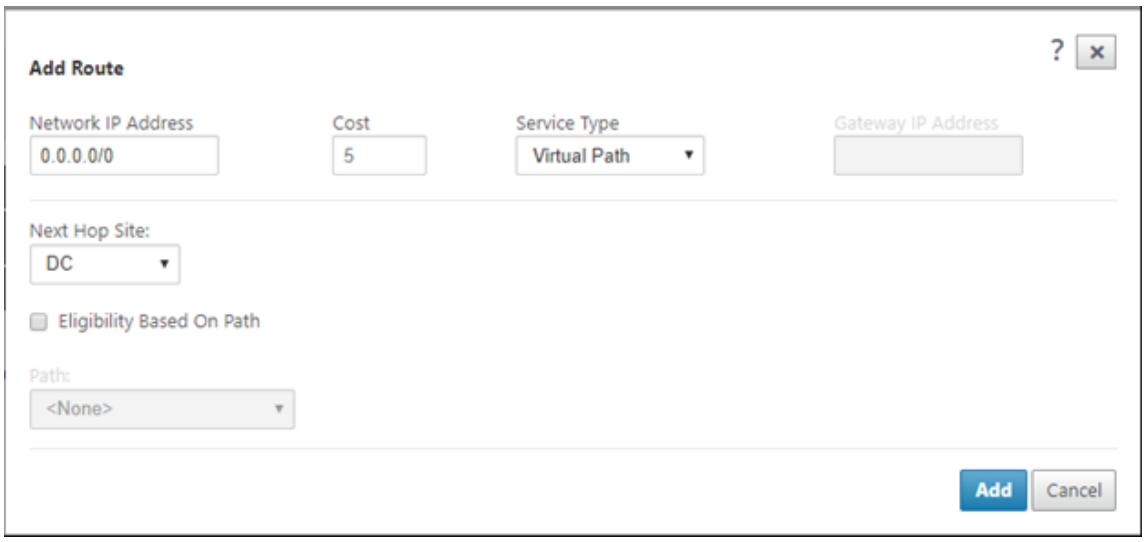
Alle Citrix SD-WAN Geräte können bis zu acht verschiedene Internet-WAN-Verbindungen in einem einzigen Gerät beenden. Lizenzierte Durchsatzfunktionen für die aggregierten WAN-Verbindungen werden pro entsprechender Appliance im Citrix SD-WAN Datenblatt aufgeführt.

Die Citrix SD-WAN Lösung unterstützt die Backhaul des Internetverkehrs mit der folgenden Konfiguration.

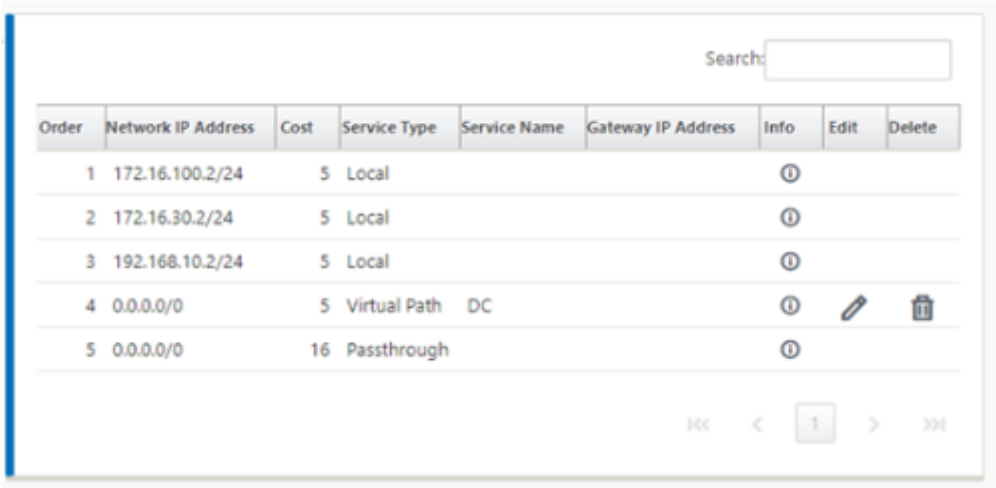
1. Aktivieren Sie den Internetdienst am MCN-Standortknoten oder jede andere Standortnotiz, an der Internetdienst gewünscht ist.

   > **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.



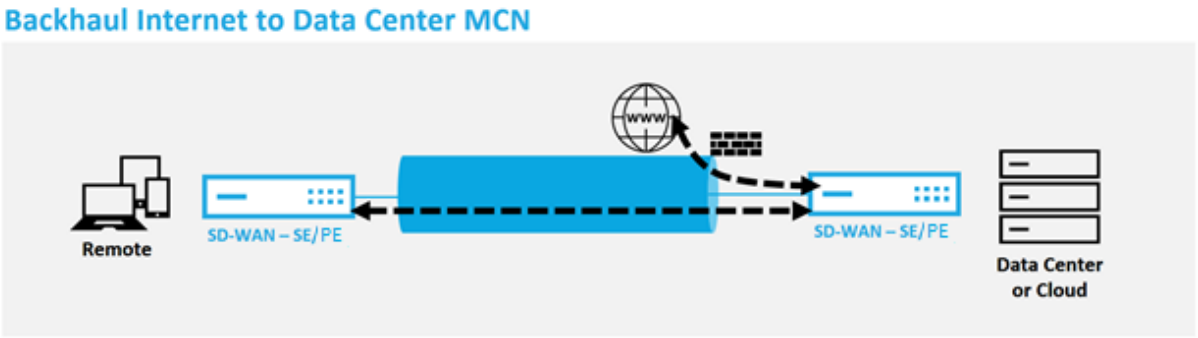
Hairpin-Modus

October 28, 2021

Mit der Bereitstellung von Haarnadeln können Sie die Verwendung einer Remote Hub-Website für den Internetzugang über Backhaul oder Hairpin implementieren, wenn lokale Internetdienste nicht verfügbar sind oder langsameren Datenverkehr verzeichnen. 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 optimierte technische Implementierung bereitzustellen. Sie können bei Bedarf einen Remote-Hub-Standort für den Internetzugang verwenden und Flows über den virtuellen Pfad zum SD-WAN-Netzwerk leiten.



Betrachten Sie beispielsweise einen Administrator mit mehreren SD-WAN-Sites, A und B. Standort A verfügt über einen schlechten Internetdienst. Standort B verfügt über einen nutzbaren Internetdienst, mit dem Sie nur den Traffic von Standort A zu Standort B zurückholen möchten. Sie können versuchen, dies zu erreichen, ohne die Komplexität strategisch gewichteter Routenkosten und die Weitergabe an Sites, die den Datenverkehr nicht erhalten sollten.

Außerdem wird die Routingtabelle nicht für alle Standorte in einer Hairpin-Bereitstellung freigegeben. Wenn beispielsweise der Verkehr zwischen Standort A und Standort B über Standort C festgeklemmt wird, ist nur Standort C die Routen von Standort A und B bekannt. Standort A und Standort B teilen sich im Gegensatz zur WAN-zu-WAN-Weiterleitung nicht die Routentabelle des anderen.

Wenn der Verkehr zwischen Standort A und Standort B durch Standort C Hairpin erfolgt, müssen die statischen Routen in Standort A und Standort B hinzugefügt werden, was darauf hinweist, dass der nächste Hop für beide Standorte der Zwischenstandort C ist.

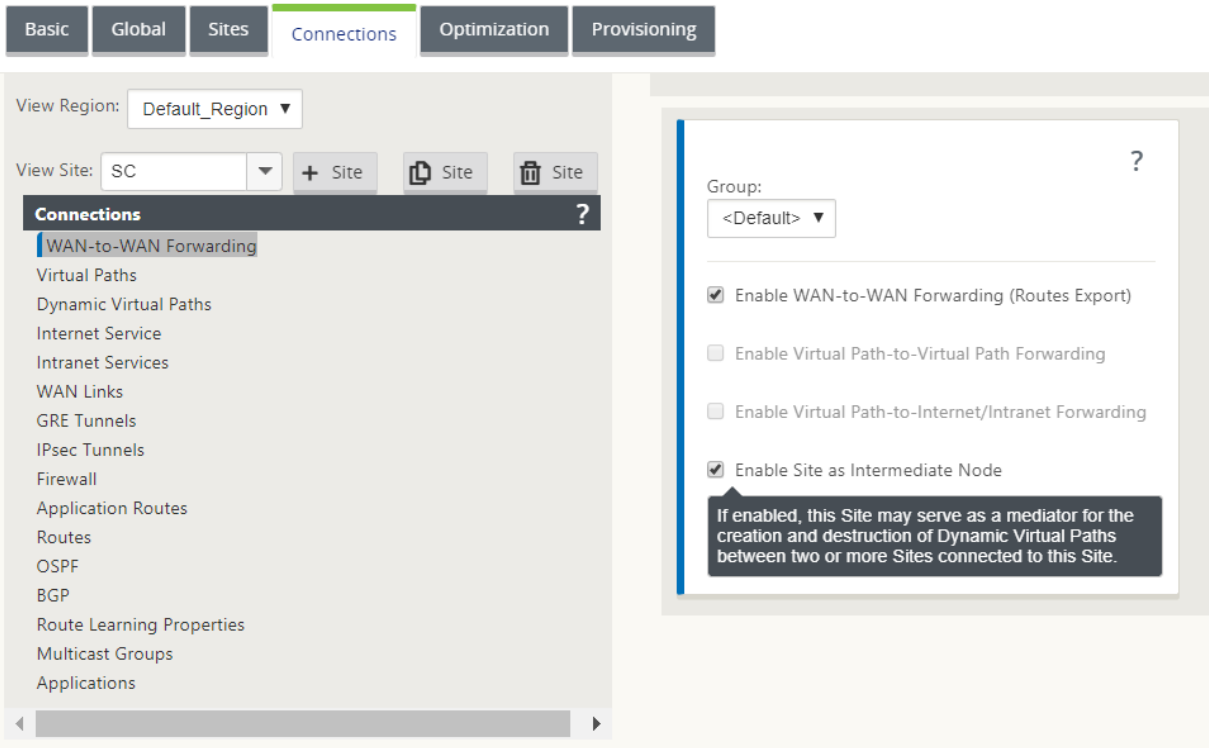
Wan-to-WAN Forwarding und Hairpin-Bereitstellung weisen bestimmte Unterschiede auf, nämlich:

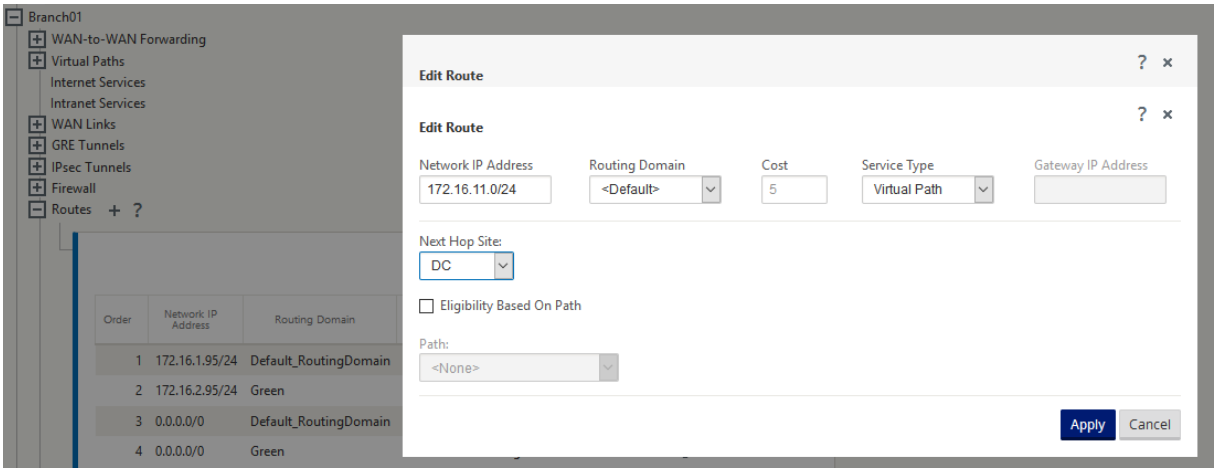
1. Dynamische virtuelle Pfade sind nicht konfiguriert. Immer sieht der Zwischenstandort den gesamten Verkehr zwischen den beiden Standorten.
2. Nimmt nicht an WAN-zu-WAN-Weiterleitungsgruppen teil.

   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 Hairpin-Bereitstellung. Sie können jetzt eine 0.0.0.0/0 Route zum Hairpin-Verkehr zwischen zwei Standorten konfigurieren, ohne zusätzliche Standorte zu beeinträchtigen. Wenn Hairpinning für den Intranet-Verkehr verwendet wird, werden bestimmte Intranet-Routen zur Client-Site hinzugefügt, um den Intranet-Verkehr 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 Hairpin-Bereitstellung über die Citrix SD-WAN Webverwaltungsoberfläche im Konfigurationseditor konfigurieren.





Gehostete Firewalls

October 28, 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

October 28, 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 Hauptziele 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

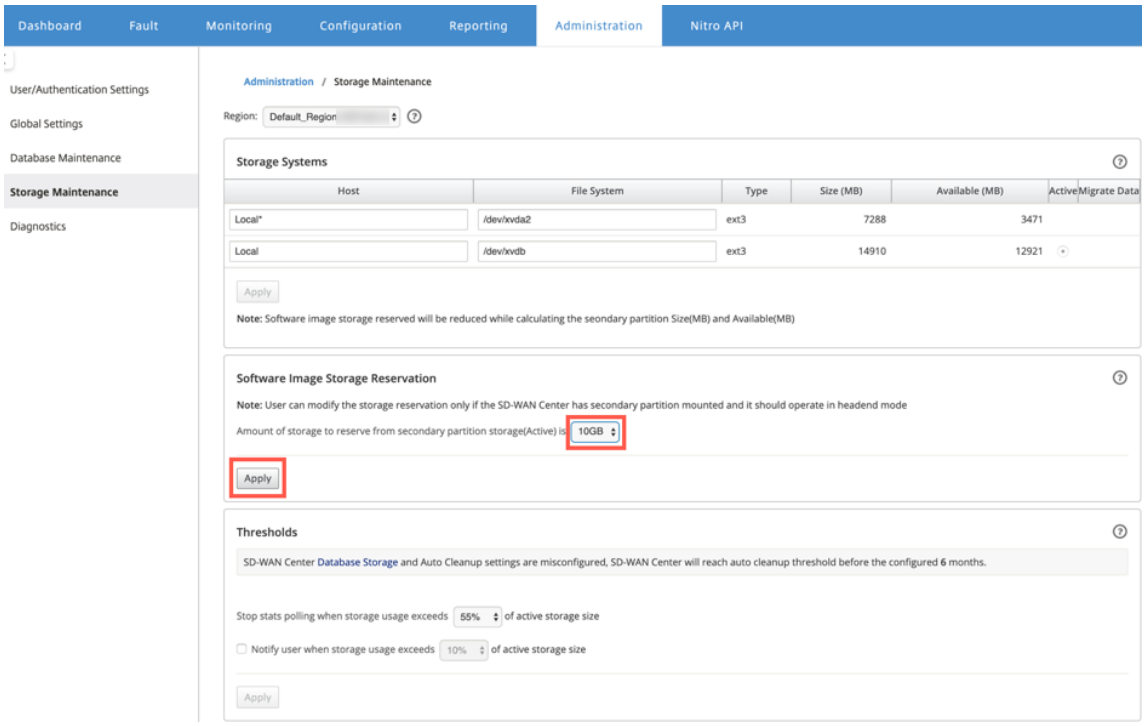
Es gibt zwei Möglichkeiten, die virtuelle Firewall-Maschine bereitzustellen:

- 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

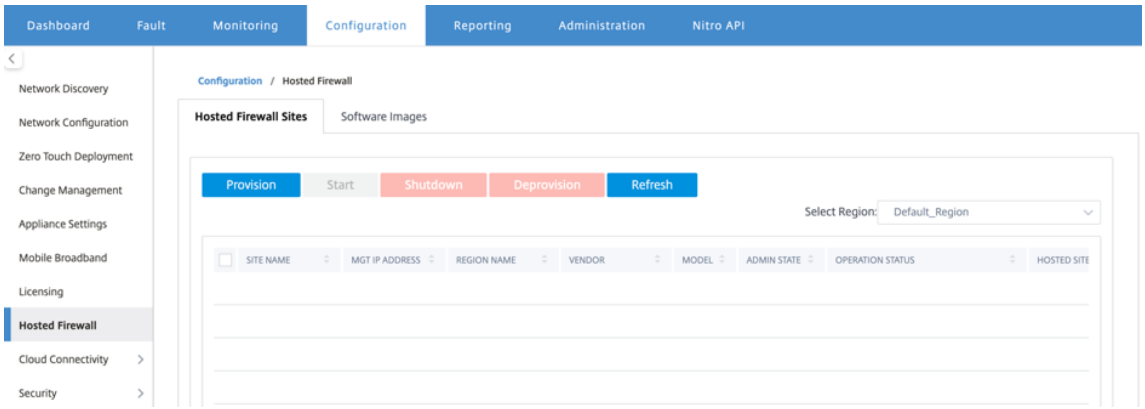
- Fügen Sie dem SD-WAN Center den sekundären Speicher hinzu, um die Firewall-VM-Imagedateien zu speichern. Weitere Informationen finden Sie unter Systemanforderungen und Installation.
- Reservieren Sie den Speicher von der sekundären Partition für die Firewall-VM-Imagedateien. Um das Speicherlimit zu konfigurieren, navigieren Sie zu **Administration > Speicherwartung**.
  - Wählen Sie die erforderliche Speichermenge aus der Liste aus.
  - Klicken Sie auf **Apply**.



> **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.

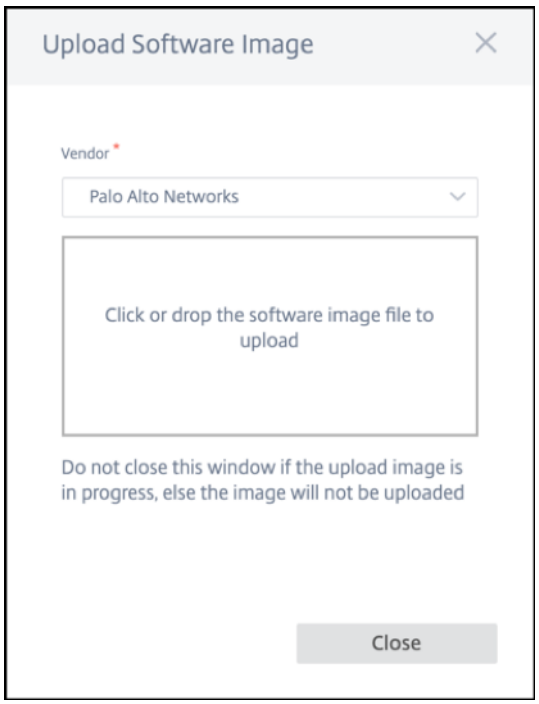


   Sie können die **Region** aus der Dropdownliste auswählen, um die bereitgestellten Site-Details für diese ausgewählte Region anzuzeigen.

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 Dropdownliste aus. Klicken oder legen Sie die Softwareimage-Datei in das Feld für den Upload ab.

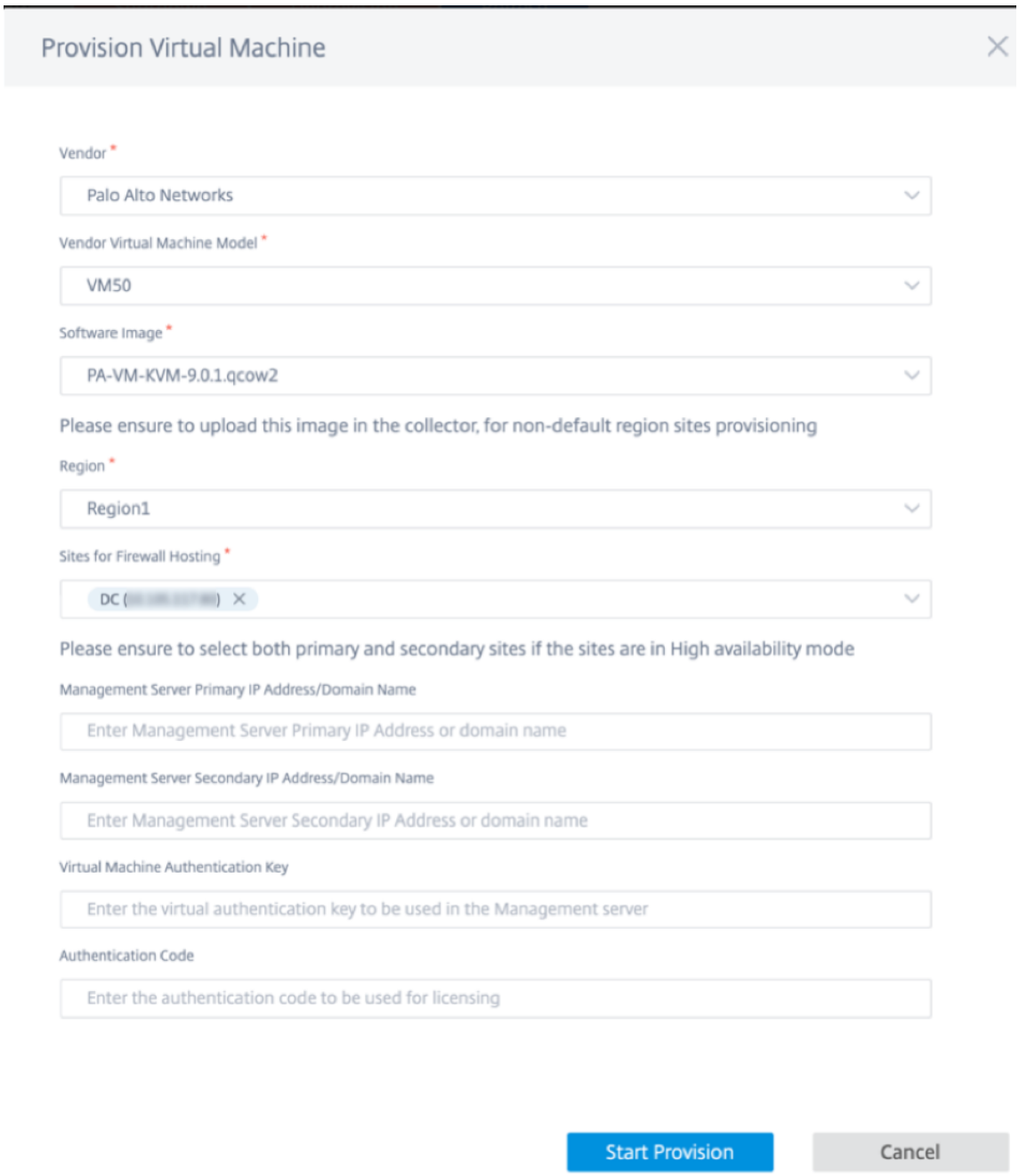


Eine Statusleiste mit dem laufenden Upload-Prozess wird angezeigt. Klicken Sie auf **Aktualisieren** oder führen Sie keine andere Aktion aus, bis die Imagedatei 100% hochgeladen zeigt.

- **Aktualisieren**: Klicken Sie auf die Option **Aktualisieren**, um die neuesten Imagedateidetails 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**.



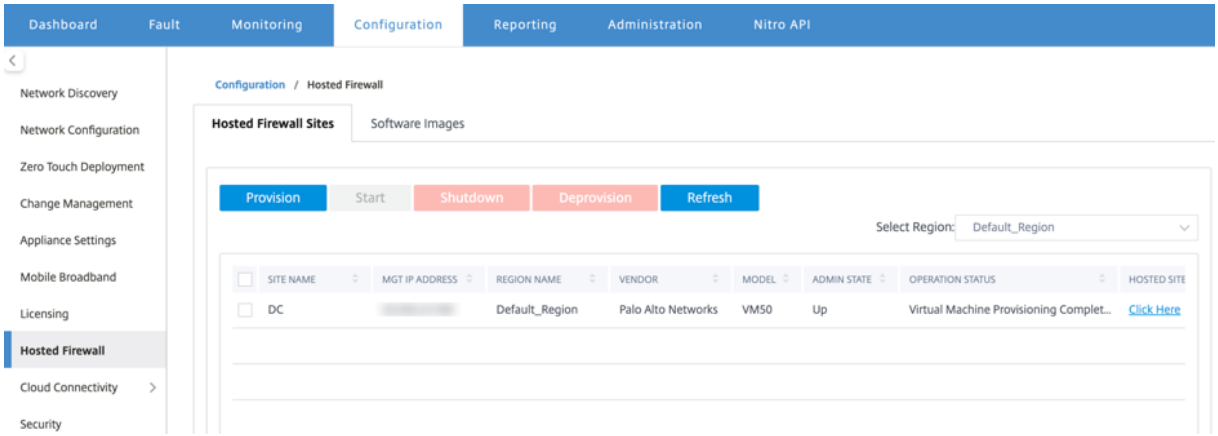
- **Anbieter**: Wählen Sie den **Anbieternamen** als **Palo Alto Networks** aus der Dropdownliste aus.
- **Vendor Virtual Machine Model**: Wählen Sie die Modellnummer der virtuellen Maschine aus der Liste aus.
- **Software-Image**: Wählen Sie die zu bereitzustellende Imagedatei aus.
- **Region**: Wählen 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 Domänennamen ein (optional).
- **Sekundäre IP-Adresse des Management-Servers**: Geben Sie die sekundäre IP-Adresse des Management-Servers oder den vollqualifizierten Domänennamen ein (optional).
- **Authentifizierungsschlüssel für virtuelle Maschinen**: Geben Sie den virtuellen Authentifizierungsschlüssel ein, der auf dem Managementserver 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 von Palo Alto Networks vollständig gestartet wurde, spiegelt sie die SD-WAN Center-Benutzeroberfläche wider.

Sie können die virtuelle Maschine nach Bedarf **starten, herunterfahren** und **deaktivieren**.

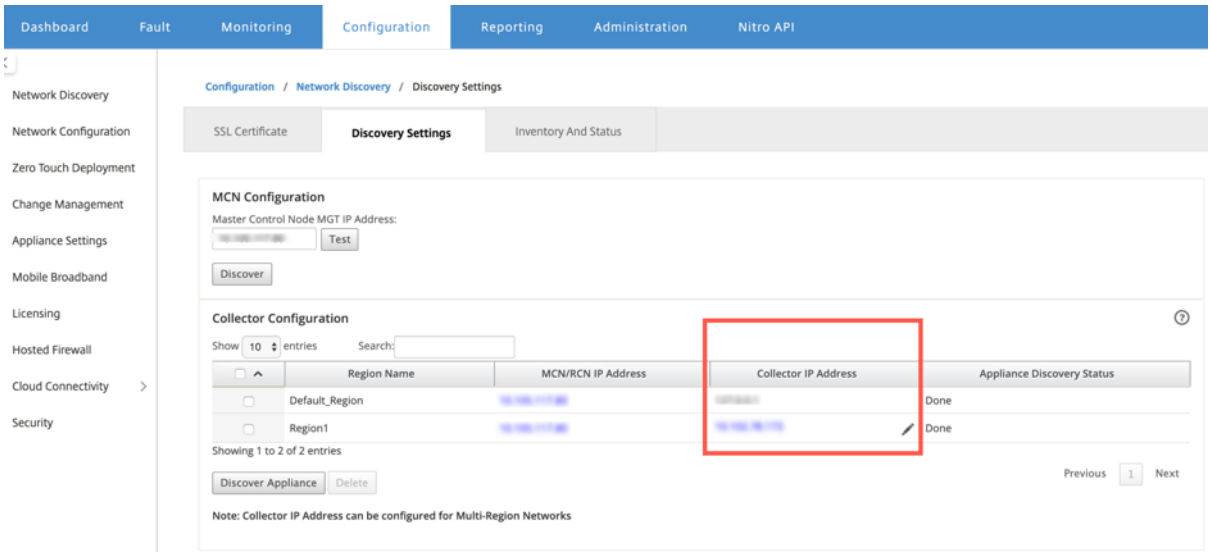


- **Standortname**: Zeigt den Standortnamen an.
- **Management-IP**: Zeigt die Management-IP-Adresse der Site an.
- **Regionsname**: Zeigt die Regionsbezeichnung an.
- **Anbieter**: Zeigt den Namen des Anbieters an (Palo Alto Networks).
- **Modell**: Zeigt die Modellnummer an (VM50/VM100).
- **Administratorstatus**: Status der virtuellen Maschine des Herstellers (Up/Down).
- **Betriebsstatus**: Zeigt die Meldung des 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 Softwareimage auf den

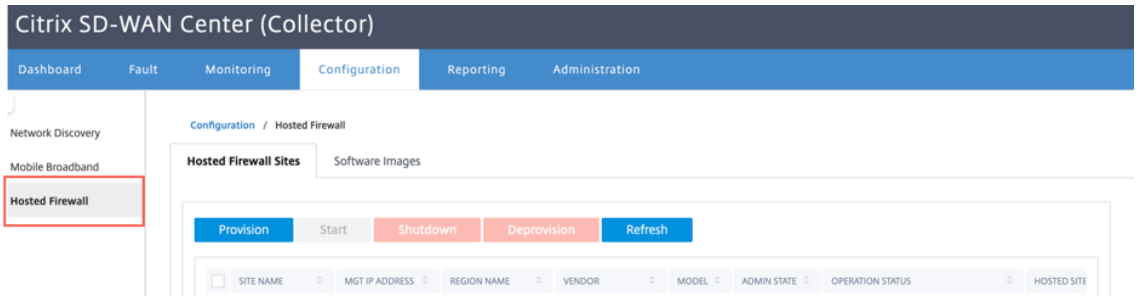
SD-WAN Center Collector hochladen. Sie können die Palo Alto Networks sowohl über die SD-WAN Center-Head-End-GUI als auch über den SD-WAN Center Collector bereitstellen.

Um die IP-Adresse des SD-WAN Center Collector abzurufen, navigieren Sie zu **Konfiguration > Netzwerkerkennung**, wählen Sie die Registerkarte **Discovery-Einstellungen**.

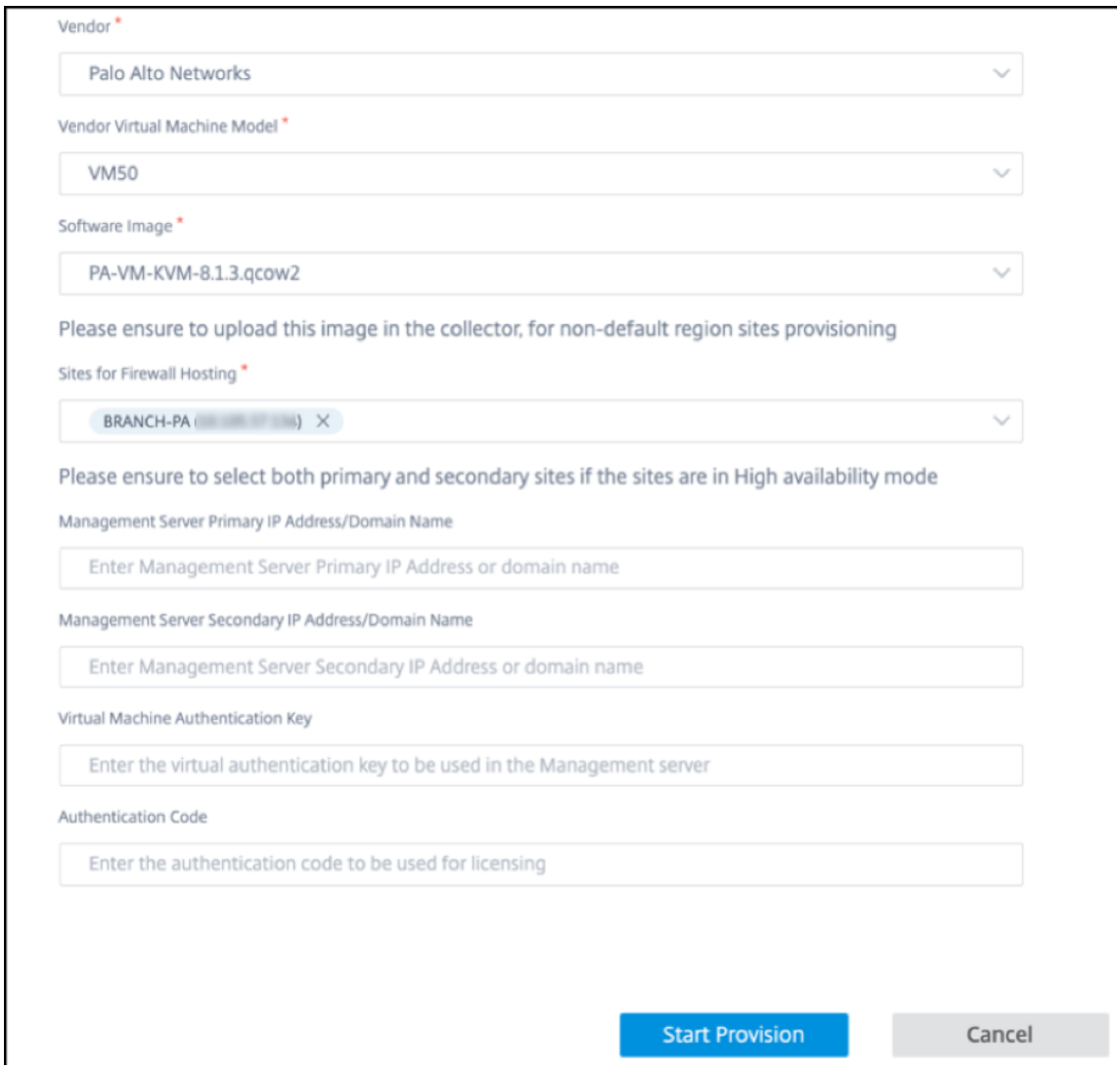


So stellen Sie die Palo Alto Networks von SD-WAN Collector bereit:

1. Navigieren Sie von 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-Websites** auf **Bereit**
4. Geben Sie die folgenden Details an und klicken Sie auf **Bereitstellung starten**.



- **Anbieter**: Wählen Sie den **Anbieternamen** als **Palo Alto Networks** aus der Dropdownliste 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 Domänennamen ein (optional).
- **Sekundäre IP-Adresse des Management-Servers**: Geben Sie die sekundäre IP-Adresse

des Management-Servers oder den vollqualifizierten Domänennamen ein (optional).

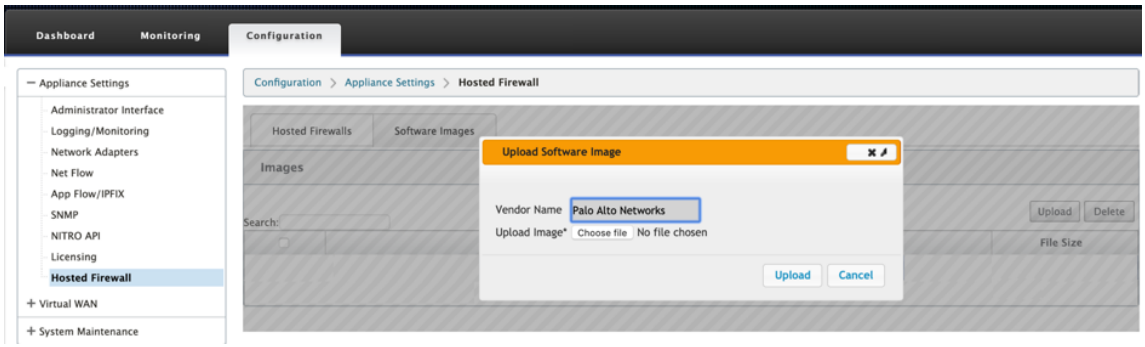
- **Authentifizierungsschlüssel für virtuelle Maschinen**: Geben Sie den virtuellen Authentifizierungsschlüssel ein, der auf dem Managementserver verwendet werden soll.
- **Authentifizierungscode**: Geben Sie den virtuellen Authentifizierungscode ein, der für die Lizenzierung verwendet werden soll.

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:

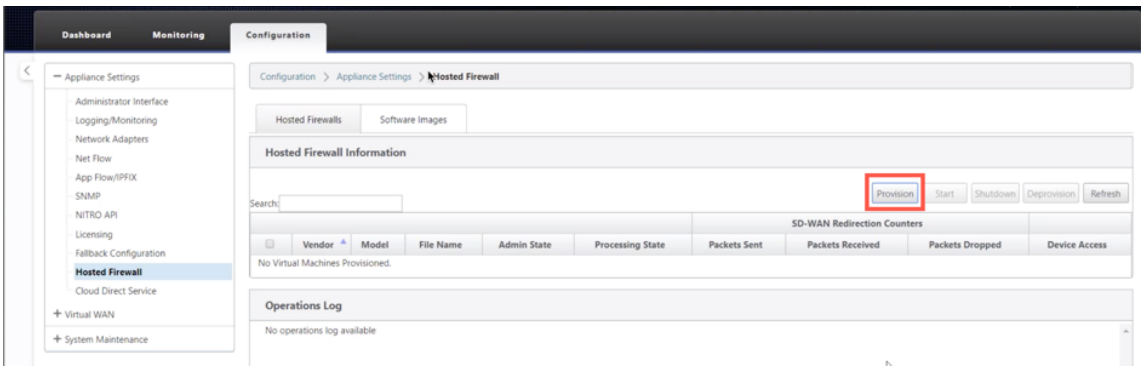
1. Navigieren Sie in der Citrix SD-WAN GUI zu **Konfiguration** > **Appliance-Einstellungen** erweitern >**Gehostete Firewall** auswählen.
2. Laden Sie das Softwareimage hoch:
   - Wählen Sie die Registerkarte **Software-Images**. Wählen Sie den Namen des Anbieters als **Palo Alto Networks**aus.
   - 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 wird aktualisiert, sobald das Image erfolgreich hochgeladen wurde. Das Image, das für die Bereitstellung verwendet wird, kann nicht gelöscht werden. Führen Sie keine Aktion aus oder gehen Sie zurück zu einer anderen Seite, bis die Imagedatei 100% hochgeladen zeigt.

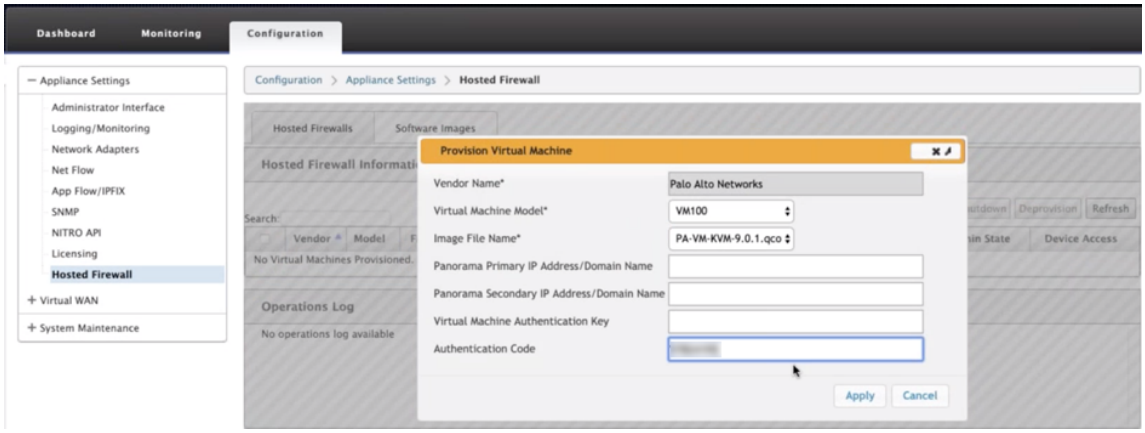
3. Wählen Sie für die Provisioning die Registerkarte **Gehostete Firewalls** aus und klicken Sie auf **die Schaltfläche Bereitstellen**.



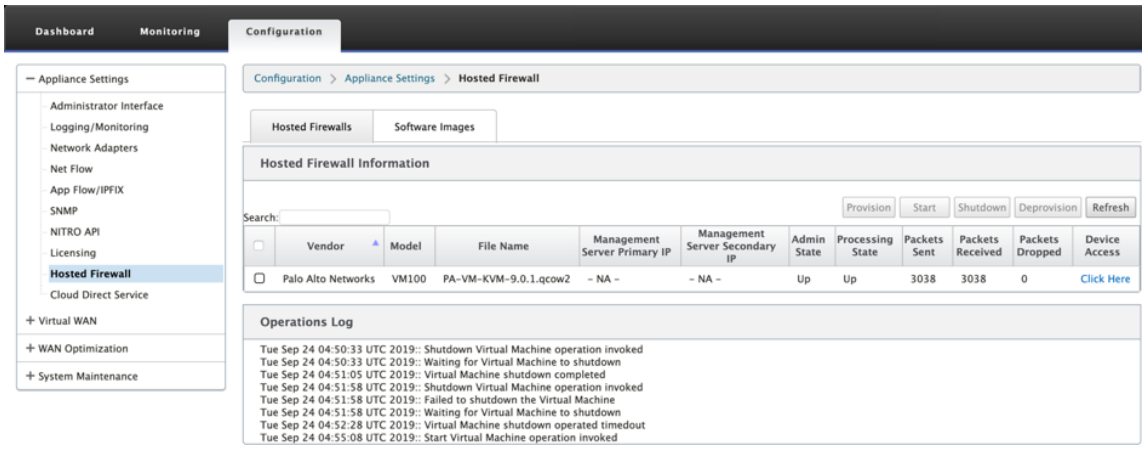
4. Geben Sie die folgenden Details für die Provisioning.

   - **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.
   - **Bilddateiname**: Wählen Sie die Image-Datei aus.
   - **Primäre IP-Adresse von Panorama**: Geben Sie die primäre IP-Adresse oder den vollqualifizierten Domainnamen von Panorama an (optional).
   - **Sekundäre Panorama-IP-Adresse/Domain-Name**: Geben Sie die sekundäre Panorama-IP-Adresse oder den vollqualifizierten Domainnamen 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 **Apply**.



5. Klicken Sie auf **Aktualisieren**, um den neuesten Status zu erhalten. Nachdem die virtuelle Maschine von Palo Alto Networks vollständig gestartet wurde, wird die SD-WAN-Benutzeroberfläche mit den Details des Vorgangs zum Protokoll reflektiert.



- **Admin-Status**: Gibt an, ob die virtuelle Maschine hoch- oder heruntergefahren ist.
- **Verarbeitungsstatus**: Datapath-Verarbeitungsstatus der virtuellen Maschine.
- **Paket gesendet**: Pakete, die von SD-WAN an die virtuelle Sicherheitsmaschine gesendet wurden.
- **Paket empfangen**: Pakete, die von SD-WAN von der virtuellen Sicherheitsmaschine empfangen wurden.
- **Paket verworfen**: Pakete, die von SD-WAN verworfen wurden (z. B. wenn die virtuelle Sicherheitsmaschine ausgefallen ist).
- **Gerätezugriff**: Klicken Sie auf den Link, um die 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 Maschine von Palo Alto Networks zuzugreifen, oder verwenden Sie Ihre Verwaltungs-IP zusammen mit dem 4100-Port (Management-IP: 4100).

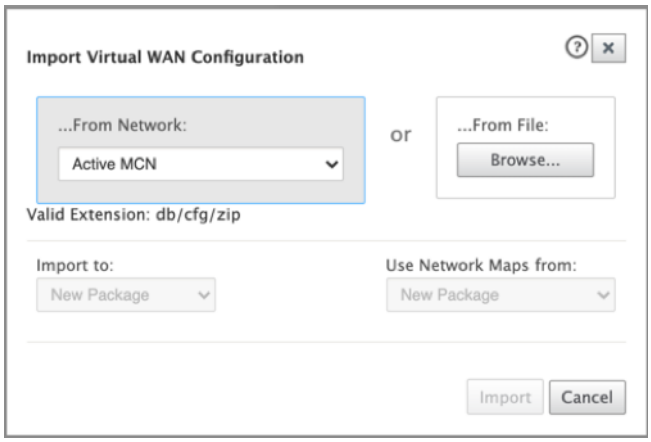
> **Hinweis**
> Verwenden Sie immer den Inkognito-Modus, um auf die Palo Alto Networks GUI zuzugreifen.

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:

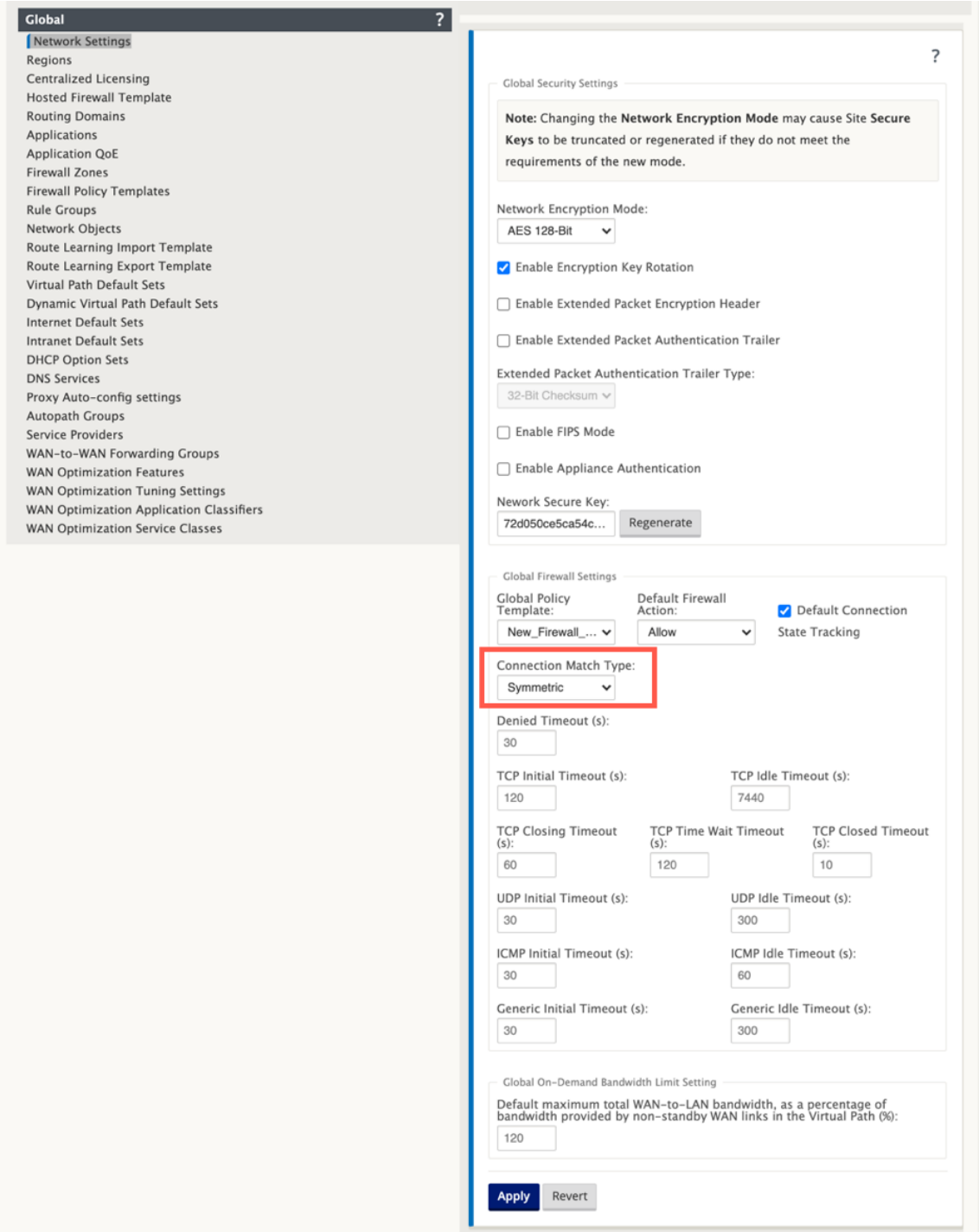
1. Öffnen Sie Citrix SD-WAN Center UI, navigieren Sie zu **Konfiguration > Netzwerkkonfigurationsimport**. Importieren Sie die virtuelle WAN-Konfiguration aus dem aktiven MCN und klicken Sie auf **Importieren**.



Die restlichen Schritte sind ähnlich wie folgt - die Konfiguration der Datenverkehrsumleitung über MCN.

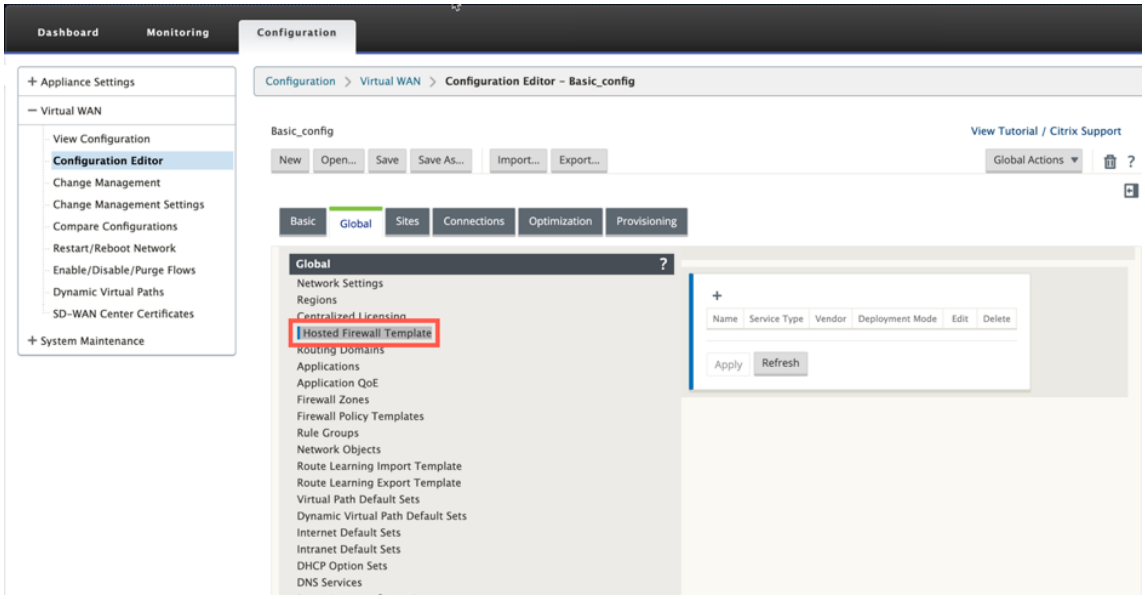
So navigieren Sie durch den Konfigurationseditor auf MCN:

1. Setzen Sie **Verbindungsanpassungstyp** unter **Global > Netzwerkeinstellungen** auf **Symmetrisch**.

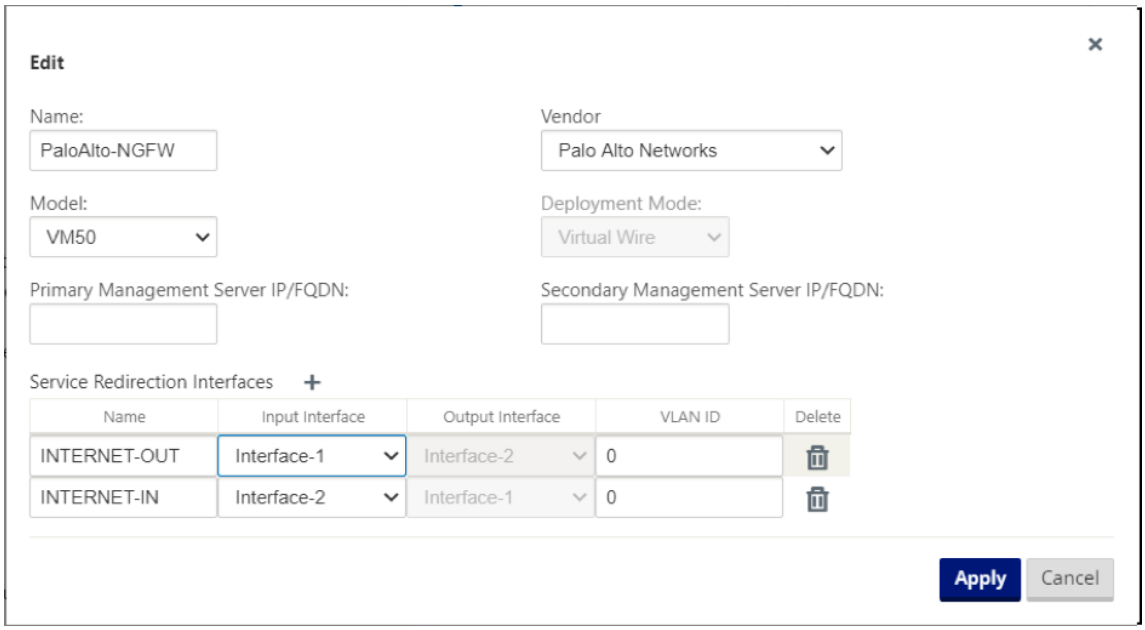


Standardmäßig sind SD-WAN-Firewallrichtlinien richtungsspezifisch. Der symmetrische Übereinstimmungstyp entspricht den Verbindungen anhand der angegebenen Übereinstimmungskriterien und wendet die Richtlinienaktion in beide Richtungen an.

2. Öffnen Sie **Citrix SD-WAN UI**, navigieren Sie zu **Konfiguration**, erweitern Sie **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**.



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, befinden sich intern im SD-WAN und der gehosteten Firewall.

> **Hinweis**
>
> Die Umleitungs-Eingabeschnittstelle 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.

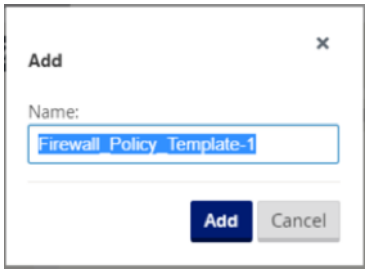
Über SD-WAN-Firewallrichtlinien oder Richtlinien auf Standortebene können Sie den gesamten Datenverkehr auf die virtuelle Maschine Palo Alto Networks umleiten.

> **Hinweis**
>
> SD-WAN-Firewall-Richtlinien werden automatisch erstellt, um den Datenverkehr zu/von gehosteten Firewall-Verwaltungsservern **zuzulassen**. Dadurch wird eine Umleitung des Verwaltungsdatenverkehrs vermieden, der von einer gehosteten Firewall stammt (oder).

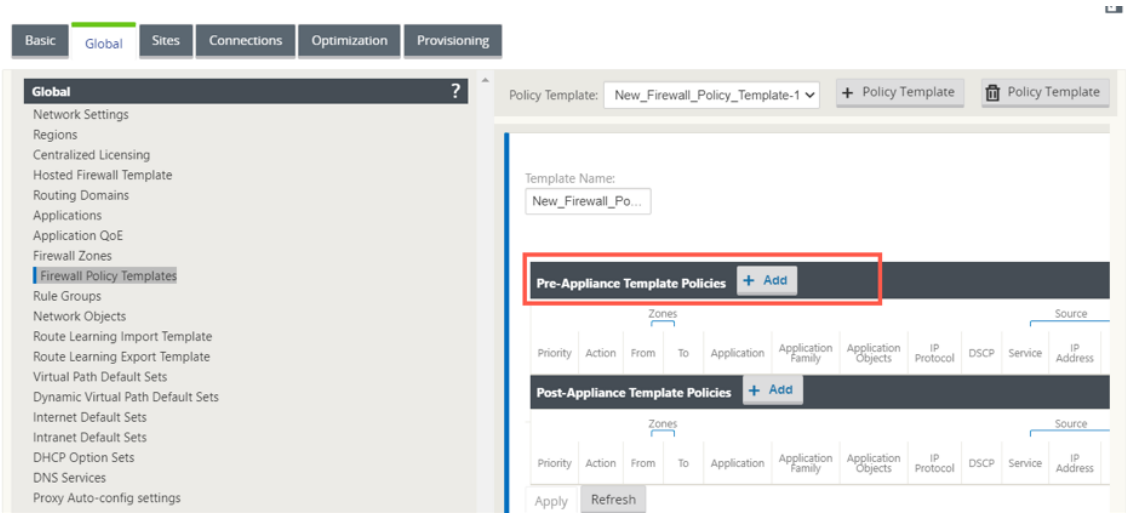
Die Umleitung des Datenverkehrs zur virtuellen Firewall-Maschine kann mithilfe von SD-WAN-Firewall-Richtlinien erfolgen. Es gibt zwei Methoden zum Erstellen von SD-WAN-Firewall-Richtlinien - entweder über Firewall-Richtlinienvorlagen im **globalen** Abschnitt oder auf Site-Ebene.

Methode - 1

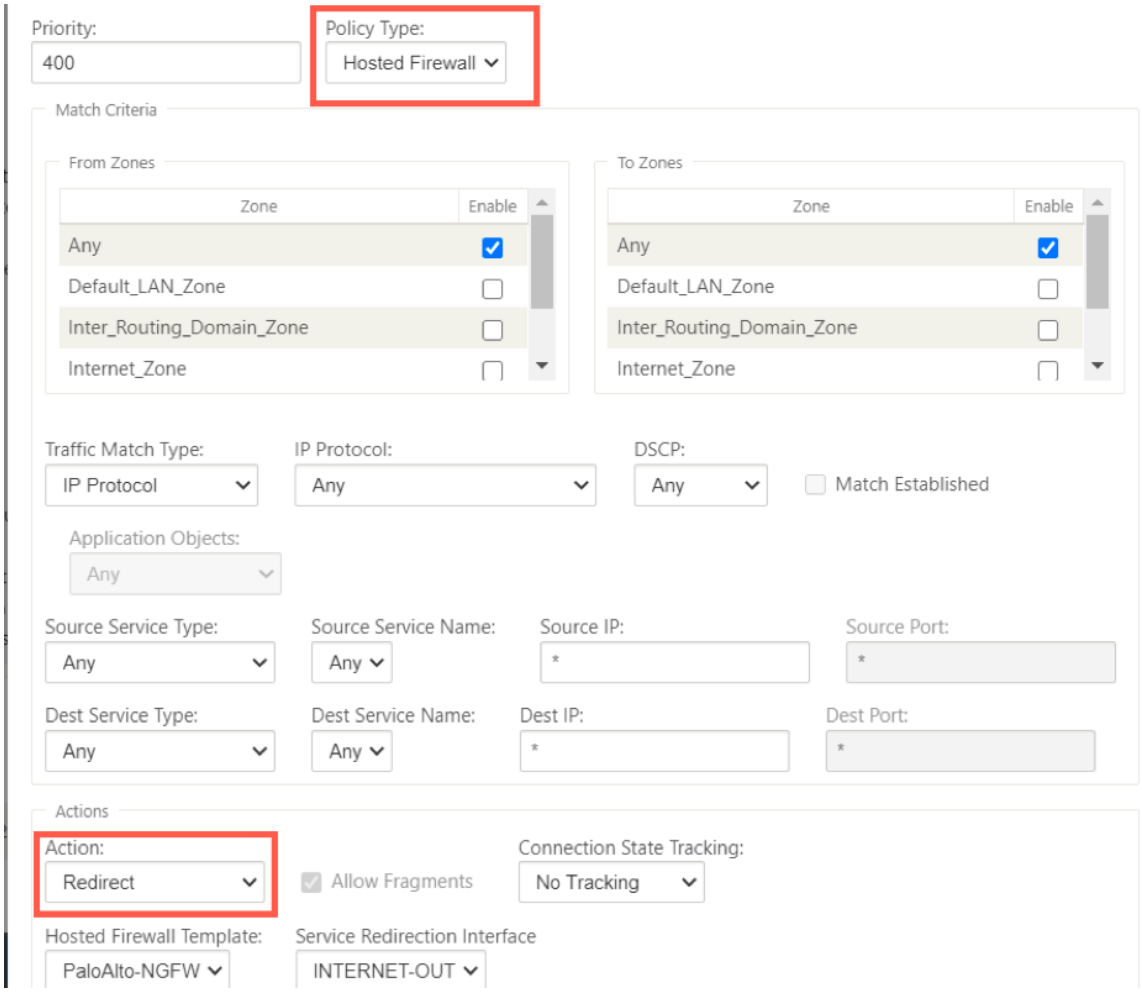
1. Navigieren Sie von Citrix SD-WAN GUI zu **Konfiguration** erweitern Sie **Virtual WAN > Konfigurationseditor**. Navigieren Sie zur Registerkarte **Global** und wählen Sie **Firewall-Richtlinienvorlagen**aus Klicken Sie auf **+ Richtlinienvorlage** Geben Sie der Richtlinienvorlage einen Namen an und klicken Sie auf **Hinzufügen**.



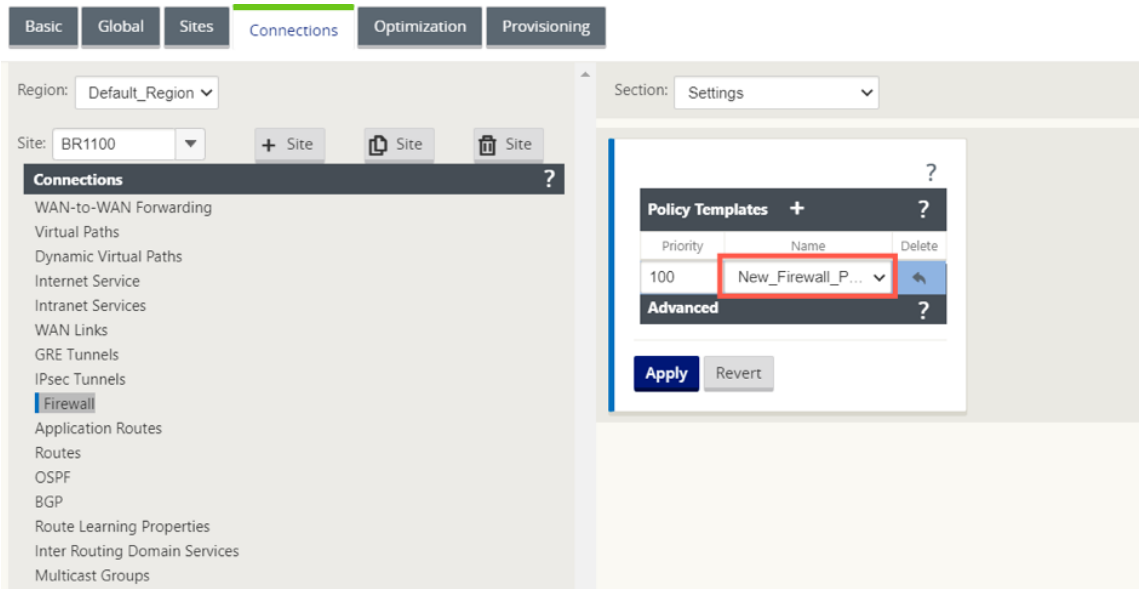
2. Klicken Sie auf **+ Hinzufügen** neben **Richtlinien für Pre-Appliance-Vorlagen**.



3. Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch mit **Redirect**gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdownliste aus. Füllen Sie die anderen Übereinstimmungskriterien nach Bedarf aus.

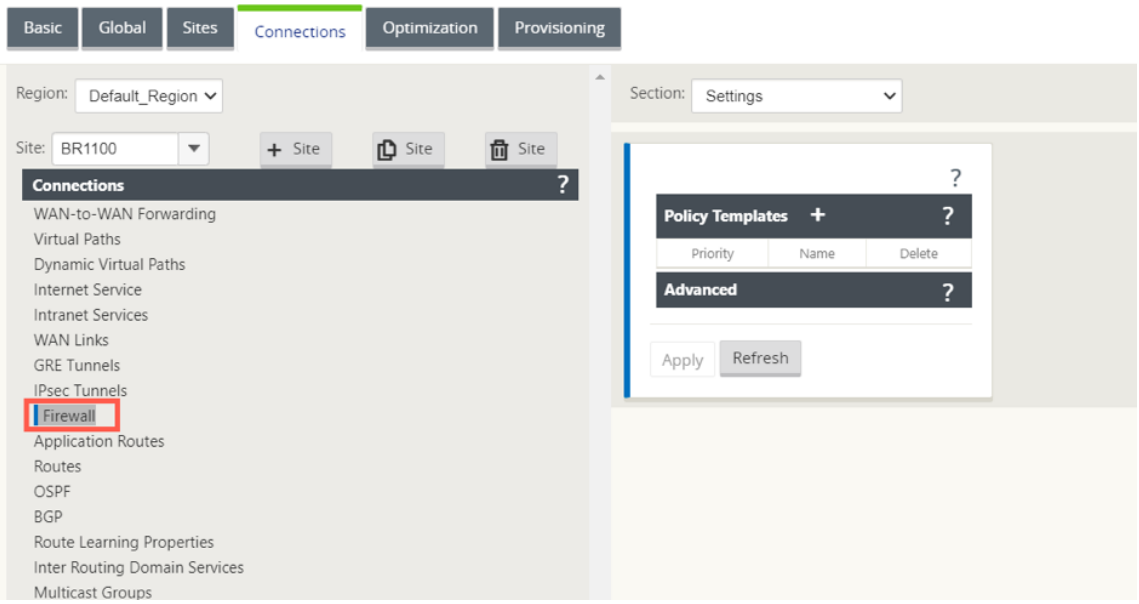


4. Navigieren Sie zu den **Verbindungen > Firewall**und wählen Sie dann die Firewall-Richtlinie (die Sie erstellt haben) unter dem Namensfeld aus. Klicken Sie auf **Apply**.

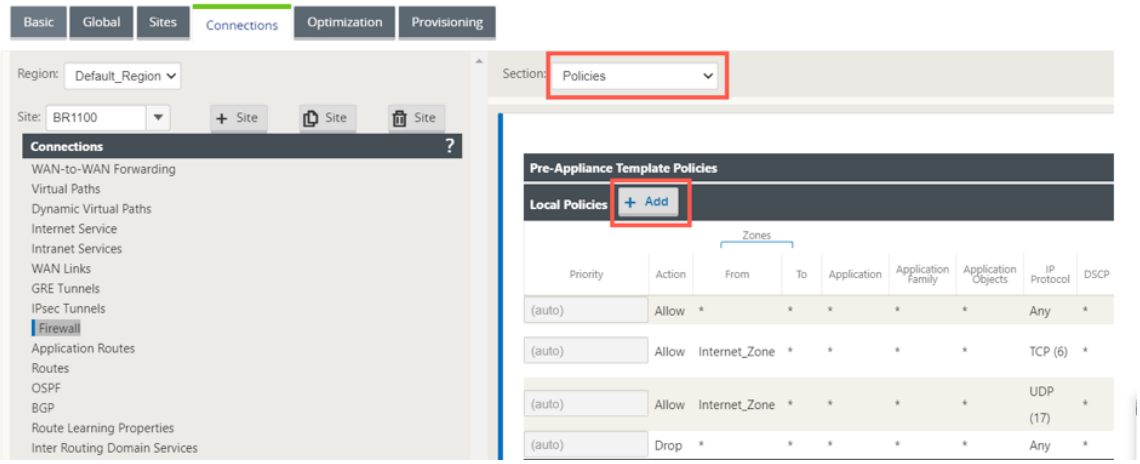


Methode - 2

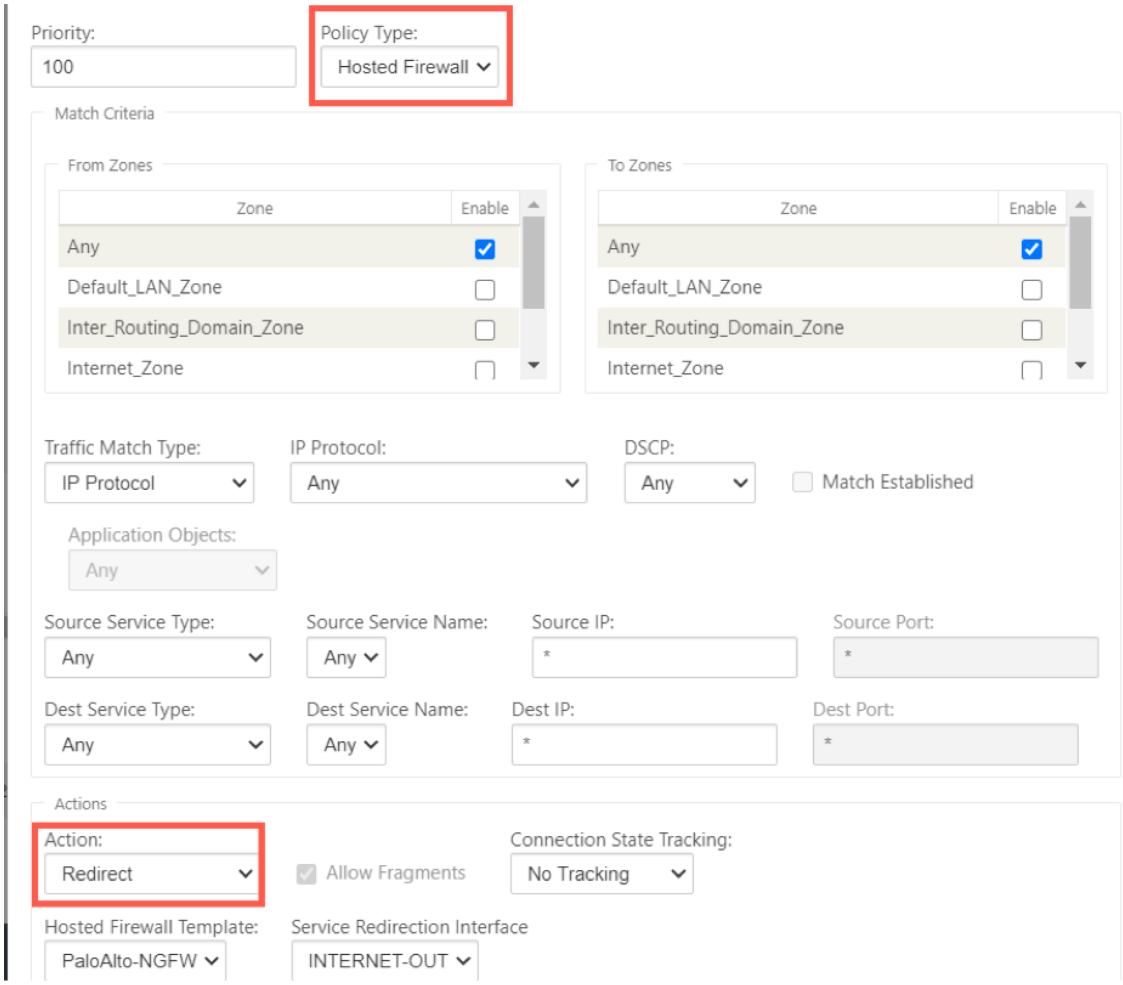
1. Um den gesamten Datenverkehr umzuleiten, navigieren Sie unter dem **Konfigurationseditor > Virtual WAN**zur Registerkarte **Verbindung** und wählen Sie **Firewall**aus.



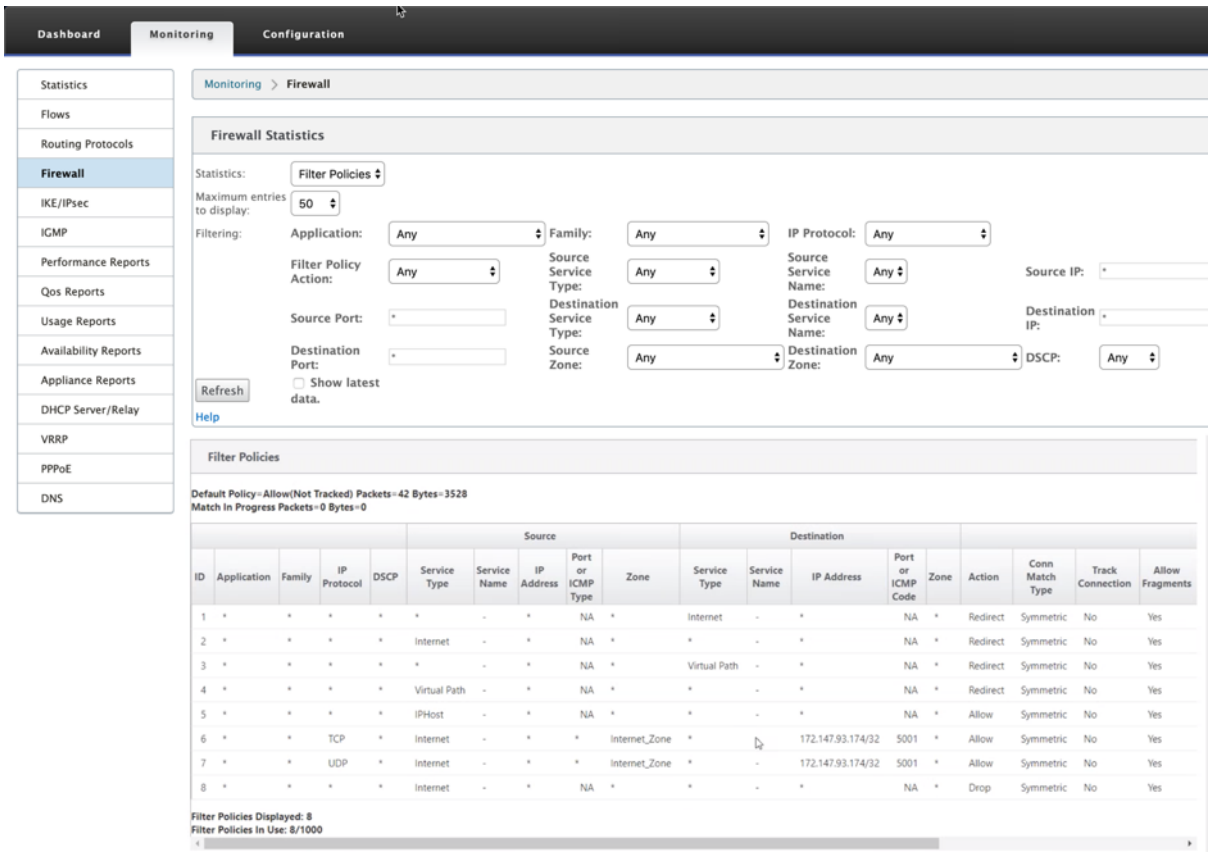
2. Wählen Sie in der Dropdownliste **Abschnitt** die Option **Richtlinien** aus und klicken Sie auf **+Hinzufügen**, um eine neue Firewall-Richtlinie zu erstellen.



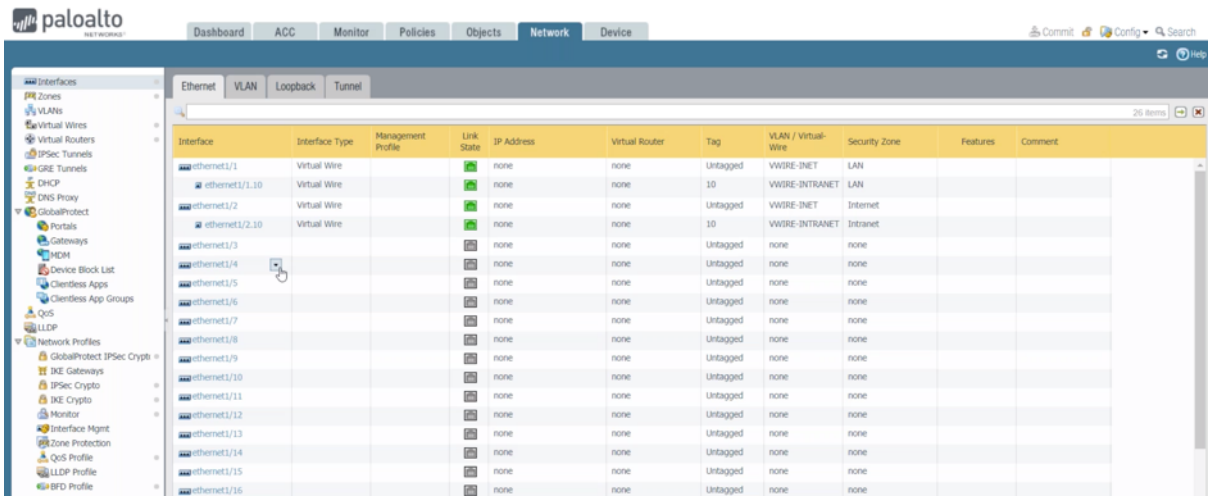
3. Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch auf Redirect gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdownliste aus. Klicken Sie auf **Hinzufügen**.



Während die gesamte Netzwerkkonfiguration ausgeführt wird, können Sie die Verbindung unter **Überwachung > Firewall** > unter **Statistikliste** überwachen und **Richtlinien filtern**.



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.



> **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.

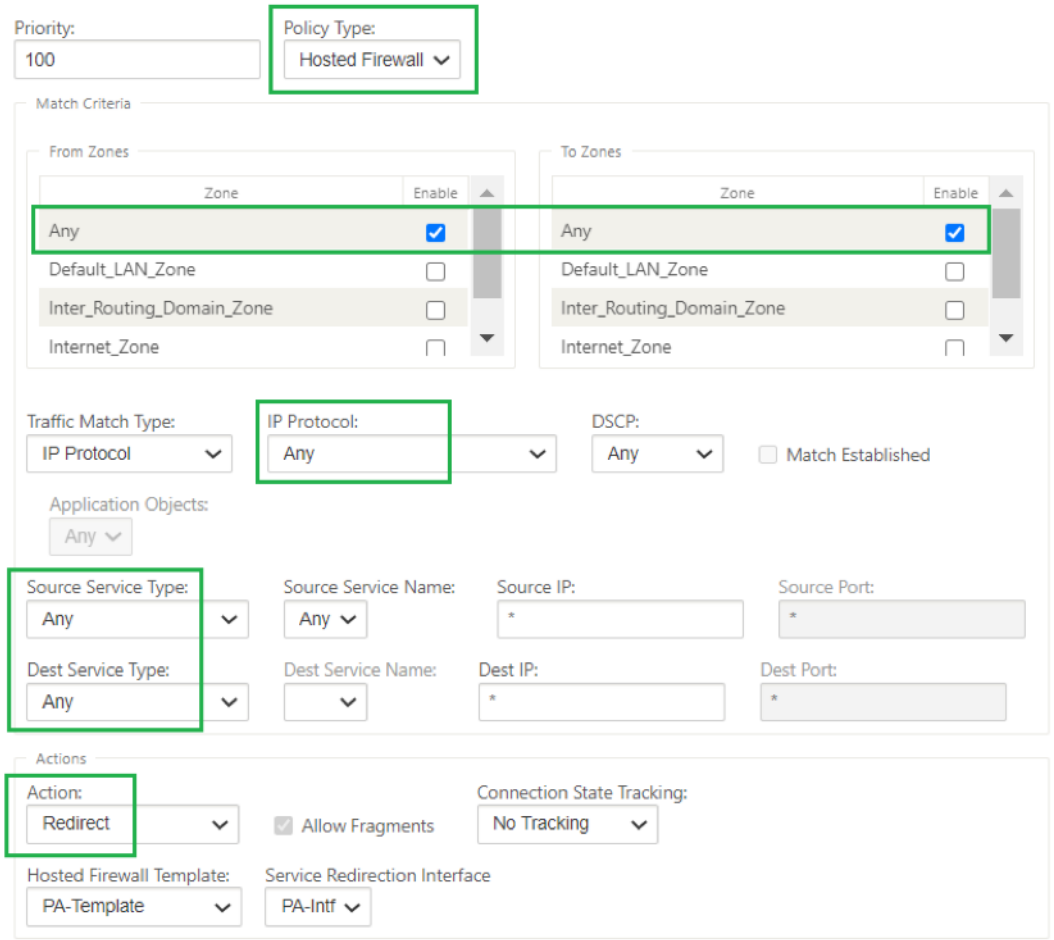
Anwendungsfälle —Hosted Firewall auf SD-WAN 1100

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.

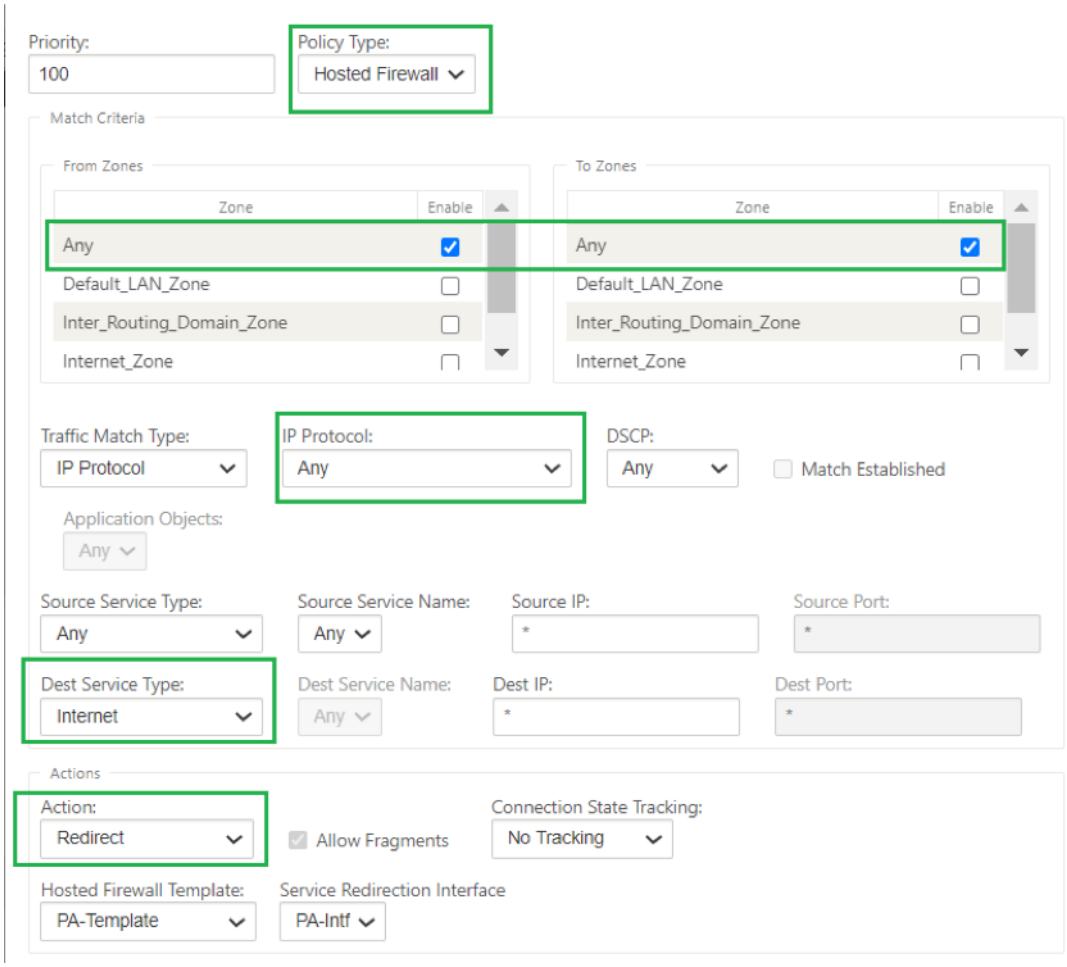
Um dies zu erreichen, erstellen Sie eine Firewall-Regel, die mit jedem Datenverkehr und **Action** as **Redirect**übereinstimmt, wie im folgenden Screenshot gezeigt:



Anwendungsfall 2: Nur Internetverkehr in die Hosted Firewall umleiten

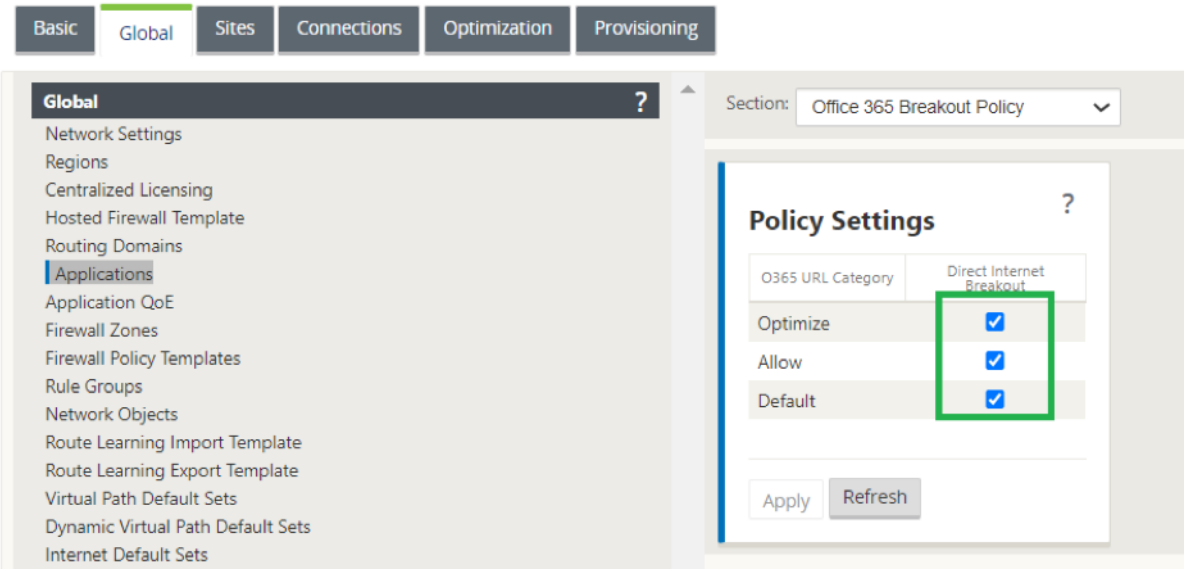
Dieser Anwendungsfall gilt für alle Zweigstellen, bei denen Internet-gebundener Datenverkehr den Umfang des unterstützten umgeleiteten Datenverkehrs nicht überschreitet. In diesem Fall wird der Datenverkehr zwischen Rechenzentren von Sicherheitsgeräten/-diensten verarbeitet, die in Rechenzentren bereitgestellt werden.

Um dies zu erreichen, erstellen Sie eine Firewall-Regel, die mit jedem Datenverkehr und **Action** as **Redirect** übereinstimmt, wie im folgenden Screenshot gezeigt:

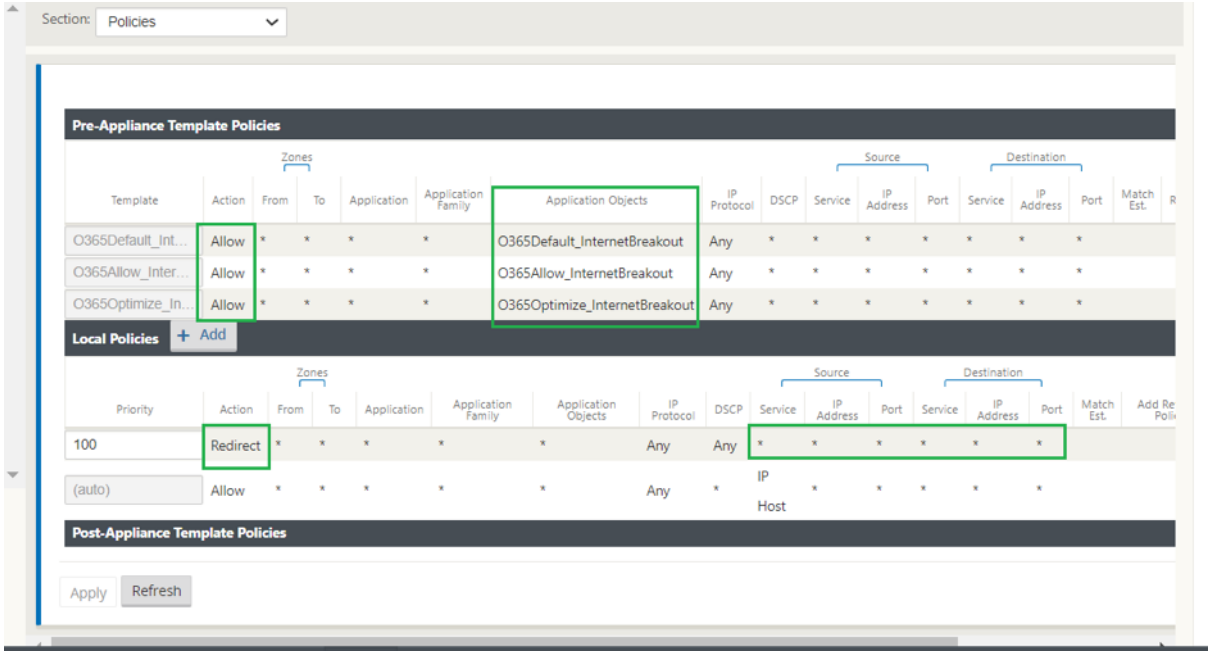


Anwendungsfall 3: Direkter Internet-Breakout für vertrauenswürdige Internet-SaaS-Anwendungen und Weiterleitung des verbleibenden gesamten Datenverkehrs auf die gehostete VM

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-Konfiguration. Daher kann die gehostete Firewall gemäß den Sicherheitsanforderungen des Unternehmens konfiguriert werden.

Check Point Firewall-Integration auf SD-WAN 1100 Plattform

October 28, 2021

Citrix SD-WAN unterstützt das Hosting von **Check Point Quantum Edge** auf der SD-WAN 1100-Plattform.

Der **Check Point Quantum Edge** läuft als virtuelle Maschine auf der SD-WAN 1100-Plattform. 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.

> **Hinweis**
>
> Ab Citrix SD-WAN 11.3.1 wird die Check Point VM Version 80.20 und höher für die Provisioning von VM auf neuen Standorten unterstützt.

Vorteile

Im Folgenden werden die wichtigsten Ziele oder Vorteile der Check Point-Integration 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 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.

Provisioning der Check Point Firewall-VM

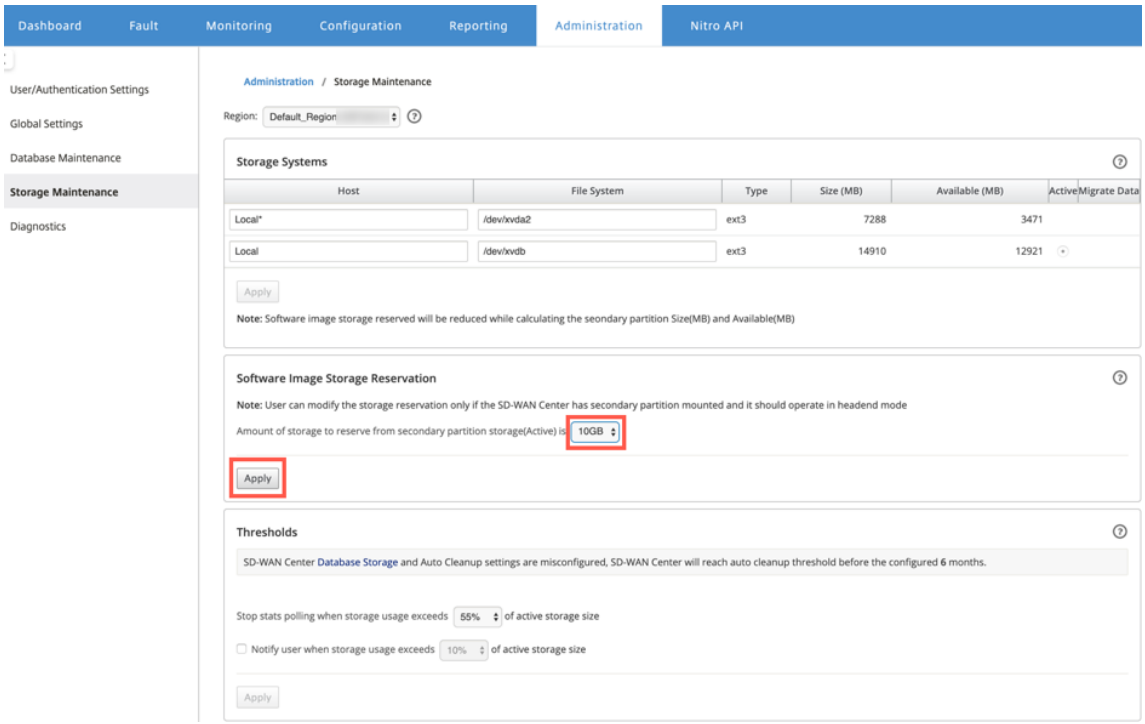
Es gibt zwei Möglichkeiten, die virtuelle Firewall-Maschine bereitzustellen:

- 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 die erforderliche Speichermenge aus der Liste aus.
  - Klicken Sie auf **Apply**.

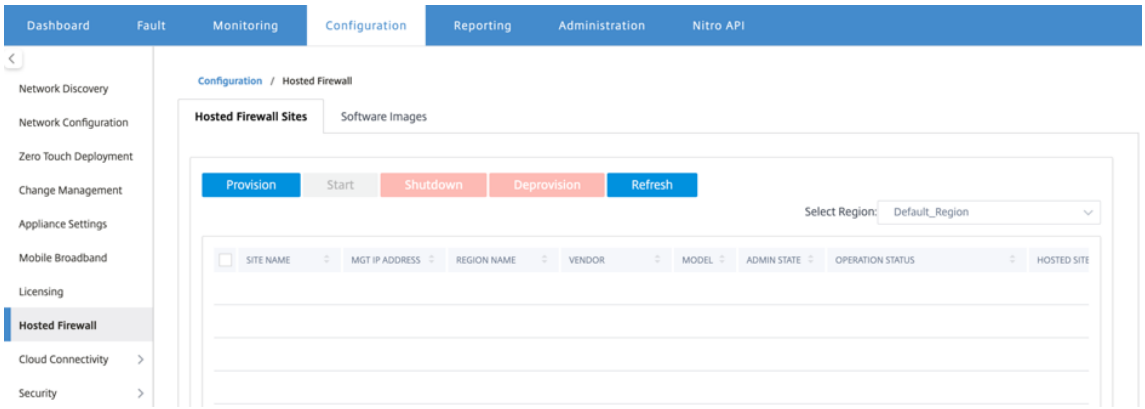


> **Hinweis:**
>
> Speicher ist von einer sekundären Partition reserviert, die aktiv ist, wenn die Bedingung erfüllt

> 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.

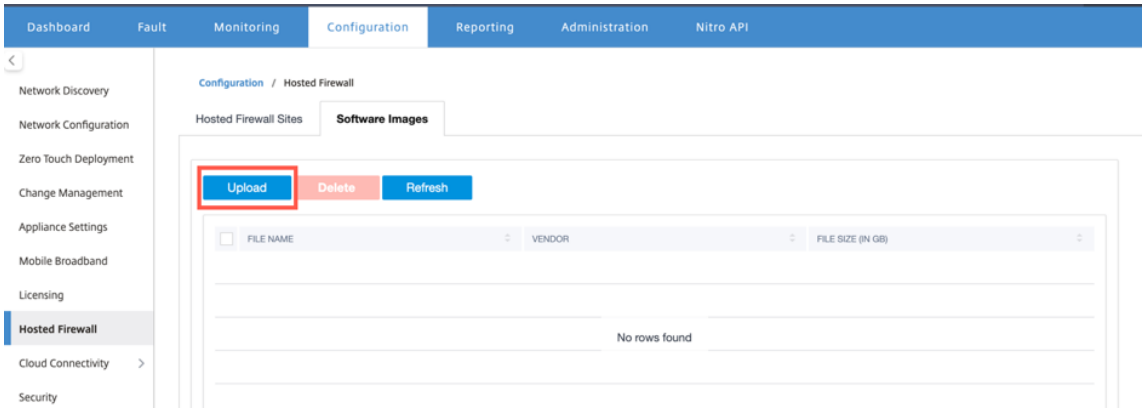


   Sie können die **Region** aus der Dropdownliste auswählen, um die bereitgestellten Site-Details für diese ausgewählte Region anzuzeigen.

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**.



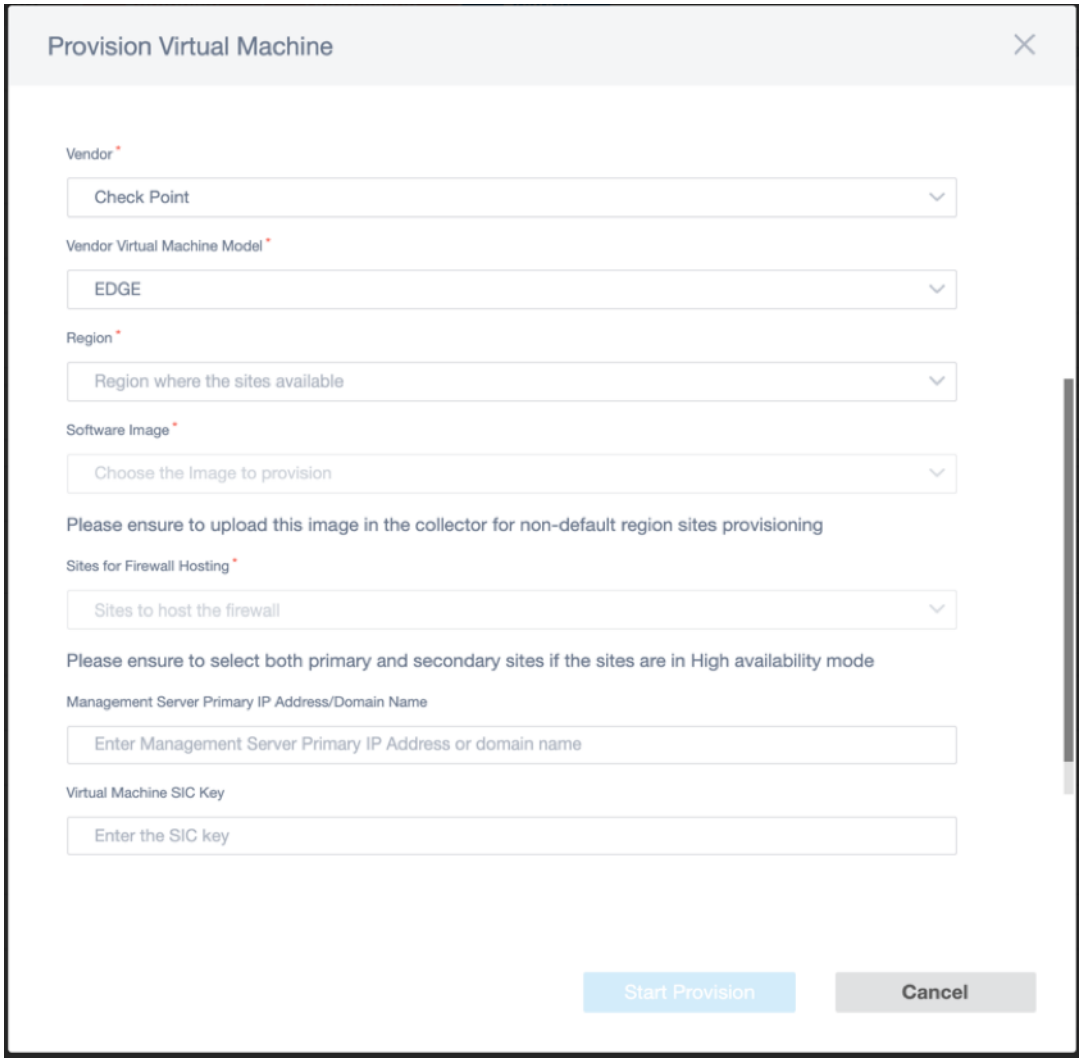
3. Wählen Sie in der Dropdownliste den Namen des Anbieters als **Check Point** aus. Klicken oder legen Sie die Softwareimage-Datei in das Feld für den Upload ab.

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 die Option **Aktualisieren**, um die neuesten Imagedateidetails zu erhalten.
- **Löschen**: Klicken Sie auf die Option **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**.

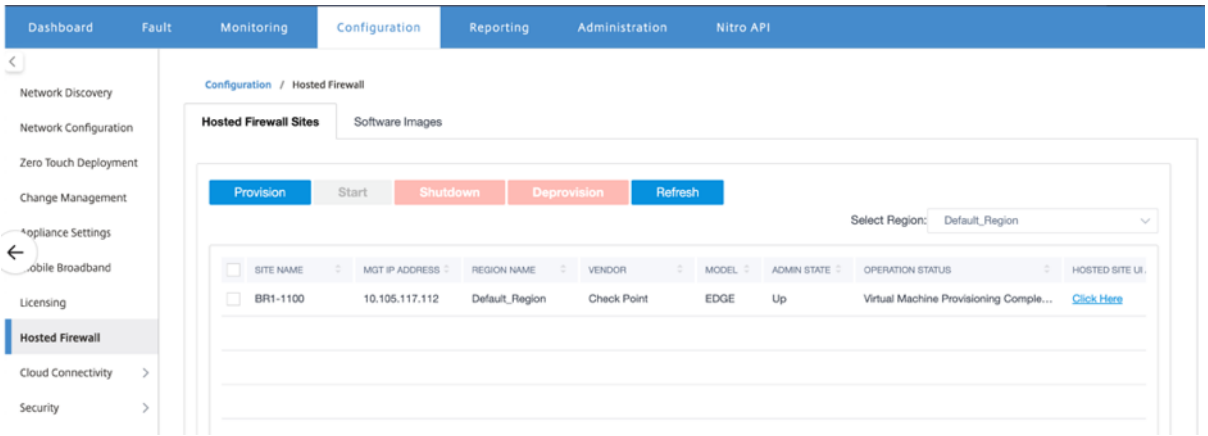


- **Anbieter**: Wählen Sie den Namen des Anbieters als **Check Point** aus der Dropdownliste aus.
- **Vendor Virtual Machine Model**: Das Feld "VM-Modell"wird automatisch als Edge gefüllt.
- **Region**: Wählen Sie den Teilsektor aus der Liste aus.
- **Software-Image**: Wählen Sie die zu bereitzustellende 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 Domänennamen 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.
- **Management-IP**: Zeigt die Management-IP-Adresse der Site 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

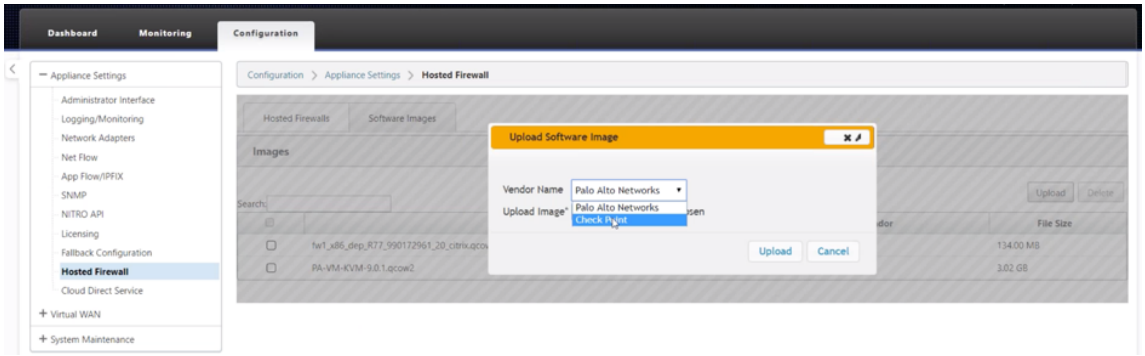
Bereitstellung virtueller Maschinen durch die Benutzeroberfläche der SD-WAN-Appliance

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 in der Citrix SD-WAN GUI zu **Konfiguration > Appliance-Einstellungen** wählen Sie **Gehostete Firewall** aus.

2. Laden Sie das Softwareimage hoch:

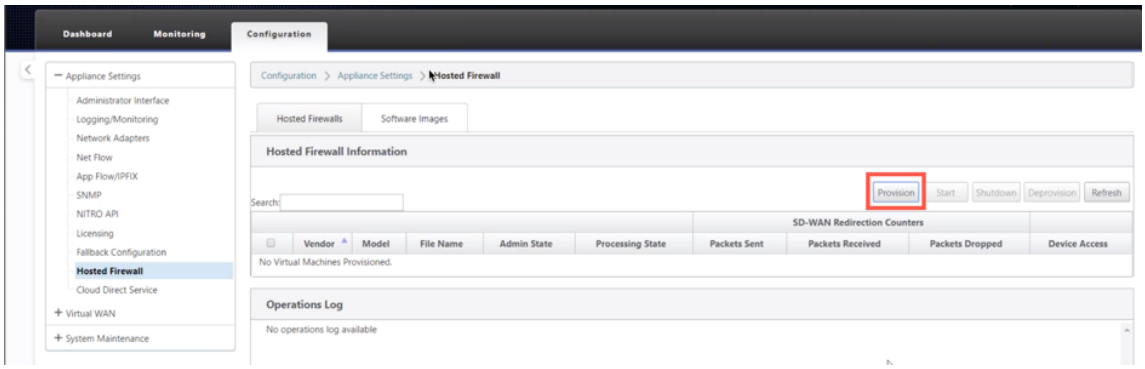
   - Wählen Sie die Registerkarte **Software-Images**. Wählen Sie den **Namen des Anbieters** als Kontrollpunkt aus.
   - Wählen Sie die Softwareimagedatei aus.
   - Klicken Sie auf **Upload**.



> **Hinweis:**
>
> Es können maximal zwei Images hochgeladen werden. Das Hochladen des Images der Check Point virtuellen Maschine kann je nach Bandbreitenverfügbarkeit länger dauern.

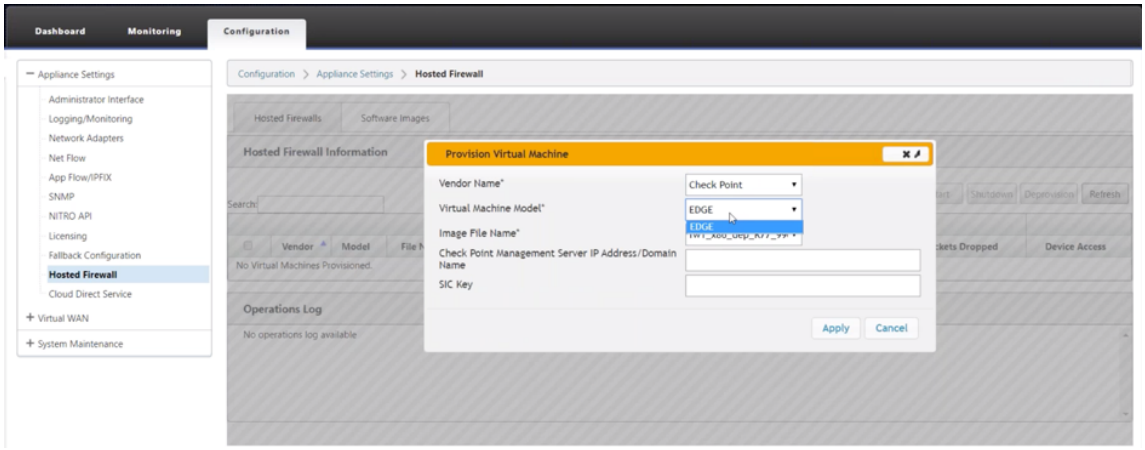
Sie können eine Statusleiste sehen, um den Upload-Prozess zu verfolgen. Das Dateidetail wird aktualisiert, sobald das Image erfolgreich hochgeladen wurde. Das Image, das für die Bereitstellung verwendet wird, kann nicht gelöscht werden. Führen Sie keine Aktion aus oder gehen Sie zurück zu einer anderen Seite, bis die Imagedatei 100% hochgeladen zeigt.

3. Wählen Sie für die Bereitstellung die Registerkarte **Gehostete Firewall** aus > klicken Sie auf die Schaltfläche **Bereitstellung**.

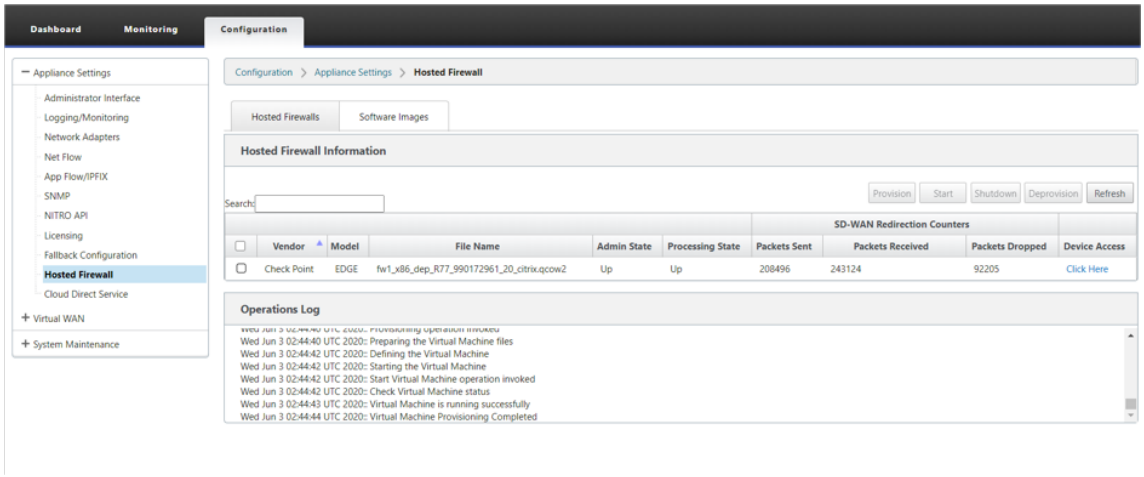


4. Geben Sie die folgenden Details für die Provisioning.

   - **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 **Apply**.



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**: Datapath-Verarbeitungsstatus der virtuellen Maschine.
- **Paket gesendet**: Pakete, die von SD-WAN an die virtuelle Sicherheitsmaschine gesendet wurden.
- **Paket empfangen**: Pakete, die von SD-WAN von der virtuellen Sicherheitsmaschine empfangen wurden.
- **Paket verworfen**: Pakete, die von SD-WAN verworfen wurden (z. B. wenn die virtuelle Sicherheitsmaschine ausgefallen ist).
- **Gerätezugriff**: Klicken Sie auf den Link, um die 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).

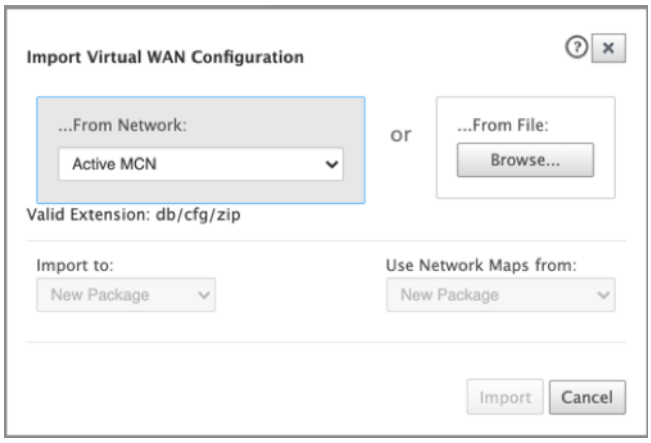
> **Hinweis: Verwenden Sie**
>
> immer den Inkognito-Modus, um auf die Checkpoint-GUI zuzugreifen.

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:

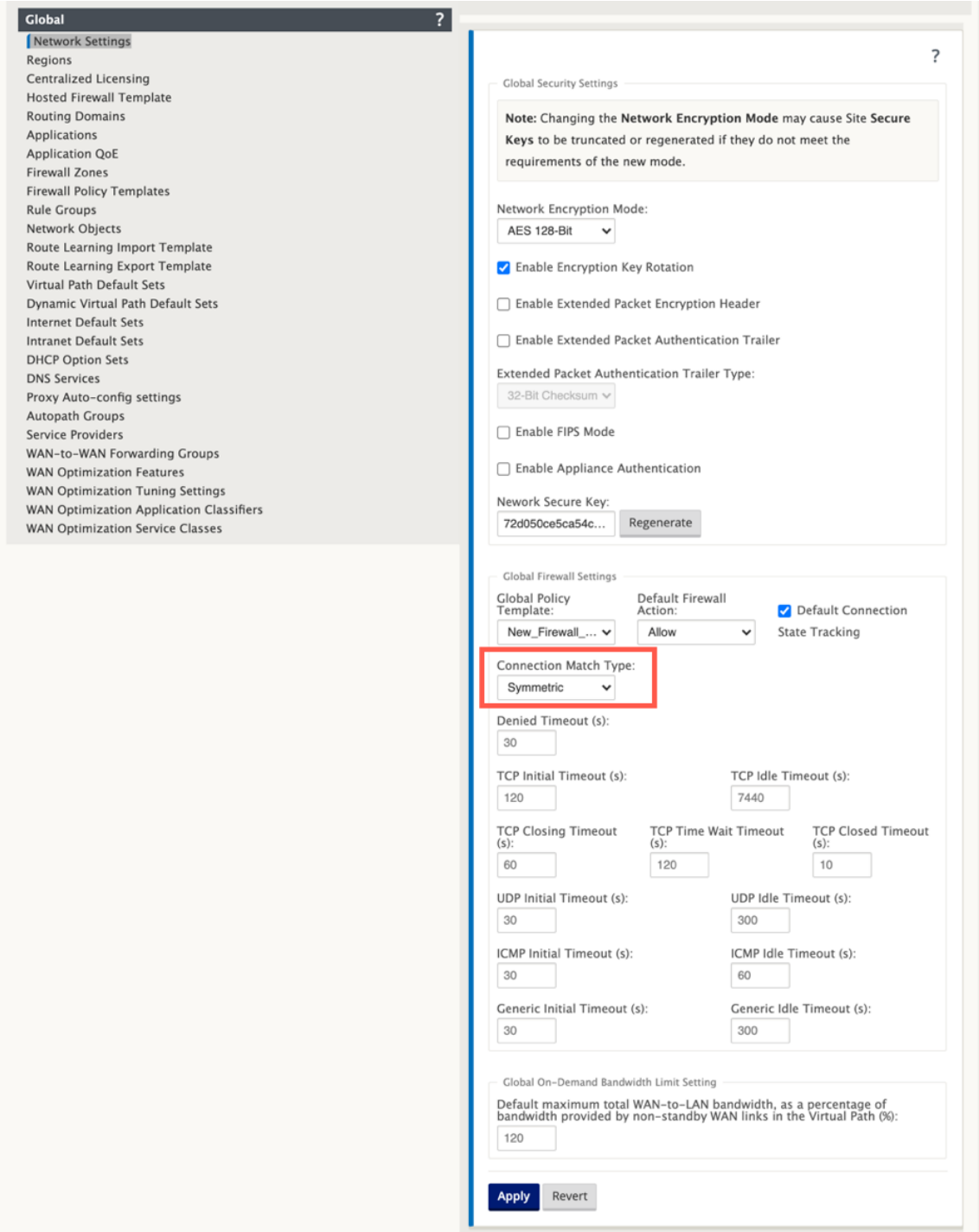
1. Öffnen Sie die Citrix SD-WAN Center-Benutzeroberfläche und navigieren Sie zu **Konfiguration > Netzwerkkonfigurationsimport**. Importieren Sie die virtuelle WAN-Konfiguration aus dem aktiven MCN und klicken Sie auf **Importieren**.



Die restlichen Schritte sind ähnlich wie folgt - die Konfiguration der Datenverkehrsumleitung über MCN.

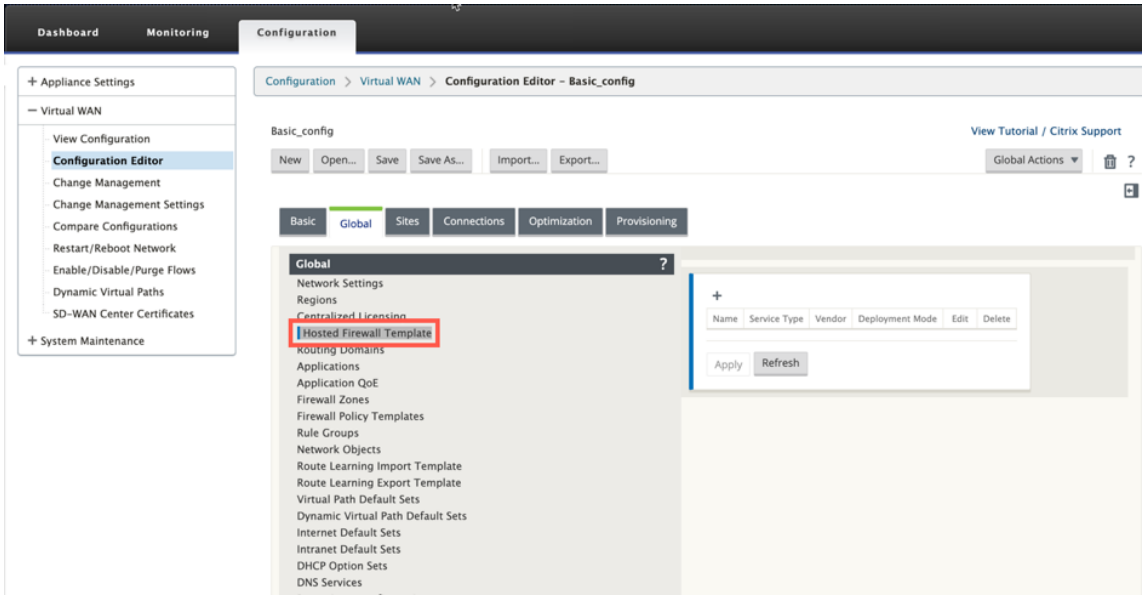
So navigieren Sie durch den Konfigurationseditor auf MCN:

1. Setzen Sie **Verbindungsanpassungstyp** unter **Global > Netzwerkeinstellungen** auf **Symmetrisch**.

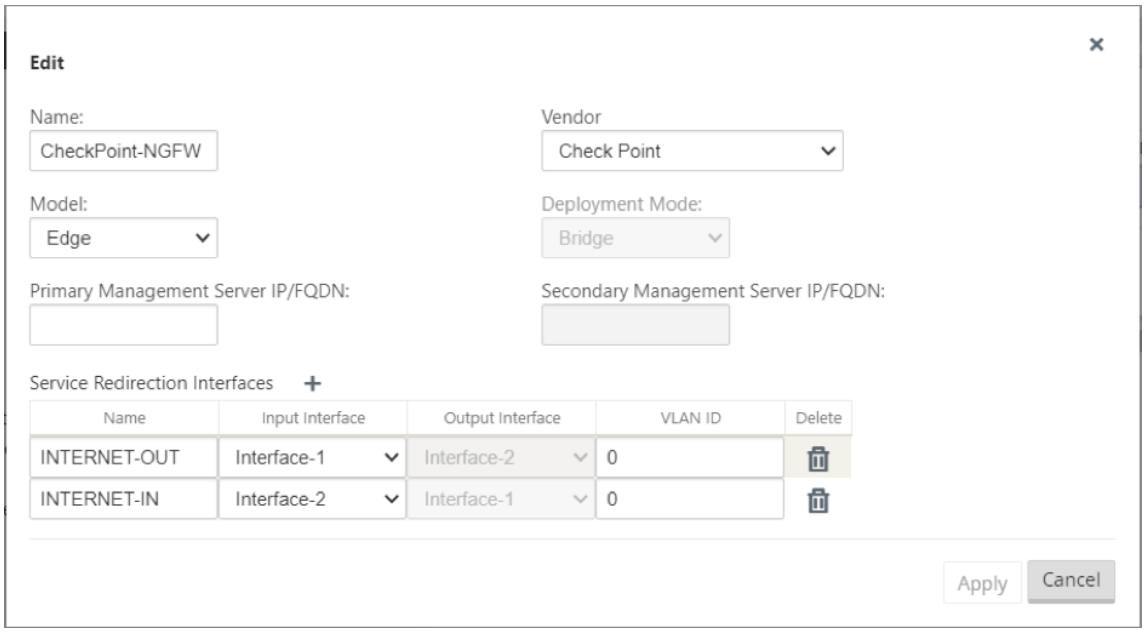


Standardmäßig sind SD-WAN-Firewallrichtlinien richtungsspezifisch. Der Match-Typ Symmetrisch entspricht den Verbindungen unter Verwendung der angegebenen Übereinstimmungskriterien und wendet die Richtlinienaktion auf beide Richtungen an

2. Öffnen Sie die Citrix SD-WAN UI, navigieren Sie zu **Konfiguration** erweitern Sie **Virtual WAN** wählen Sie **Konfigurationseditor** und wählen Sie **Hosted Firewall Template** im Abschnitt **Global**.



3. Klicken Sie auf **+** und geben Sie die erforderlichen Informationen an, die im folgenden Screenshot verfügbar sind, um die **Vorlage für gehostete Firewall**hinzuzufügen. Klicken Sie auf **Hinzufügen**.



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 Umleitungs-Eingabeschnittstelle 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.

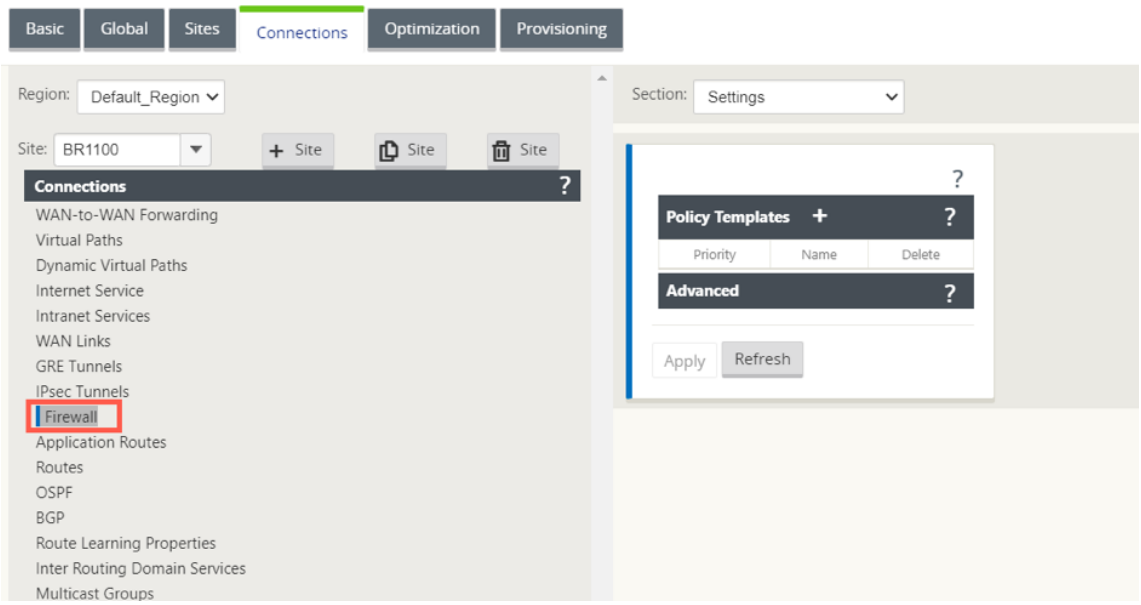
Der virtuellen Maschine Check Point sind nur zwei Datenschnittstellen zugewiesen.

> **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.

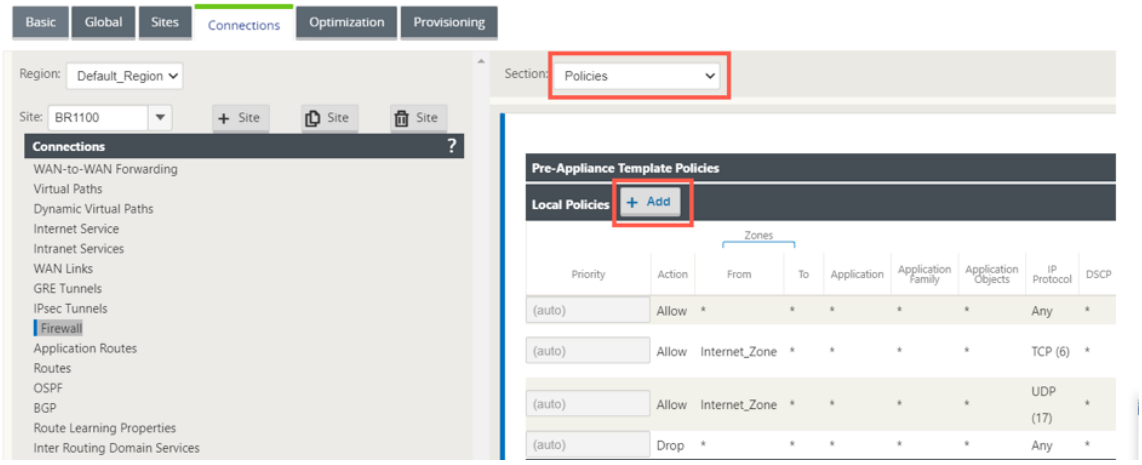
Die Umleitung des Datenverkehrs zur virtuellen Firewall-Maschine kann mithilfe von SD-WAN-Firewall-Richtlinien erfolgen. Es gibt zwei Methoden, um SD-WAN-Firewall-Richtlinien zu erstellen - entweder über Firewall-Richtlinienvorlagen im Abschnitt **Global** oder auf Site-Ebene.

Methode - 1

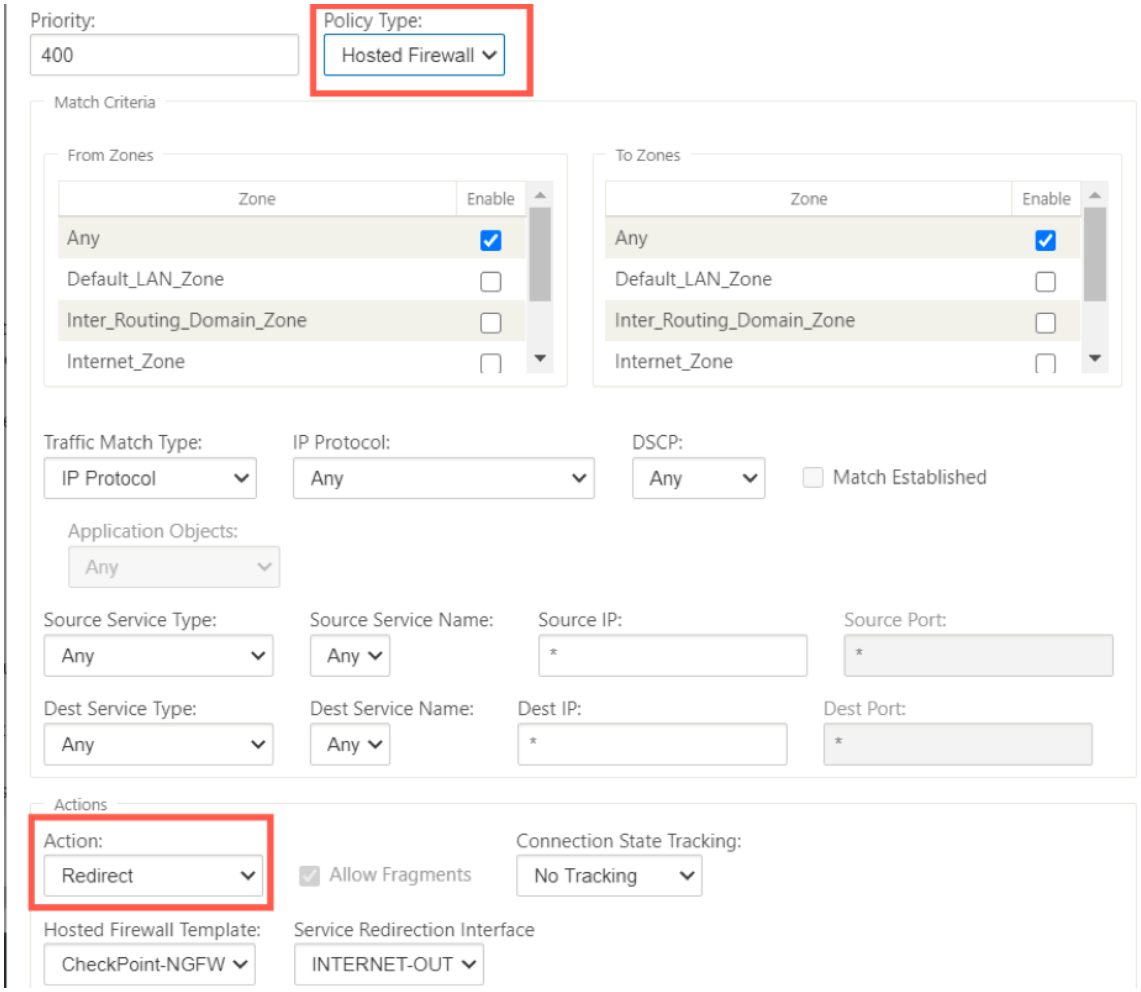
1. Navigieren Sie von Citrix SD-WAN GUI zu **Konfiguration** erweitern Sie **Virtual WAN > Konfigurationseditor**. Wählen Sie **Firewall** unter **Verbindungen**aus.



2. Wählen Sie **Richtlinien** aus der Dropdownliste **Abschnitt** aus und klicken Sie auf **+Hinzufügen**, um eine Firewall-Richtlinie zu erstellen.

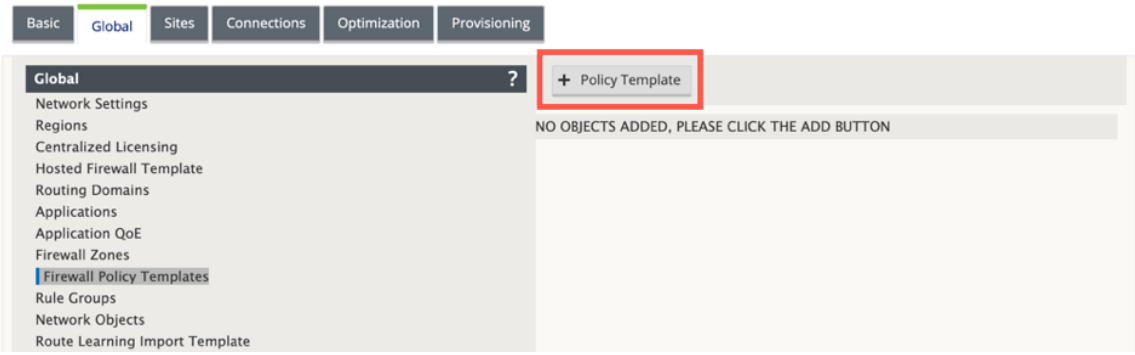


3. Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch auf Redirect gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdownliste aus. Klicken Sie auf **Hinzufügen**.

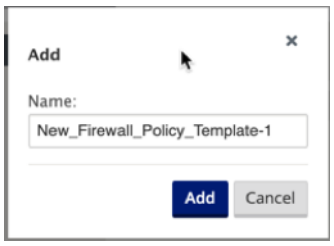


Methode - 2

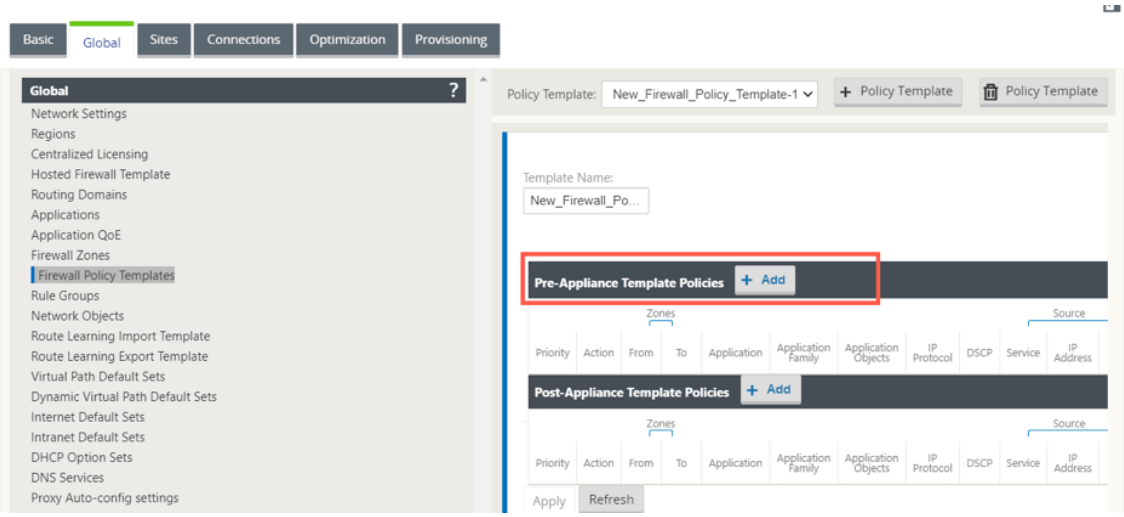
1. Navigieren Sie zur Registerkarte **Global** und wählen Sie **Firewall-Richtlinienvorlagen**aus Klicken Sie auf **+ Richtlinienvorlage**



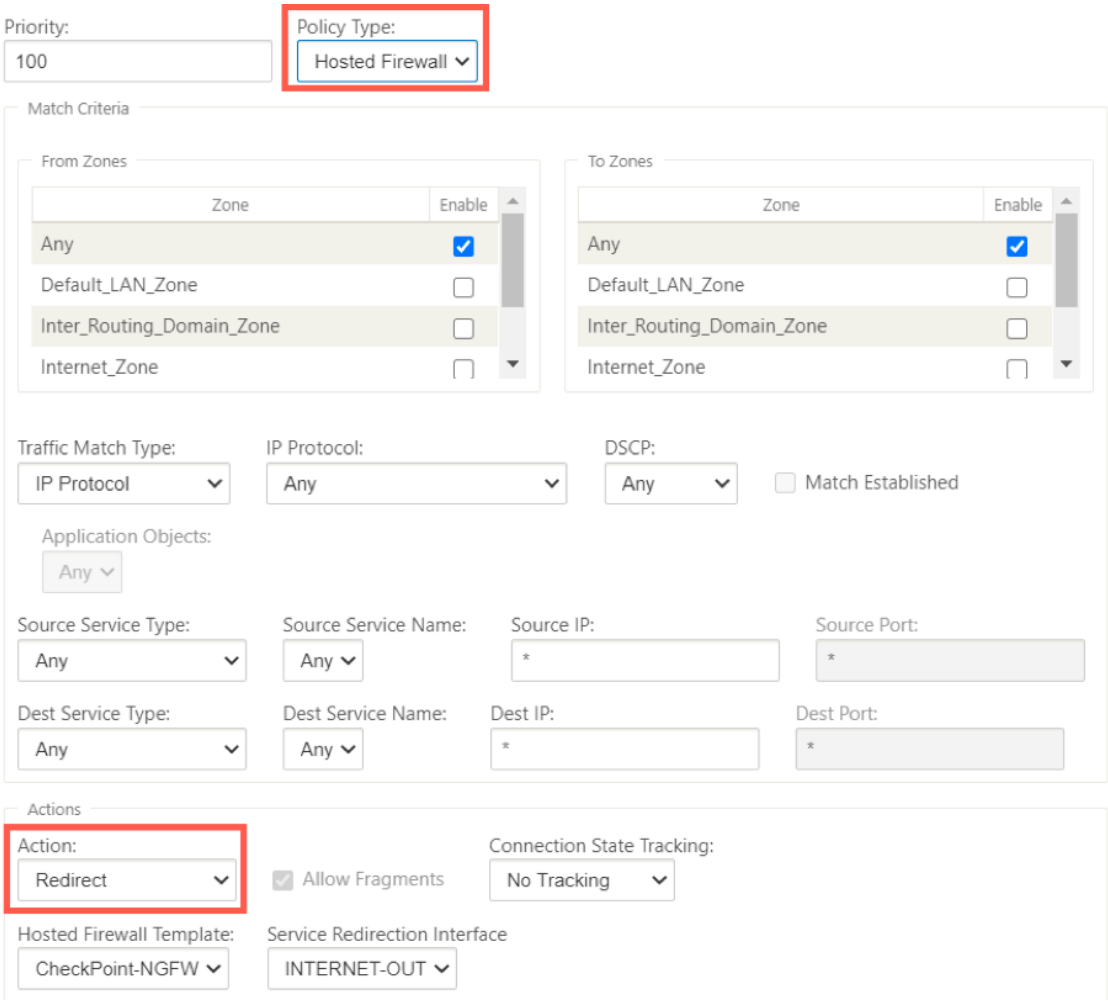
2. Geben Sie der Richtlinienvorlage einen Namen und klicken Sie auf **Hinzufügen**.



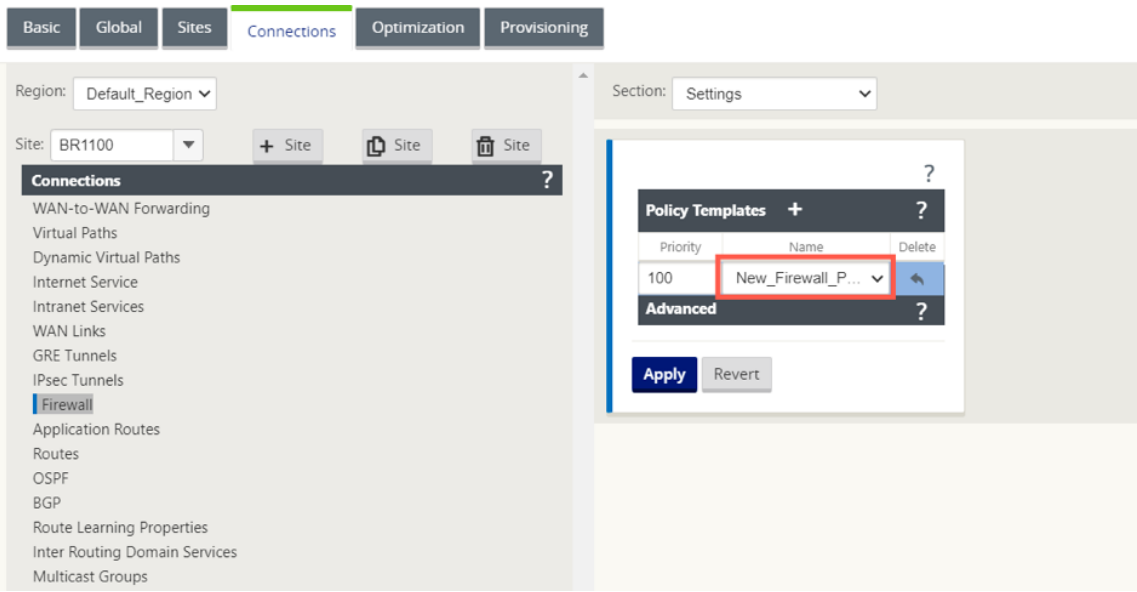
3. Klicken Sie auf **+ Hinzufügen** neben **Richtlinien für Pre-Appliance-Vorlagen**.



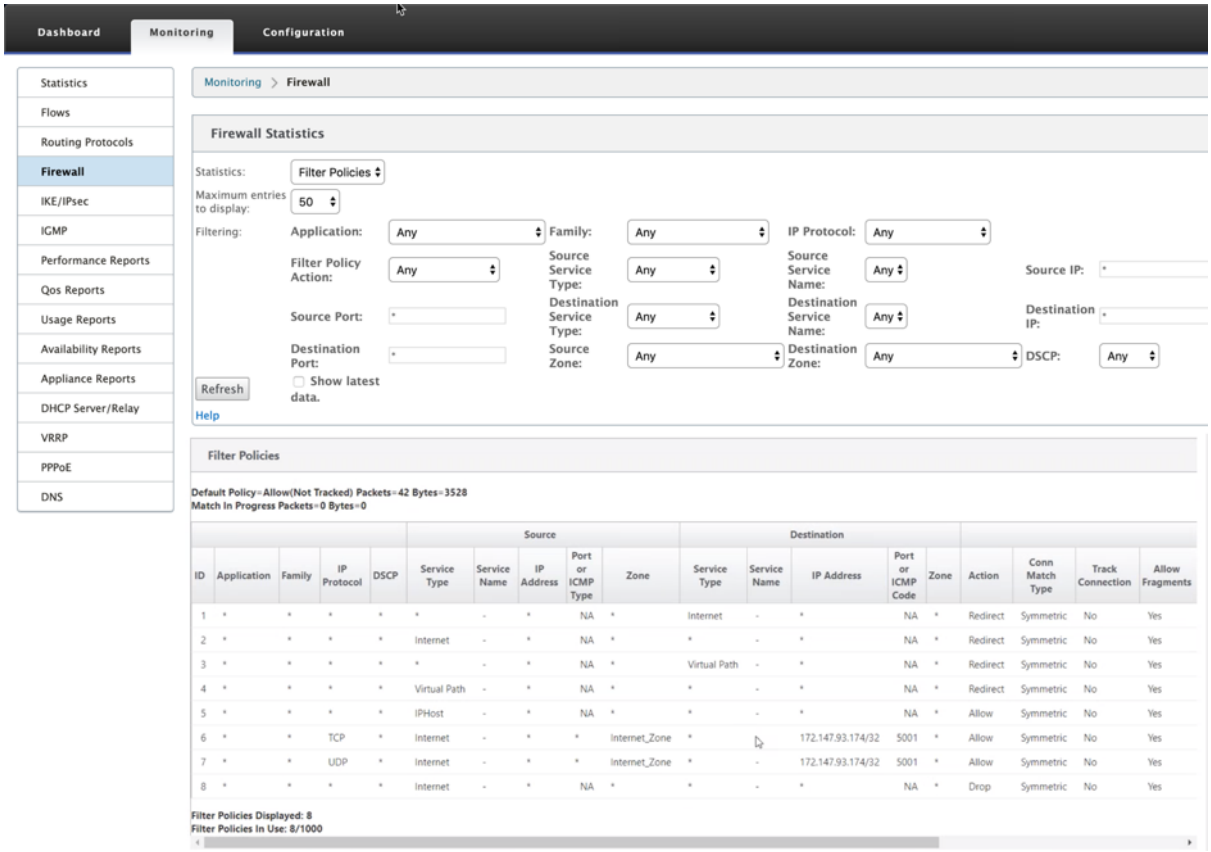
4. Ändern Sie den **Richtlinientyp** in **Hosted Firewall**. Das Feld **Aktion** wird automatisch mit **Redirect**gefüllt. Wählen Sie die **Vorlage Gehostete Firewall** und die **Schnittstelle für die Serviceumleitung** aus der Dropdownliste aus. Klicken Sie auf **Hinzufügen**.



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 **Apply**.



Während die gesamte Netzwerkkonfiguration ausgeführt wird, können Sie die Verbindung unter **Überwachung > Firewall** > unter **Statistikliste** überwachen und **Richtlinien filtern**.



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.

Zuvor wurde in LAG nur der Active-Backupmodus unterstützt. Ab Version 11.3 werden die protokollbasierten 802.3AD Link Aggregation Control Protocol-Verhandlungen (LACP) unterstützt. Das LACP ist ein Standardprotokoll und bietet mehr Funktionalität für LAGs.

Im Active-Backupmodus ist zu jeder Zeit 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.

Mit dem LACP können Sie den Datenverkehr gleichzeitig durch alle Ports senden. Als Vorteil erhalten

Sie mehr Bandbreite zusammen mit dem Link-Redundanz-Mechanismus. Die LACP-Implementierung unterstützt den **Active-Active-Modus**. Jetzt mit dem Active-Backupmodus haben Sie auch die Möglichkeit, den vollständigen LACP-Active-Active-Modus aus der SD-WAN-Benutzeroberfläche auszuwählen.

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.

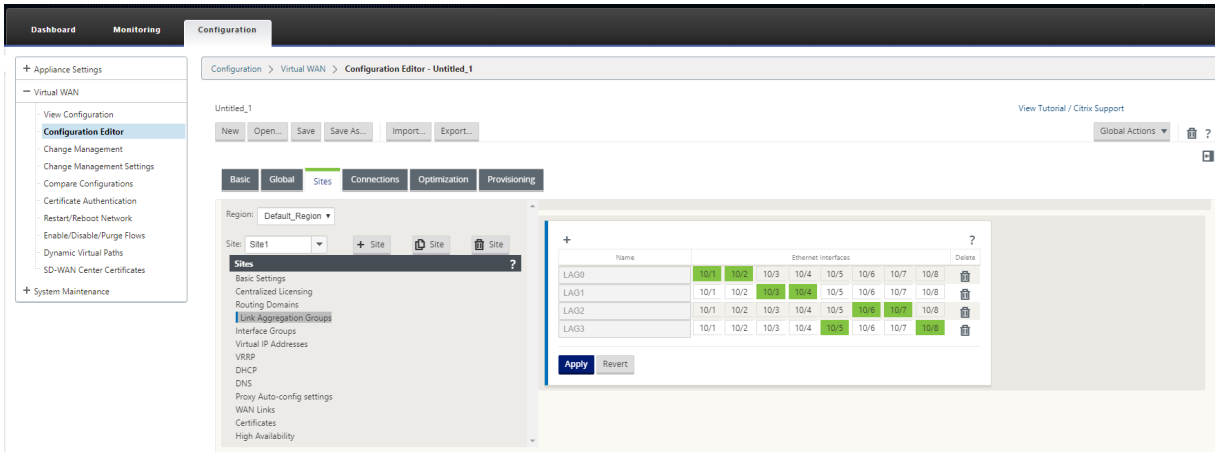
Einschränkungen

- Sie können maximal vier LAGs mit maximal vier Ports erstellen, die in jeder LAG auf den Citrix SD-WAN-Appliances gruppiert sind.
- Die Optionen für Portpriorität und Systempriorität werden bei der LACP-Implementierung nicht unterstützt.

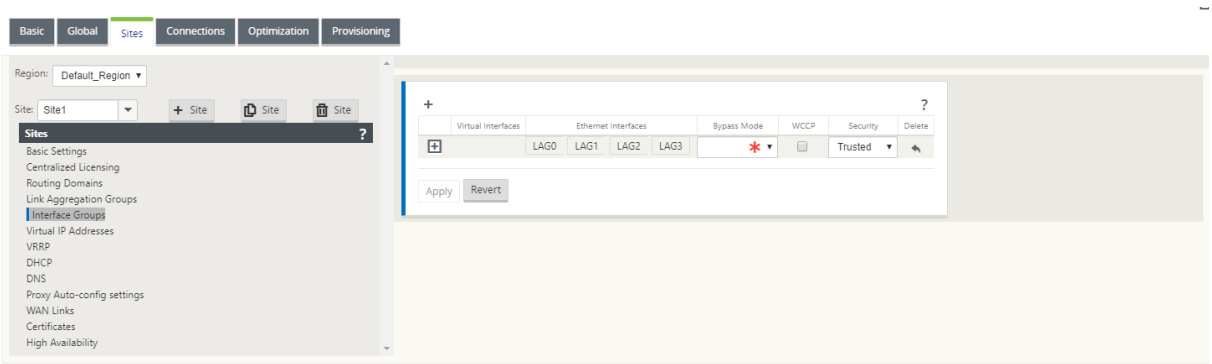
Mit Version 11.3 befinden sich die Ports in SD-WAN mit der LACP-Implementierung immer im aktiven Modus. Das bedeutet, dass SD-WAN immer mit den Verhandlungen beginnen kann.

> **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 Mitglied-sports sehen.

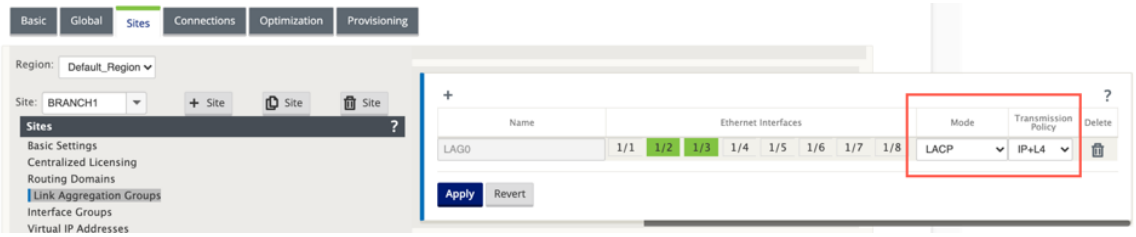


Ebenso, wenn Sie die LAGs mit LACP-Modus konfigurieren möchten:

1. Klicken Sie auf **+**, um eine LAG zu erstellen und die Ethernet-Schnittstellenports auszuwählen.
2. Wählen Sie in der Dropdownliste den Konfigurationsmodus als **LACP** aus
3. Wählen Sie die **Übertragungsrichtlinie** aus der Dropdownliste aus.

   > **HINWEIS**
   >
   > Wenn der Modus als **Active-Backup**ausgewählt ist, wird das Feld **Übertragungsrichtlinie** deaktiviert.

4. Klicken Sie auf **Apply**.



Da LAG-Gruppen viele Ports haben, hilft die **Übertragungsrichtlinie** bei der Auswahl des Ports, der zum Senden von Datenverkehr verwendet werden kann. Das Feld "Übertragungsrichtlinie"kann nur aktiviert werden, wenn der Aggregationsmodus **Aktiv-Aktiv**ist. Es sind zwei Übertragungsrichtlinien definiert: MAC+IP und IP+L4.

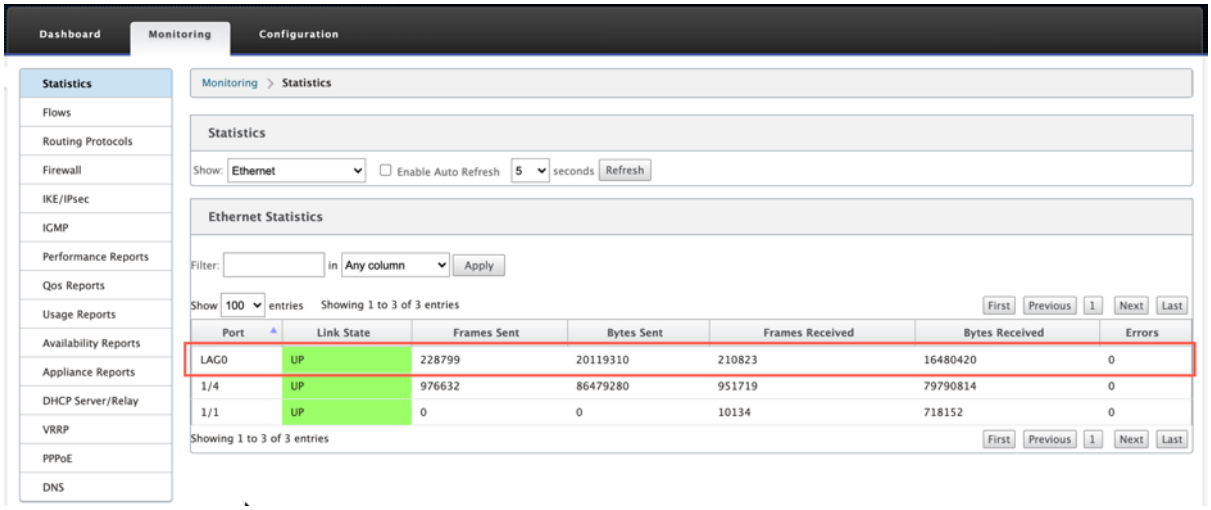
- **MAC+IP**: Die Linkauswahl für ein bestimmtes Paket basiert auf den Layer-2- und 3-Parametern. Die Quell- und Ziel-MAC- und IP-Adressen nehmen diese Parameter und hashen sie. Laut Hash wählt es den Port aus.
- **IP+L4**: Die IP+L4-Richtlinie basiert auf den Quell- und Ziel-IP- und Layer-4-Ports und dem Protokoll. Die IP+L4-Richtlinie benachrichtigt, welches Paket welchen Port durchläuft.
  Paket mit den gleichen Parametern wird immer über einen der Links gesendet. Das bedeutet, dass derselbe oder einzelne Flow (derselbe Quell- und Ziel-Mac und IP) immer über dieselben Ports läuft und sich nicht auf die anderen Ports verteilt. Als Vorteil können die nicht in Ordnung bestellten Pakete das Zielgerät nicht erreichen

Sie können virtuelle Schnittstellen mit LAGs erstellen und diese Schnittstellen werden weiter verwendet, um LAN/WAN-Verbindungen und HA zu konfigurieren.

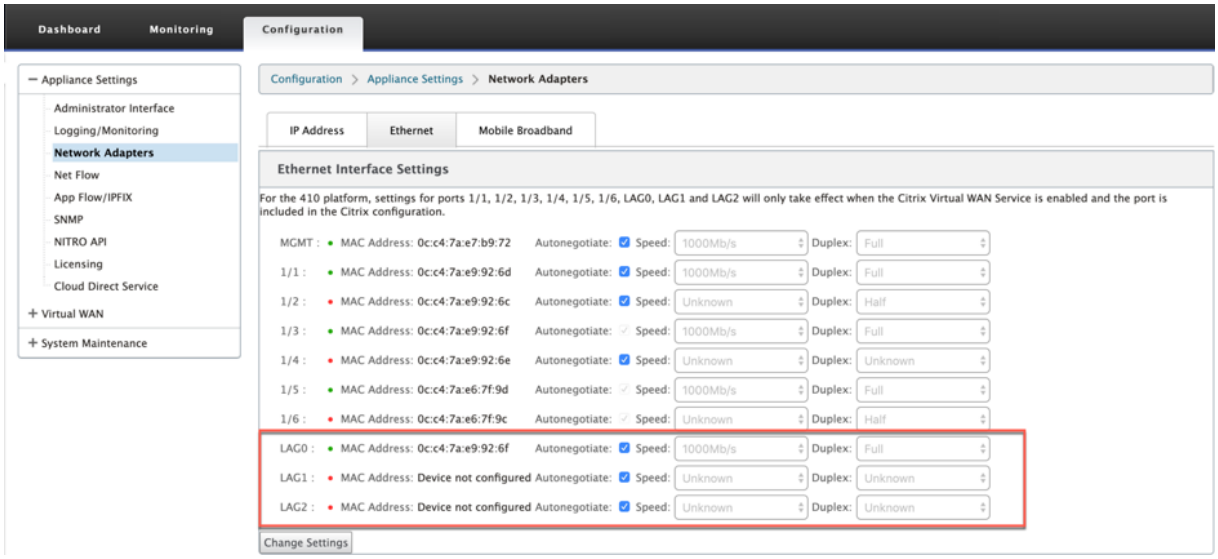
> **Hinweis**
>
> Die Funktion Link State Propagation (LSP) wird nicht unterstützt, wenn LAGs als Ethernet-Schnittstellen in Schnittstellengruppen verwendet werden.

Überwachung und Fehlerbehebung

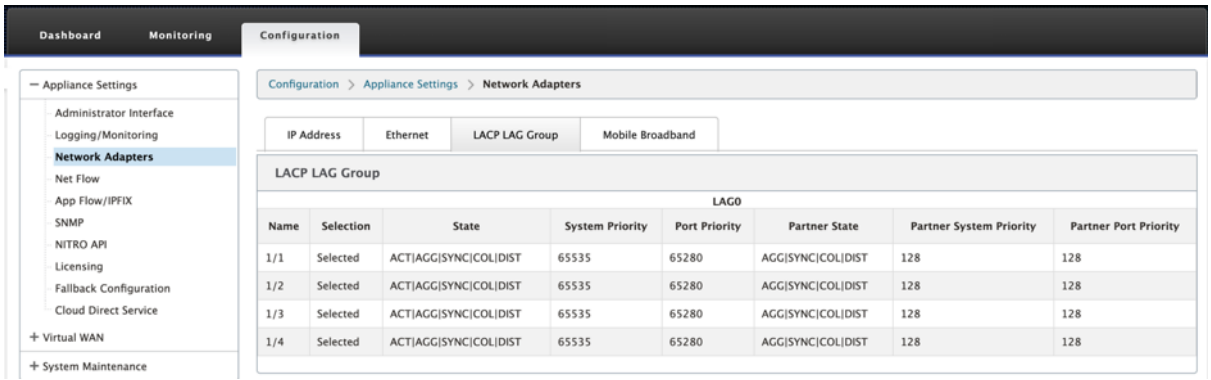
Um die Statistiken oder den Linkstatus anzuzeigen, navigieren Sie zu **Überwachung > Statistiken**. Wählen Sie **Ethernet** aus der Dropdownliste **Anzeigen** aus.



Um die aktiven und Standby-LAG-Ports anzuzeigen, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Netzwerkadapter** > **Ethernet**.

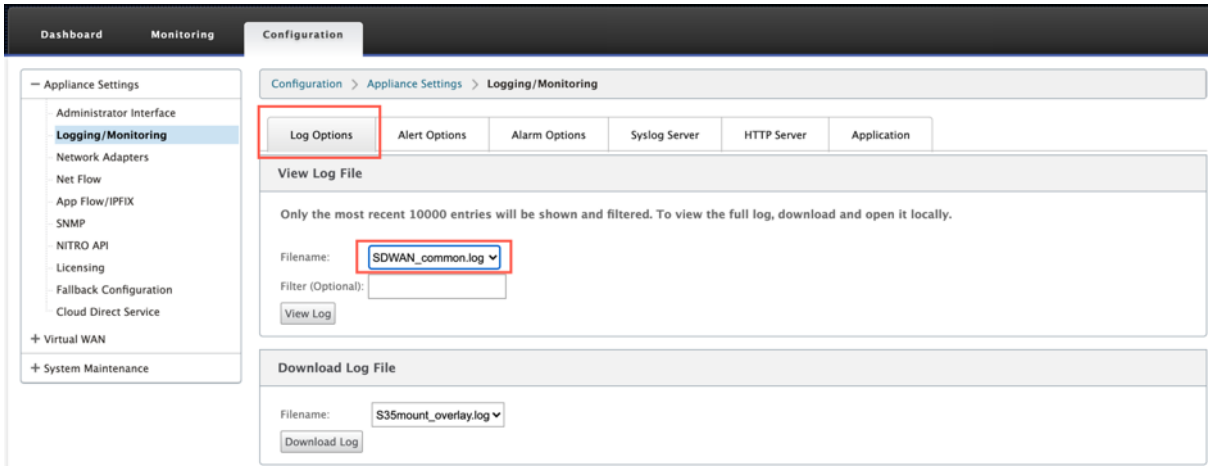


Wählen Sie die Registerkarte **LACP LAG Group**, um die verschiedenen Details zur LACP LAG-Gruppe anzuzeigen.



> **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.

Sie können die Protokolldateien zur weiteren Fehlerbehebung herunterladen. Navigieren Sie zu **Konfiguration > Logging/Monitoring** und wählen Sie auf der Registerkarte **Log-Optionen** die Option **SDWAN_common.log** aus.



Verknüpfen Zustandspropagierung

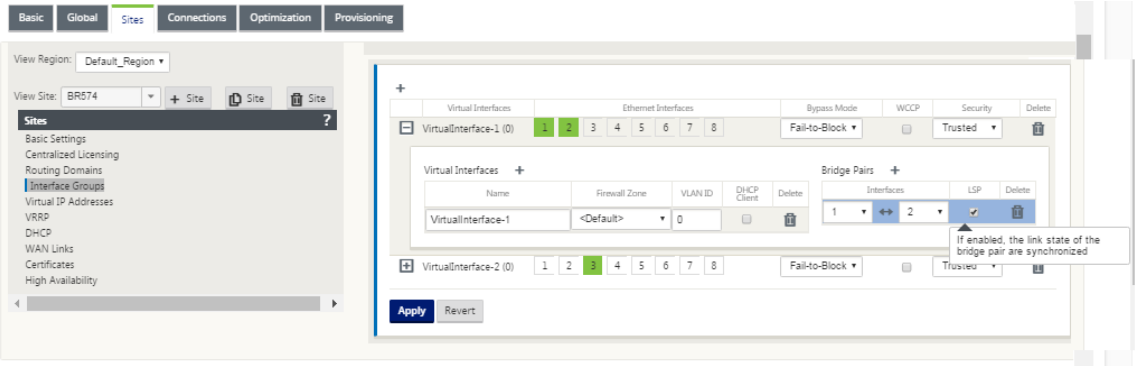
October 28, 2021

Die Funktion Link-Statuspropagierung (LSP) ermöglicht es Netzwerkadministratoren, den Linkstatus eines Bypass-Paares zu synchronisieren, um das Anhängen zu ermöglichen -Geräte auf der anderen Seite des Links, um anzuzeigen, wann Links inaktiv sind. Wenn ein Port eines Bypass-Paares inaktiv wird, wird die gekoppelte Verbindung administrativ deaktiviert. Wenn Ihre Netzwerkarchitektur ein paralleles Failovernetzwerk enthält, zwingt dies den Datenverkehr, auf dieses Netzwerk zu Sobald der unterbrochene Link wiederhergestellt ist, wird der entsprechende Link automatisch aktiv.

So konfigurieren Sie die Weitergabe des Verbindungsstatus

So konfigurieren Sie die Hyperlinkstatuspropagierung:

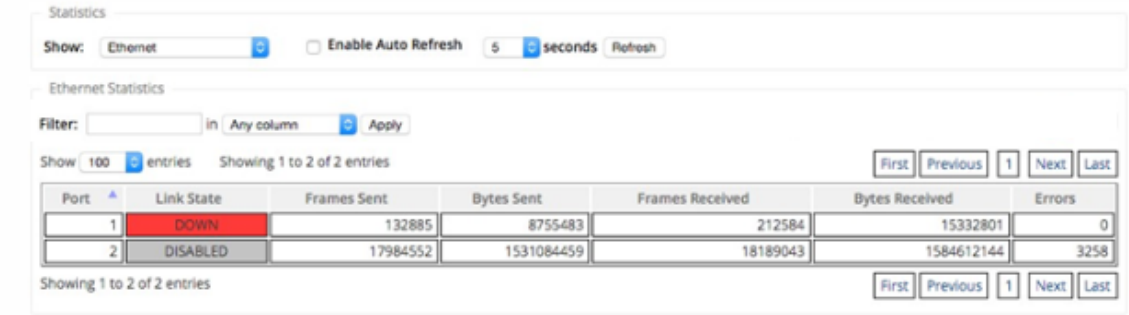
1. Navigieren Sie zu **Konfigurationseditor** > **Standorte** > **[Site-Name]** > **Schnittstellengruppen**.
2. Erweitern Sie **Virtuelle Schnittstellen** und klicken Sie unter **Bridge-Paare**auf das Kontrollkästchen **LSP**, um die **Verbindungsstatusausbreitung** für ein Bridge-Paar zu aktivieren. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.



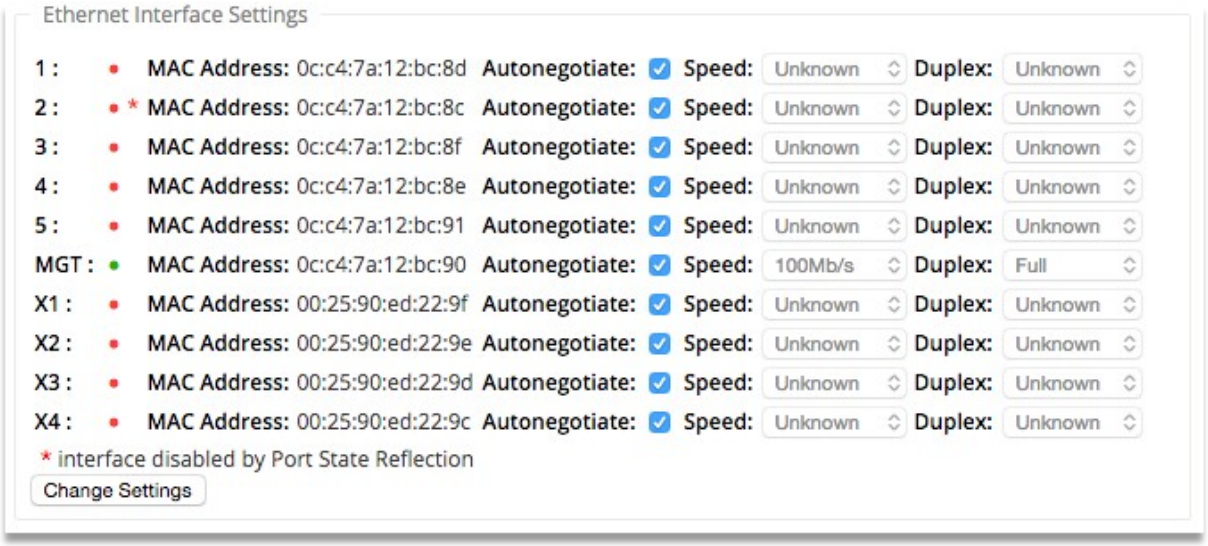
Überwachung von Linkstatistiken

So überwachen Sie Linkstatistiken:

1. Wählen Sie auf der Seite **Monitor > Statistiken** im Dropdownmenü **Anzeigen** die Option **Ethernet aus**, um den Status des Bypass-Portpaars mit aktivierter Verbindungsstatus-Propagierung anzuzeigen. Beachten Sie, dass die LAN-Seiten-Verbindung ausgefallen ist und später die WAN-Seiten-Verbindung des Bypass-Paares administrativ DEAKTIVIERT ist.



2. Navigieren Sie zur Registerkarte **Konfiguration > Einheiteneinstellungen** > **Netzwerkadapter > Ethernet**. Die administrativ ausgefallenen Ports sind in der Liste **Ethernet-Schnittstelleneinstellungen** durch ein rotes Sternchen (*) gekennzeichnet.



Mess- und Standby-WAN-Verbindungen

October 28, 2021

Citrix SD-WAN unterstützt das Aktivieren von gemessenen Verbindungen, die so konfiguriert werden können, dass Benutzerverkehr nur auf einer bestimmten Internet-WAN-Verbindung übertragen wird, wenn alle anderen verfügbaren WAN-Links deaktiviert sind.

Metered Links sparen Bandbreite bei 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. Set Last Resort ist normalerweise aktiviert, wenn drei WAN-Verbindungen zu einem Standort vorhanden sind (dh MPLS, Breitband-Internet, 4G/LTE) und eine der WAN-Verbindungen 4G/LTE ist und für ein Unternehmen möglicherweise zu kostspielig ist, um die Nutzung zuzulassen, sofern dies nicht erforderlich ist. 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:

- Datenmaximum
- Abrechnungszeitraum (wöchentlich/monatlich)
- Start-Datum
- 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 mindestens ein

Heartbeat-Intervall lang kein Datenverkehr (Benutzer/Steuerung) auf dem Pfad stattgefunden hat

Bei einem lokalen getakteten Link zeigt das Dashboard einer Appliance unten eine **WAN-Link-Metering-Tabelle** mit Messinformationen an.

Die Bandbreitennutzung auf einer lokalen gemessenen Verbindung wird anhand der konfigurierten Datenobergrenze 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 ein Pfad zwischen zwei gemessenen Verbindungen gebildet wird, ist das aktive Heartbeat-Intervall, das auf dem gemessenen Pfad verwendet wird, das größere der beiden konfigurierten aktiven Heartbeat-Intervalle auf den Verbindungen.

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

- Auf**Anforderung**: 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:

  - eine Standby-Verbindung mit Priorität 1 wird zuerst aktiv, während eine Standby-Verbindung mit Priorität 3 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.

- **On-Demand** - 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
  - eine On-Demand-Standby-Verbindung und eine Standby-Verbindung der letzten Instanz
  - 2 Standby-Links der letzten Instanz

Die auf einem Standby-Pfad verwendeten Heartbeat-Intervalle werden wie folgt bestimmt:

- Wenn der Standby-Heartbeat bei mindestens einer der 2 Verbindungen deaktiviert ist, wird der Heartbeat auf dem Standby-Pfad deaktiviert, während er inaktiv ist.
- Wenn der Standby-Heartbeat bei keiner Verbindung deaktiviert ist, wird der größere der beiden Werte verwendet, wenn der Standby-Pfad Standby ist.
- Wenn aktives Heartbeat-Intervall für beide Verbindungen konfiguriert ist, wird der größere der beiden Werte verwendet, wenn der Standby-Pfad aktiv ist.

Heartbeat (Keep-Alive-Meldungen):

- Auf einem Nicht-Standby-Pfad werden Heartbeat-Nachrichten nur gesendet, wenn für mindestens ein Heartbeat-Intervall kein Verkehr (Steuerung oder Benutzer) vorhanden war. Das Heartbeat-Intervall variiert je nach Pfadstatus. Für **nicht standbybezogene, nicht dosierte** Pfade:
  - 50 ms wenn der Pfadstatus GOOD ist
  - 25 ms wenn der Pfadstatus 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 Pfadstatus BAD ist.
- Während aktiv, wie Nicht-Standby-Pfade, werden Heartbeat-Nachrichten nur gesendet, wenn für mindestens das konfigurierte aktive Heartbeat-Intervall kein Verkehr (Steuerung oder Benutzer) vorhanden war.
- das konfigurierte Standby-Heartbeat-Intervall wird verwendet, wenn der Pfadstatus GOOD ist.
- 1/2 das konfigurierte Standby-Heartbeat-Intervall wird verwendet, wenn der Pfadstatus BAD ist.

Während sie inaktiv sind, sind Standby-Pfade nicht für Benutzerverkehr berechtigt. Die einzigen Steuerprotokollnachrichten, 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 Benutzerverkehr mit zusätzlichen Zeitkosten berechtigt. Dies geschieht, damit die Nicht-Standby-Pfade, falls verfügbar, bei der Auswahl des Weiterleitungspfads bevorzugt werden.

Der Pfadstatus eines Standby-Pfads mit deaktiviertem Heartbeat wird, obwohl er inaktiv ist, als GOOD angenommen und in der Tabelle Pfadstatistiken unter **Überwachung**als GOOD angezeigt. Wenn es aktiv wird, beginnt er im Gegensatz zu einem Nicht-Standby-Pfad, der im Zustand DEAD beginnt, bis er von seinem virtuellen Pfad-Peer hört, im Zustand GOOD. Wenn keine Konnektivität 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 Pfadstatus nicht sofort zu (angenommen) GOOD. Stattdessen wird es für die Zeit im DEAD-Status gehalten, sodass es nicht sofort verwendet werden kann. Dies soll verhindern, dass die Aktivität zwischen einer Pfadgruppe mit niedrigerer Priorität mit angenommenen guten DEAD Pfaden und einer Pfadgruppe mit höherer Priorität mit Pfaden, die tatsächlich den Status GOOD haben, oszilliert. Diese Haltezeit (NO_HB_PATH_ON_HOLD_PERIOD_MS) ist auf 5 min festgelegt und kann über t2_variablen 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).

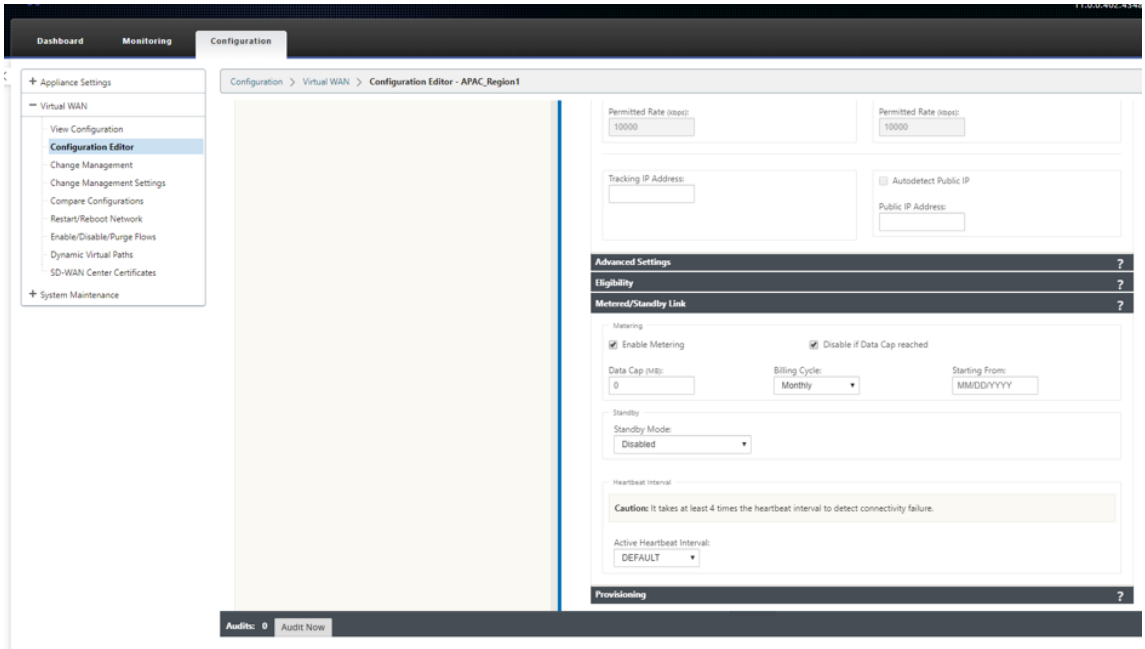
Ereignisse und Protokollmeldungen werden generiert, wenn ein Standby-Pfad zwischen Standby und Aktiv wechselt.

Konfigurationsvoraussetzungen:

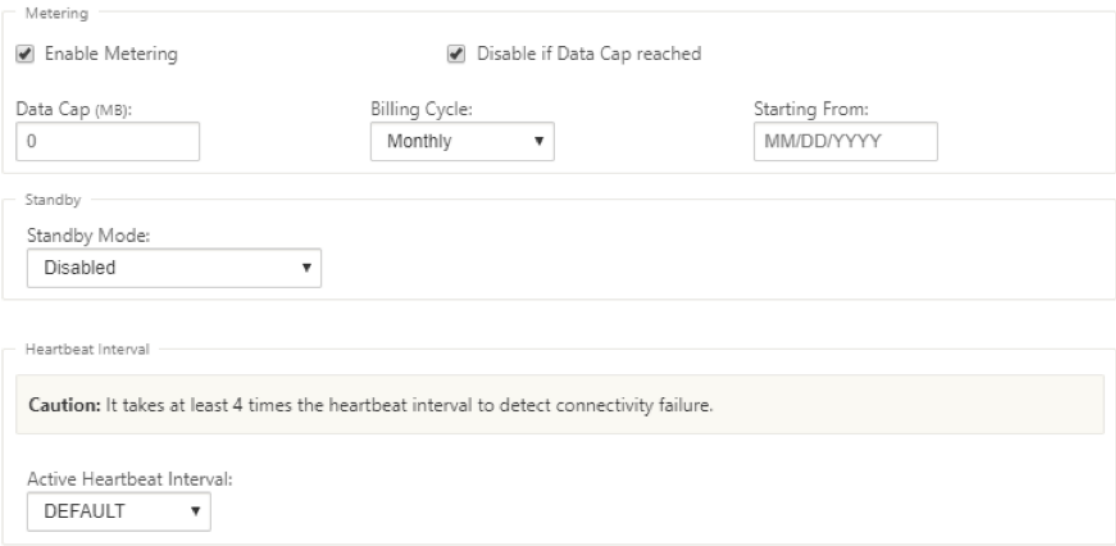
- Eine Zählerverbindung kann von jedem Zugriffstyp sein.
- Alle Links an einem Standort können mit aktivierter Messung konfiguriert werden.
- Ein Standby-Link kann vom Zugriffstyp “Public Internet”oder “Private Intranet”sein. Eine WAN-Verbindung vom Privaten MPLS-Zugriffstyp kann nicht als Standby-Verbindung 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 auf On-Demand-Standby-Verbindungen konfiguriert. On-Demand-Standby-Links unterstützen nur den Virtual Path Service.
- Der Internetdienst kann auf einer Standby-Verbindung der letzten Instanz konfiguriert werden, es wird jedoch nur der Lastausgleichsmodus unterstützt.
- Der Intranetdienst kann auf einer Standby-Verbindung der letzten Instanz konfiguriert werden, aber nur der sekundäre Modus wird 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 Dropdownliste 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.

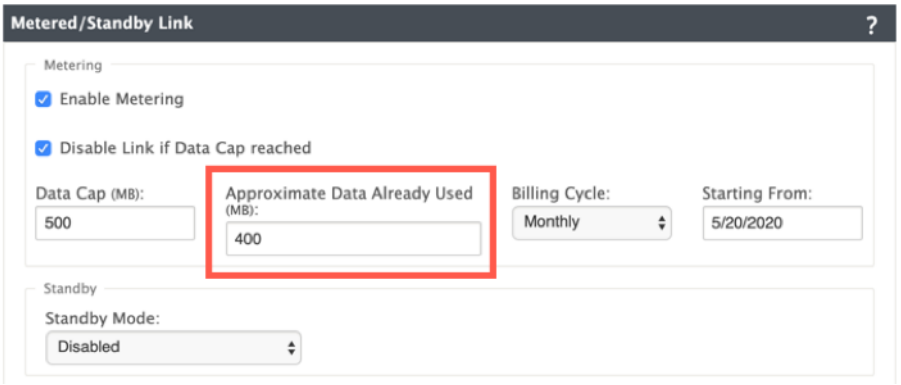


3. Link deaktivieren, wenn die Datenobergrenze erreicht ist:

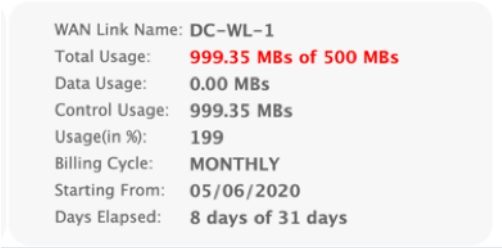
   - Wenn das Kontrollkästchen **Link deaktivieren, wenn Data Cap erreicht** ist aktiviert ist, werden der gemessene Link und alle zugehörigen Pfade bis zum nächsten Abrechnungszyklus deaktiviert, wenn die Datennutzung die Datenobergrenze erreicht.
   - Standardmäßig ist das Kontrollkästchen **Link deaktivieren, 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 nächsten 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.

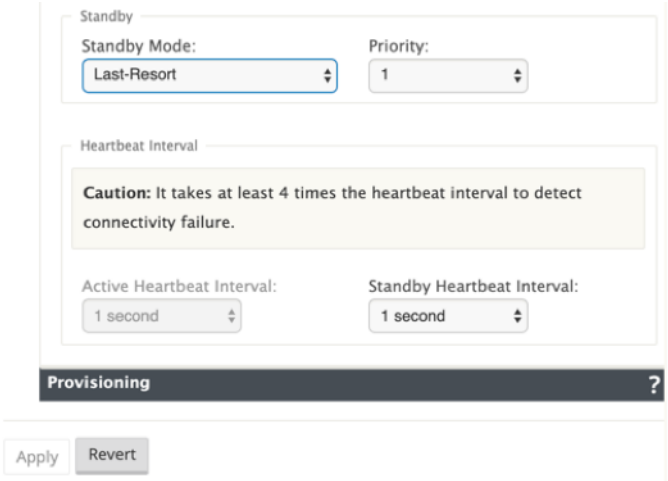


Nachdem Sie das Konfigurationsupdate durchgeführt haben, können Sie die Verwendungsdetails im Dashboard anzeigen.



So konfigurieren Sie Standby-Links:

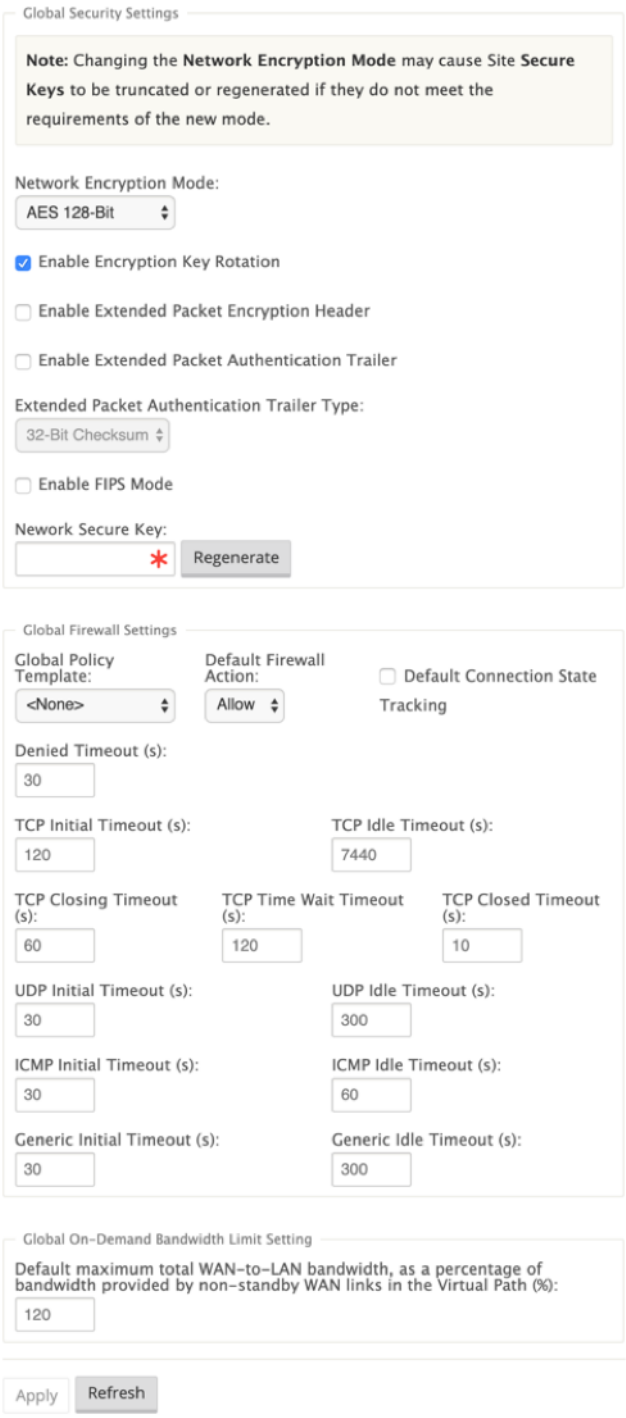
1. Standardmäßig ist der Standby-Modus einer WAN-Verbindung deaktiviert. Um die WAN-Link als Standby zu konfigurieren, wählen Sie einen der Standby-Modi (Last-Resort/On-Demand) aus der Dropdownliste aus.



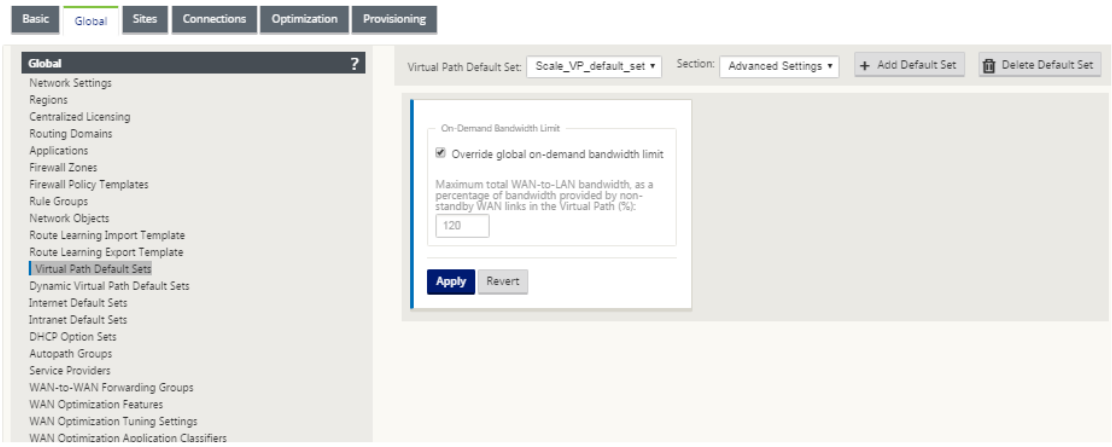
2. Sobald ein Standby-Modus ausgewählt ist, wählen Sie die Standby-Priorität, das aktive Heartbeat-Intervall und das Standby-Heartbeat-Intervall entsprechend aus. Klicken Sie auf **Übernehmen**, um die Konfiguration zu validieren.

3. Wenn eine On-Demand-Standby-Verbindung konfiguriert ist, wird das globale Standard-On-Demand-Bandbreitenlimit (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 ausgedrückt, 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.

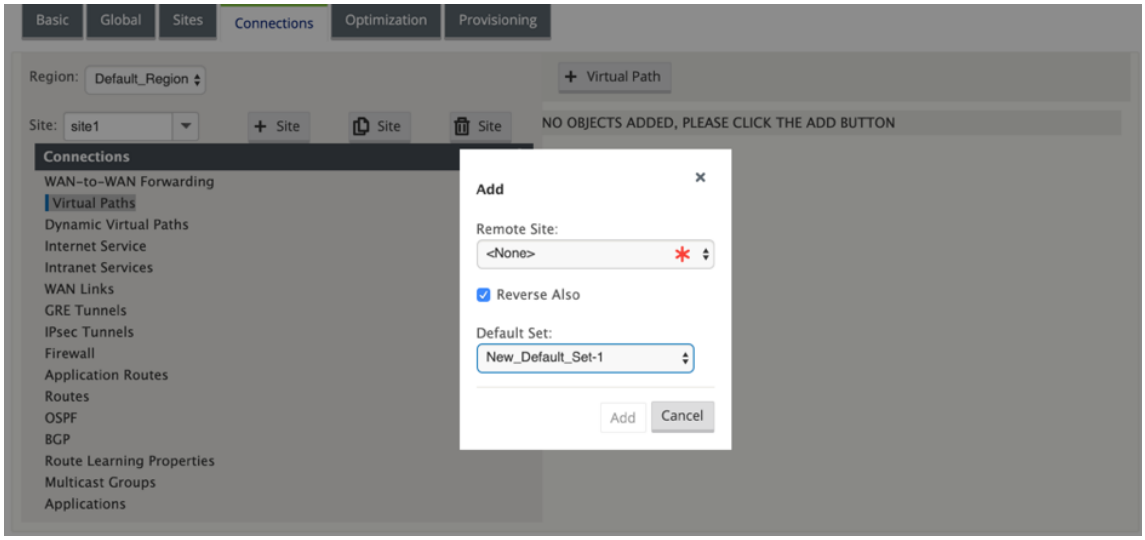
4. Um das globale Standard-Bandbreitenlimit bei Bedarf anzuzeigen oder zu ändern, öffnen Sie die Abschnitte **Global** > **Virtual WAN-Netzwerkeinstellungen**.



5. 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.



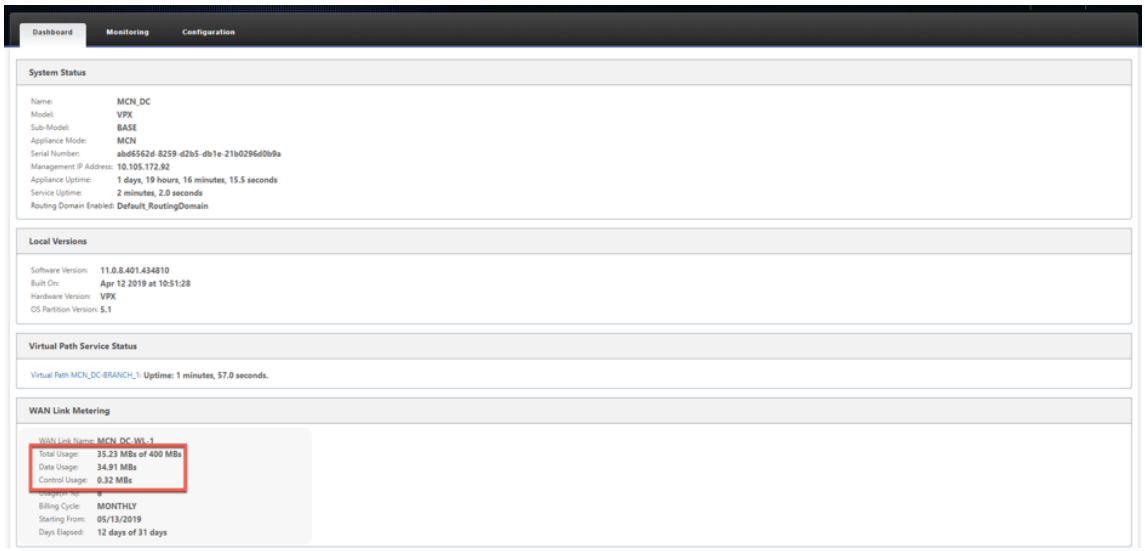
6. Um Einstellungen für einen bestimmten virtuellen Pfad anzuwenden, navigieren Sie zum Abschnitt **Verbindungen > Virtuelle Pfade**, und klicken Sie auf **+ Virtueller Pfad**.



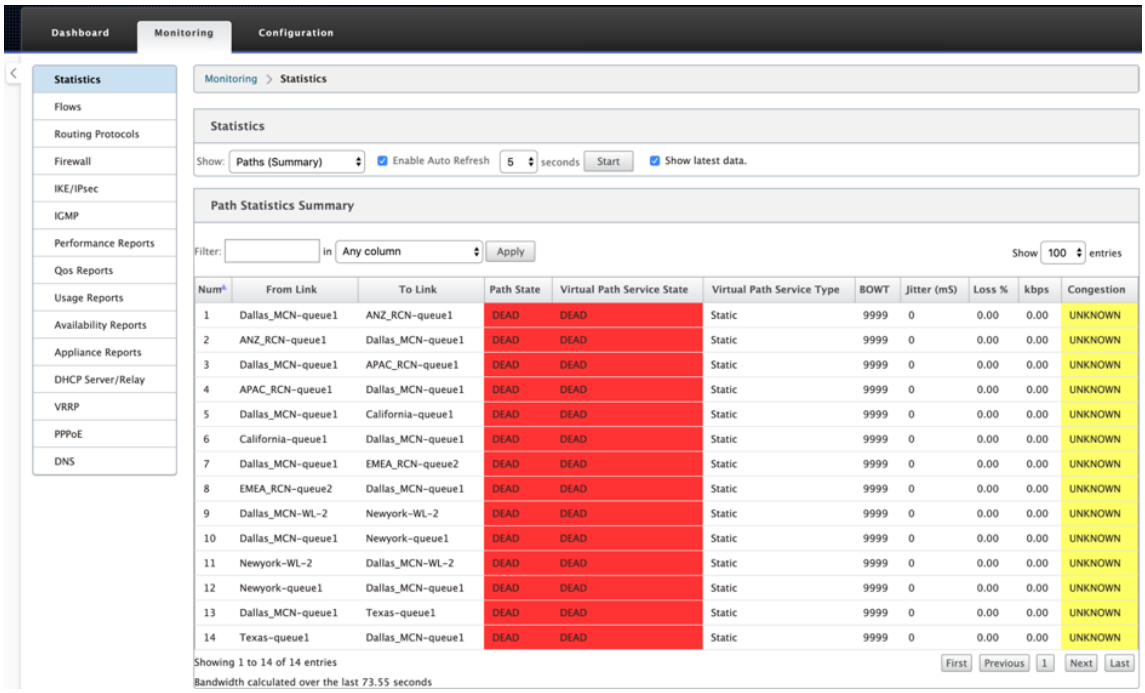
Überwachung von getakteten und Standby-WAN-Verbindungen

- Die Seite Dashboard enthält die folgenden **WAN-Link-Metering-Informationen** mit den Nutzungswerten:
  - **WAN-Linkname**: Zeigt den WAN-Linknamen an.
  - **Gesamtnutzung**: Zeigt die gesamte Verkehrsnutzung an (Datennutzung + Steuerungsnutzung).
  - **Datennutzung**: Zeigt die Verwendung durch den Benutzerverkehr an.
  - **Control Usage**: Zeigt die Verwendung durch Steuerverkehr an.
  - **Verwendung (in%)**: Zeigt den Wert der verwendeten Datenobergrenze in Prozent (Gesamtnutzung/Datenobergrenze) x 100 an.
  - **Abrechnungszeitraum**: Abrechnungshäufigkeit (wöchentlich/monatlich)
  - **Beginnend von**: Startdatum des Abrechnungszyklus

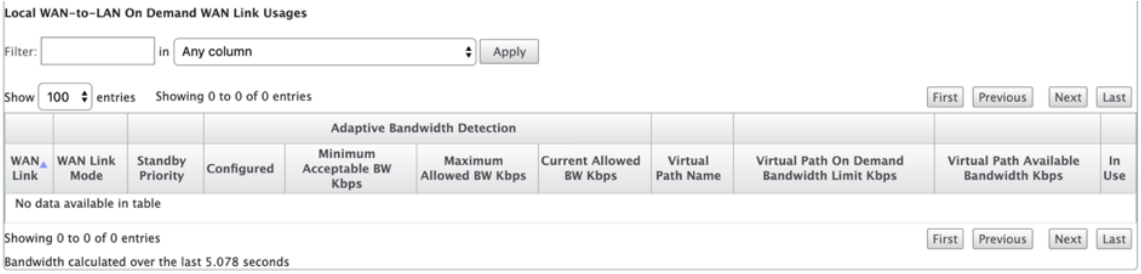
– **Verstrichene Tage**: Die verstrichene Zeit (in Tagen, Stunden, Minuten und Sekunden)



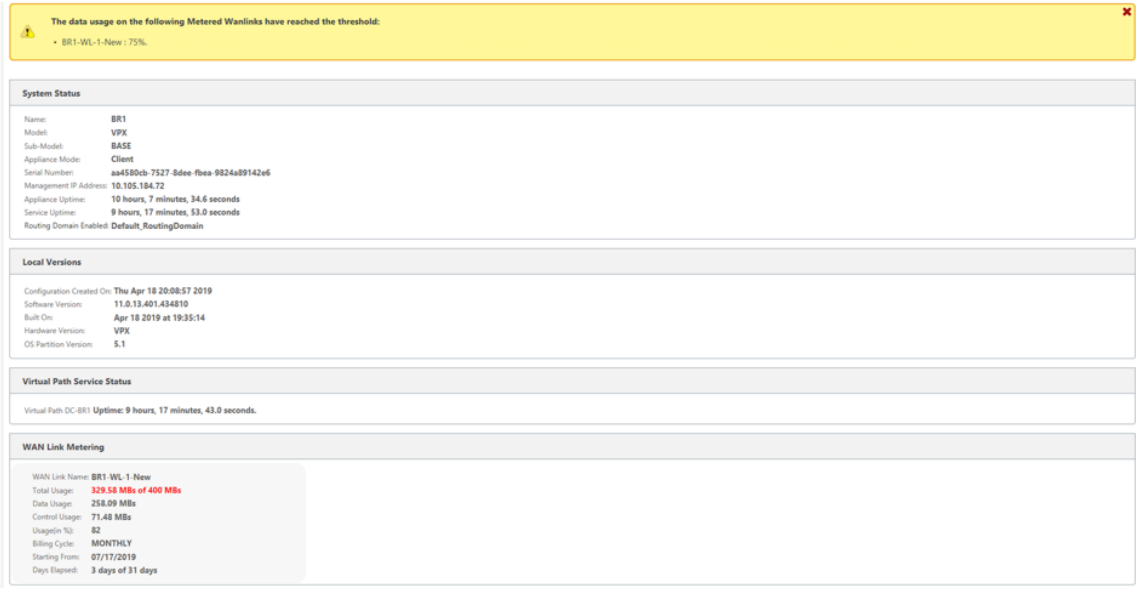
- Wenn Pfadstatistiken (**Monitoring > Statistics > Paths**) angezeigt werden, werden gemessene Links und Standby-Links wie im Screenshot gezeigt markiert.



- Wenn die Appliance über einen virtuellen Pfad verfügt, der über eine lokale oder Remote-On-Demand-Standby-Verbindung verfügt, wird beim Anzeigen von WAN-Link-Nutzungsstatistiken unten auf der Seite eine zusätzliche Tabelle mit der On-Demand-Bandbreite angezeigt (**Überwachung > Statistik > WAN-Link-Nutzung**).



- Wenn die Verwendung eines getakteten Links 50% des konfigurierten Datendeckels überschreitet, wird oben im Dashboard ein Warnbanner angezeigt. Wenn die Nutzung 75% der konfigurierten Datenbegrenzung übersteigt, werden außerdem die numerischen Messinformationen am unteren Rand des Dashboards hervorgehoben.

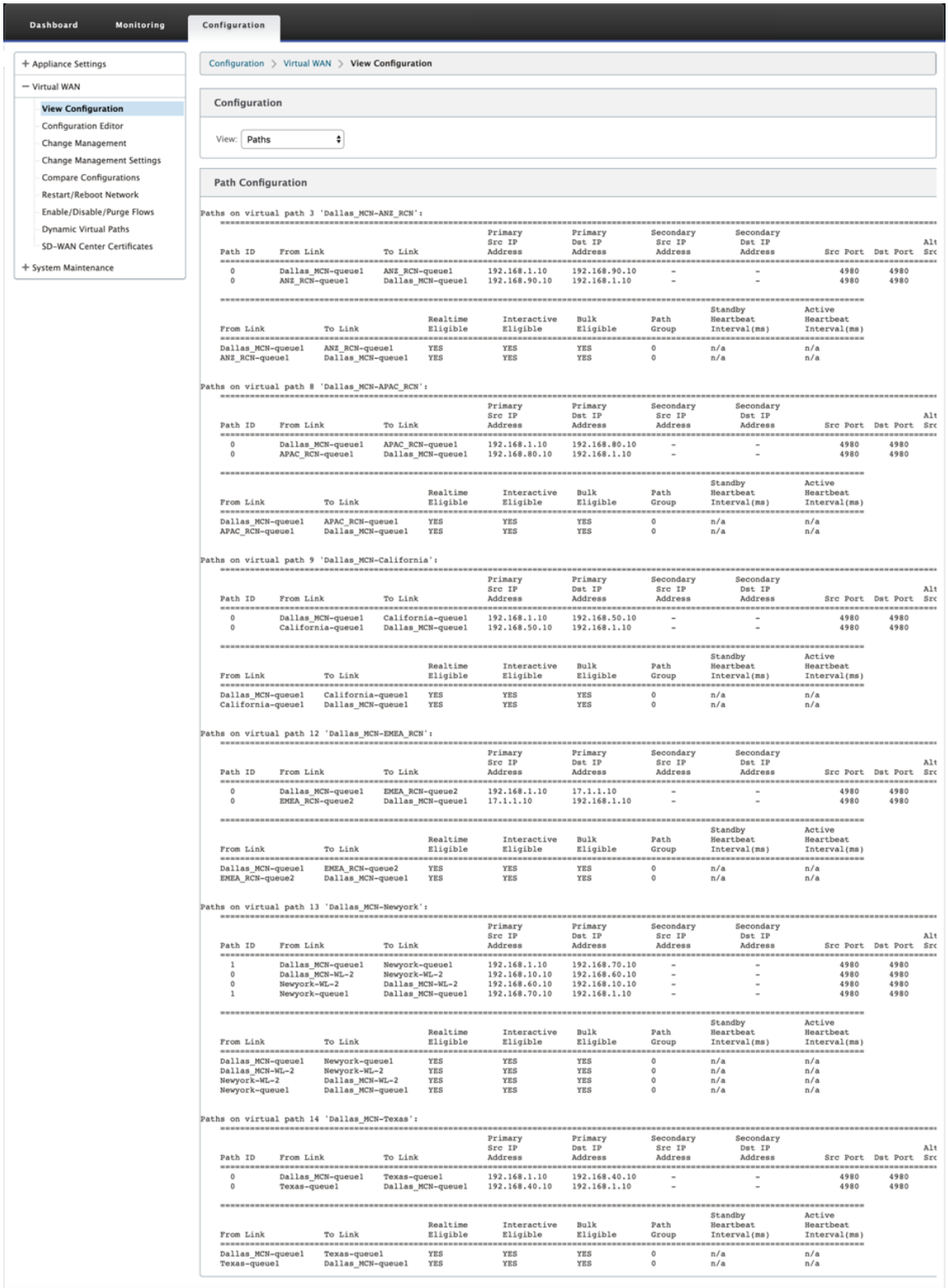


Ein WAN-Link-Verwendungsereignis wird auch an der Appliance generiert, wenn die Verwendung 50%, 75% und 90% der konfigurierten Datenobergrenze überschreitet.

1. 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**> Konfigurationanzeigen**>**Pfade** angezeigt werden.



Office 365-Optimierung

February 7, 2022

Die **Office 365-Optimierungsfunktionen** entsprechen den Microsoft Office 365-Netzwerkkonnektivitätsprinzipien um Office 365 zu optimieren. Office 365 wird als Service über mehrere Service-Endpunkte (Fronttüren) bereitgestellt, die sich global befinden. Um eine optimale Benutzererfahrung für den Office 365-Datenverkehr zu erzielen, empfiehlt Microsoft, Office365-Datenverkehr von Zweigstellenumgebungen direkt auf das Internet umzuleiten. Vermeiden Sie Praktiken wie Backhauling zu einem zentralen Proxy. Office 365-Datenverkehr wie Outlook, Word reagiert empfindlich auf Latenz und Backhauling-Verkehr führt zu mehr Latenz, was zu einer schlechten Benutzererfahrung führt. Mit Citrix SD-WAN können Sie Richtlinien konfigurieren, um Office 365-Datenverkehr zum Internet auszuschalten.

Der Office 365-Verkehr wird zum nächstgelegenen Office 365-Dienstendpunkt geleitet, der an den Rändern der Microsoft Office 365-Infrastruktur weltweit existiert. Sobald der Verkehr eine Haustür erreicht, geht er über das Netzwerk von Microsoft und erreicht das eigentliche Ziel. Es minimiert die Latenz, 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. Serviceanfragen an diese Endpunkte müssen von der Zweigstelle zum Internet abbrechen und dürfen 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. Serviceanfragen an diese Endpunkte können von der Zweigstelle 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

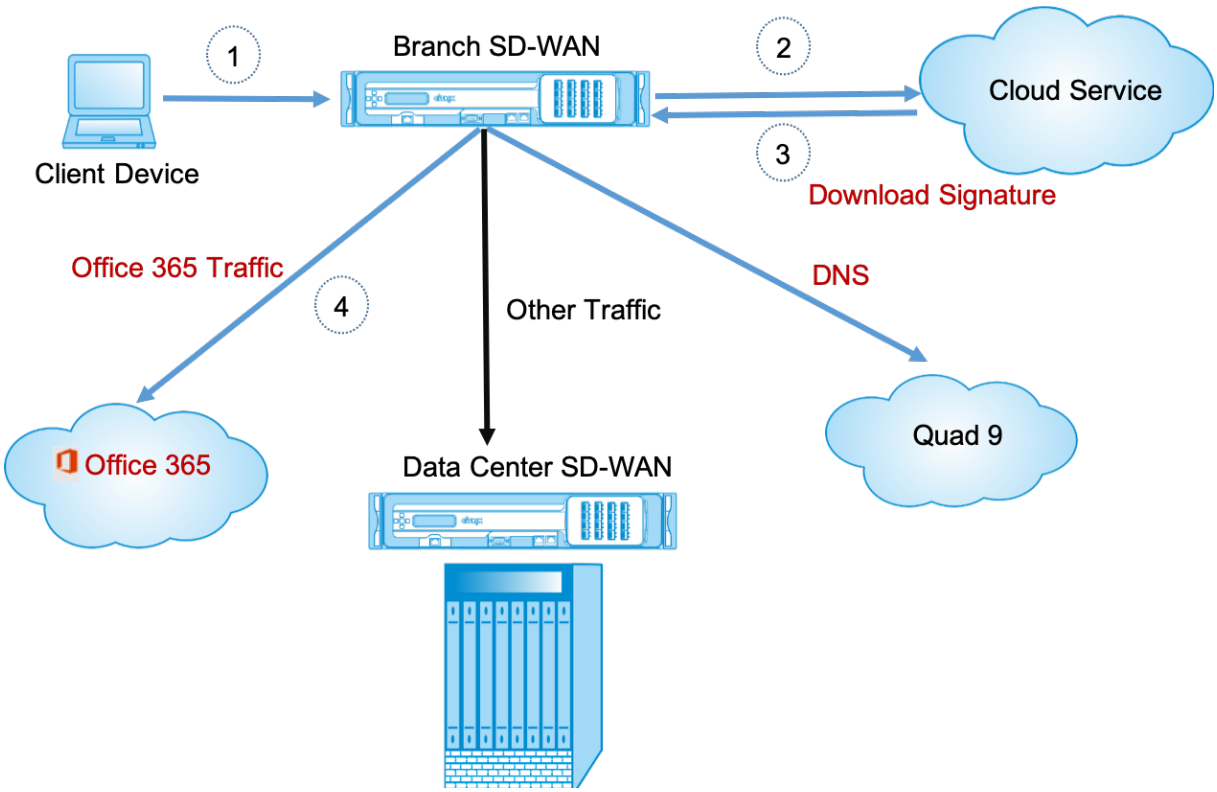
hinaus ist der Datenverkehr in dieser Kategorie möglicherweise nicht immer Office 365-Verkehr. Daher wird empfohlen, diese Option zu deaktivieren, wenn Sie Office 365 Breakout in Ihrem Netzwerk aktivieren.

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 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**
>
> Die erste Paketerkennung und Klassifizierung des Office 365-Datenverkehrs erfolgt standardmäßig, unabhängig davon, ob die Office 365-Breakout-Funktion aktiviert ist oder nicht.

Wenn eine Anforderung für die Office 365-Anwendung eintrifft, führt der Anwendungsklassifizierer eine erste Paketklassifizierungsdatenbank durch, identifiziert und markiert den Office-365-Datenverkehr. Sobald der Office 365-Datenverkehr klassifiziert ist, werden die automatisch erstellten Anwendungsroute 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 Domainnamensystem.



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 des Office 365-Breakouts und der Kompilierung der Konfiguration wird ein DNS-Objekt, ein Anwendungsobjekt, eine Anwendungsroute und eine Firewall-Richtlinienvorlage automatisch erstellt und mit dem Internetdienst auf Zweigstellen angewendet.

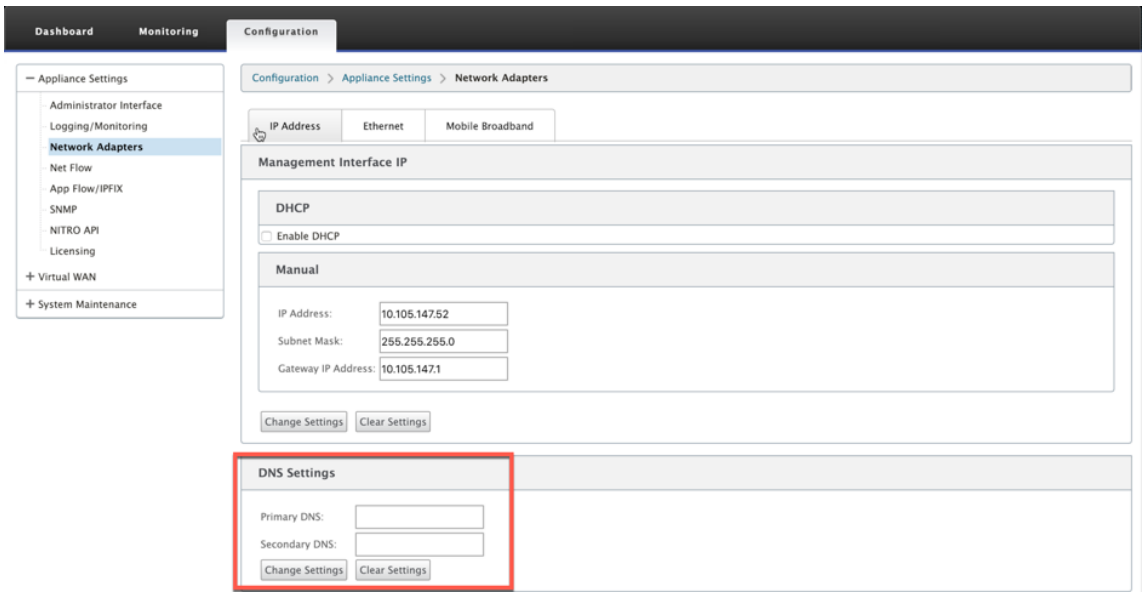
Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben:

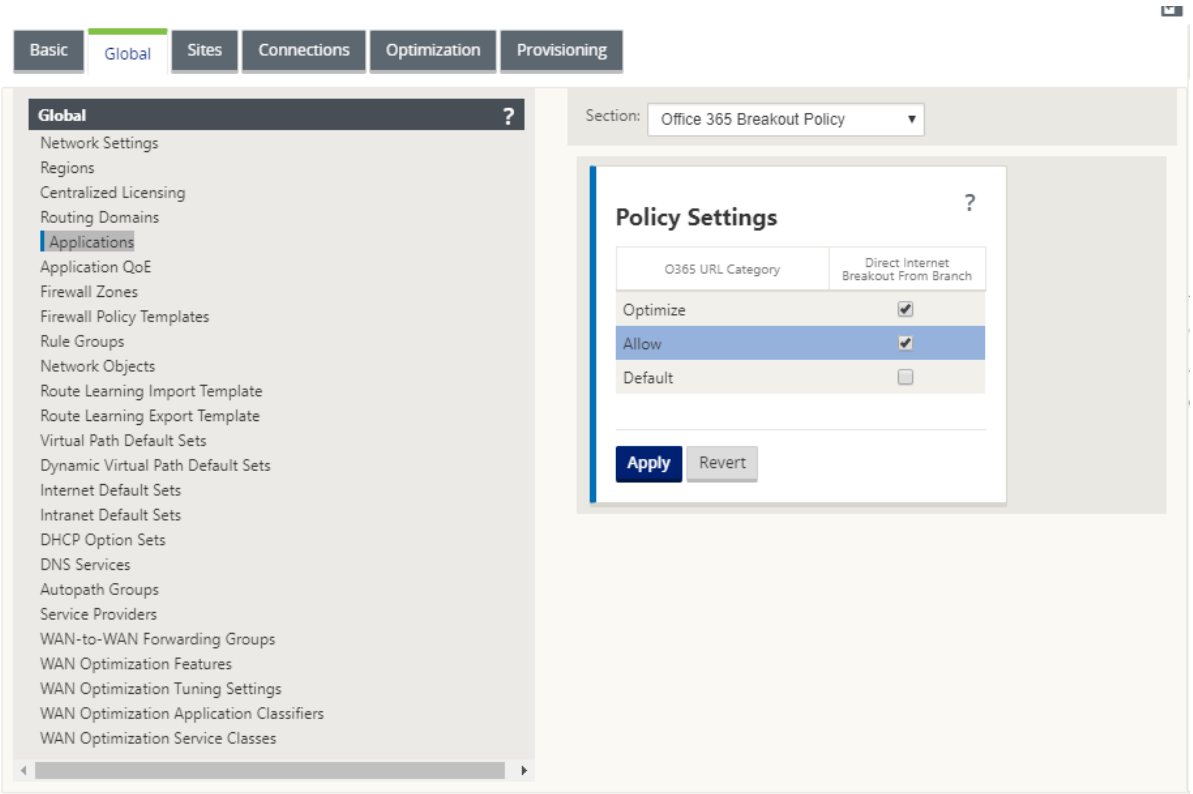
1. Um Office 365 Breakout durchzuführen, muss ein Internetdienst auf der Appliance konfiguriert werden. Weitere Informationen zur Konfiguration des Internetdienstes finden Sie unter Internetzugriff.
2. Stellen Sie sicher, dass die Verwaltungsschnittstelle über eine Internetverbindung verfügt.

   Sie können das Citrix SD-WAN-Webinterface verwenden, um die Einstellungen der Verwaltungsschnittstelle zu konfigurieren.

3. Stellen Sie sicher, dass das Management-DNS konfiguriert ist. Um das DNS der Verwaltungsschnittstelle zu konfigurieren, navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter**. Geben Sie im Abschnitt **DNS-Einstellungen** die Details des primären und sekundären DNS-Servers ein, und klicken Sie auf **Einstellungen ändern** .

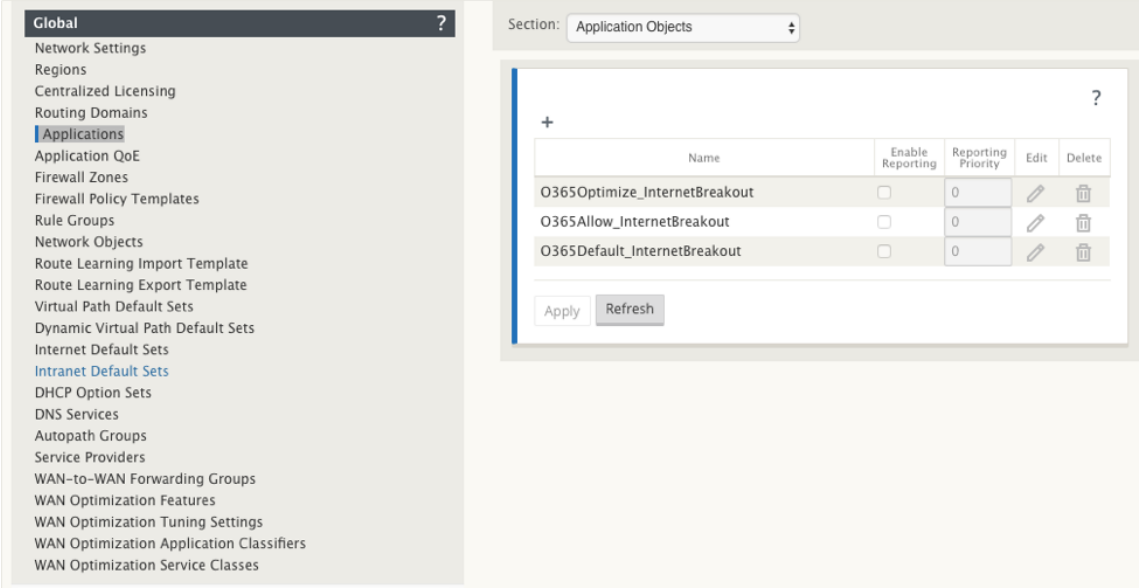


Die Einstellung der **Office 365-Breakoutrichtlinie** ist unter den globalen Einstellungen verfügbar. Wählen Sie die erforderliche Office 365-Kategorie für das Internetbreakout aus und klicken Sie auf **Übernehmen**.

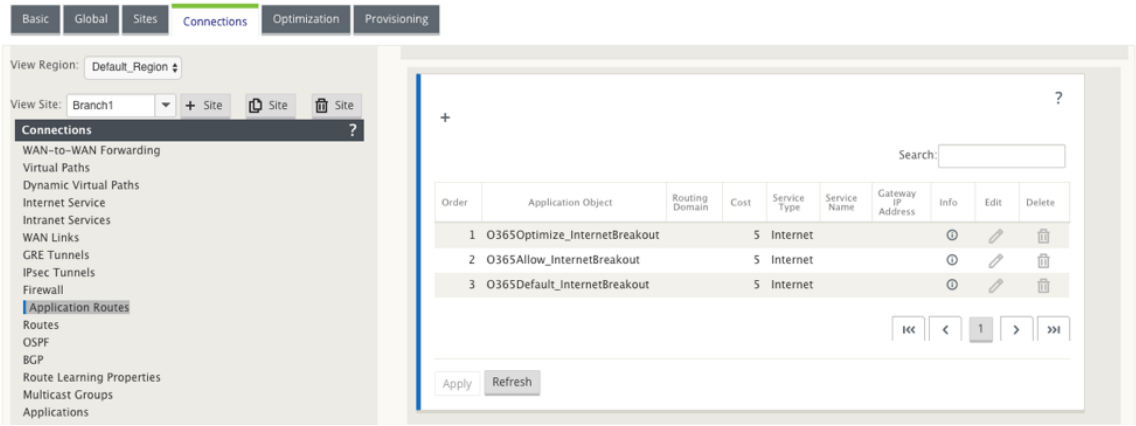


Nachdem Sie Office 365 konfiguriert haben, brechen Sie Richtlinieneinstellungen aus und kompilieren Sie die Konfiguration. Die folgenden Einstellungen werden automatisch ausgefüllt.

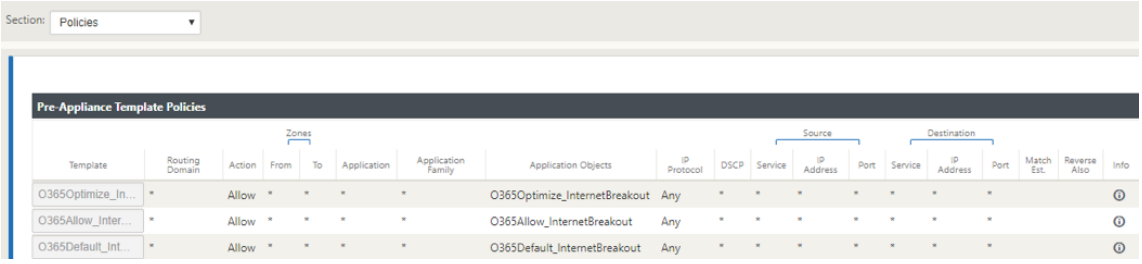
- **DNS-Objekt** - Das DNS-Objekt gibt an, welche Art von Datenverkehr an den DNS-Dienst weitergeleitet werden soll, dass der Benutzer konfiguriert ist. Die DNS-Anfragen werden auf allen vertrauenswürdigen Schnittstellen gehört, und DNS-Weiterleitungen sind enthalten, um Office 365-DNS-Anfragen an den 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 Zweigsites angewendet, die über einen Internetdienst verfügen. Die Richtlinie vor der Appliance hat Vorrang vor lokalen Richtlinienvorlagen und Post-Appliance-Richtlinien.

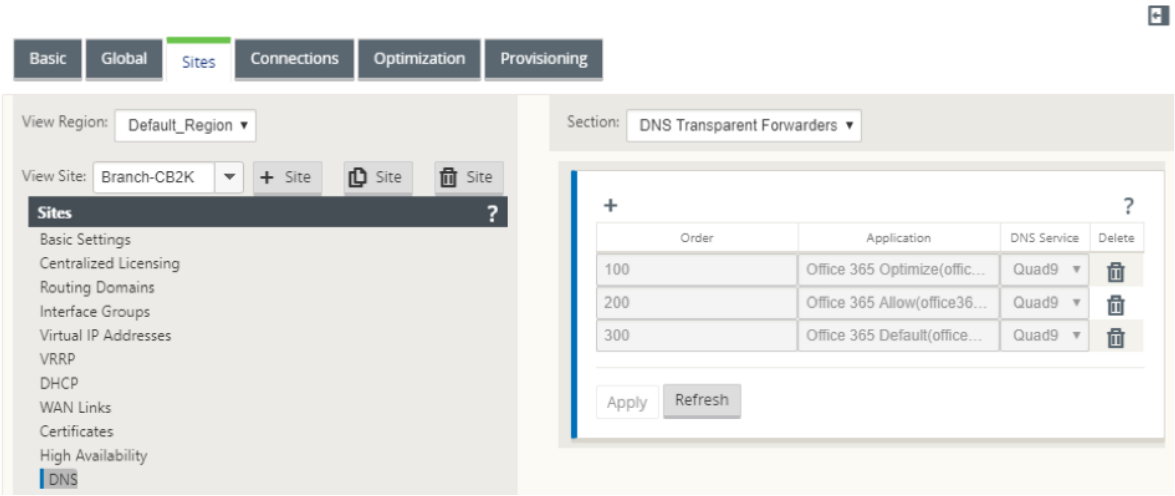


Transparente Weiterleitung für Office 365

Der Zweig bricht für Office 365 aus, beginnt mit einer DNS-Anfrage. Die DNS-Anfrage, die Office 365-Domänen durchläuft, muss lokal gesteuert werden. Wenn Office 365-Internet-Break Out aktiviert ist, werden die internen DNS-Routen ermittelt und die Liste der transparenten Weiterleitungen automatisch ausgefüllt. Office 365-DNS-Anfragen werden standardmäßig an den Open Source DNS-Dienst Quad 9 weitergeleitet. Der Quad 9 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.

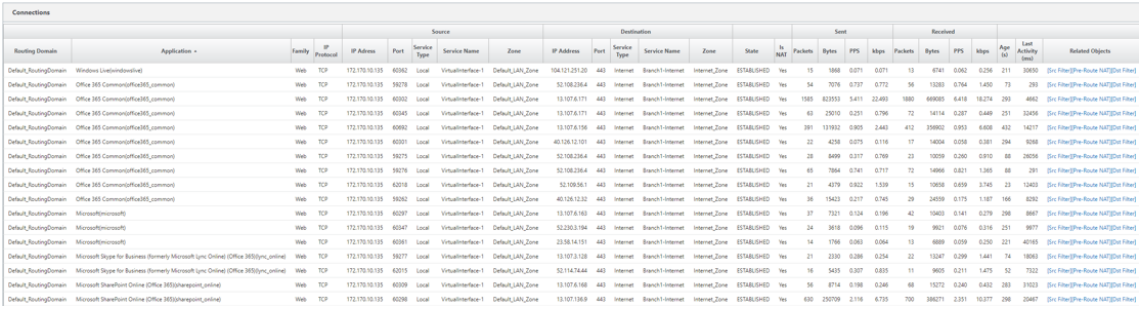
Wenn Sie einen anderen DNS-Proxy verwenden oder SD-WAN als DNS-Proxy konfiguriert ist, wird die Weiterleitungsliste automatisch mit Weiterleitungen für Office 365-Anwendungen gefüllt.



Überwachen

Sie können die Office 365-Anwendungsstatistiken in den folgenden SD-WAN-Statistikberichten überwachen:

- Firewall-Statistiken



- 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
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
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

- Anwendungs-Routenstatistiken

Monitoring > Statistics

Statistics

Show: Application Routes | Enable Auto Refresh | 5 seconds | Stop | Clear Counters on Refresh | Processing...

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 3 of 3 entries

First Previous 1 Next Last

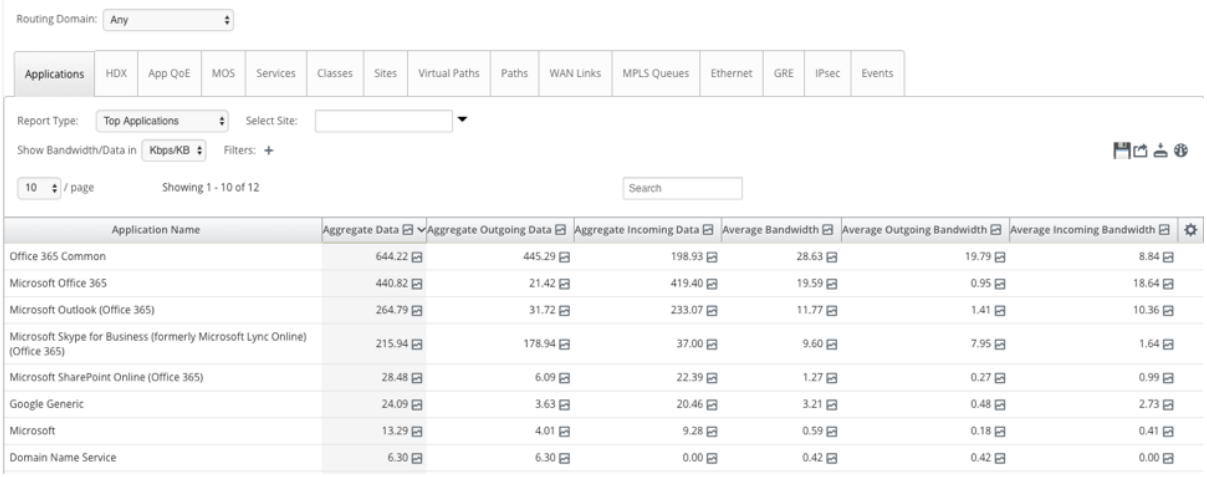
Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1792	YES	N/A	N/A
2	O365Allow_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1395	YES	N/A	N/A
1	O365Default_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

Sie können Office 365-Anwendungsstatistiken auch im SD-WAN Center-Anwendungsbericht

anzeigen.

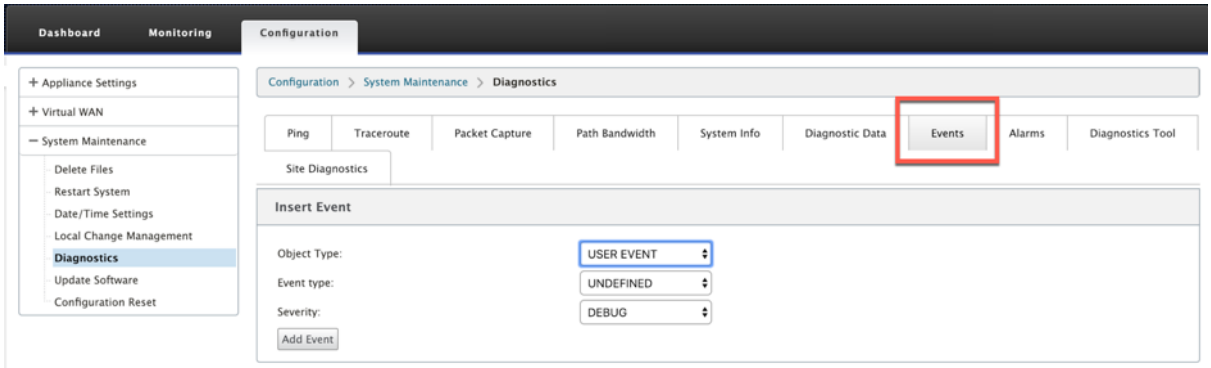


Application Name	Aggregate Data	Aggregate Outgoing Data	Aggregate Incoming Data	Average Bandwidth	Average Outgoing Bandwidth	Average Incoming Bandwidth
Office 365 Common	644.22	445.29	198.93	28.63	19.79	8.84
Microsoft Office 365	440.82	21.42	419.40	19.59	0.95	18.64
Microsoft Outlook (Office 365)	264.79	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

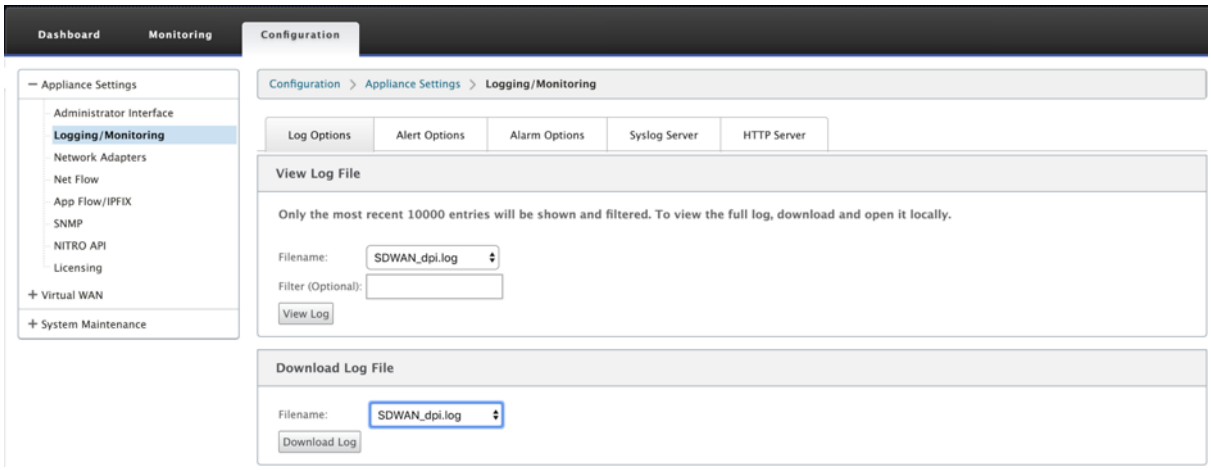
ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API

Times are in UTC

Die Verbindungsfehler werden auch in **SDWAN_dpi.log** protokolliert. Um das Protokoll anzuzeigen, navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Protokollierung/Überwachung >**

Protokolloptionen. Wählen Sie die **SDWAN_dpi.log** aus der Dropdownliste aus und klicken Sie auf **Protokoll**anzeigen.

Sie können die Protokolldatei auch herunterladen. Um die Protokolldatei herunterzuladen, wählen Sie die erforderliche Protokolldatei aus der Dropdownliste unter dem Abschnitt **Protokolldatei herunterladen** aus und klicken Sie auf **Protokoll herunterladen**.



Einschränkungen

- Wenn die Office 365-Breakout-Richtlinie konfiguriert ist, wird Deep Packet Inspection nicht 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 Firewall-Richtlinie hat die niedrigste Priorität und ist nicht editierbar.
- Die Routenkosten für die automatisch erstellte Anwendungsroute betragen fünf. Sie können es mit einer kostengünstigeren Route überschreiben.

Office 365-Beacon-Dienst

Microsoft bietet den Office 365-Beacon-Dienst an, um die Office 365-Erreichbarkeit 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.

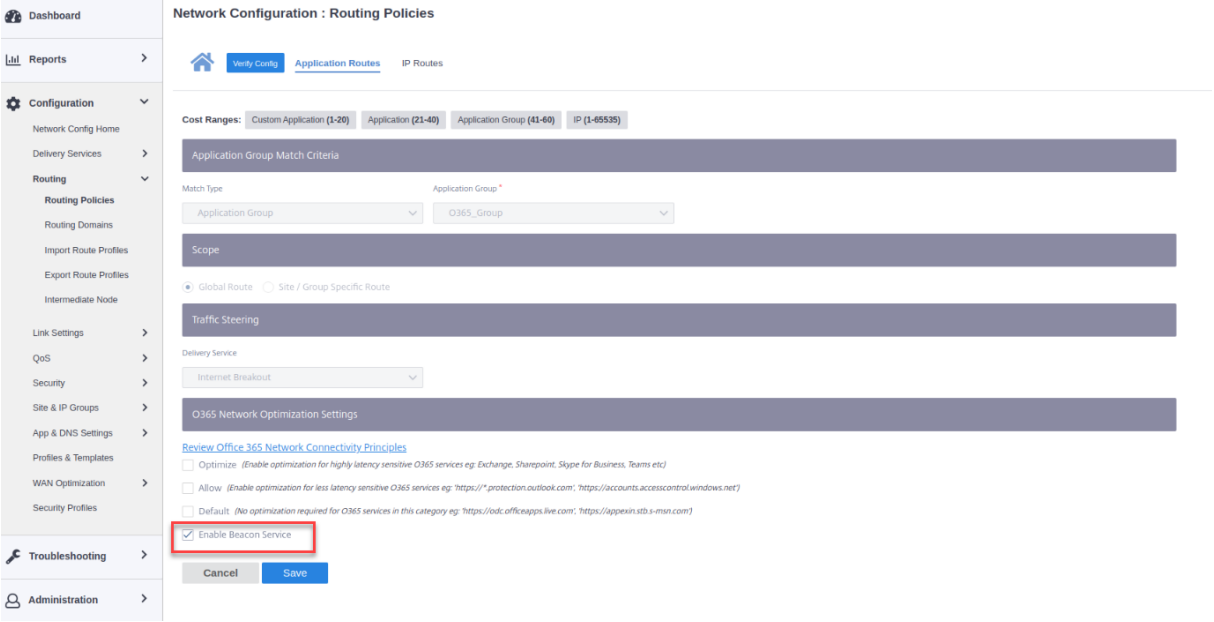
Mit Citrix SD-WAN können Sie nicht nur Beacon-Probing durchführen, sondern auch die Latenz bestimmen, mit der Office 365-Endpunkte über jede WAN-Verbindung erreicht werden. Die Latenz ist die Roundtrip-Zeit, die zum Senden einer Anfrage und zum Abrufen einer Antwort vom Office 365-Beacon-Dienst über 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. Das Beacon-Sondieren ist nur über Citrix SD-WAN Orchestrator aktiviert. Standardmäßig ist das Beacon-Sondieren für alle internetfähigen WAN-Verbindungen aktiviert, wenn der Office 365-Ausbruch über Citrix SD-WAN Orchestrator aktiviert ist.

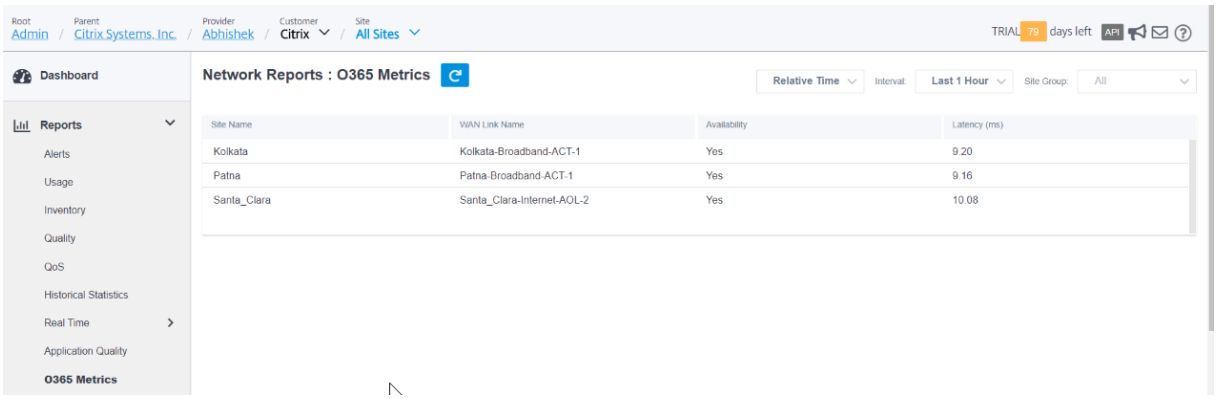
> **Hinweis**
>
> Die Prüfung von Office 365-Beacons ist für getaktete Verbindungen nicht aktiviert.

Sie können Office 365-Beacon-Probing deaktivieren und Latenzberichte im SD-WAN Orchestrator anzeigen. Weitere Informationen finden Sie unter Office 365-Optimierung.

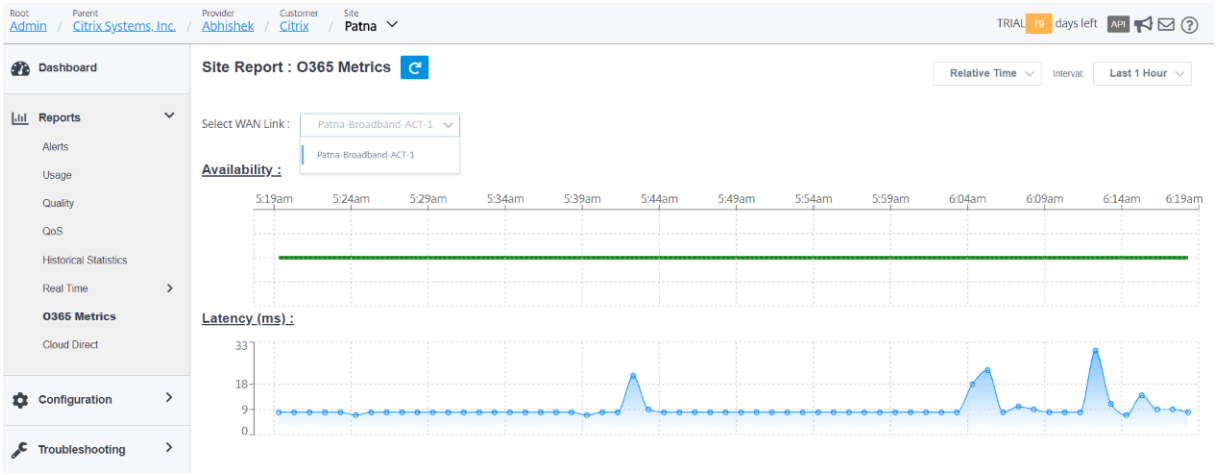
Um den Office 365 Beacon-Dienst zu deaktivieren, navigieren Sie in SD-WAN Orchestrator auf Netzwerkebene zu **Konfiguration** > **Routing** > **Routing-Richtlinien** > **O365 Network Optimization Settings** und deaktivieren **Sie Enable Beacon Service**.



Um die Beacon-Sondierungs- und Latenzberichte in Citrix 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-Softwareversion 11.2.1 und höher standardmäßig aktiviert.

Für die Citrix SD-WAN-Softwareversion unter 11.3.0 wird die erste Paketerkennung und -klassifizierung des Citrix Cloud- und Gateway-Dienstverkehrs nur durchgeführt, wenn die Breakout-Feature für den Citrix Cloud- und Gateway-Dienst nicht deaktiviert ist.

Für die Citrix SD-WAN-Softwareversion 11.3.0 und höher wird die erste Paketerkennung und -klassifizierung des Citrix Cloud- und Gateway-Dienstdatenverkehrs unabhängig davon durchgeführt, ob die Breakout-Feature für Citrix Cloud and Gateway Service aktiviert ist oder nicht.

> **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-Softwareversion 11.2.3 oder höher eingeführt. Das Ziel besteht darin, eine detailliertere 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:

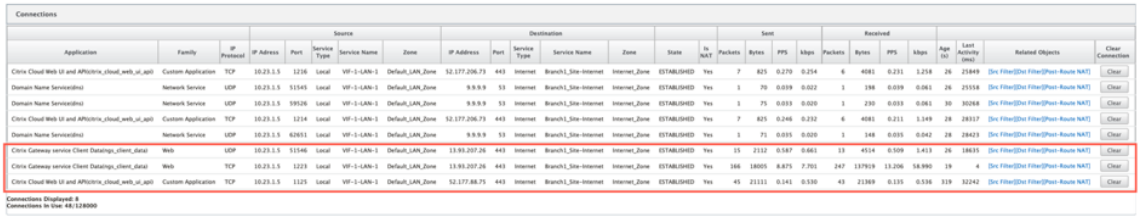
- **Citrix Cloud**: Ermöglicht die Erkennung und Weiterleitung von Datenverkehr, der für Citrix Cloud Web-Benutzeroberfläche und APIs bestimmt ist.
  - Citrix SD-WAN Orchestrator und abhängige kritische Services:
    - **Citrix SD-WAN Orchestrator**: Ermöglicht direktes Internetbreakout von Heartbeat 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-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.

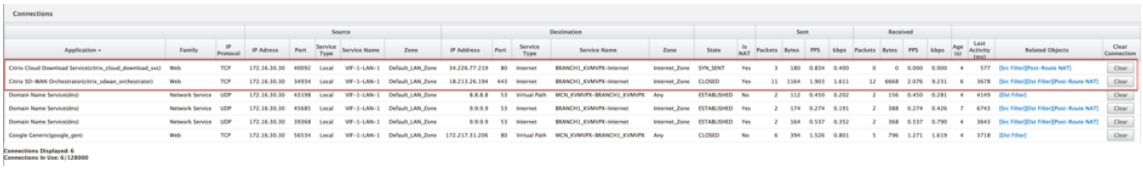
– **Gateway Service Web Proxy Traffic**: Ermöglicht direktes Internetbreakout des Webproxydatenverkehrs. Es erfordert eine hohe Bandbreite, aber die Latenzanforderungen können variieren.

Überwachen

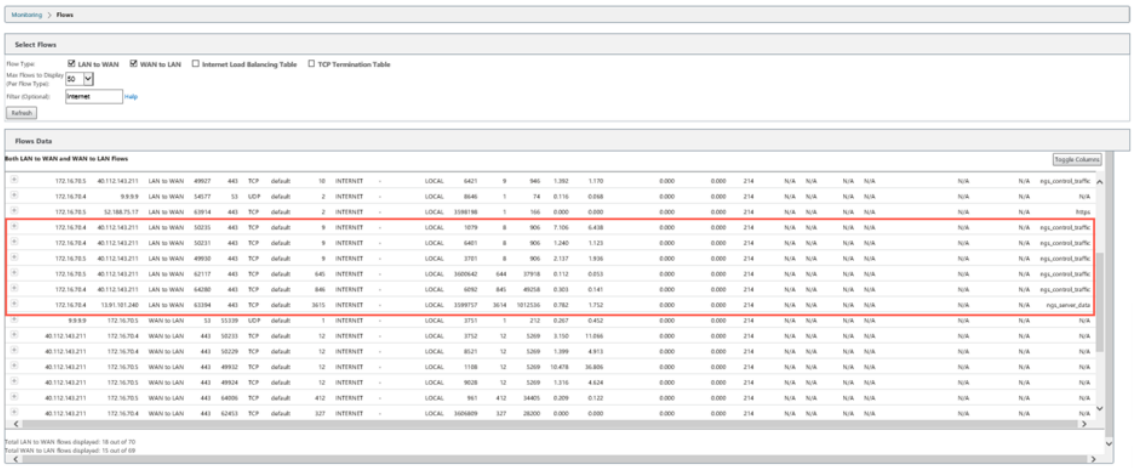
Sie können die Gateway Service-Statistiken in den folgenden SD-WAN-Statistikberichten überwachen:

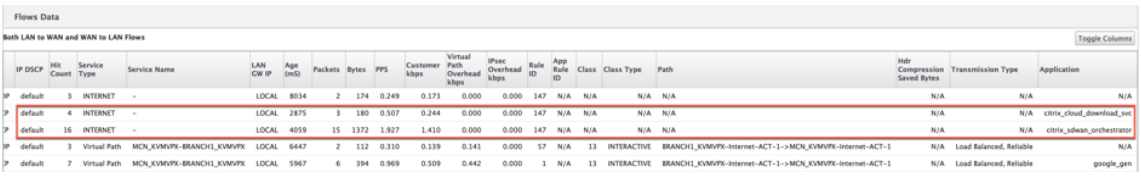
- Firewall-Statistiken





- Strömungen





- DNS-Statistiken

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

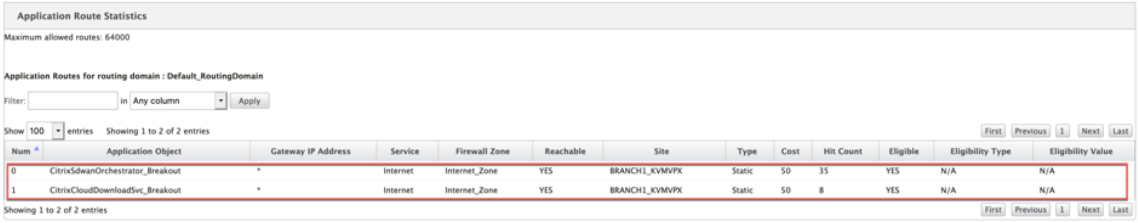
Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 6 of 6 entries First Previous 1 Next Last

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	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

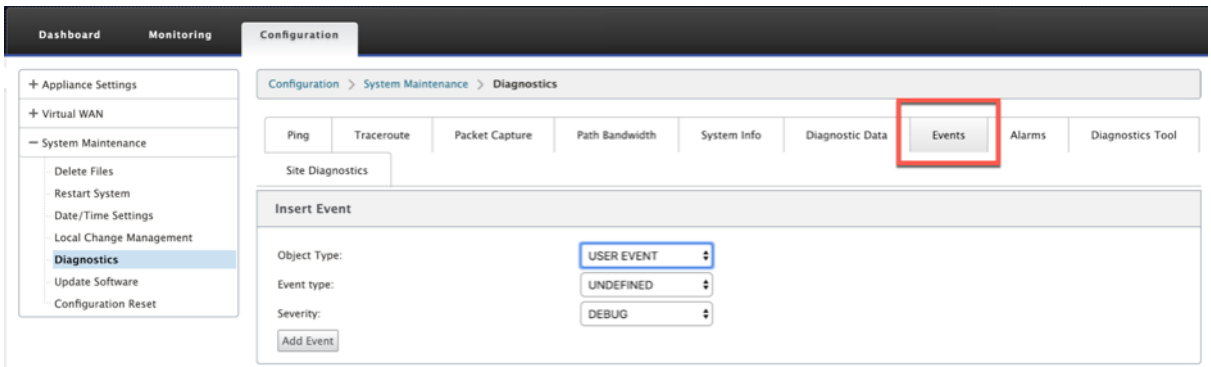
Showing 1 to 6 of 6 entries First Previous 1 Next Last



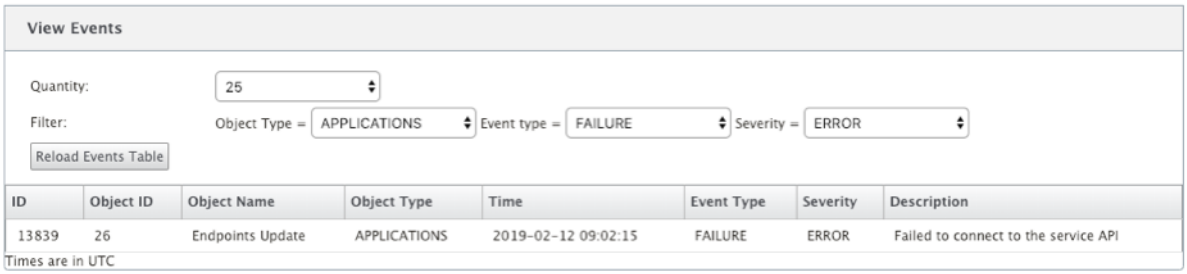
Problembehandlung

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**.

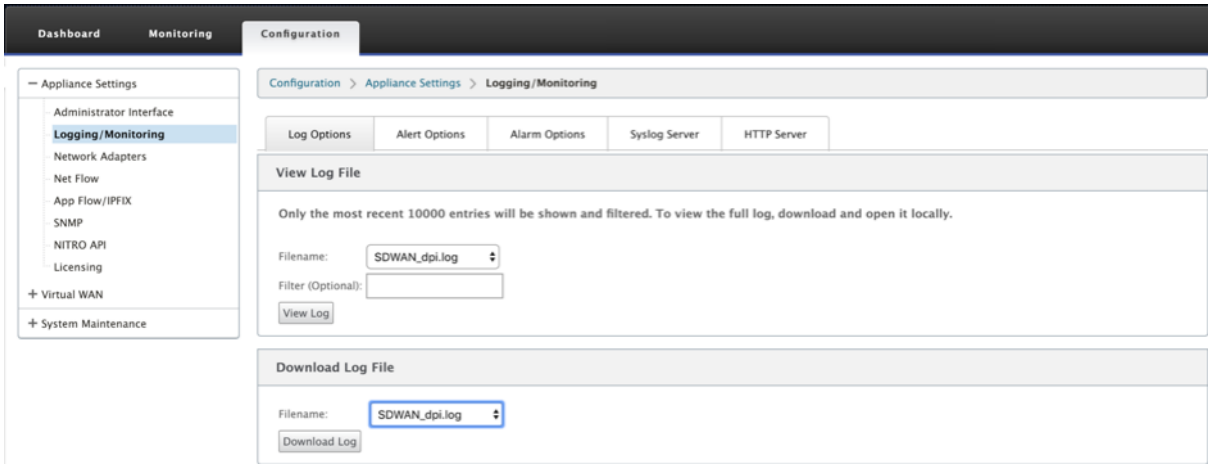


Wenn bei der Verbindung mit dem Citrix Dienst ein Problem auftritt (sdwan-app-routing.citrixnetworkapi.net), wird die Fehlermeldung in der Tabelle **Ereignisse anzeigen** angezeigt.



Die Verbindungsfehler werden auch in **SDWAN_dpi.log** protokolliert. Um das Protokoll anzuzeigen, navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Protokollierung/Überwachung > Protokolloptionen**. Wählen Sie die SDWAN_dpi.log aus der Dropdownliste aus und klicken Sie auf **Protokoll anzeigen**.

Sie können die Protokolldatei auch herunterladen. Um die Protokolldatei herunterzuladen, wählen Sie die erforderliche Protokolldatei aus der Dropdownliste 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.

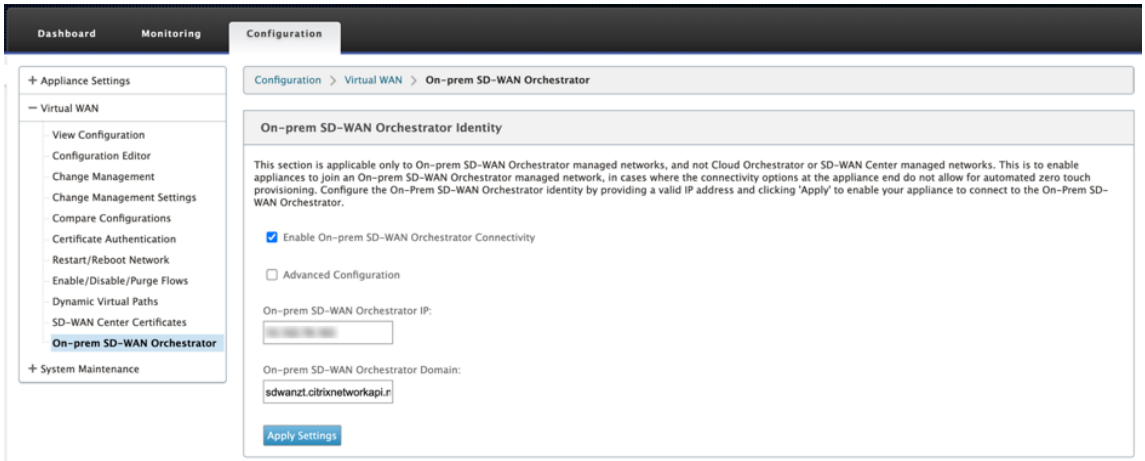
Sie können eine Verbindung zwischen Ihrer Citrix SD-WAN-Appliance und dem Citrix SD-WAN Orchestrator für lokale Standorte herstellen, indem Sie Orchestrator-Konnektivität aktivieren und den Citrix SD-WAN Orchestrator für lokale Identität angeben.

> **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 Problemumgehung 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:

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.



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

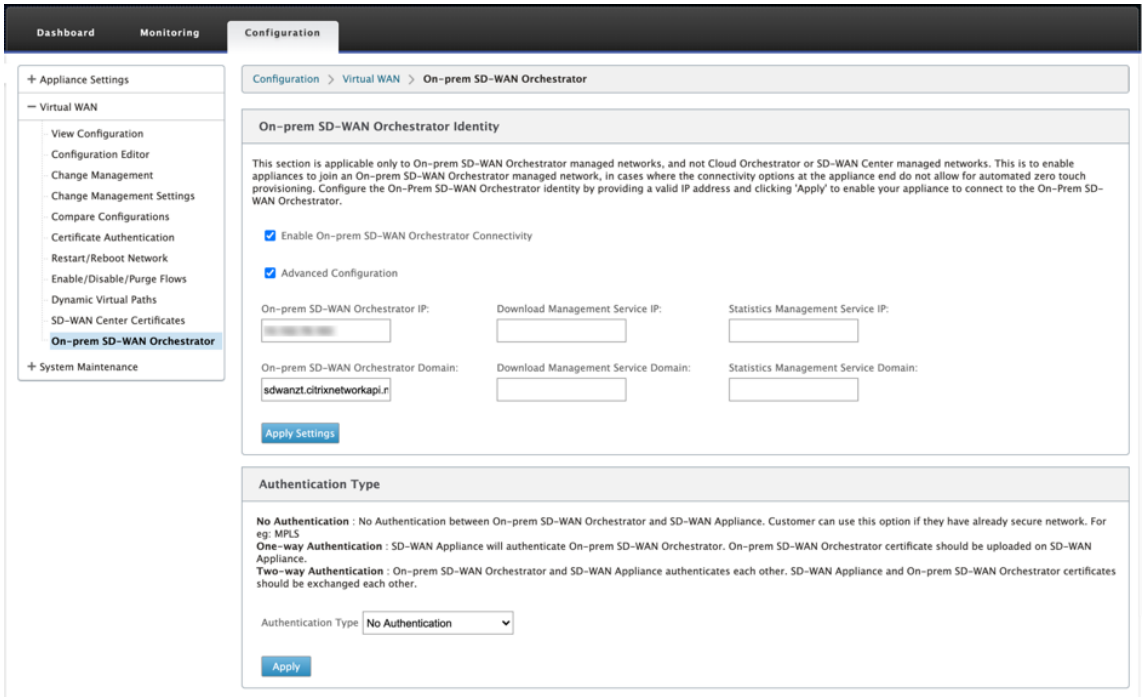
   - download.citrix.com
   - sdwanzt.citrix.com
   - sdwan-home.citrix.com

   Im Falle einer erweiterten Konfiguration:

   Beispiel: Wenn die on-premises Orchestrator-Domäne als **citrix.com**konfiguriert ist, wird die Download-Verwaltungsdienstdomäne als **download.citrix.com**konfiguriert, und die Statistikverwaltungsdienstdomäne wird 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



Orchestrator on-premises unterstützt möglicherweise laufende Dienste 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/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 aufge-

führt, die zwischen der SD-WAN-Appliance und dem Citrix SD-WAN Orchestrator für lokale Konnektivität unterstützt werden:

- **Keine Authentifizierung** —Keine Authentifizierung zwischen dem on-premises SD-WAN Orchestrator und der SD-WAN-Appliance, und es ist nicht erforderlich, die **SD-WAN-Appliance oder das lokale SD-WANOrchestrator-Zertifikat**zu verwenden. Sie können diese Option jedoch verwenden, wenn Sie über ein sicheres Netzwerk wie MPLS verfügen.
- **Einseitige Authentifizierung** —Bei Auswahl des Typs **Einwegauthentifizierung** müssen Sie das on-premises Orchestrator-Zertifikat hochladen. Laden Sie das lokale Orchestrator-Zertifikat von Orchestrator on-premises herunter und klicken Sie auf **Hochladen**. Die SD-WAN-Appliance vertraut dem Orchestrator on-premises mit den hochgeladenen Zertifikaten.
- **Zwei-Wege-Authentifizierung** —Orchestrator-On-Premises- und Appliance-Zertifikate müssen untereinander ausgetauscht werden. Für die **Zwei-Wege-Authentifizierung**müssen Sie das SD-WAN-Appliance-Zertifikat auf dem Orchestrator on=premises regenerieren, herunterladen und hochladen. SD-WAN Appliance und Orchestrator on-premises sich gegenseitig mit den ausgetauschten Zertifikaten.

> **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.

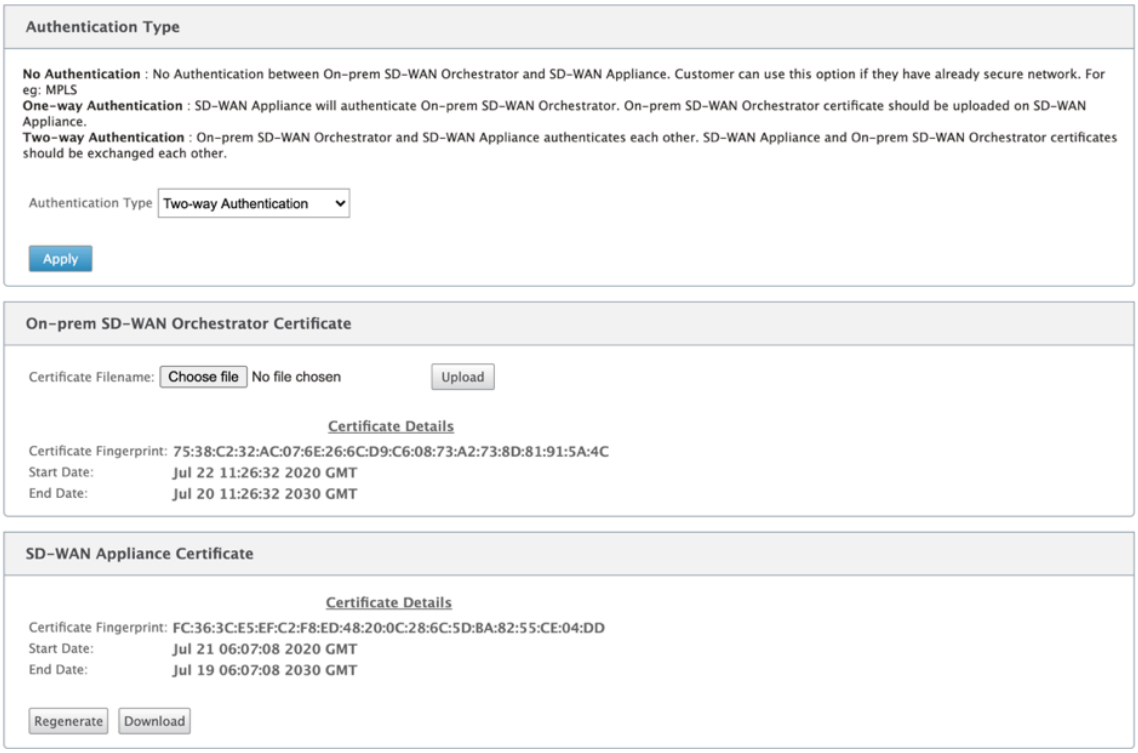
Wenn der lokale **Authentifizierungstyp** von Orchestrator deaktiviert ist, kann sich die Appliance on-premises entweder über **Keine Authentifizierung oder über die einseitige Authentifizierungoder den **Zweiwege-Authentifizierungsmodus**** mit Orchestrator verbinden.

Wenn der on-premises **Orchestrator-Authentifizierungstyp** aktiviert ist, kann Appliance nur über **Zwei-Wege-Authentifizierung**eine Verbindung mit Orchestrator vor Ort herstellen.

Beim Deaktivieren des **Authentifizierungstyps** in Orchestrator on-premises vom Enable-Status wird vorhandene Geräte im Modus "Einwegauthentifizierung"in den Status "Getrennt"versetzt. Kunden müssen den Authentifizierungstyp der Appliance in Zwei-Wege-Authentifizierung ändern und das SD-WAN Appliance-Zertifikat on-premises in den 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 regeneriert und zwischen Orchestrator on-premises und SD-WAN-Appliance ausgetauscht werden, um den Verlust der Appliance-Konnektivität mit Orchestrator on-premises zu vermeiden.



5. Klicken Sie auf **Einstellungen anwenden**.

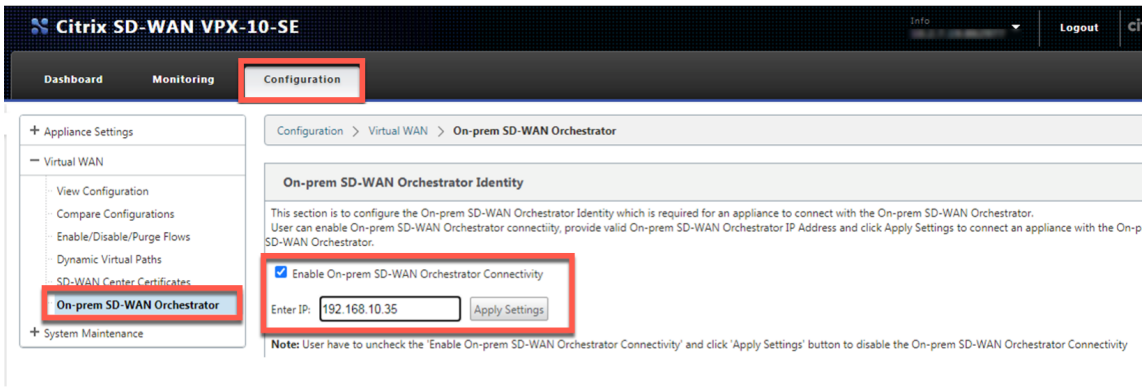
Deaktivieren Sie die Option Citrix SD-WAN Orchestrator für lokale Konnektivität **aktivieren und klicken Sie auf**Einstellungen anwenden**, um den Citrix SD-WAN Orchestrator für on-premises Konnektivität**zu deaktivieren. Um ein lokales verwaltetes Orchestrator-Netzwerk entweder in Cloud Orchestrator 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

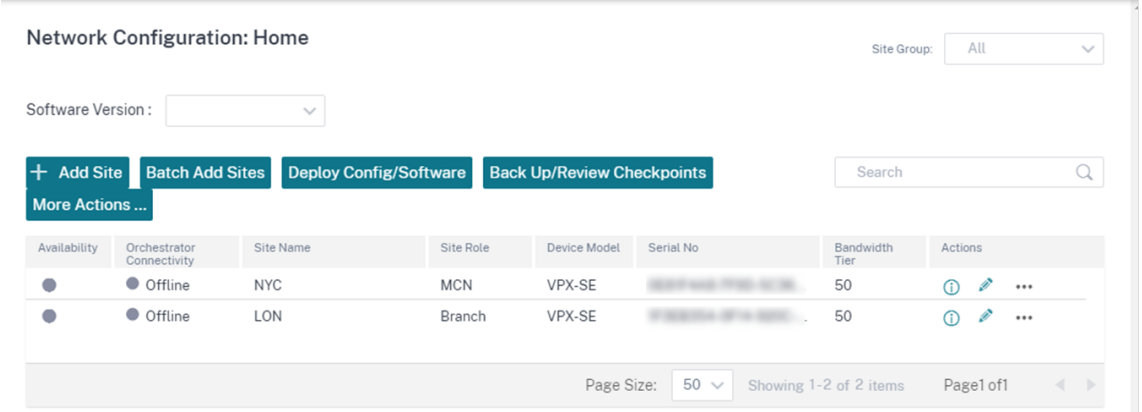
> **HINWEIS**
>
> Um Citrix SD-WAN Appliances mit den Softwareversionen 10.2.7, 11.1.1 oder 11.2.0 bereitzustellen, benötigen Sie Citrix SD-WAN Orchestrator für die lokale Version 11.1 oder höher.

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:

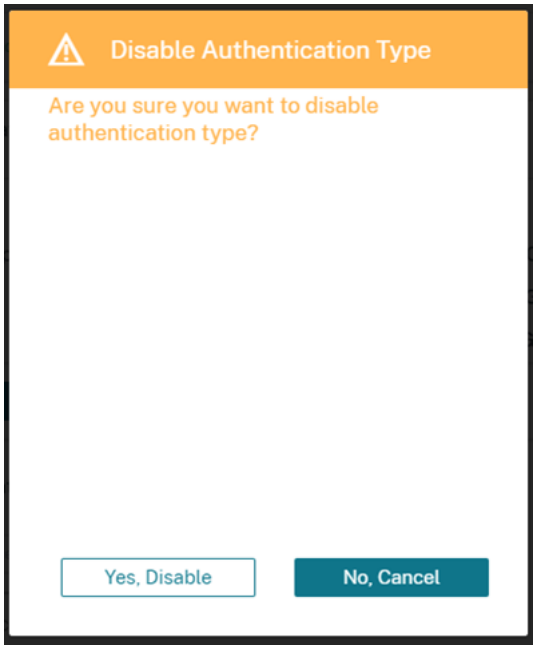
   a) Navigieren Sie zu **Konfiguration > Virtual WAN > On-Prem SD-WAN Orchestrator** und **aktivieren Sie das Kontrollkästchen On-Prem SD-WAN Orchestrator-Konnektivität** aktivieren.
   b) Geben Sie die IP-Adresse von Citrix SD-WAN Orchestrator für lokal ein.
   c) Klicken Sie auf **Einstellungen anwenden**.

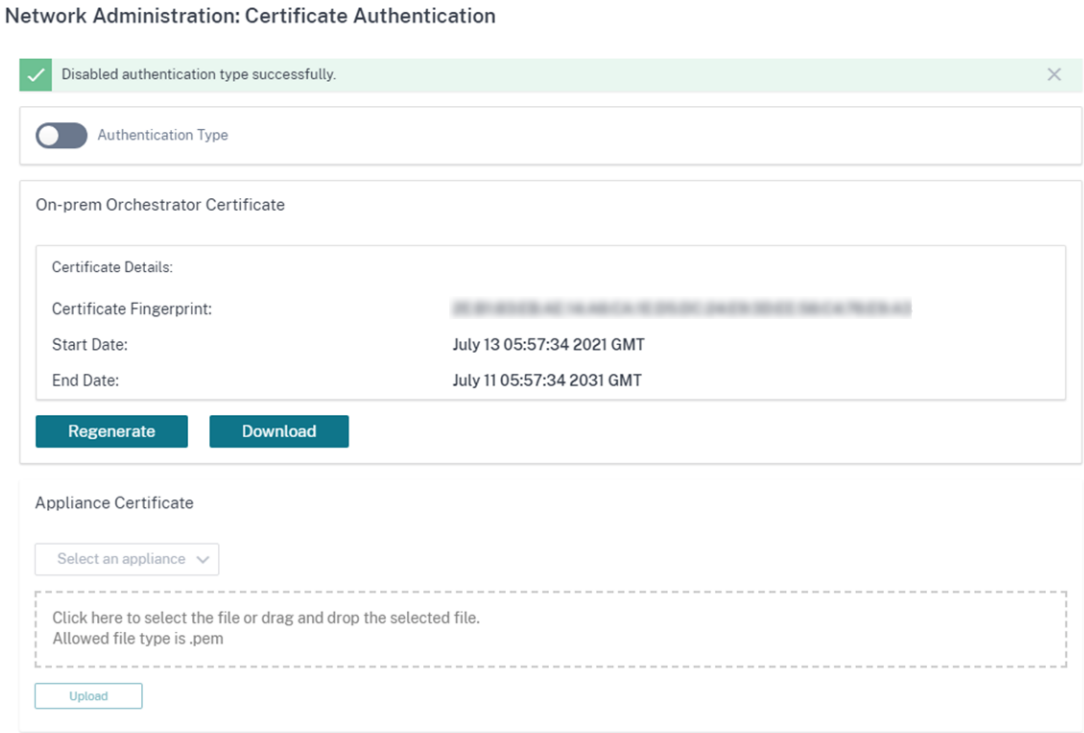


2. Melden Sie sich bei Citrix SD-WAN Orchestrator für die lokale Benutzeroberfläche an. Erstellen Sie eine Site und erstellen Sie die Konfiguration. Geben Sie die Seriennummer jeder Citrix SD-WAN-Appliance in der jeweiligen Site-Konfiguration ein. Speichern Sie die Konfiguration.

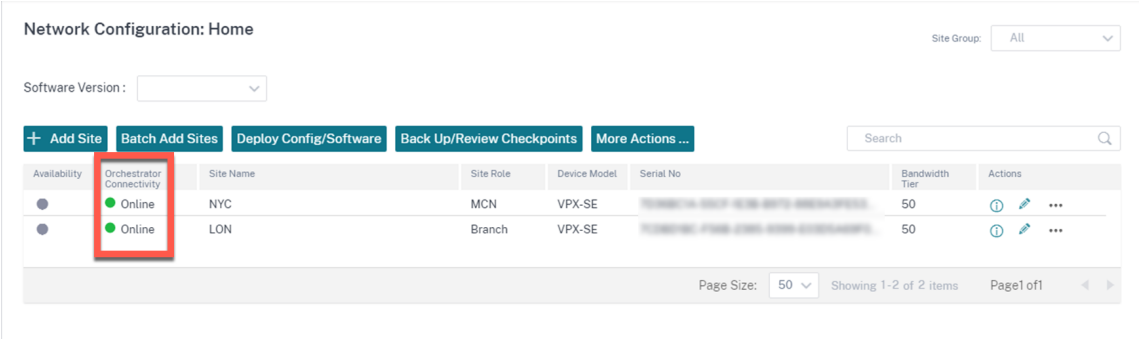


3. Navigieren Sie zu **Administration > Zertifikatauthentifizierung** und schalten Sie den Schalter **Authentifizierungstyp** auf **AUS**. Klicken Sie auf **Ja, Deaktivieren,** um das Pop-up "**Deaktivierter Authentifizierungstyp** "

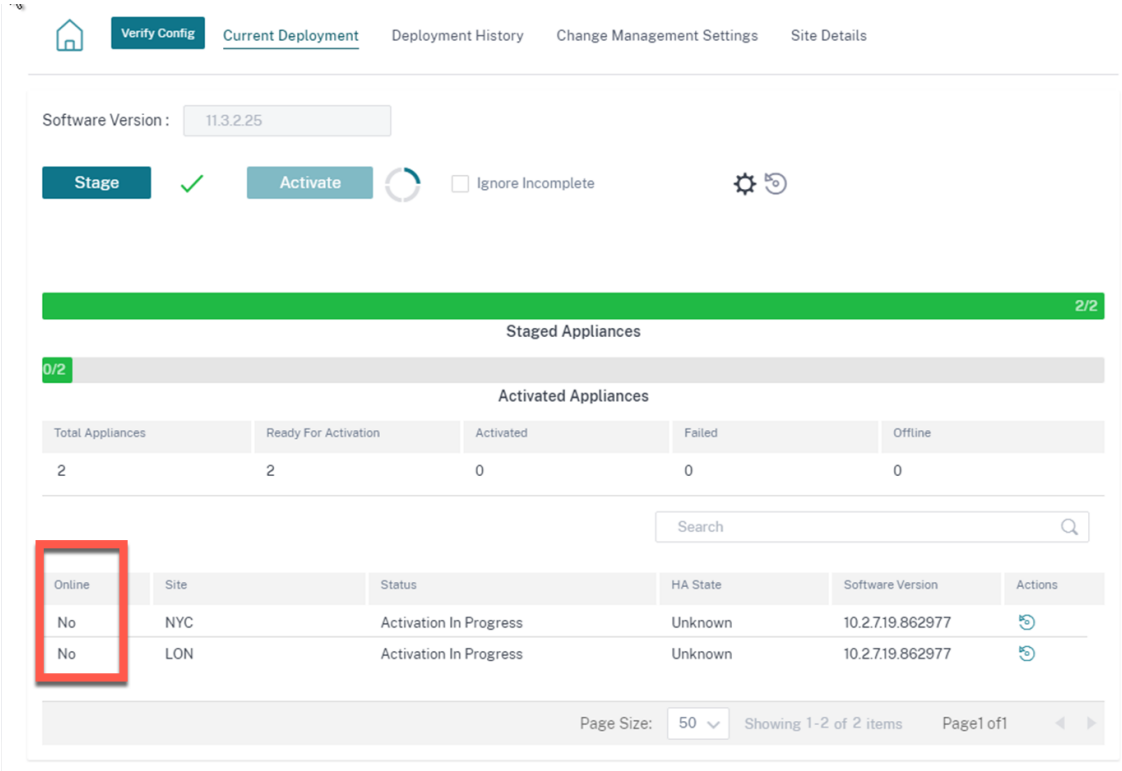




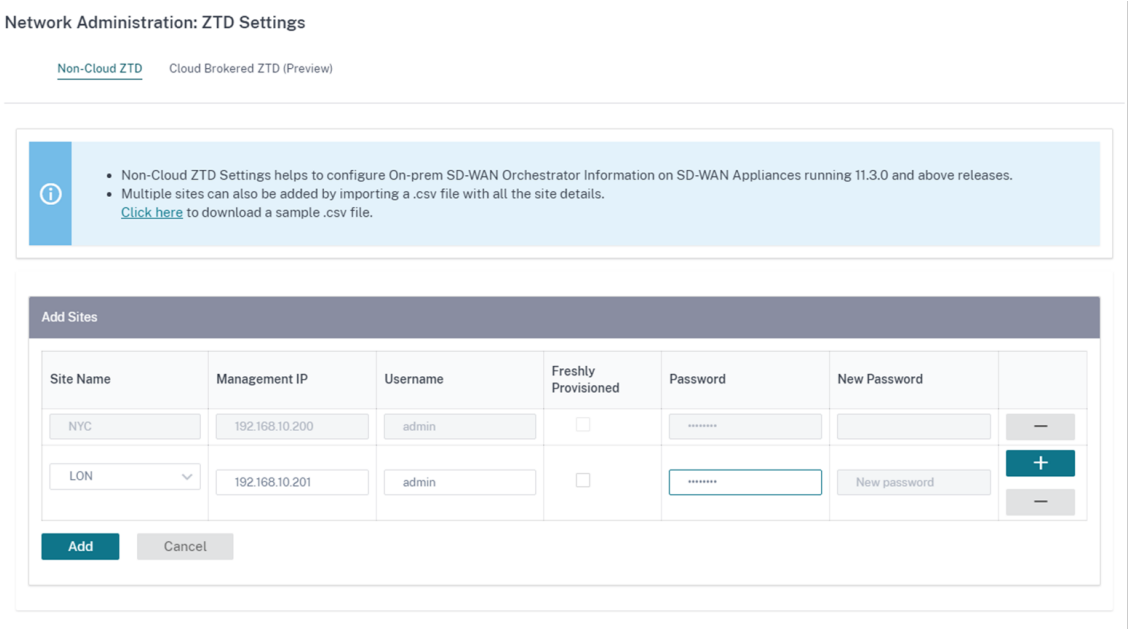
4. Auf der **Homepage Konfiguration > Netzwerkkonfiguration** werden SD-WAN-Appliances in der Spalte **Cloud-Konnektivität** als **Online** angezeigt. Dies ist auf die deaktivierte Zertifikatauthentifizierung auf Citrix SD-WAN Orchestrator für lokale und SD-WAN-Appliances zurückzuführen, die für Citrix 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.



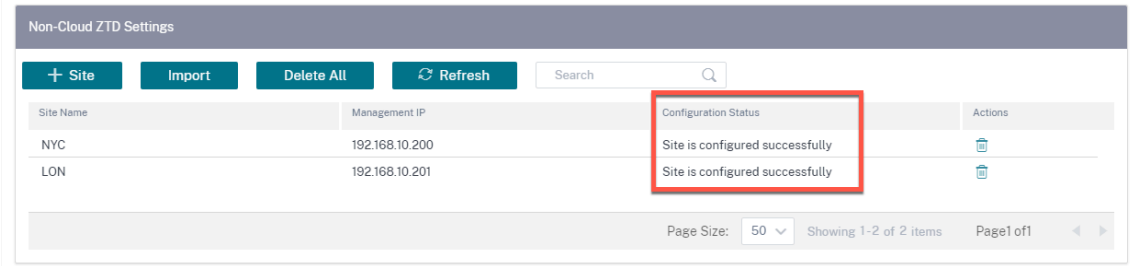
5. Wählen Sie eine veröffentlichte Softwareversion (11.3.0 oder höher) aus und klicken Sie auf **Konfiguration/Software bereitstellen**. Weitere Einzelheiten zur Auswahl der veröffentlichten Softwareversion finden Sie unter Software. **Stage** und **Activate** der Sites. Nach der Aktivierung zeigen die Geräte in der Spalte **Online** die Option **Nein** an.



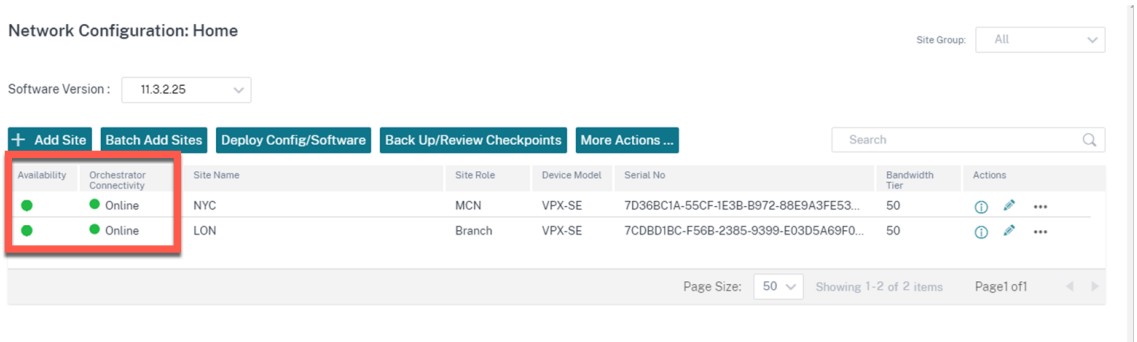
6. Navigieren Sie zu **Administration > ZTD-Einstellungen > Non-Cloud ZTD**. Klicken Sie auf **+Site** und fügen Sie eine Site hinzu. Geben Sie die Management-IP und die Anmeldeinformationen für jede Appliance ein. Klicken Sie auf **+**, um weitere Websites hinzuzufügen. Klicken Sie auf **Hinzufügen**.



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**.



8. Navigieren Sie zu **Homepage Configuration > Network Config**. Erfolgreich konfigurierte Sites werden in der Spalte **Orchestrator-Konnektivität** als **Online** angezeigt.



9. Gehen Sie genauso vor, um zusätzliche Websites hinzuzufügen. Die Durchführung der vorangegangenen Schritte hat keine Auswirkungen auf bestehende Standortbereitstellungen.

PPPoE-Sitzungen

October 28, 2021

PPPoE (Point to Point Protocol over Ethernet) verbindet mehrere Computerbenutzer in einem Ethernet-LAN mit einem Remotestandort über gängige Appliances, 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 üblicherweise in DFÜ-Verbindungen verwendet wird, mit dem Ethernet-Protokoll, das mehrere Benutzer in einem LAN unterstützt. Die PPP-Protokollinformationen sind in einem Ethernet-Frame gekapselt.

Citrix SD-WAN-Appliances verwenden PPPoE zur Unterstützung von Internetdienstanbietern (Internet Service Provider, ISP), um fortlaufende und kontinuierliche DSL- und Kabelmodemverbindungen im Gegensatz zu DFÜ-Verbindungen zu haben. PPPoE bietet jeder Benutzer-Remotestandortsitzung die Möglichkeit, die Netzwerkadressen des anderen durch einen ersten Austausch namens “Discovery” zu erfahren. Nachdem eine Sitzung zwischen einem einzelnen Benutzer und dem Remotestandort, beispielsweise einem ISP-Anbieter, eingerichtet wurde, kann die Sitzung überwacht werden. Unternehmen nutzen gemeinsam genutzten Internetzugang über DSL-Leitungen mit 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.

Folgendes ist erforderlich, um erfolgreiche PPPoE-Sitzungen einzurichten:

- Konfigurieren Sie die virtuelle Netzwerkschnittstelle (VNI).
- Eindeutige Anmeldeinformationen für die Erstellung einer PPPoE-Sitzung.
- Konfigurieren Sie WAN-Verbindung. Für jedes VNI kann nur eine WAN-Verbindung konfiguriert sein.
- 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 Schnittstellengruppe.

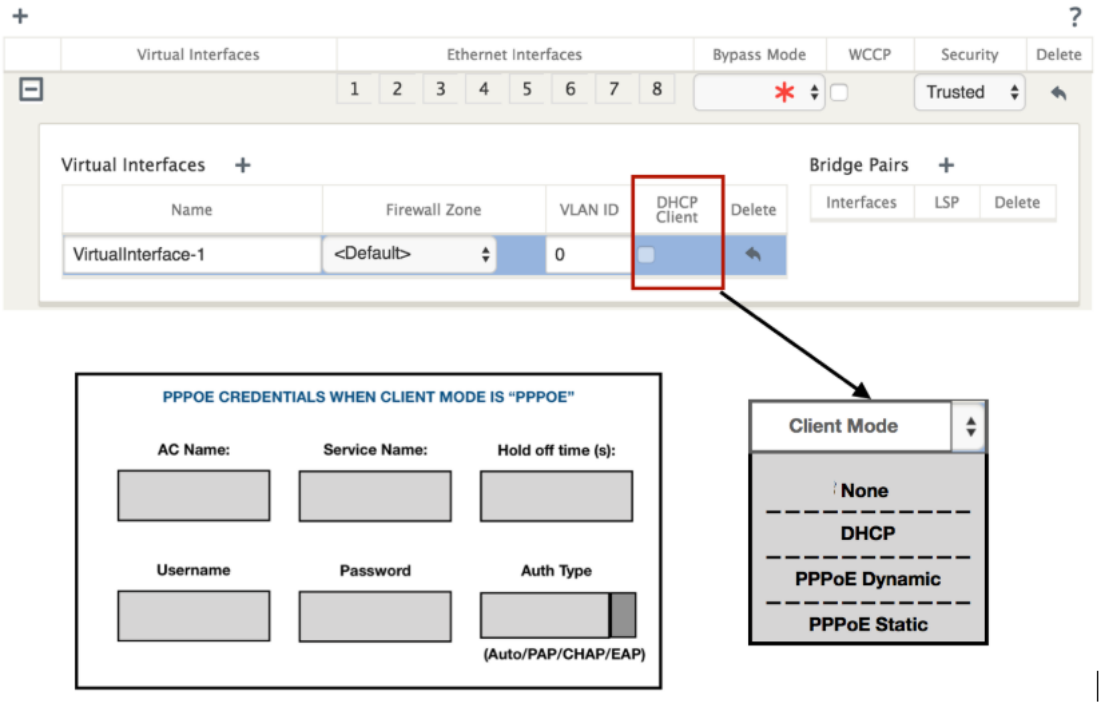
> **Hinweis**:
>
> Mehrere VNIs dürfen mit demselben 802.1Q VLAN-Tag erstellen.

Einschränkungen für die PPPoE-Konfiguration:

- 802.1q VLAN-Tagging wird nicht unterstützt.
- Die EAP-TLS-Authentifizierung wird nicht unterstützt.
- Adress-/Steuerungskomprimierung.
- Entleeren Sie die Kompression.
- Verhandlung über Protokoll-Feld-Komprimierung
- Protokoll zur Kompressionssteuerung.
- BSD Kompression komprimieren.
- IPv6- und IPX-Protokolle.
- PPP Multilink.
- TCP/IP-Header-Kompression im Van Jacobson-Stil.
- Verbindungs-ID-Komprimierungsoption in Van Jacobson-Stil TCP/IP-Header-Komprimierung.
- PPPoE wird auf LTE-Schnittstellen nicht unterstützt

Ab der Citrix SD-WAN 11.3.1-Version wird ein zusätzlicher 8-Byte-PPPoE-Header für die Anpassung der TCP-Maximal-Segmentgröße (MSS) berücksichtigt. Der zusätzliche 8-Byte-PPPoE-Header passt den MSS in den Synchronisierungspaketen basierend auf der MTU an.

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

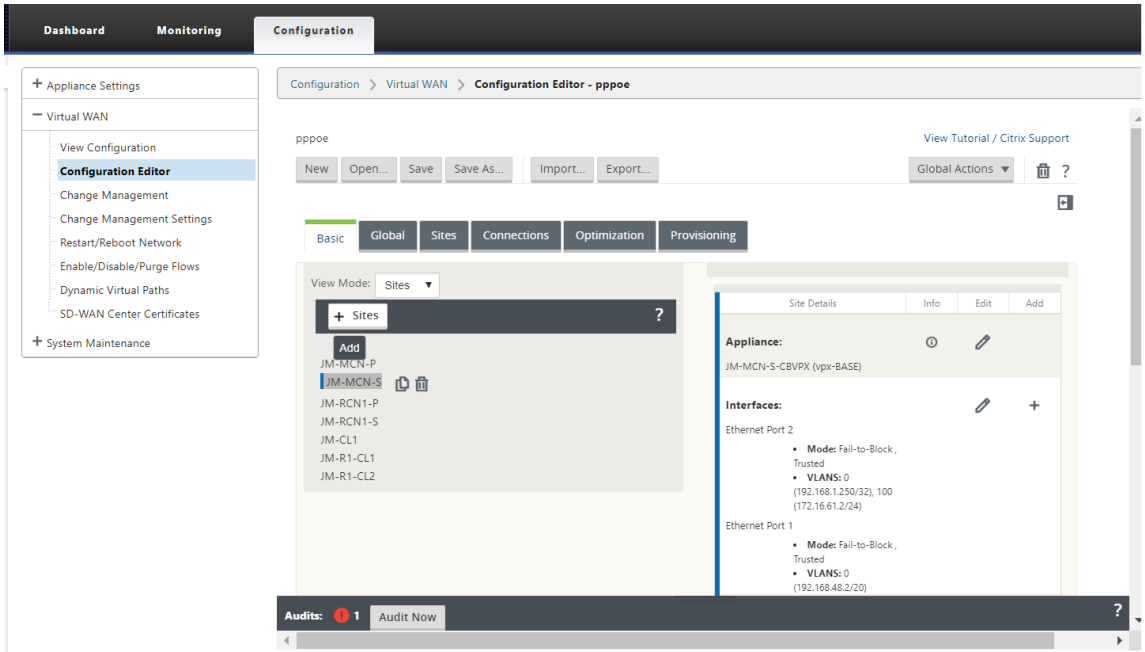
- –
- PPPoE Static

Branch

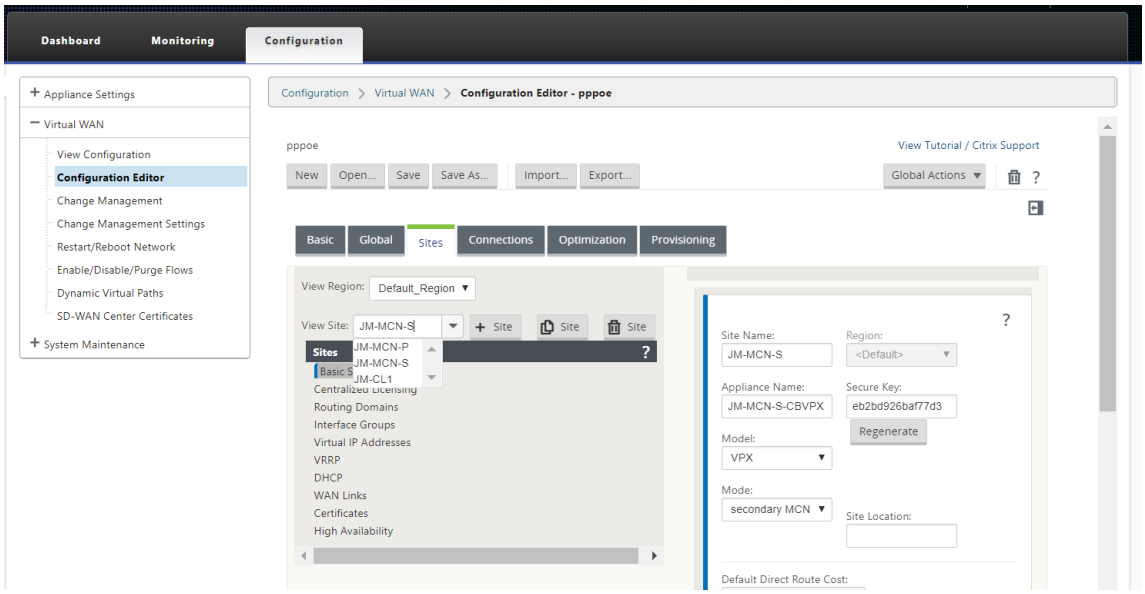
- –
- PPPoE Static
- PPPoE dynamisch
- DHCP

Konfigurieren der MCN-Einheit

1. Navigieren Sie in der GUI der SD-WAN MCN Appliance zu **Konfiguration** > **Virtuelles WAN** > **Konfigurationseditor**. Fügen Sie eine Site unter der Registerkarte **Basic** hinzu. Weitere Informationen finden Sie in der Konfiguration von Zweigknoten unter, konfigurieren MCN.



2. Öffnen Sie nach dem Erstellen der neuen Website die Registerkarte **Sites** . Wählen Sie die neu erstellte Website aus der Dropdownliste **Site anzeigen** aus.

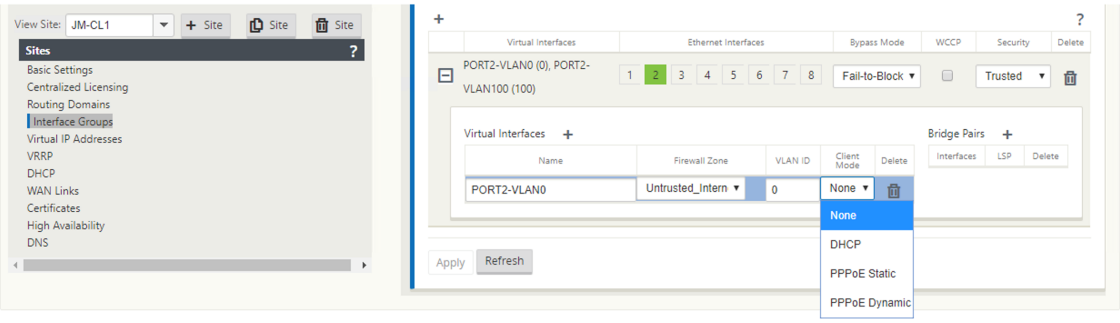


3. Wählen Sie **Schnittstellengruppen** für den MCN-Site aus. Führen Sie folgende Schritte aus:

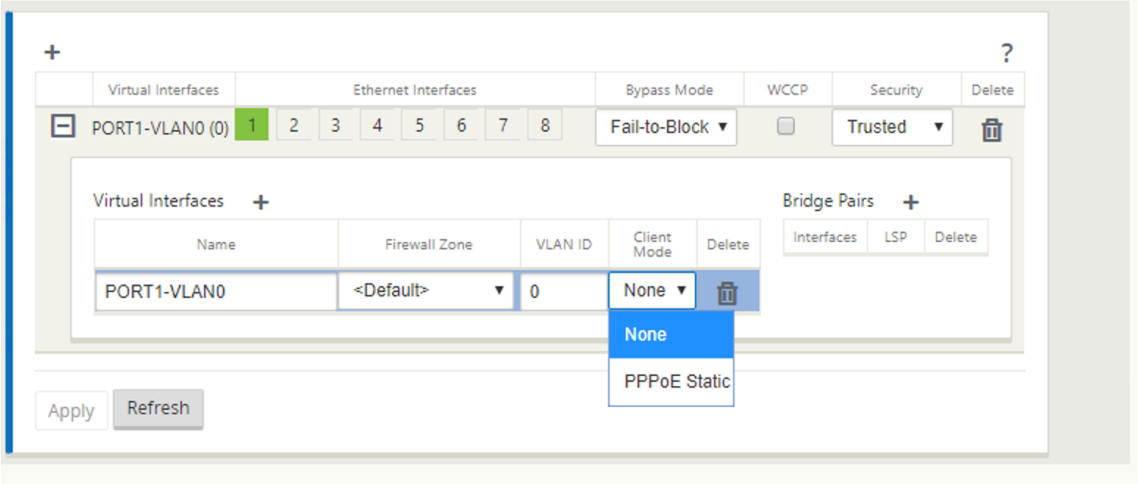
   - Fügen Sie virtuelle Schnittstellen hinzu.
   - Konfiguration von Ethernet-Schnittstellen.
   - Konfigurieren Sie den Bypass-Modus.
   - Entscheiden Sie sich bei Bedarf für **WCCP**.
   - Wählen Sie Sicherheit —Vertrauenswürdig/Nicht vertrauenswürdig.

   Für virtuelle Schnittstelle:

- Konfigurieren Sie den Namen, die Firewallzone, die VALN-ID und den Clientmodus.
- 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.

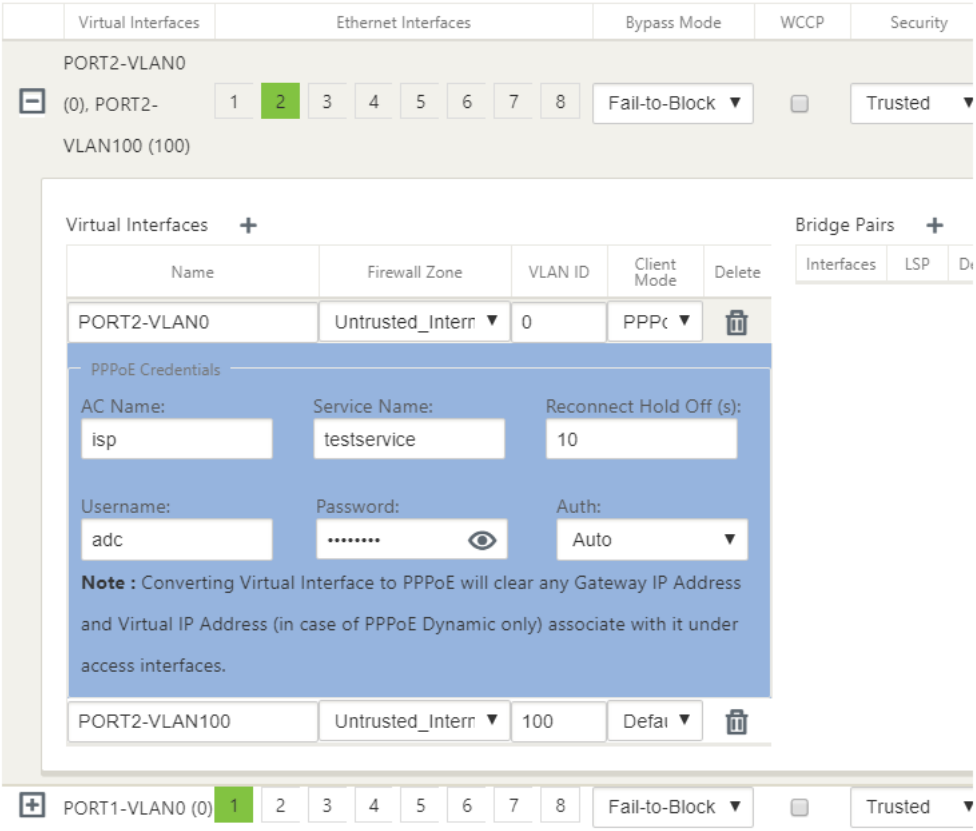


Konfigurieren Sie die folgenden PPPoE-Parameter, und klicken Sie auf **Übernehmen**.

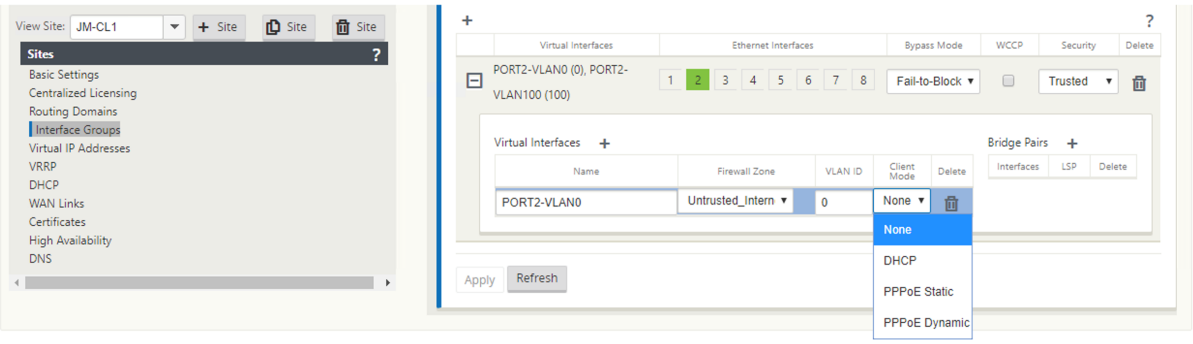
- Zugriff auf das Namensfeld des Konzentrators (AC).
- Service Name:
- Hold-Off-Wiederverbindungszeit (Standard ist die sofortige Wiederverbindung, ‘0’)
- Authentifizierungstyp - (AUTO/PAP/CHAP/EAP).
  - Wenn die Option Auth auf Auto festgelegt ist, berücksichtigt die SD-WAN-Appliance die vom Server empfangene Anforderung des unterstützten Authentifizierungsprotokolls.

  - Wenn die Option Auth auf PAP/CHAP/EAP eingestellt ist, werden nur bestimmte Authentifizierungsprotokolle berücksichtigt. Wenn sich PAP in der Konfiguration befindet und der Server eine Authentifizierungsanfrage 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.



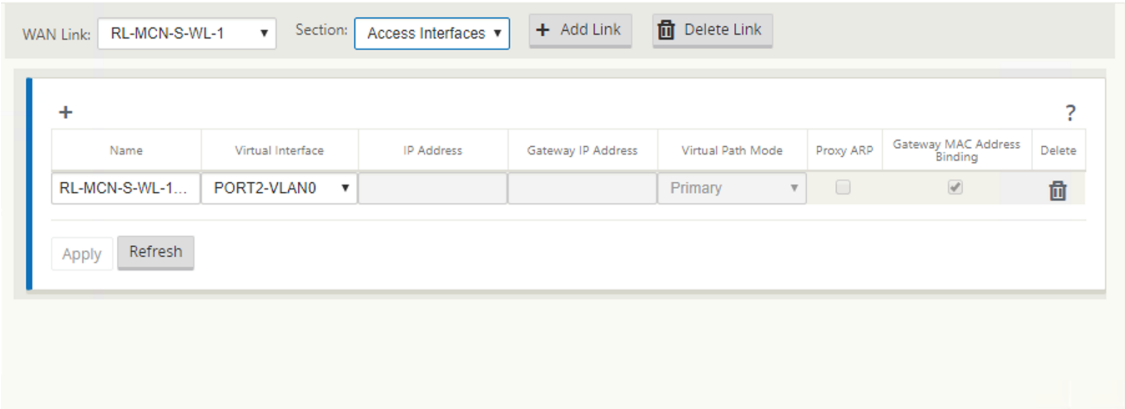
Die folgende Abbildung zeigt die PPPoE-Clientmodus-Optionen für eine Zweig-SD-WAN-Appliance. Wenn PPPoE Dynamic ausgewählt ist, muss der VNI “Nicht vertrauenswürdig”sein.



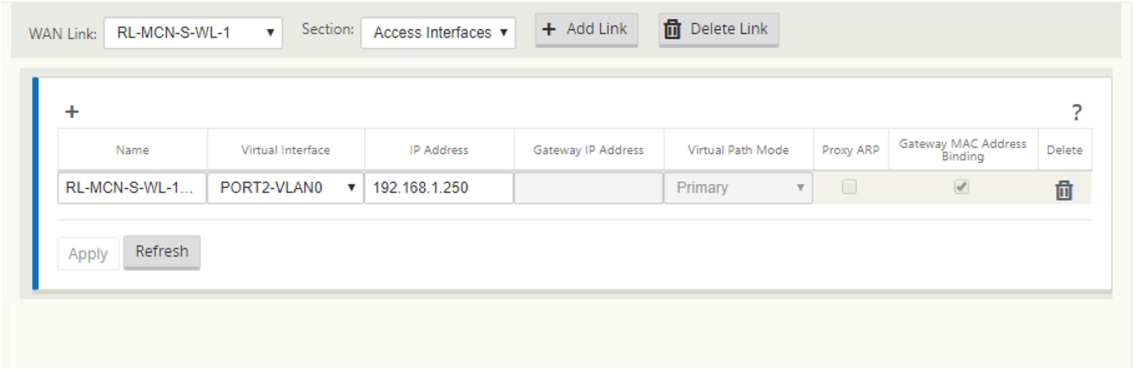
Konfigurieren von WAN-Verbindungen

1. Navigieren Sie in der SD-WAN-GUI zu **Sites > WAN-Links**. Pro statischem oder dynamischem PPPoE-VNI ist nur eine WAN-Link-Erstellung zulässig. Die WAN-Verbindungskonfiguration hängt von der VNI-Auswahl des Clientmodus ab.
2. Wenn der VNI mit dem dynamischen PPPoE-Clientmodus konfiguriert ist:
   - IP-Adress- und Gateway-IP-Adressfelder werden inaktiv.
   - Der virtuelle Pfadmodus 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.



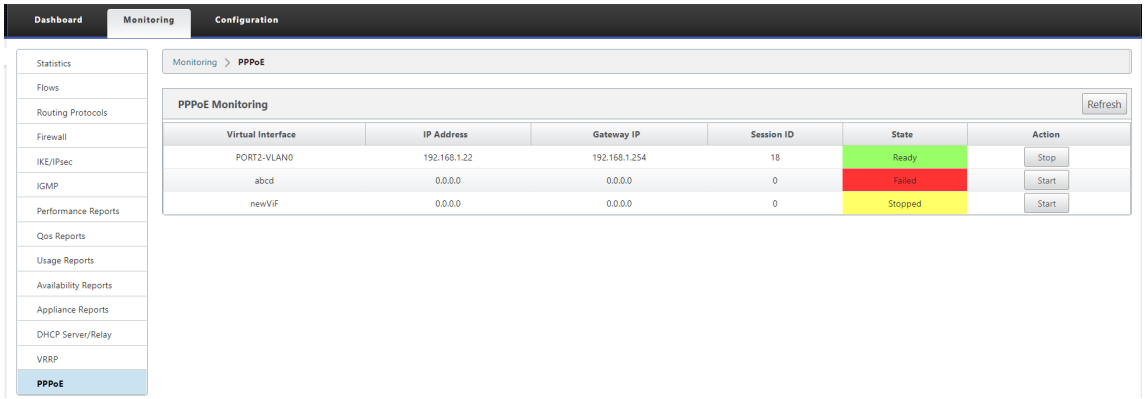
> **Hinweis**:
>
> Wenn der Server die konfigurierte statische IP-Adresse nicht einhält und eine andere IP-Adresse anbietet, tritt ein Fehler auf. Die PPPoE-Sitzung versucht, die Verbindung in regelmäßigen Abständen wiederherzustellen, bis der Server die konfigurierte IP-Adresse akzeptiert.

Überwachen Sie PPPoE-Sitzungen

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-Clientmodus. Es ermöglicht Ihnen, die Sitzungen zur Fehlerbehebung manuell zu starten oder zu beenden.

- Wenn der VNI betriebsbereit ist, zeigen die **IP- und Gateway-IP-Spalten** die aktuellen Werte in der Sitzung an. Es zeigt an, dass es sich um kürzlich empfangene Werte handelt.
- Wenn der VNI gestoppt ist oder sich im Status “fehlgeschlagen”befindet, sind die Werte zuletzt empfangene 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.



In der Spalte **Status** wird der Status der PPPoE-Sitzung mit drei Farbcodes angezeigt: Grün, Rot, Gelb und Werte. In der folgenden Tabelle werden Status und Beschreibungen erklärt. Sie können mit der Maus über den Status gehen, um Beschreibungen zu erhalten.

PPPoE-Sitzungstyp	Farbe	Beschreibung
Konfiguriert	Gelb	Ein VNI ist mit PPPoE konfiguriert. Dies ist ein Ausgangszustand.
Dialing	Gelb	Nachdem ein VNI konfiguriert wurde, wechselt der PPPoE-Sitzungsstatus in den Wählzustand, indem die PPPoE-Erkennung gestartet wird. Paketinformationen werden erfasst.
Sitzung	Gelb	VNI wird vom Ermittlungsstatus in den Sitzungsstatus verschoben. Wartet auf den Empfang von IP, wenn dynamisch oder wartet auf Bestätigung vom Server für die angekündigte IP, wenn statisch.
Bereit	grün	IP-Pakete werden empfangen und VNI und die zugehörige WAN-Verbindung sind einsatzbereit.

PPPoE-Sitzungstyp	Farbe	Beschreibung
Fehlgeschlagen	rot	PPP/PPPoE-Sitzung wird beendet. Der Grund für den Fehler kann auf eine ungültige Konfiguration oder einen schwerwiegenden Fehler zurückzuführen sein. Die Sitzung versucht nach 30 Sekunden wieder eine Verbindung herzustellen.
Beendet	gelb	PPP/PPPoE-Sitzung wird manuell gestoppt.
Kündigung	gelb	Ein Zwischenzustand, der aus einem bestimmten Grund endet. Dieser Zustand beginnt automatisch nach einer bestimmten Dauer (5 Sekunden für normalen Fehler oder 30 Sekunden für einen schwerwiegenden Fehler).
Deaktiviert	gelb	Der SD-WAN-Dienst ist deaktiviert.

Fehlerbehebung bei PPPoE-Sitzungsfehlern

Wenn auf der Seite Überwachung ein Problem beim Einrichten einer PPPoE-Sitzung auftritt:

- Wenn Sie mit der Maus über den Status “Fehlgeschlagen”fahren, wird der Grund für den jüngsten Fehler angezeigt.
- Um eine neue Sitzung einzurichten oder um eine aktive PPPoE-Sitzung zu beheben, verwenden Sie die Seite Monitoring->PPPoE und starten Sie die Sitzung neu.
- Wenn eine PPPoE-Sitzung manuell gestoppt wird, kann sie erst gestartet werden, wenn sie manuell gestartet und eine Konfigurationsänderung aktiviert wurde oder der Dienst neu gestartet wurde.

Eine PPPoE-Sitzung kann aus folgenden Gründen fehlschlagen:

- Wenn SD-WAN sich aufgrund eines falschen Benutzernamens/Kennworts in der Konfiguration nicht beim Peer authentifiziert.

- Die PPP-Verhandlung schlägt fehl - die Verhandlung erreicht nicht den Punkt, an dem mindestens ein Netzwerkprotokoll ausgeführt wird.
- Problem mit Systemspeicher oder Systemressourcen.
- Ungültig/schlechte Konfiguration (falscher AC-Name oder Dienstname).
- Die serielle Port konnte aufgrund eines Betriebssystemfehlers nicht geöffnet werden.
- Für die Echo-Pakete wurde keine Antwort erhalten (Link ist schlecht oder der Server reagiert nicht).
- Es gab mehrere ununterbrochene erfolglose Wählsitzungen in einer Minute.

Nach 10 aufeinanderfolgenden Ausfällen wird der Grund für das Scheitern beobachtet.

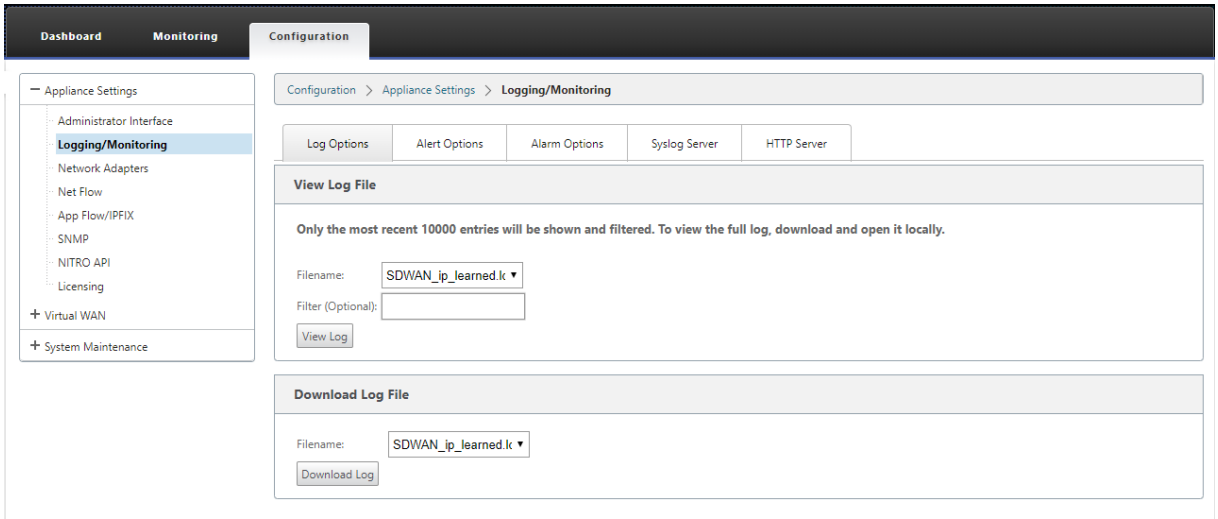
- Wenn der Fehler normal ist, wird er sofort neu gestartet.
- Wenn der Fehler ein Fehler ist, wird der Neustart für 10 Sekunden zurückgesetzt.
- Wenn der Fehler schwerwiegend ist, wird der Neustart vor dem Neustart für 30 Sekunden zurückgesetzt.

LCP-Echo-Anforderungspakete werden alle 60 Sekunden von SD-WAN generiert, und das Nichtempfangen von 5 Echoantworten wird als Verbindungsfehler angesehen und stellt die Sitzung wieder her.

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** > **Protokollierung/Überwachung** > **Protokolloptionen**. Zeigen Sie die Datei *SDWAN_IP_Learned.log an oder laden Sie* sie herunter.



Qualität der Dienstleistung

October 28, 2021

Das Netzwerk zwischen Bürostandorten und dem Rechenzentrum oder der Cloud muss eine Vielzahl von Anwendungen und Daten transportieren, einschließlich hochwertiger Video- oder Echtzeit-Sprache. Bandbreitensensitive Anwendungen erweitern die Fähigkeiten und Ressourcen des Netzwerks. Citrix SD-WAN bietet garantierte, sichere, messbare und vorhersehbare Netzwerkdienste. Dies wird erreicht, indem Verzögerung, Jitter, Bandbreite und Paketverlust im Netzwerk verwaltet werden.

Die Citrix SD-WAN-Lösung umfasst eine ausgeklügelte Application Quality of Service (QoS) -Engine, die auf den Anwendungsverkehr 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-Adress-/Port-basierten QoS finden Sie unter Regeln nach Anwendungsnameund Regeln nach IP-Adresse bzw. Portnummer.

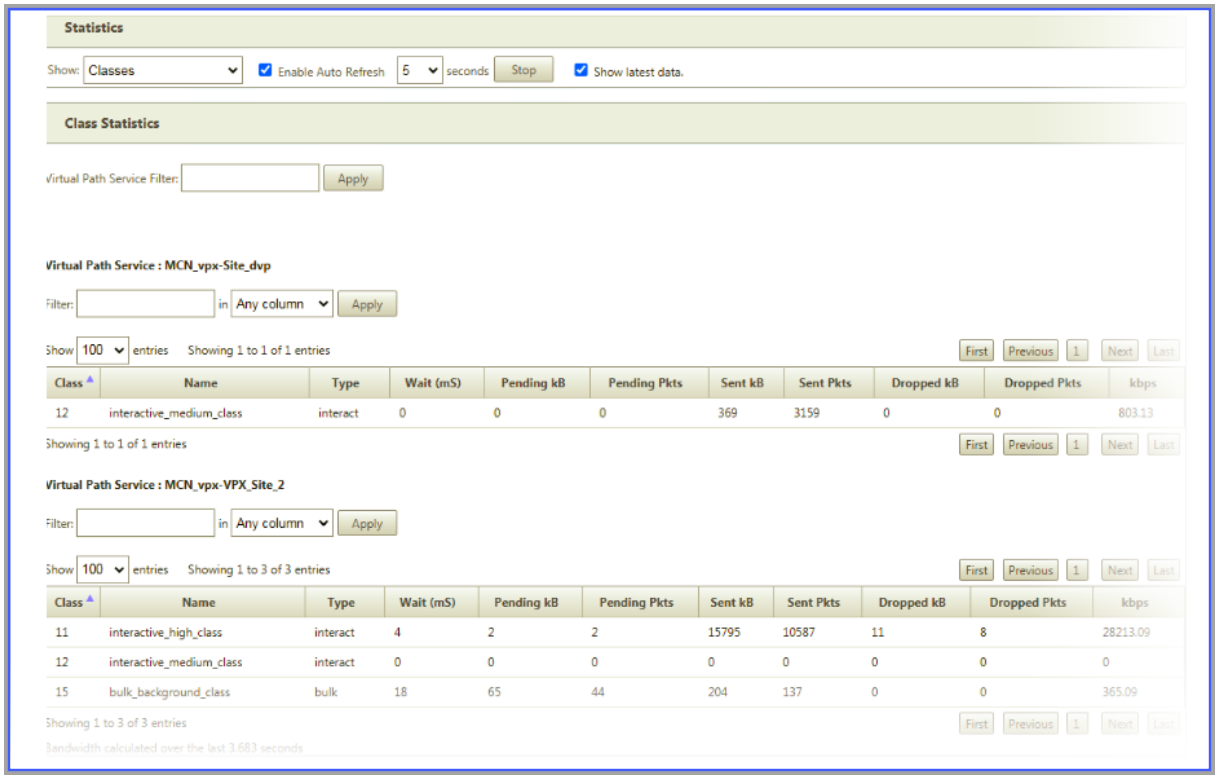
Das SD-WAN bietet 17 Klassen (IDs: 0—16). Es folgt die Standardkonfiguration aller 17 Klassen.

Virtual Path Default Set: New_Default_Set-1 Section: Classes + Add Default Set Delete Default Set

ID	Name	Type	Initial Period	Initial Rate	Initial %/Kbps	Initial Share %	Sustained Rate	Sustained Share %	Reset
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

Citrix SD-WAN zeigt nur die Klassen an, bei denen der Datenverkehr auf virtuellen Pfaden und dynamischen virtuellen Pfaden fließt. Wenn eine Klasse angezeigt wird und 0 als Wert anzeigt, bedeutet dies, dass der zuvor fließende Verkehr jetzt gestoppt wurde. Wenn jedoch eine Klasse überhaupt nicht angezeigt wird, bedeutet dies, dass für diese Klasse nie ein Verkehrsfluss erfolgt ist, da der Status des virtuellen Pfaddienstes zurückgesetzt wurde (z. B. Softwareupgrade oder Neustart).



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 Massenklasse 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 **Klassen**aus.

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

October 28, 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-Konfigurationseditor 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 **Regeln** aus und klicken Sie auf **+**.
3. Geben Sie im Feld **Reihenfolge** den Auftragswert ein, um festzulegen, 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, um mit dem Datenverkehr übereinzustimmen.
- **Ziel-IP-Adresse**: Ziel-IP-Adresse und Subnetzmaske, um mit dem Datenverkehr übereinzustimmen.

  > **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, um mit dem Verkehr übereinzustimmen.
- **Zielport**: Ziel-Portnummer oder Portbereich, um mit dem Verkehr übereinzustimmen.

  > **Hinweis**
  >
  > Wenn das Kontrollkästchen **Dest=Src** aktiviert ist, wird der Quellport auch für den Zielport verwendet.

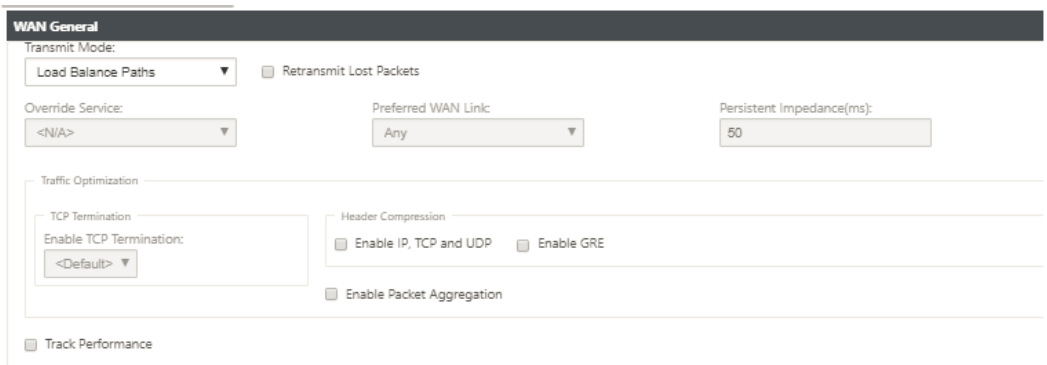
- **DSCP**: Das **DSCP-Tag**im IP-Header, das mit dem Datenverkehr übereinstimmt.
- **VLAN**: Die **VLAN-ID**, die mit dem Datenverkehr übereinstimmt.

7. Klicken Sie neben der neuen Regel auf das Symbol “Hinzufügen”(+).
8. Klicken Sie auf **Eigenschaften mithilfe des Protokolls** 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 General**, um die folgenden Eigenschaften zu konfigurieren.
   - **Übertragungsmodus**: Wählen Sie einen der folgenden Übertragungsmodi aus.
     - **Load Balance-Pfad**: Der Verkehr für den Fluss wird über mehrere Pfade für den Dienst ausgeglichen. Der Datenverkehr wird über den besten Pfad gesendet, bis dieser Pfad verwendet wird. Übleibspakete werden über den nächstbesten Pfad gesendet.
     - **Persistenter Pfad**: Der Verkehr für den Fluss bleibt auf demselben Pfad, bis der Pfad nicht mehr verfügbar ist.
     - **Pfad duplizieren**: Der Verkehr für den Fluss wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht.
     - **Dienst außer Kraft setzen**: Der Verkehr für den Fluss wird zu einem anderen Dienst überschrieben. 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.
- **IP, TCP und UDP aktivieren**: Komprimieren Sie Header in IP-, TCP- und UDP-Paketen.

  > **HINWEIS**
  >
  > IPv6-Pakete unterstützen keine Header-Komprimierung.

- **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).

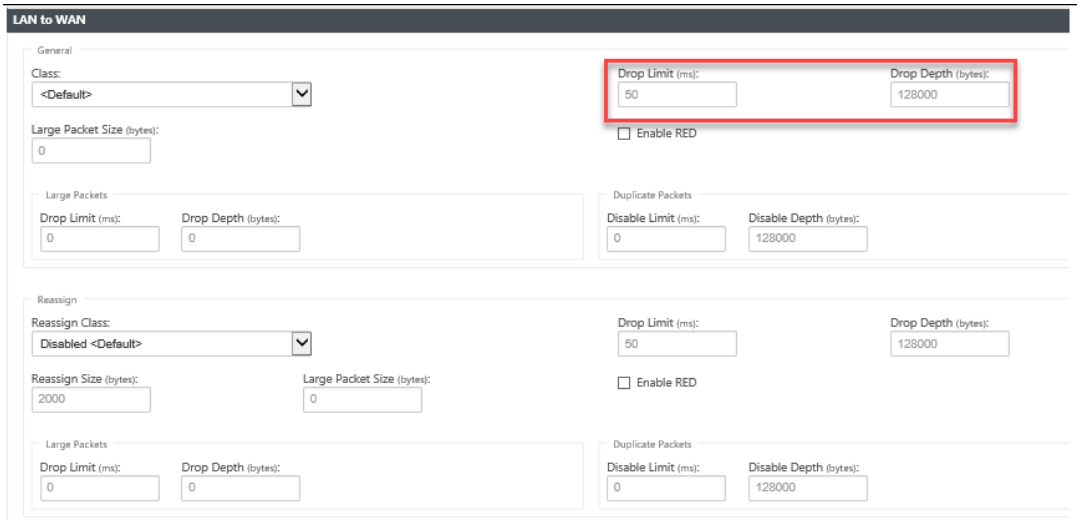


10. Klicken Sie auf die Kachel **LAN-zu-WAN**, um das LAN-zu-WAN-Verhalten für diese Regel zu konfigurieren.

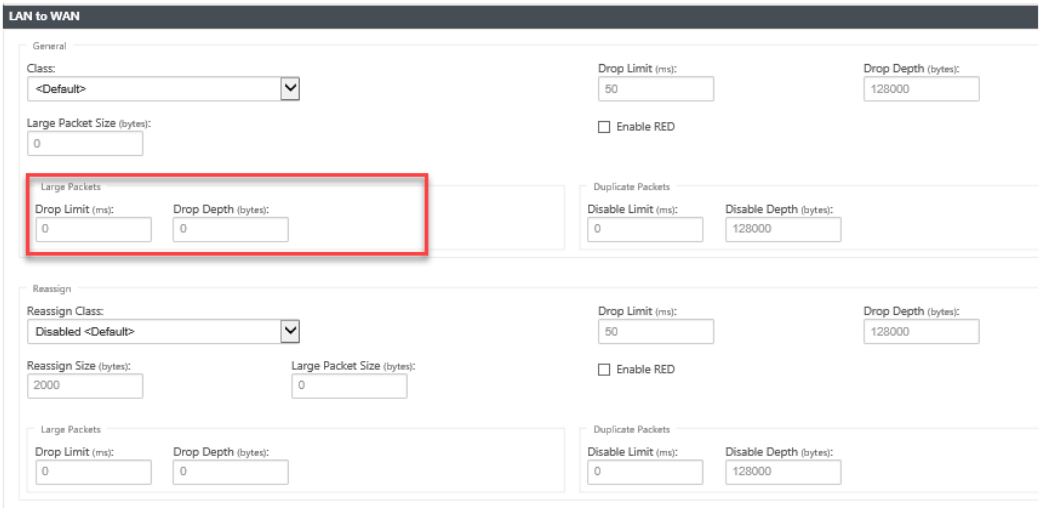
    - **Klasse**: Wählen Sie eine Klasse aus, der diese Regel zugeordnet werden soll.

      > **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.

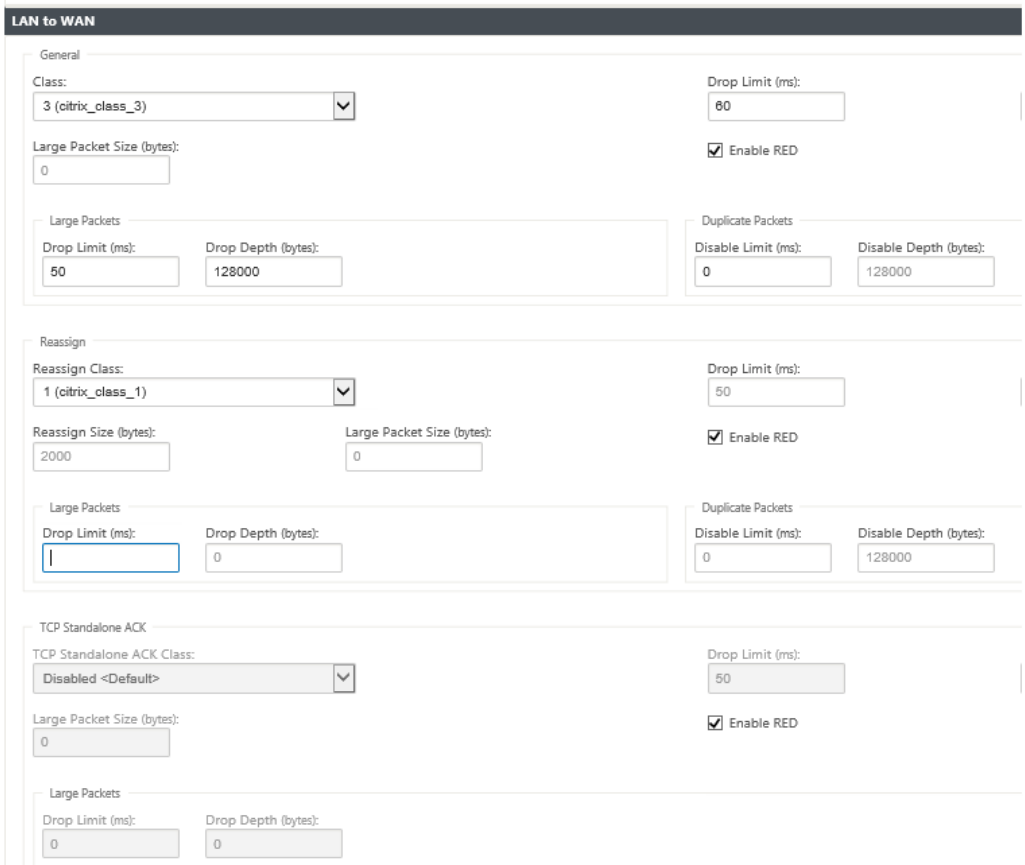


Pakete, die größer als diese Größe sind, werden den Werten zugewiesen, die in den Standardfeldern **Drop Limit** und **Drop Depth** im Abschnitt **Große Pakete** des Bildschirms angegeben sind.



- **Drop-Limit**: Länge der Zeit, nach der Pakete, die im Klassenplaner warten, gelöscht werden. Gilt nicht für eine Massenklasse.
- **Drop-Tiefe**: Schwellenwert für die Warteschlangentiefe, nach dem Pakete verworfen werden.
- **RED aktivieren**: Random Early Detection (RED) gewährleistet eine faire gemeinsame Nutzung von Klassenressourcen, indem Pakete verworfen werden, wenn eine Überlastung auftritt.

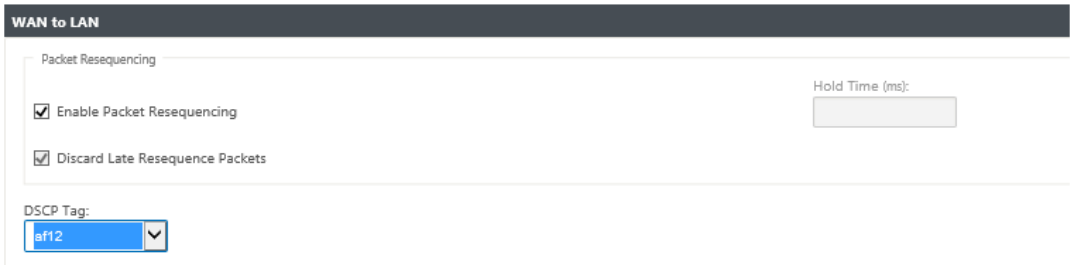
- **Größe neu zuweisen**: Paketlänge, die bei Überschreitung bewirkt, dass das Paket der im Feld Klasse neu zuweisen angegebenen Klasse neu zugewiesen wird.
- Klasse**neu zuweisen: Klasse**, die verwendet wird, wenn die Paketlänge die im Feld Größe neu zuweisen angegebene Paketlänge überschreitet.
- **Deaktivierungslimit**: Zeit, für 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.
- **TCP-Standalone-ACK-Klasse**: Klasse mit hoher Priorität, der TCP-Standalone-Bestätigungen bei großen Dateiübertragungen zugeordnet werden.



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 zur erneuten Sequenzierung gehalten werden, nach dem die Pakete an das LAN gesendet werden.

- **Verwerfen Sie Pakete mit später Neusequenzierung**: Verwerfen Sie Pakete außerhalb der Reihenfolge, die eintrafen, nachdem die für die erneute Sequenzierung benötigten 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.



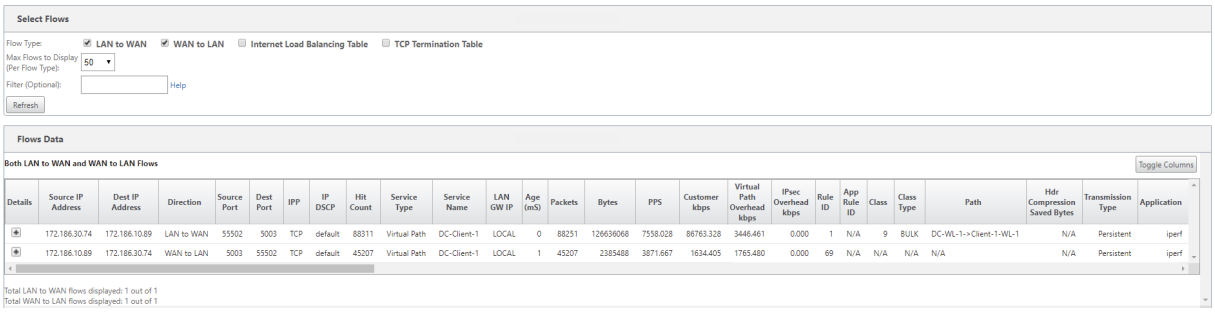
12. Klicken Sie auf **Deep Packet Inspection** (Deep Packet Inspection), und wählen Sie **Passive FTP-Erkennung aktivieren** (Enable Passive FTP-Erkennung), damit die Regel den für die FTP-Datenübertragung verwendeten Port erkennt und die Regeleinstellungen automatisch auf
13. Klicken Sie auf **Apply**.

> **Hinweis**
>
> Speichern Sie die Konfiguration, exportieren Sie sie in den Posteingang der Änderungsverwaltung und starten Sie den Änderungsverwaltungsprozess.

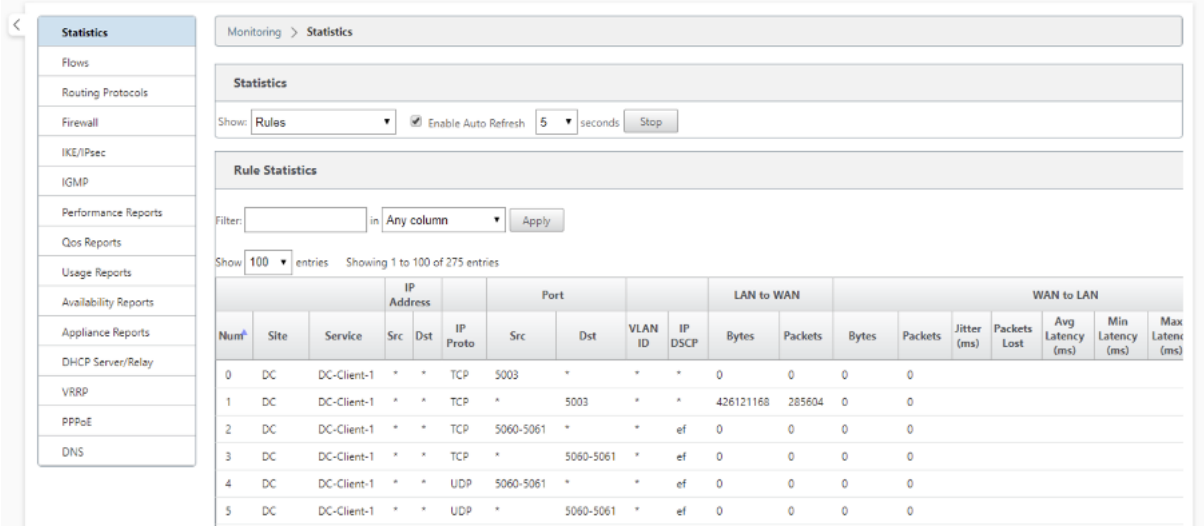
Regeln überprüfen

Navigieren Sie im Konfigurationseditor 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.



Navigieren Sie im Konfigurationseditor zu **Monitoring > Statistiken** und überprüfen Sie die konfigurierten Regeln.



Regeln nach Anwendungsname

October 28, 2021

Mit der Anwendungsklassifizierungsfunktion kann die Citrix SD-WAN-Appliance eingehenden Datenverkehr analysieren und als zu einer bestimmten Anwendung oder Anwendungsfamilie gehörend klassifizieren. Diese Klassifizierung ermöglicht es uns, die QoS einzelner Anwendungen oder Anwendungsfamilien zu verbessern, indem Anwendungsregeln erstellt und angewendet werden.

Sie können Verkehrsflüsse basierend auf Anwendungs-, Anwendungsfamilien- oder Anwendungsobjekt-Übereinstimmungstypen filtern und Anwendungsregeln auf sie anwenden. Die Anwendungsregeln ähneln den IP-Regeln (Internet Protocol). Weitere 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 Anwendungsverkehr für den Flow wird über mehrere Pfade verteilt. 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 Anwendungsverkehr bleibt 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 Klassen anpassen.

Standardmäßig sind die folgenden fünf vordefinierten Anwendungsregeln für Citrix ICA-Anwendungen verfügbar:

Regel	Klasse	Übertragungsmodus	Übertragen Sie verlorene Pakete	Paketaggregation aktivieren	Aktivieren Paket-Neusequenzierung	Haltezeit neu angeordnen (ms)	Späte Wiedersequenzierung von Paketen verwerfen	Drop-Limit (ms)	Drop-Tiefe (Byte)	RED aktivieren	Deaktivieren Sie Limit (ms)	Deaktivieren Sie Tiefe (Byte)
HDX_Priority_0	0 (HDX_priority_tag_0)	Lastausgleich	Teilen	False	True	250	True	350	30000	True	0	128000
HDX_Priority_1	1 (HDX_priority_tag_1)	Lastausgleich	Teilen	False	True	250	True	350	30000	True	0	128000
HDX_Priority_2	2 (HDX_priority_tag_2)	Lastausgleich	Teilen	False	True	250	True	350	30000	True	0	128000
HDX_Priority_3	3 (HDX_priority_tag_3)	Lastausgleich	Teilen	False	True	250	True	350	30000	True	0	128000
HDX	11 (interactive_high_class)	Lastausgleich	Teilen	False	True	250	True	350	30000	True	0	128000

Wie werden Anwendungsregeln angewendet?

Wenn im SD-WAN-Netzwerk die eingehenden Pakete die SD-WAN-Appliance erreichen, werden die ersten paar Pakete keiner DPI-Klassifizierung unterzogen. An dieser Stelle werden die IP-Regelattribute wie Klasse, TCP-Terminierung auf die Pakete angewendet. Nach der DPI-Klassifizierung überschreiben die Anwendungsregelattribute wie Klasse, Übertragungsmodus die IP-Regelattribute.

Die IP-Regeln haben im Vergleich zu den Anwendungsregeln eine größere Anzahl von Attributen. Die Anwendungsregel überschreibt nur wenige IP-Regelattribute, der Rest der IP-Regelattribute bleibt für die Pakete verarbeitet.

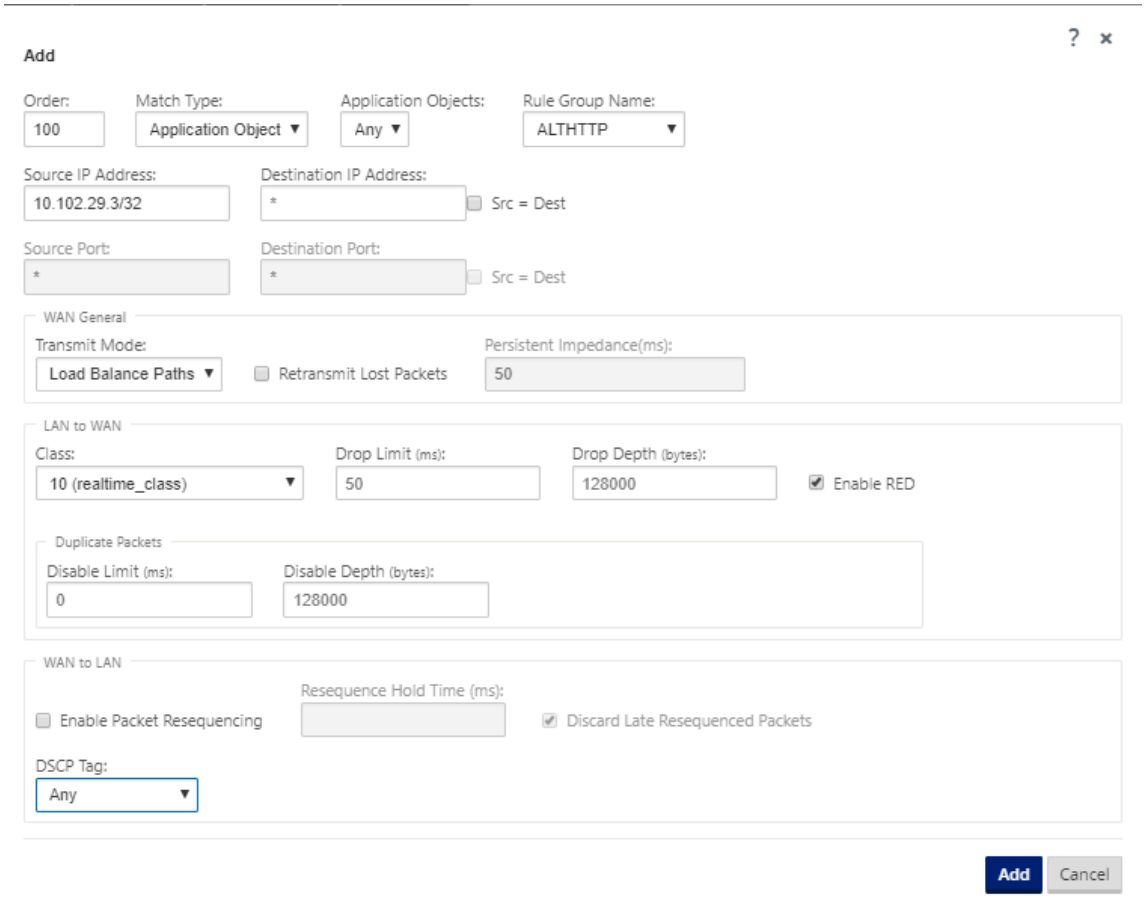
Angenommen, Sie haben eine Anwendungsregel für eine Webmail-Anwendung wie Google Mail angegeben, die das SMTP-Protokoll verwendet. Der IP-Regelsatz für das SMTP-Protokoll wird zunächst vor der DPI-Klassifizierung angewendet. Nach dem Parsen der Pakete und der Klassifizierung als zur Google Mail-Anwendung gehörend, wird die für die Google Mail-Anwendung angegebene Anwendungsregel angewendet.

Anwendungsregeln erstellen

So erstellen Sie Anwendungsregeln:

1. Navigieren Sie im SD-WAN-Konfigurationseditor 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.



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 **Übereinstimmungstyp** einen der folgenden Übereinstimmungstypen aus:

   - **Anwendung** —Wenn dieser Übereinstimmungstyp ausgewählt ist, geben Sie die Anwendung an, die als Übereinstimmungskriterium 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 Informationen 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 von benutzerdefinierten 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, um mit dem Datenverkehr übereinzustimmen.
   - **Ziel-IP-Adresse**: Ziel-IP-Adresse und Subnetzmaske, um mit dem Datenverkehr übereinzustimmen.
   - **Quellport**: Quellportnummer oder Portbereich, um mit dem Verkehr übereinzustimmen.
   - **Zielport**: Ziel-Portnummer oder Portbereich, um mit dem Verkehr übereinzustimmen.

   > **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 Anwendungsverkehr für den Flow wird über mehrere Pfade verteilt. Der Verkehr wird über den besten Pfad gesendet, bis dieser Pfad vollständig genutzt ist. Die verbleibenden Pakete werden über den nächstbesten Pfad gesendet.
     - **Persistenter Pfad**: Der Anwendungsverkehr bleibt 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 auf demselben Pfad verbleiben würde, bis die Wartezeit auf dem Pfad länger als der konfigurierte Wert ist.
     - **Doppelter Pfad**: Anwendungsdatenverkehr wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht.
   - Überprüfen Sie **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 Einstellungen von LAN zu WAN:

   - **Klasse**: Wählen Sie eine Klasse aus, der diese Regel zugeordnet werden soll.

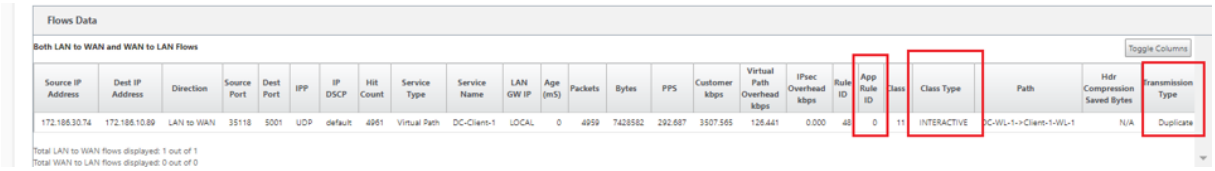
     Sie können Klassen auch anpassen, bevor Sie Regeln anwenden. Weitere Informationen finden Sie unter Anpassen von Klassen.

- **Drop-Limit**: Länge der Zeit, nach der Pakete, die im Klassenplaner warten, gelöscht werden. Gilt nicht für eine Massenklasse.
- **Drop-Tiefe:** Schwellenwert für die Warteschlangentiefe, nach der Pakete verworfen werden.
- **RED aktivieren**: Random Early Detection (RED) gewährleistet eine faire gemeinsame Nutzung von Klassenressourcen, indem Pakete verworfen werden, wenn eine Überlastung auftritt.
- **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:
   - **Paketneusequenzierung aktivieren:** Sequenziert die Pakete in der richtigen Reihenfolge am Ziel.
   - **Haltezeit neu**anordnen: Zeitintervall, für das die Pakete zur erneuten Sequenzierung gehalten werden, nach dem die Pakete an das LAN gesendet werden.
   - **Verwerfen Sie Pakete mit später Neusequenzierung**: Verwerfen Sie Pakete außerhalb der Reihenfolge, die eintrafen, nachdem die für die erneute Sequenzierung benötigten Pakete an das LAN gesendet wurden.
10. Klicken Sie auf **Apply**.

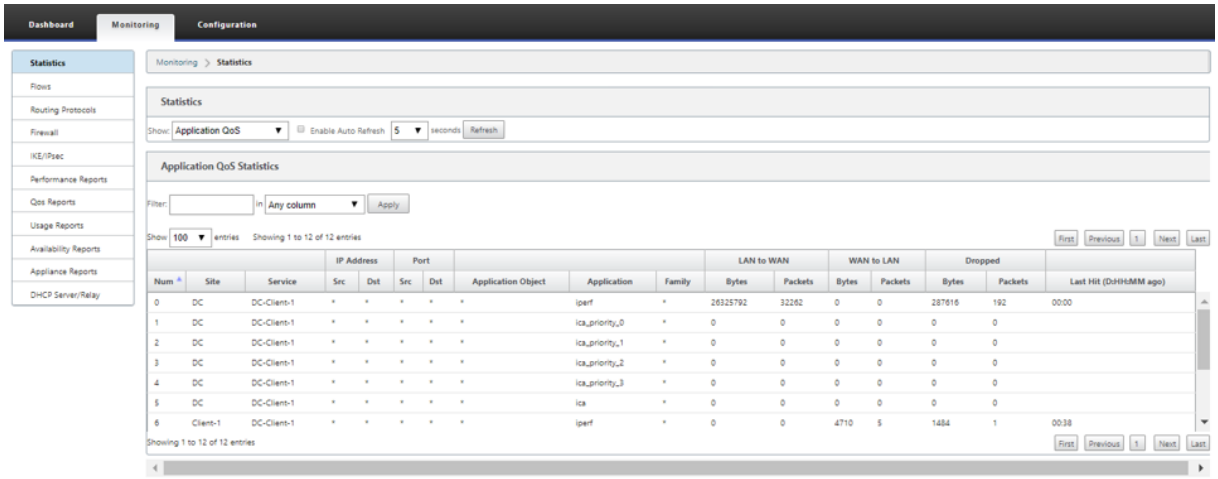
Um zu bestätigen, ob Anwendungsregeln auf den Verkehrsfluss angewendet werden, navigieren Sie zu **Überwachung** > **Flows**.

Notieren Sie sich die App-Regelkennung und überprüfen Sie, ob der Klassentyp und der Übertragungsmodus gemäß Ihrer Regelkonfiguration sind.



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-Regel-ID an. Überprüfen Sie die App-Regelkennung, die aus dem Flow erhalten wurde.



Erstellen benutzerdefinierter Anwendungen

Sie können Anwendungsobjekte verwenden, um benutzerdefinierte Anwendungen basierend auf den folgenden Übereinstimmungstypen zu definieren:

- IP-Protokoll
- Anwendungsname
- Anwendungs-Familie

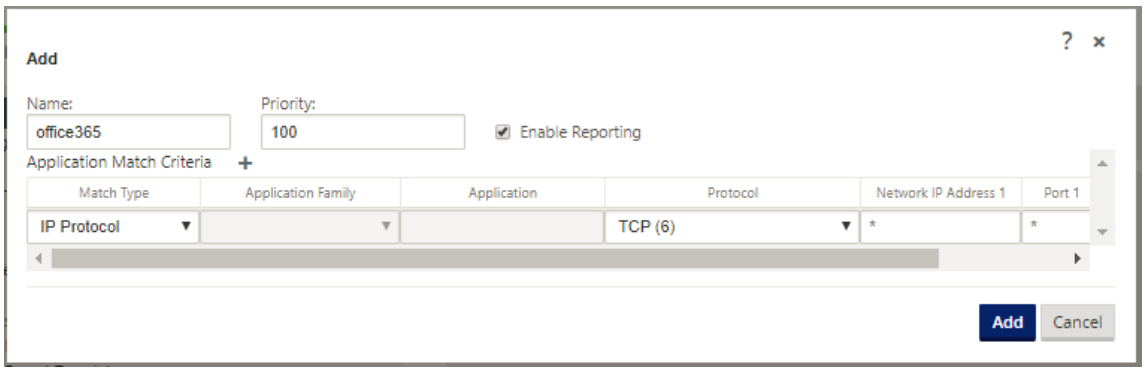
Der DPI-Klassifikator analysiert die eingehenden Pakete und klassifiziert sie basierend auf den angegebenen Übereinstimmungskriterien als Anwendungen. Sie können diese klassifizierten benutzerdefinierten Anwendungen in QoS, Firewall und Anwendungsrouting verwenden.

> **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 Konfigurationseditor zu **Global** > **Anwendungen** > **Benutzerdefinierte Anwendungen**, und klicken Sie auf **+**.



2. Legen Sie die folgenden Parameter fest:

   - **Name:** Name für die benutzerdefinierte Anwendung
   - **Reporting aktivieren:** Ermöglicht das Anzeigen von benutzerdefinierten Anwendungsberichten im SD-WAN Center. Weitere Informationen finden Sie unter 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 aus:

   - **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 **Apply**.

Regelgruppen hinzufügen und MOS aktivieren

October 28, 2021

Eine bestimmte Anwendung im Netzwerk kann durch die Gruppe von Regeln definiert werden, die auf sie 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 sowie 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.

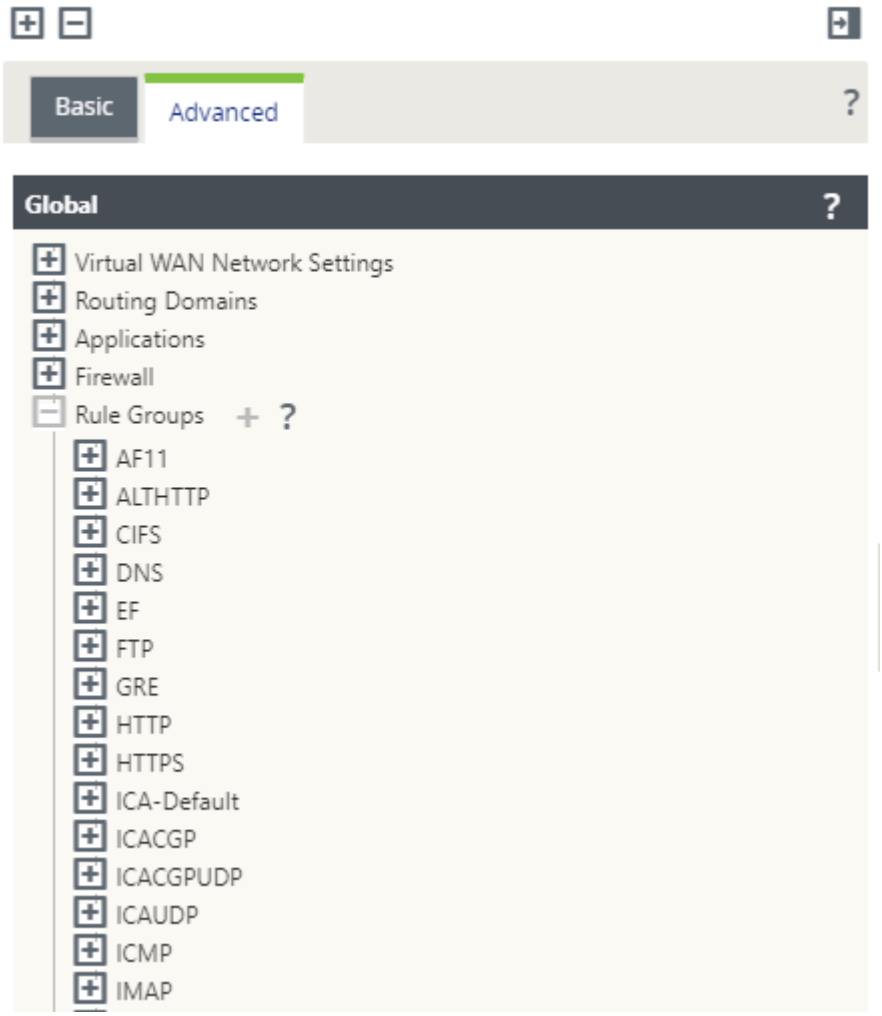
Der mittlere Meinungswert (MOS) ist ein numerisches Maß für die Qualität der Erfahrung, die eine Anwendung an Endbenutzer liefert. Es wird hauptsächlich für VoIP-Anwendungen verwendet. In SD-WAN wird MOS auch verwendet, um die Qualität von Nicht-VoIP-Anwendungen zu bewerten, indem der Datenverkehr so beurteilt wird, als wäre es ein VoIP-Anruf.

Der durchschnittliche MoS-Score wird mit einem Abtastintervall von 1 Minute berechnet. Der von anderen Tools von Drittanbietern berechnete MoS-Wert kann je nach verwendetem Abtastintervall variieren.

SD-WAN Center zeigt den MOS für vorhandenen Datenverkehr an, der den virtuellen Pfad durchläuft. Weitere Informationen zum Anzeigen von MOS im SD-WAN Center finden Sie unter MOS for Applications.

So fügen Sie eine benutzerdefinierte Regelgruppe hinzu:

1. Navigieren Sie im Konfigurationseditor 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 **Apply**.

> **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. Für weitere Informationen. siehe MOS für Anwendungen.

Anwendungsklassifizierung

November 16, 2022

Die Citrix SD-WAN-Appliances führen Deep Packet Inspection (DPI) durch, um Anwendungen mithilfe 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)
- Domänennamenbasierte Anwendungsklassifizierung

Klassifizierung der DPI-Bibliothek

Die Deep Packet Inspection (DPI) Bibliothek erkennt Tausende kommerzieller Anwendungen. Es ermöglicht die Erkennung und Klassifizierung von Anwendungen in Echtzeit. 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 **Konfigurationseditor**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)
- HDX Adaptiver Transport
- ICA über WebSocket (wird von HTML5 Receiver verwendet)

> **Hinweis**
>
> Die Klassifizierung des über SSL/TLS oder DTLS gelieferten ICA-Datenverkehrs wird in der SD-WAN Standard Edition nicht unterstützt, wird jedoch in SD-WAN Premium Edition und SD-WAN WANOP Edition unterstützt.
>
> Die Klassifizierung des Netzwerkverkehrs erfolgt während der anfänglichen Verbindungen oder

der Flow-Einrichtung. Daher werden bereits bestehende 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 Version 10 Version 1 kann die SD-WAN-Appliance jeden ICA-Datenstrom in Multistream-ICA auch in einer Single-Port-Konfiguration 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 benutzerbasierte HDX-Berichte auf SDWAN-Center angezeigt werden, benötigen Sie SD-WAN Standard Edition oder Premium Edition 11.0 oder höher.

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 in der Citrix Workspace-App Feature Matrix nach **HDX Insight mit NSAP VC**und Multiport/Multistream-ICA. Sehen Sie sich die aktuell unterstützten Release-Versionen bei HDX Insightsan.
- 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_prority_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 **Konfigurationseditor**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 Gateway Service Optimization.

Domänennamenbasierte Anwendungsklassifizierung

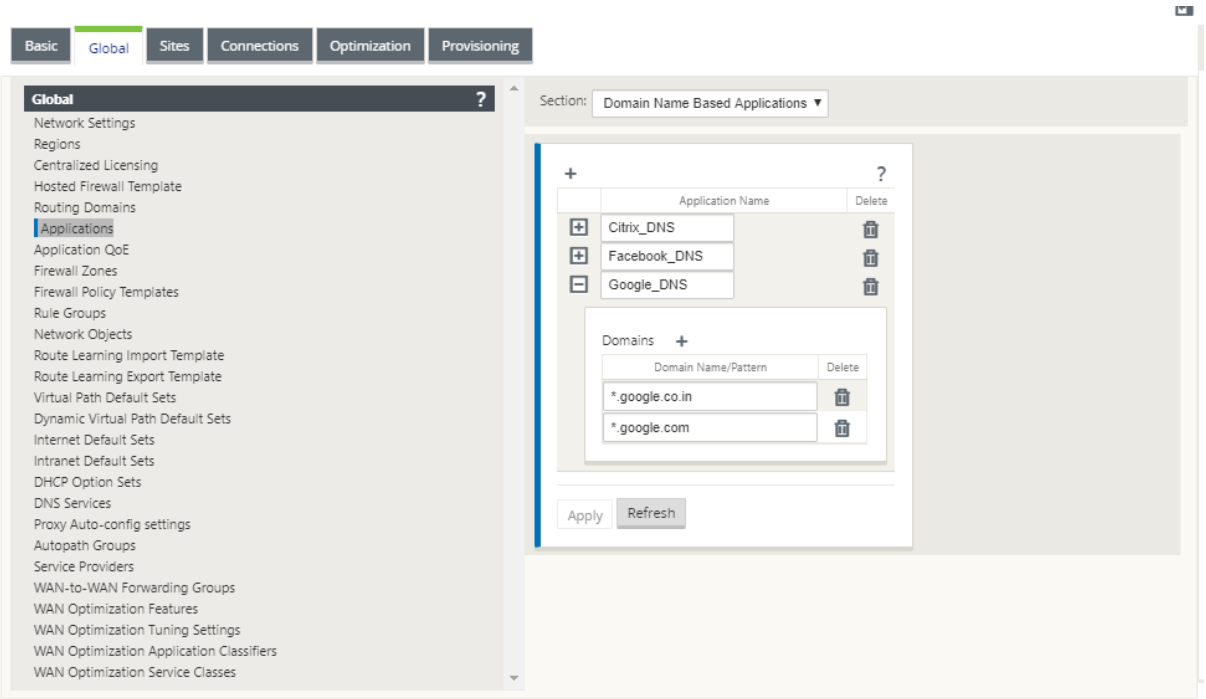
Die DPI-Klassifikations-Engine wurde erweitert, um Anwendungen basierend auf dem Domänennamen und -mustern zu klassifizieren. Nachdem der DNS-Forwarder die DNS-Anforderungen abgefangen und analysiert hat, verwendet die DPI-Engine den IP-Klassifizierer, um die erste Paketklassifizierung durchzuführen. Weitere DPI-Bibliothek und ICA-Klassifizierung werden durchgeführt und die auf Domänennamen basierende Anwendungs-ID wird angehängt.

Mit der auf Domänennamen basierenden Anwendungsfunktion können Sie mehrere Domainnamen gruppieren und als eine einzige Anwendung behandeln. Dies erleichtert die Anwendung von Firewall, Anwendungssteuerung, QoS und anderen Regeln. Maximal 64 auf Domänennamen basierende Anwendungen können konfiguriert werden.

Um auf Domänennamen basierende Anwendungen zu definieren, navigieren Sie im Konfigurationseditor zu **Global** > **Anwendungen** > **Domänennamen-basierte Anwendungen**. Geben Sie einen An-

wendungsnamen ein und fügen Sie die erforderlichen Domainnamen oder -muster hinzu. Sie können entweder den vollständigen Domainnamen eingeben oder am Anfang Wildcards verwenden. Die folgenden Domainnamen-Formate sind zulässig:

- beispiel.com
- *.beispiel.com



Die klassifizierten Domänennamen-basierten Anwendungen werden für die Konfiguration der folgenden verwendet:

- DNS-Proxy
- DNS Transparenter Spediteur
- Anwendungsobjekte
- Anwendungsrouten
- Firewall-Richtlinie
- QoS-Regeln für Anwendungen
- Anwendung QoE

Einschränkungen

- Wenn keine DNS-Anfrage/Antwort vorhanden ist, die einer domänennamenbasierten 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. Es werden nur DNS-Antworten in einem einzigen Paket verarbeitet.
- DNS über TCP wird nicht unterstützt.
- Nur Top-Level-Domains werden als Domainnamenmuster unterstützt.

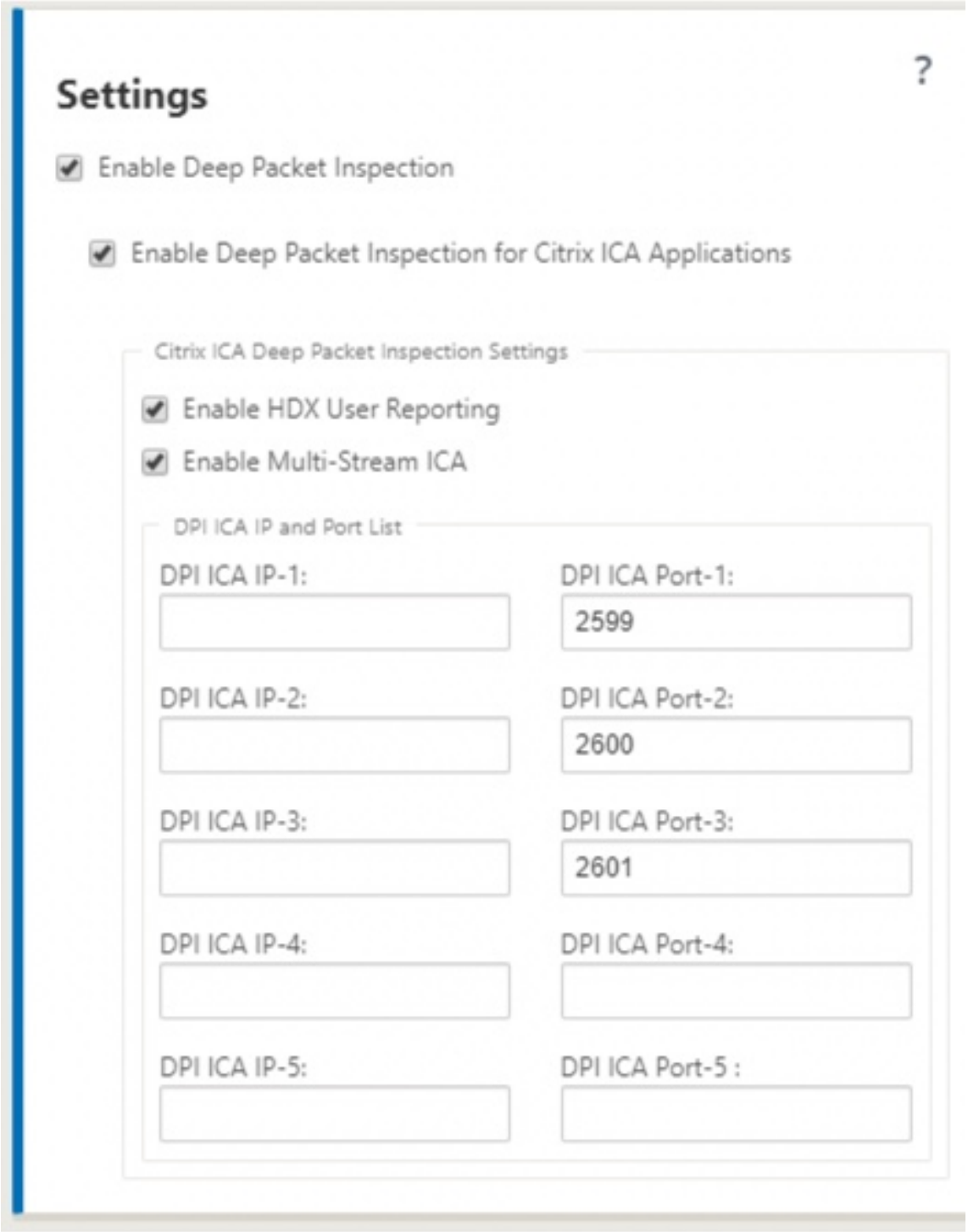
Verschlüsselten Datenverkehr klassifizieren

Die Citrix SD-WAN Appliance erkennt und meldet verschlüsselten Datenverkehr im Rahmen der Anwendungsberichterstattung mit den folgenden zwei Methoden:

- Für den HTTPS-Verkehr überprüft die DPI-Engine das SSL-Zertifikat, um den gebräuchlichen Namen zu lesen, der den Namen des Dienstes trägt (z. B. Facebook, Twitter). Abhängig von der 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.
- Für Anwendungen, die ihr eigenes Verschlüsselungsprotokoll verwenden, sucht die DPI-Engine nach binären Mustern in den Flows, zum Beispiel sucht die DPI-Engine im Zertifikat nach einem Binärmuster und bestimmt die Anwendung.

So konfigurieren Sie Einstellungen für die Anwendungsklassifizierung:

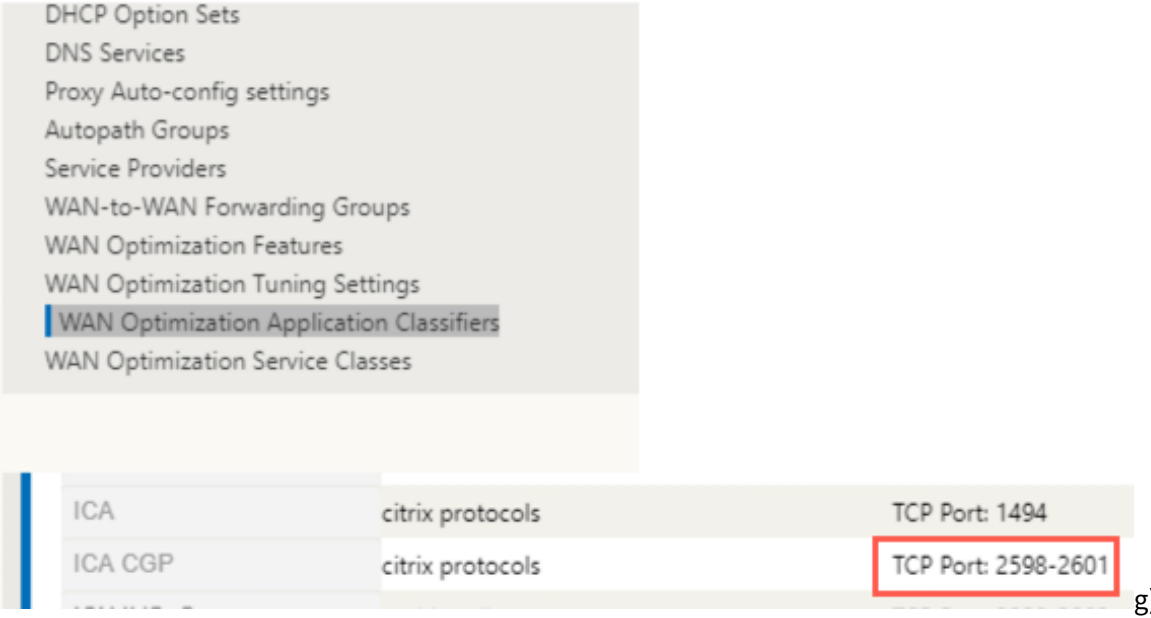
1. Klicken Sie im **Konfigurationseditor**auf **Global** > **Anwendungen** > **Einstellungen**.



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.



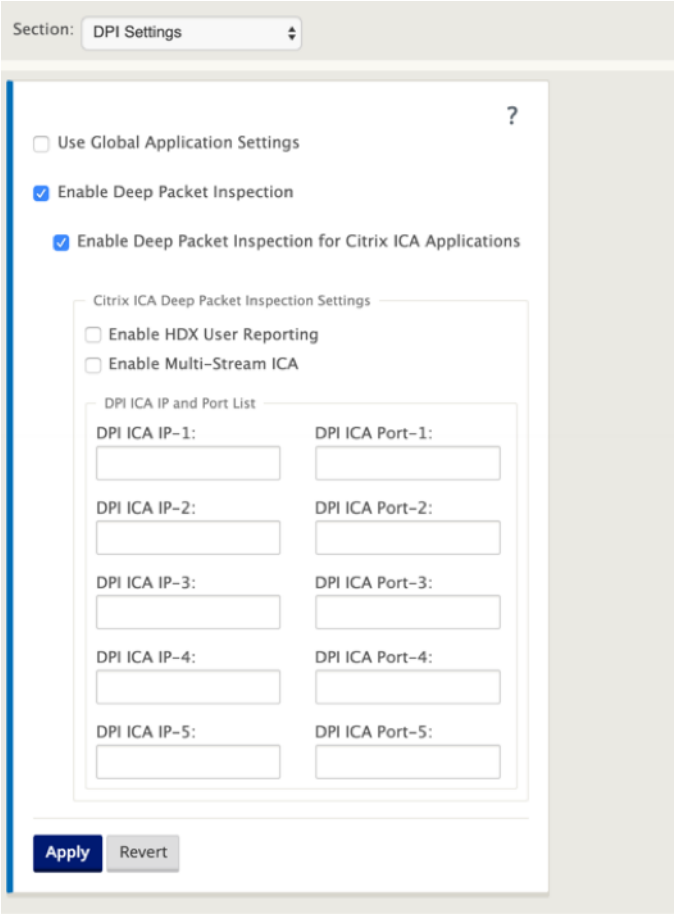
g)

2. Wählen Sie **Deep Packet Inspection aktivieren**aus. Dies ermöglicht eine Anwendungsklassifizierung auf der Appliance. Sie können Anwendungsstatistiken im SD-WAN Center anzeigen und überwachen. Weitere Informationen finden Sie unter Anwendungsbericht.

> **Hinweis**
>
> Standardmäßig sammelt **Enable Deep Packet Inspection** Statistiken für klassifizierte Daten.

3. 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. Ohne diese Option aktiviert, könnte ein Teil des HDX-Datenverkehrs immer noch klassifiziert und QoE berechnet werden, aber Statistiken zum SD-WAN-Center sind nicht verfügbar. Sie können ICA-Anwendungsstatistiken im SD-WAN Center anzeigen, anzeigen und überwachen. Diese Option ist standardmäßig aktiviert. Weitere Informationen finden Sie unter HDX-Berichte.

4. 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 **Konfigurationseditor**auf **Verbindungen > Anwendungen**.



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. Nehmen Sie keine Standardportnummern 2598 oder 1494 in diese Liste auf, da diese bereits intern enthalten sind.
6. Geben Sie in **DPI-ICA-IP**die IP-Adresse an, die verwendet werden soll, um die Ports weiter auf ein bestimmtes Ziel zu beschränken.

   > **Hinweis**
   >
   > Verwenden Sie '*'für Port, der zu einer beliebigen IP-Adresse bestimmt ist.

7. Klicken Sie auf **Anwenden**

Sie können die Einstellungen für die Anwendungsklassifizierung an jedem Standort einzeln konfigurieren. Klicken Sie auf **Verbindungen**, wählen Sie eine Site aus und klicken Sie auf **Anwendungseinstellungen**. Sie können auch die globalen Anwendungseinstellungen verwenden.

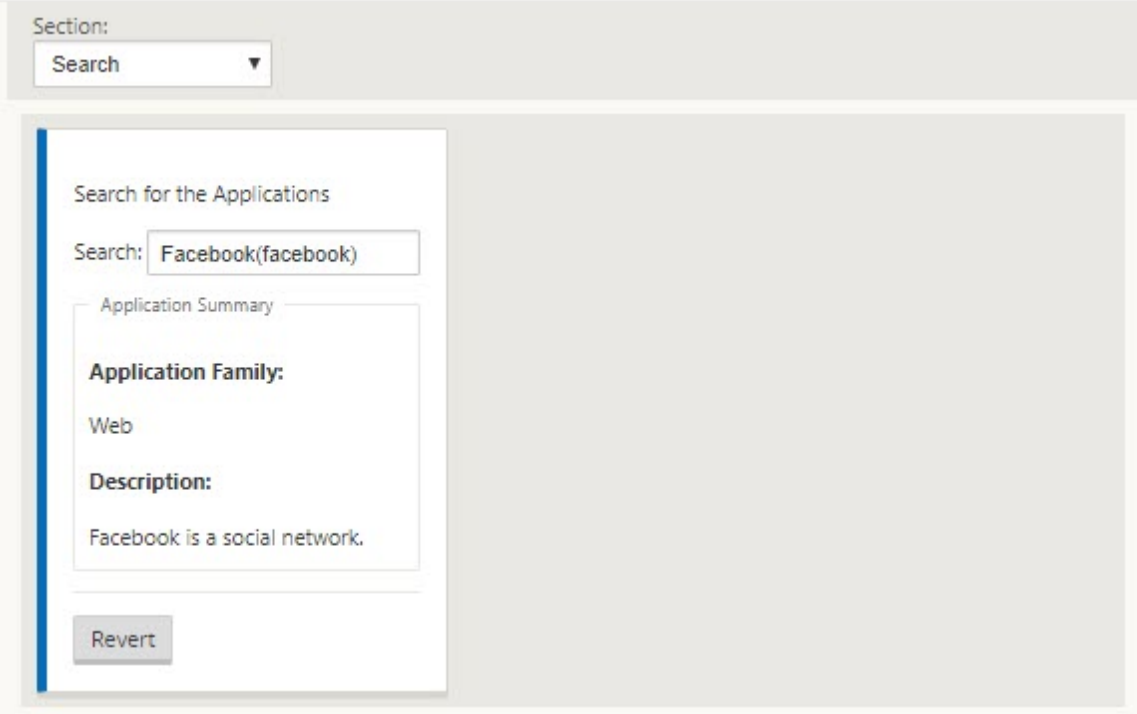
Suche nach Anwendungen

Sie können nach einer Anwendung suchen, um den Familiennamen der Anwendung zu ermitteln. Eine kurze Beschreibung der Anwendung wird ebenfalls bereitgestellt.

So suchen Sie nach einer Anwendung:

1. Klicken Sie im Konfigurationseditor auf **Global** > **Anwendungen** > **Suchen** .
2. Geben Sie im Suchfeld 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
- QoS-Regeln für Anwendungen
- Anwendung QoE

> **Hinweis**
>
> Informationen zu Anwendungen, die die SD-WAN-Appliance mithilfe von Deep Packet Inspection identifizieren kann, finden Sie unter Anwendungssignaturbibliothek.

Anwendungsobjekte

Anwendungsobjekte ermöglichen es Ihnen, verschiedene Arten von Übereinstimmungskriterien in einem einzigen Objekt zu gruppieren, das für Firewall-Richtlinien und Anwendungssteuerung verwen-

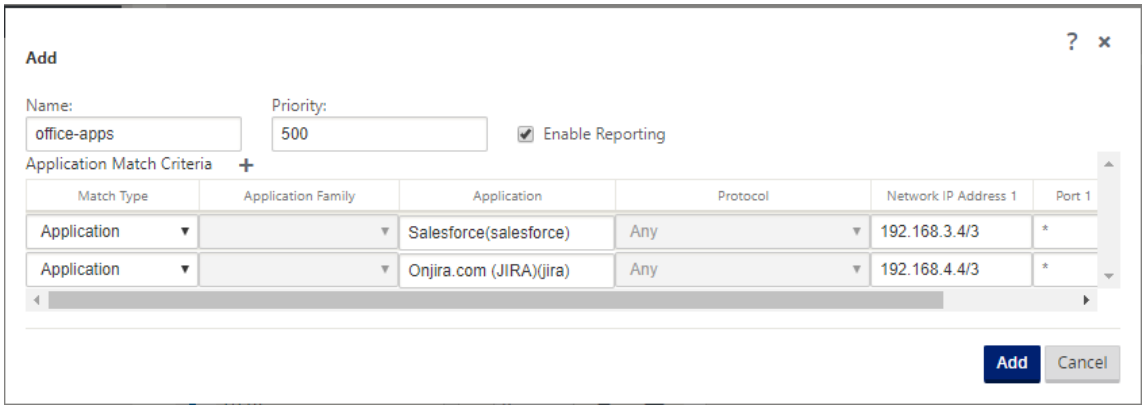
det werden kann. IP-Protokoll, Anwendung und Anwendungsfamilie sind die verfügbaren Übereinstimmungstypen.

Die folgenden Features verwenden Anwendungsobjekt als Übereinstimmungstyp:

- Anwendungsrouten
- Firewall-Richtlinie
- QoS-Regeln für Anwendungen
- Anwendung QoE

So erstellen Sie ein Anwendungsobjekt:

1. Klicken Sie im Konfigurationseditor auf **Global** > **Anwendungen** > **Anwendungsobjekte**.
2. Klicken Sie auf **Hinzufügen** und geben Sie im Feld **Name** einen Namen für das Objekt ein.

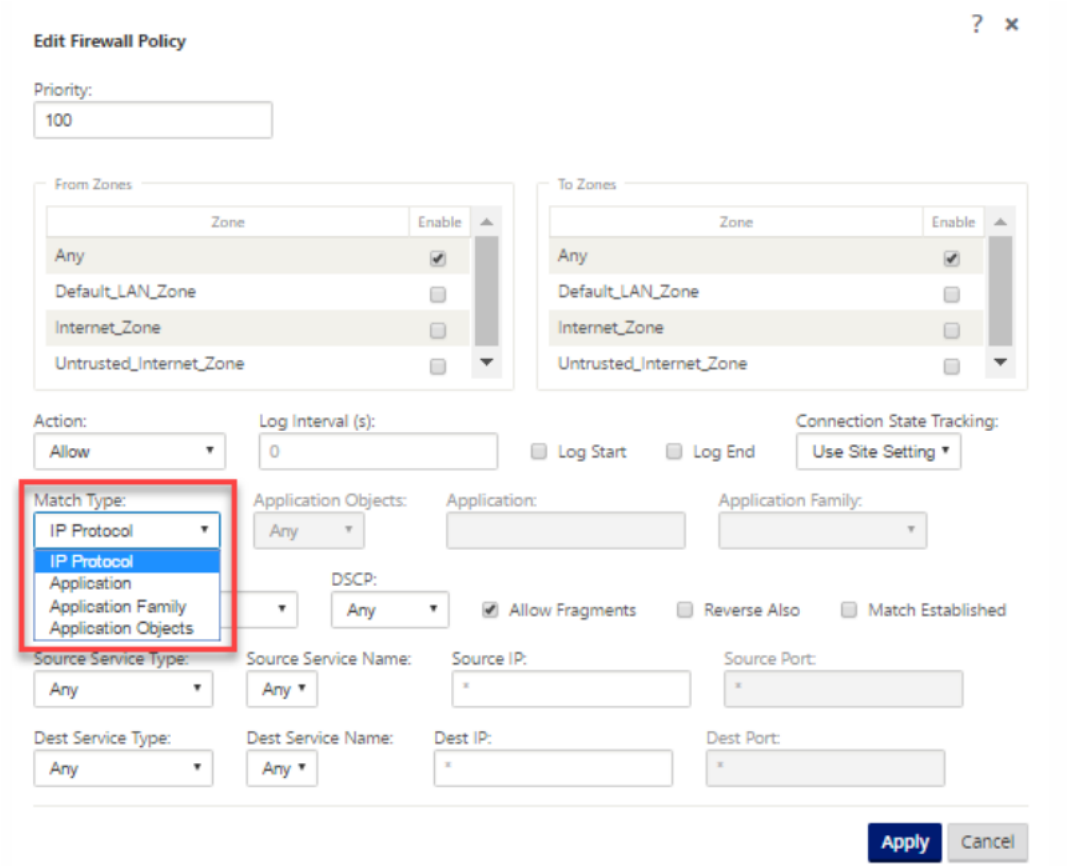


3. Wählen Sie **Reporting aktivieren** aus, um die Anzeige benutzerdefinierter Anwendungsberichte in Citrix SD-WAN Center zu ermöglichen. Weitere Informationen finden Sie unter Anwendungsbericht.
4. Geben Sie im Feld **Priorität** die Priorität des Anwendungsobjekts ein. Wenn die eingehenden Pakete mit 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 aus:
   - **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

Die Klassifizierung des Datenverkehrs als Anwendungen, Anwendungsfamilien oder Domainnamen ermöglicht es Ihnen, die Anwendung, Anwendungsfamilien und Anwendungsobjekte als Übereinstimmungstypen zu verwenden, um den Datenverkehr zu filtern und Firewall-Richtlinien und -Regeln anzuwenden. Sie gilt für alle Vor-, Post- und lokalen Richtlinien. Weitere Informationen zur Firewall finden Sie unter Stateful Firewall und NAT-Support.



Anwendungsklassifizierung anzeigen

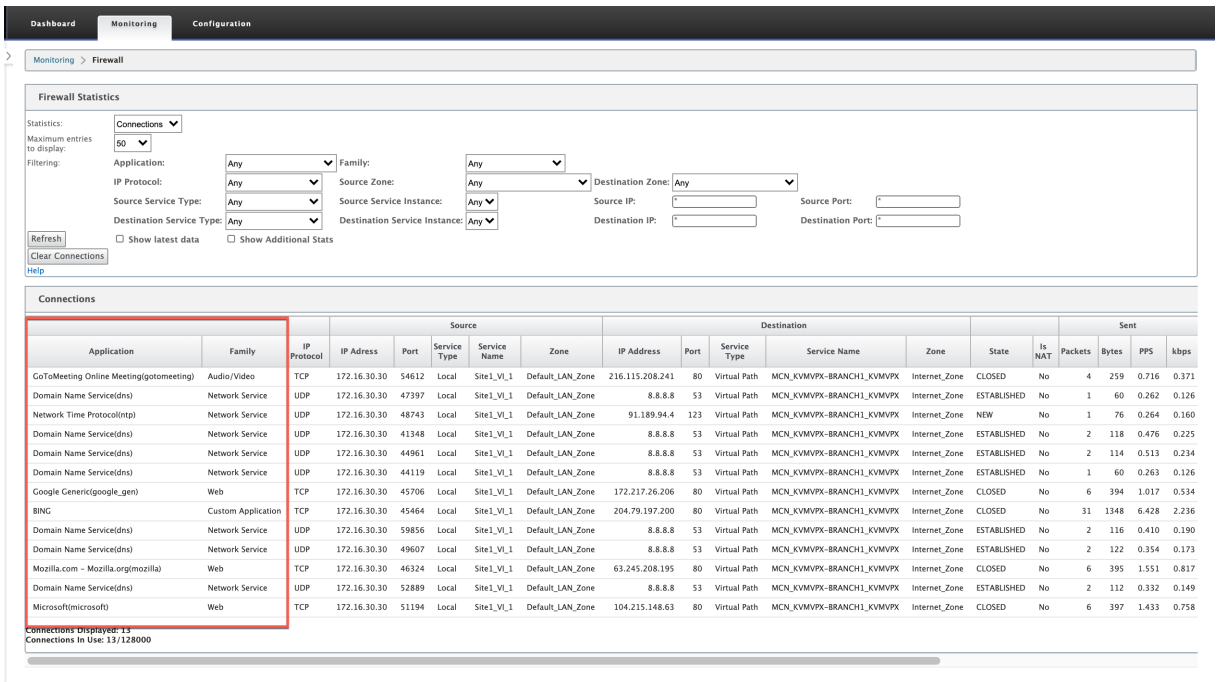
Nachdem Sie die Anwendungsklassifizierung aktiviert haben, können Sie den Anwendungsnamen und die Anwendungsfamilie in den folgenden Berichten anzeigen:

- Firewall-Verbindungsstatistiken
- Informationen zu Flows

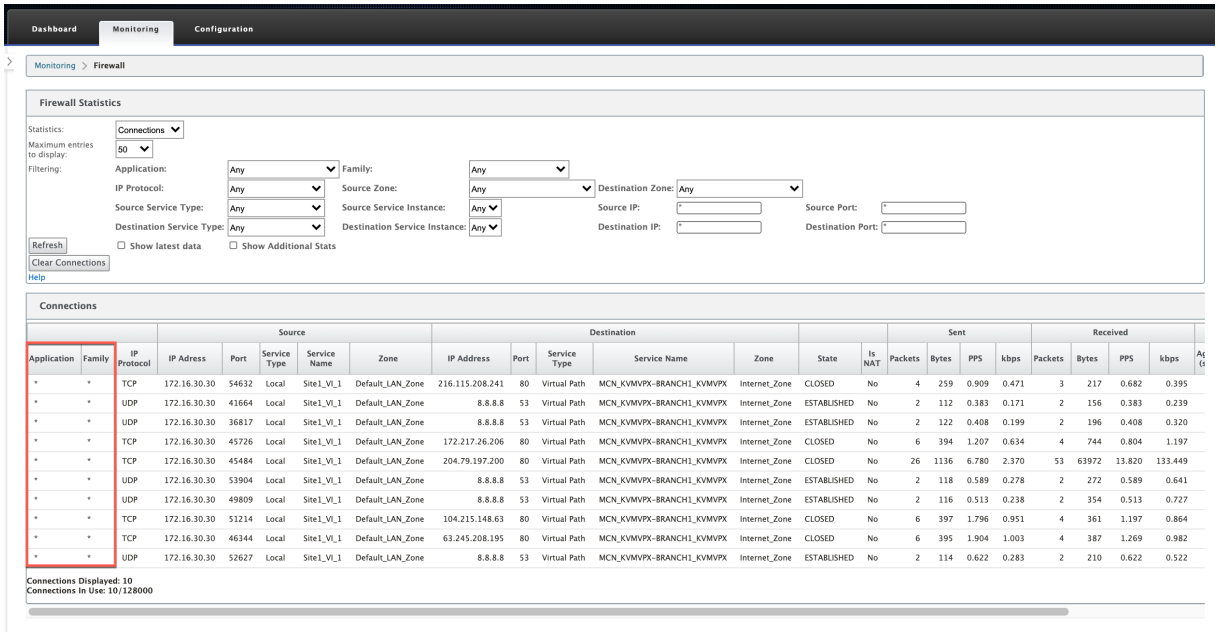
- Anwendungsstatistiken

Firewall-Verbindungsstatistiken

Navigieren Sie im **Konfigurationseditor**zu **Monitoring > Firewall**. Im Abschnitt **Verbindungen** werden in den Spalten **Anwendung** und **Familie** die Anwendungen und die zugehörige Familie aufgeführt.

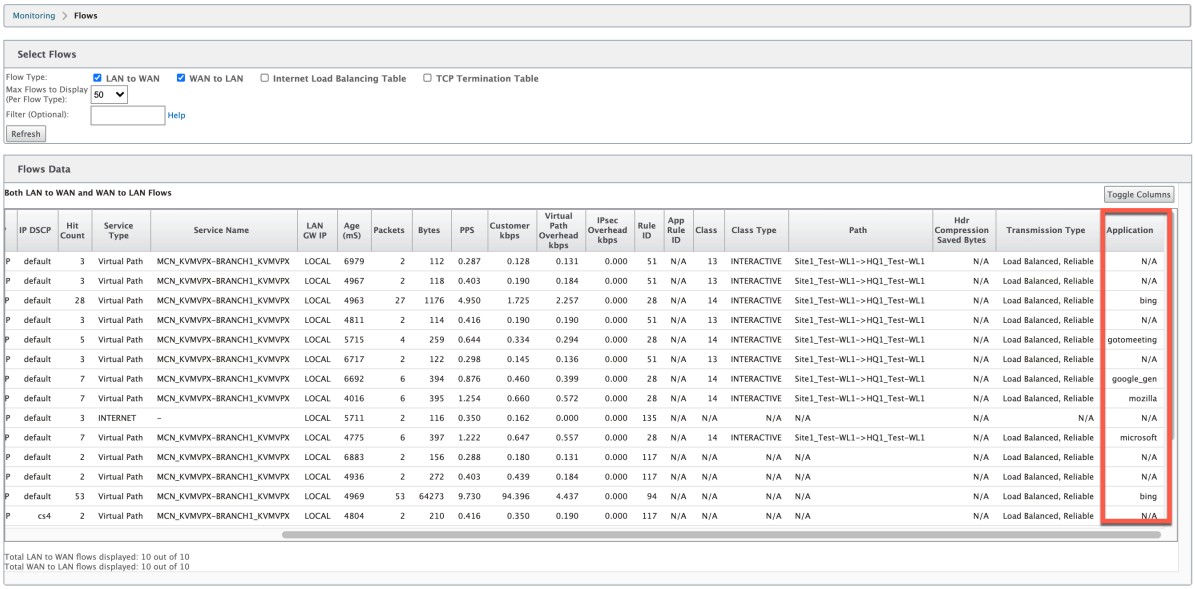


Wenn Sie die Anwendungsklassifizierung nicht aktivieren, zeigen die Spalten **Anwendung** und **Familie** keine Daten an.



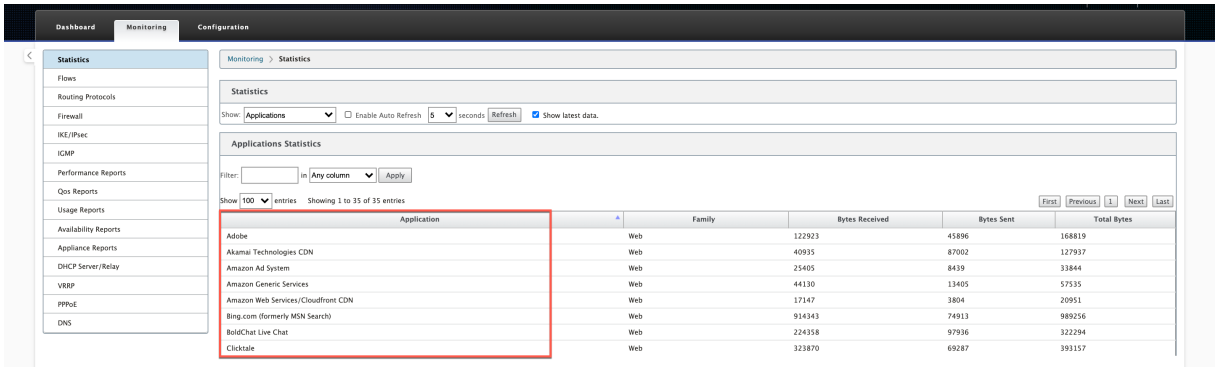
Informationen zu Flows

Navigieren Sie im **Konfigurationseditor**zu **Überwachung > Flows**. Im Abschnitt "**Flows Data** "werden in der Spalte "**Anwendung** "die Anwendungsdetails aufgeführt.



Anwendungsstatistiken

Navigieren Sie im **Konfigurationseditor**zu **Monitoring > Statistiken**. Im Abschnitt **Anwendungsstatistiken** werden in der Spalte **Anwendung** die Anwendungsdetails aufgelistet.



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 Anzeigen der Anwendungsklassifizierung.

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)

October 28, 2021

Die QoS-Fairness-Funktion verbessert die Fairness mehrerer virtueller Pfadflüsse durch die Verwendung von QoS-Klassen und Random Early Detection (RED). Ein virtueller Pfad kann einer von 16 verschiedenen Klassen zugewiesen werden. Eine Klasse kann einer von drei Grundtypen sein:

- Echtzeitklassen bedienen Verkehrsströme, die einen prompten Service bis zu einer bestimmten Bandbreitenbegrenzung erfordern. Niedrige Latenz wird gegenüber dem aggregierten Durchsatz bevorzugt.
- Interaktive Klassen haben eine niedrigere Priorität als Echtzeit, haben jedoch absolute Priorität vor Massenverkehr.
- Massenklassen erhalten, was von Echtzeit- und interaktiven Klassen übrig bleibt, da die Latenz für den Massenverkehr weniger wichtig ist.

Benutzer geben unterschiedliche Bandbreitenanforderungen für verschiedene Klassen an, die es dem virtuellen Pfadplaner ermöglichen, konkurrierende Bandbreitenanforderungen von mehreren

Klassen desselben Typs zu arbitrieren. Der Scheduler verwendet den Algorithmus Hierarchical Fair Service Curve (HFSC), um Fairness zwischen den Klassen zu erreichen.

HFSC bedient Klassen in First-In, First-Out-Reihenfolge (FIFO). Vor dem Planen von Paketen untersucht Citrix SD-WAN die Menge des für die Paketklasse ausstehenden Datenverkehrs. Wenn übermäßiger Verkehr ansteht, werden die Pakete verworfen, anstatt in die Warteschlange gestellt zu werden (Tail Dropping).

Warum verursacht TCP Warteschlangen?

TCP kann nicht steuern, wie schnell das Netzwerk Daten übertragen kann. Um die Bandbreite zu steuern, implementiert TCP das Konzept eines Bandbreitenfensters, bei dem es sich um die Menge an nicht bestätigtem Verkehr handelt, die es im Netzwerk zulässt. Es beginnt zunächst mit einem kleinen Fenster und verdoppelt die Größe dieses Fensters, wenn Bestätigungen eingehen. Dies wird als langsame Start- oder exponentielle Wachstumsphase bezeichnet.

TCP identifiziert Netzwerküberlastung, indem es verworfene Pakete erkennt. Wenn der TCP-Stapel einen Paket-Burst sendet, der eine Verzögerung von 250 ms einführt, erkennt TCP keine Überlastung, wenn keines der Pakete verworfen wird, sodass das Fenster weiter vergrößert wird. Dies kann so lange dauern, bis die Wartezeit 600—800 ms erreicht.

Wenn sich TCP nicht im langsamen Startmodus befindet, reduziert es die Bandbreite um die Hälfte, wenn ein Paketverlust erkannt wird, und erhöht die zulässige Bandbreite für jede empfangene Bestätigung um ein Paket. TCP wechselt daher zwischen dem Ausüben von Aufwärtsdruck auf die Bandbreite und dem Absichern. Wenn die Wartezeit bis zum Zeitpunkt des Erkennens des Paketverlusts 800 ms erreicht, verursacht die Bandbreitenreduzierung leider eine Übertragungsverzögerung.

Auswirkungen auf die QoS-Fairness

Wenn eine TCP-Übertragungsverzögerung auftritt, ist es schwierig, eine Fairness-Garantie innerhalb einer virtuellen Pfadklasse bereitzustellen. Der virtuelle Pfadplaner muss Tail-Drop-Verhalten anwenden, um zu vermeiden, dass enorme Mengen an Traffic zurückgehalten werden. Die Art der TCP-Verbindungen besteht darin, dass eine kleine Anzahl von Verkehrsströmen den virtuellen Pfad füllen, was es für eine neue TCP-Verbindung schwierig macht, einen angemessenen Anteil an der Bandbreite zu erreichen. Um die Bandbreite angemessen zu teilen, muss sichergestellt werden, dass Bandbreite für die Übertragung neuer Pakete verfügbar ist.

Zufällige Früherkennung

Random Early Detection (RED) verhindert, dass sich Traffic-Warteschlangen füllen und Tail-Drop-Aktionen verursachen. Es verhindert unnötiges Anstehen durch den virtuellen Pfadplaner, ohne den

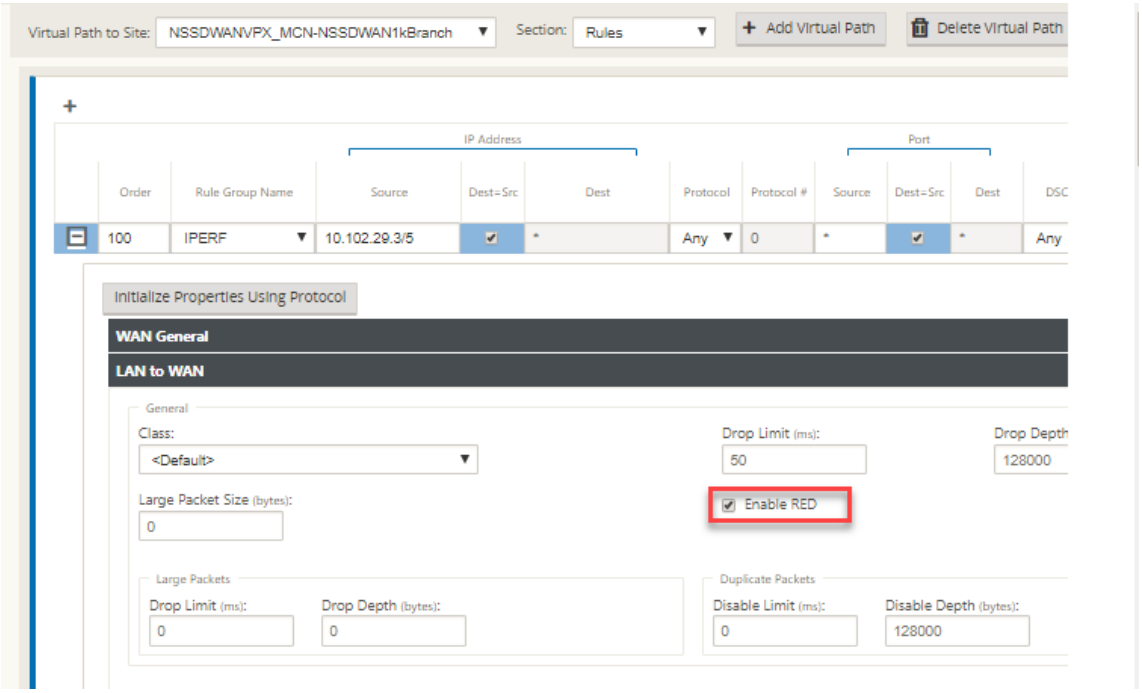
Durchsatz zu beeinträchtigen, den eine TCP-Verbindung erreichen kann.

Wie benutzt man RED

1. Starten Sie eine TCP-Sitzung, um den virtuellen Pfad zu erstellen. Stellen Sie sicher, dass bei aktiviertem RED die Wartezeit für diese Klasse im stationären Zustand bei etwa 50 ms bleibt.
2. Starten Sie eine zweite TCP-Sitzung und stellen Sie sicher, dass beide TCP-Sitzungen die Bandbreite des virtuellen Pfads gleichmäßig teilen. Stellen Sie sicher, dass die Wartezeit für die Klasse im stationären Zustand bleibt.
3. Stellen Sie sicher, dass der Konfigurationseditor 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 zum **Konfigurationseditor** > **Verbindungen** > **[Virtuelle **Pfade** > Virtueller Pfad]** auswählen > **Regeln** > Regel auswählen **(VOIP)**.
2. Erweitern Sie den Bereich **LAN zu WAN**. Klicken Sie im Abschnitt **LAN zu WAN** auf das Kontrollkästchen **RED aktivieren**, um es für TCP-basierte Regeln zu aktivieren.



MPLS-Warteschlangen

October 28, 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-Verbindung zu erstellen, und ein eindeutiges Tag für Differentiated Services Code Point (DSCP), das dem Warteschlangenschema des Anbieters entspricht. Nach dem Definieren eines WAN-Links für jede MPLS-Warteschlange wird der Intranetdienst für die Zuordnung zu einer bestimmten Warteschlange definiert.

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 Private MPLS.
2. Definieren Sie die MPLS-Warteschlangen, die den MPLS-Warteschlangen des Dienstanbieters entsprechen.
3. Aktivieren Sie den WAN-Link für den virtuellen Pfaddienst (standardmäßig für private MPLS-WAN-Links aktiviert).
4. Weisen Sie vom virtuellen Pfad auf einem 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.

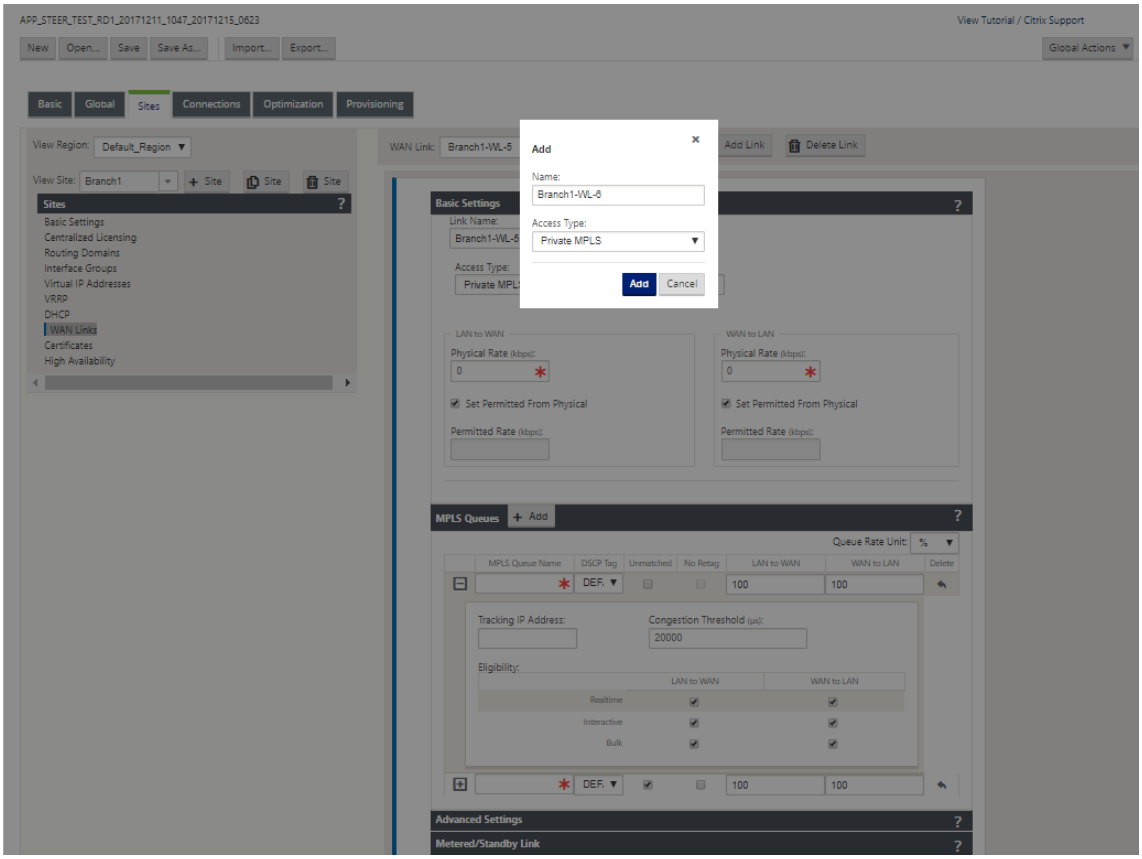
5. Stellen Sie sicher, dass dieselbe Autopath-Gruppe am MCN und Client konfiguriert ist.
6. Stellen Sie sicher, dass die Pfade für den WAN-Link automatisch erstellt werden.
7. Weisen Sie den Intranetdienst bei Bedarf einer bestimmten Warteschlange zu.

> **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 Internetzugangstyp 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 Konfigurationseditor zu **Sites** > **[Site-Name]** > **WAN-Links**. Klicken Sie auf **Link hinzufügen**. Geben Sie den WAN-Link-Namen ein und wählen Sie **Private MPLS** als Zugriffstyp aus.



2. Unter den **Grundeinstellungen**gibt es jetzt eine neue Registerkarte **MPLS-Warteschlangen**. Klicken Sie auf + Hinzufügen, um bestimmte MPLS-Warteschlangen hinzuzufügen. Diese sollten den vom Dienstanbieter definierten Warteschlangen entsprechen.

Feld	Beschreibung
MPLS-Warteschlangenname	Der Name der MPLS-Warteschlange
DSCP-Tag	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 das Hochladen verwenden dürfen, die die definierte physische Upload-Rate des WAN-Link nicht überschreiten darf.

Feld	Beschreibung
WAN zu WAN Zulässige 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-Warteschlangendefinition (indem Sie auf das + klicken), und weitere Optionen werden angezeigt. Zu diesen Optionen gehören:

Feld	Beschreibung
Tracking-IP-Adresse	WAN-Link-Tracking-Adresse
Überlastungsschwelle	Die definierte Zeitspanne für Überlastung (in Mikrosekunden), nach der die MPLS-Warteschlange die Paketübertragung drosselt, um eine größere Überlastung zu vermeiden. Wenn die Überlastung den festgelegten Schwellenwert überschreitet, sichert SD-WAN die Senderate ab.
Teilnahmeberechtigung	Die Berechtigung der MPLS-Warteschlange, bestimmte Traffic-Klassen zu verarbeiten. Wenn die Berechtigung für eine bestimmte Klasse von Verkehr deaktiviert ist, wird diese Verkehrsklasse wahrscheinlich nicht durch die MPLS-Warteschlange geleitet, es sei denn, die Netzwerkbedingungen erfordern dies.

Konfigurieren Sie die MPLS-Warteschlangen, die den vorhandenen WAN-Link-Warteschlangendefinitionen des Dienstanbieters entsprechen.

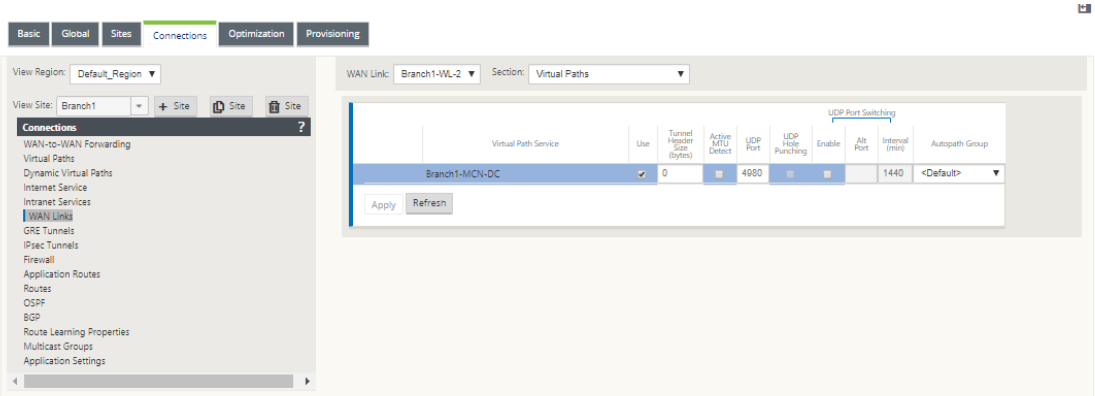
> **Hinweis**
>
> Alle vorhandenen MPLS WAN Links, die vor SD-WAN 9.1 konfiguriert wurden, sind nicht betroffen.

Definieren von WAN-Link-Eigenschaften für private MPLS

Sobald der Private MPLS WAN Link mit seinen 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 Link-Name**] > **Virtuelle Pfade** > [**Virtueller Pfadname**] > [**Lokaler Standort**] > **WAN-Links** und klicken Sie auf **Bearbeiten** ().
2. Klicken Sie auf das Dropdownmenü **Autopath-Gruppe** und wählen Sie aus den 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.

Weisen Sie Autopath-Gruppe virtuellem Pfad-WAN Link zu

Die definierte Autopath-Gruppe ist für die MCN- und 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

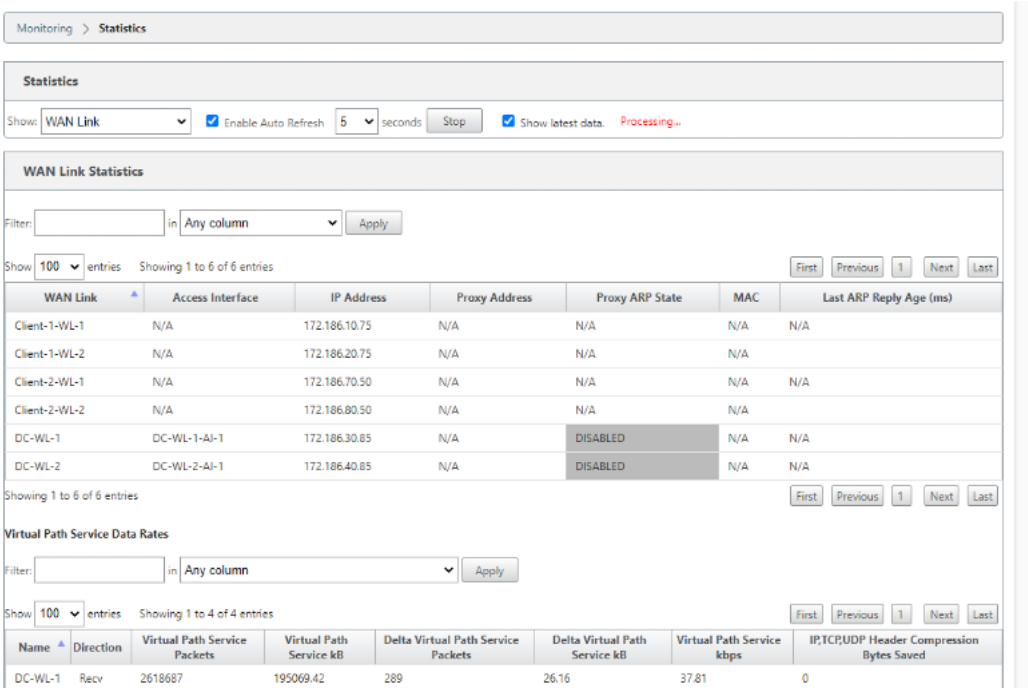
und über die CLI verfügbar. Diese Optionen sind jetzt im Webinterface verfügbar, um bei der Fehlerbehebung zu helfen.

Zulässigen Tarif anzeigen

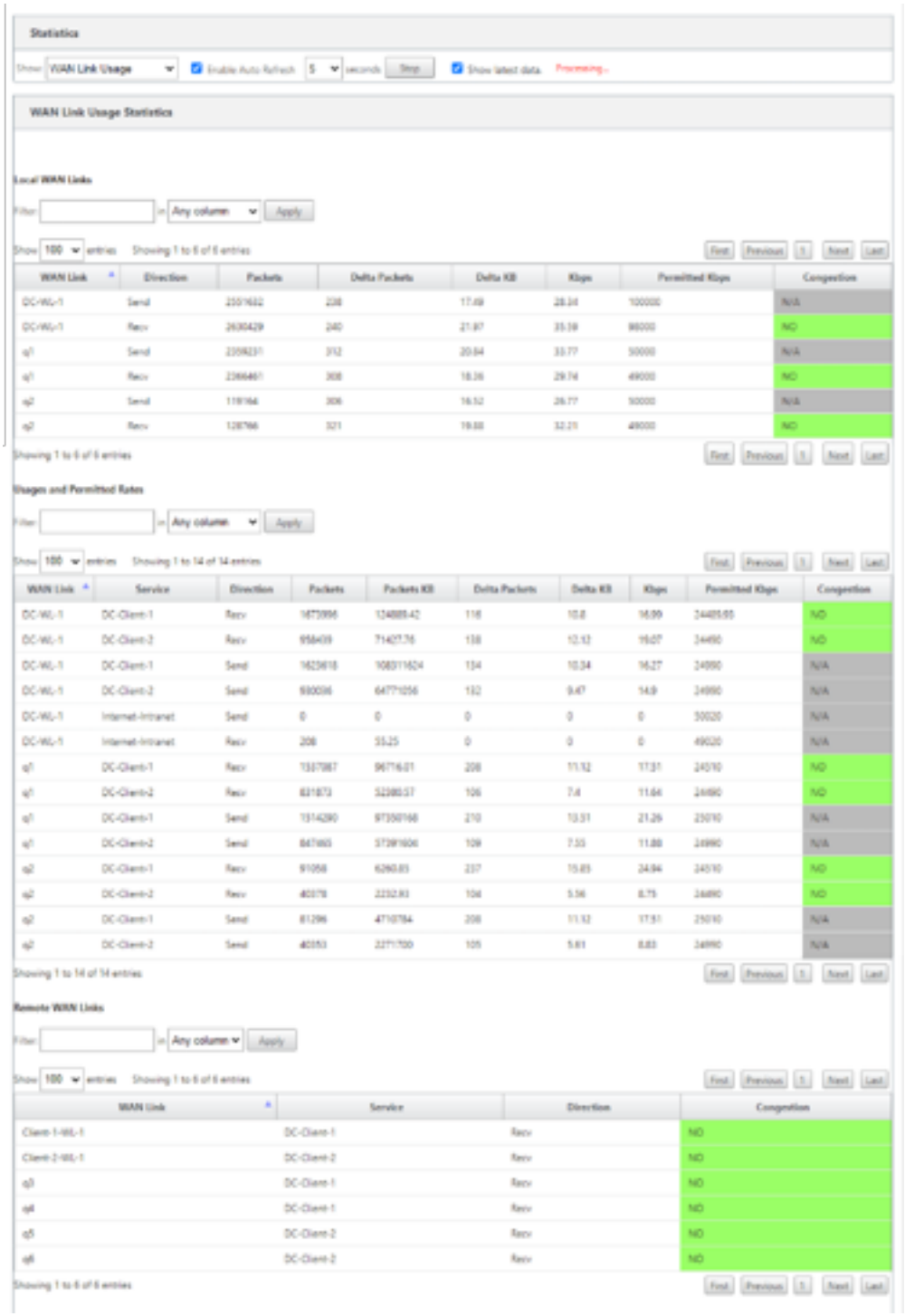
Zulässige Rate ist die Menge an Bandbreite, die eine bestimmte WAN-Verbindung, ein virtueller Pfaddienst, ein Intranetdienst oder ein Internetdienst zu einem bestimmten Zeitpunkt verwenden darf. Die zulässige Rate für eine WAN-Verbindung ist statisch und wird explizit in der SD-WAN-Konfiguration definiert. Der zulässige Tarif für einen virtuellen Pfaddienst, einen Intranetdienst oder einen Internetdienst schwankt im Laufe der Zeit als Reaktion auf Überlastung, Benutzernachfrage und faire Anteile, ist jedoch immer größer oder gleich der reservierten Mindestbandbreite für den Dienst.

WAN-Link überwachen

Gehen Sie zu **Monitor Statistiken**und wählen Sie **WAN-Link** aus der Dropdownliste **Anzeigen** aus.

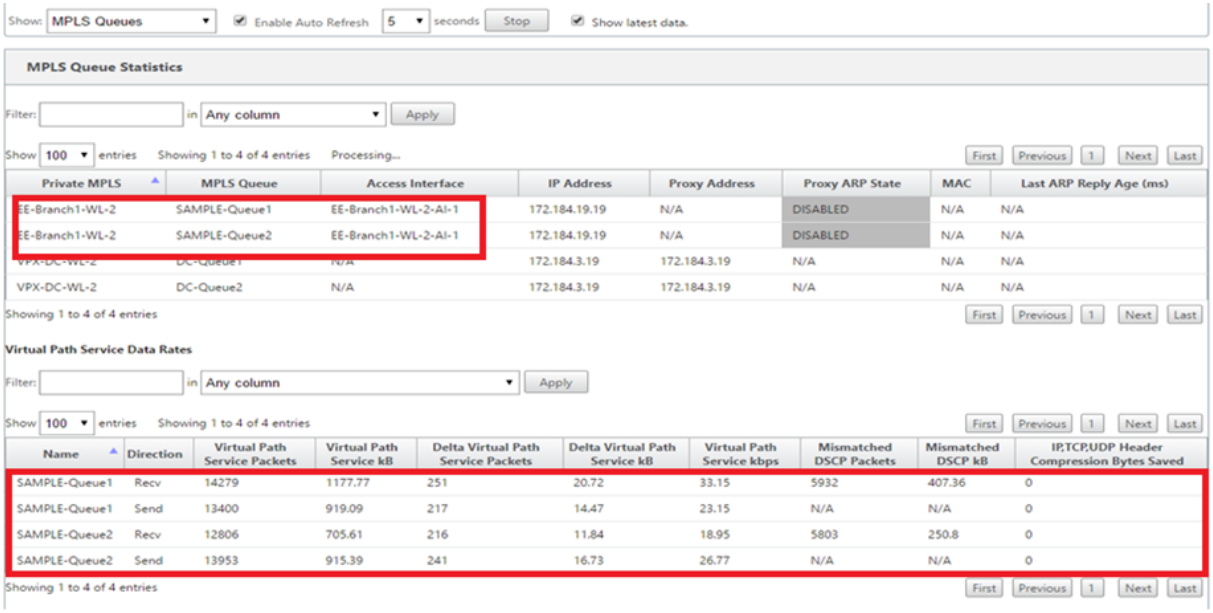


Gehen Sie zu **Monitor > Statistiken**und wählen Sie in der Dropdownliste **Anzeigen** die Option **WAN-Link-Nutzung** aus.



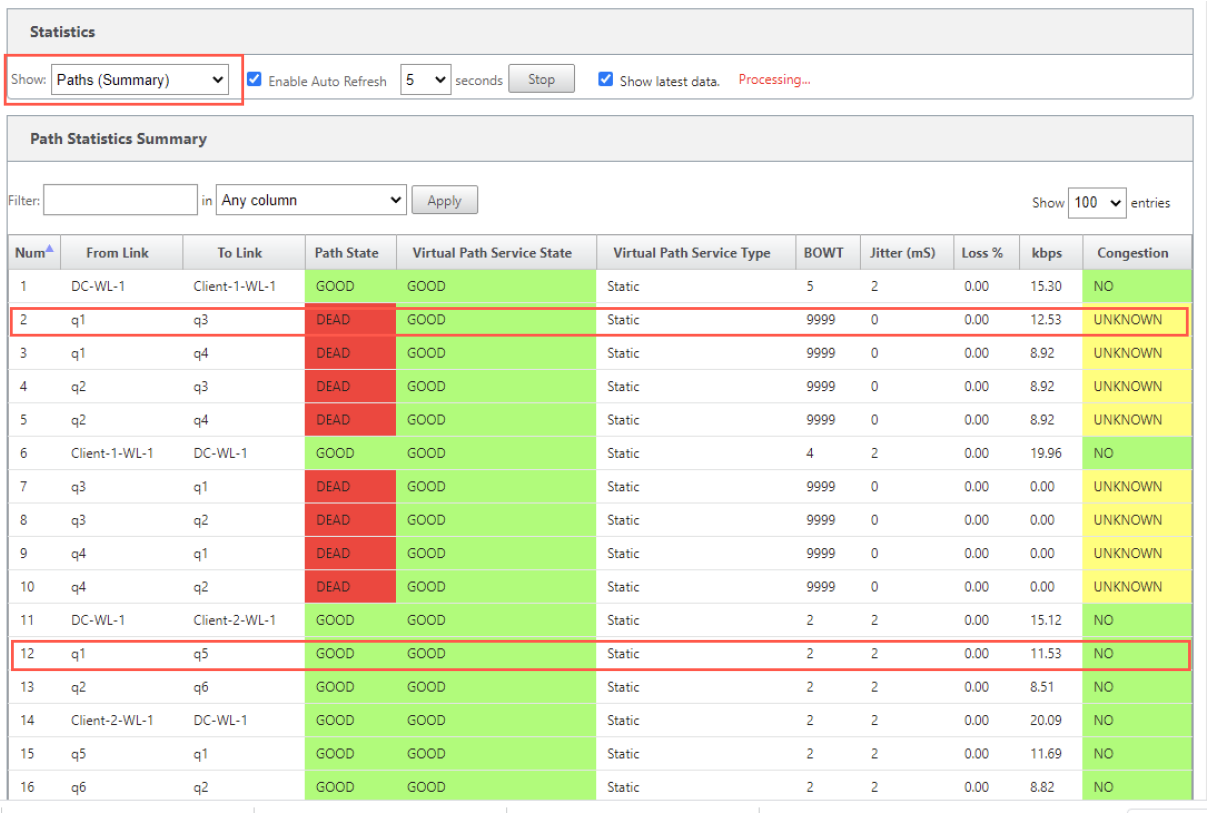
MPLS-Warteschlangen überwachen

Gehen Sie zu **Überwachen Statistiken**und wählen Sie in der Dropdownliste **Anzeigen** die Option **MPLS-Warteschlangen** aus.



Problembehandlung bei MPLS-Warteschlangen

Um den Status von MPLS-Warteschlangen zu überprüfen, navigieren Sie zu **Überwachen > Statistiken** und wählen Sie in der Dropdownliste **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.



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 Dropdownliste **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 Dropdownliste **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:

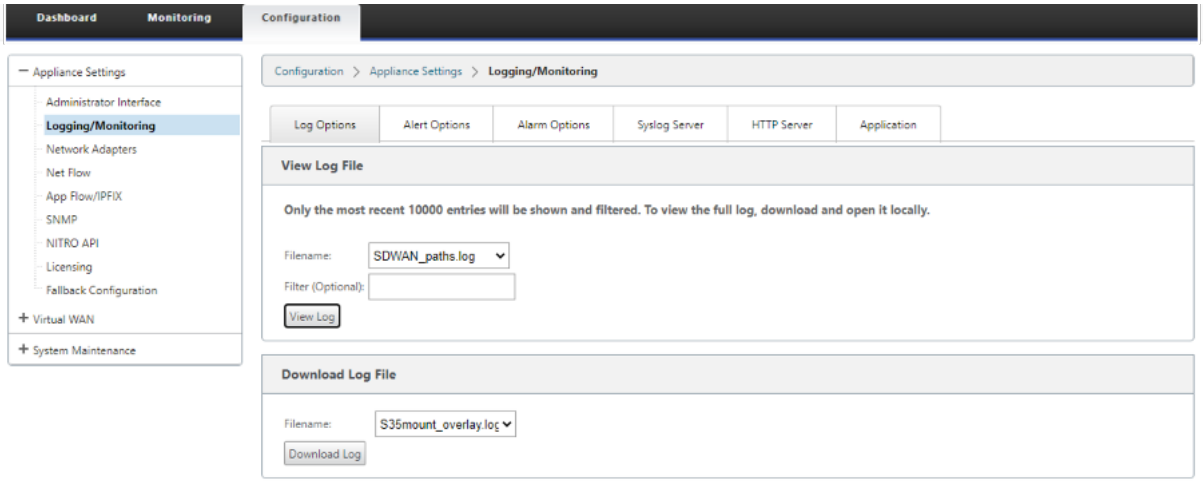
Filter: in Any column Apply

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-**

figuration > Logging/Monitoring und wählen Sie auf der Registerkarte **Log-Optionen** die Option **SDWAN_paths.log** oder **SDWAN_common.log** aus.



Berichterstellung

October 28, 2021

Anwendung QoE

Mehrere Net Flow Kollektoren

Anwendung QoE

October 28, 2021

Anwendung 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 **QoE-Wert der Anwendung** ist ein Wert zwischen 0 und 10. Der Wertungsbereich, in den er fällt, bestimmt die Qualität einer Anwendung.

Qualität	Reichweite
Gut	8–10
Fair	4–8
Schlecht	0–4

Qualität	Reichweite

Application QoE Score 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 Application QoE-Berechnung für Echtzeitanwendungen verwendet eine innovative Citrix Technik, die aus dem MOS-Score abgeleitet wird.

Die Standardschwellenwerte sind:

- Latenzschwelle: 160 ms
- Jitter-Schwellenwert: 30 ms
- Schwellenwert für Paketverlust: 2%

Ein Fluss einer Echtzeitanwendung, der die Schwellenwerte für Latenz, Verlust und Jitter erfüllt, wird als von guter Qualität angesehen.

QoE für Echtzeitanwendungen wird aus dem Prozentsatz der Flüsse, die den Schwellenwert erreichen, geteilt durch die Gesamtzahl der Flussproben bestimmt.

QoE für Echtzeit = (Anzahl der Flussproben, die den Schwellenwert erreichen/Gesamtzahl der Durchflussproben) * 100

Es wird als QoE-Score von 0 bis 10 dargestellt.

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 Paketverlust und Burst-Rate-Schwellenwerten basiert.

Interaktive Anwendungen reagieren empfindlich auf Paketverlust und -durchsatz. Daher messen wir den Prozentsatz des Paketverlusts und die Burst-Rate des Ein- und Ausstiegsverkehrs in einem Flow.

Die konfigurierbaren Schwellenwerte sind:

- Prozentsatz des Paketverlusts.
- Prozentsatz der erwarteten Austritt Burst Rate im Vergleich zur Ingress Burst Rate.

Die Standardschwellenwerte sind:

- Schwellenwert für Paketverlust: 1%
- Burst-Rate: 60%

Ein Fluss ist von guter Qualität, wenn die folgenden Bedingungen erfüllt sind:

- Der prozentuale Verlust für einen Fluss liegt unter dem konfigurierten Schwellenwert.
- Die ausgehende Burstrate entspricht mindestens dem konfigurierten Prozentsatz der eingehenden Burstrate.

Konfigurieren der Anwendung QoE

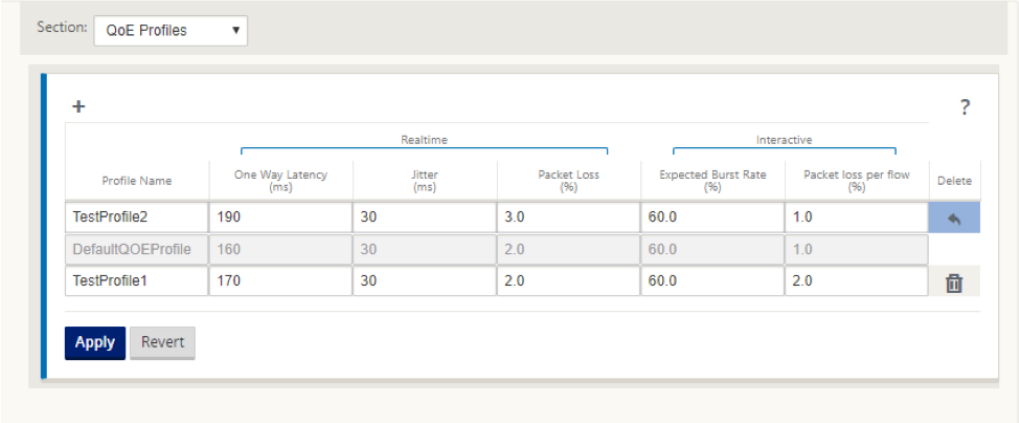
Ordnen Sie Anwendungs- oder Anwendungsobjekte Standard-oder benutzerdefinierten QoE-Profilen Sie können benutzerdefinierte QoE-Profile für Echtzeit- und interaktiven Datenverkehr erstellen.

So erstellen Sie benutzerdefinierte QoE-Profile:

1. Navigieren Sie im Konfigurationseditor zu **Global > Application QoE > QoE-Profile** und klicken Sie auf **+**.
2. Geben Sie einen Wert für die folgenden Parameter ein:
    - **Profilname**: Ein Name zur Identifizierung des Profils, das Schwellenwerte für Echtzeit- und interaktiven Verkehr festlegt.
    - **Echtzeit**: Konfigurieren Sie Schwellenwerte für Verkehrsflüsse, die die QoS-Richtlinie in Echtzeit treffen. Ein Fluss einer Echtzeitanwendung, der die unteren Schwellenwerte für Latenz, Verlust und Jitter erreicht, wird als von guter Qualität angesehen.
        - **Einweg-Latenz**: Der Latenzschwellenwert in Millisekunden. Der standardmäßige QoE-Profilwert beträgt 160 ms.

  - **Jitter**: Der Jitter-Schwellenwert in Millisekunden. Der standardmäßige QoE-Profilwert beträgt 30 ms.
  - **Paketverlust**: Der Prozentsatz des Paketverlusts. Der standardmäßige QoE-Profilwert beträgt 2%.

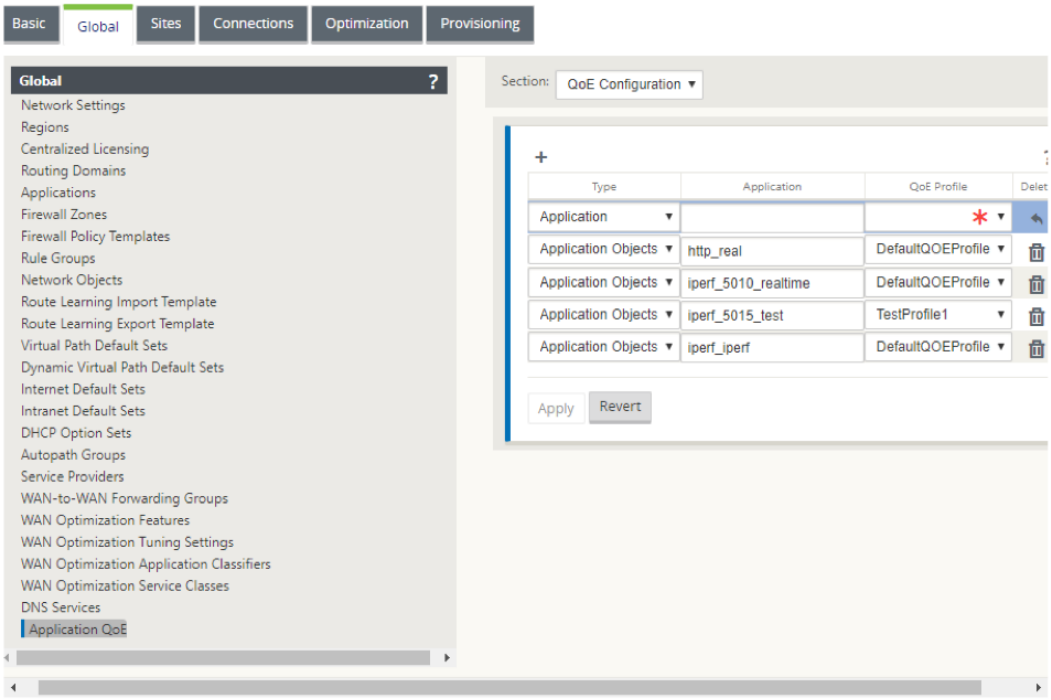
- **Interaktiv**: Konfigurieren Sie Schwellenwerte für Verkehrsflüsse, die die interaktive QoS-Richtlinie treffen. Ein Fluss einer interaktiven Anwendung, der den unteren Schwellenwert für Burst-Ratio und Paketverlust erreicht, wird als von guter Qualität angesehen.
  - **Erwartete Burst-Rate**: Der Prozentsatz der erwarteten Burst-Rate. Die ausgehende Burstrate sollte mindestens der konfigurierte Prozentsatz der eingehenden Burstrate sein. Der standardmäßige QoE-Profilwert beträgt 60%.
  - **Paketverlust pro Fluss**: Der Prozentsatz des Paketverlusts. Der standardmäßige QoE-Profilwert beträgt 1%.



3. Klicken Sie auf **Apply**.

So ordnen Sie Anwendungen oder Anwendungsobjekte mit QoE-Profilen zu:

1. Navigieren Sie im Konfigurationseditor zu **Global > Application QoE > QoE-Konfiguration** und klicken Sie auf **+**.
2. Wählen Sie Werte für die folgenden Parameter aus:
   - **Typ**: Eine DPI-Anwendung oder ein Anwendungsobjekt.
   - **Anwendung**: Suchen und wählen Sie eine Anwendung oder ein Anwendungsobjekt basierend auf dem ausgewählten Typ aus.
   - **QoE-Profil**: Wählen Sie ein QoE-Profil aus, das der Anwendung oder dem Anwendungsobjekt zugewiesen werden soll.



3. Klicken Sie auf **Apply**.

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 Bericht des Anwendungs-QOE-Berichts.

HDX QoE

October 28, 2021

Netzwerkparameter wie Latenz, Jitter und Paketabfall wirken sich auf die Benutzererfahrung von HDX-Benutzern aus. Quality of Experience (QoE) wird eingeführt, um den Benutzern zu helfen, ihre ICA-Qualität zu verstehen und zu überprüfen. QoE ist ein berechneter Index, der die ICA-Verkehrsleistung angibt. Die Benutzer können die Regeln und Richtlinien zur Verbesserung der QoE einstellen.

Die QoE ist ein numerischer Wert zwischen 0—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 Flussstufe 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 HDX-Dashboard von Citrix SD-WAN Orchestrator können Sie eine grafische Darstellung der Gesamtqualität von HDX-Anwendungen anzeigen. Die HDX-Anwendungen werden in die folgenden drei Qualitätskategorien eingeteilt:

Qualität	QoE-Bereich
Gut	80–100
Fair	50–80
Schlecht	0–50

Eine Liste der untersten fünf Websites mit der geringsten QoE wird ebenfalls im HDX-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 HDX-Dashboard und -Berichte.

> **Hinweis**
>
> - *Erwarten Sie nicht, dass die Latenz der WAN-Verbindung, der Jitter und der Paketabwurf immer mit Anwendungslatenz, Jitter und Paketabfall übereinstimmen. Der Verlust von WAN-Verbindungen korreliert mit dem tatsächlichen WAN-Paketverlust, während der Anwendungsverlust nach der erneuten Übertragung auftritt, was geringer ist als der Verlust der WAN-Verbindung.*
> - *Die in der GUI angezeigte WAN-Link-Latenz ist BOWT (beste Einwegzeit). Es ist die beste Metrik des Links, um den Zustand des Links zu beurteilen. Die Anwendung QoE verfolgt und berechnet die Gesamt- und Durchschnittslatenz aller Pakete für diese Anwendung. Dies stimmt oft nicht mit dem Link BOWT überein.*
> - *Wenn eine MSI-Sitzung während des ICA-Handshakes beginnt, wird die Sitzung möglicherweise vorübergehend als 4 SSI statt als 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.*

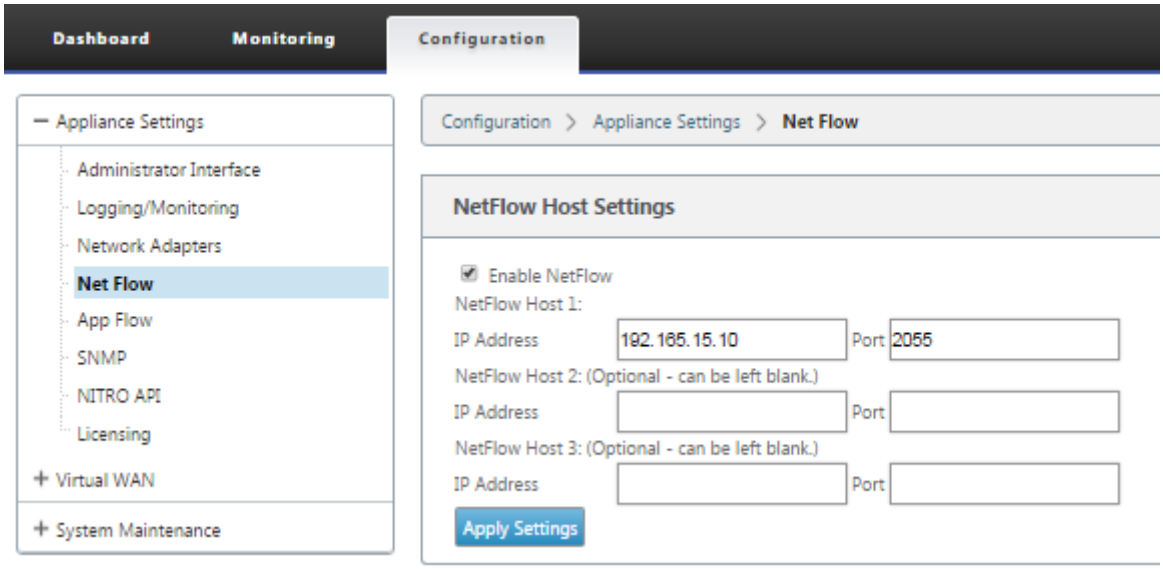
Mehrere Net Flow Kollektoren

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.

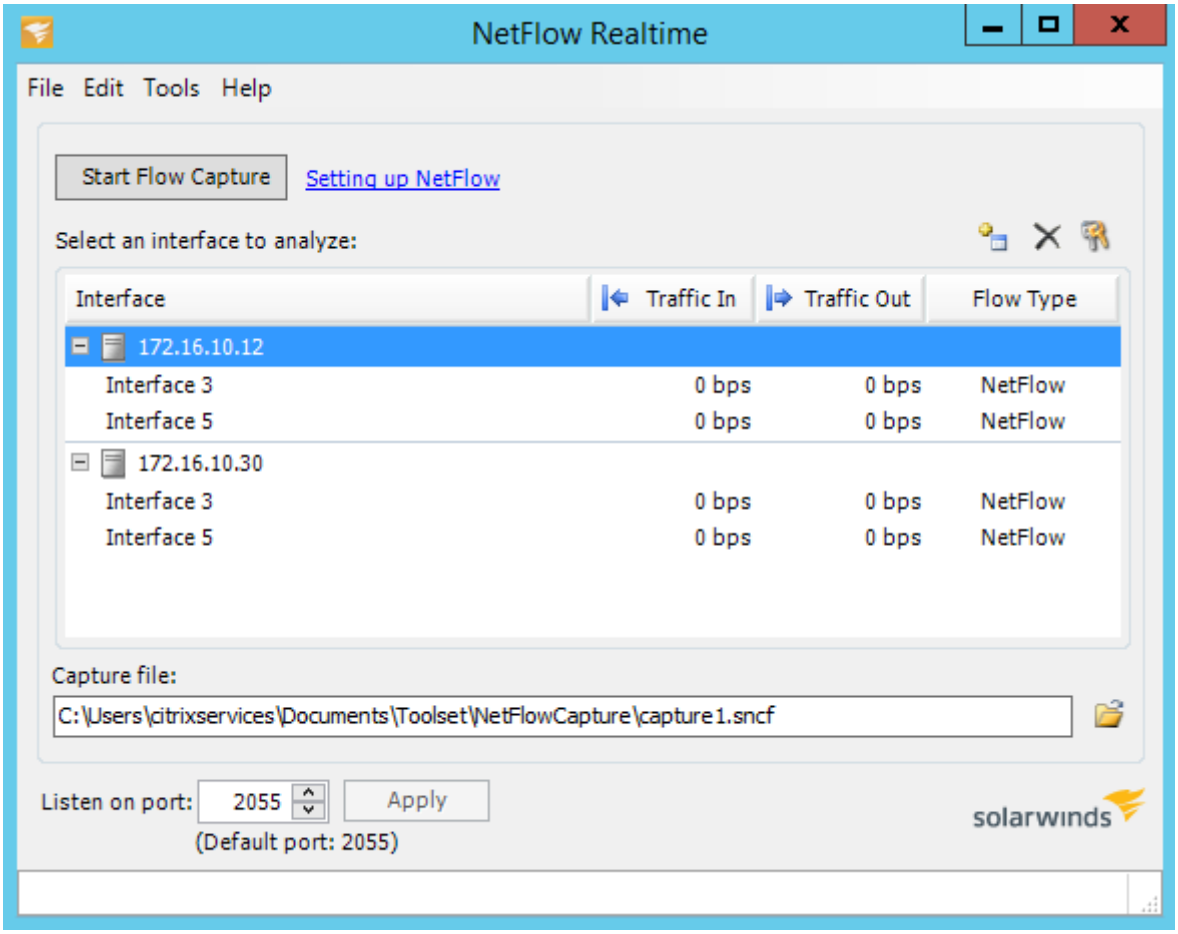
So konfigurieren Sie Net Flow-Hosts:

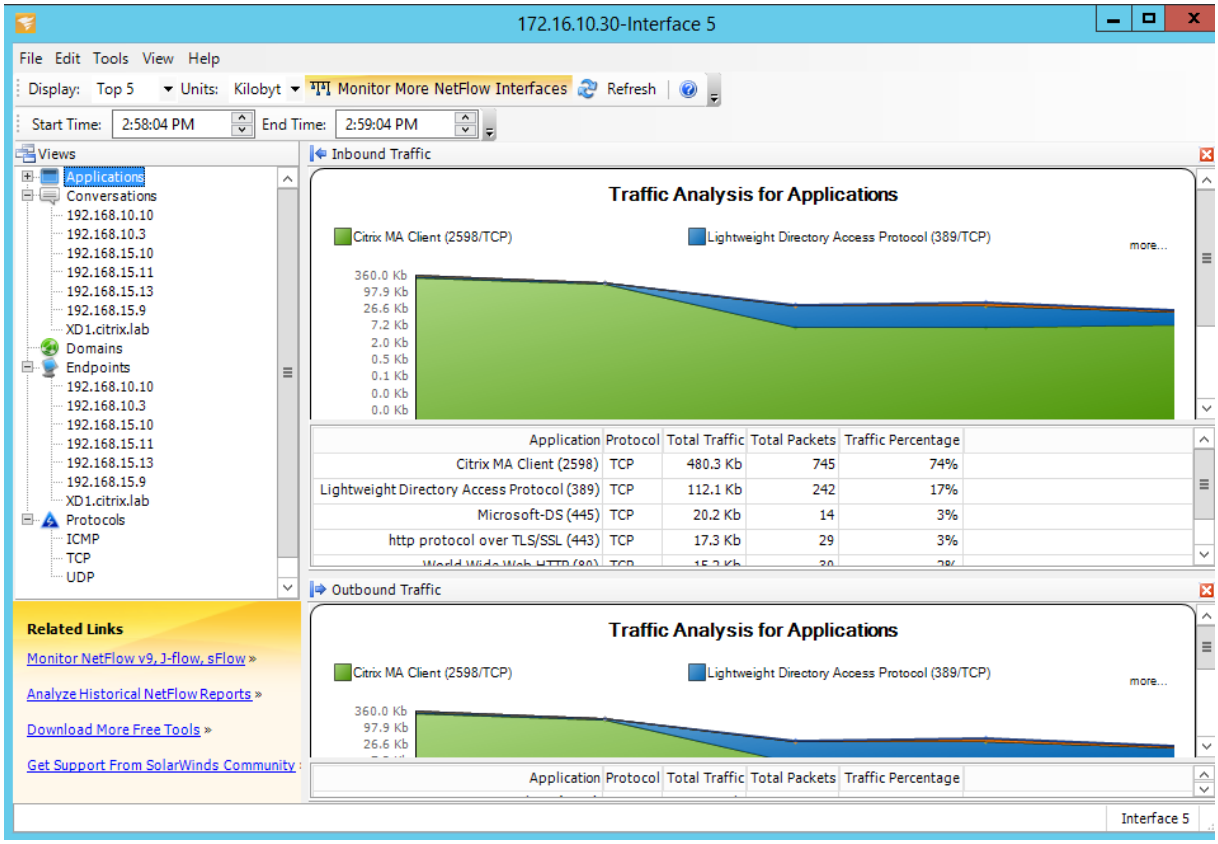
Navigieren Sie zur Seite **Konfiguration > Appliance-Einstellungen > Net Flow Netflow-Host-Einstellungen**. Klicken Sie auf das **KontrollkästchenNetFlow aktivieren**, geben Sie die**IP-Adresse**und die**Portnummern**für bis zu drei Net Flow-Hosts ein und klicken Sie dann auf**Einstellungen anwenden, 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.





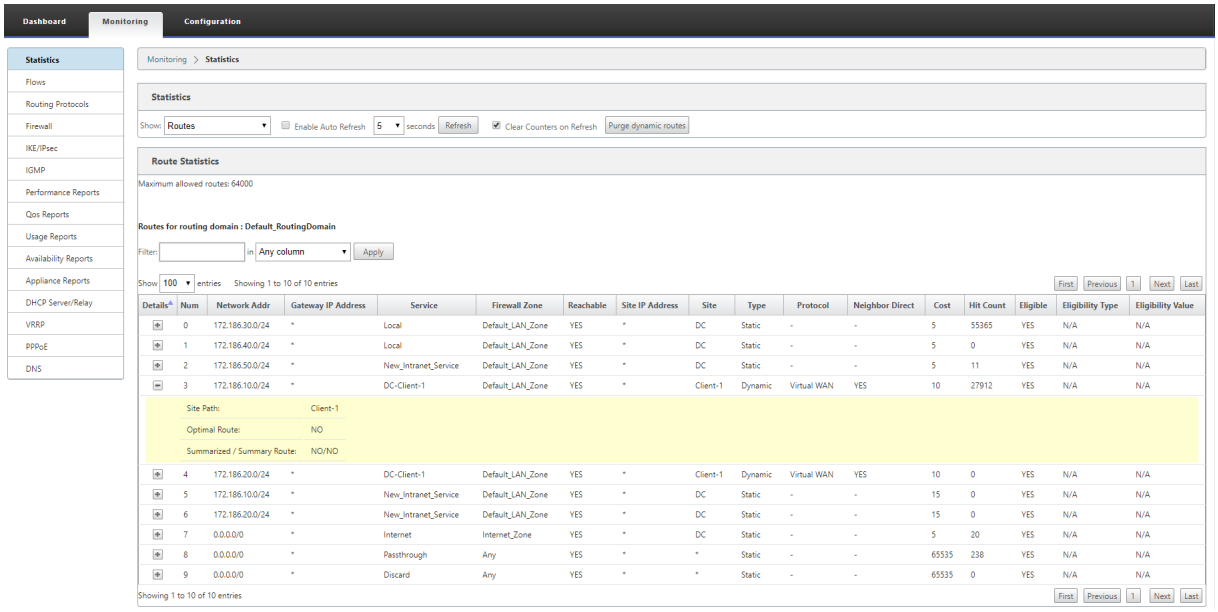
NetFlow-Einschränkungen

- 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 Internet-standard 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

October 28, 2021

Um Routenstatistiken Ihrer SD-WAN-Appliances anzuzeigen, navigieren Sie in der SD-WAN-GUI zu **Überwachung** > **Statistiken** > **Routen**.



Sie können die folgenden Parameter anzeigen:

- **Netzwerkadresse**: Die Netzwerkadresse und Subnetzmaske der Route.
- **Details**: Klicken Sie auf +, um die folgenden Informationen anzuzeigen.
  - **Site Path**: Site Path ist eine Quelle der Wahrheit Metrik für das empfangene Präfix. Es wird in Situationen verwendet, in denen die WAN-zu-WAN-Weiterleitung auf mehreren Geräten und in der Mesh-Bereitstellung aktiviert ist. Es werden mehrere solcher Präfixe empfangen, und die Administratoren können die Präfix-Attribute anhand des Standortpfads beurteilen.

    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 kommen. Geo MCN und MCN haben die 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 unterschiedlichen Präfixe wird die Routingtabelle mit ihrer Standortpfadmetrik aktualisiert. Die Standortpfadmetrik gibt den Ursprung des Routenpräfixes und die damit verbundenen Kosten an, um zu Branch2 zu gelangen.
  - **Optimale Route**: Die optimale Route zeigt 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.
  - **Zusammenfassende/Zusammenfassungsroute**: Eine Übersichtsroute 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 Übersichtsroute fallen.

Angenommen, wir haben eine Zusammenfassungsroute 172.16.0.0/16. Dies ist nur eine zusammenfassende Route und keine zusammengefasste Route. Eine zusammenfassende Route hat Zusammenfassung "JA"und "NEIN"zusammengefasst. 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 "JA"und Zusammenfassung "NEIN"zusammengefasst.

- **Gateway-IP-Adresse**: Die IP-Adresse des Gateways/der Route, mit der diese Route erreicht wurde.
- **Dienst**: Der Typ des Citrix SD-WAN-Dienstes.
- **Firewall-Zone**: Die von der Route verwendete Firewall-Zone.
- **Erreichbar**: Ist die Route erreichbar oder nicht.
- **Site-IP-Adresse**: Die IP-Adresse der Site.
- **Seite**: Der Name der Site.
- **Typ**: Die Art einer Route hängt von der Quelle des Routenlernens ab. Die Routen auf der LAN-Seite und Routen, die während der Konfiguration manuell eingegeben wurden, sind statische Routen. Von den SD-WAN- oder dynamischen Routing-Peers erlernte Routen sind dynamische Routen.
- **Protokoll**: Das Protokoll der Präfixe.
  - **Lokal**: Lokale virtuelle IPs der Appliance.
  - **Virtuelles WAN**: Präfixe, die von Peer-SD-WAN-Appliances gelernt wurden.
  - **OSPF**: Präfixe, die vom dynamischen OSPF-Routing-Peer gelernt wurden.
  - **BGP**: Präfixe wurden vom dynamischen BGP-Routing-Peer gelernt.
- **Neighbor Direct**: Zeigt an, ob das Subnetz mit dem Zweig verbunden ist, von dem die Route zur Appliance kam.
- **Kosten**: Die Kosten, die zur Bestimmung des besten Pfads zu einem Zielnetzwerk verwendet werden.
- Anzahl der**Treffer**: Die Häufigkeit, mit der eine Route getroffen wurde, um ein Paket an dieses Subnetz weiterzuleiten.
- **Berechtigt**: Zeigt an, dass die Route berechtigt ist und zum Weiterleiten oder Weiterleiten der Pakete an das Präfix verwendet wird, das während der Verkehrsverarbeitung 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. Beispielsweise kann eine Route basierend auf einem Pfad als berechtigt bezeichnet werden MCN-WL-1->BR1-WL-2. Der Berechtigungswert für diese Route im Streckenabschnitt ist also der Wert MCN-WL-1->BR1-WL-2.

Routing

October 28, 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 nahtloser 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 zusammenfassende Route ist eine einzelne Route, die zur Darstellung mehrerer Routen verwendet wird. Es spart Bandbreite, indem eine Anzeige für eine einzelne Route gesendet wird, wodurch die Anzahl der Verbindungen zwischen Routern reduziert wird. Es spart Speicher, da nur eine Routenadresse beibehalten 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. Mit VRRP können Sie zwei oder mehr Router 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

October 28, 2021

Citrix SD-WAN bietet robuste und robuste Konnektivität zwischen Remotestandorten, Rechenzentren und Cloud-Netzwerken. Die SD-WAN-Lösung kann dies erreichen, indem Tunnel zwischen SD-WAN-Appliances im Netzwerk eingerichtet werden, die die Konnektivität zwischen Standorten ermöglichen,

indem Routentabellen angewendet werden, die das vorhandene Unterlagennetzwerk überlagern. 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-Routingtabelle

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 auch durch ihren Servicetyp 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 Virtual Interface-Subnetze (erstellt automatisch lokale Routen) und jede in der Routentabelle definierte lokale Route (mit einem lokalen nächsten Hop). Die Route wird anderen SD-WAN-Appliances angekündigt, die über einen virtuellen Pfad zu diesem lokalen Standort verfügen, an dem diese Route konfiguriert wird, wenn sie als Partner vertraut wird.

> **Hinweis**
>
> Seien Sie vorsichtig beim Hinzufügen von Standardrouten und Zusammenfassungsrouten als lokale Routen, 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 für die Zustellung an einen Standort klassifiziert, der keine SD-WAN-Lösung hat.

> **Hinweis**
>
> Beachten Sie, dass es beim Hinzufügen einer Intranet-Route keinen nächsten Hop gibt, sondern eine Weiterleitung zu einem Intranetdienst. Der Dienst ist mit einer bestimmten WAN-Verbindung verknüpft.

- **Internet** - Dies ähnelt Intranet, wird jedoch verwendet, um den Datenverkehr zu definieren, der zu öffentlichen Internet-WAN-Verbindungen und nicht zu privaten WAN-Verbindungen fließt. Ein einzigartiger Unterschied besteht darin, dass der Internetdienst mehreren WAN-Verbindungen zugeordnet und auf Lastausgleich (pro Fluss) oder Aktiv/Backup eingestellt werden kann. Eine Standard-Internetroute wird erstellt, wenn der Internetdienst aktiviert ist (standardmäßig ist sie ausgeschaltet). Jeder Datenverkehr, der dieser Route (Subnetz) entspricht, wird für diese Appliance als Internet für die Zustellung an öffentliche Internetressourcen klassifiziert.

> **Hinweis**
>
> Internetdienstrouten können für die anderen SD-WAN-Appliances angekündigt oder am Exportieren gehindert werden, je nachdem, ob Sie den Internetzugang über die virtuellen Pfade zurückziehen.

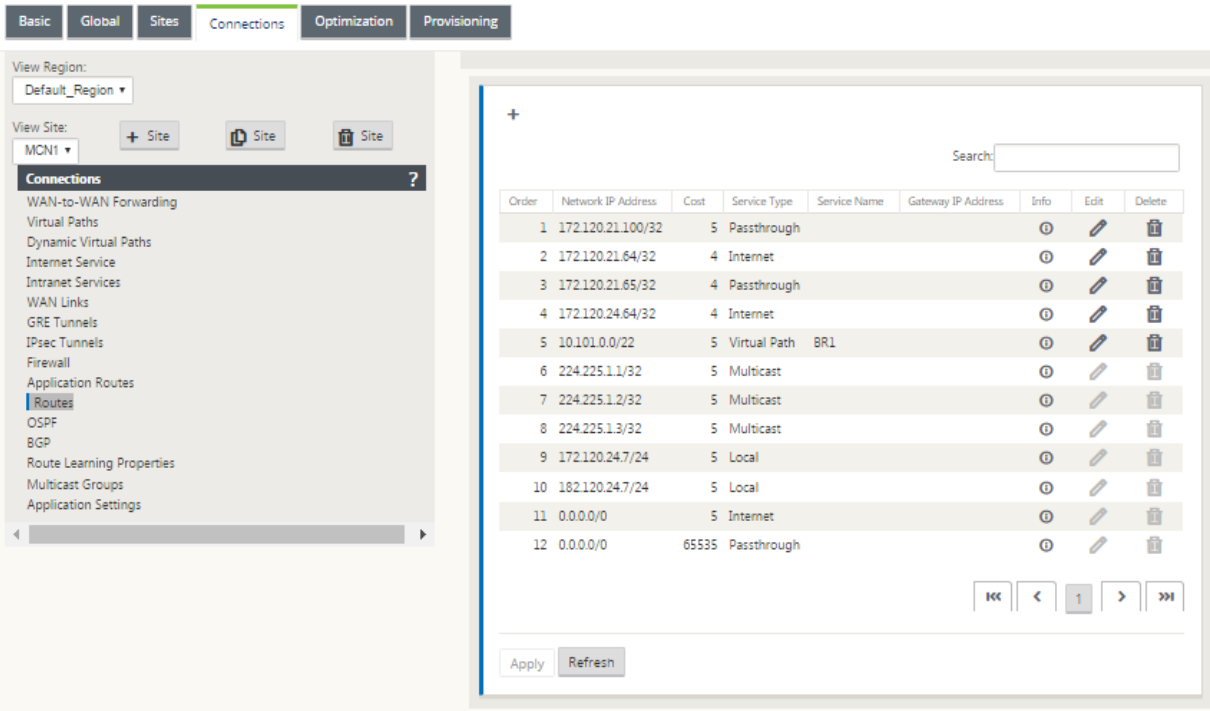
- **Passthrough** —Dieser Dienst fungiert als letzter Ausweg oder Override-Dienst, wenn sich eine Appliance im Inline-Modus befindet. Wenn eine Ziel-IP-Adresse nicht mit einer anderen Route übereinstimmt, leitet die SD-WAN-Appliance sie einfach an die WAN-Verbindung im nächsten Hop weiter. Eine Standardroute: 0.0.0.0/0 Kosten von 16 Pass-Through-Routen 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 außerhalb 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:



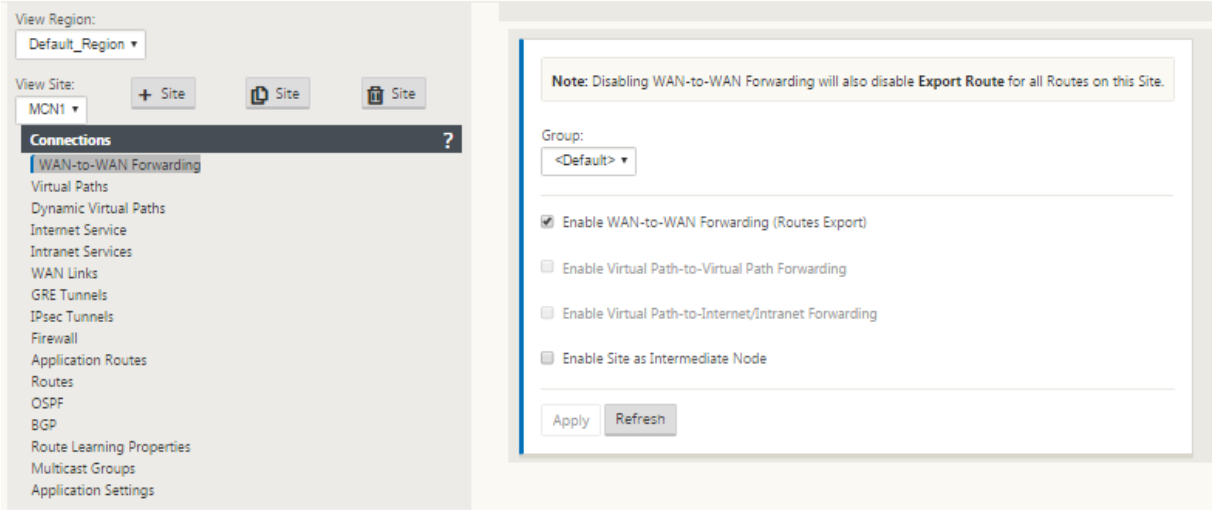
Routentabelleneinträge werden aus verschiedenen Eingaben aufgefüllt:

- 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.
- Der Administrator definierte statische Routen pro Standort, die auch als lokale Route vom Servicetyp definiert werden.
- Ein Standardwert (0.0.0.0/0) fängt alle Routen ab, wobei Kosten 16 als Passthrough definiert sind.

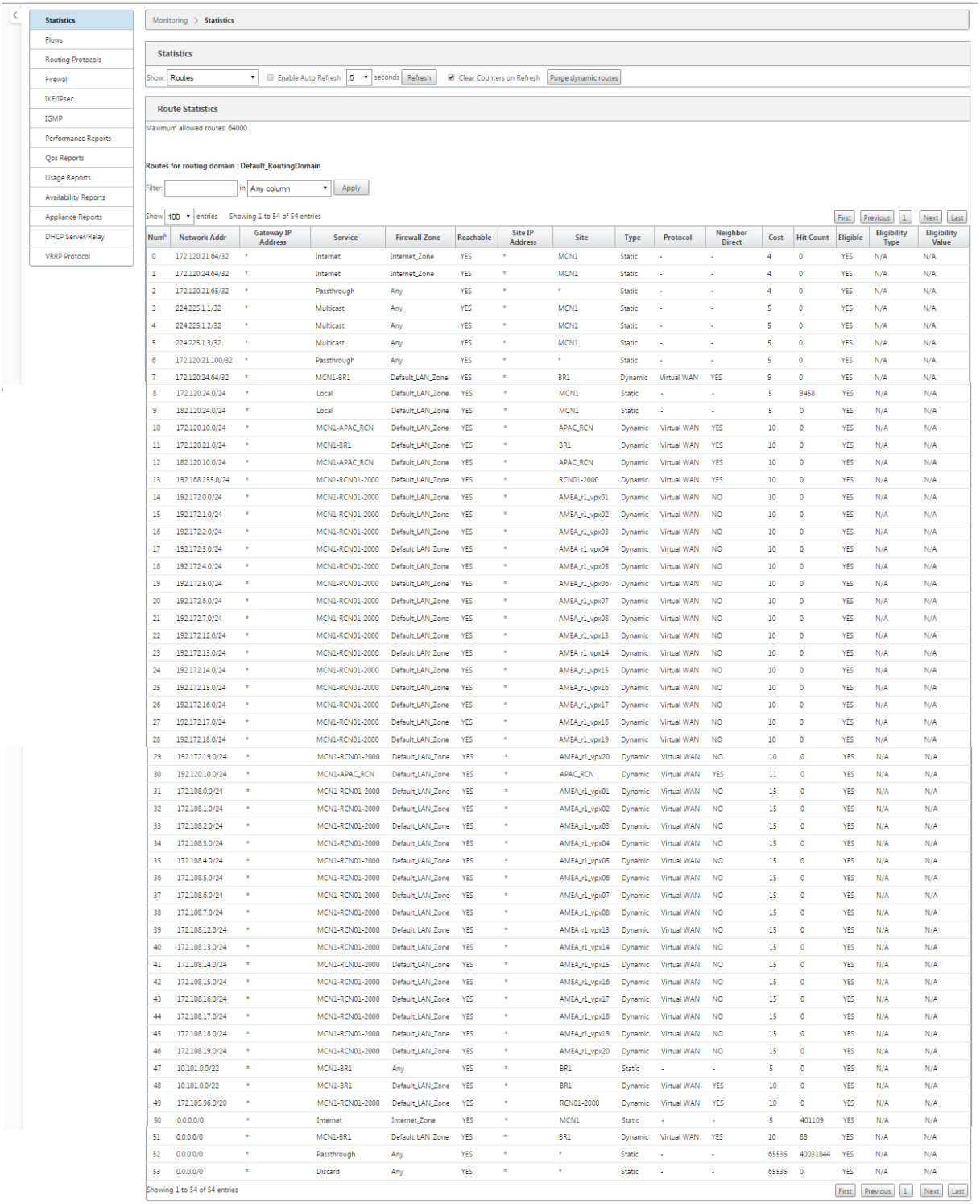
Administratoren können eine der oben genannten Routen konfigurieren, aber zusätzlich zu den Routenkosten auch einen Diensttyp, nächsten Hop oder Gateway einschließen. Zu jedem Routentyp

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 Dropdownliste **Anzeigen** ausgewählt sind.

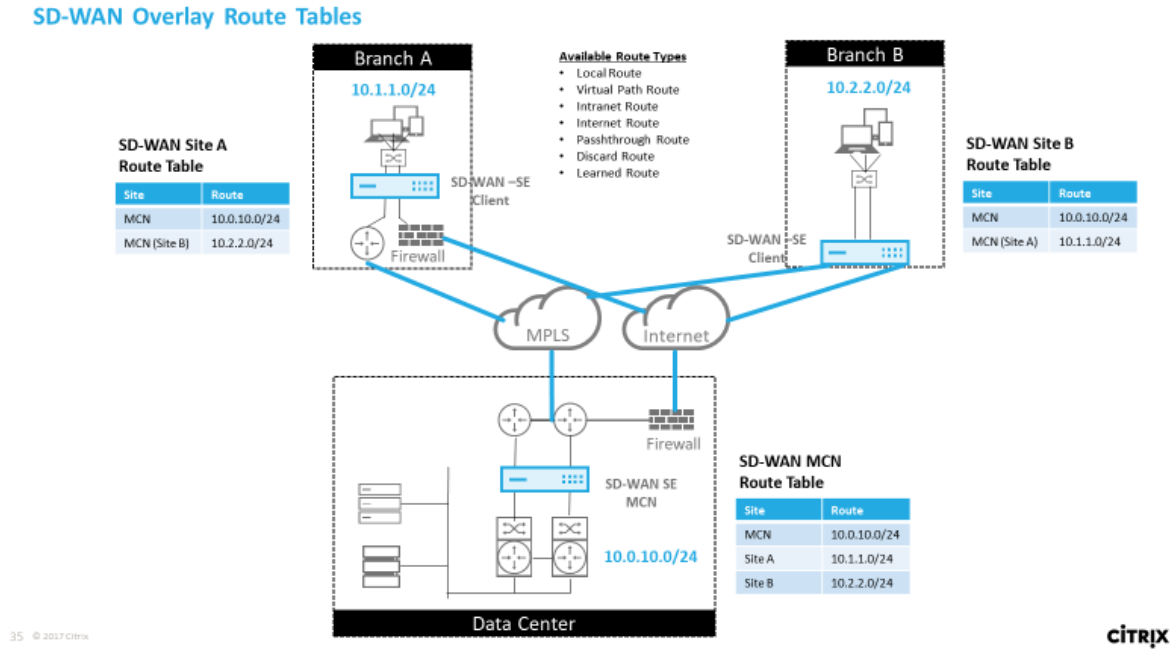


Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	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	40031844	YES	N/A	N/A
53	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

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.



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 einer /31-Route voraus. Bei zwei /32-Strecken geht eine kostengünstige 4-Route immer einer Route mit Kosten 5 voraus. 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 (virtueller Pfad) Traffic Route Matching:
  1. Eingehender Verkehr 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 (virtueller Pfad) Traffic Route Matching:
  1. Virtual Path Traffic wird von SD-WAN vom Tunnel empfangen und verarbeitet.
  2. Die Appliance vergleicht die Quell-IP-Adresse, um festzustellen, ob die Quelle lokal ist.
     - Wenn ja, dann ist WAN berechtigt und passt das IP-Ziel mit der Routingtabelle/dem virtuellen Pfad an.
     - Wenn nein - dann wurde die 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 für Citrix SD-WAN Routingprotokoll

Citrix SD-WAN Version 9.1 führte OSPF- und BGP-Routingprotokolle in die Konfiguration ein. Die Einführung von Routing-Protokollen in SD-WAN ermöglichte eine einfachere Integration von SD-WAN in

komplexere Unterlagsnetzwerke, in denen Routing-Protokolle aktiv verwendet werden. Da dieselben Routingprotokolle auf SD-WAN aktiviert waren, wurde die Konfiguration von Subnetzen erleichtert, die für die Verwendung des SD-WAN-Overlays bestimmt sind. Darüber hinaus ermöglichen die Routing-Protokolle die Kommunikation zwischen SD-WAN- und Nicht-SD-WAN-Standorten mit direkter Kommunikation mit bestehenden Kunden-Edge-Routern unter Verwendung des gemeinsamen Routing-Protokolls. 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.

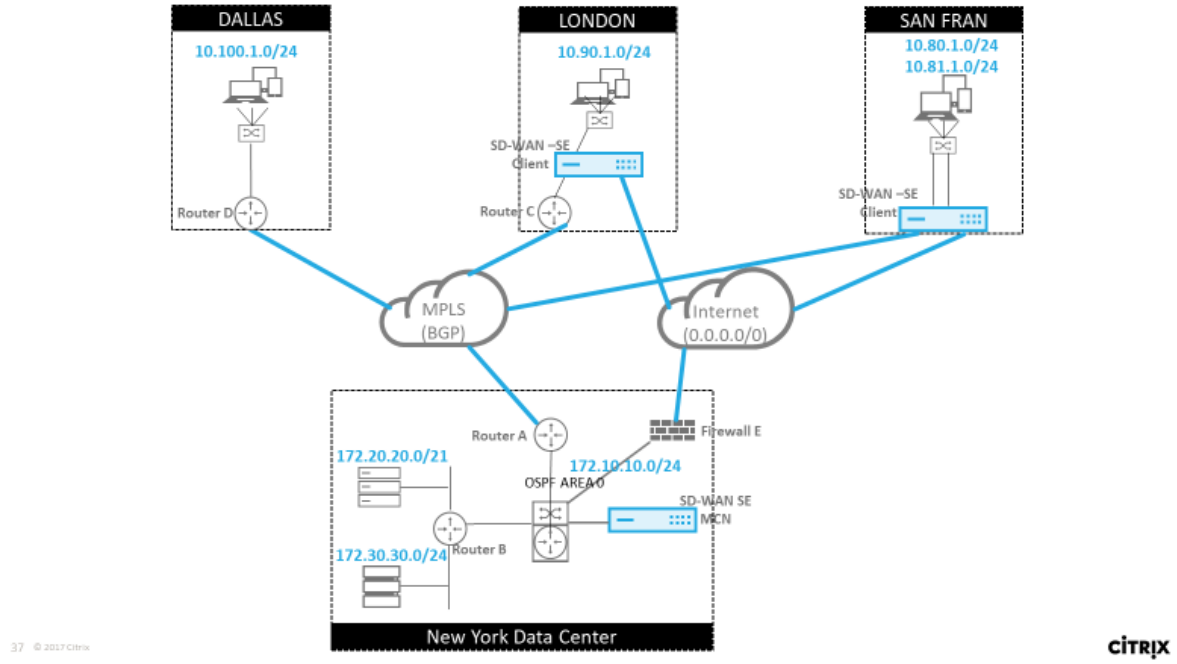
> **Wichtig**
>
> Es ist einfach, den unerwünschten Weg zu lecken, wenn Sie nicht vorsichtig sind.

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 IGPs 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 Ankündigungsrouten von der SD-WAN-Appliance zu aktivieren. Verwenden Sie die Import- und Exportfilter für eine schrittweise Einführung von Routing-Protokollen 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 Autonome Systemnummer (ASN).

Im New Yorker Rechenzentrum wird OSPF ausgeführt, um die Kernsubnetze des Rechenzentrums an die Remotestandorte 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 Yorker Rechenzentrum, dass das SD-WAN im virtuellen Inline-Modus bereitgestellt wird. Die Absicht besteht darin, am vorhandenen OSPF-Routing-Protokoll teilzunehmen, um den Datenverkehr als bevorzugtes Gateway an die Appliance weiterzuleiten.

- Der Standort London wird im traditionellen Inline-Modus eingesetzt. Der Upstream-WAN-Router (C) wird weiterhin das Standardgateway für das Londoner Subnetz sein.
- Der Standort San Francisco ist ein neu eingeführter Standort für dieses Netzwerk, und das SD-WAN soll im Edge/Gateway-Modus bereitgestellt werden und als Standardgateway 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 Subnetze von Dallas (10.90.1.0/24) und London (10.100.1.0/24) über 172.10.10.1 (MPLS Router A) verfügbar sind. Die Streckenkosten 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 eine niedrigere administrative Domäne und kostet standardmäßig 20/1 im Vergleich zu OSPF 110/10.

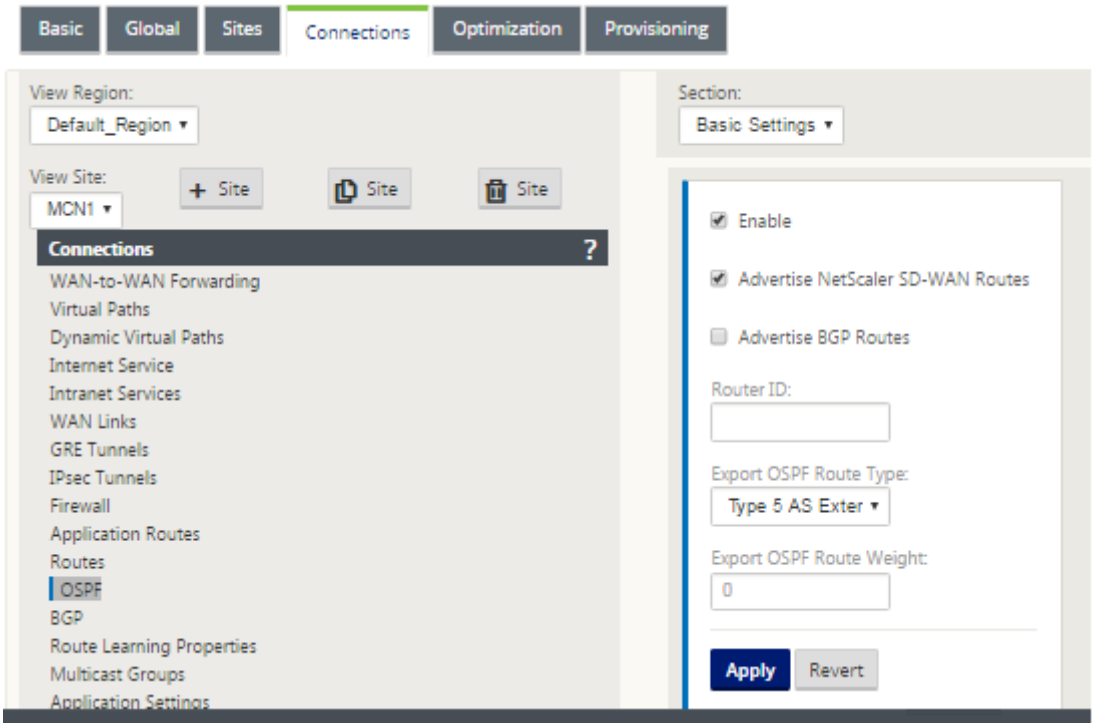
Dallas Router D:

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
```

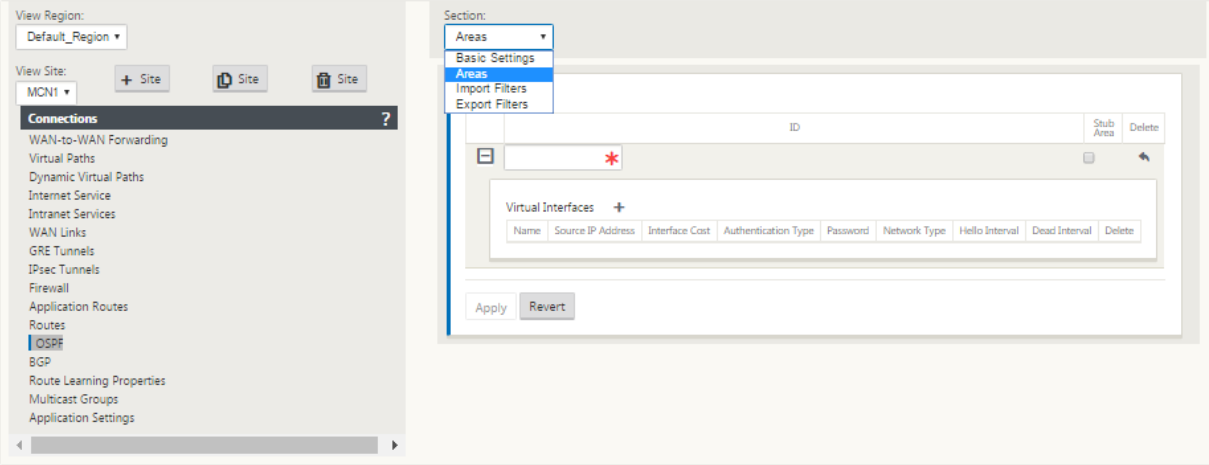
> **Hinweis**
>
> In diesem Beispiel können Sie das Subnetz 192.168.65.0/24 ignorieren. Dies ist ein Management-Netzwerk und nicht relevant für das Beispiel. Alle Router sind mit dem Management-Subnetz verbunden, werden jedoch in keinem Routingprotokoll angekündigt.

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.

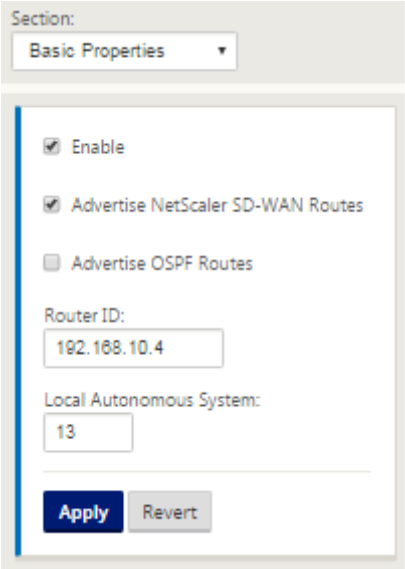
Wenn OSPF über das WAN (also MPLS-Netzwerke) verwendet wird, kann dies in Typ 1 innerhalb des Bereichs geändert werden. OSPF-Bereiche können wie unten dargestellt konfiguriert werden.

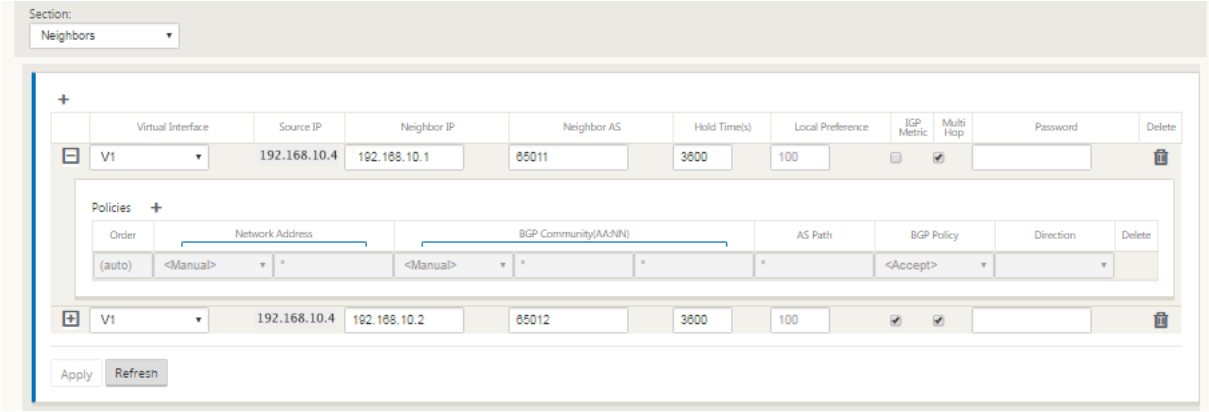


Bereich 0 hinzugefügt mit dem lokalen Netzwerk abgeleitet von der virtuellen Schnittstelle (172.10.10.0), alle anderen Einstellungen wurden standardmäßig belassen.

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.





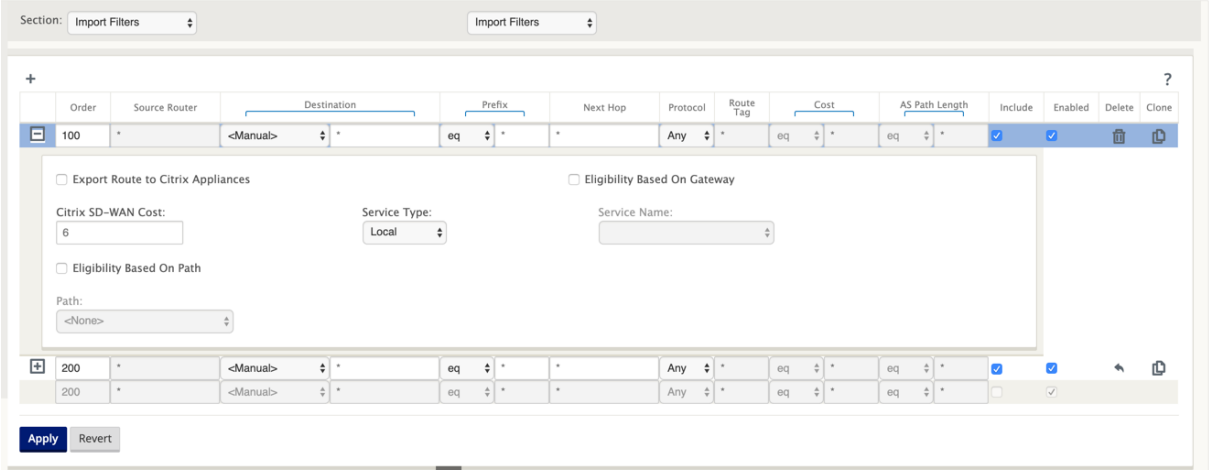
Der eBGP-Peers untereinander. Jede ASN ist anders.

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 die Routing-Tabelle ein- und ausgeht. Wir betrachten jeden Standort nacheinander.

- 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

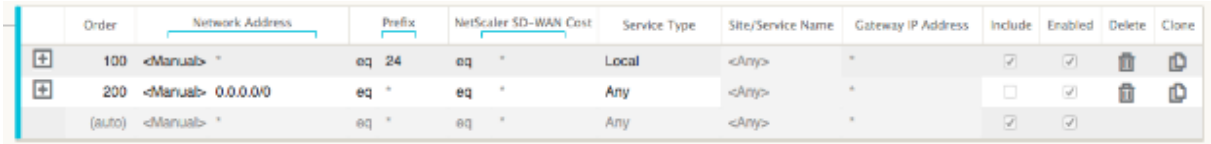
Virtual Path Overlay ausfällt und die Umgebung auf die Verwendung von MPLS zurückgreifen muss. Wir wollen auch nichts lesen, was SD-WAN von eBGP bis zu den SD-WAN-Routern lernt. Um dies zu erreichen, müssen die Filter wie folgt konfiguriert werden:

- Importieren Sie alle Routen aus eBGP. Routen nicht in SD-WAN-Appliances lesen/exportieren.



- Lokale Routen nach eBGP exportieren

Die Standardregel für den Export lautet, alles zu exportieren. Regel 200 wird verwendet, um die Fehlerregel außer Kraft zu setzen, um die Routen nicht zu revertisieren. Jede Route, die mit einem Präfix SD-WAN übereinstimmt, hat über die virtuellen Pfade gelernt.



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 durch eBGP vom San Francisco SD-WAN aus 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 Apply

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

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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

Citrix SD-WAN 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 insofern statisch, als 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.

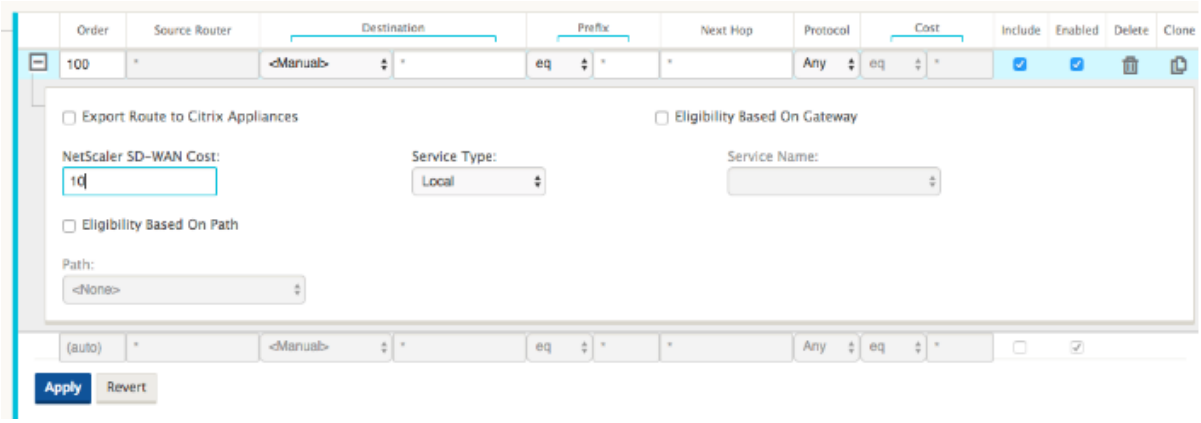
- Als beworbene Route durch BGP (Nummer 6), mit einem Preis von 6. Dies gilt jetzt als Fallback-Route.

Da das Präfix gleich ist und die Kosten unterschiedlich sind, verwendet SD-WAN die virtuelle Pfadroute, 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 Routing-protokoll, 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.



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.

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) First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
12	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
13	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

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 letzter Ausweg verwendet. Wenn also ein Paket nicht mit einer spezifischeren Route abgeglichen werden kann, leitet SD-WAN es an den nächsten Hop der Schnittstellengruppe weiter. Wenn sich das SD-WAN außerhalb des Pfades befindet oder sich im Edge-/Gateway-Modus befindet, gibt es keinen Passthrough-Dienst. In diesem Fall verlässt SD-WAN das Paket mithilfe der standardmäßigen Discard-Route. Die Anzahl der Treffer gibt die Anzahl der Pakete an, die jede Route erreichen, was bei der Fehlerbehebung wertvoll sein kann.

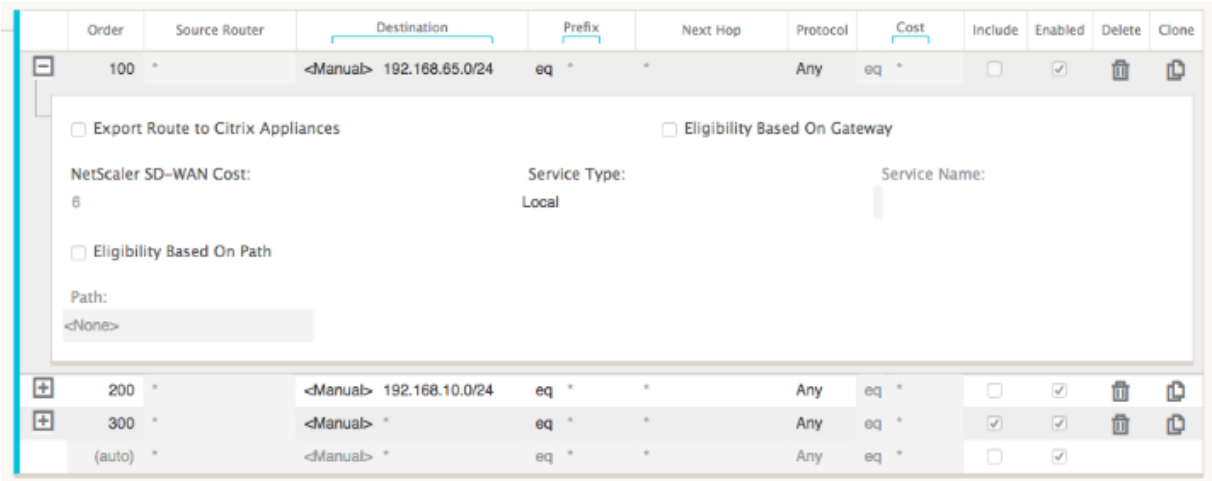
Wenn wir uns jetzt auf die New Yorker Site konzentrieren, möchten wir den Datenverkehr für entfernte Standorte (London und San Francisco) an die SD-WAN-Appliance weiterleiten, wenn der virtuelle Pfad aktiv ist.

Auf der New Yorker Site sind mehrere Subnetze verfügbar:

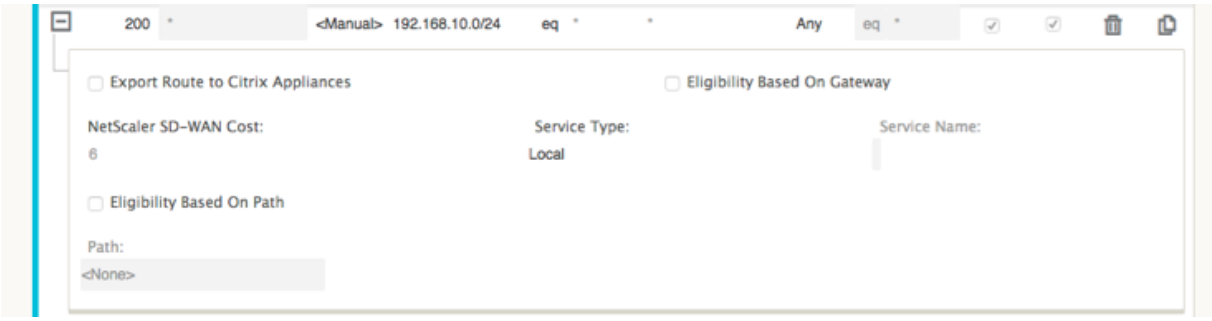
- 172.10.10.0/24 (direkt angeschlossen)
- 172.20.20.0/24 (über OSPF vom Core-Router B aus beworben)
- 172.30.30.0/24 (über OSPF vom Core-Router B aus beworben)

Wir müssen auch den Verkehrsfluss nach Dallas (10.100.1.0/24) über MPLS bereitstellen.

Schließlich wollen wir die gesamte internetgebundene Verkehrsroute zur Firewall E bis 172.10.10.3 als nächsten Hop. SD-WAN lernt diese Standardroute über OSPF und kündigt über den virtuellen Pfad an. Die Filter für die New Yorker Site sind:

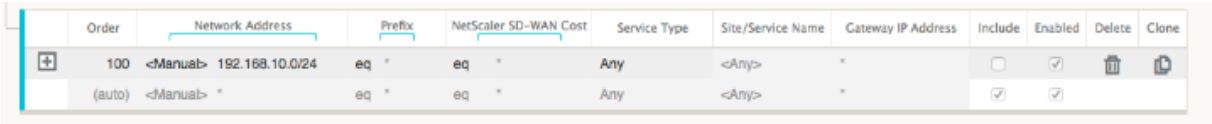


Der New York SD-WAN-Standort importiert alle Routen für das Management-Netzwerk. Dies kann ignoriert werden. Wir können uns auf Filter 200 konzentrieren.



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.



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 immer noch über die Unterlage MPLS Router A beworben. Lassen Sie uns die SD-WAN-Routentabelle des New Yorker Standorts 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 First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24	*	Local	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0.0/0	172.10.10.3	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
10	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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 konfiguriert werden, um den Router zu zwingen, die OSPF-Route der BGP-Route vorzuziehen. 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, der über 172.10.10.10 (New York SD-WAN) beworben wird. Es wird auch empfohlen, eine Override-Dienstregel zu erstellen, um alle 4.980-Pakete von UDP auf der SD-WAN-Appliance zu verwerfen, um zu verhindern, dass der virtuelle Pfad zu sich selbst zurückkehrt.

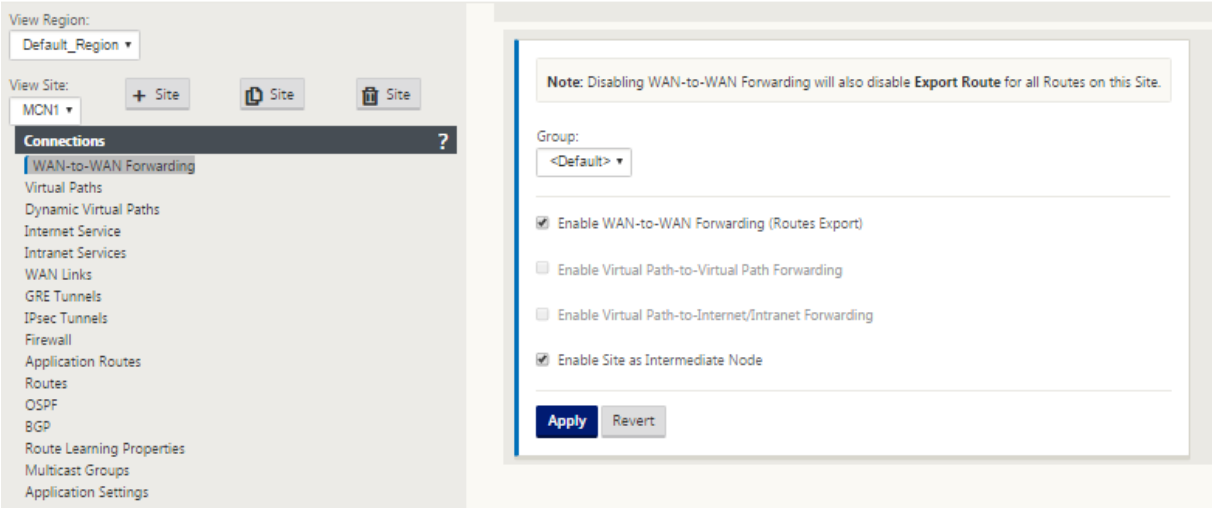
Dynamische virtuelle Pfade

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 werden entweder als Pakete pro Sekunde (pps) oder Bandbreite (kbps) definiert. Diese Funktion ermöglicht eine dynamische Full-Mesh-SD-WAN-Overlay-Topologie.

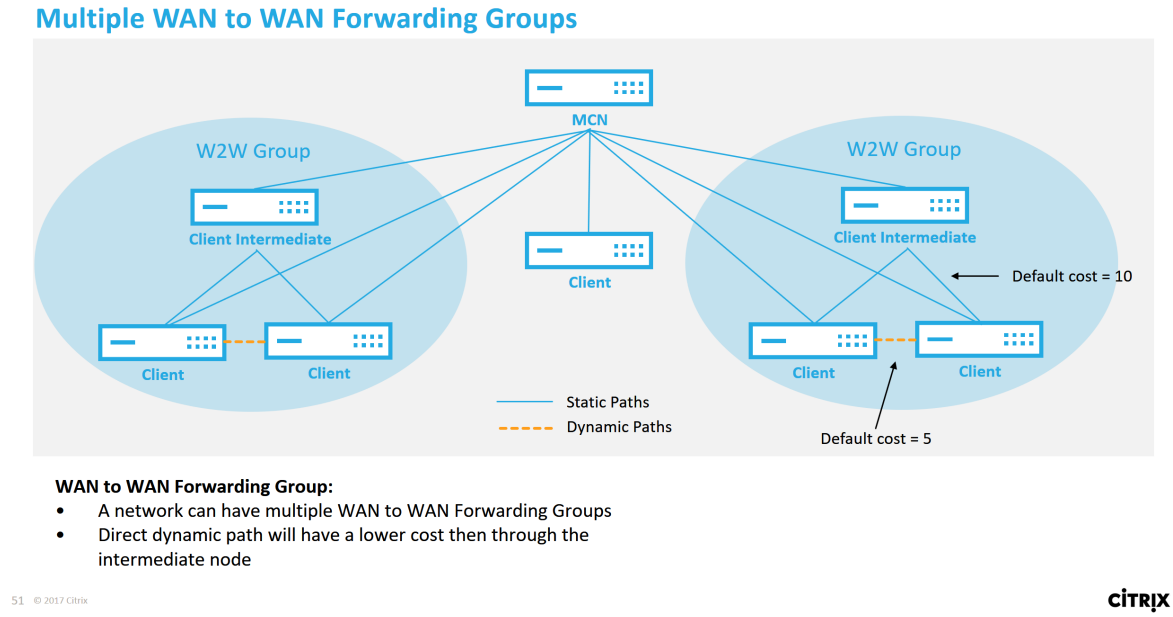
Sobald die Schwellenwerte für dynamische virtuelle Pfade erreicht sind, erstellen die Clientknoten dynamisch ihren virtualisierten Pfad zueinander unter Verwendung aller verfügbaren WAN-Pfade zwischen den Standorten und nutzen ihn auf folgende Weise voll aus:

- Senden Sie Massendaten, falls vorhanden, und überprüfen Sie dann keinen Verlust
- Senden Sie interaktive Daten und überprüfen Sie dann keinen Verlust
- Senden Sie Echtzeitdaten, nachdem die Bulk- und interaktiven Daten als stabil angesehen wurden (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

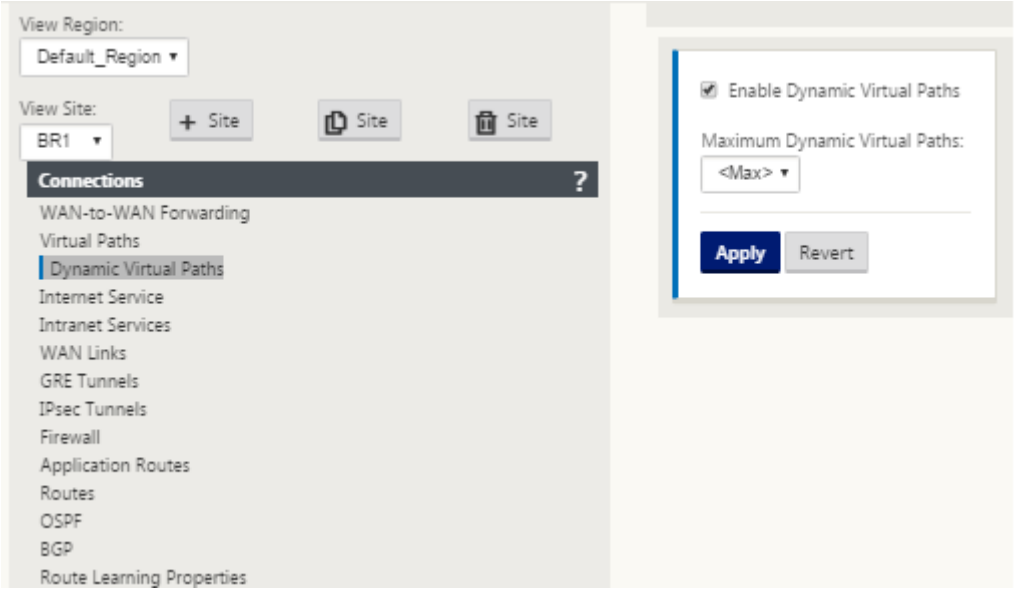
  Dynamische virtuelle Pfade haben das Konzept einer Zwischen-Site. Der Zwischenstandort kann ein MCN-Standort oder ein anderer Standort im Netzwerk sein, für den der statische virtuelle Pfad konfiguriert und mit zwei oder mehr anderen Clientknoten verbunden ist. Eine weitere Anforderung zur Entwurfsüberlegung 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.



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:

- Num —Reihenfolge der Route dieser Appliance basierend auf dem Übereinstimmungsprozess (niedrigste zuerst verarbeitete Num)
- Netzwerkadresse —Subnetz- oder Hostadresse
- Gateway bei Bedarf
- Service —welcher Dienst wird für diese Route angewendet
- Firewallzone —die Firewallzonenklassifizierung der Route
- Erreichbar —Identifiziert, ob der Status des virtuellen Pfads für diese Site aktiv ist
- Standort —Der Name des Standorts, an dem die Route voraussichtlich existieren wird
- Typ —Identifizierung des Routentyps (statisch oder dynamisch)
- Nachbar Direkt
- Kosten - Kosten der spezifischen Route
- Anzahl der Treffer —wie oft wurde die Route pro Paket verwendet. Dies würde verwendet, um zu überprüfen, ob eine Route korrekt getroffen wird.
- Berechtigt
- Art der Teilnahmeberechtigung
- Berechtigungswert

Der folgende Code ist ein Beispiel für eine SD-WAN-Standortroute:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

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

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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

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, die die Routentabelle anzeigt.
- Route 2—4 —Dies sind die Subnetze, die Teil der virtuellen Schnittstellen sind, die für das DC-Standort SD-WAN konfiguriert sind. Diese Subnetze werden von den definierten vertrauenswürdigen virtuellen Schnittstellen abgeleitet.
- Route 5 —Dies ist eine gemeinsame Route zu einem anderen Clientknoten, der vom MCN mit dem Erreichbarkeitsstatus Nein aufgrund des virtuellen Pfads nach unten zwischen diesem Standort und dem MCN gemeinsam genutzt wird.
- Route 6—9 —Diese Routen existieren an einem anderen Kundenstandort. Für diese Route wird eine virtuelle Pfadroute für den passenden WAN-Datenverkehr erstellt, der für die Remotesite 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.

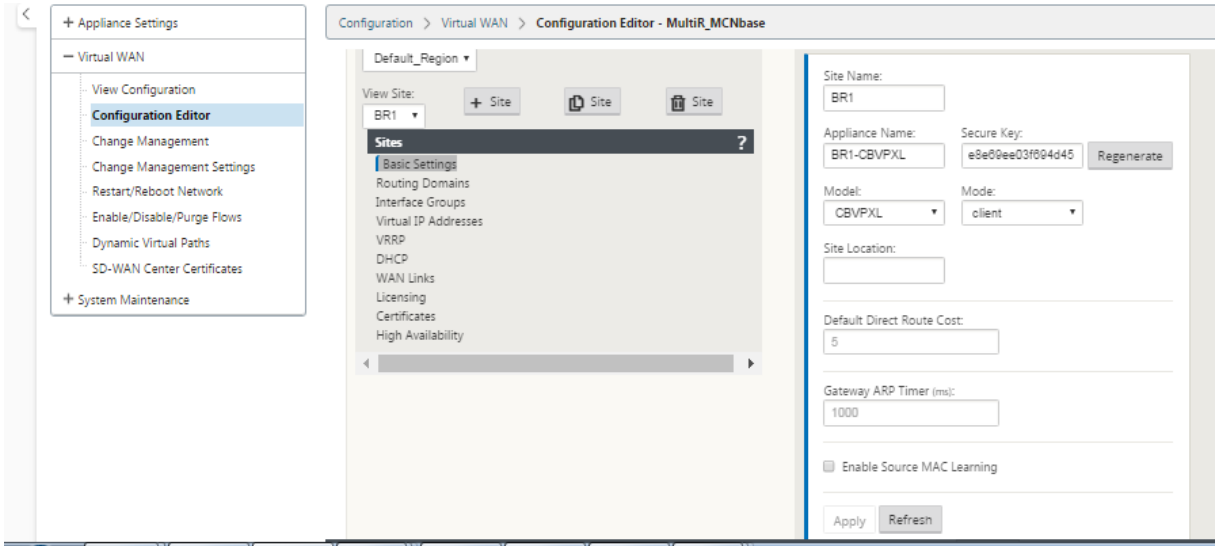
Die Standardwerte für die Routenkosten:

- WAN-zu-WAN-Weiterleitung —10
- Standardkosten für direkte Routen —5
- Automatisch generierte Routen —5
- Virtueller Pfad —5
- Lokal —5
- Intranet —5
- Internet —5
- Passthrough —5
- Optional —Route ist 0.0.0.0/0 definiert als Service-Level

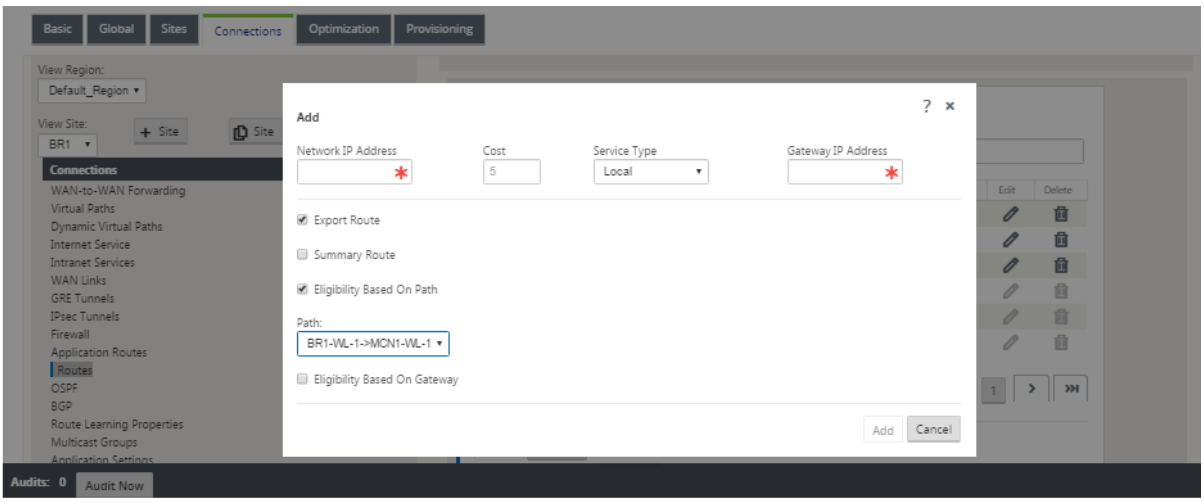
Nach der Definition dieser Routen ist es wichtig zu verstehen, wie der Verkehr über die definierten Routen fließt. Diese Verkehrsströme sind in folgende Flüsse unterteilt:

- LAN zu WAN (virtueller Pfad) —Verkehr in den SD-WAN-Overlay-Tunnel
- WAN zu LAN (Virtual Path) —Verkehr, der den SD-WAN-Overlay-Tunnel existiert
- Nicht-virtueller Pfadverkehr —Verkehr wird an das Unterlagennetzwerk weitergeleitet

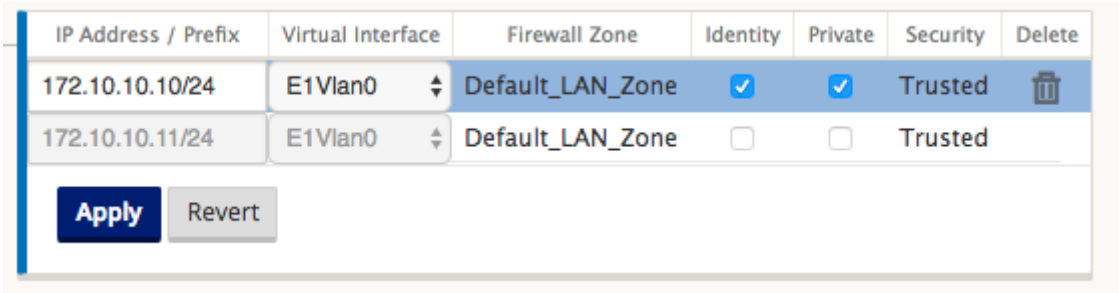
Die standardmäßigen Routenkosten können pro Standort geändert werden. Die Konfiguration finden Sie unter **View Site** > **Basic Settings** :



Statische Routen können pro Standort unter dem Knoten **Verbindungen** > **Standort** > **Route** s definiert werden:



Sie stellen fest, dass Routen an den virtuellen Pfad oder die Gateway-IP-Verfügbarkeit gebunden werden können. Internet-Routen können je nach gewünschtem Verhalten in das virtuelle Pfad-Overlay exportiert werden oder nicht. Sie können auch statische Virtual Path-Routen erstellen, um den Datenverkehr auf einen virtuellen Pfad zu erzwingen, obwohl wir das für SD-WAN angekündigte Präfix nicht erhalten (dh eine kostengünstigere Route der letzten Instanz). SD-WAN kann auch lokale Subnetze unterdrücken, indem die Virtual IP Address (VIP) privat gemacht wird.



> **Hinweis**
>
> Die Konfiguration erfordert mindestens einen nicht privaten VIP in jeder Routendomäne.

Intranet und Internetrouten

Für die Intranet- und Internetdiensttypen muss der Benutzer einen SD-WAN-WAN-Link definiert haben, um diese Arten von Diensten zu unterstützen. Es ist eine Voraussetzung für alle definierten Strecken für einen dieser Dienste. Wenn die WAN-Verbindung nicht zur Unterstützung des Intranetdienstes definiert ist, wird sie als lokale Route betrachtet. Die Intranet-, Internet- und Passthrough-Routen sind nur für die Site/Appliance relevant, für die sie konfiguriert sind.

Bei der Definition von Intranet-, Internet- oder Passthrough-Routen sind folgende Entwurfsüberlegungen:

- Muss Dienst auf der WAN-Verbindung definiert haben (Intranet/Internet —erforderlich)
- Intranet/Internet muss ein 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 Standort: 512
- Maximale Exportfilter für Route Learning pro Standort: 512
- Maximale BGP-Routing-Richtlinien: 255
- Maximale BGP-Community-String-Objekte: 255

Routingdomäne

October 28, 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 hat ihre 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 Routing-Domäneninformationen 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:
  - Interface-Gruppe
  - Virtuelle IP
  - GRE
  - WAN-Verbindung -> Zugriffsschnittstelle
  - IPsec-Tunnel
  - Routen
  - Regeln
- Routingdomänen werden in der Webinterface-Konfiguration 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

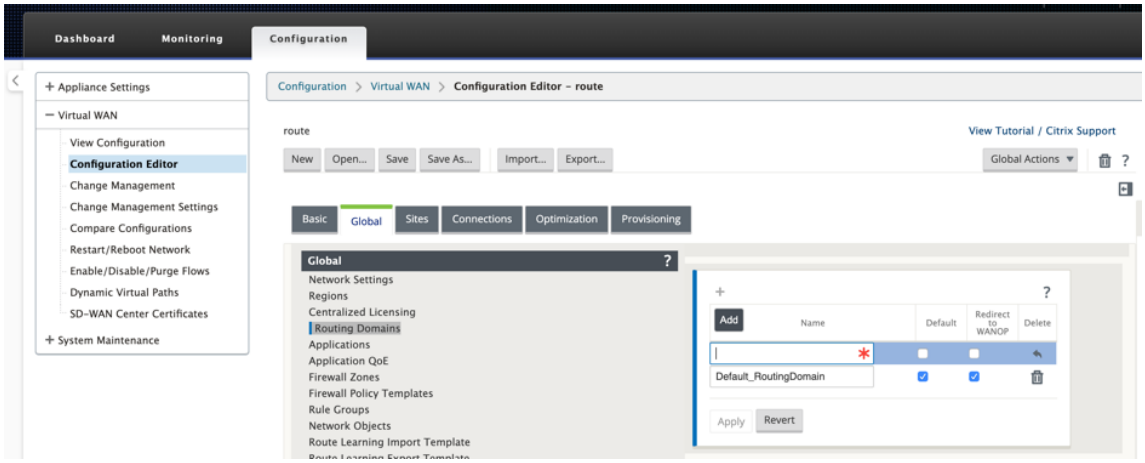
October 28, 2021

Citrix SD-WAN-Appliances ermöglichen die Konfiguration von Routingprotokollen und bieten einen einzigen Verwaltungspunkt für die Verwaltung eines Unternehmensnetzwerks, eines Zweigstellen-

netzwerks oder eines Rechenzentrumsnetzwerks. Sie können bis zu 254 Routingdomänen konfigurieren.

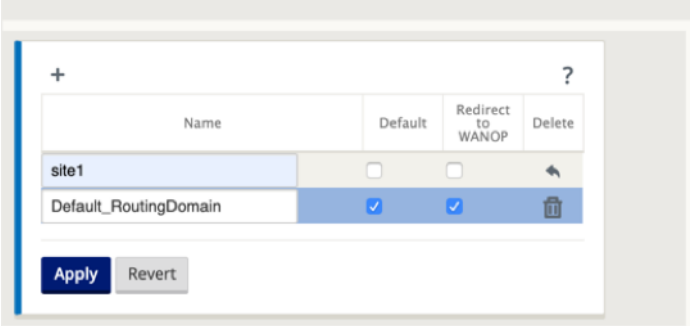
So konfigurieren Sie die Routingdomäne:

1. Navigieren Sie im SD-WAN-Webinterface zu **Konfiguration** > **Virtuelles WAN** > **Konfigurationseditor**. Navigieren Sie im **Konfigurationseditor**zu **Global**> **Routingdomänen**, klicken Sie auf **Hinzufügen (+)**, und geben Sie einen Namen für die neue Routingdomäne ein.



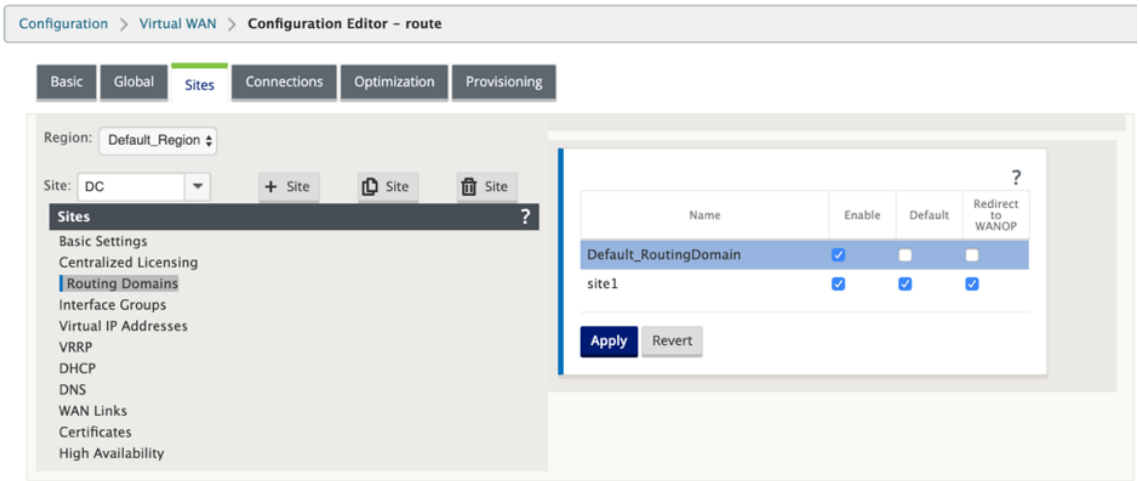
2. Wenn Sie diese Routingdomäne standardmäßig verwenden möchten, aktivieren Sie das Kontrollkästchen **Standard**. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern. Wenn Sie planen, eine einzelne Routingdomäne zu implementieren, ist keine explizite Konfiguration erforderlich.

   Alle neuen Konfigurationen werden automatisch mit einer Standard-Routingdomäne gefüllt.



3. Navigieren Sie zu **Sites** → **[Client-Sitenname]** > **Routingdomänen**. Klicken Sie auf das Kontrollkästchen **Aktivieren**, um eine konfigurierte Routingdomäne für die Site zu aktivieren.

4. Klicken Sie auf das Kontrollkästchen **Standard**, um diese Routingdomäne zur Standardeinstellung für die Site zu machen. 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.

Mit Version 11.0.2 ist **das Routing von Domains ohne routbare virtuelle IPs (VIPs)** mit den folgenden Funktionen zulässig:

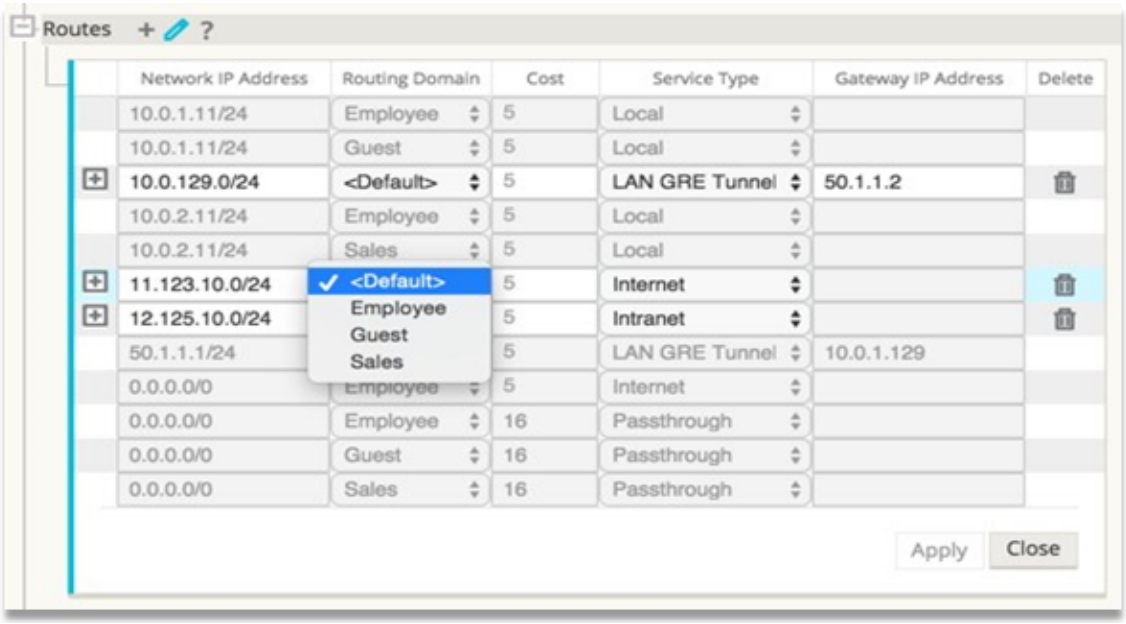
- Erlauben Sie einem Gerät, eine Routingdomäne für nicht vertrauenswürdige oder keine Schnittstellen zu haben.
- Zweige können untereinander über eine Routingdomäne kommunizieren, die keine physische Präsenz an einem Zwischenstandort hat.

Routen konfigurieren

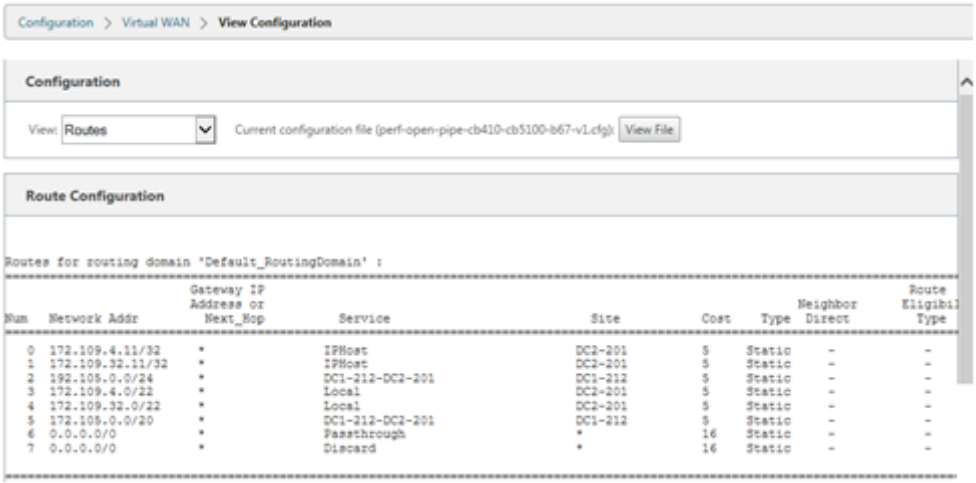
October 28, 2021

So konfigurieren Sie Routen:

1. Navigieren Sie im **Konfigurationseditor**zu **Verbindungen** > **[Site-Name]** > **Routen**.
2. Wählen Sie eine **Routing-Domäne** aus dem Dropdownmenü aus. 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

October 28, 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.

```
dynamic_routing?
```


Dynamisches Routing

October 28, 2021

Die folgenden beiden dynamischen Routingprotokolle werden von Citrix SD-WAN unterstützt:

- Öffnen Sie zuerst den kürzesten Pfad (OSPF)
- Border Gateway Protocol (BGP)

Vor der Veröffentlichung von Citrix SD-WAN 11.3.1 standen die dynamischen Routingfunktionen nur für eine einzelne Router-ID zur Verfügung. Sie können eine eindeutige Router-ID entweder global für das gesamte Protokoll (eine für OSPF und BGP) konfigurieren oder keine Router-ID angeben. Wenn keine Router-ID angegeben wird, wird die niedrigste IP der Virtual Network Instances (VNIs), die am dynamischen Routing teilnehmen, automatisch als Standard-Router-ID ausgewählt.

Ab Citrix SD-WAN 11.3.1 können Sie nicht nur eine Router-ID für das gesamte Protokoll konfigurieren, sondern auch eine Router-ID für jede Routingdomäne konfigurieren. Mit dieser Verbesserung können Sie stabiles dynamisches Routing über mehrere Instanzen hinweg ermöglichen, wobei verschiedene Router-IDs auf stabile Weise konvergieren.

Wenn Sie eine Router-ID für eine bestimmte Routingdomäne konfigurieren, überschreibt die spezifische Router-ID die Routingdomäne auf Protokollebene.

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 Routing-Protokolls Intermediate System to Intermediate System (IS-IS) von OSI.

Das OSPF-Protokoll ist offen, was bedeutet, dass seine Spezifikation gemeinfrei ist (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 erfordert. 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) -Editionen) konfigurieren, um Routen zu lernen und Routen mithilfe von OSPF anzukündigen.

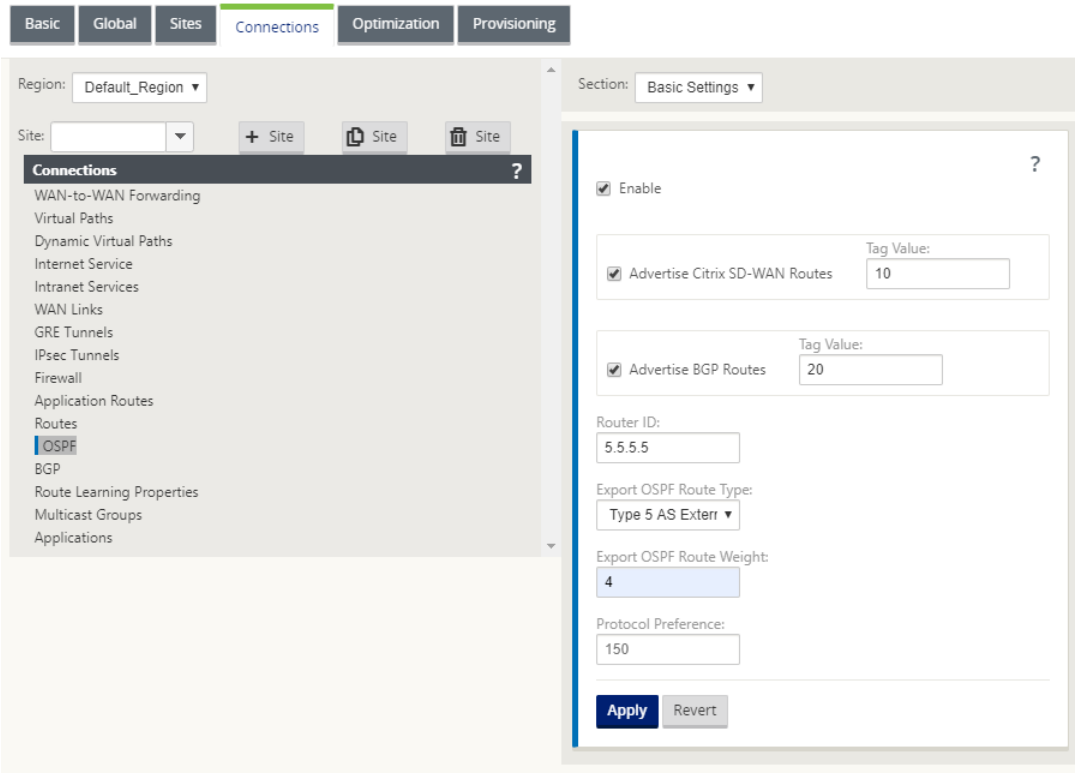
> **Hinweis**
>
> - Citrix SD-WAN-Appliances nehmen nicht als Designated Router (DR) und BDR (Backup Des-

> ignated Router) an jedem Multi-Access-Netzwerk teil, da die Standard-DR-Priorität auf "0" festgelegt ist.
>
> - Die Citrix SD-WAN Appliance unterstützt keine Zusammenfassung als Area Border Router (ABR).

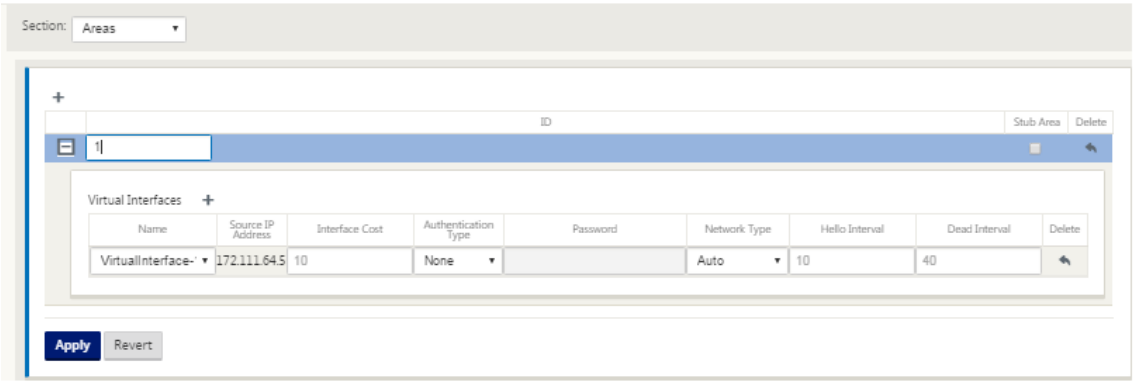
Konfigurieren Sie OSPF

So konfigurieren Sie OSPF:

1. Navigieren Sie im **Konfigurationseditor**zu **Verbindungen > Region > Standort > OSPF > Grundeinstellungen**.
2. Klicken Sie auf **Aktivieren**, wählen oder geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Übernehmen**.
   - **Ankündigen von 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.
   - **Werben Sie für BGP-Routen**: Erlauben Sie, dass von BGP-Peers gelernte Routen 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-Werbung verwendet. Wenn die Router-ID nicht angegeben wird, wird sie automatisch als die niedrigste virtuelle IP ausgewählt, die im SD-WAN-Netzwerk gehostet wird.
   - **OSPF-Routentyp exportieren: Geben**Sie die Citrix SD-WAN-Routen für OSPF-Peers als flächeninterne Routen 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.
   - **Protokollpräferenz**: Wenn Präfixe über mehrere Routingprotokolle erlernt werden, bestimmt der Voreinstellungswert des Protokolls die Auswahl des Routing-Protokolls. Weitere Informationen finden Sie unter Protokolleinstellungen.



3. Erweitern Sie **OSPF** -> **Area**und klicken Sie auf **Bearbeiten**.



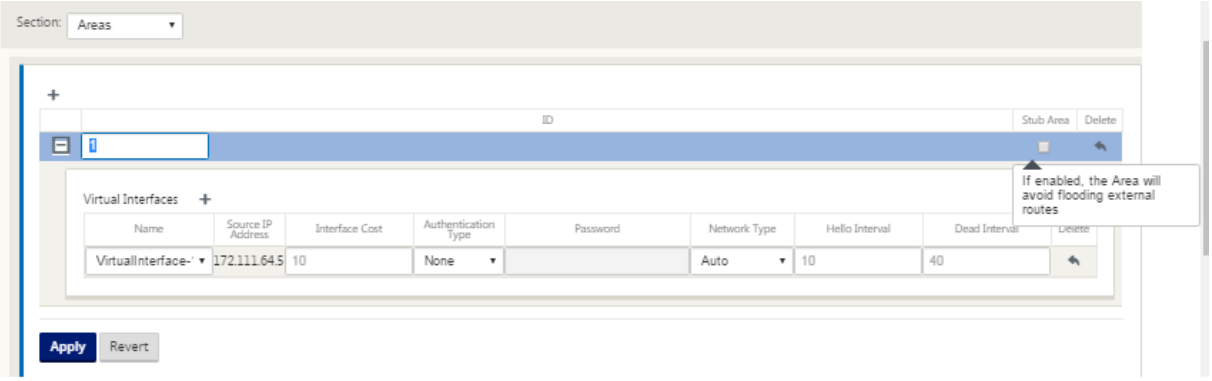
4. Geben Sie eine **Bereichs-ID** ein, um Routen zu lernen und anzukündigen.
5. Wenn Identity nicht für eine bestimmte virtuelle IP-Adresse geprüft wird, ist die zugeordnete virtuelle Schnittstelle für IP-Dienste nicht verfügbar.
6. Wählen Sie eine der verfügbaren virtuellen Schnittstellen aus dem Menü **Name**. Das virtuelle Interface bestimmt die **Quell-IP-Adresse**.
7. Geben Sie die **Schnittstellenkosten** ein (10 ist der Standardwert).
8. Wählen Sie einen **Authentifizierungstyp** aus dem Menü.
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 Interval** das Warteintervall ein, bevor Sie einen Router als tot markieren. Das standardmäßige Totintervall beträgt 40 Sekunden.
12. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Stub-Bereich

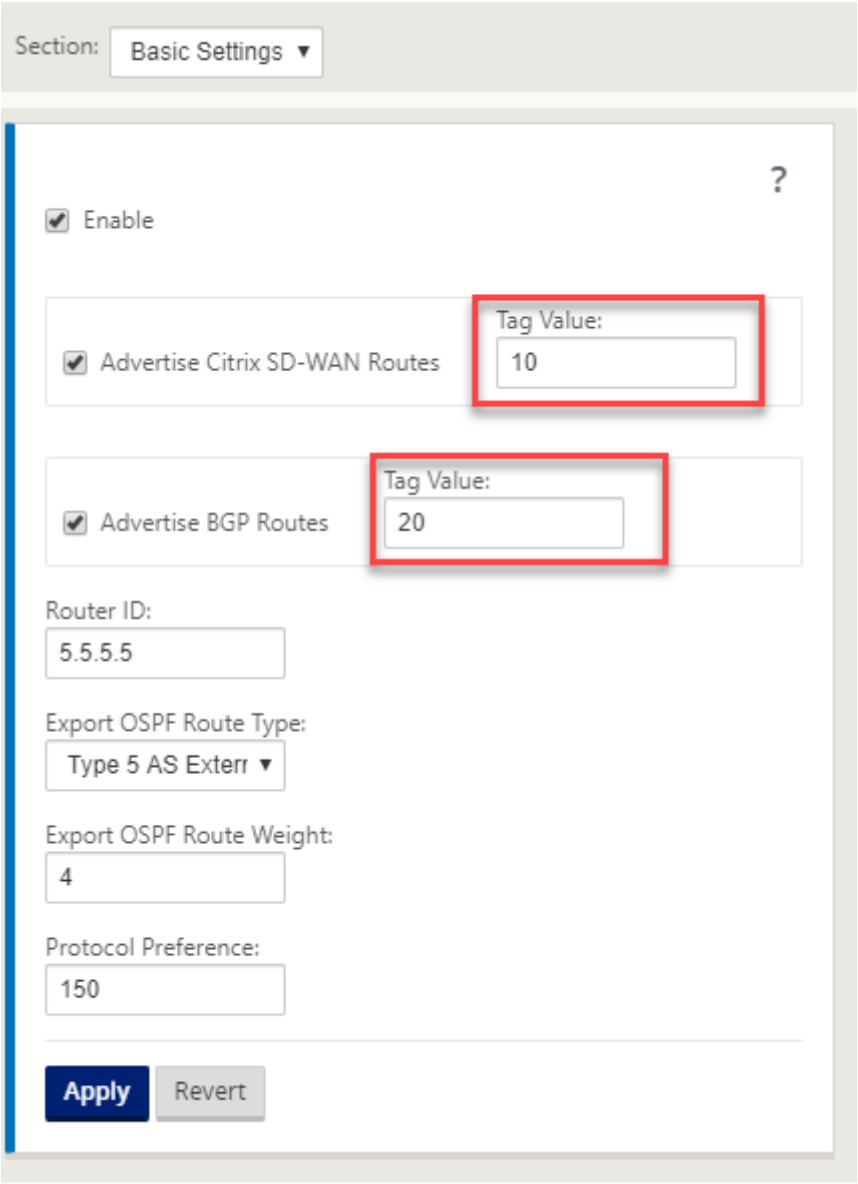
Stub-Bereiche sind von externen Routen abgeschirmt und erhalten Informationen über Netzwerke, die zu anderen Bereichen derselben OSPF-Domäne gehören.

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-gelernte Routen zu demselben Subnetz vorhanden sind, identifiziert der OSPF-Schleifenverhinderungsmechanismus es 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**.



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 setzen Interior-Gateway-Protokolle wie RIP oder OSPF für den Austausch von Routing-Informationen innerhalb ihrer Netzwerke ein. 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

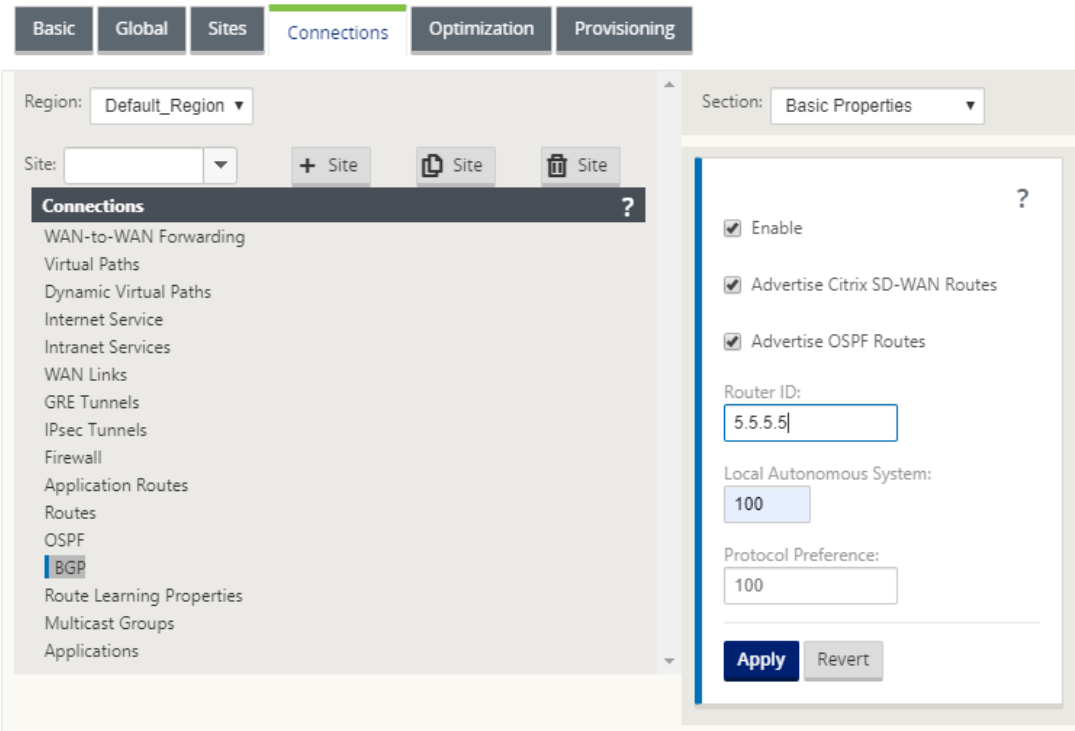
innerhalb eines AS auszutauschen, heißt das Protokoll Interior BGP (IBGP).

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 Routing-Richtlinien zu definieren und eine stabile Routing-Umgebung aufrechtzuerhalten. BGP-Nachbarn tauschen vollständige Routinginformationen aus, wenn die TCP-Verbindung zwischen Nachbarn zum ersten Mal hergestellt wird. Wenn Änderungen an der Routingtabelle festgestellt werden, senden die BGP-Router nur die Routen an ihre Nachbarn, die sich geändert haben. BGP-Router senden keine regelmäßigen Routing-Updates und geben nur den optimalen Pfad zu einem Zielnetzwerk bekannt. Sie können Citrix SD-WAN Appliances konfigurieren, um Routen zu lernen und Routen mit BGP zu bewerben.

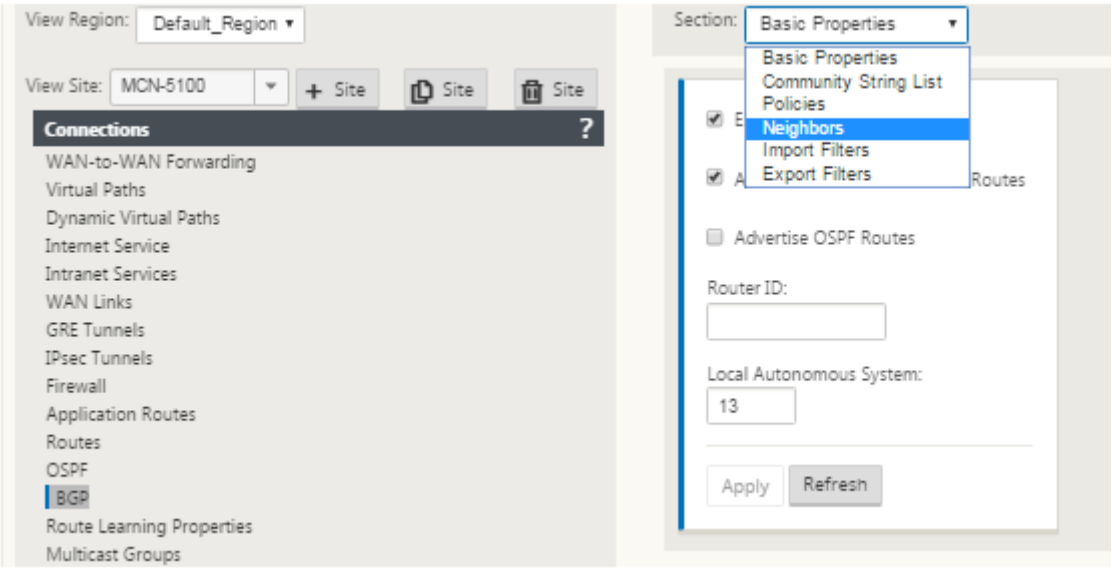
BGP konfigurieren

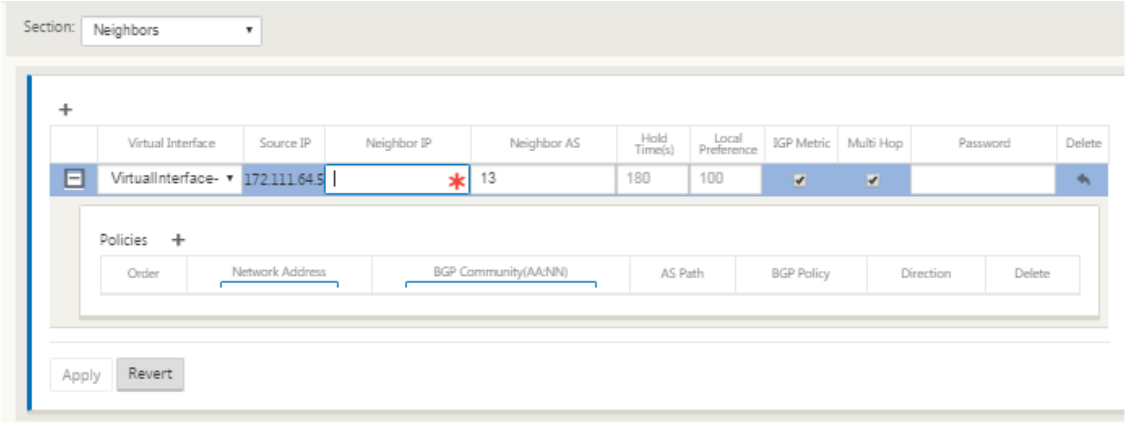
So konfigurieren Sie BGP:

1. Navigieren Sie im **Konfigurationseditor**zu **Verbindungen > Region > Standort > BGP > Grundeinstellungen.**
2. Klicken Sie auf **Aktivieren**, wählen oder geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Übernehmen**.
   - **Citrix SD-WAN-Routen ankündigen**: Erlauben Sie, dass Citrix SD-WAN-Routen über BGP angekündigt werden.
   - **Werben Sie für OSPF-Routen**: Erlauben Sie, dass Routen, die von OSPF-Peers gelernt wurden, über BGP beworben werden.
   - **Router-ID**: Die eindeutige Router-ID, der Router, wird für OSPF-Werbung verwendet. Wenn die Router-ID nicht angegeben wird, wird sie automatisch als die niedrigste virtuelle IP ausgewählt, die im SD-WAN-Netzwerk gehostet wird.
   - **Lokales autonomes System**: Die lokale Nummer des autonomen Systems, von der aus die Routen erlernt und beworben werden. Die Nummer des autonomen Systems muss mit einer auf den benachbarten Routern übereinstimmen.
   - **Protokollpräferenz**: Wenn Präfixe über mehrere Routingprotokolle erlernt werden, bestimmt der Voreinstellungswert des Protokolls die Auswahl des Routing-Protokolls. Weitere Informationen finden Sie unter Protokolleinstellungen.



3. Erweitern Sie **Grundeinstellungen > Nachbarn** und klicken Sie auf das Symbol **Hinzufügen (+)**.





Wählen Sie für Sites mit mehreren Routingdomänen eine Routingdomäne aus. Routingdomäne bestimmt, welche virtuellen Schnittstellen verfügbar sind.

4. Wählen Sie ein **virtuelles Interface** aus dem Menü. Das virtuelle Interface bestimmt die Quell-IP-Adresse.
5. Geben Sie die **IP-Adresse** des IBGP-Nachbar-Routers in das Feld Nachbar-IP und die Nummer des **lokalen autonomen Systems** in das Feld Neighbor AS ein.
6. Geben Sie im Feld **Haltezeit (en)** die Haltezeit in Sekunden ein, um zu warten, bevor Sie einen Nachbarn deklarieren (der Standardwert ist 180).
7. 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).
8. Aktivieren Sie das Kontrollkästchen **IGP Metric**, um den Vergleich interner Entfernungen zur Berechnung der besten Route zu ermöglichen.
9. Klicken Sie auf das Kontrollkästchen **Multi-Hop**, um mehrere Hops für die Route zu aktivieren.
10. Geben Sie im Feld **Kennwort** ein Kennwort für die MD5-Authentifizierung von BGP-Sitzungen ein (Authentifizierung ist nicht erforderlich).

> **Hinweis**
>
> Die Konfiguration von Routenreflektoren und Konföderationen für iBGP wird im SD-WAN-Netzwerk nicht unterstützt.

Exterieur BGP (eBGP)

Citrix SD-WAN-Appliances stellen eine Verbindung zu einem Switch auf der LAN-Seite und einem Router auf der WAN-Seite her. Da die SD-WAN-Technologie zunehmend integraler für die Bereitstellung von Unternehmensnetzwerken 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 auf, die eBGP gegenüber WAN-Seite verwenden, und ist in der Lage, Routen von und zu Peers zu lernen, zu bewerben. 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:

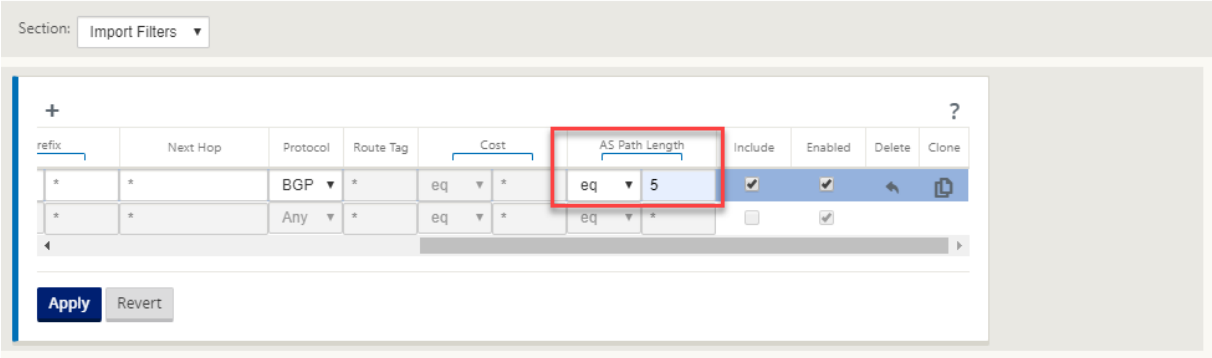
- SD-WAN-Site Kommunikation mit Nicht-SD-WAN-Site über eBGP
- Kommunikation zwischen SD-WAN-Sites mit Virtual Path und eBGP
- Implementierung von OSPF in einarmiger Topologie
- OSPF-Typ5-zu-Typ1-Bereitstellung im MPLS-Netzwerk
- OSPF-Bereitstellung von SD-WAN- und Nicht-SD-WAN (Drittanbieter) -Appliance
- Implementierung von OSPF mit SD-WAN-Netzwerk mit Hochverfügbarkeits-Setup

AS-Pfadlänge

Das BGP-Protokoll verwendet das **AS-Pfadlängenattribut**, um die beste Route zu ermitteln. Die AS-Pfadlänge gibt die Anzahl der autonomen Systeme an, die in einer Route durchquert werden. Citrix SD-WAN verwendet das **Pfadlängenattribut BGP AS**, um Routen zu filtern und zu importieren.

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 Secondary DC steuern, indem Sie einfach die AS-Pfadlänge der primären DC-Appliance auf dem Router erhöhen, was sie nicht bevorzugt macht. Es entfällt die Notwendigkeit, die Routenkosten zu ändern und ein Konfigurationsupdate durchzuführen.

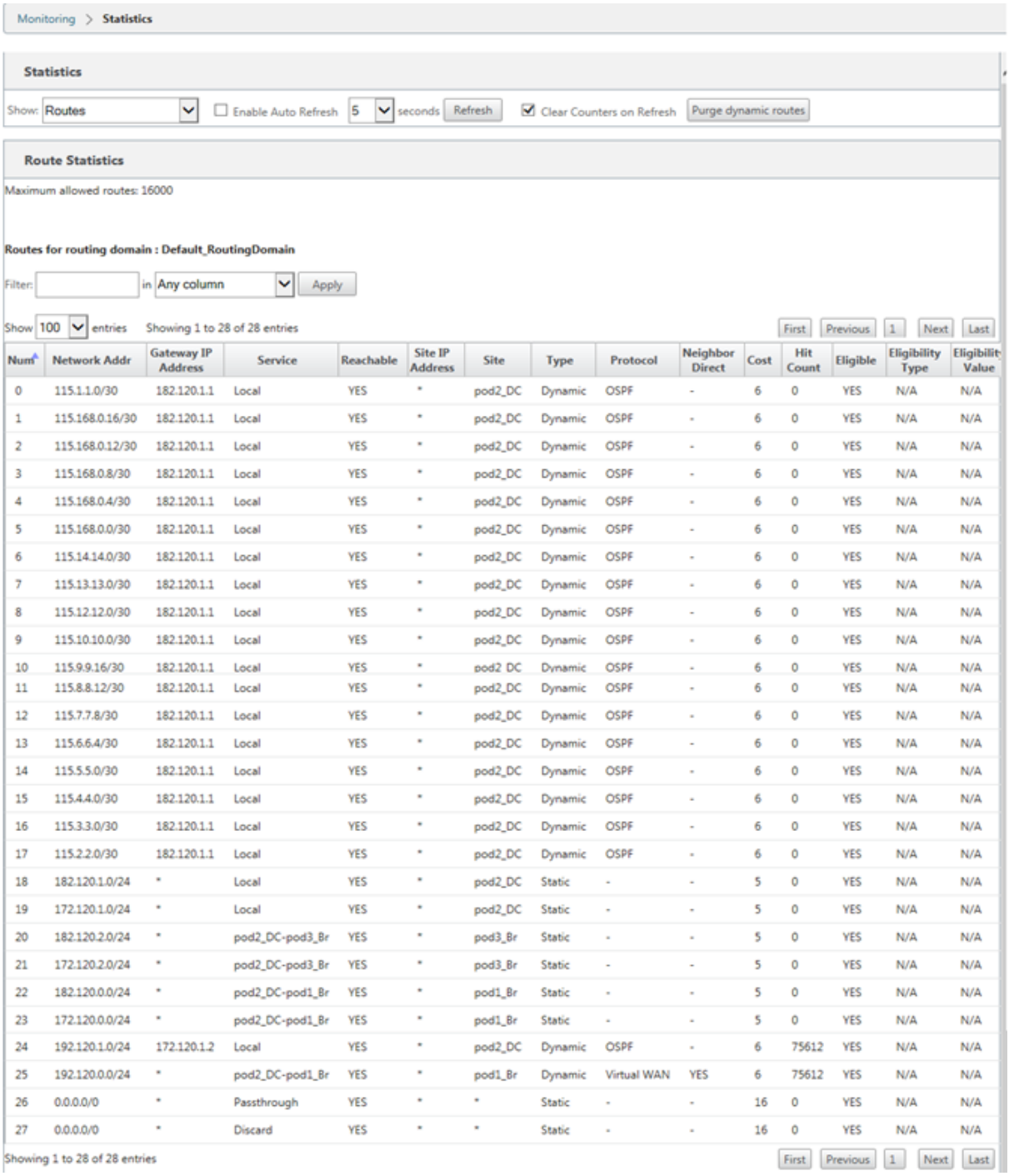
Um die AS-Pfadlänge in Importfiltern zu konfigurieren, wählen Sie BGP als Protokoll aus, wählen Sie ein Prädikat aus und geben Sie die **AS-Pfadlänge**ein. Weitere Informationen finden Sie unter Routenfilterung



Routenstatistiken überwachen

Navigieren Sie zu **Überwachen**> **Statistiken**. Wählen Sie im Dropdownmenü **Anzeigen** die Option **Routen** aus.

Alle Funktionen für entsprechende Routen werden im Citrix SD-WAN Netzwerk unterstützt, unabhängig davon, ob eine Route Dynamic oder Static ist.



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

OSPF

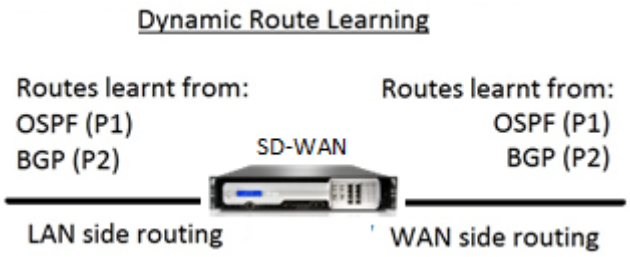
October 28, 2021

LAN-Seite: Dynamisches Routenlernen

OSPF läuft auf dem LAN-Port der Citrix SD-WAN-Appliance, 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 mit einem AREA, der als STUB-Bereich definiert ist, indem das Lernen von Typ 5 AS-externes LSA eingeschränkt wird.

Citrix SD-WAN-Appliances können die lokal erlernten dynamischen Routen mit dem MCN bewerben. 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 von SD-WAN als externe Routen nur mit Typ 5 LSA behandelt. Diese Routen wurden seinen Nachbarroutern in Typ 5 External LSA beworben. Dies führte dazu, dass SD-WAN-Routen gemäß dem OSPF-Pfadauswahlalgorithmus weniger bevorzugte Routen sind.

Mit der neuesten Version kann SD-WAN jetzt Routen als flächeninterne Routen (LSA Typ 1) ankündigen, um mithilfe 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

In der einarmigen 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:

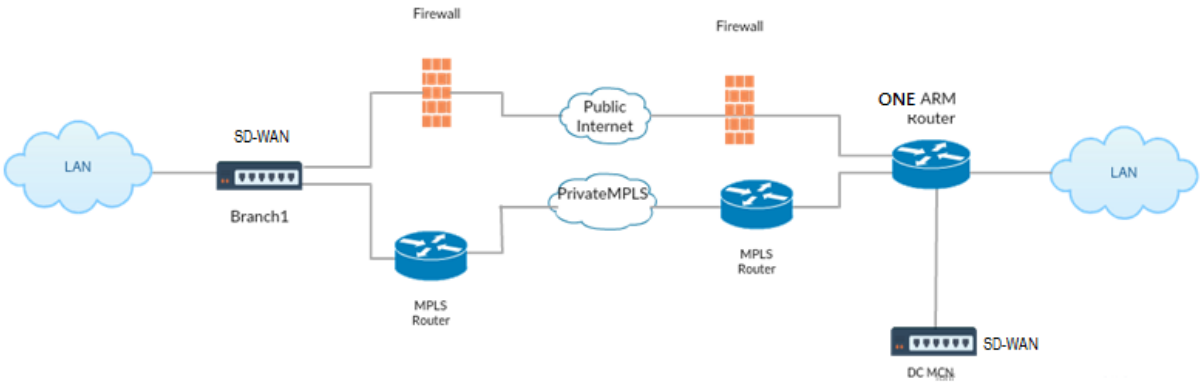
1. Konfigurieren Sie **virtuelle Schnittstellen** und **WAN-Verbindungen** sowohl auf den DC- als auch auf Branch-Sites, damit Sie den virtuellen Pfad zwischen ihnen erstellen können.
2. Wählen Sie unter **Verbindungen** > [**MCN**] > **Route Learning** > **OSPF**->**Grundeinstellungen**die Option **OSPF-Routentyp exportieren** als **Typ 1 Intrabereich**aus.
3. Speichern Sie die Konfiguration, stellen Sie die Konfiguration ein und aktivieren Sie die Konfiguration.

Sie müssen die folgenden Routentypen unter
Export-OSPF-Routentypsehen 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.

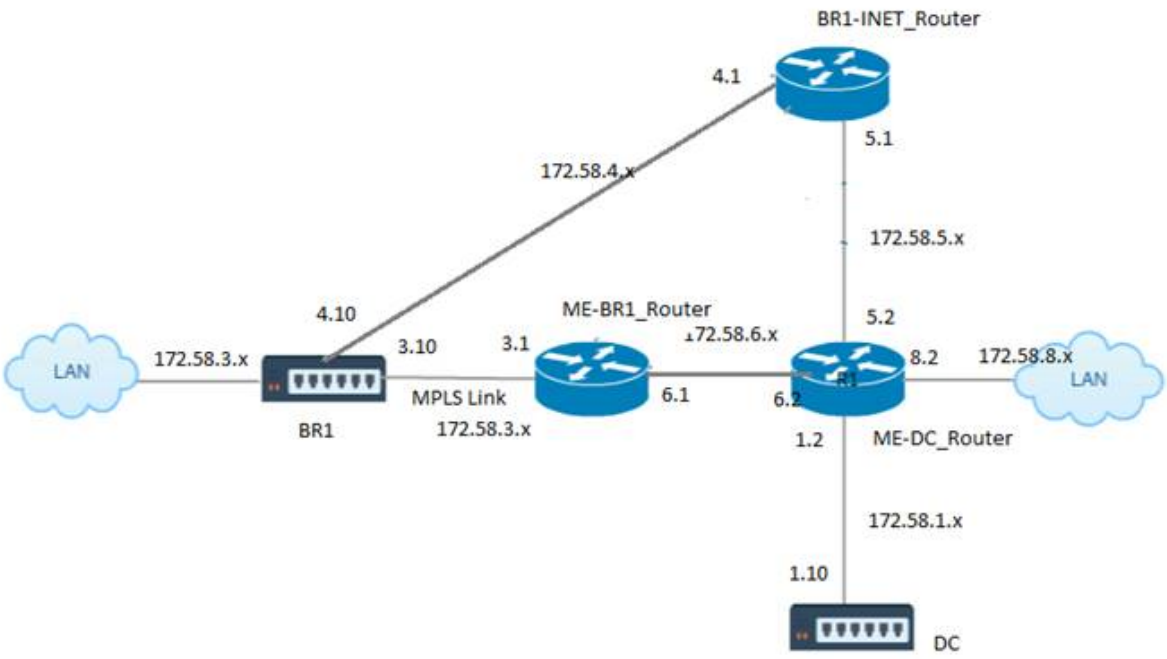


Wie in der Abbildung oben gezeigt, wird DC MCN in der Einarm-Topologie eingesetzt. Wenn der DC-Standort hochgefahren ist, leitet der einarmige Router den gesamten Datenverkehr vom lokalen LAN an andere Standorte weiter, z. B. das lokale LAN der Zweigstelle, dessen Ziel-IP-Adresse sich innerhalb desselben 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 bereitgestellt, um die Bildung von Schleifen in einem MPLS-Netzwerk zu vermeiden, 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 area0
- ME-BR1_Router und ME-DC_Router auf Bereich0
- BR1 VW und ME-BR1_Router auf Bereich0

Auf dem ME-DC_Router:

1. Statische Route für 172.58.3.10/32 (virtuelle IP von BR1 für MPLS Link) bis 172.58.6.1 hinzufügen
2. Hinzufügen einer statischen 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 unterbrechungsfreien 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 Entkapselung des LAN-Subnetzes bewusst ist. Wenn DC SD-WAN ausfällt, würde die alte Routing-

Infrastruktur ME-BR1_Router 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 Virtual Interfaces und WAN-Links auf DC- und Branch-Standorten, 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.

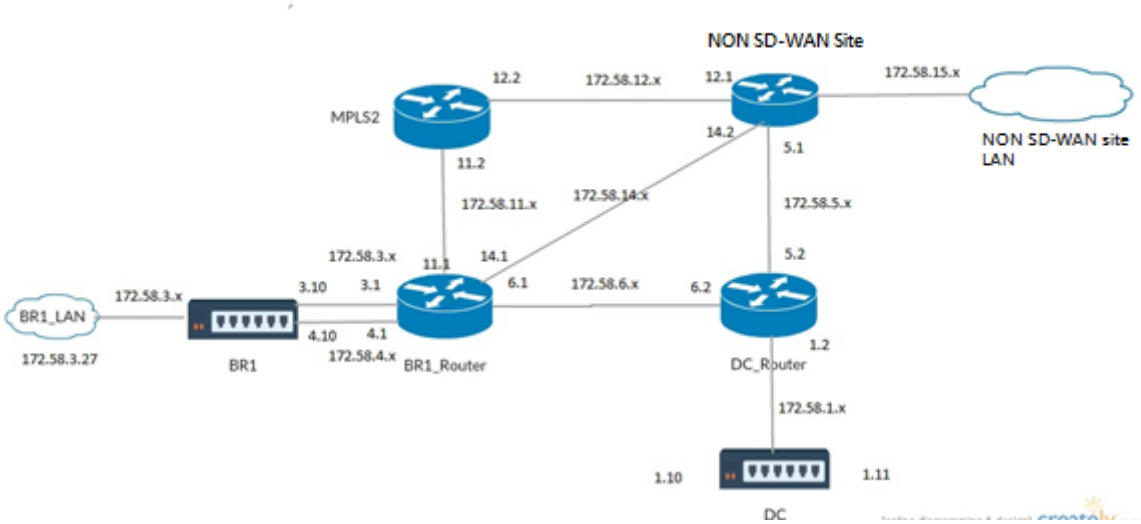
So konfigurieren Sie die exportierte OSPF-Routengewichtung unter den Einstellungen des Exportfilters:

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:

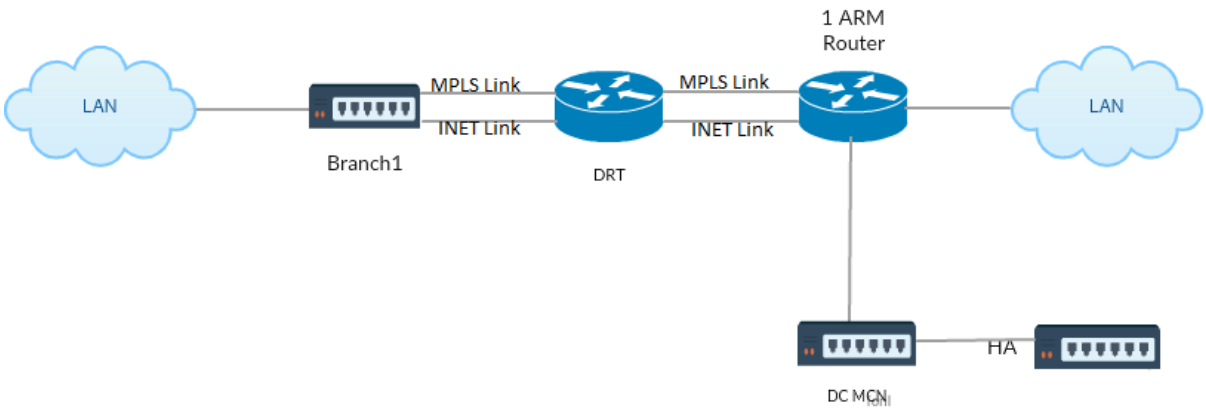
1. Konfigurieren Sie **virtuelle Schnittstellen** und **WAN-Verbindungen** sowohl auf DC als auch auf Branch, sodass ein virtueller Pfad zwischen den Standorten erstellt wird.
2. Konfigurieren Sie den **Routentyp exportieren** als **Typ1**, und weisen Sie die Kosten auf der SD-WAN-Appliance als **195** 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. Schließen Sie die Verbindung zwischen R1 und R2.
8. Senden Sie Datenverkehr zwischen den Endhosts auf DC- und Zweigstandorten.
9. Deaktivieren Sie den virtuellen WAN-Dienst auf der DC-Site, damit virtuelle Pfade ausfallen.
10. Senden Sie den Verkehr 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



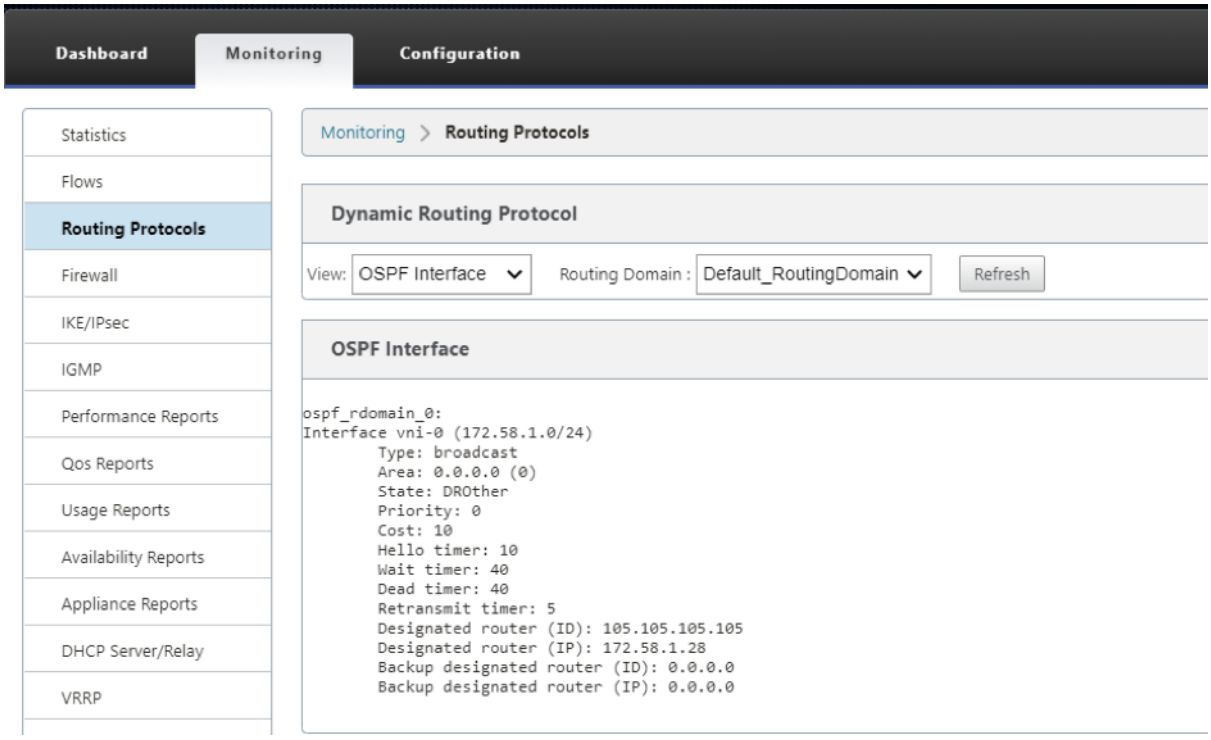
OSPF Typ5 zu Typ1 mit Hochverfügbarkeitsstandorten während des Failovers auf Standby-Appliance und Bereitstellung in Hochverfügbarkeits-Setup:

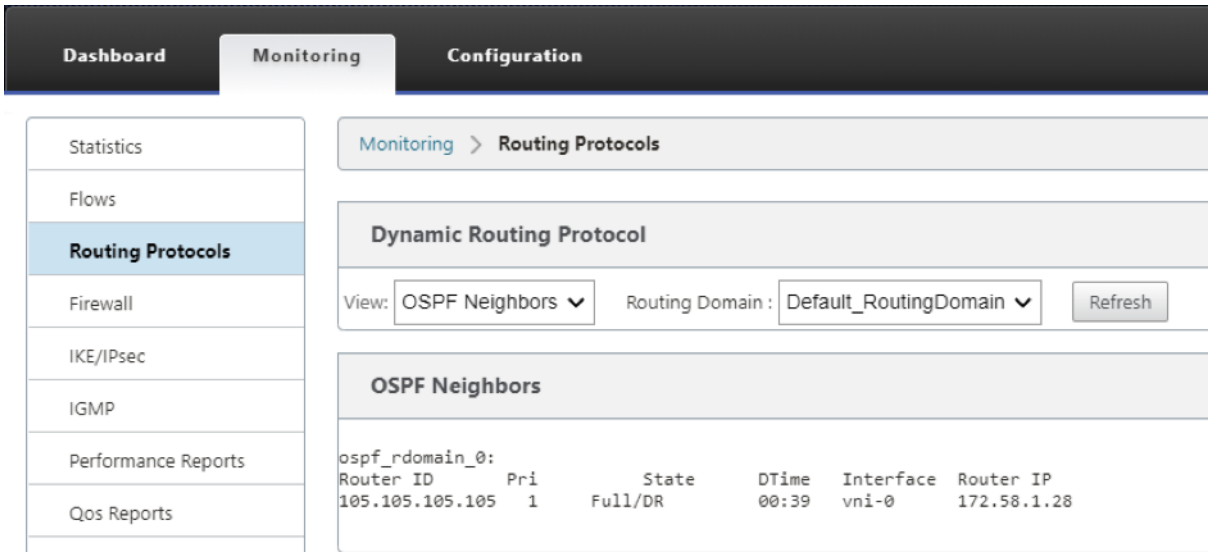
So konfigurieren Sie OSPF in der HA-Bereitstellung:

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 Trefferzahl für OSPF-Routen mit geringsten Kosten steigt.
7. Bringen Sie den Active MCN runter und beobachten Sie das Verhalten.
8. Bringen Sie das ursprüngliche Active MCN wieder hoch.
9. Das **Dashboard** > **Hochverfügbarkeitsstatus** wird für HA Local 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. Selbst nach dem Failover zeigt der Hochverfügbarkeitsstatus die korrekte OSPF-Konfiguration für 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.

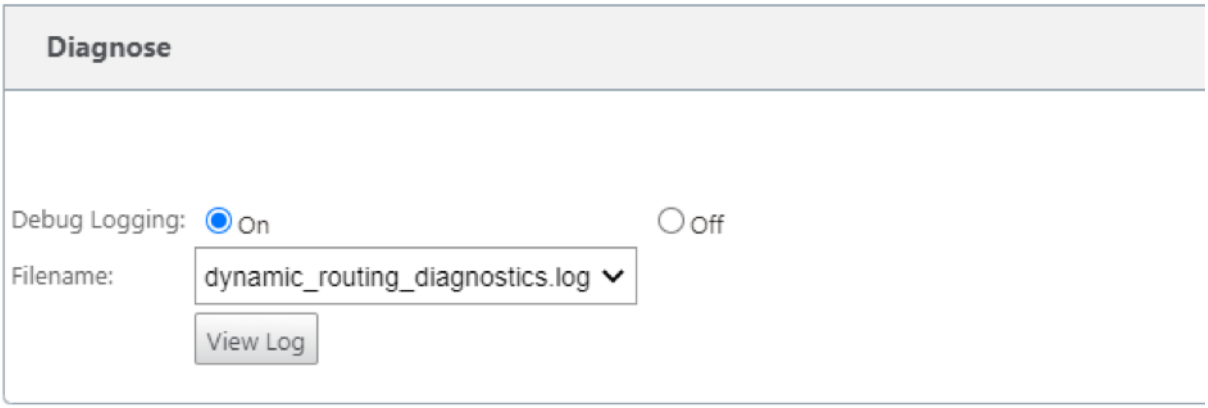
Problembehandlung

Sie können die OSPF-Parameter unter **Monitoring > Routing Protocols**anzeigen.





Sie können auch die dynamischen Routingprotokolle beobachten, um festzustellen, ob ein Problem mit der OSPF-Konvergenz vorliegt.



BGP

October 28, 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-Zeichenfolgen 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.

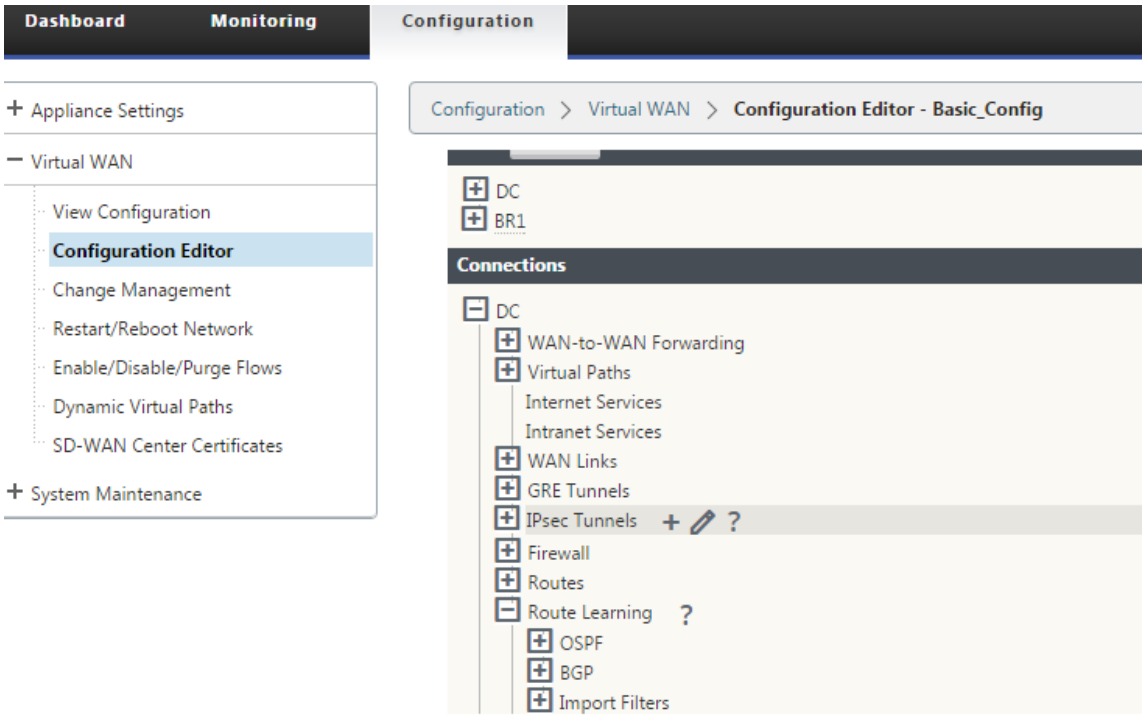
Sie können jede Community-Zeichenfolge manuell konfigurieren oder keine Werbung oder keine Exportgemeinschaftszeichenfolge aus einem Dropdownmenü auswählen. Zur manuellen Konfigura-

tion 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.

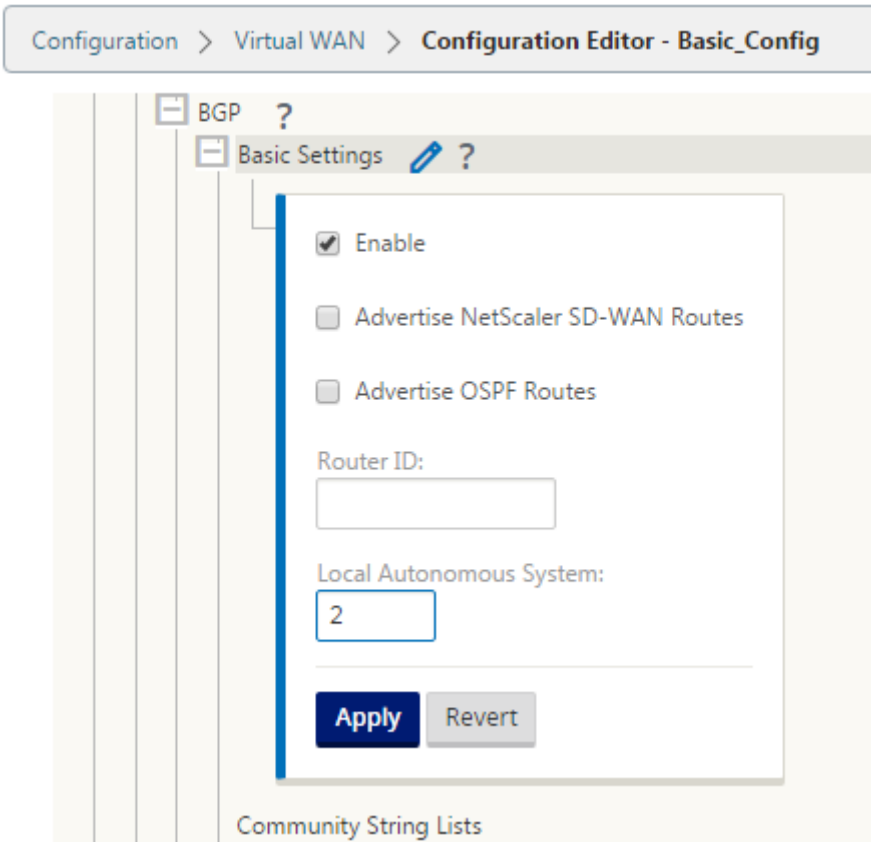
Sie können konfigurieren, wie oft Sie das lokale AS dem AS-Pfad voranstellen möchten, bevor Sie außerhalb des lokalen Netzwerks werben. Sie können MED für übereinstimmende Routen konfigurieren.

So konfigurieren Sie die BGP-Richtlinie:

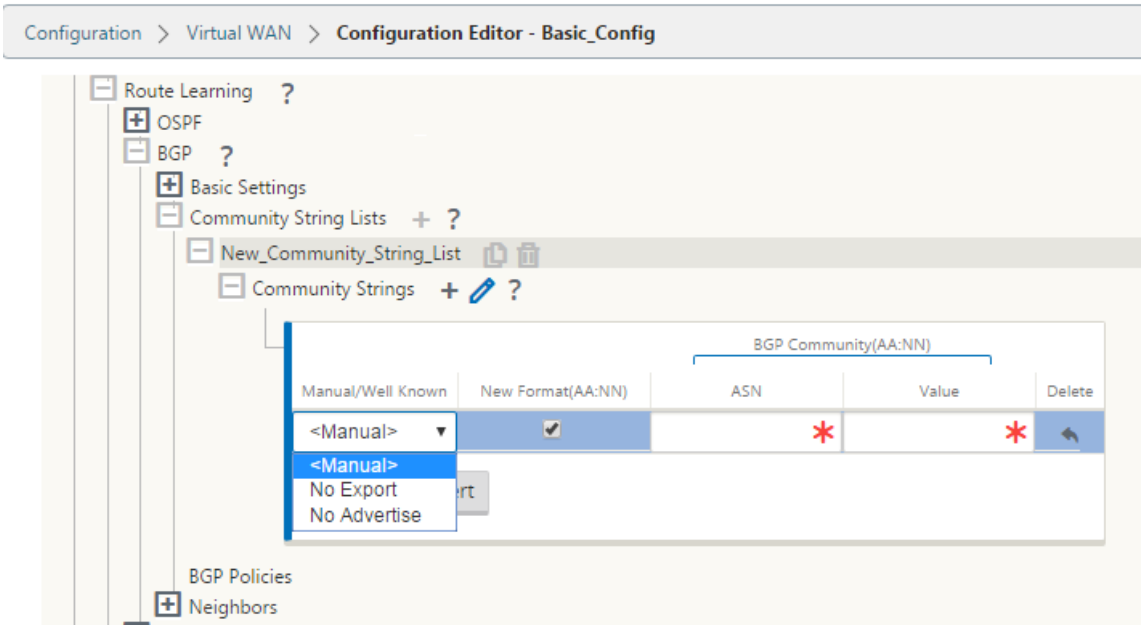
1. Wechseln Sie in der NetScaler SD-WAN-Webverwaltungsoberfläche zu **Konfiguration** > **Virtuelles WAN** > **Konfigurationseditor**. Öffnen Sie ein vorhandenes Konfigurationspaket. Wechseln Sie zu **Sites** > **DC-** oder **Zweigeinstellungen** .



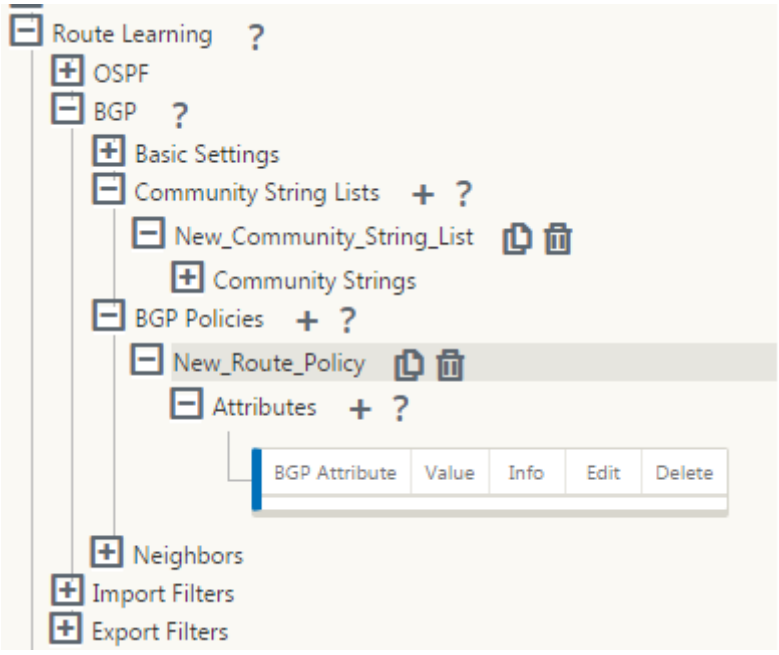
2. Erweitern Sie **BGP** und klicken Sie unter **Grundeinstellungen** auf **Aktivieren** . Geben Sie **Router-ID** und Wert **des lokalen autonomen Systems ein**, und klicken Sie auf **Übernehmen** .



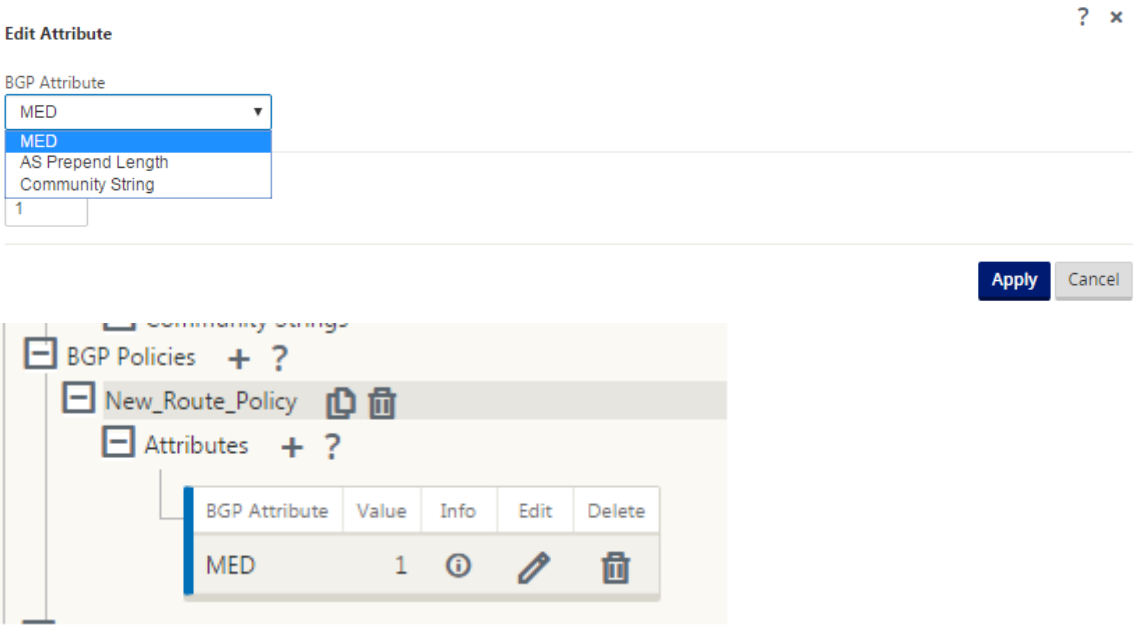
3. Klicken Sie neben den **Community-Zeichenfolgenlisten** auf **+** Zeichen. Konfigurieren Sie jede Community-Zeichenfolge manuell oder indem Sie im Dropdownmenü keine Werbung oder keine Export-Community-Zeichenfolge auswählen. Zur manuellen Konfiguration können Sie eine AS-Nummer und eine Community 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 das gewünschte BGP-Attribut aus dem Dropdownmenü aus. Geben Sie den gewünschten Wert für **MED**, **AS Prepend Length**oder **Community String** gemäß Ihrer Auswahl ein. Klicken Sie auf **Apply**.



> **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.

Konfigurieren von erweiterten Nachbarn

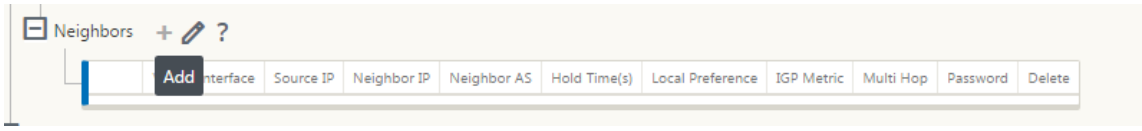
Mit dieser Option können Sie Netzwerkobjekte hinzufügen und eine konfigurierte BGP-Richtlinie für dieses Netzwerkobjekt hinzufügen. Dies ähnelt dem Erstellen einer Routenkarte und einer ACL, um bestimmte Routen abzugleichen, und dem Konfigurieren von BGP-Attributen für diesen Nachbarn. Sie können die 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.

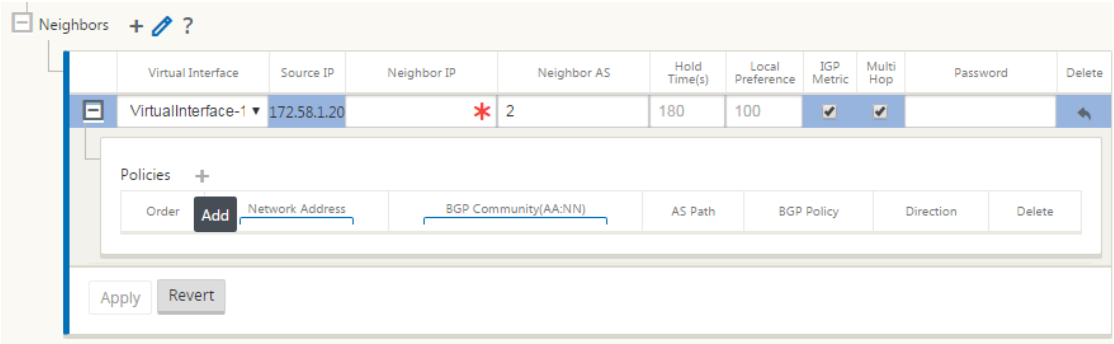
Sie haben die Möglichkeit, Routen basierend auf Netzwerkadresse (Zieladresse), AS-Pfad, Community-Zeichenfolge abzugleichen und eine Richtlinie zuzuweisen und die Richtung für die anzuwendende Richtlinie auszuwählen.

So konfigurieren Sie Nachbarn:

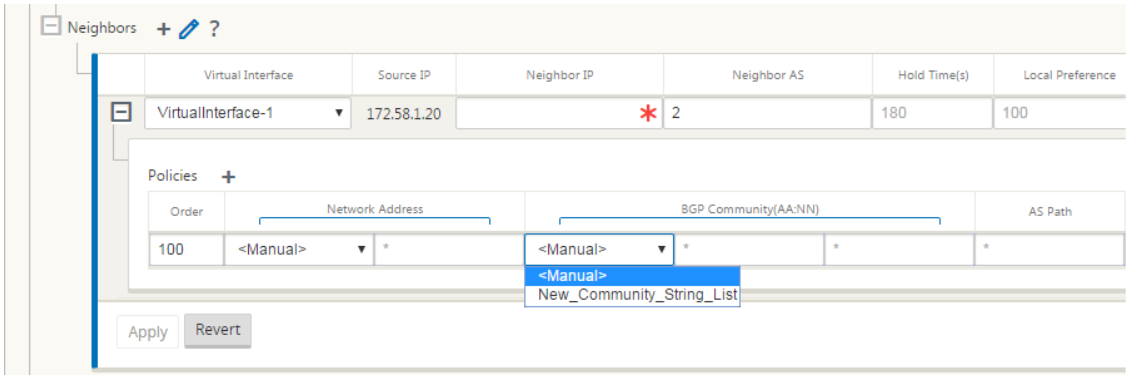
1. Konfigurieren Sie Nachbarn, indem Sie auf **Hinzufügen** klicken, wie unten gezeigt.

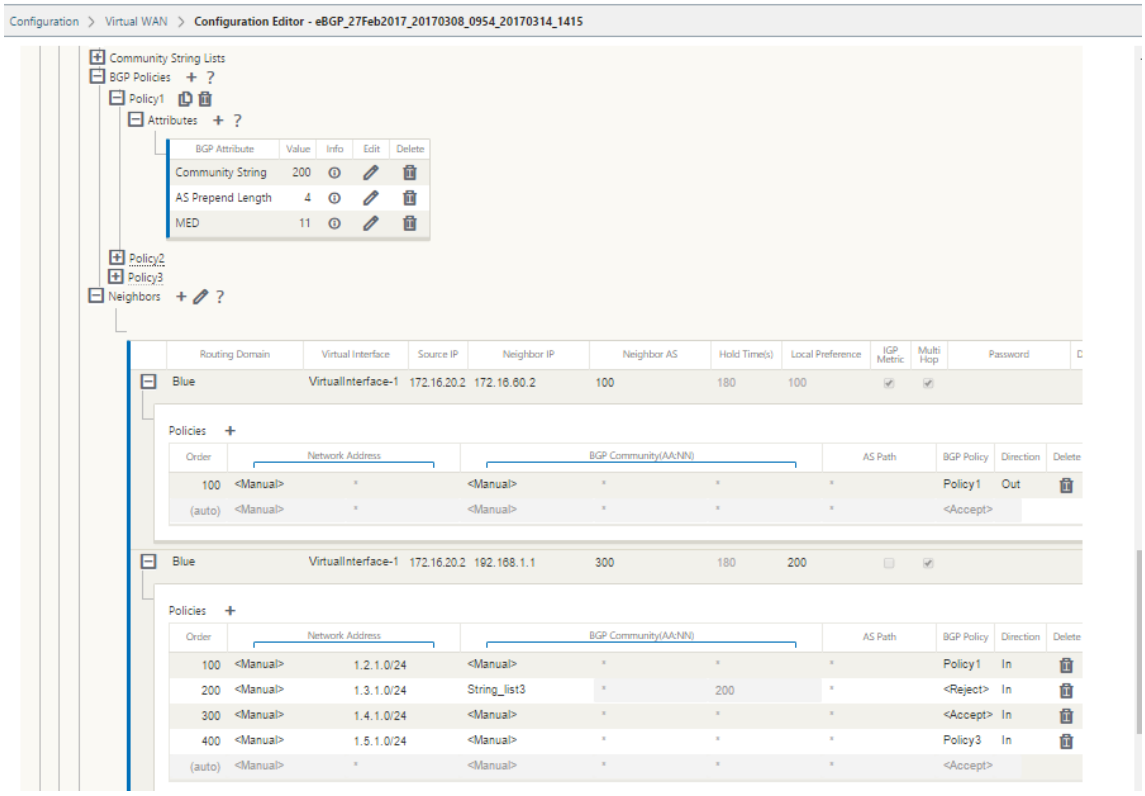


2. Klicken Sie auf das **+** Zeichen. Wählen Sie ein **virtuelles Interface**aus. Geben Sie die **Nachbar-IP-Adresse** ein.



3. Richtlinien hinzufügen. Wählen Sie nach Bedarf **Netzwerkadresse**, **BGP Community**und **AS-Pfaddetails** aus. Klicken Sie auf **Apply**.





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.

Auf der Seite **Monitor** > Routing-Protokoll können Sie die Debug-Protokollierung aktivieren und **Protokolldateien für das Routing** anzeigen. Die Protokolle für den Routing-Daemon werden in separate Protokolldateien aufgeteilt. Die Standard-Routing-Informationen werden in *dynamic_routing.log* gespeichert, während dynamische Routingprobleme in *dynamic_routing_diagnostics.log* erfasst werden, die über die Überwachung von Routingprotokollen angezeigt werden können.

BGP Soft-Rekonfiguration

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.

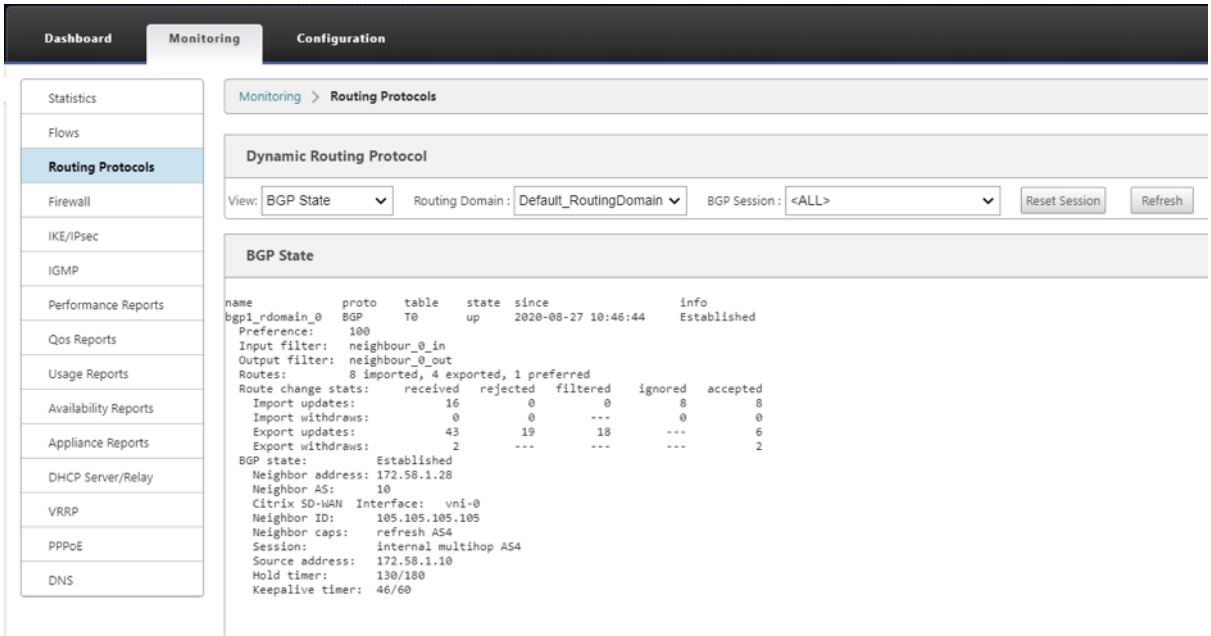
Das Löschen einer BGP-Sitzung mit einem Hard Reset macht den Cache ungültig und führt zu negativen Auswirkungen auf den Betrieb der Netzwerke, da die Informationen im Cache nicht verfügbar werden.

Die BGP Soft Reset Enhancement Funktion bietet automatische Unterstützung für dynamisches Soft-

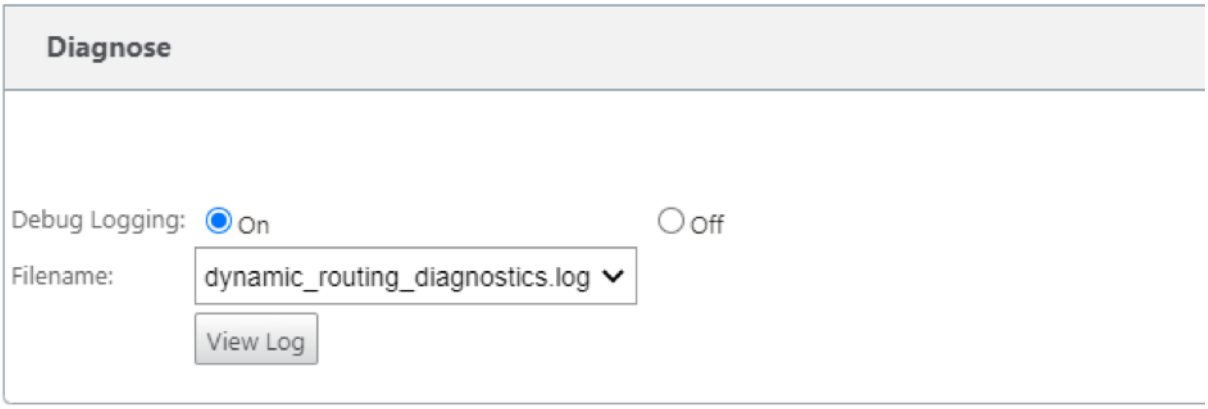
Reset eingehender BGP-Routing-Tabellenaktualisierungen, die nicht von Aktualisierungsinformationen für gespeicherte Routingtabellen abhängig sind.

Problembehandlung

Um die BGP-Parameter anzuzeigen, navigieren Sie zu **Überwachung > Routingprotokolle** > wählen Sie im Feld **AnsichtBGP-Status** aus.



Sie können die Dynamische Routingprotokolle beobachten, um festzustellen, ob ein Problem mit der BGP-Konvergenz vorliegt.



iBGP

October 28, 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 direktem Peering und vernetzt mit Citrix SD-WAN.

Einschränkungen:

- AS-Pfad-Prepend-, Med- und Community-Attribute werden nicht unterstützt.
- Routenfilterung zwischen OSPF und BGP während der Umverteilung wird nicht unterstützt. Entweder werden alle (oder) keine der von OSPF gelernten Routen für BGP-Peers beworben und umgekehrt.
- Die Routenaggregation wird nicht unterstützt.
- Es können nur maximal 16 BGP-Peers (einschließlich iBGP und eBGP) konfiguriert werden.

eBGP

October 28, 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 einzigen WAN-Pfad kommuniziert (nur Internet ist verfügbar) und wenn der Standort mit SD-WAN-Appliance (Site-A) die Internetverbindung verliert, kann der Standort ohne SD-WAN über ein anderes SD-WAN mit Site-A kommunizieren Appliance-Standort (Standort-B). Site-B leitet den Datenverkehr von der Site ohne SD-WAN-Appliance zum Site-A.

Kommunikation zwischen SD-WAN-Sites mithilfe von 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.

Anwendungsroute

October 28, 2021

In einem typischen Unternehmensnetzwerk greifen die Zweigstellen auf Anwendungen im on-premises 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 im Internet auf die SaaS-Anwendungen zugreifen können, ohne zuerst das Rechenzentrum durchlaufen zu müssen.

Mit Citrix SD-WAN können Sie die Anwendungsrouten für die folgenden Dienste definieren:

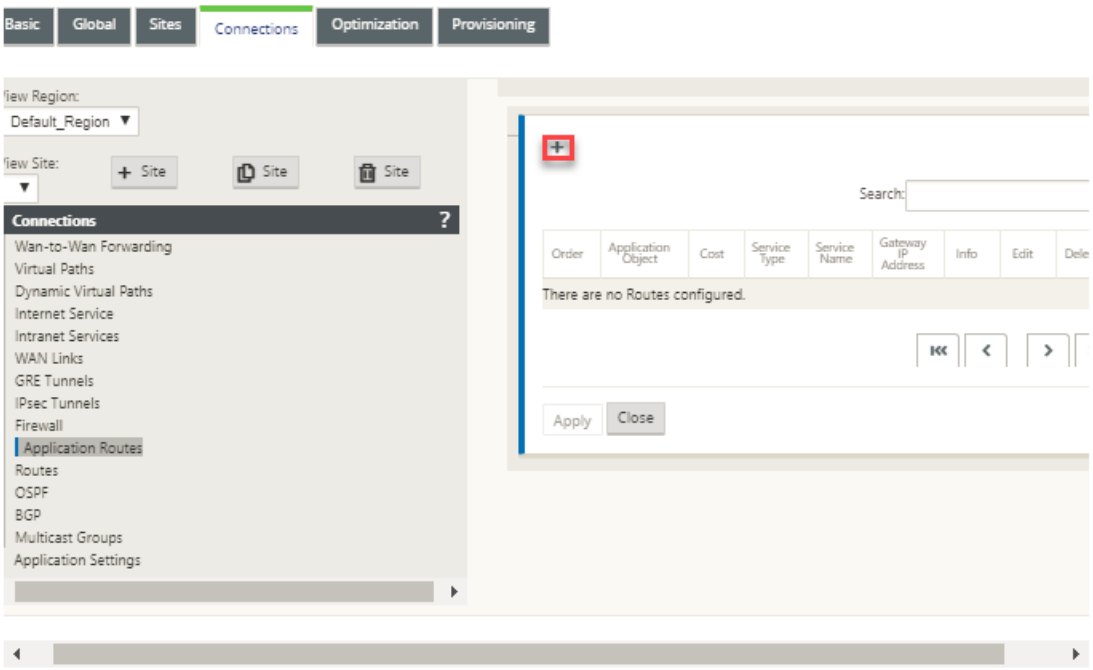
- **Virtueller Pfad**: Dieser Dienst verwaltet den Datenverkehr über die virtuellen Pfade. Ein virtueller Pfad ist eine logische Verbindung zwischen zwei WAN-Verbindungen. Es umfasst eine Sammlung von WAN-Pfaden, die kombiniert werden, um eine hohe Service-Level-Kommunikation zwischen zwei SD-WAN-Knoten zu ermöglichen. Die SD-WAN-Appliance misst das Netzwerk auf einer Pro-Pfad-Basis und passt sich an sich ändernde 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 Verkehr zwischen einer Enterprise-Site 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 den Intranetverkehr begrenzt.
- **Intranet**: Dieser Dienst verwaltet Enterprise Intranet-Verkehr, der nicht für die Übertragung über einen virtuellen Pfad definiert wurde. Der Intranet-Verkehr ist nicht gekapselt. Das SD-WAN verwaltet die Bandbreite, indem es diesen Datenverkehr im Vergleich zu anderen Diensttypen in Zeiten der Überlastung begrenzt. 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-Verkehr 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 GRE-Tunnel-Funktion können Sie SD-WAN-Appliances konfigurieren, um GRE-Tunnel im LAN zu beenden. 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 die Servicesteuerung für Anwendungen durchzuführen, ist es wichtig, eine Anwendung auf dem ersten Paket selbst zu identifizieren. Anfangs fließen die Pakete durch die IP-Route, sobald der Datenverkehr klassifiziert ist 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 anhand historischer Klassifizierungsergebnisse des DPI-Klassifizierers und benutzerkonfigurierter IP-Port-Übereinstimmungstypen erhalten.

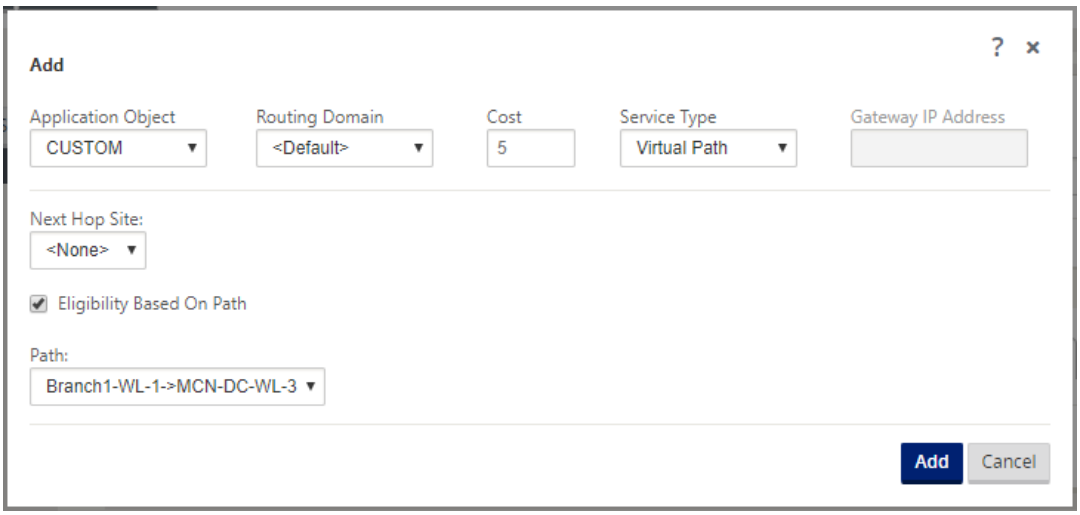
So konfigurieren Sie das Anwendungsrouting:

1. Navigieren Sie im Konfigurationseditor 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** von Anwendungsklassifizierung.



- **Routingdomäne**: Die Routingdomäne, die von der Anwendungsroute verwendet werden soll. Wählen Sie eine der konfigurierten Routingdomänen aus.
- **Kosten**: Ein Gewicht zur Bestimmung der Routenpriorität für diese Route. 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 den Anwendungsverkehr als Virtual Path Traffic und stimmt mit einem virtuellen Pfad basierend auf virtuellen Pfadregeln überein. Geben Sie im Feld **Next Hop Site** die Next-Hop-Remote-Site ein, an die Virtual Path-Pakete geleitet werden.

  > **Hinweis**
  >
  > Jeder Fluss, der die Anwendungsrouten für virtuelle Pfade trifft, durchläuft keinen dynamischen virtuellen Pfad.

- **Internet**: Identifiziert den Anwendungsverkehr als Internetverkehr und stimmt mit dem Internetdienst überein.
- **Intranet**: Identifiziert den Anwendungsverkehr als Intranet-Verkehr und stimmt mit einem Intranetdienst basierend auf den Intranet-Regeln überein. Wählen Sie im Feld **Intranetdienst** einen Intranetdienst aus, der für die Route verwendet werden soll.
- **Lokal**: Identifiziert den Anwendungsverkehr als lokal auf der Website und stimmt mit keinem Dienst überein. Verkehr, der für eine lokale Route beschafft und bestimmt ist, wird ignoriert.

> **Hinweis**
>
> Für den lokalen Diensttyp treffen die konfigurierten IP-Routen nach Abschluss der DPI-Klassifizierung die Routing-Entscheidung.

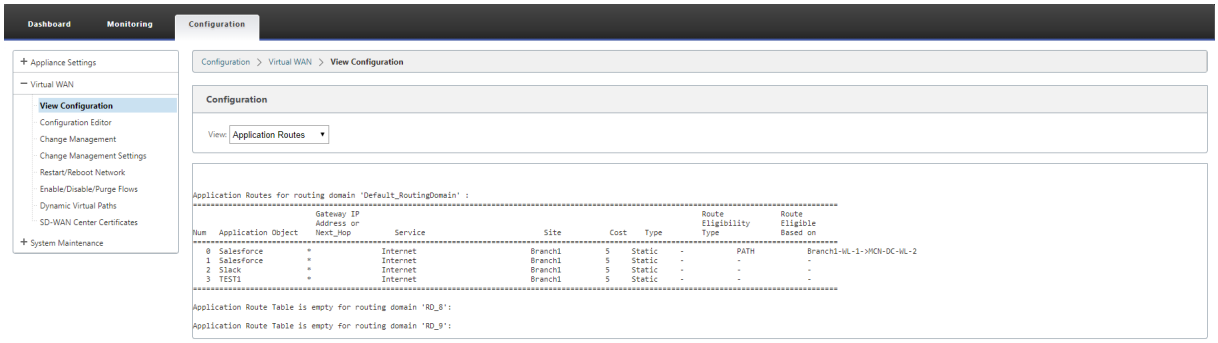
- **GRE-Tunnel**: Identifizierte den Anwendungsverkehr als für einen GRE-Tunnel bestimmt und stimmt mit dem am Standort konfigurierten LAN GRE-Tunnel überein. Geben Sie **im Feld Gateway-IP-Adresse** die Gateway-IP-Adresse ein, die sich im Subnetz des LAN GRE-Tunnels befinden muss. Wählen Sie **Berechtigung 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 Verkehr erhält, 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 Verkehr erhält, wenn der angegebene Pfad nicht verfügbar ist. Geben Sie im Feld **Pfad** den Pfad an, der zur Bestimmung der Routenberechtigung verwendet werden soll.

3. Klicken Sie auf **Apply**.

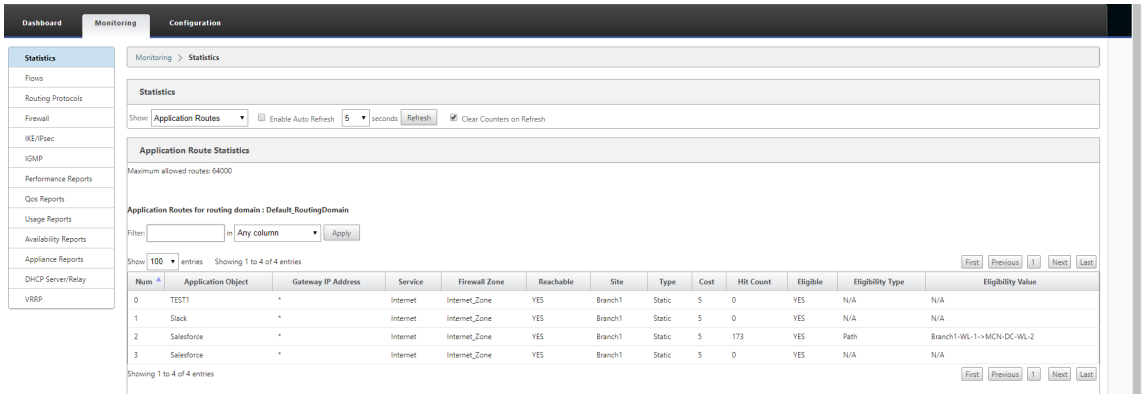
Anzeigen der auf Ihrer SD-WAN-Appliance konfigurierten Anwendungsrouten. Navigieren Sie in der SD-WAN-GUI zu **Konfiguration** > **Virtuelles WAN** > **Konfiguration anzeigen**. Wählen Sie im Dropdownmenü **Ansicht** die Option **Anwendungsrouten** aus.



So zeigen Sie Statistikdaten für die Anwendungsrouten an:

1. Navigieren Sie in der SD-WAN GUI zu **Monitoring** > **Statistik**.

2. Wählen Sie in der Dropdownliste **Anzeigen** die Option **Anwendungsrouten** aus.



Sie können die folgenden Statistiken anzeigen:

- **Application Object**: Name des Anwendungsobjekts.
- **Gateway-IP-Adresse**: Die Gateway-IP-Adresse, die von Anwendungsobjekten mit GRE-Tunneldiensttyp verwendet wird
- **Dienst**: Der Diensttyp, der dem Anwendungsobjekt zugeordnet ist.
- **Firewall-Zone**: Die Firewall-Zone, in die diese Route fällt.
- **Erreichbar**: Der Status der Anwendungsroute.
- **Seite**: Name der Website.
- **Typ**: Zeigt an, ob die Route statisch oder dynamisch ist.
- **Kosten**: Die Priorität der Route.
- **Anzahl der Treffer**: Die Häufigkeit, mit der die Anwendungsroute verwendet wird, um den Verkehr zu steuern.
- **Berechtigt**: Ist die Anwendungsroute berechtigt, den Verkehr zu senden?
- **Teilnahmeberechtigungstyp**: Die für diese Route angewendete Art der Berechtigungsbedingung für die Route. Der Berechtigungstyp kann Pfad, Gateway oder Tunnel sein.
- **Berechtigungswert**: Der für die Routenberechtigungsbedingung angegebene Wert.

> **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

October 28, 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.

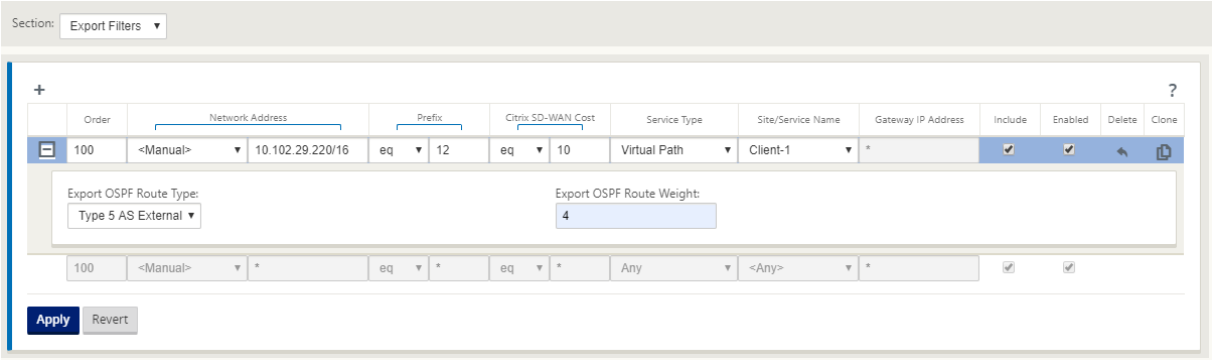
- Exportfilter werden verwendet, um Routen für Werbung mit OSPF- und BGP-Protokollen basierend auf bestimmten Übereinstimmungen ein- oder auszuschließen Kriterien. Exportfilterregeln sind die Regeln, die erfüllt sein müssen, wenn SD-WAN-Routen über dynamische Routingprotokolle Werbung gemacht werden. 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 **Konfigurationseditor**zu **Verbindungen > Regionen > Standort > OSPF** oder **BGP > Exportfilter**.



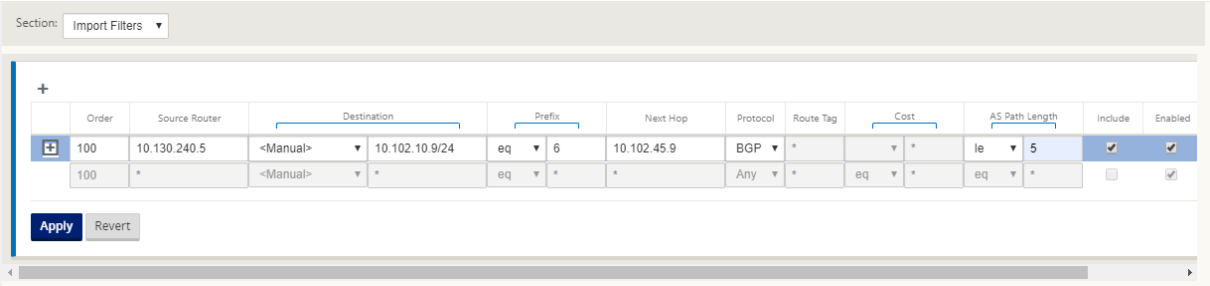
Verwenden Sie die folgenden Kriterien, um jeden Exportfilter zu erstellen, den Sie erstellen möchten.

Feld-Kriterien	Beschreibung	Wert
Bestellung	Die Reihenfolge, in der Filter priorisiert werden. Der erste Filter, mit dem eine Route übereinstimmt, wird auf diese Route angewendet.	100, 200, 300, 400, 500, 600
Netzwerkadresse	Geben Sie die **IP-Adresse** und Subnetzmaske des konfigurierten Netzwerkobjekts ein, das das Netzwerk der Route beschreibt	• IP-Adresse
Prefix	Um Routen nach Präfix abzugleichen, wählen Sie ein Übereinstimmungs-Prädikat aus dem Menü und geben Sie ein Routen-Präfix 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
Citrix SD-WAN Kosten	Die Methode (Prädikat) und die SD-WAN-Routenkosten, die verwendet werden, um die Auswahl der exportierten Routen einzugrenzen	Numerischer Wert
Servicetyp	Wählen Sie die Diensttypen aus, die übereinstimmenden Routen aus einer Liste von Citrix SD-WAN-Diensten zugewiesen sind	Beliebig, Lokal, Virtueller Pfad, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel

Feld-Kriterien	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 den LAN GRE-Tunnel als Servicetyp wählen, geben Sie die Gateway-IP für den Tunnel ein.	IP-Adresse
Einschließen	Aktivieren Sie das Kontrollkästchen, um Routen einzuschließen, die diesem Filter entsprechen. Ansonsten werden passende Routen ignoriert	–
Aktiviert	Aktivieren Sie das Kontrollkästchen, um diesen Filter zu aktivieren. Andernfalls wird der Filter ignoriert	–
Löschen	Wählen Sie das Löschen-Symbol, um diesen Filter zu löschen.	–
Klonen	Klicken Sie auf das Klonsymbol, um eine Kopie eines vorhandenen Filters zu erstellen	–

Konfigurieren Sie Importfilter

Navigieren Sie im **Konfigurationseditor**zu **Verbindungen > Regionen > Standort > OSPF** oder **BGP > Importfilter**.



Verwenden Sie die folgenden Kriterien, um jeden Exportfilter zu erstellen, den Sie erstellen möchten.

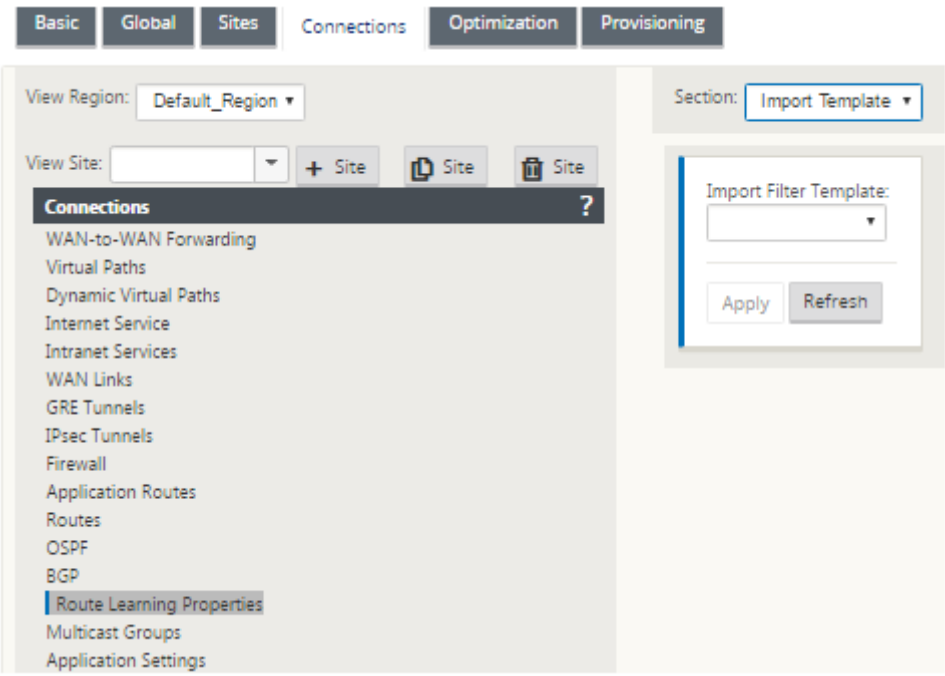
Feld-Kriterien	Beschreibung	Wert
Bestellung	Die Reihenfolge, in der Filter priorisiert werden. Der erste Filter, mit dem eine Route übereinstimmt, wird auf diese Route angewendet.	100, 200, 300, 400, 500, 600
Quell-Router	Die IP-Adresse des Quellrouters gilt nur für iBGP	• IP-Adresse
Ziel	Die IP-Adresse und Subnetzmaske des Ziels einer Route	• IP-Adresse
Prefix	Um Routen nach Präfix abzugleichen, wählen Sie ein Übereinstimmungs-Prädikat aus dem Menü und geben Sie ein Routen-Präfix 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
Weiter Hop	Die IP-Adresse des nächsten Hop	• IP-Adresse
Protokoll	Das Routing-Protokoll, mit dem eine Route erlernt wird	OSPF oder BGP
Routen-Tag	Das OSPF-Route-Tag, mit dem der Filter übereinstimmt. OSPF-Route-Tags verhindern Routingschleifen bei gegenseitiger Umverteilung zwischen OSPF und anderen Protokollen	Numerischer Wert

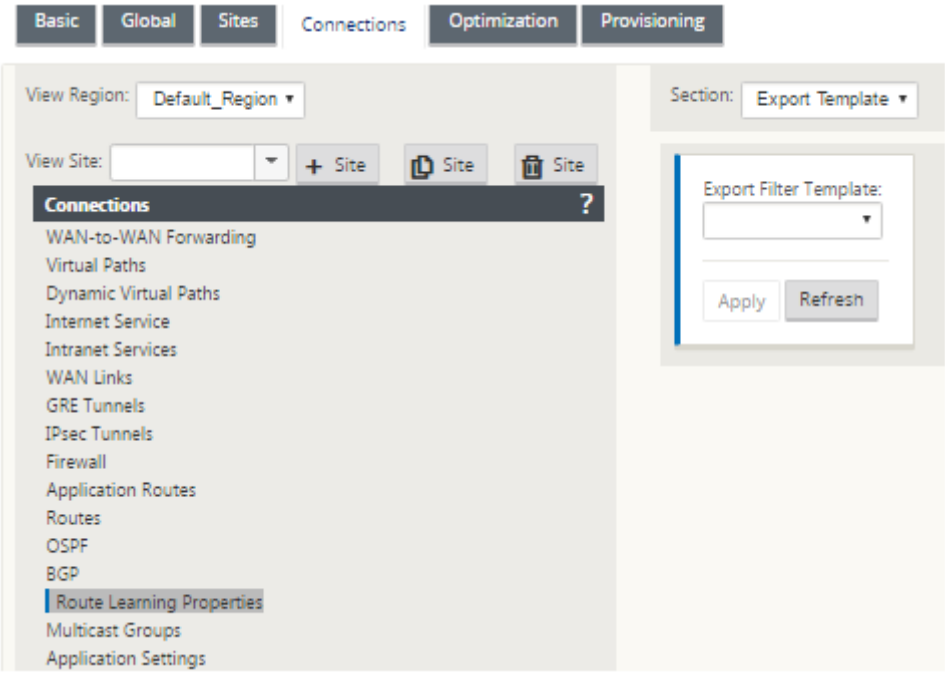
Feld-Kriterien	Beschreibung	Wert
Kosten	Die Routenkosten, mit denen OSPF-Routen für den Import übereinstimmen	Numerischer Wert
AS-Pfadlänge	Die AS-Pfadlänge, mit der BGP-Routen für den Import übereinstimmt	Numerischer Wert
Einschließen	Aktivieren Sie das Kontrollkästchen, um Routen einzuschließen, die diesem Filter entsprechen. Ansonsten werden passende Routen ignoriert	–
Aktiviert	Aktivieren Sie das Kontrollkästchen, um diesen Filter zu aktivieren. Andernfalls wird der Filter ignoriert	–
Löschen	Klicken Sie auf das Löschsymbol, um diesen Filter zu löschen.	–
Klonen	Klicken Sie auf das Klonsymbol, um eine Kopie eines vorhandenen Filters zu erstellen	–

Konfigurieren von Routenrichtlinienfilter

Sie können mehrere Import- oder Exportfiltervorlagen mit verschiedenen Filterregeln erstellen und die Vorlage an jeder Site zuordnen.

Die vom Benutzer erstellten Import/Exportfilterregeln auf Siteebene haben mehr Vorrang. Die Vorlagenregeln folgen den vom Benutzer erstellten Regeln, wenn sie mit der Site im Abschnitt **Route Learning** von Verbindungen verknüpft sind.





Routenzusammenfassung

October 28, 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 Übersichtsroute mit den Diensttypen Lokal und Discard konfigurieren. Diese zusammenfassende Route wird für die Next-Hop-Geräte beworben.

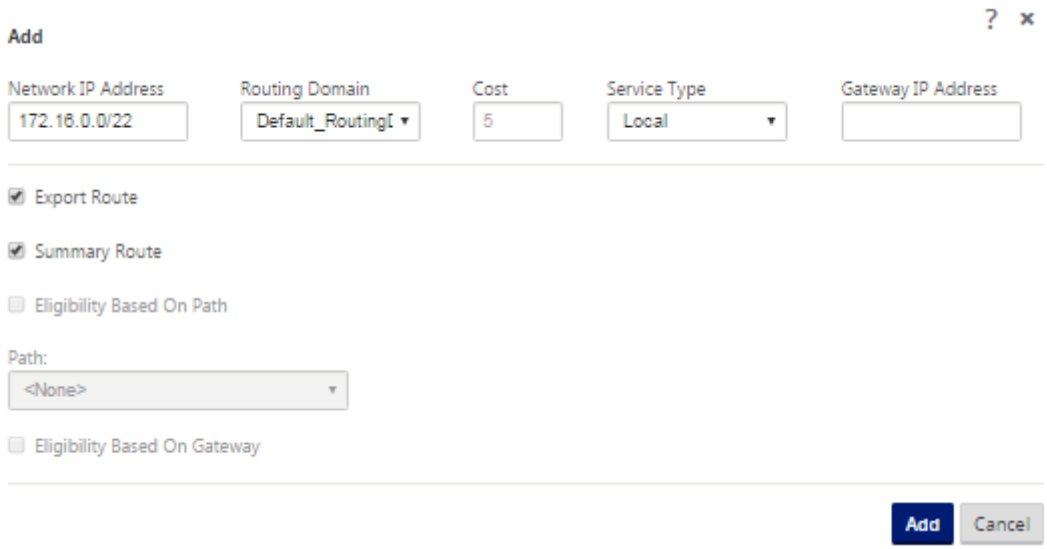
So konfigurieren Sie eine Übersichtsroute für ein lokales Subnetz:

1. Navigieren Sie im Konfigurationseditor 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 Übersichtsroute.
- **Kosten**: Ein Gewicht zur Bestimmung der Routenpriorität für diese Route. Lower-Cost-Routen haben Vorrang vor höheren Kosten Routen. Der Bereich liegt zwischen 1—15. Der Standardwert ist 5.
- **Routingdomäne**: Routing-Protokolle, die den zentralen Verwaltungspunkt für die Verwaltung eines Unternehmensnetzwerks, eines Zweigstellennetzwerks oder eines Rechenzentrumsnetzwerks bereitstellen.
- **Dienstart:** Wählen Sie Lokaler Diensttyp aus.

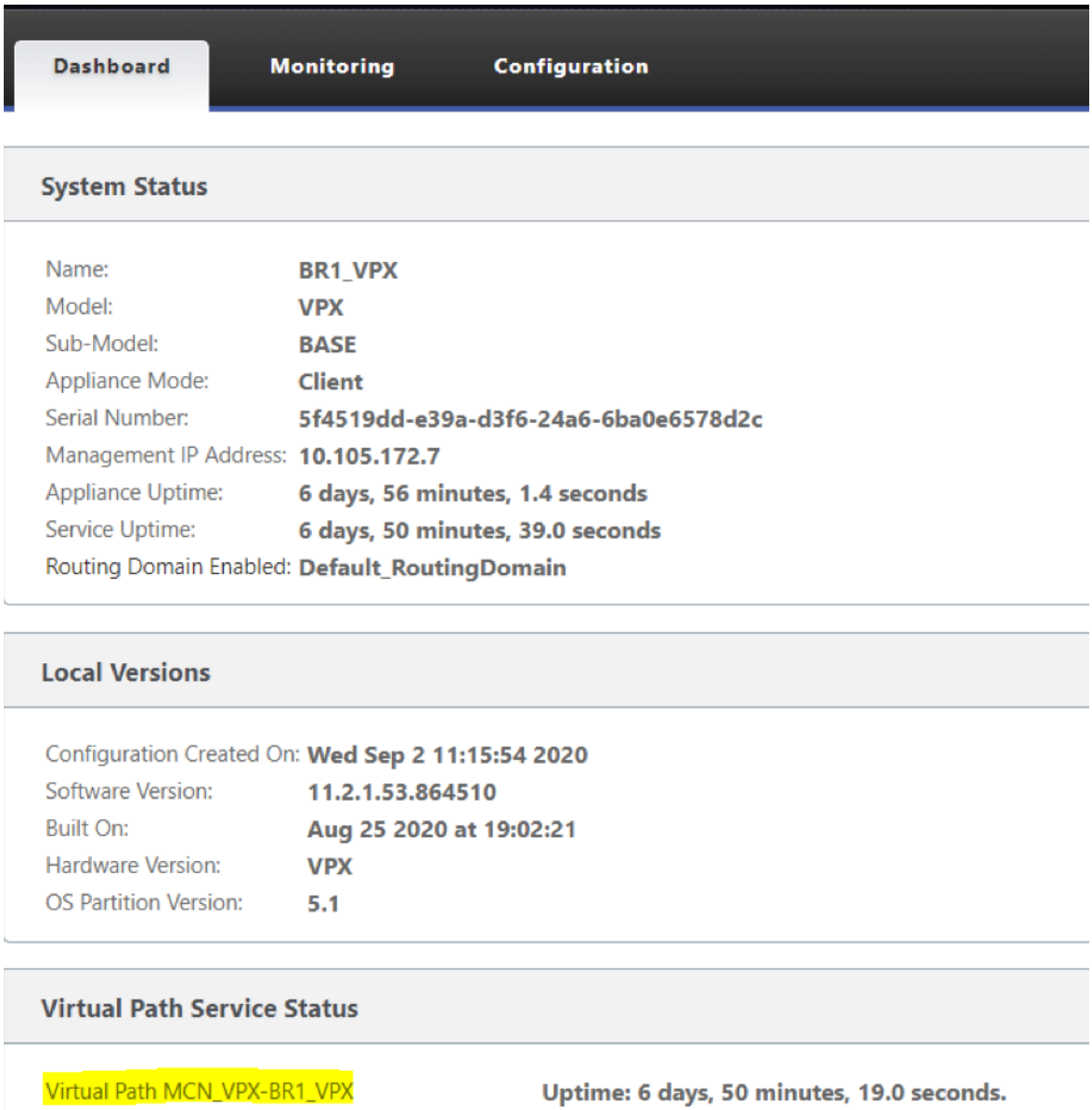
> **Hinweis**
>
> Sie können nur die Servicetypen "**Lokal** "und "**Verwerfen** "für Übersichtsrouten auswählen.

- **Gateway-IP-Adresse:** Gateway-IP-Adresse für diese Route.
- **Route exportieren:** Exportiert die Route zu anderen verbundenen Standorten.
- **Summary Route**: Werbt die Route als einzelne Sammelroute zu den anderen verbundenen Geräten anstelle aller anderen übereinstimmenden Subnetze an.



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.

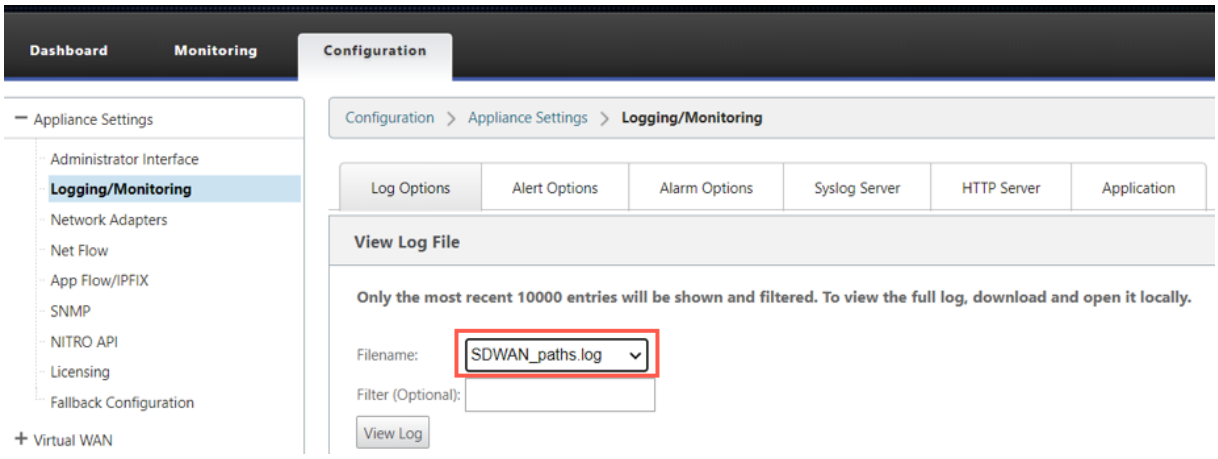


Wenn der virtuelle Pfad ausgefallen ist, überprüfen Sie den Grund dafür unter **Konfiguration > Logging/Monitoring**.

Wählen Sie eine der folgenden Dateien aus der Dropdownliste **Dateiname** aus, um dies zu überprüfen:

- SDWAN_paths.log

- SDWAN_common.log



Protokollpräferenz

October 28, 2021

Die Protokolleinstellung ist eine Citrix SD-WAN-spezifische Funktion, die der administrativen Entfernung des Routers ähnelt.

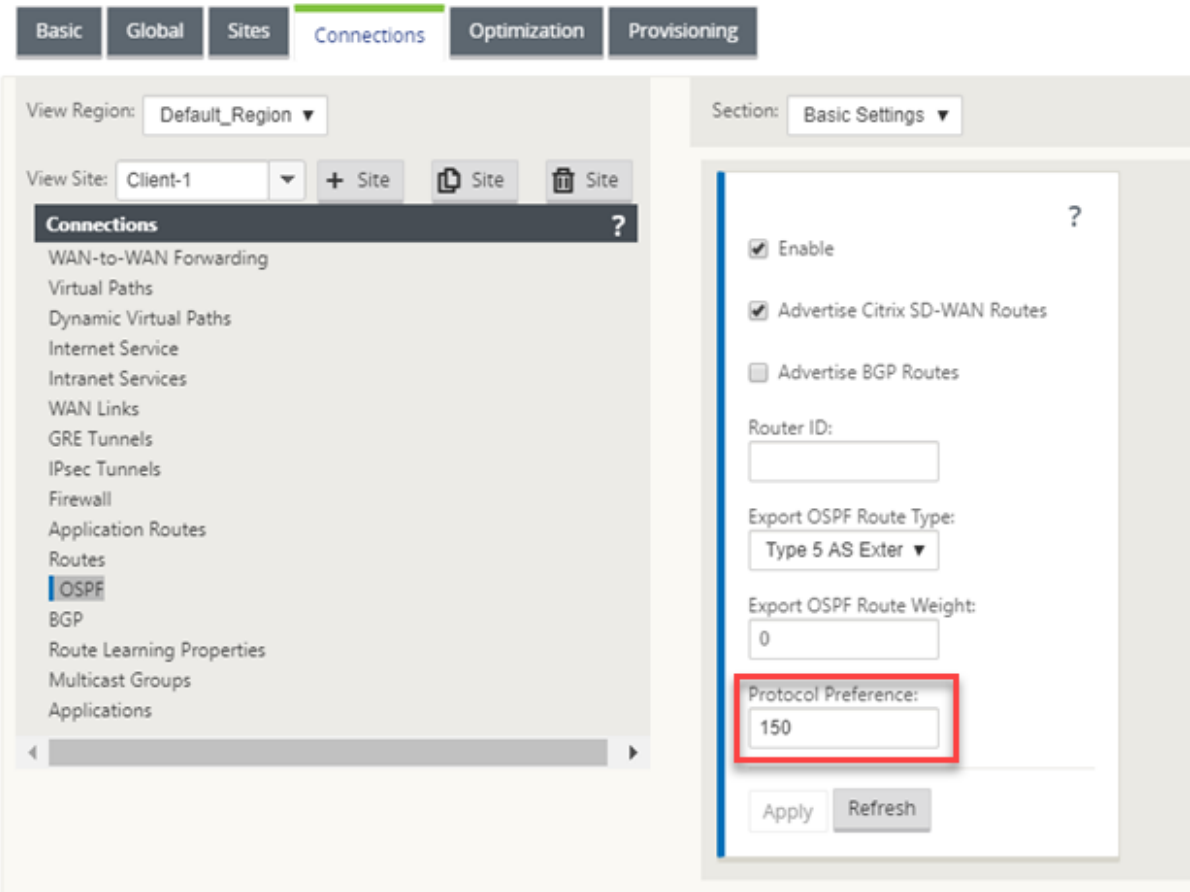
Wenn Citrix SD-WAN gleichzeitig ein Routenpräfix über virtuelle Pfade, das OSPF-Protokoll oder das BGP-Protokoll lernt, folgt es der folgenden Standardeinstellungsreihenfolge.

- 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 Protokollpräferenzwert festlegen, während Sie das BGP- oder OSPF-Protokoll konfigurieren. Sie können eine Einstellung im Bereich 100—200 angeben.

Die Protokollprioritätsinformationen befinden sich lokal auf der Citrix SD-WAN-Appliance und werden nicht für Peer-Netzwerkelemente angekündigt.



Multicast-Routing

October 28, 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 Multicastrouting auf der Citrix SD-WAN Appliance aktivieren, fungiert die Appliance als Multicastrouter.

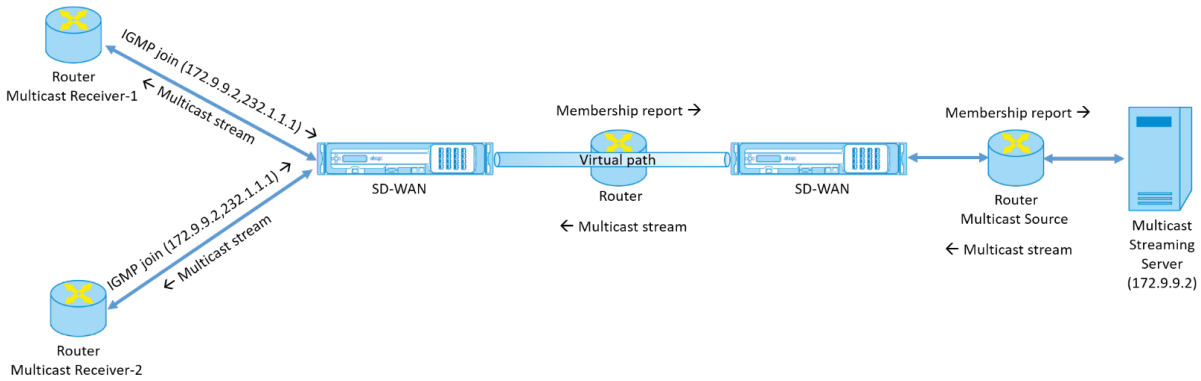
Quellspezifischer Multicast

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.

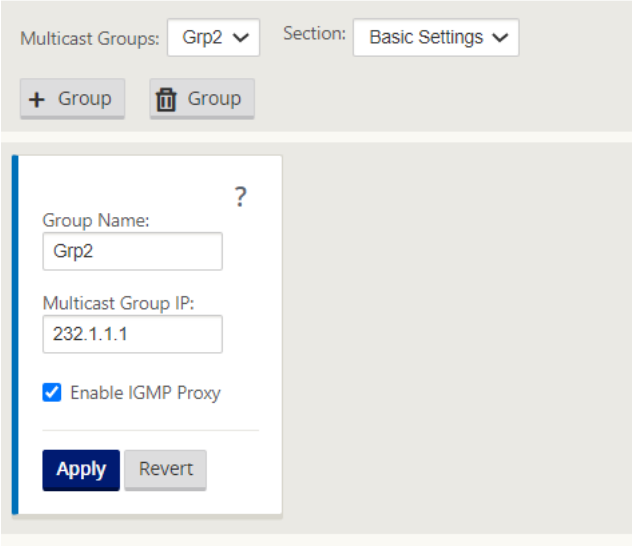
Der Datenverkehr des Kontrollkanals und der Multicast-Stream fließen durch den etablierten virtuellen Pfad zwischen der Zweigstelle und dem Rechenzentrum. Der Citrix SD-WAN Overlay-Pfad sichert und isoliert Multicast-Datenverkehr vor WAN-Verschlechterung oder Link-Brownouts.

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.

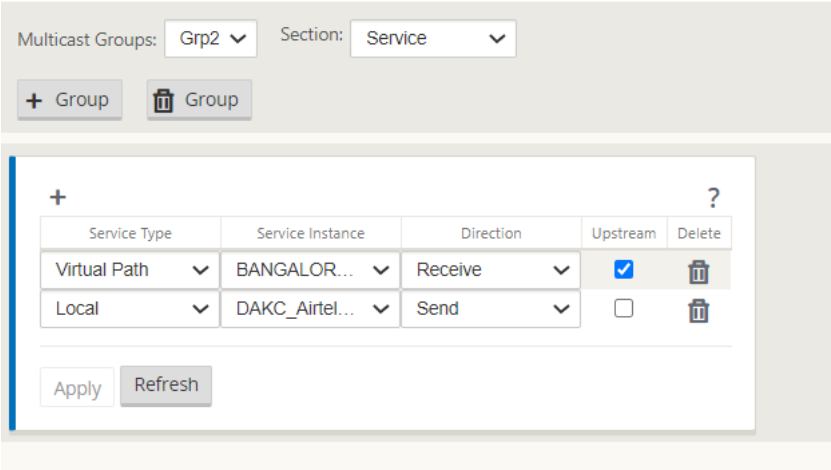
1. Multicastgruppe erstellen - Geben Sie einen Namen und eine IP-Adresse für die Multicastgruppe an. Die IP der Multicastgruppe muss im Bereich 232.0.0.0/8 für quellspezifisches Multicast liegen.
2. IGMP-Proxy aktivieren —Sie können die Citrix SD-WAN Appliance als IGMP-Proxy konfigurieren, um die IGMP-Kontrollkanalinformationen 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-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**.

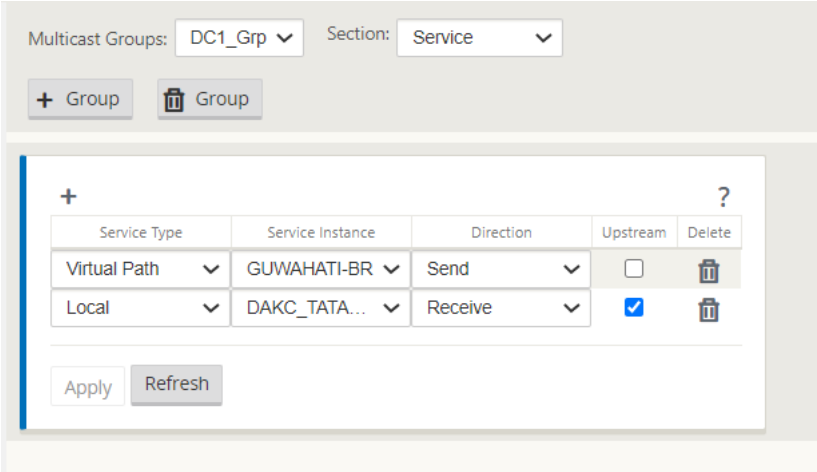


Konfigurieren Sie die Upstream- und Downstream-Pfade für die Zweigstellen- und Rechenzentrumsgeräte.

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.



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.

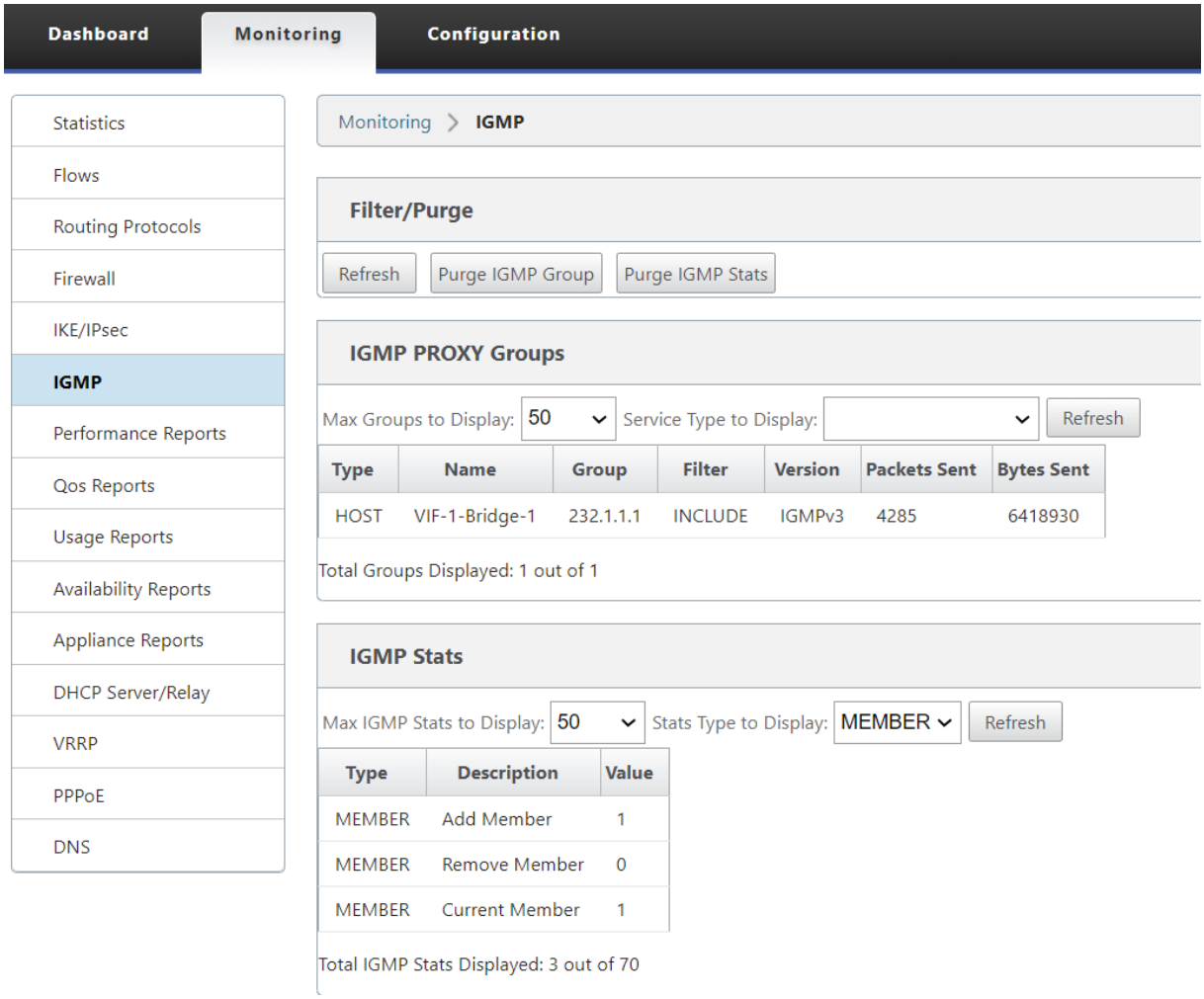


Überwachen

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.



Routenkosten für virtuelle Pfade konfigurieren

October 28, 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.

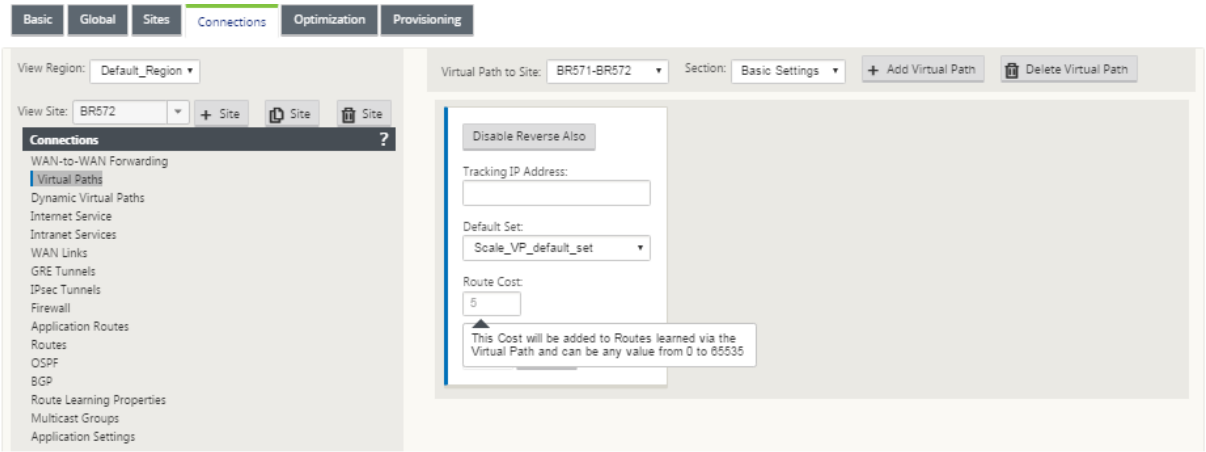
- OSPF-Routenkosten: Sie können jetzt OSPF-Routenkosten (Typ-1-Metrik) importieren, indem **Sie OSPF-Routenkosten kopieren** in den Importfiltern aktivieren. OSPF Routenkosten werden bei der Routenauswahl anstelle der SD-WAN-Kosten berücksichtigt. Kosten bis zu 65534 statt 15 werden unterstützt. Es ist 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 über mehr virtuelle Pfade eine Verbindung zu Diensten besteht, kann es manchmal zwei virtuelle Pfade vom Zweigstandort aus 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 standardmäßigen Standortkosten zu manipulieren. Auf diese Weise können wir manipulieren, welches Rechenzentrum für das Versenden 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 verwerfen die Kosten für die WAN-zu-WAN-Weiterleitung, die in Release-Versionen vor Version 10.0 existierten. Die auf WAN-zu-WAN-Weiterleitungskosten basierenden Routing-Entscheidungen müssen durch die Verwendung von VP-Routenkosten neu beeinflusst 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.

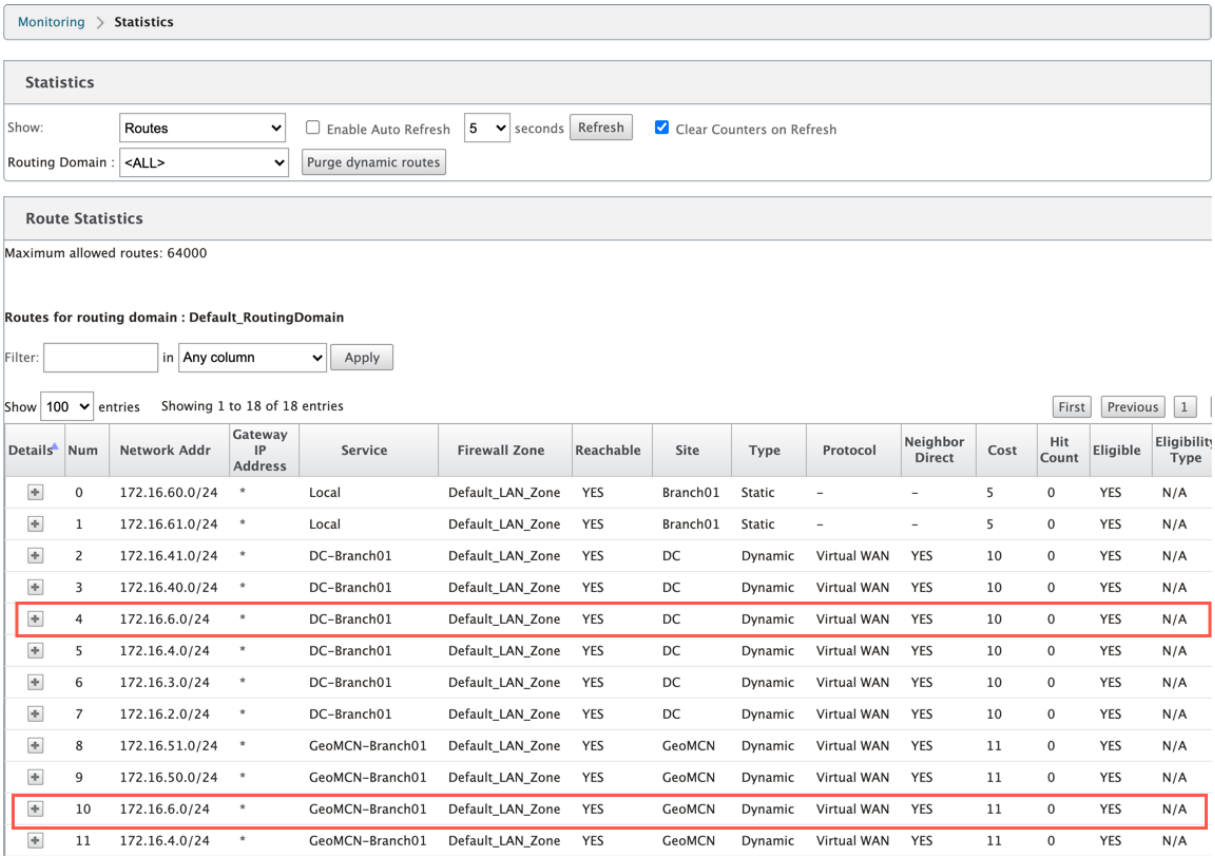
Sie können vier Routen haben, zwei Routen bis 172.16.2.0/24; eine über DC1 mit niedrigeren Kosten und dann über DC2 mit höheren Kosten und 2 weitere für 172.16.3.0/24.

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 Pfadroute 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.



Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	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

October 28, 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. Mit VRRP können Sie zwei oder mehr Router 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 die Kontrolle, wenn der Primär-/Master-Router ausfällt. In einem VRRP-Setup sendet der Master-Router ein VRRP-Paket, das als Ankündigung bezeichnet wird,

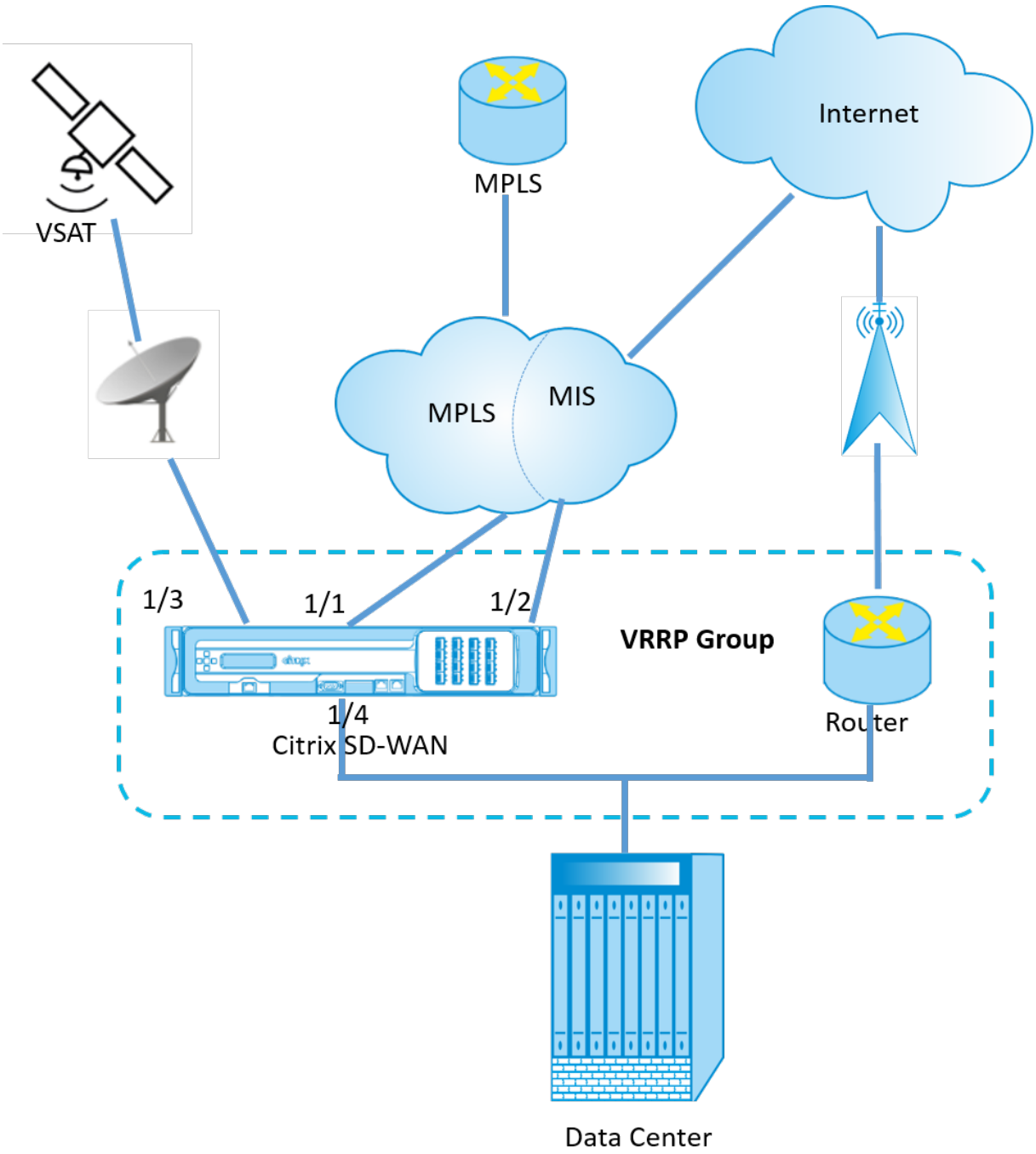
an die Backup-Router. Wenn der Master-Router die Ankündigung nicht mehr sendet, stellt der Backup-Router den Intervall-Timer ein. Wenn innerhalb dieser Haltezeit keine Ankündigung eingeht, leitet der Backup-Router die Failover-Routine ein.

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 eingeleitet, wenn der Master ausfällt, ein neuer Router der Gruppe beitritt oder ein vorhandener Router die Gruppe verlässt.

VRRP stellt einen Standardpfad für hohe Verfügbarkeit sicher, ohne dynamische Routing- oder Routererkennungsprotokolle auf jedem Endhost zu konfigurieren.

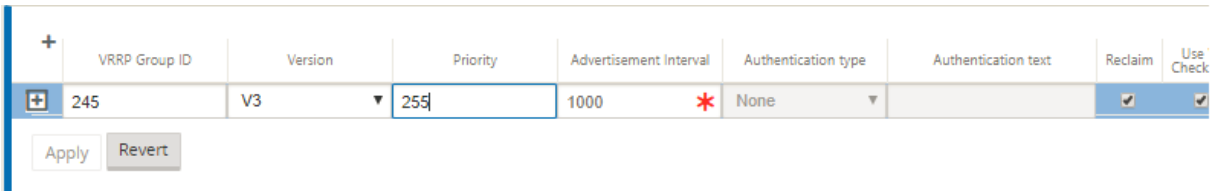
Citrix SD-WAN Version 10.1 unterstützt VRRP Version 2 und Version 3, um mit Routern von Drittanbietern zu arbeiten. Die SD-WAN-Appliance fungiert als Master-Router und leitet den Datenverkehr an, den Virtual Path Service zwischen Standorten zu verwenden. Sie können die SD-WAN-Appliance als VRRP-Master 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 als VRRP-Gruppe konfigurierten Router. 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 Konfigurationseditor zu **Sites > Site-Name > VRRP**, und klicken Sie auf **+** .



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 liegt zwischen 1—254. Stellen Sie diesen Wert auf Maximum (254) ein, um die SD-WAN-Appliance zum Master zu machen.

> **Hinweis**
>
> Wenn der Router der Besitzer der VRRP-IP-Adresse ist, ist die Priorität standardmäßig auf 255 festgelegt.

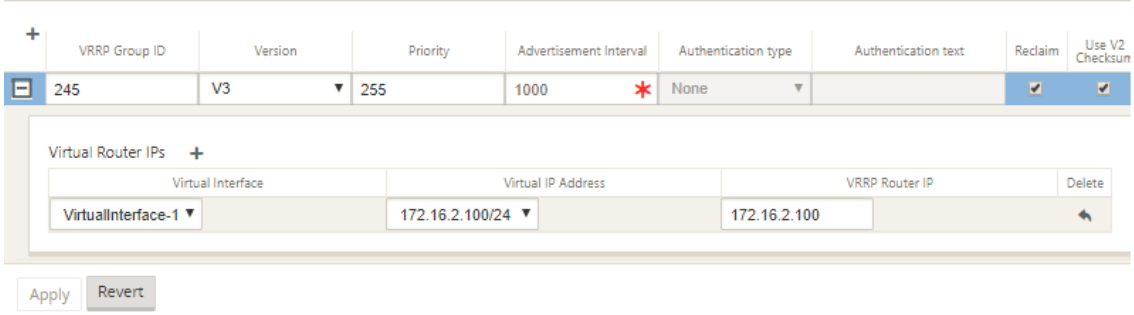
- **Advertisement Interval**: Die Frequenz in Millisekunden, mit der die VRRP-Ankündigungen gesendet werden, wenn die SD-WAN-Appliance der Master ist. Das standardmäßige Ankündigungsintervall beträgt eine Sekunde.
- **Authentifizierungstyp:** Sie können **Klartext** wählen, um eine Authentifizierungszeichenfolge einzugeben. Die Authentifizierungszeichenfolge wird in den VRRP-Ankündigungen als Klartext ohne Verschlüsselung gesendet. Wählen Sie **Keine**, wenn Sie keine Authentifizierung 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.

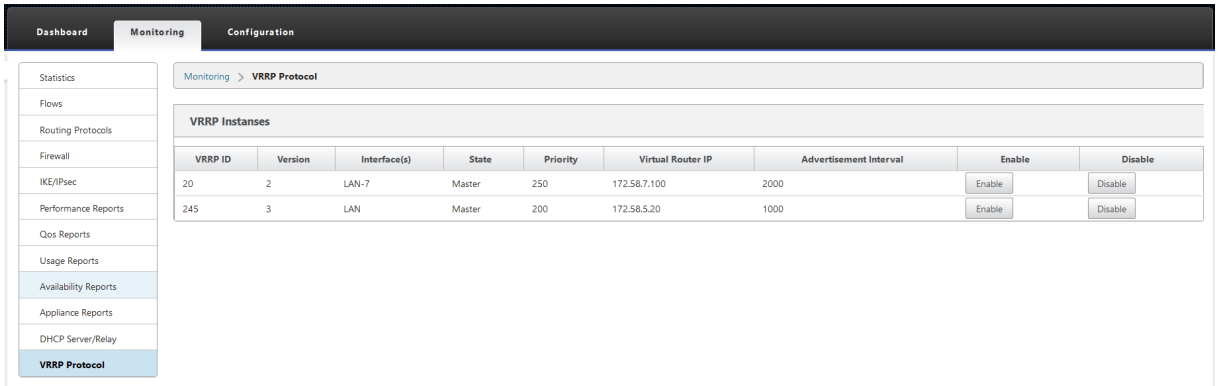
Konfigurieren Sie die VRRP-IP-Adresse. Geben Sie Werte für die folgenden Felder ein und klicken Sie auf **Übernehmen**.

- **Virtuelle Schnittstelle**: Die virtuelle Schnittstelle, die für VRRP verwendet werden soll. Wählen Sie eine der konfigurierten virtuellen Schnittstellen.
- **Virtuelle IP-Adresse**: Die virtuelle IP-Adresse, die der virtuellen Schnittstelle zugewiesen ist. Wählen Sie eine der konfigurierten virtuellen IP-Adressen für die virtuelle Schnittstelle.
- **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-Statistik

Sie können die VRRP-Statistiken unter **Überwachung** > **VRRP-Protokoll** anzeigen.



Sie können die folgenden Statistikdaten anzeigen:

- **VRRP-ID:** Die VRRP-Gruppen-ID
- **Version:** Die VRRP-Protokollversion.
- **Schnittstelle:** Die für VRRP verwendete virtuelle Schnittstelle.
- **Zustand:** Der VRRP-Status der SD-WAN-Appliance. Es zeigt an, ob die Appliance ein Master oder ein Backup ist.
- **Priorität:** Die Priorität der SD-WAN-Appliance für eine VRRP-Gruppe
- **IP des virtuellen Routers:** Die IP-Adresse des virtuellen Routers für die VRRP-Gruppe.
- **Advertisement Intervall:** Die Häufigkeit von VRRP-Werbung.
- **Aktivieren:** Wählen Sie diese Option, um die VRRP-Instanz auf der SD-WAN-Appliance zu aktivieren.

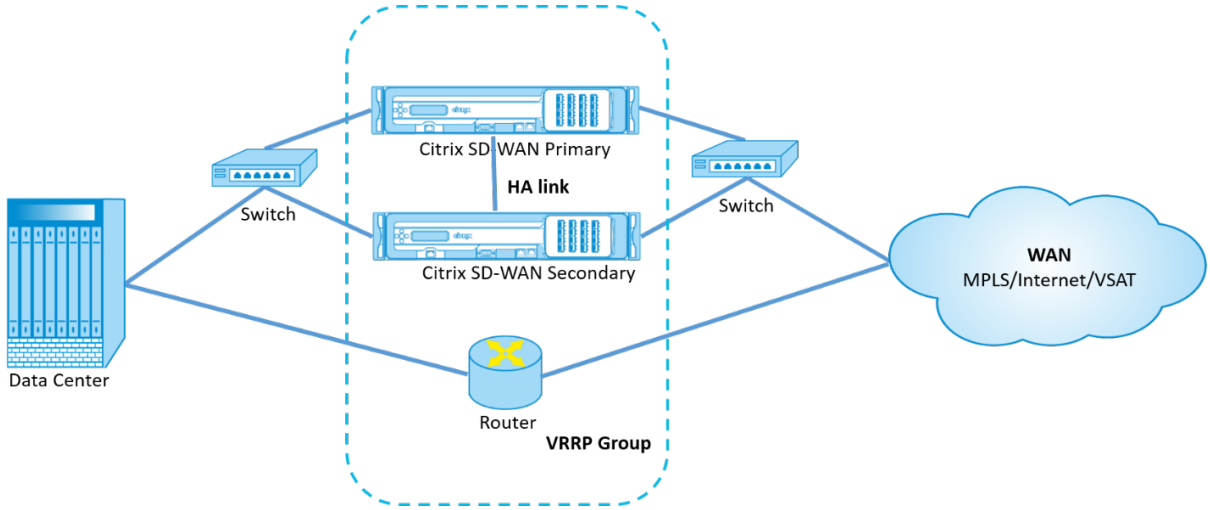
- **Deaktivieren:** Wählen Sie diese Option, um die VRRP-Instanz auf der SD-WAN-Appliance zu deaktivieren.

Einschränkungen

- VRRP wird nur in der Gateway-Modus-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 die 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 bereit, um die VRRP-Gruppe zu bilden. 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 Hochverfügbarkeit.

Konfigurieren von Netzwerkobjekten

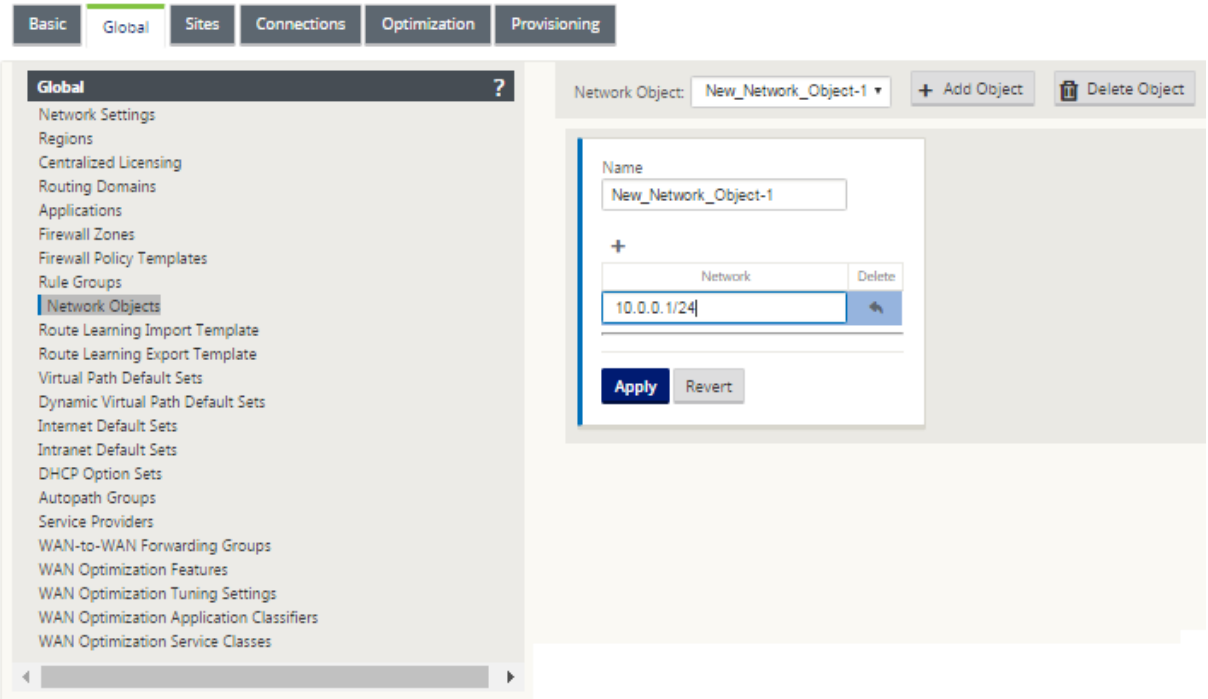
October 28, 2021

Citrix SD-WAN führt die Option ein, Netzwerkobjekte im Bereich **Global** im Konfigurationseditor hinzuzufügen. Sie können beim Definieren eines Routenfilters mehrere Subnetze gruppieren und auf ein einzelnes Netzwerkobjekt verweisen, anstatt einen Filter für jedes Subnetz zu erstellen.

So konfigurieren Sie Netzwerkobjekte:

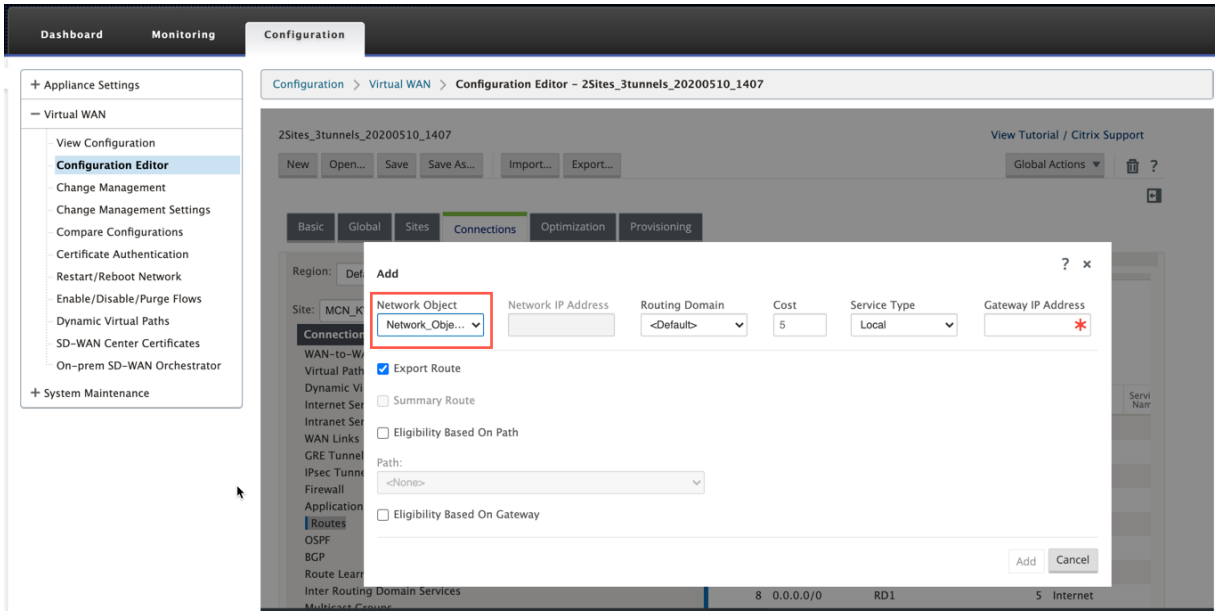
1. Navigieren Sie im **Konfigurationseditor**zu **Global** → **Netzwerkobjekte**und klicken Sie auf **Hinzufügen (+)**.
2. Klicken Sie unter Netzwerke auf **Hinzufügen (+)**.
3. Geben Sie die **IP-Adresse** und das **Subnetz** des neuen Netzwerkobjekts ein.
4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Um den Namen des Netzwerkobjekts zu bearbeiten, klicken Sie auf den Namen des Netzwerkobjekts und geben einen neuen Namen ein.

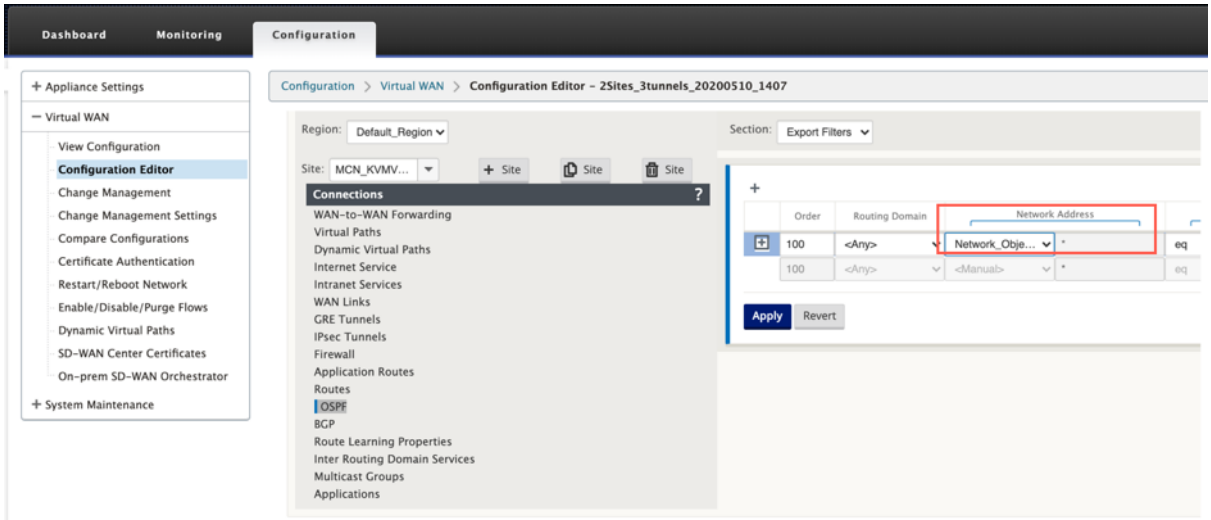


Folgende Funktionen nutzen die Netzwerkobjekte:

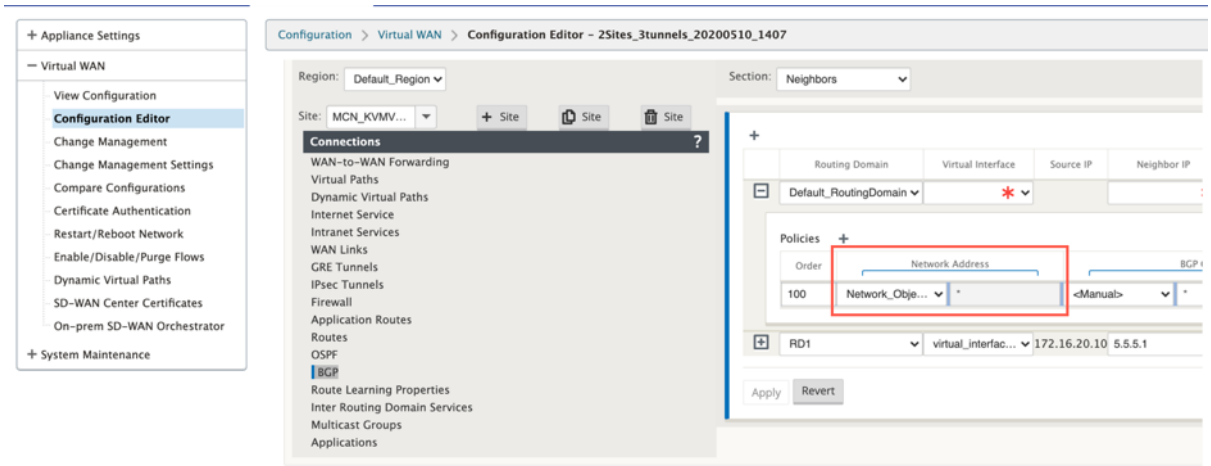
- Routen (**Konfigurationseditor > Verbindungen > Routen > Klick**+******Netzwerkobjekt****)



- BGP- und OSPF-Import- und Exportfilter (**Konfigurationseditor > Verbindungen > BGP/OSPF > Filter exportieren/importieren** click **+ > Netzwerkadresse**)



- BGP-Nachbar-Richtlinien (**Konfigurationseditor > Verbindungen > BGP > Nachbarn > Richtlinien** click **+ > Netzwerkadresse**)



Routing-Unterstützung für die LAN-Segmentierung

October 28, 2021

Die SD-WAN Standard (Enterprise) Edition-Appliances implementieren die LAN-Segmentierung an verschiedenen Standorten, an denen eine der beiden Appliances 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 Remotestandort 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 das WAN immer noch über denselben vorab festgelegten virtuellen Pfad zwischen den beiden Appliances durchqueren (es müssen keine neuen Pfade erstellt werden).

Ein Beispiel für diese Funktionalität ist, dass ein WAN-Administrator möglicherweise in der Lage ist, die Netzwerkumgebung für lokale Zweigstellen über ein VLAN zu segmentieren und einigen dieser Segmente (VLANs) Zugriff auf DC-Seitige LAN-Segmente zu gewähren, die Zugriff auf das Internet haben, während andere möglicherweise keinen solchen Zugriff erhalten. Die Konfiguration der VLAN-zu-VLAN-Zuordnungen erfolgt über den Konfigurationseditor des MCN in der SD-WAN-Management-Weboberfläche.

Domänendienst für den übergreifenden Routing

October 28, 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 Routing-Domäne finden Sie unter Routing-Domäne.

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-Domänendienst, 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.

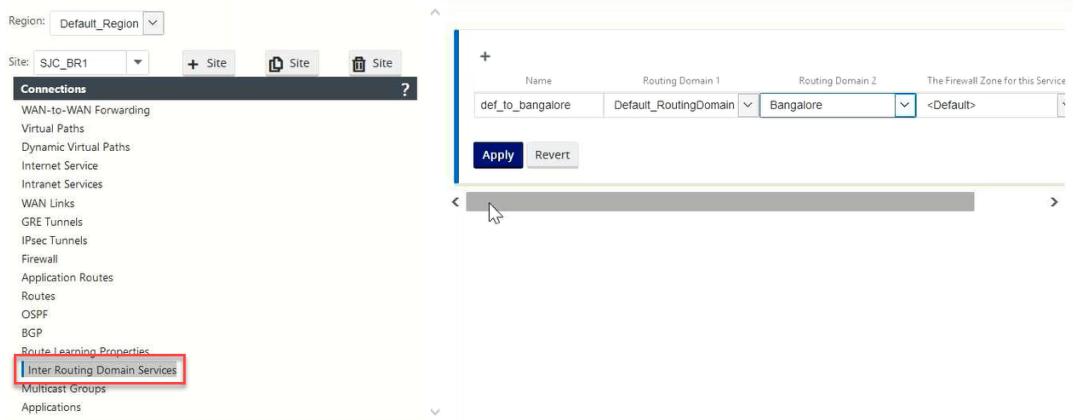
> **Hinweis**
>
> Citrix SD-WAN PE-Appliances führen keine WAN-Optimierungsfunktionen für Inter-Routing-Domänenpakete durch.

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. Weitere Informationen zur Konfiguration der Routingdomäne finden Sie unter Konfigurieren der Routingdomäne.

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.

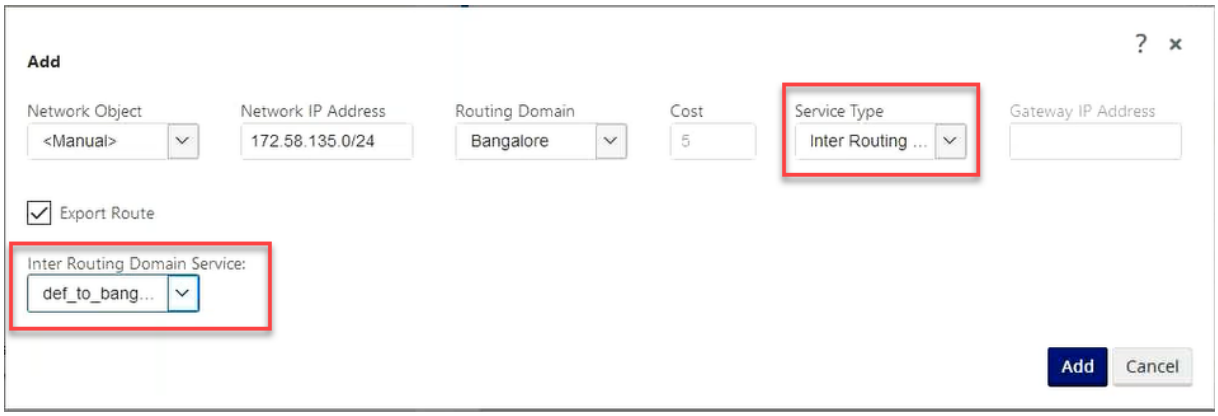


1. Klicken Sie auf **Anwenden**, um den Domänendienst zwischen Routing zu erstellen. Der erstellte Dienst kann zum Erstellen von Routen, Firewall-Richtlinien und NAT-Richtlinien verwendet werden.

> **Hinweis:**
>
> Sie können einen Domänendienst zwischen Routing nicht konfigurieren, der Routingdomänen verwendet, die auf einer Site nicht aktiviert sind.

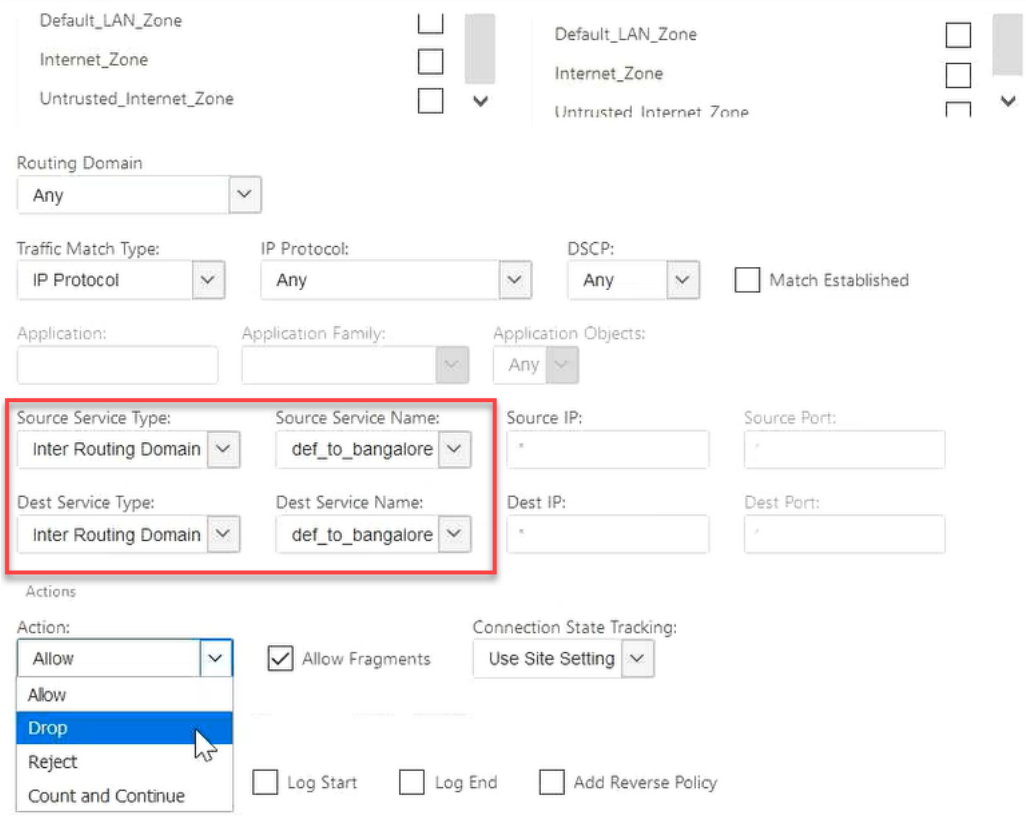
Um Routen mit dem Domänendienst zwischen Routing zu erstellen, erstellen Sie eine Route mit dem

Diensttyp als **Inter-Routing Domain Service** und wählen Sie den Inter-Routing-Domänendienst aus. Weitere Informationen zum Konfigurieren von Routen finden Sie unter How to Configure Routes.



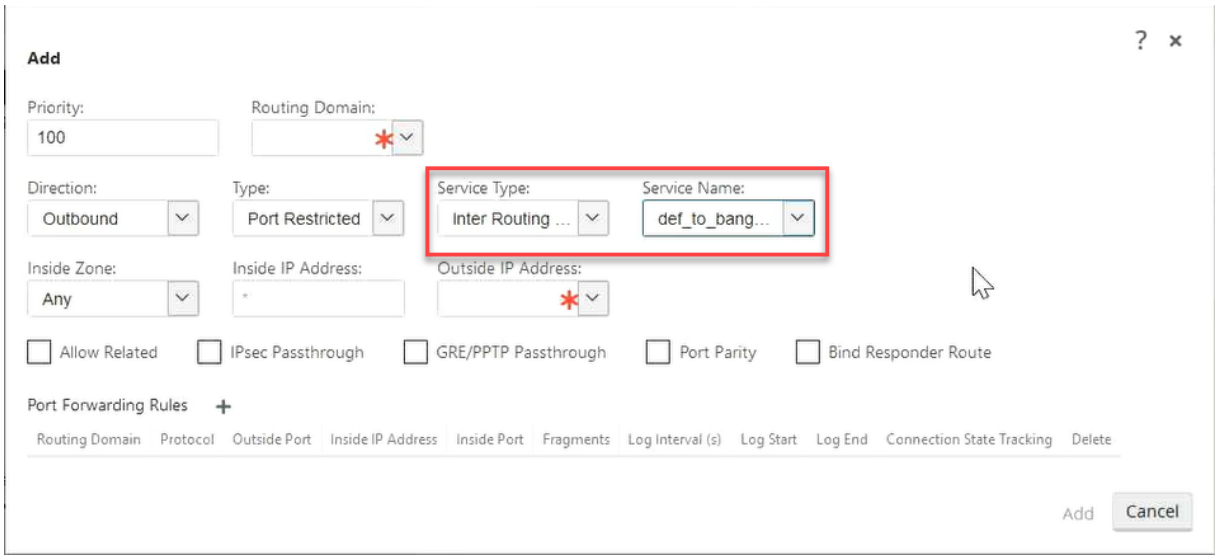
Fügen Sie außerdem eine Route aus dem anderen Routingdomänenpaar hinzu, um eine Verbindung zwischen den beiden Routingdomänen herzustellen.

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.



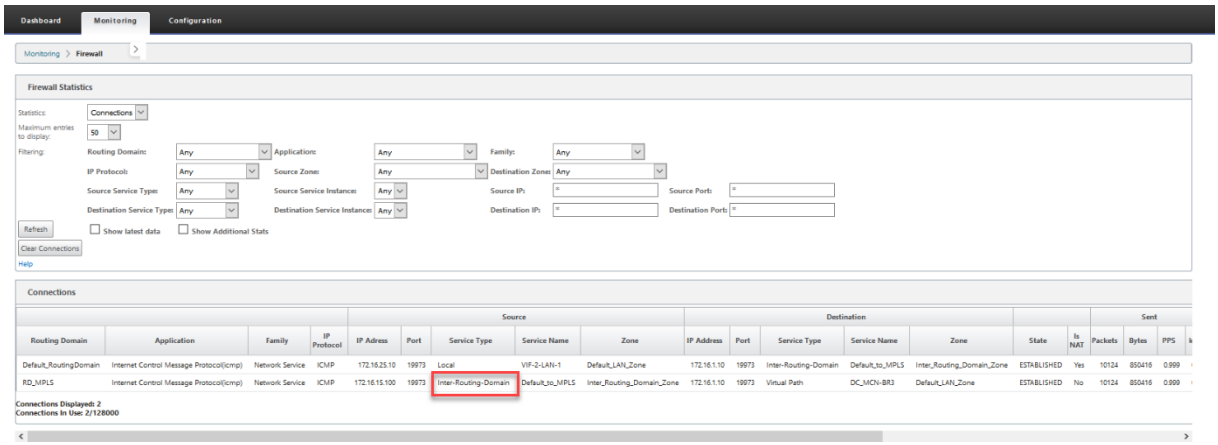
Sie können auch den Intranetdiensttyp auswählen, um statische und dynamische NAT-Richtlinien zu

konfigurieren. Weitere Informationen zum Konfigurieren von NAT-Richtlinien finden Sie unter Netzwerkadressübersetzung.



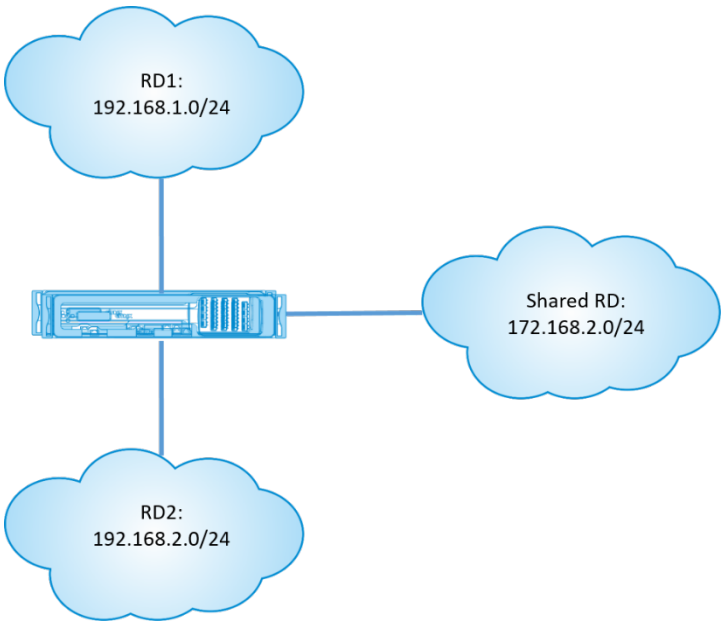
Überwachen

Unter Überwachung >Firewall-Statistiken**> Verbindungen können Sie**Überwachungsstatistiken**für Verbindungen anzeigen, die Interrouting-Domain-Dienste verwenden.**



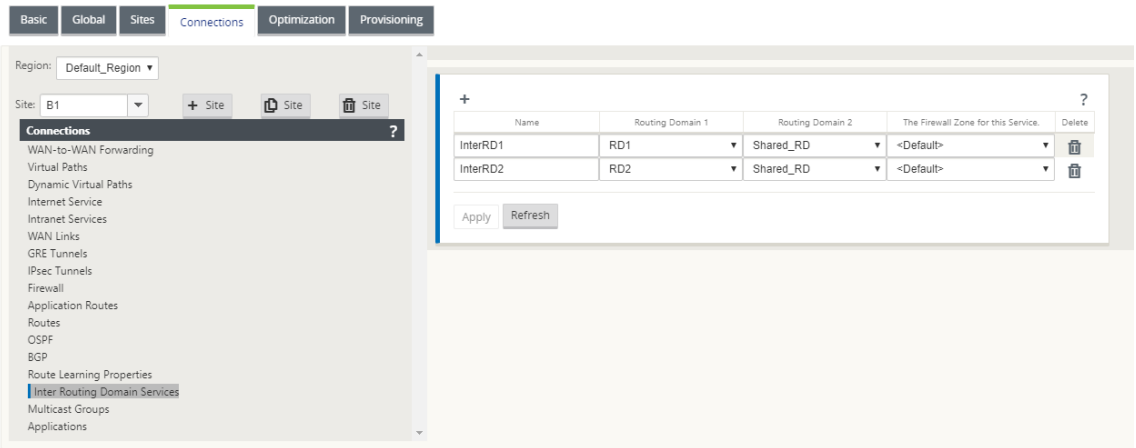
Anwendungsfall: Teilen von Ressourcen über Routingdomänen hinweg

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.

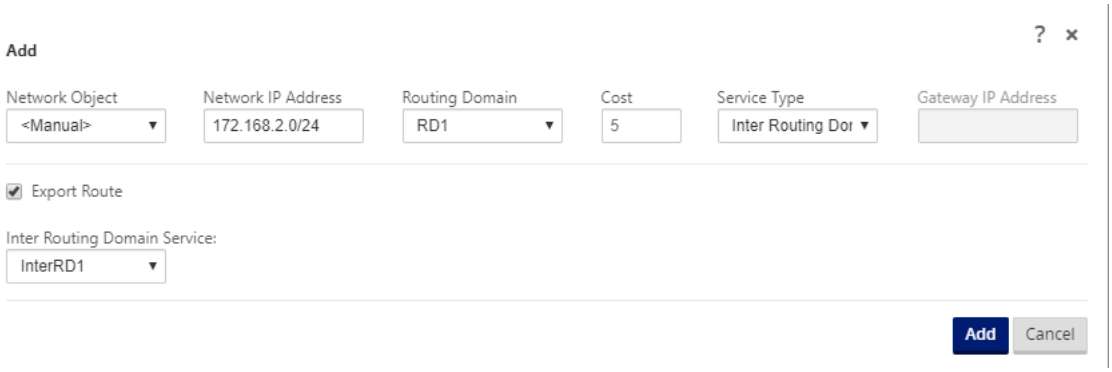


So ermöglichen Sie Benutzern in RD1 und RD2 den Zugriff auf Ressourcen in freigegebener RD:

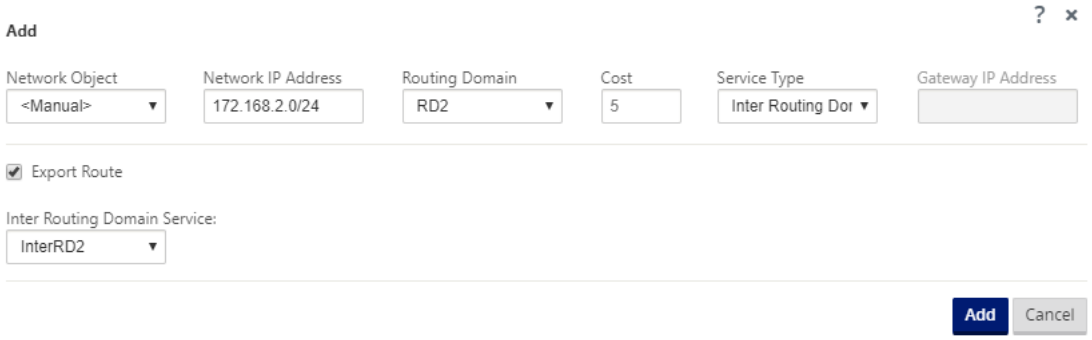
1. Erstellen Sie einen Inter-Routing Domain-Dienst zwischen RD1 und Shared RD, zum Beispiel **Inter RD1**.
2. Erstellen Sie einen Inter-Routing Domain-Dienst zwischen RD2 und Shared RD, zum Beispiel **Inter RD2**.



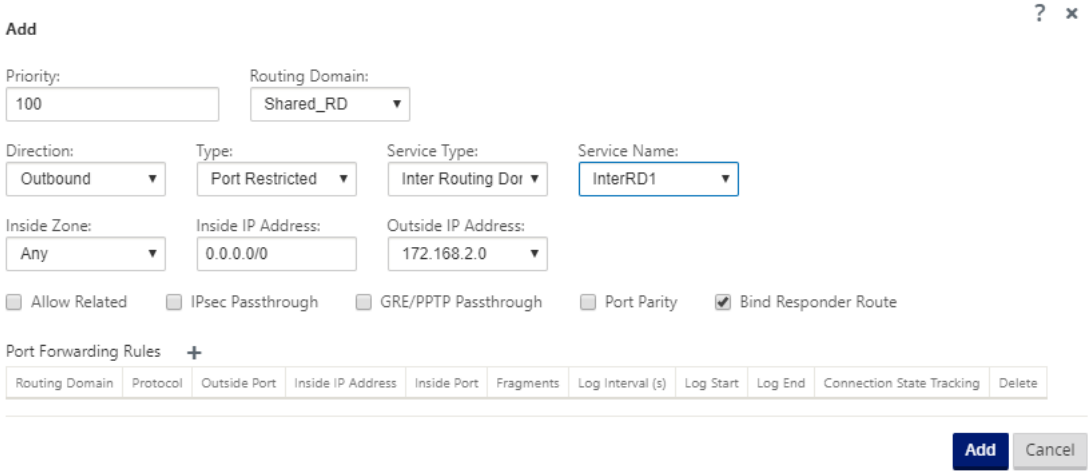
3. Konfigurieren Sie eine statische Route zu freigegebener RD von RD1 und RD2. Fügen Sie in RD1 eine Route 172.168.2.0/24 zu InterRD1 hinzu.



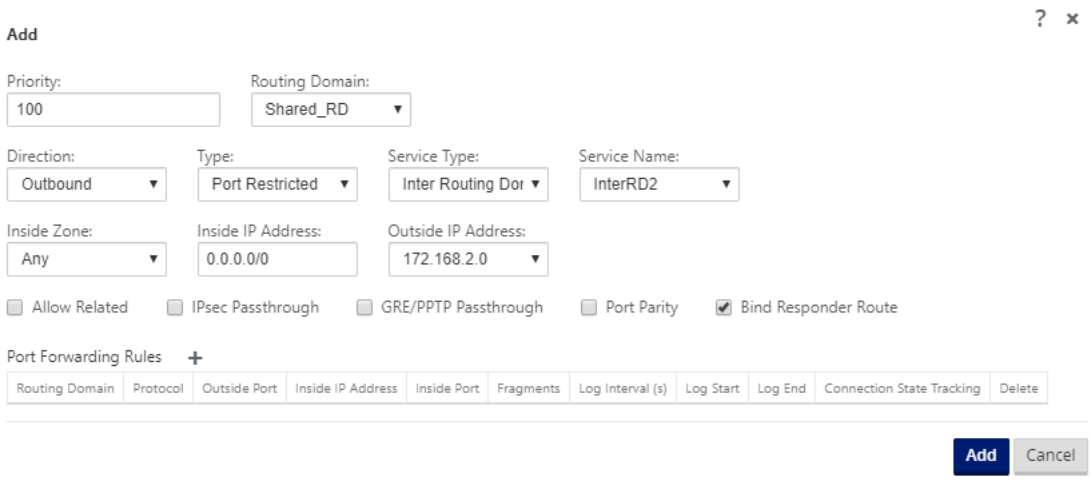
4. Fügen Sie in RD2 eine Route 172.168.2.0/24 zu InterRD2 hinzu.



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 Diensttyp verwendet.



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 “Responder Route binden “, um sicherzustellen, dass die umgekehrte Route denselben Diensttyp verwendet.



7. Verwenden Sie Filter, um zu begrenzen, auf welche Ressourcen in freigegebener RD von Benutzern in RD1/RD2 zugegriffen werden darf.

Sicheres Peering

October 28, 2021

Die Premium (Enterprise) Edition-Appliance kann im Rechenzentrum installiert werden und automatisches oder manuelles sicheres Peering initiieren, ein SSL-Profil erstellen und die Serviceklasse zuordnen und die Appliance mit einem Windows-Domänencontroller verbinden, damit Benutzer/Administrator die erweiterte umfangreiche Funktion des eigenständigen WANOP verwenden können Gerät.

Im Folgenden sind die für Auto Secure Peering und Manual Secure Peering unterstützten Bereitstellungsmodi aufgeführt:

Auto Secure Peering-Bereitstellungen:

Um Auto Secure Peering auf eine PE-Appliance von einem eigenständigen WANOP/SDWAN SE/WANOP am DC-Standort durchzuführen.

Schritte zum Initiieren dieser Bereitstellung:

- Das WANOP DC-Gerät befindet sich im LISTEN-ON-Modus (2312/Jeder nicht standardmäßige Port) und Branch PE 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.

Zur Durchführung von Auto-Secure-Peering, das von einer PE-Appliance am DC-Standort und an der PE-Appliancean

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-Einheit initiiert automatisches sicheres Peering zur Branch WANOP/SD-WAN SE-Appliance, die die privaten CA-Zertifizierungsstellen und CERT KEY-Paare installiert und CONNECT-TO auf der PE-Appliance mit der LISTEN-ON-IP von DC PE konfiguriert.

Manuelle Secure Peering-Bereitstellungen:

Manuelles Secure Peering wurde vom PE-Gerät am DC-Standort zur Zweigstelle 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 Zweigstelle 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 für PE befindet sich in der Schnittstellen-IP, die der Routingdomäne zugeordnet ist, für die "Umleitung zu WANOP"aktiviert ist
- Laden Sie CA- und Cert Key-Paare Zertifikate manuell hoch, die von authentischer Quelle der Zertifizierungsstelle erhalten wurden.

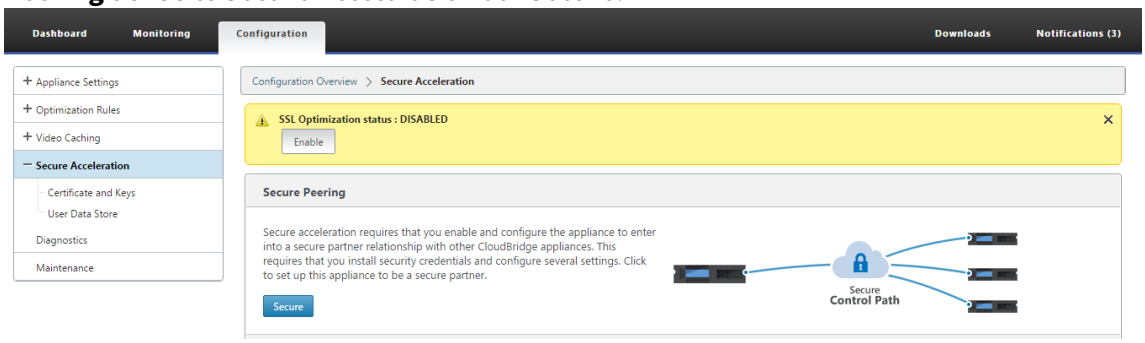
Auto Secure Peering an eine PE-Appliance von einer eigenständigen SD-WAN SE und WANOP Appliance am DC-Standort

October 28, 2021

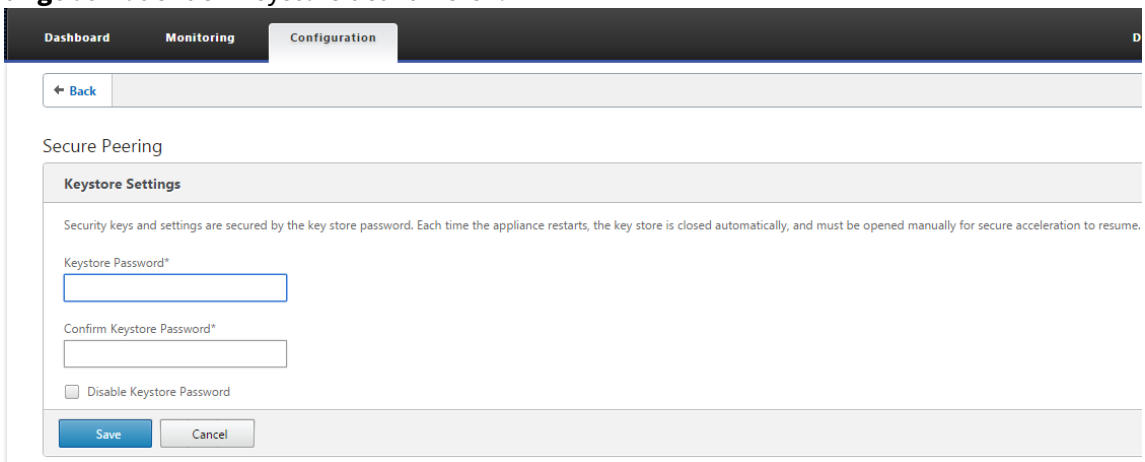
So führen Sie Auto Secure Peering auf einer PE-Appliance von einer eigenständigen SD-WAN SE- und WANOP-Appliance auf der DC-Seite aus durch:

- Das WANOP DC-Gerät befindet sich im LISTEN-ON-Modus (2312/Jeder nicht standardmäßige Port).
- Die Zweigstelle PE 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.

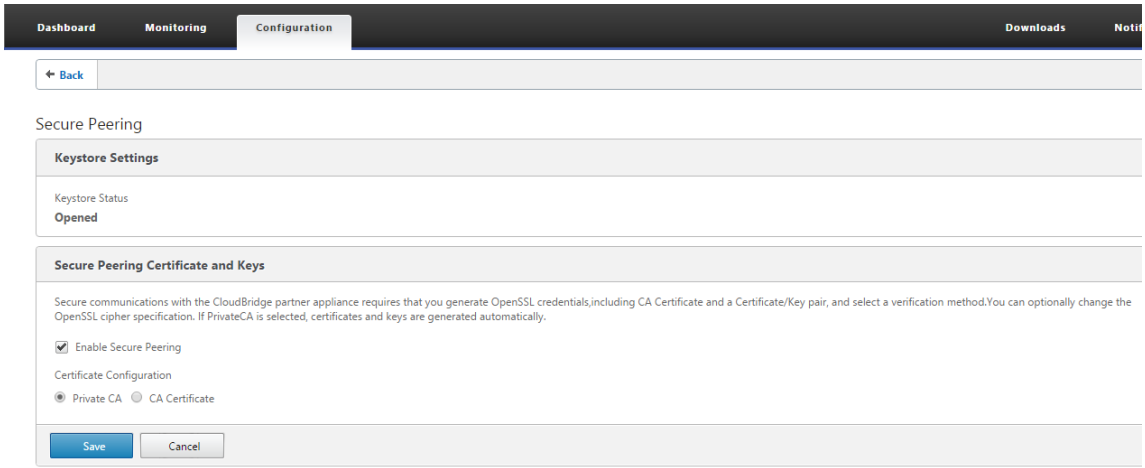
1. Klicken Sie auf einer eigenständigen WANOP-Appliance im Rechenzentrum im Bereich **Secure Peering** der Seite **Secure Acceleration** auf **Secure**.



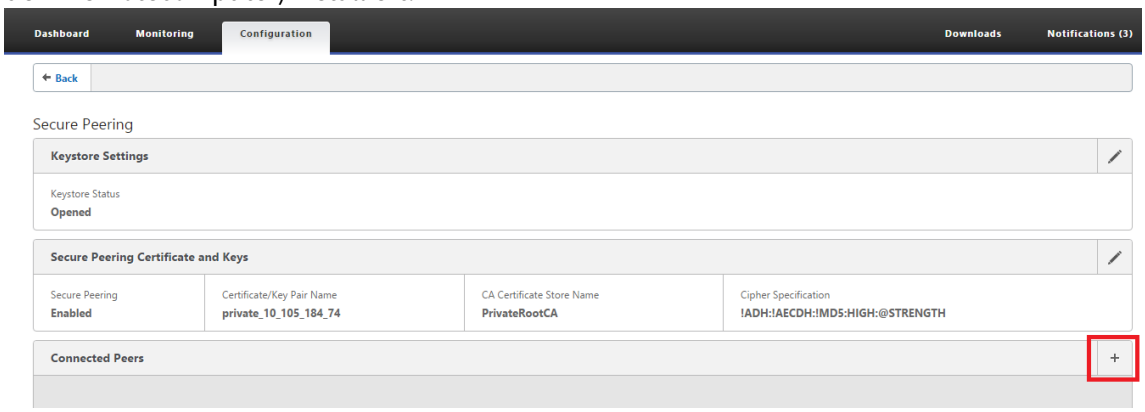
2. Konfigurieren Sie die Keystore-Einstellungen, indem Sie das **Schlüsselspeicherkennwort angeben** oder den Keystore deaktivieren.



3. **Aktivieren Sie Secure Peering**, indem Sie **Private CA** auswählen, um AUTOMATISCHES SICHERES PEERING durchzuführen

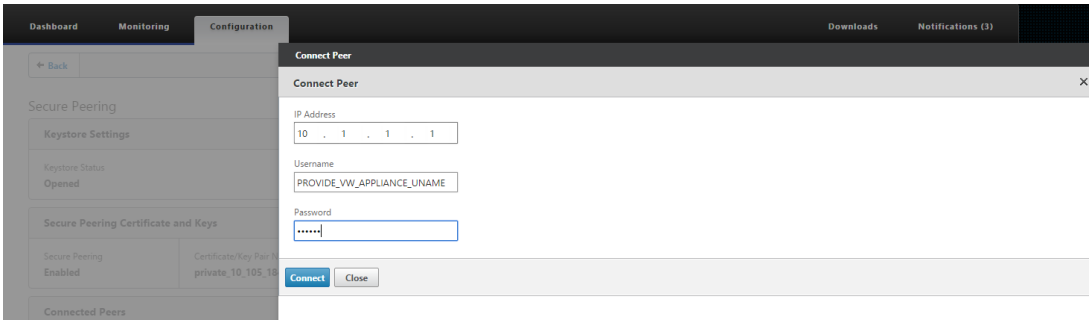


4. Das CA-Zertifikat auf Appliance-Ebene und das private Zertifikat und der Schlüssel werden auf dem lokalen WANOP generiert und eine Tabelle zum Hinzufügen eines sicheren REMOTE PEER TO Perform AUTO Peering with wird angezeigt.
5. Klicken Sie auf das Symbol “**+**”und ein Popup-Fenster zum Hinzufügen einer IP-Adresse mit Benutzernamen und Kennwort wird angezeigt. Nach erfolgreicher Authentifizierung mit der Remote-IP mit bereitgestellten Anmeldeinformationen wird eine Anforderung an den Remote-Computer gesendet, der das CA-Zertifikat und das private Zertifikat und den Schlüssel lokal (auf dem Remotecomputer) installiert.

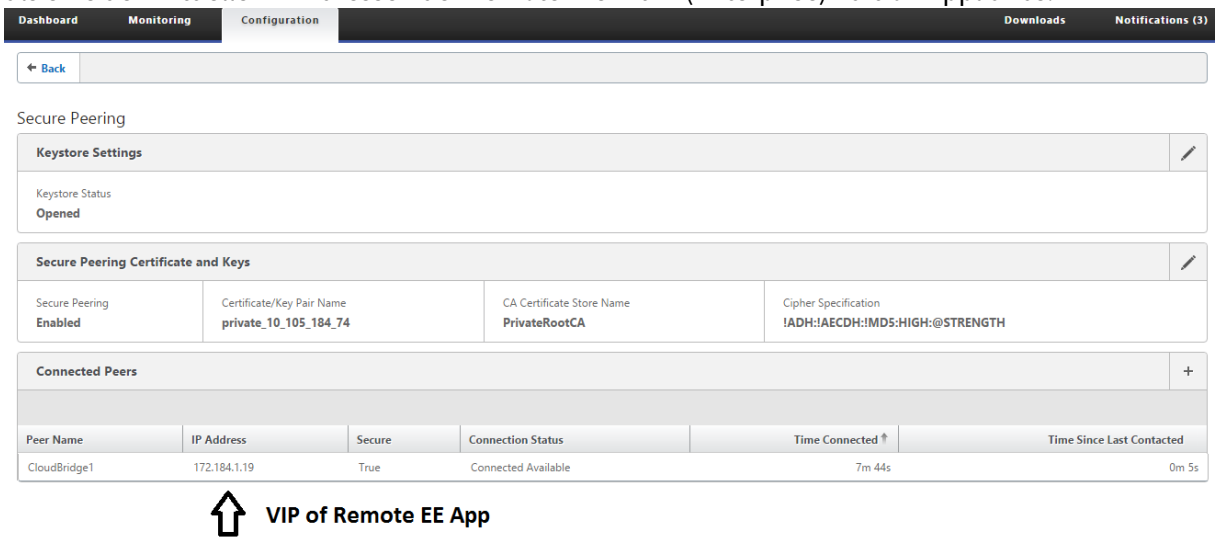


Hinweis

- IP-Adresse —IP-Adresse remote PREMIUM (ENTERPRISE) EDITION APPLIANCE MANAGEMENT IP
- Benutzername —Benutzername remote PREMIUM (ENTERPRISE) EDITION APPLIANCE
- Kennwort —Kennwort von PREMIUM (ENTERPRISE) EDITION APPLIANCE



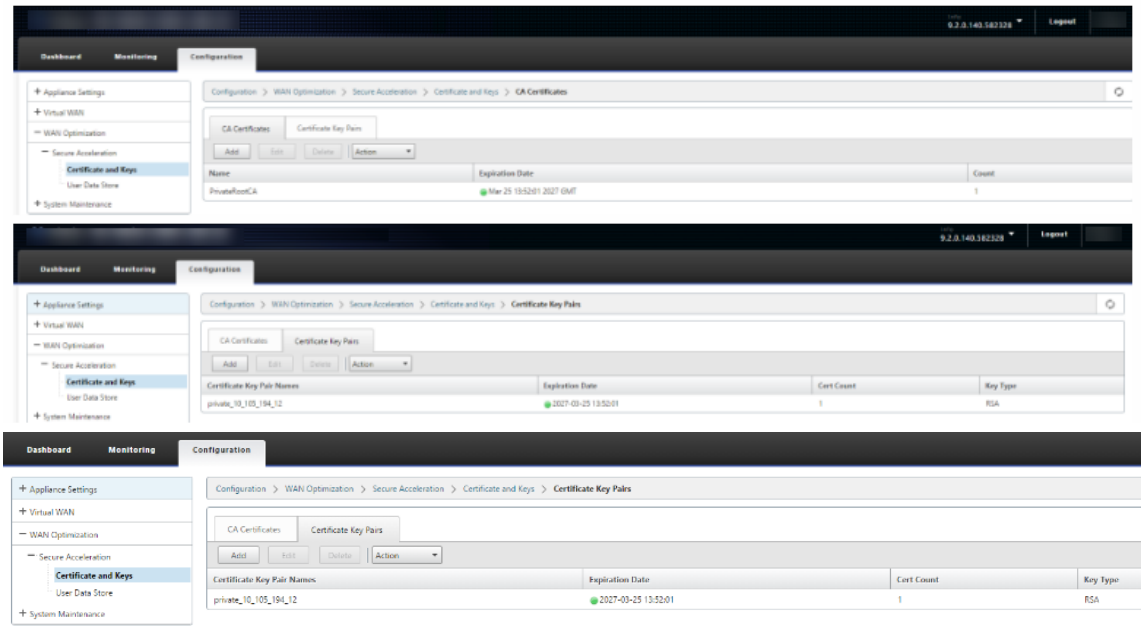
Nach erfolgreicher Authentifizierung sehen Sie Secure Peering als TRUE und die Partner-IP-Adresse als eine der virtuellen IP-Adressen der Remote Premium (Enterprise) Edition Appliance.



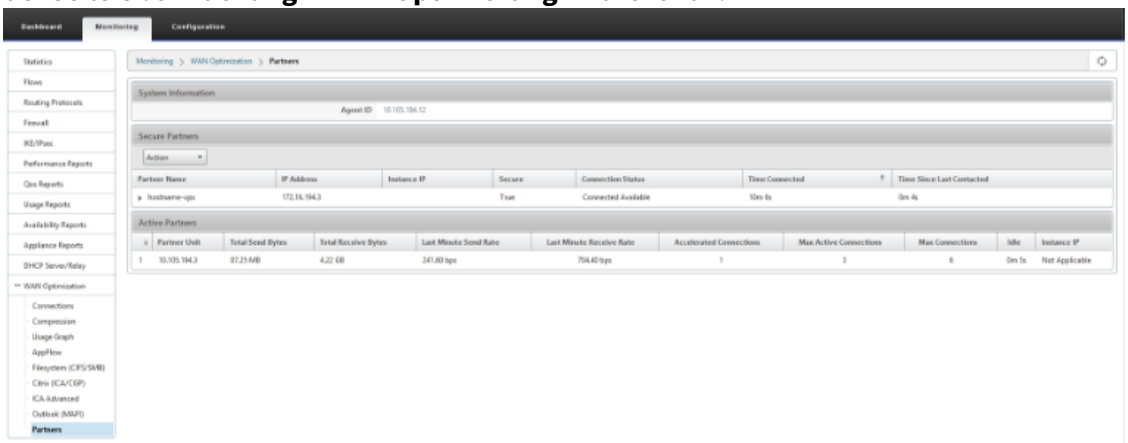
Überwachen

Sichere Partnerinformationen auf der Premium (Enterprise) Edition-Appliance unter **WANOPTIMIZATION** > **Partner** auf der Seite **Überwachung** anzeigen.

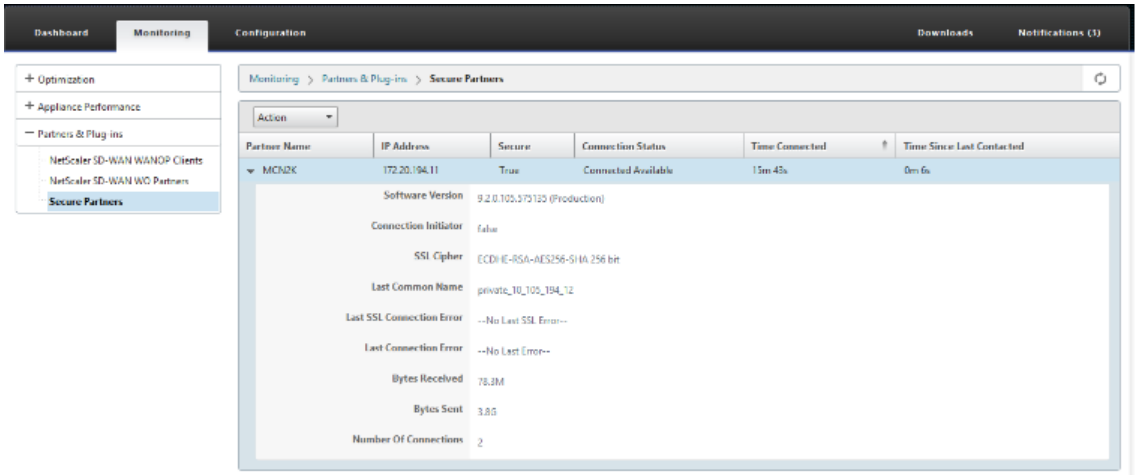
1. Data Store Encryption kann auf der Premium (Enterprise) Edition-Appliance durch Feature-Aktivierung vom MCN unter Optimierungs-Knoten für eine Premium (Enterprise) Edition-Appliance durchgeführt werden.
2. Bei einer Premium (Enterprise) Edition-Appliance ist Secure Peering immer aktiviert.
3. Um zu überprüfen, ob das Paar **Private CA** und **Private Certificate Key** erfolgreich generiert wurde, überprüfen Sie die folgenden Informationen:



4. Zeigen Sie **Secure Partner Information** auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung** > **WAN-Optimierung** > **Partner** an.

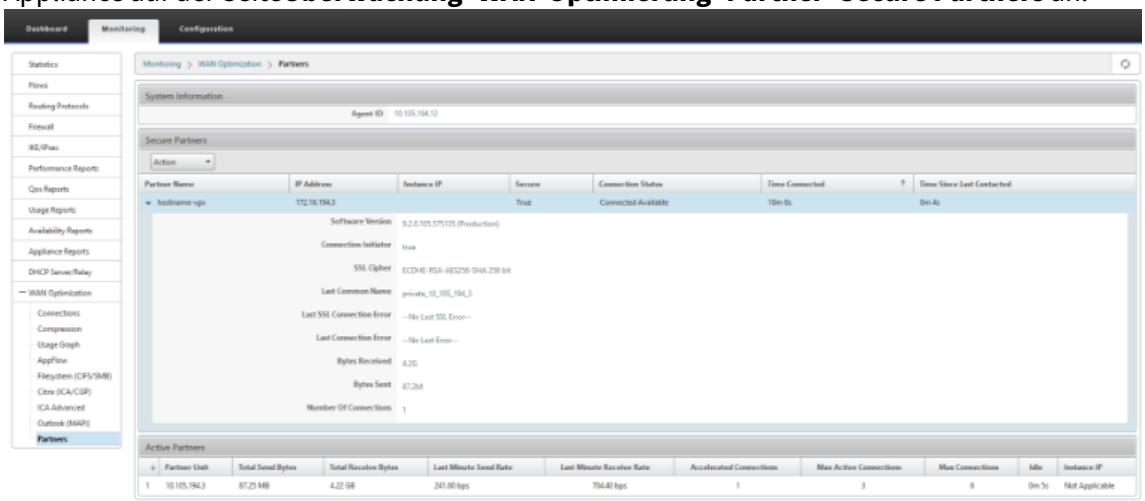


5. Auf der Partner-Appliance die **Secure Partnerinformationen der Premium (Enterprise) Edition-Appliance auf der Seite**Überwachung**>**Partner & Plug-ins**>**Secure Partner**anzeigen**.

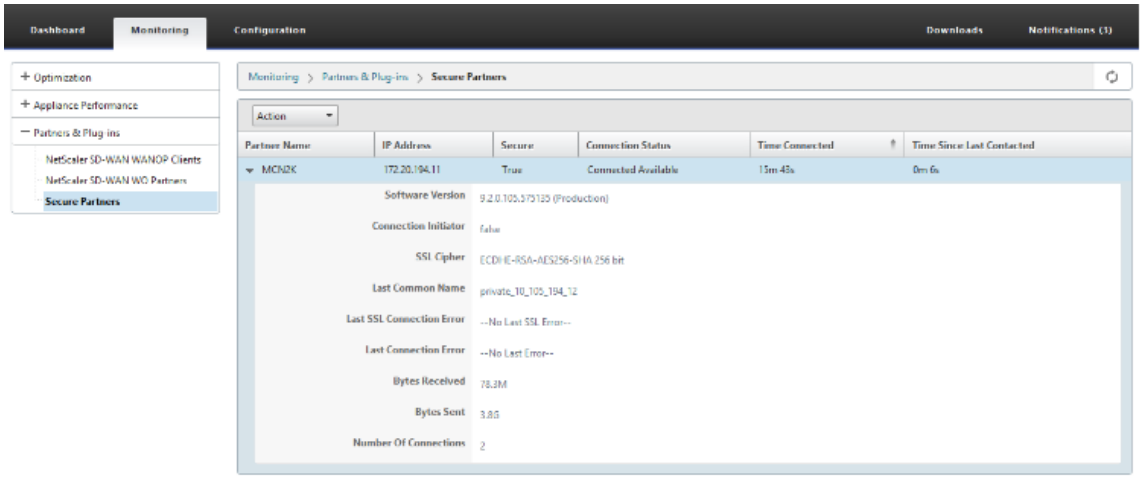


Problembehandlung

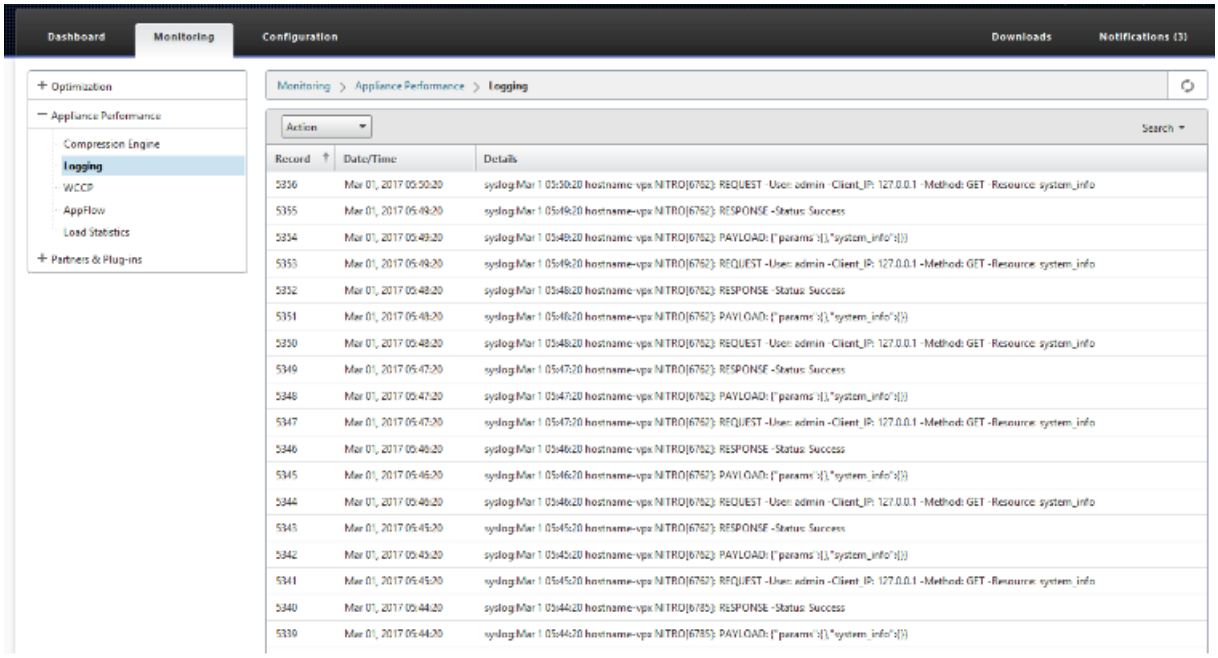
1. Zeigen Sie **Secure Partner Success/FailureInformation**auf der Premium (Enterprise) Edition-Appliance auf der Seite**Überwachung**>**WAN-Optimierung**>**Partner**>**Secure Partners** an.



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.



3. Zeigen Sie auf der Partner-Appliance Secure Partner Information auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung** > **Appliance-Performance** > **Logging** an.



Auto Secure Peering wurde von der PE-Appliance am DC-Standort und der PE-Appliance des Zweigstellenstandorts initiiert

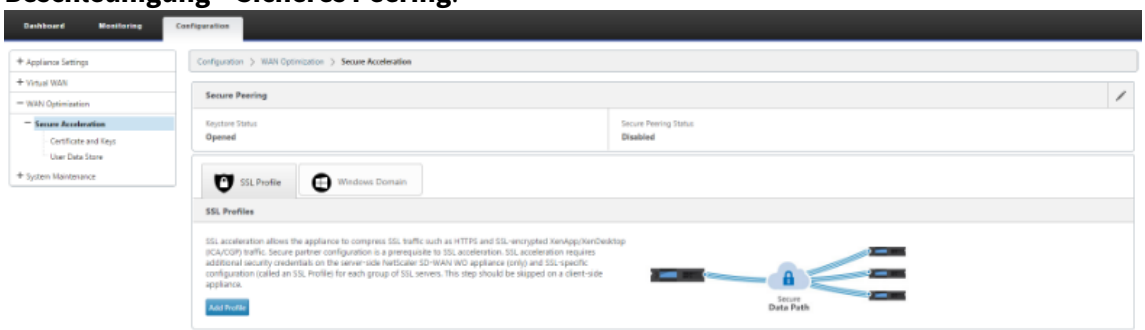
October 28, 2021

Konfiguration

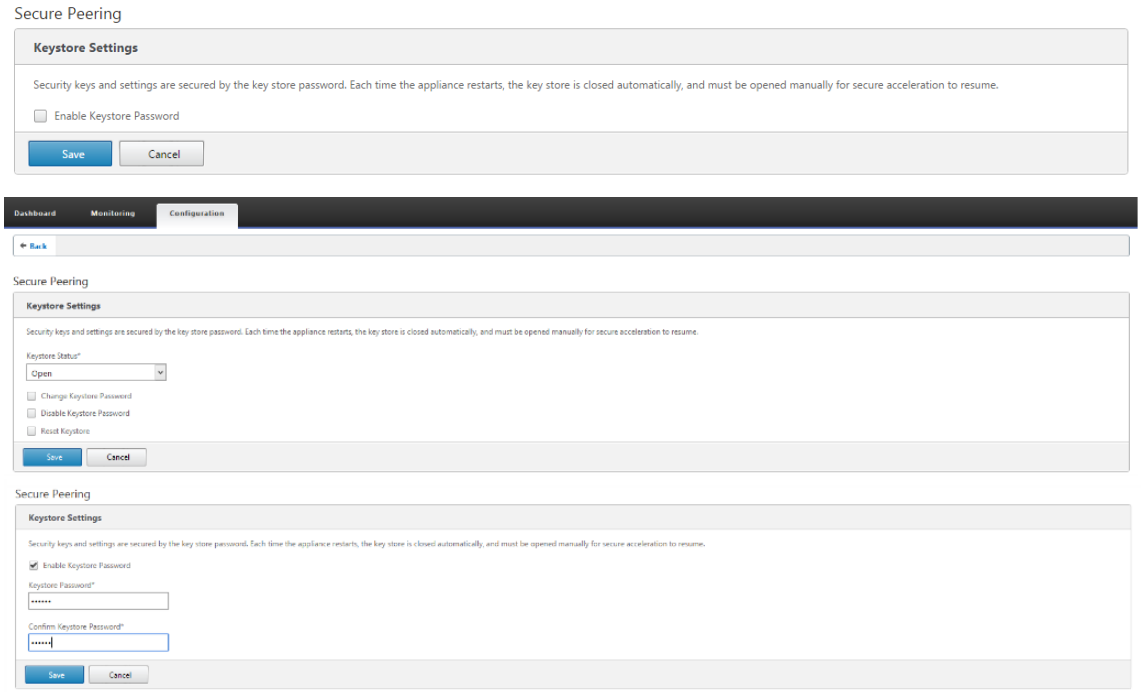
So konfigurieren Sie Auto Secure Peering auf einer neuen Premium (Enterprise) Edition-Appliance bei DC:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443). Die Zweigstelle PE 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-Zweige-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.

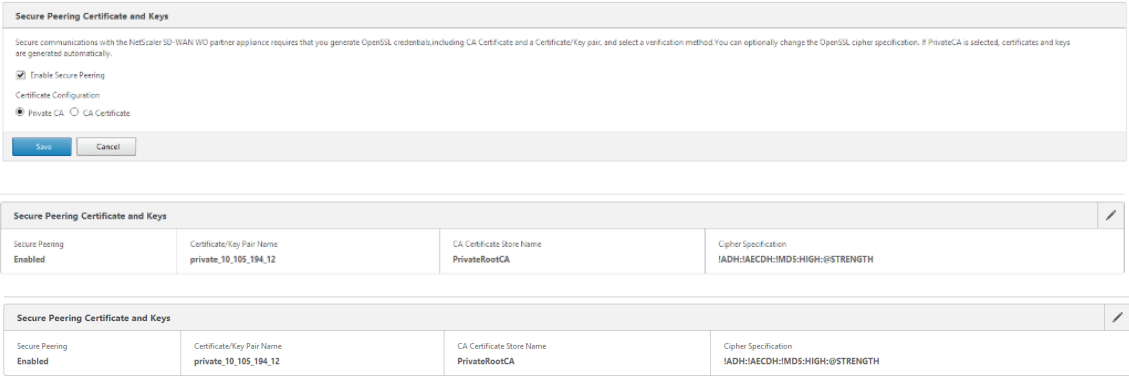
1. Navigieren Sie in der SD-WAN-Web-GUI zu **Konfiguration** > **WAN-Optimierung** > **Sichere Beschleunigung** > **Sicheres Peering**.



2. Konfigurieren Sie den Keystore, indem Sie das Keystore-Kennwort angeben oder den Keystore deaktivieren.

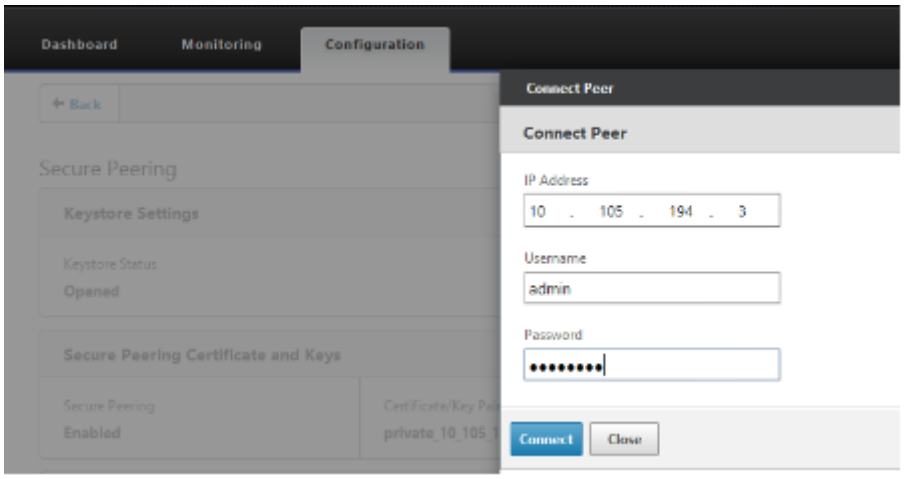


3. Aktivieren Sie **Secure Peering**, indem Sie **Private CA** auswählen, um AUTOMATIC SECURE PEERING durchzuführen.



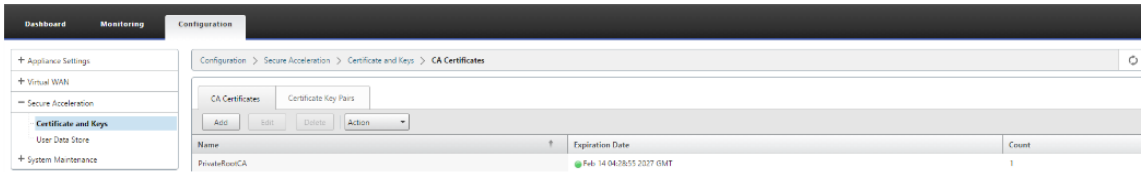
4. Klicken Sie auf das “+”-Symbol und fügen Sie IP mit Benutzername und Kennwort hinzu. Nach erfolgreicher Authentifizierung mit der angegebenen Remote-IP und den angegebenen Anmeldeinformationen wird eine Anforderung an den Remotecomputer gesendet, der das Zertifizierungsstellenzertifikat und den privaten Schlüssel für sich selbst lokal auf dem Remotecomputer installiert.

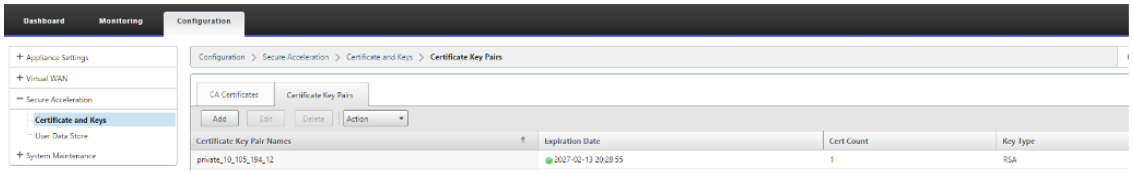
> **Hinweis**
>
> IP-Adresse —IP-Adresse der Remote-EE-Appliance-VERWALTUNGS-IP
>
> Benutzername —Benutzername der Remote-EE-Appliance
>
> Kennwort —Kennwort der Remote-EE-Appliance



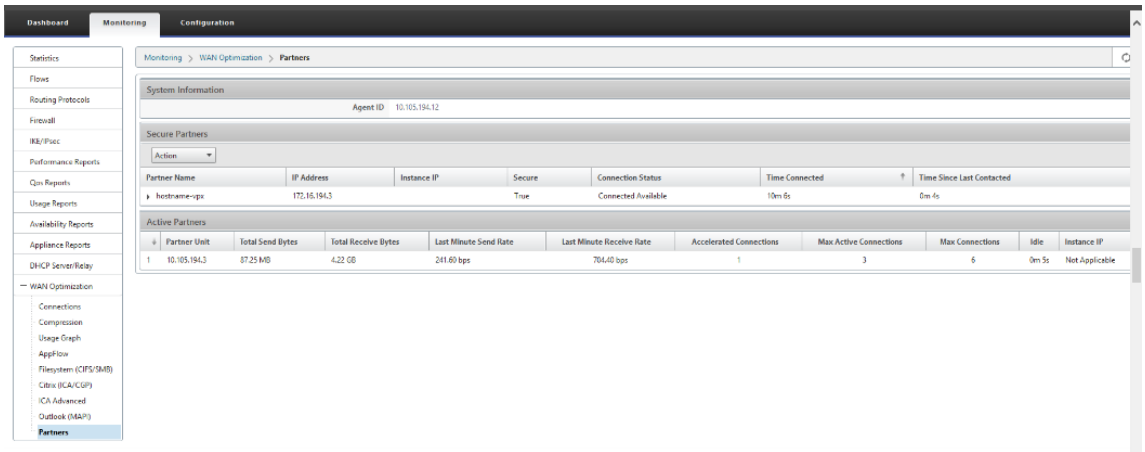
Überwachen

1. Um zu überprüfen, ob das Paar Private CA und Private Certificate Key erfolgreich generiert wurde, überprüfen Sie die unten angezeigten Informationen.

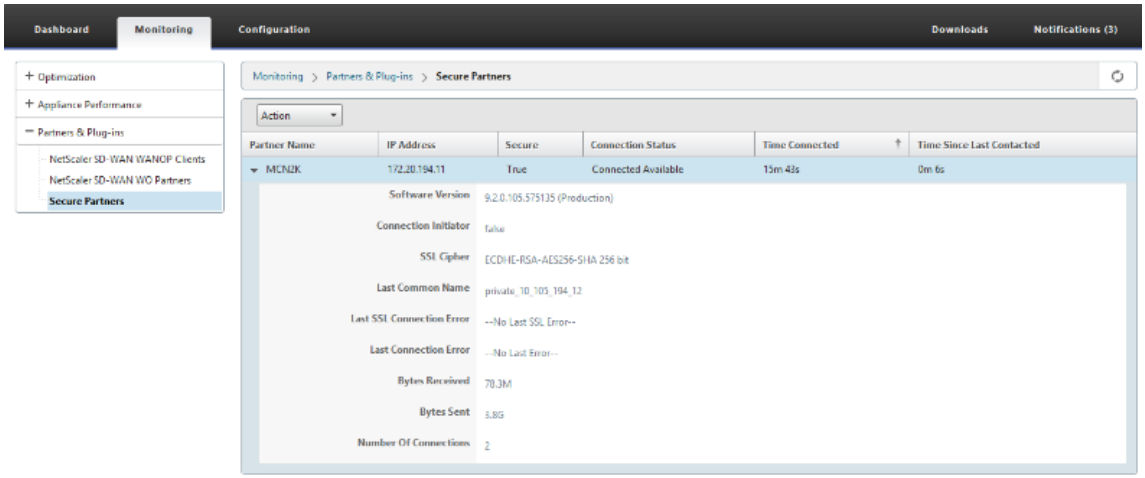




2. Zeigen Sie **Secure Partner Information** auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung** > **WAN-Optimierung** > **Partner** an.

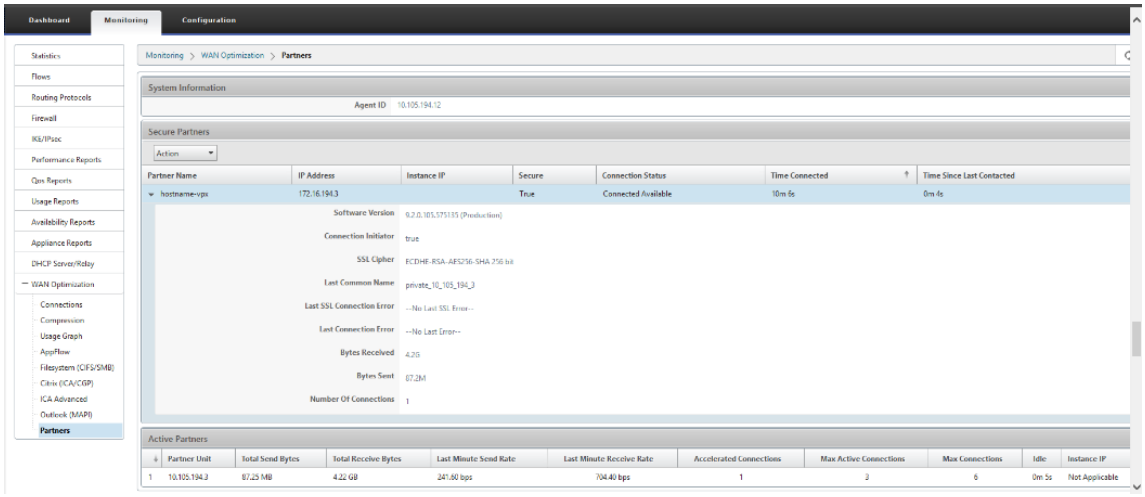


3. Zeigen Sie auf der Partner-Appliance Secure Partner Informationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Partner & Plug-ins** > **Sichere Partner** an.

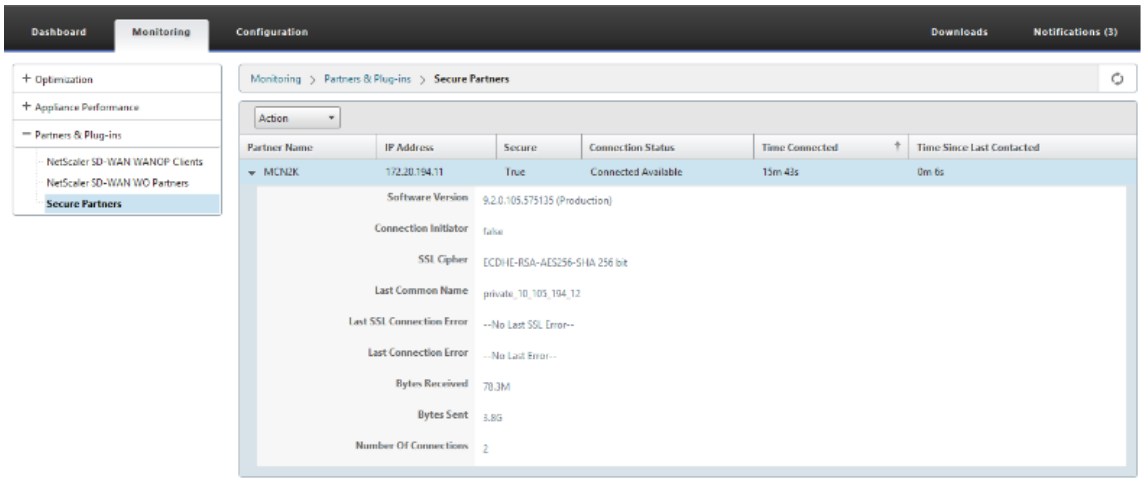


Problembehandlung

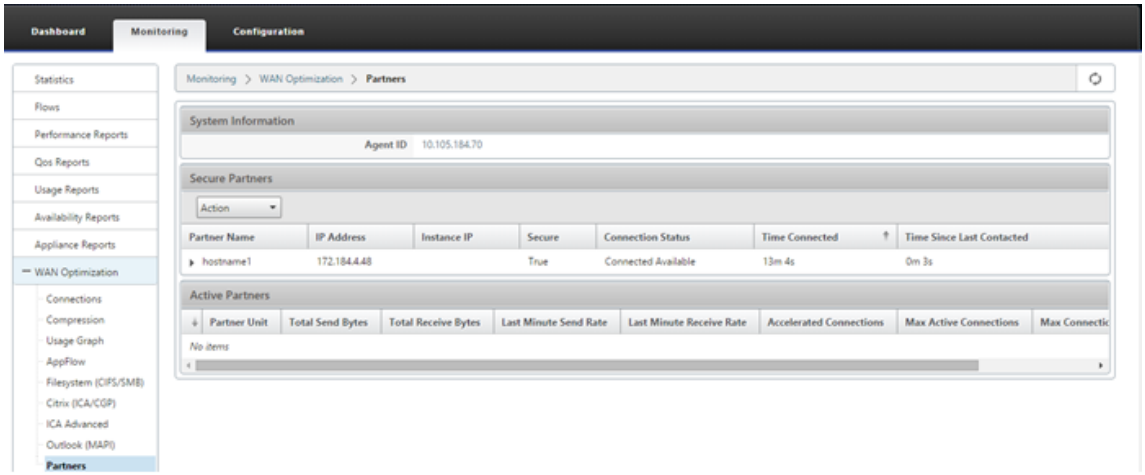
1. Sehen Sie sich die Erfolgs-/Fehlerinformationen für sichere Partner auf der Premium (Enterprise) Edition-Appliance auf der Seite **Überwachung** > **WAN-Optimierung** > **Partner** > **Secure Partners** an.

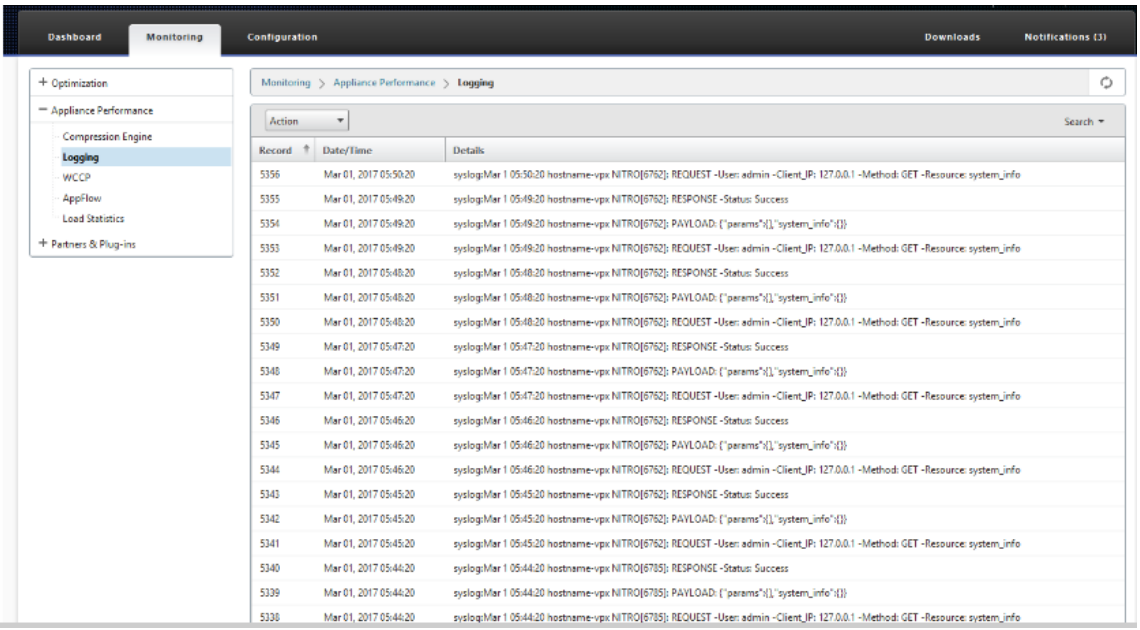


2. Zeigen Sie auf der Partner-Appliance Secure Partner Informationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Partner & Plug-ins** > **Sichere Partner** an.



3. Zeigen Sie auf der Partner-Appliance Secure Partner Informationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Appliance-Performance** > **Protokollierung** an.





Auto Secure Peering initiiert von PE-Appliance am DC-Standort und Zweigstelle mit eigenständiger SD-WAN SE und WANOP Appliance

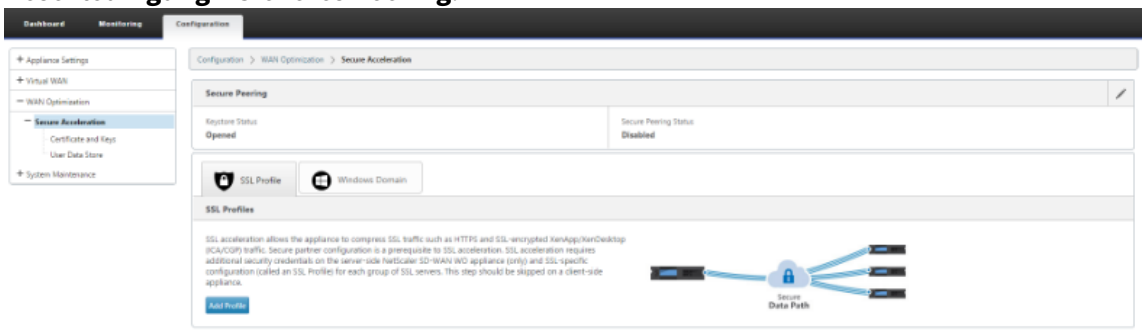
October 28, 2021

Konfiguration

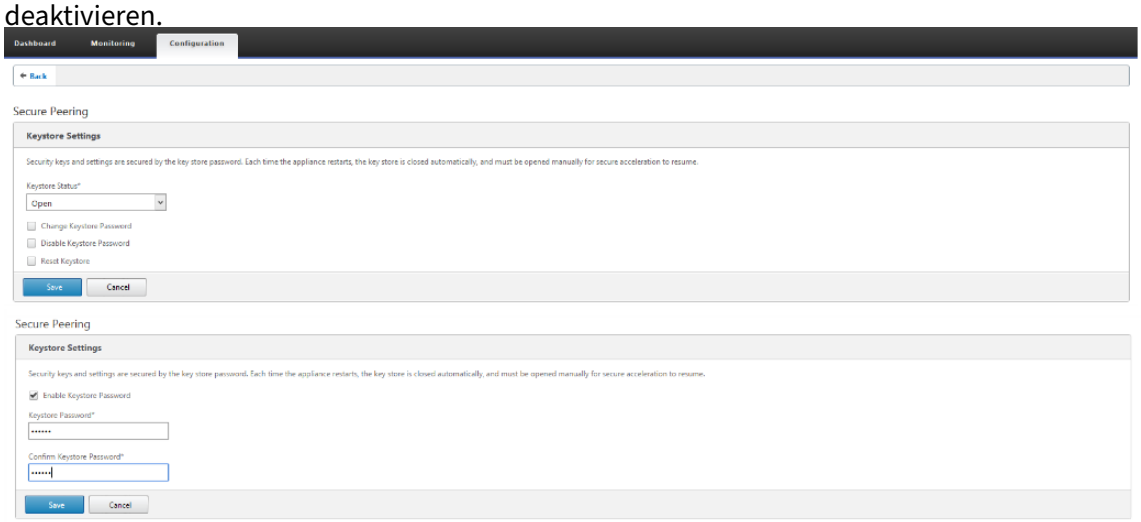
So konfigurieren Sie eine neue Premium (Enterprise) Edition-Appliance mit Auto Secure Peering am DC-Standort und Zweig mit eigenständiger SD-WAN- und WANOP-Appliance:

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443).
- Branch Standalone SD-WAN SE und WANOP befinden sich im CONNECT-TO-Modus.
- PE DC Appliance initiiert automatisches sicheres Peering auf Branch Standalone SD-WAN SE und WANOP Appliance, die die privaten CA Certs und CERT KEY Pairs installiert und CONNECT-TO auf der PE Appliance mit LISTEN-ON IP von DC EE konfiguriert.

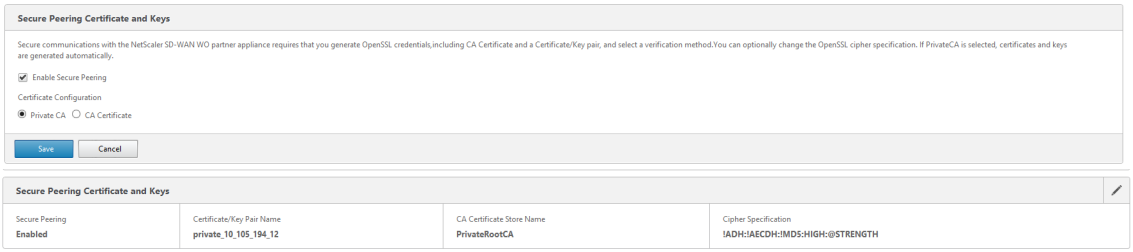
1. Navigieren Sie in der SD-WAN-Web-GUI zu **Konfiguration** > **WAN-Optimierung** > **Sichere Beschleunigung** > **Sicheres Peering**.



2. Konfigurieren Sie den Keystore, indem Sie das Keystore-Kennwort angeben oder den Keystore deaktivieren.



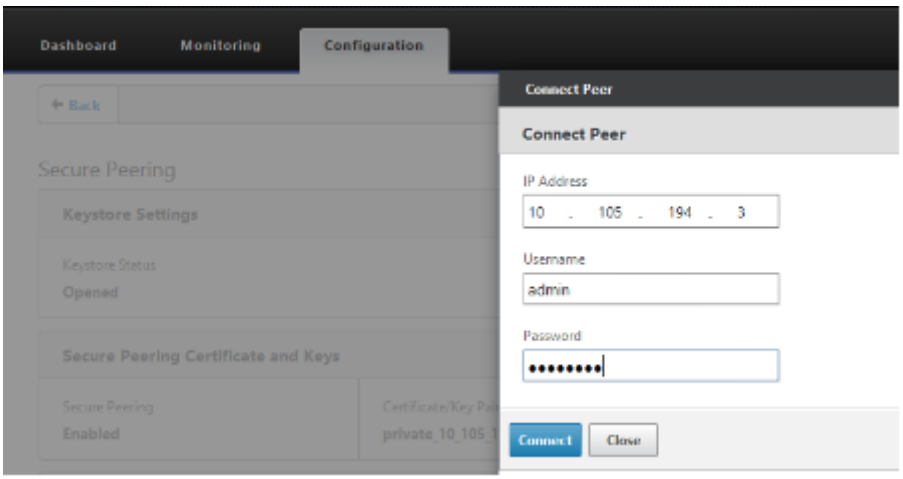
3. Aktivieren Sie **Secure Peering**, indem Sie **Private CA** auswählen, um AUTOMATIC SECURE PEERING durchzuführen.



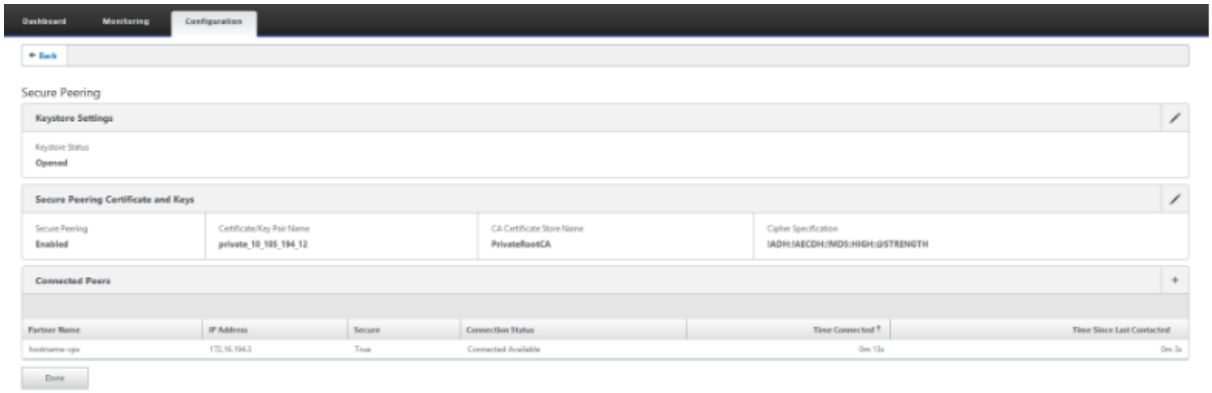
4. Klicken Sie auf das '+'-Symbol und fügen Sie IP mit Benutzernamen und Kennwort hinzu. Nach erfolgreicher Authentifizierung mit der angegebenen Remote-IP und den angegebe-

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.

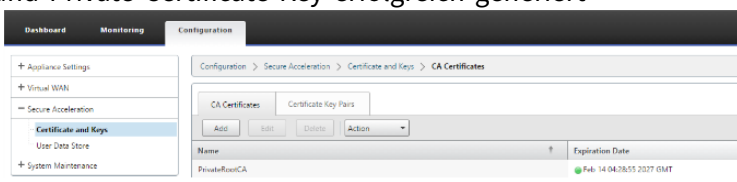


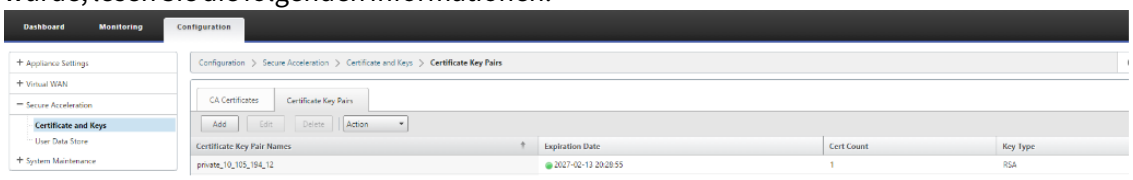
Nach erfolgreicher Authentifizierung können Sie Secure Peering als TRUE und die Partner-IP als eine der virtuellen IP der eigenständigen WANOP Remote-Appliance anzeigen.



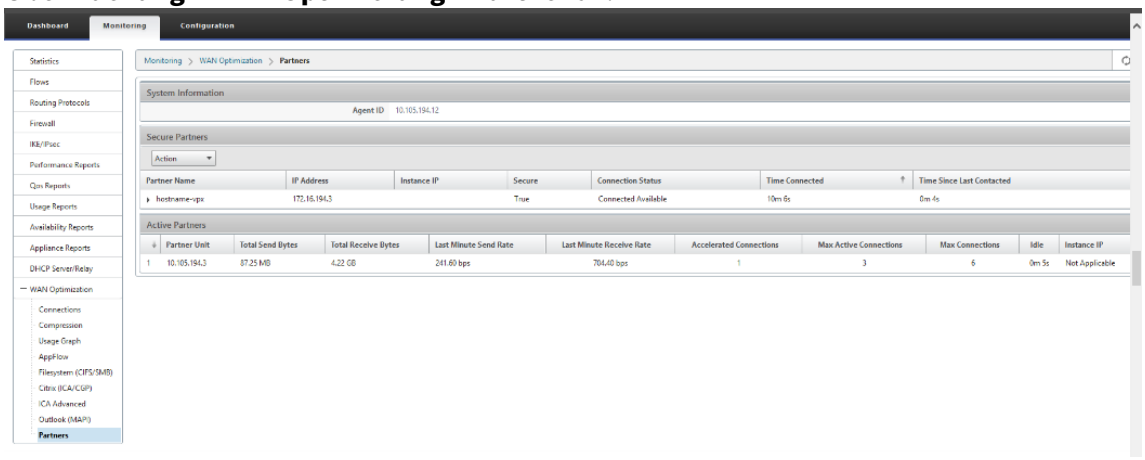
Überwachen

1. Um zu überprüfen, ob das Paar Private CA und Private Certificate Key erfolgreich generiert wurde, lesen Sie die folgenden Informationen.

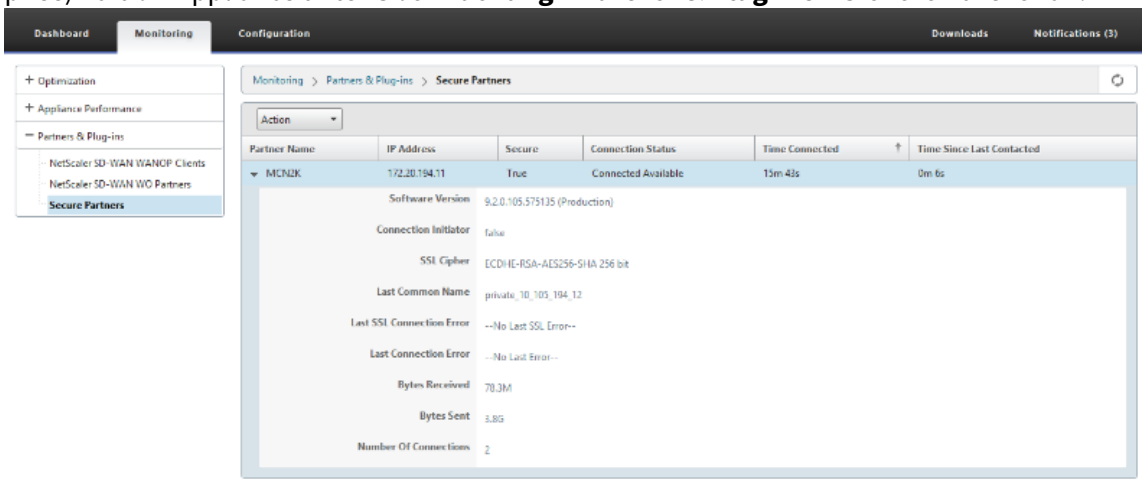




2. Zeigen Sie sichere Partnerinformationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **WAN-Optimierung** > **Partner** an.

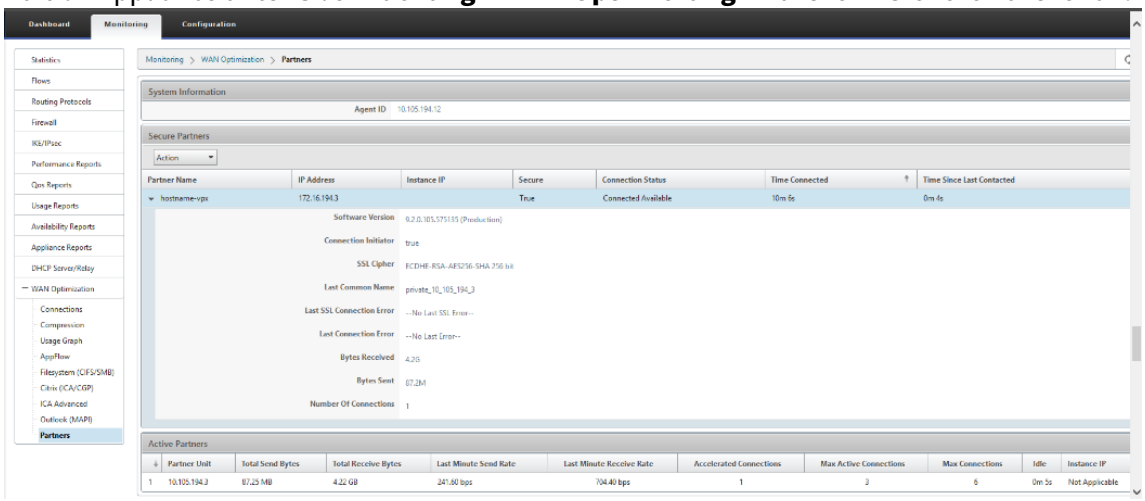


3. Zeigen Sie auf der Partner-Appliance Secure Partner Informationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Partner & Plug-ins** > **Sichere Partner** an.

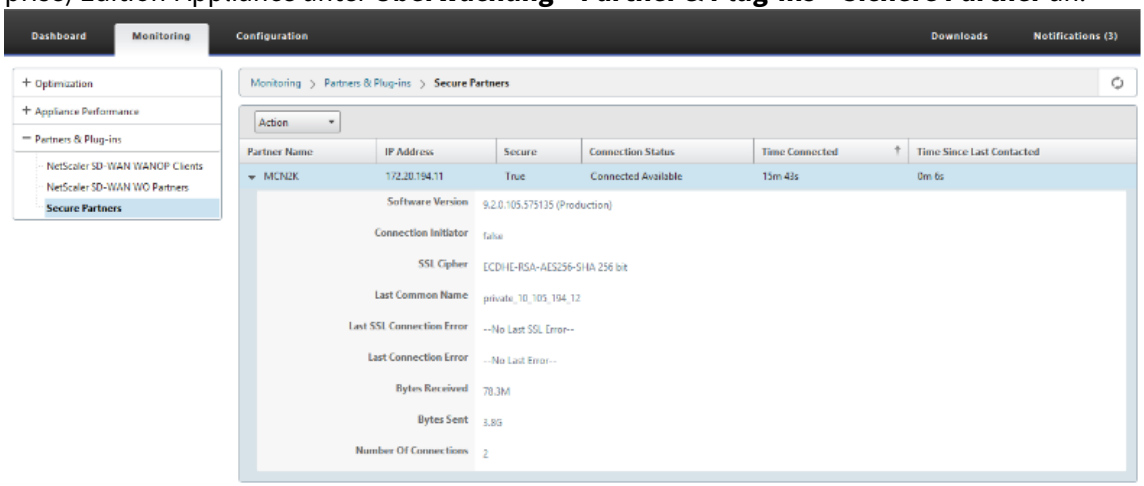


Problembehandlung

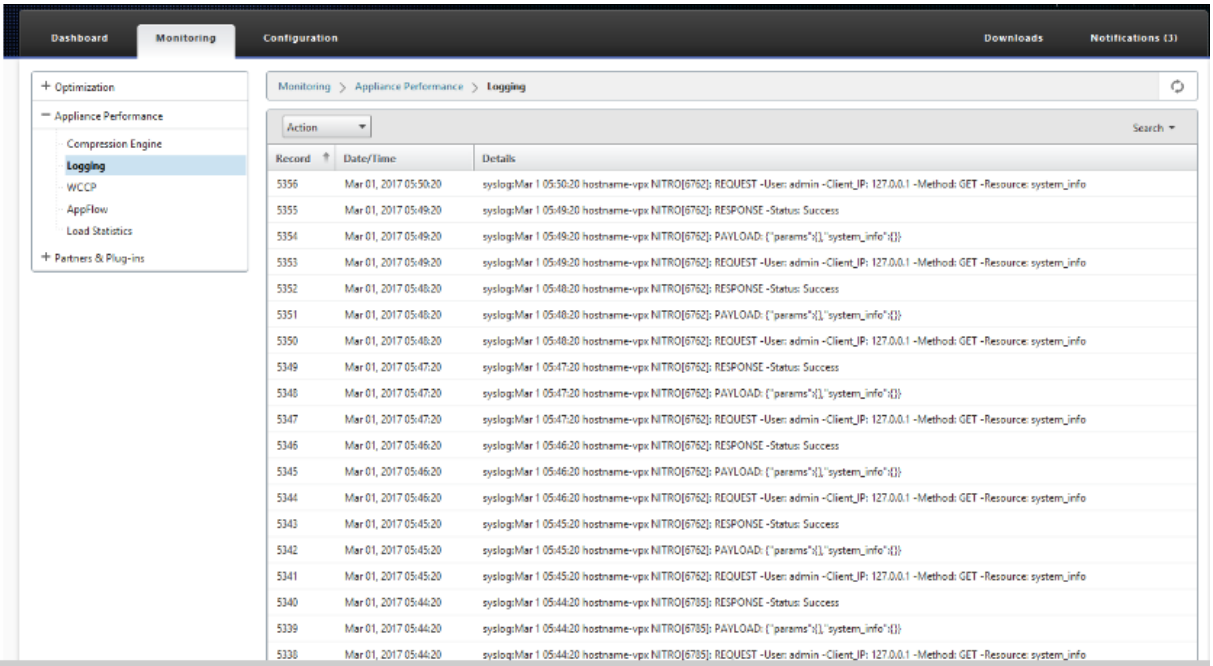
1. Zeigen Sie Secure Partner Erfolgs- und Fehlerinformationen auf der Premium (Enterprise) Edition Appliance unter **Überwachung** > **WAN-Optimierung** > **Partner** > **Sichere Partner** an.



2. Zeigen Sie auf der Partner-Appliance **Secure Partner Informationen** auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Partner & Plug-ins** > **Sichere Partner** an.



3. Zeigen Sie auf der Partner-Appliance **Secure Partner Informationen** auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Appliance-Performance** > **Protokollierung** an.



Manuelles Secure Peering von der PE-Appliance am DC-Standort und Branch PE-Appliance initiiert

October 28, 2021

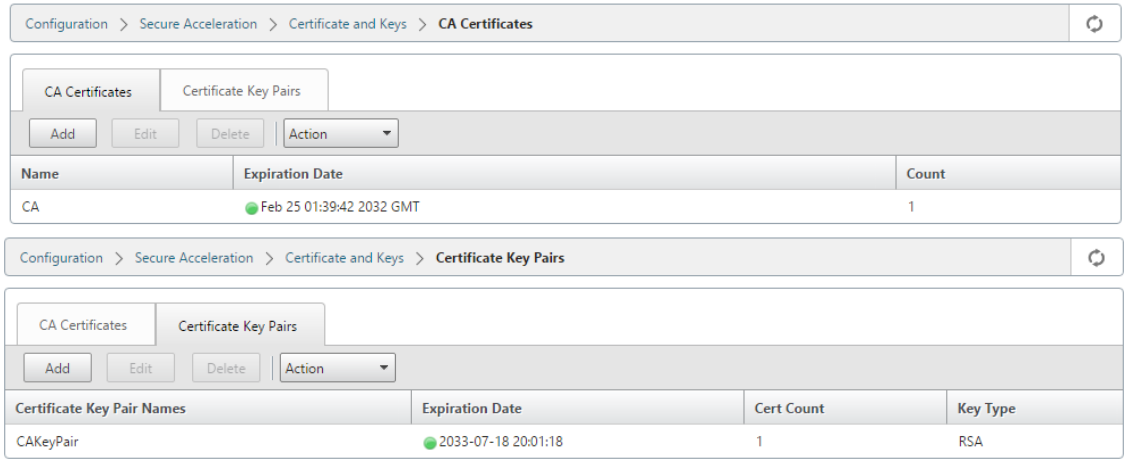
Diese Bereitstellung konfiguriert die DC-Standort-PE-Appliance im LISTEN-ON-Modus und die PE-Einheit des Zweigstandorts im CONNECT TO-Modus.

- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443).
- Die Zweigstelle 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.

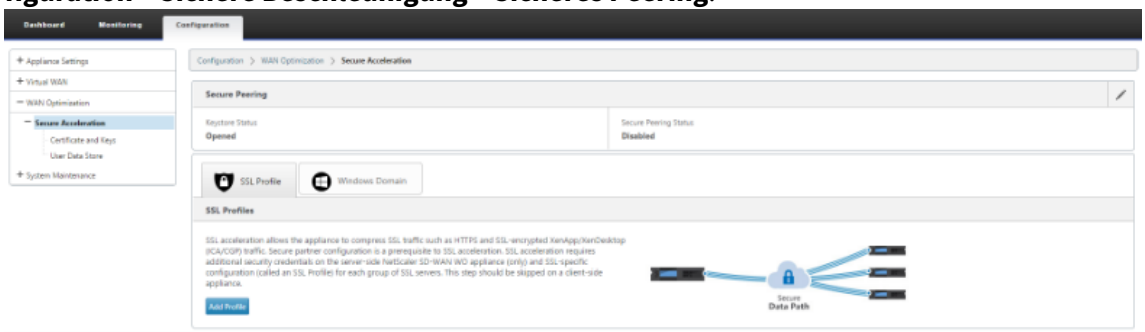
Konfiguration

So konfigurieren Sie automatisch Secure Peering, das von einer PE-Appliance am DC-Standort und einer PE-Appliance am Zweigstandort initiiert wurde:

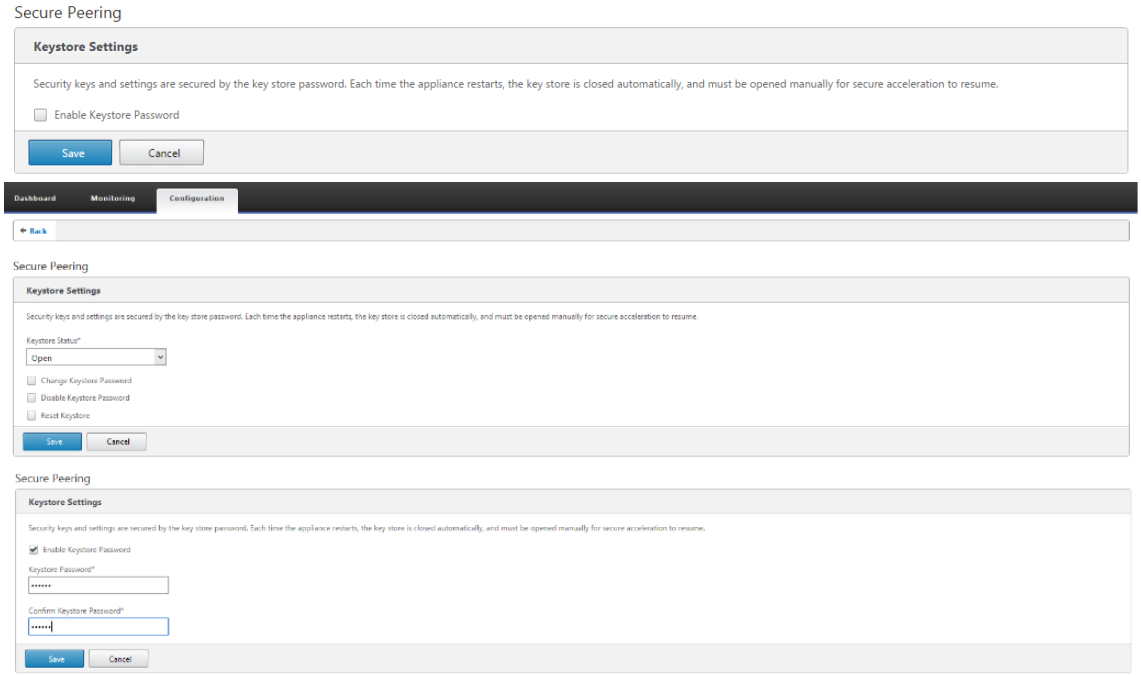
1. Laden Sie das **CA-Zertifikat** und das **CA-Schlüsselzertifikat** hoch, das Sie aus dem authentischen Zertifikat erhalten haben, und stellen Sie es wie unten gezeigt



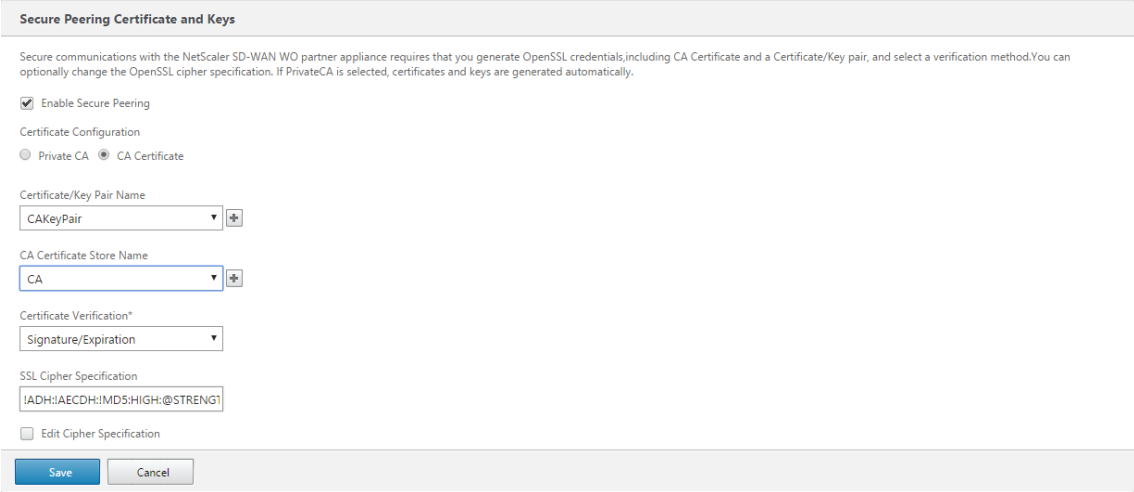
2. Wechseln Sie auf einer neuen PE-Appliance am DC-Standort in der SD-WAN-Web-GUI zu **Konfiguration** > **Sichere Beschleunigung** > **Sicheres Peering**.



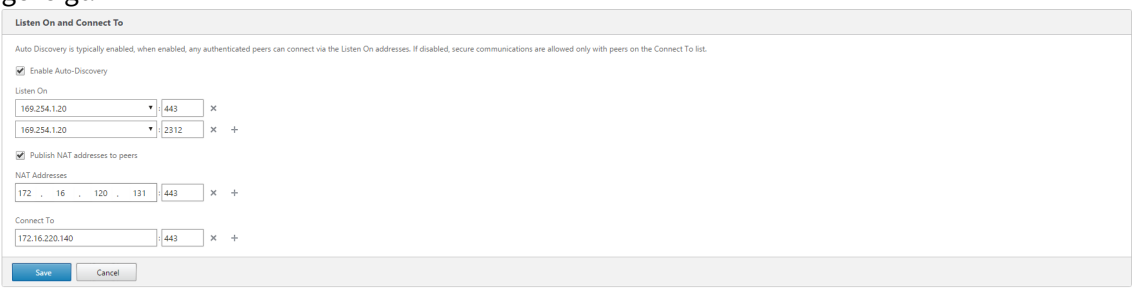
3. Konfigurieren Sie den Keystore, indem Sie das Keystore-Kennwort angeben oder den Keystore deaktivieren.



4. Aktivieren Sie sicheres Peering, indem Sie das Optionsfeld **CA-Zertifikat** auswählen und hochgeladene CA- und CA-Schlüsselpaar-Zertifikate entsprechend bereitstellen, wie unten gezeigt.

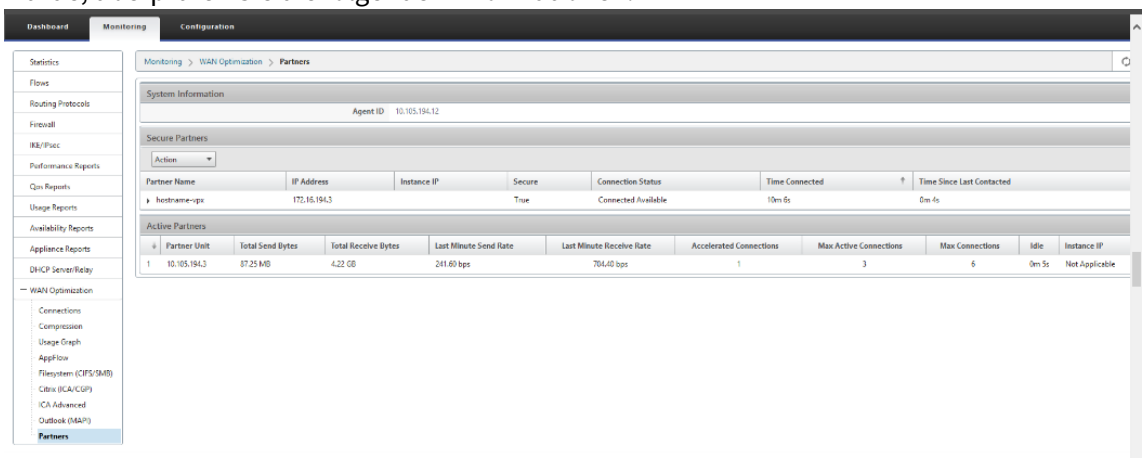


5. Stellen Sie die virtuelle IP der Remote-Maschine zusammen mit Port 443 bereit, wie unten gezeigt.

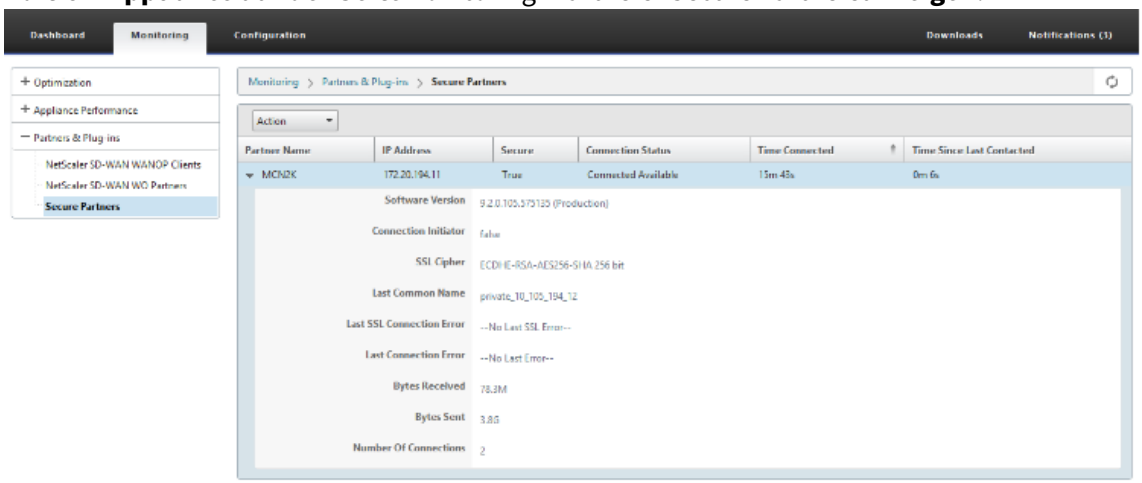


Überwachen

1. Um zu überprüfen, ob das Paar **Private CA** und **Private Certificate Key** erfolgreich generiert wurde, überprüfen Sie die folgenden Informationen.

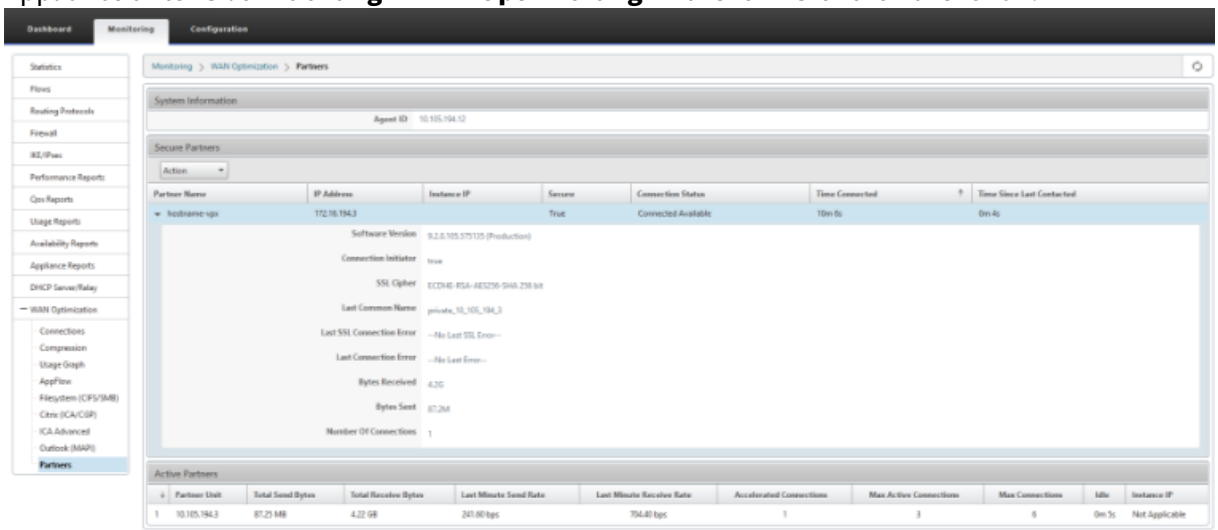


2. Auf der Partner-Appliance die **Secure Partnerinformationen auf der Premium (Enterprise) Edition-Appliance auf der Seite**Monitoring**>**Partners**>**Secure Partners**anzeigen**.



Problembehandlung

Zeigen Sie **Secure Partner Erfolgs- und Fehlerinformationen** auf der Premium (Enterprise) Edition Appliance unter **Überwachung** > **WAN-Optimierung** > **Partner** > **Sichere Partner** an.



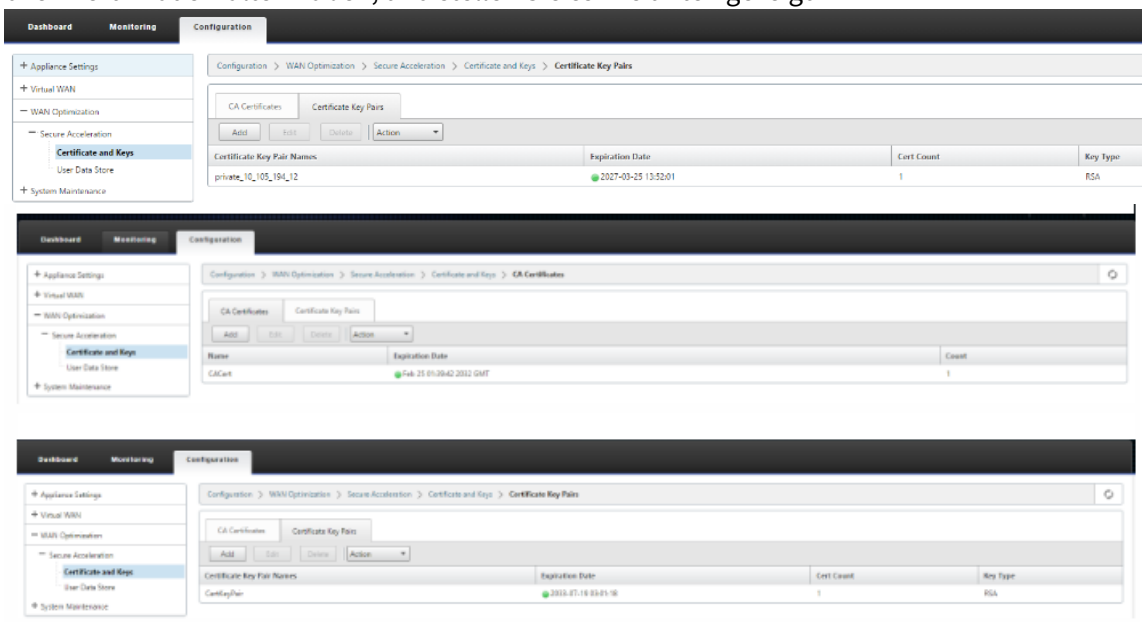
Manuelles Secure Peering von der PE-Appliance am DC-Standort in Zweigstelle Standalone SD-WAN SE und WANOP Appliance initiiert

October 28, 2021

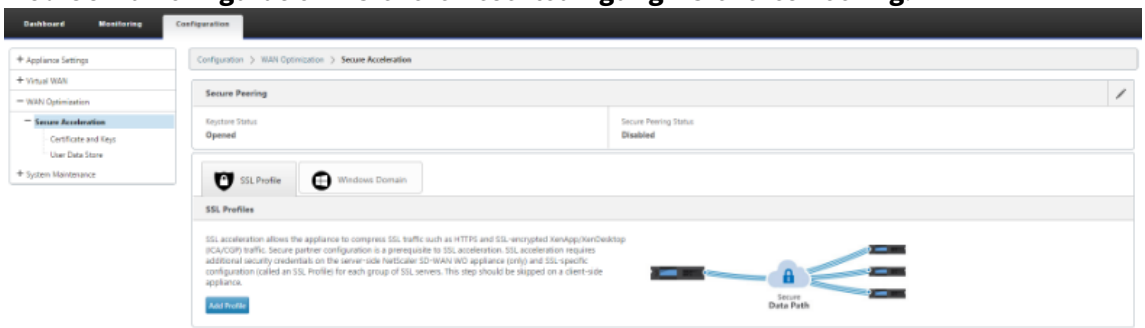
- Die PE-DC-Einheit befindet sich im LISTEN ON Modus (an Port 443).

- Die Zweigstelle 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.

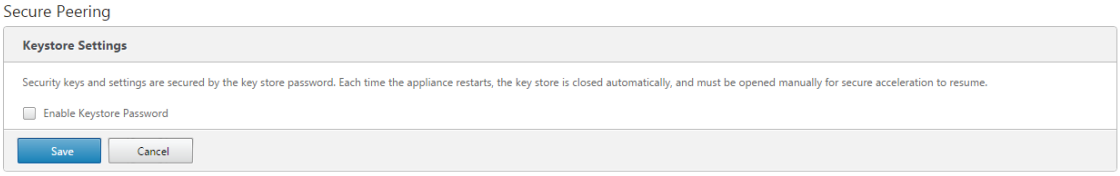
1. Laden Sie das **CA-Zertifikat** und das **CA-Schlüsselzertifikat** hoch, das Sie aus dem authentischen Zertifikat erhalten haben, und stellen Sie es wie unten gezeigt

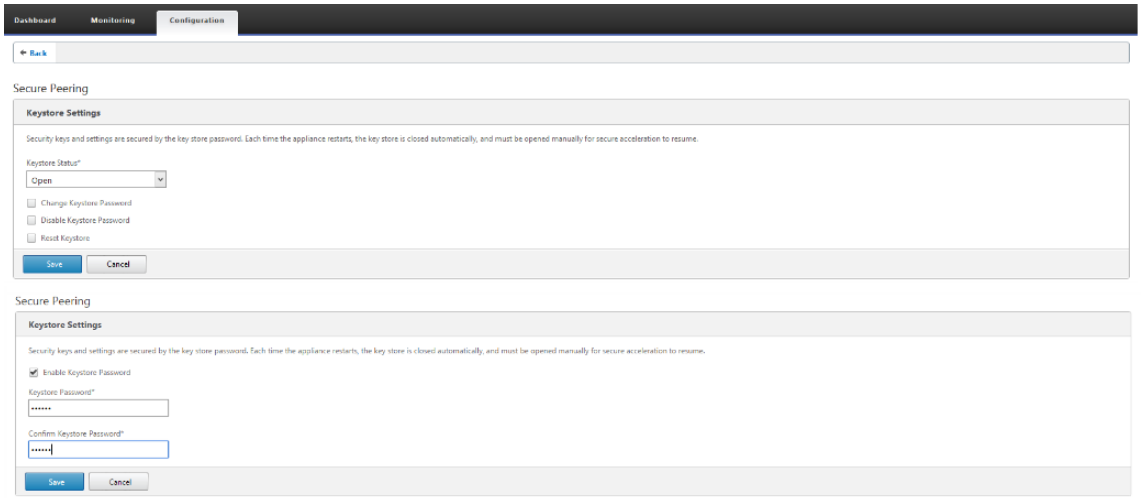


2. Wechseln Sie auf einer neuen PE-Appliance (Premium Edition) am DC-Standort in der SD-WAN-Web-GUI zu **Konfiguration** > **Sichere Beschleunigung** > **Sicheres Peering**.

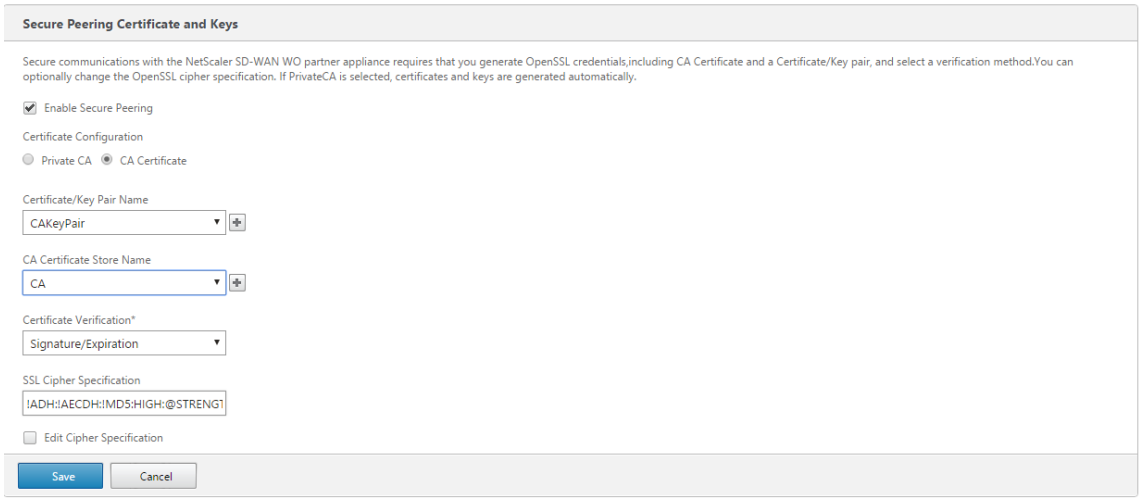


3. Aktivieren Sie den Keystore, indem Sie das **Schlüsselspeicherkennwort angeben** oder den Keystore deaktivieren.

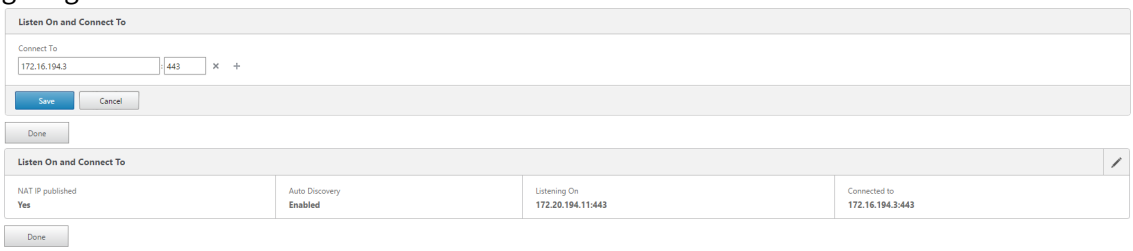




4. Aktivieren Sie sicheres Peering, indem Sie das Optionsfeld **CA-Zertifikat** auswählen und hochgeladene CA- und CA-Schlüsselpaar-Zertifikate entsprechend bereitstellen, wie unten gezeigt.

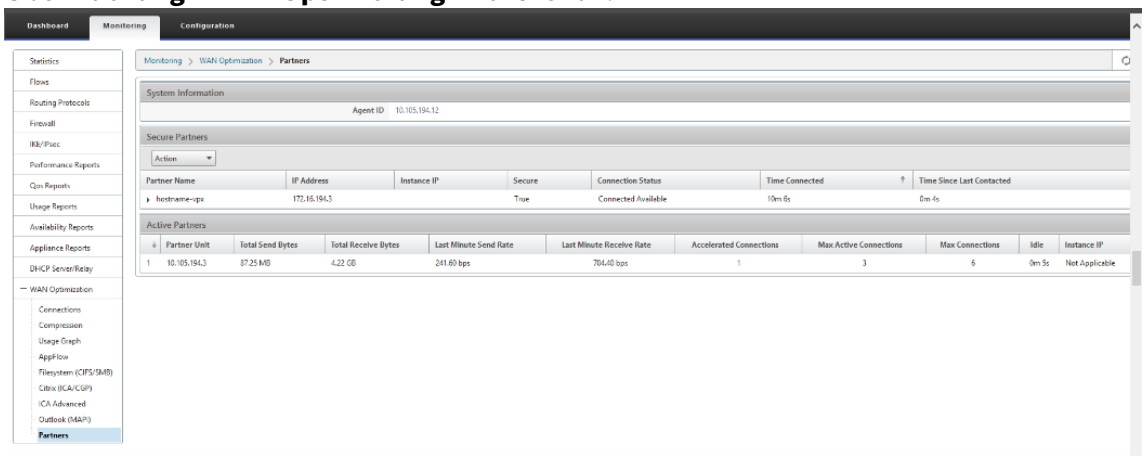


5. Stellen Sie die virtuelle IP der Remote-Maschine zusammen mit Port 443 bereit, wie unten gezeigt.

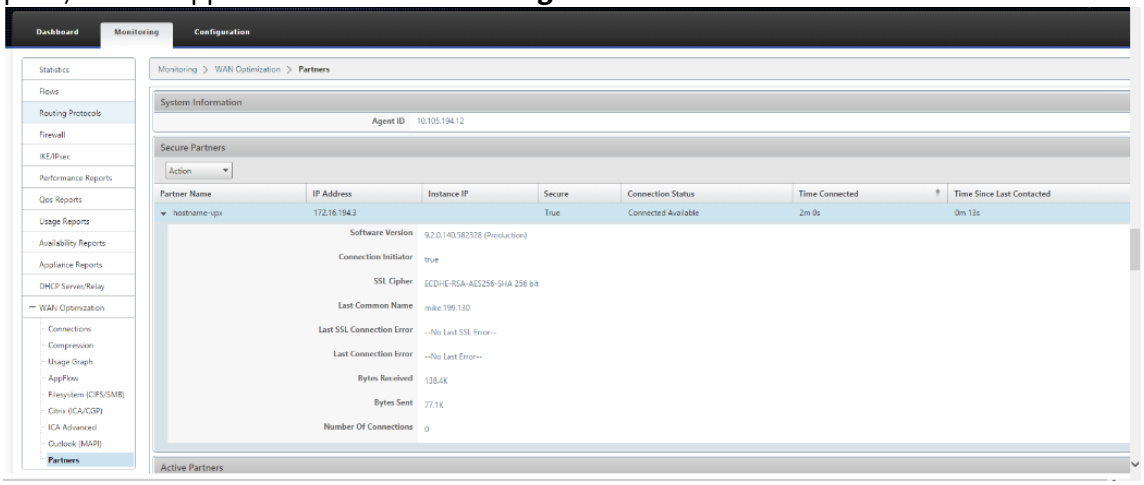


Überwachen

1. Zeigen Sie sichere Partnerinformationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **WAN-Optimierung** > **Partner** an.

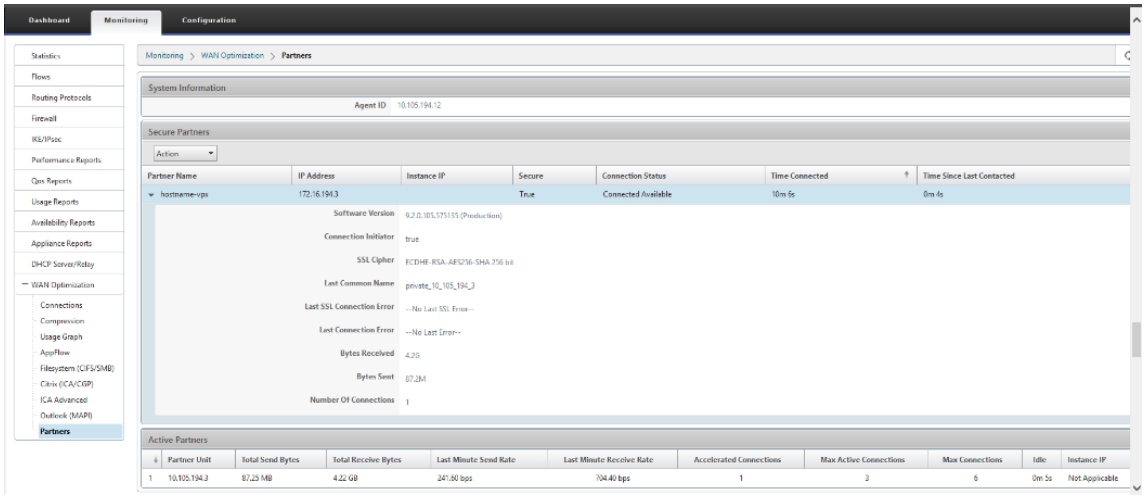


2. Zeigen Sie auf der Partner-Appliance Secure Partner Informationen auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Partner** > **Sichere Partner** an.

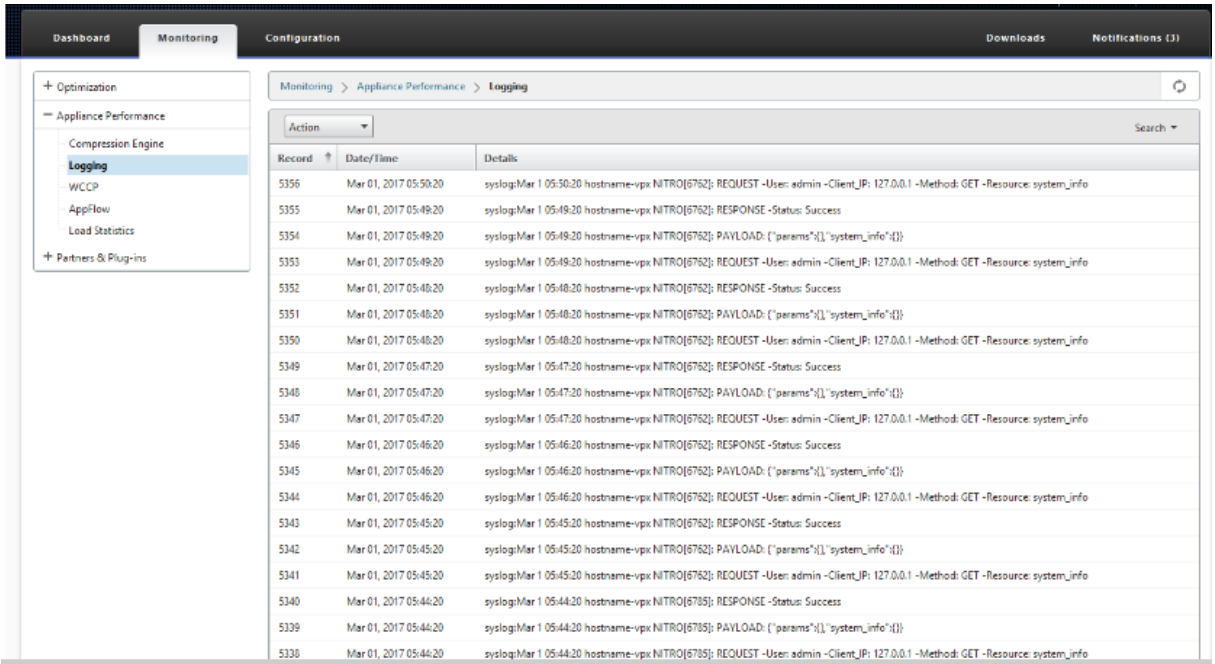


Problembehandlung

1. Zeigen Sie **Secure Partner Erfolgs** - und **Fehlerinformationen** auf der Premium (Enterprise) Edition Appliance unter **Überwachung** > **WAN-Optimierung** > **Partner** > **Sichere Partner** an.



2. Zeigen Sie auf der Partner-Appliance **Secure Partner Informationen** auf der Premium (Enterprise) Edition-Appliance unter **Überwachung** > **Appliance-Performance** > **Protokollierung** an.

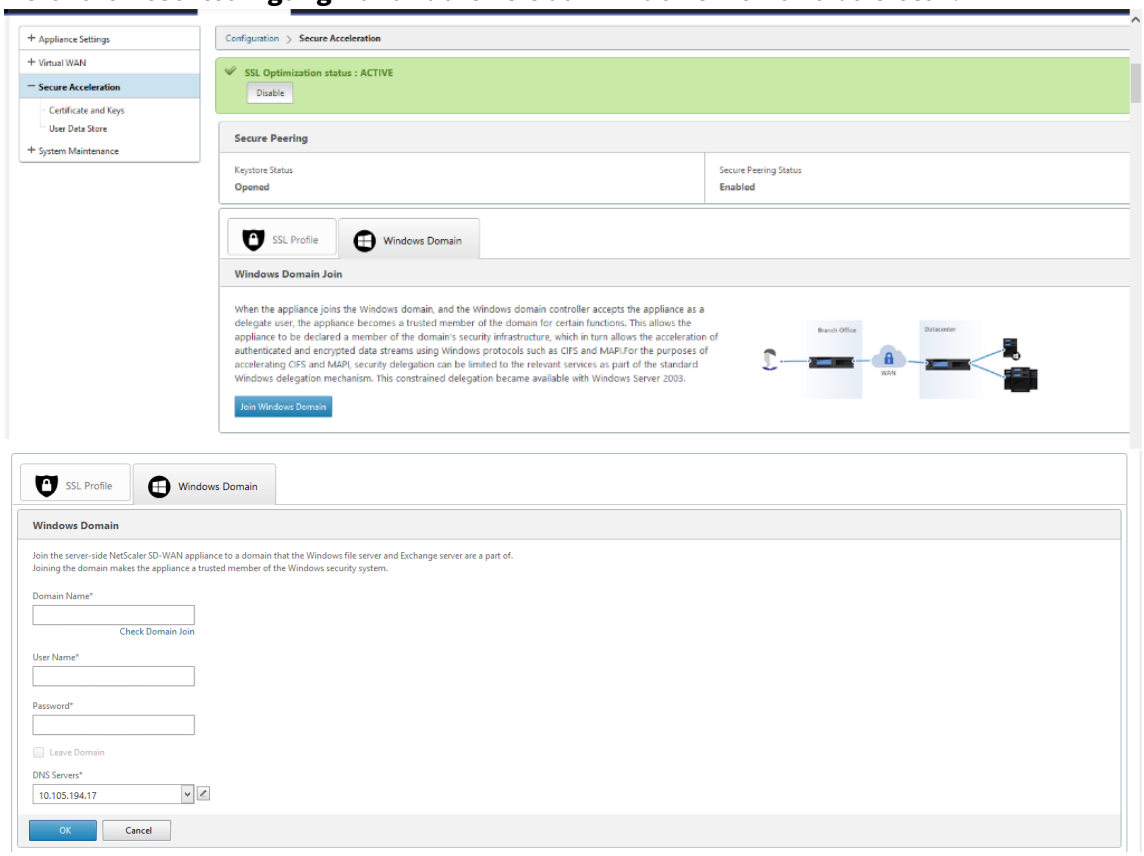


Domänenbeitritt und Delegieren der Benutzererstellung

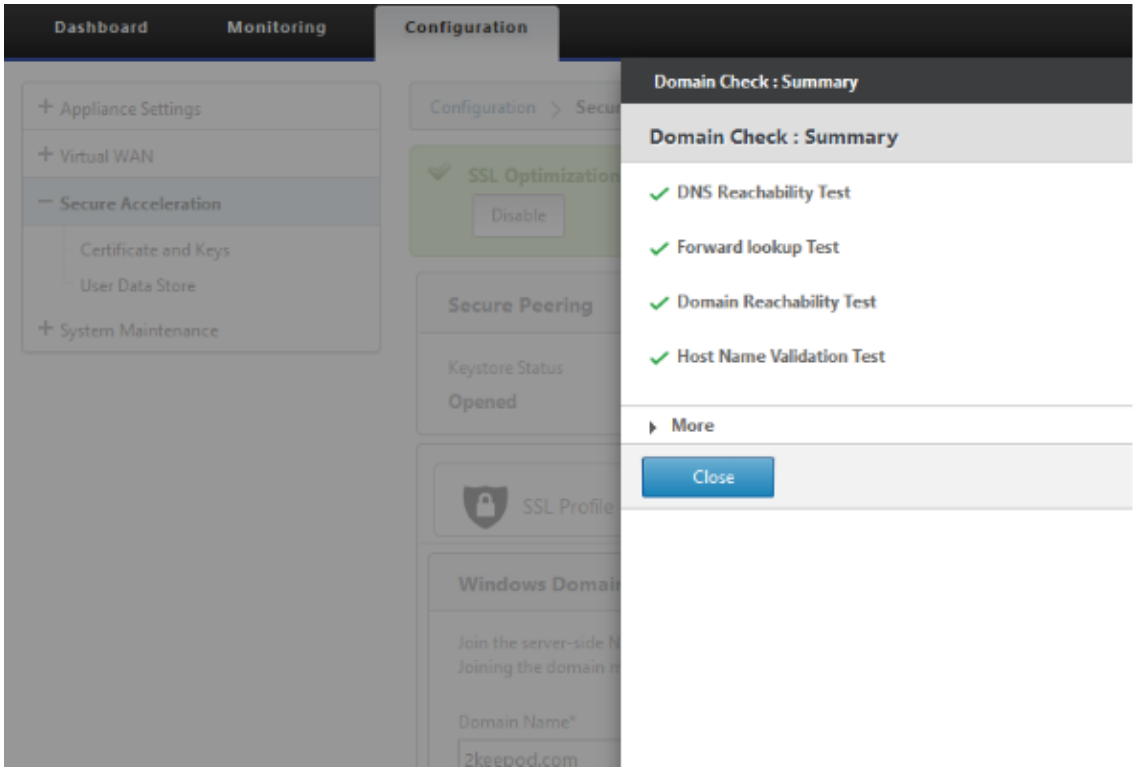
October 28, 2021

So konfigurieren Sie eine neue Premium (Enterprise) Edition (PE) -Appliance in der DC-zu-Windows-Domäne:

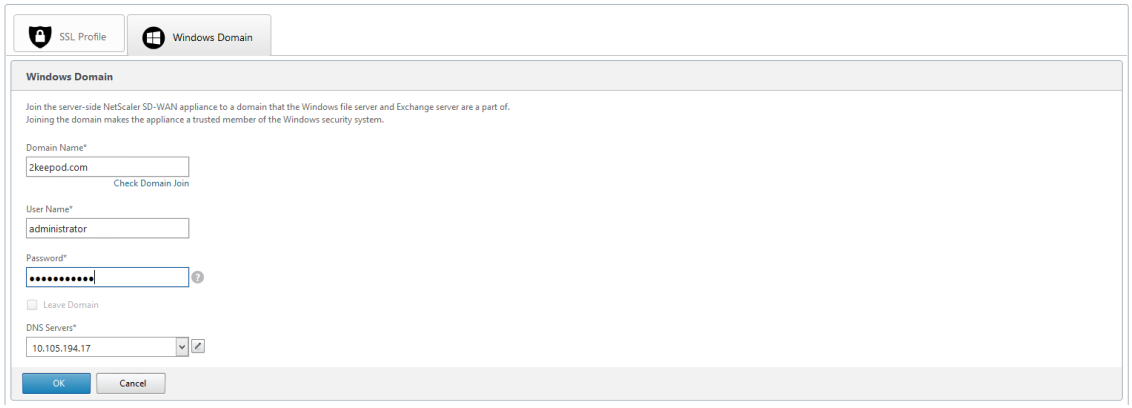
1. Wechseln Sie in der SD-WAN-Web-GUI zur Windows-Domäne, navigieren Sie zu **Konfiguration** > **Sichere Beschleunigung** > und klicken Sie auf **Windows-Domäne beitreten**.

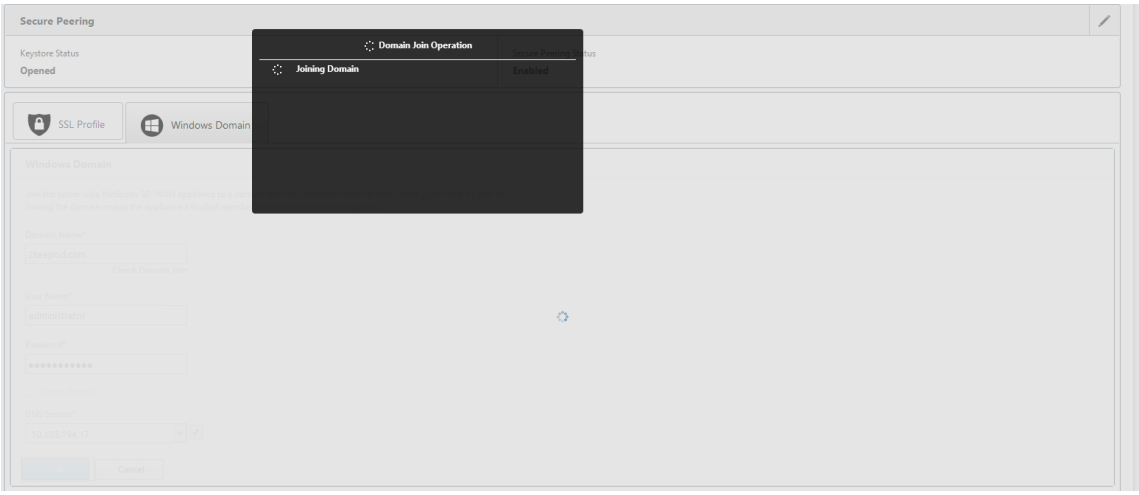


2. Geben Sie den **Windows-Domänennamen** an und führen **Sie** Vorabprüfungen für

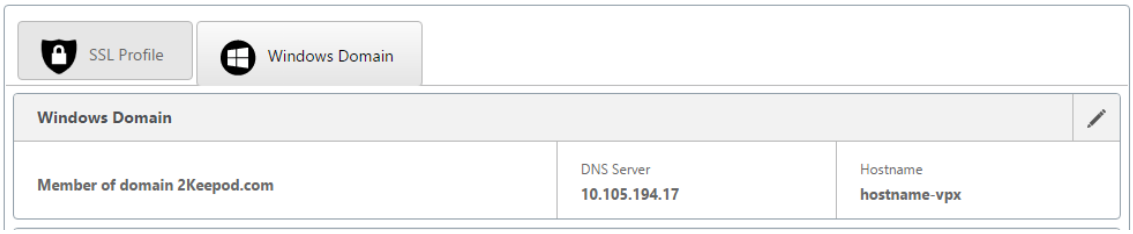


3. Nachdem die Zusammenfassung der Vorprüfung als erfolgreich angezeigt wurde, geben Sie die Anmeldeinformationen des Domänencontrollers ein.





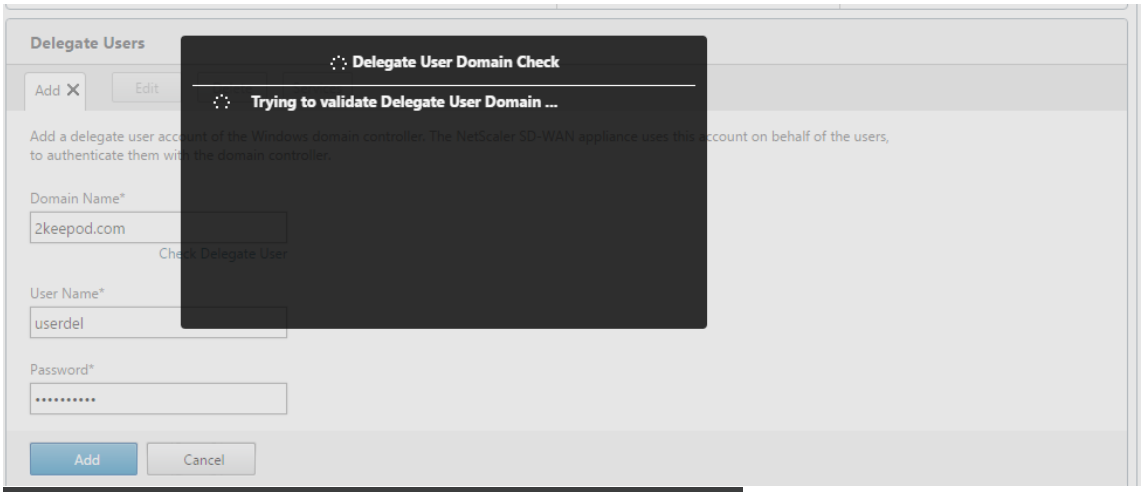
4. Bei erfolgreichem Domainbeitritt erhalten Sie die folgende Ausgabe.

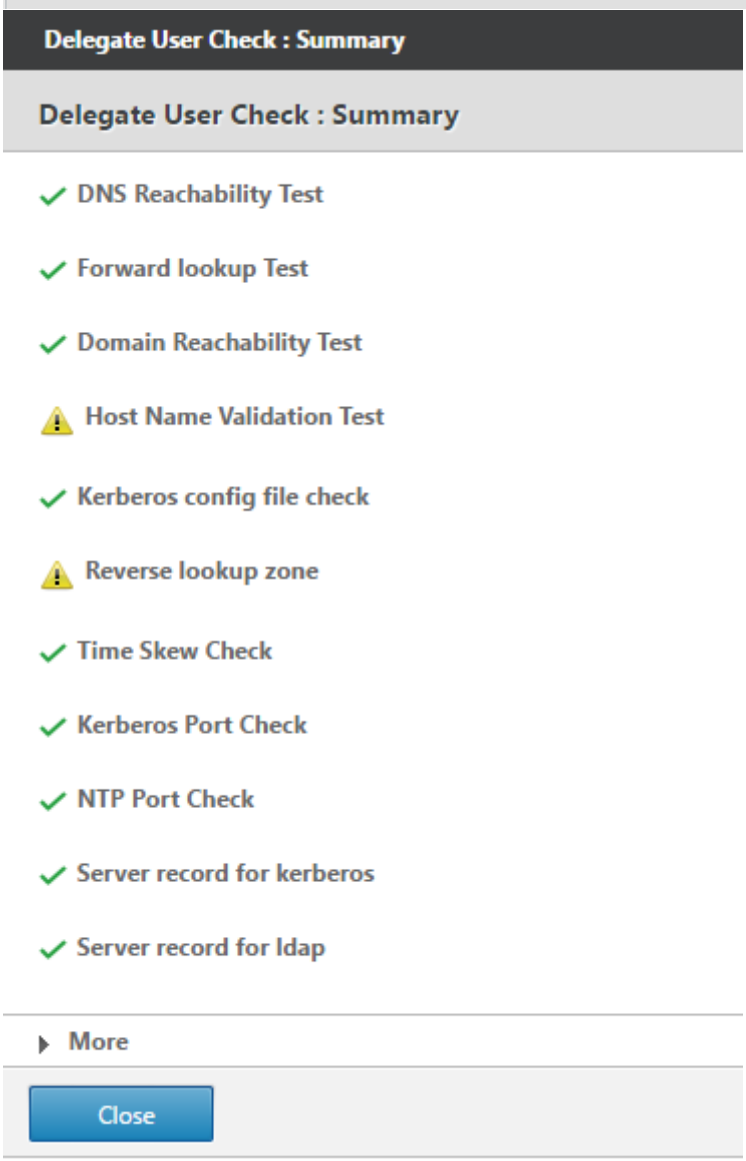


Benutzer delegieren

1. Fügen Sie einen delegierten Benutzer hinzu, um die Dienste wie unten gezeigt zu delegieren.

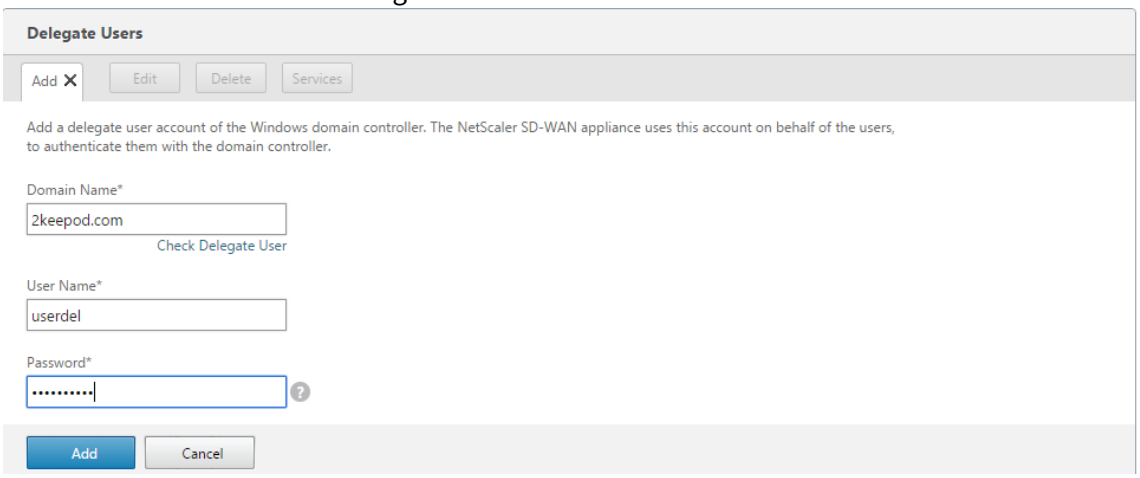
2. Geben Sie den korrekten Domainnamen an und führen Sie eine Vorabprüfung des Delegierten durch



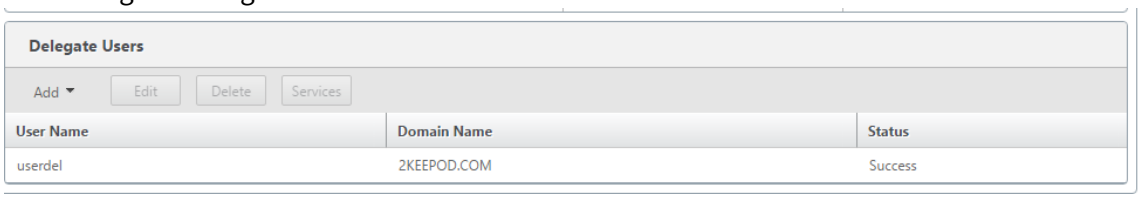


3. Nachdem die Vorabprüfungen für delegierte Benutzer erfolgreich waren, geben Sie gültige

Anmeldeinformationen des delegierten Benutzers an.



4. Nachdem der delegierte Benutzer erfolgreich zu SD-WAN hinzugefügt wurde, bemerken Sie eine Erfolgsmeldung.



5. Um zu überprüfen, welche Dienste vom delegierten Benutzer delegiert werden, zeigen Sie auf den Benutzer und wählen Sie Dienste aus.

Sicherheit

October 28, 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 die folgenden Sicherheitsüberlegungen:

- Physische Sicherheit
- Gerätesicherheit
- Netzwerksicherheit
- Verwaltung und Verwaltung

Die in den folgenden Links beschriebenen Themen enthalten weitere Informationen zur Konfiguration der Sicherheit für SD-WAN-Netzwerke mit:

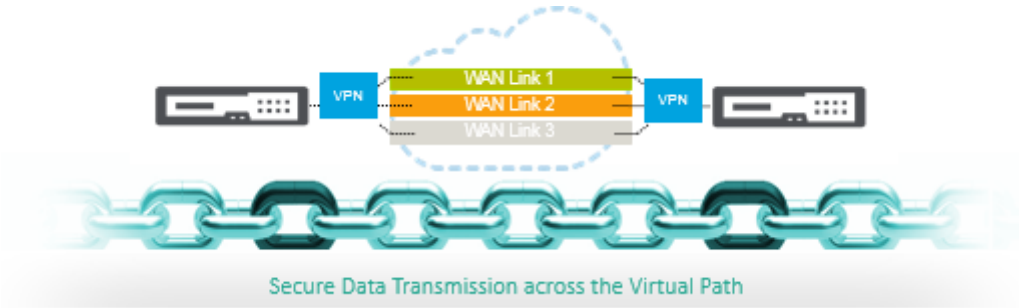
- IPsec-Tunnel
- Firewall

IPsec-Tunnelterminierung

October 28, 2021

Citrix SD-WAN unterstützt virtuelle IPsec-Pfade, sodass Geräte von Drittanbietern IPsec-VPN-Tunnel auf 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

October 28, 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 nahebasierten 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

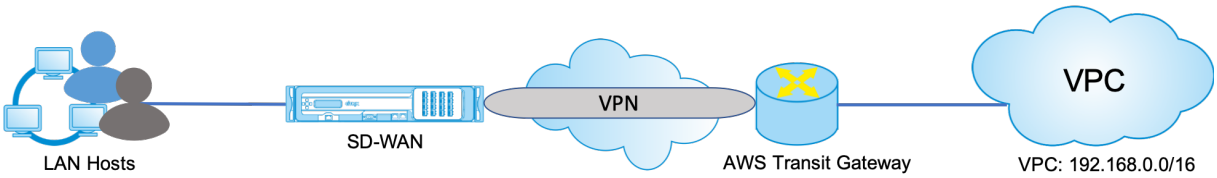
(VPCs) zu lernen.

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.

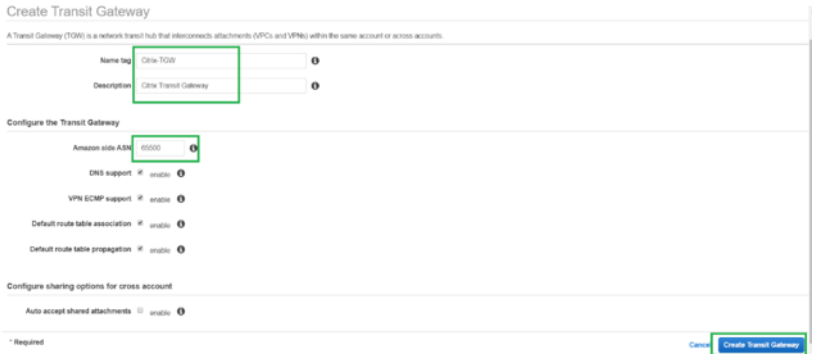
Unabhängig davon, welche Methode gewählt wird, erreicht der Datenverkehr zu den VPCs, die mit dem Transit Gateway verbunden sind, ohne das Routing innerhalb von AWS infra manuell zu verwalten.



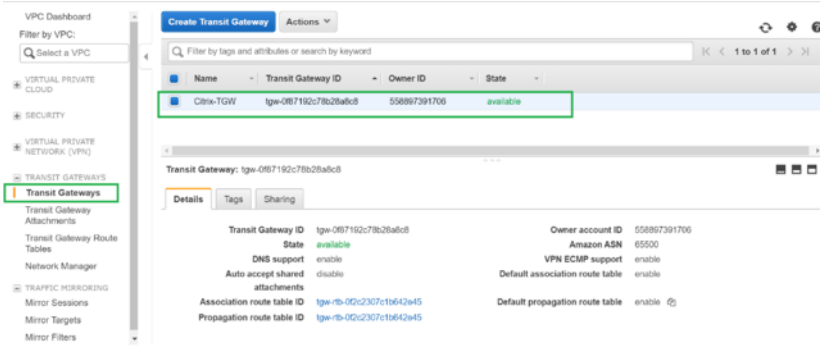
Konfiguration von AWS Transit Gateway

Um das **AWS Transit Gateway**zu erstellen, navigieren Sie zum VPC-Dashboard und wechseln Sie zum Abschnitt **Transit Gateway**.

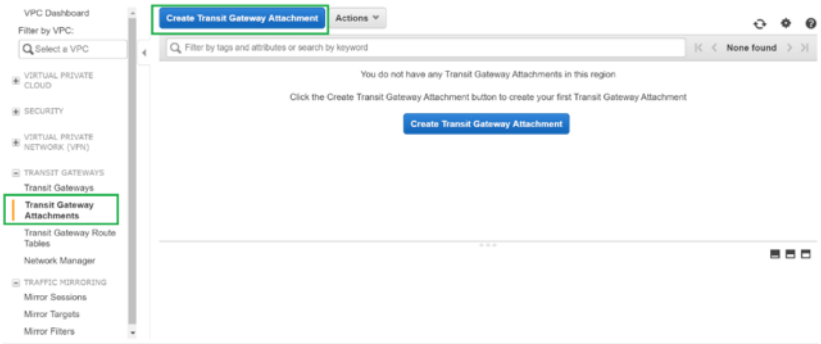
1. Geben Sie den Transit Gateway-Namen, die Beschreibung und die Amazon-ASN-Nummer wie im folgenden Screenshot hervorgehoben an, und klicken Sie auf **Transit Gateway erstellen**.



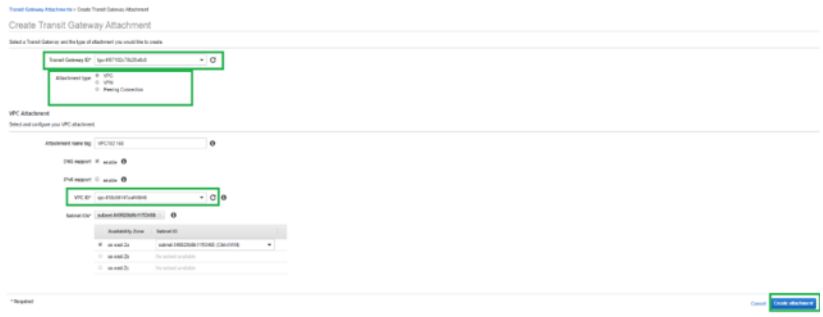
Sobald die Transit Gateway-Erstellung abgeschlossen ist, können Sie den Status als **Verfügbar**sehen.



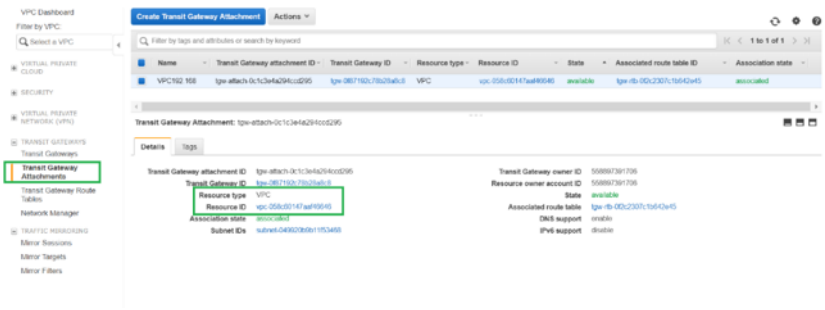
2. Um die **Transit Gateway-Anhänge**zu erstellen, navigieren Sie zu **Transit Gateways > Transit Gateway Attachments** und klicken Sie auf **Transit-Gateway-Anlage erstellen**



3. Wählen Sie das Transit Gateway aus der Dropdownliste 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.

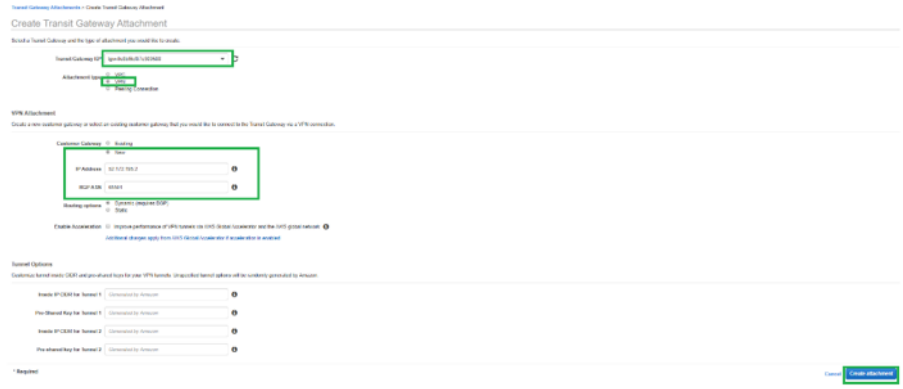


4. Nachdem Sie die VPC an das Transit-Gateway angeschlossen haben, können Sie sehen, dass die **VPC des Ressourcentyps** mit dem Transit-Gateway verknüpft wurde.

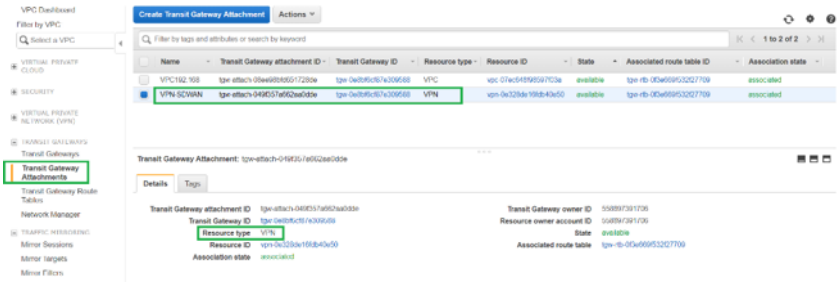


5. Um SD-WAN über VPN an das Transit Gateway anzuschließen, wählen Sie die **Transit Gateway-ID** aus der Dropdownliste aus und wählen Sie **Anhangstyp** als **VPN**aus. Stellen Sie sicher, dass Sie die richtige Transit Gateway ID auswählen.

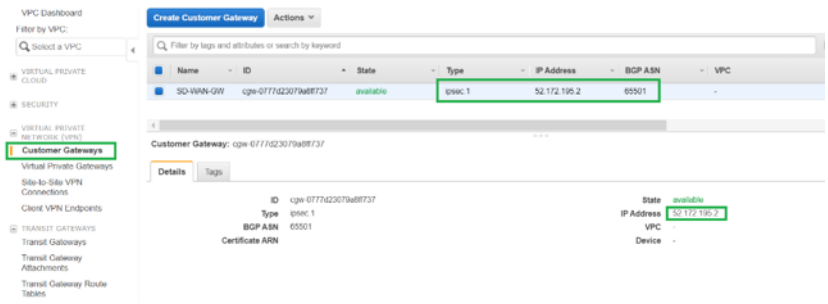
   Fügen Sie ein neues VPN Customer Gateway hinzu, indem Sie die öffentliche IP-Adresse des SD-WAN-Links und die BGP-ASN-Nummer angeben. Klicken Sie auf **Anlage erstellen**, um VPN mit Transit Gateway zu verbinden.



6. Sobald das VPN an das Transit Gateway angeschlossen ist, können Sie die Details sehen, wie im folgenden Screenshot gezeigt:

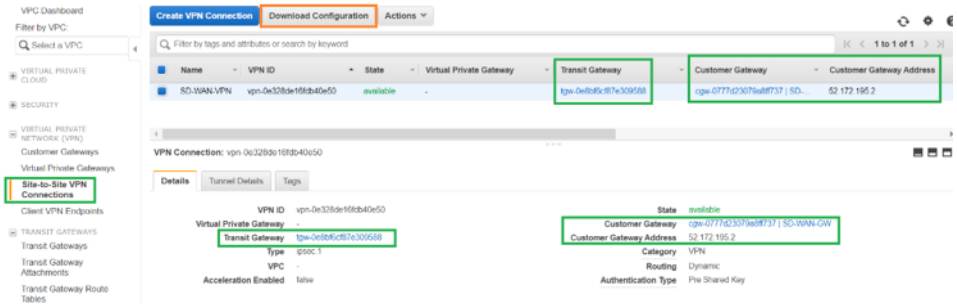


7. Unter **Customer Gateways** werden SD-WAN Customer Gateway und Site-to-Site VPN Connection als Teil von VPN Attachment to Transit Gateway erstellt. Sie sehen, dass das SD-WAN Customer Gateway zusammen mit der IP-Adresse dieses Customer Gateways erstellt wird, das die öffentliche WAN-Link-IP-Adresse von SD-WAN darstellt.

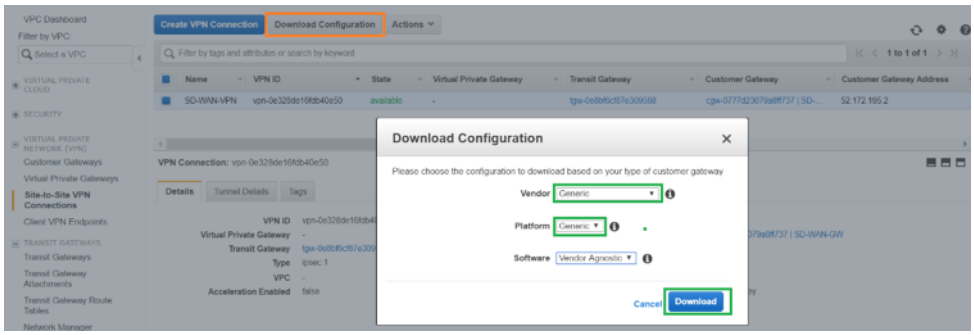


8. Navigieren Sie zu **Site-to-Site VPN Connections**, um die **VPN-Konfiguration des SD-WAN-Kunden-Gateways** Diese Konfigurationsdatei enthält zwei IPsec-Tunneldetails zusammen mit den BGP-Peer-Informationen. Zwei Tunnel werden aus SD-WAN zu Transit Gateway für Redundanz erstellt.

   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**aus.



   Die heruntergeladene Konfigurationsdatei enthält die folgenden Informationen:

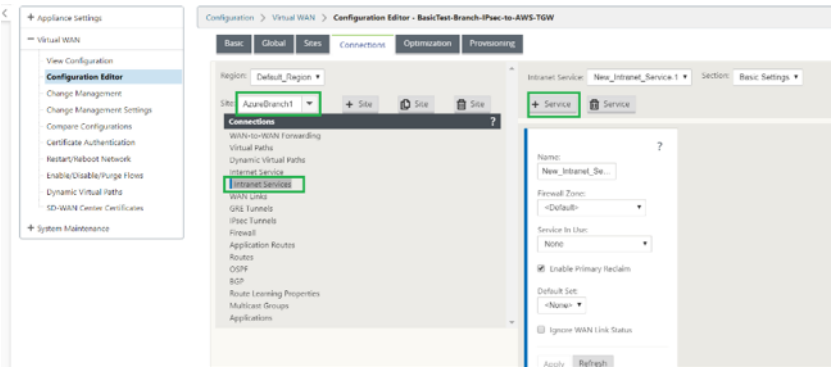
   - IKE-Konfiguration
   - IPsec-Konfiguration für AWS Transit Gateway
   - Konfiguration der Tunnelschnittstelle
   - BGP-Konfiguration

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:

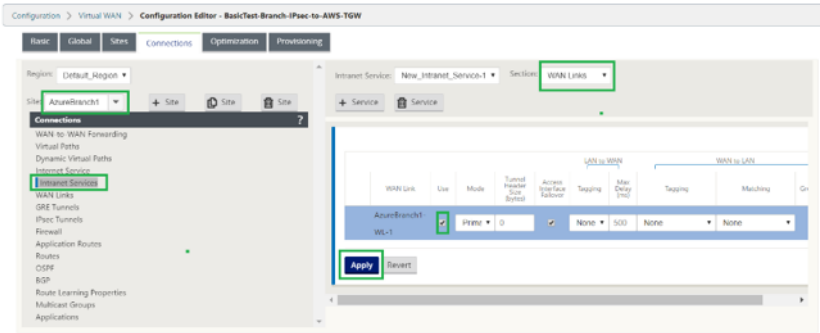
```
#3: Tunnel Interface Configuration

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

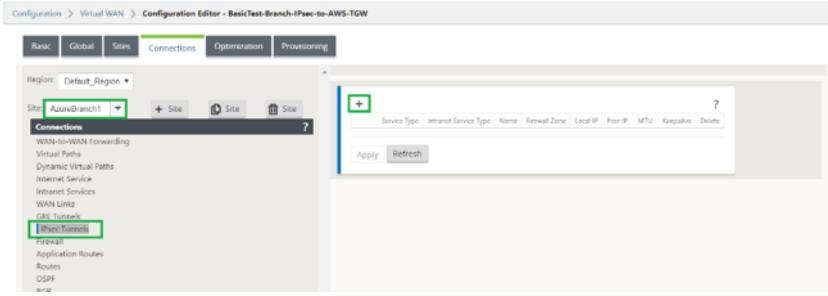
1. Um den Intranetdienst zu konfigurieren, der in der IPsec-Tunnelkonfiguration auf SD-WAN verwendet wird, navigieren Sie zu **Konfigurationseditor > Verbindungen**, wählen Sie die Site aus der Dropdownliste aus und wählen Sie **Intranetdienst**aus. Klicken Sie auf **+ Service**, um einen neuen Intranetdienst hinzuzufügen.



2. 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.

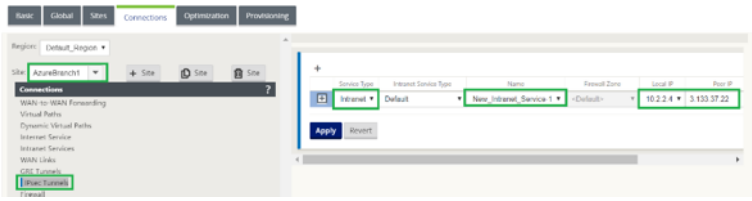


3. Um den IPsec-Tunnel in Richtung AWS Transit Gateway zu konfigurieren, navigieren Sie zu **Configuration Editor > Verbindungen** wählen Sie die Site aus der Dropdownliste aus und klicken Sie auf **IPsec-Tunnels**. Klicken Sie auf **+**, um IPsec-Tunnel hinzuzufügen.

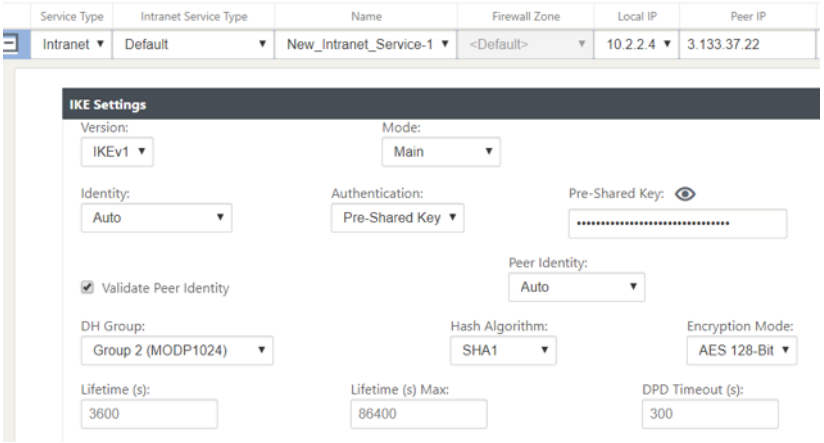


4. Wählen Sie den **Diensttyp** als **Intranet** aus und wählen Sie den **Namen des Intranetdienstes aus, den** Sie hinzugefügt haben. Wählen Sie die **lokale IP-Adresse** als WAN-Link-IP-Adresse und **Peer-Adresse** als Transit Gateway Virtual Private Gateway IP-Adresse aus.

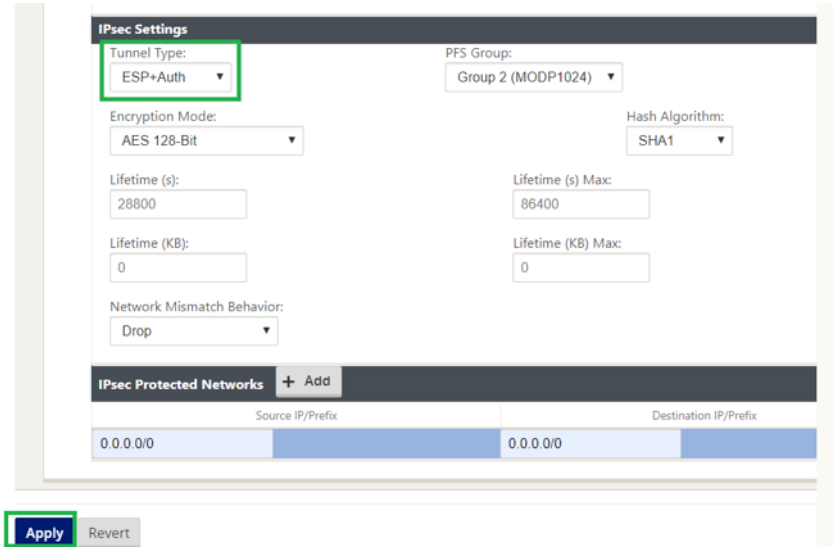
   Klicken Sie auf das Kontrollkästchen **Keepalive**, damit der Tunnel sofort nach der Aktivierung der Konfiguration von SD-WAN initiiert wird.



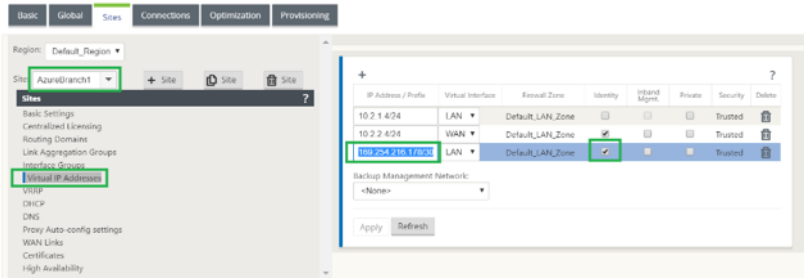
5. Konfigurieren Sie IKE-Parameter basierend auf der VPN-Konfigurationsdatei, die Sie von AWS heruntergeladen haben.



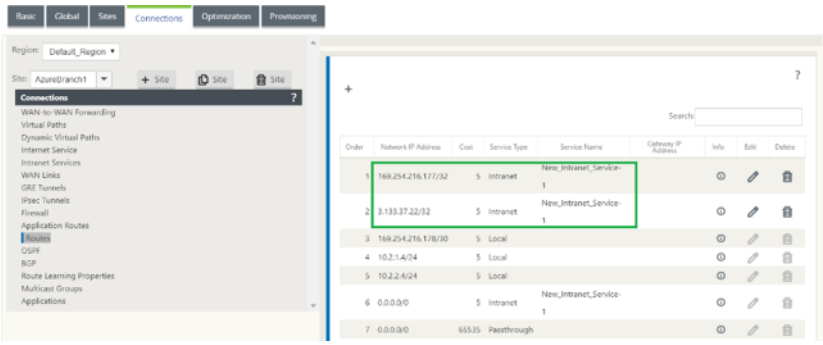
6. Konfigurieren Sie IPsec-Parameter basierend auf der VPN-Konfigurationsdatei, die Sie von AWS heruntergeladen haben. Konfigurieren Sie **IPsec-geschützte Netzwerke** auch basierend auf dem Netzwerk, das Sie durch den Tunnel senden möchten. Sie können sehen, dass es so konfiguriert ist, dass jeder Datenverkehr über den IPsec-Tunnel zugelassen wird.



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**.

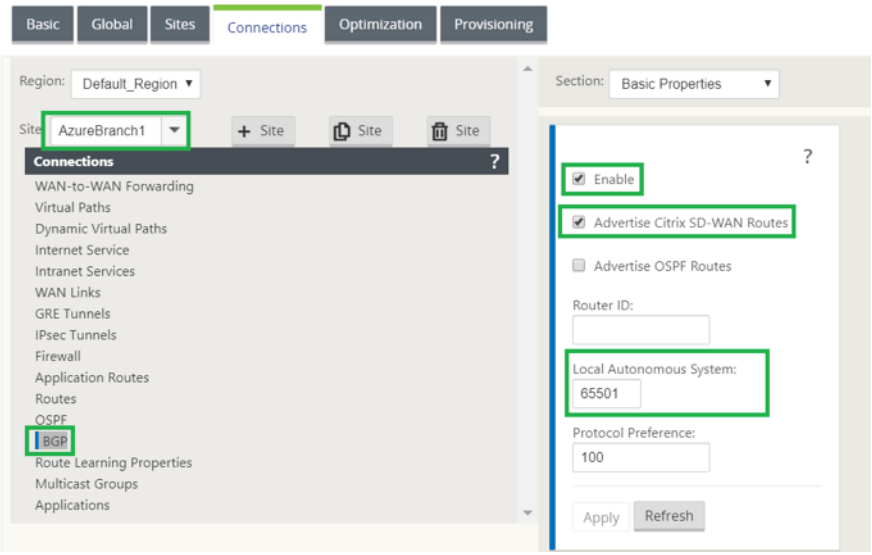


8. Fügen Sie **Routen** auf SD-WAN hinzu, um **Virtual Private Gateway** von Transit Gateway zu erreichen. Suchen Sie in der heruntergeladenen VPN-Konfigurationsdatei innerhalb und außerhalb der IP-Adresse von Virtual Private Gateway im Zusammenhang mit Tunnel-1. Fügen Sie Routen zur inneren und äußeren 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.

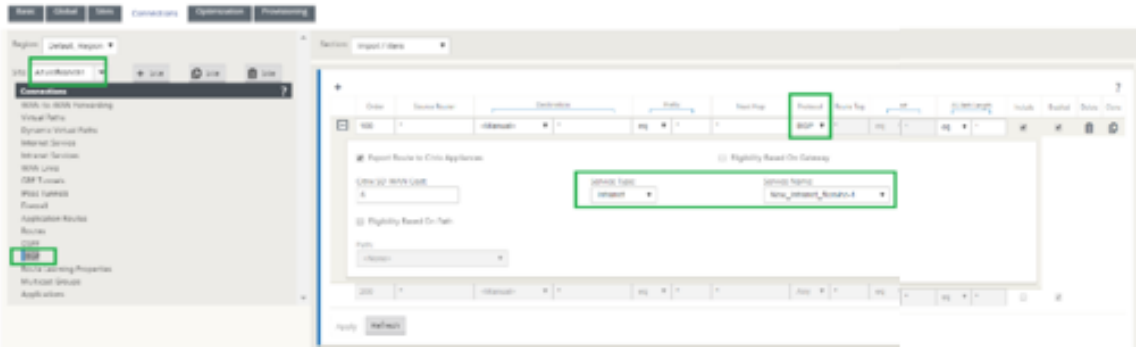
   Um BGP auf SD-WAN zu aktivieren, navigieren Sie zu **Verbindungen** wählen Sie die Site aus der Dropdownliste und wählen Sie dann **BGP**aus. Klicken Sie auf **Aktivieren**, um BGP zu aktivieren. Aktivieren Sie das Kontrollkästchen **Citrix SD-WAN Routes** ankündigen, um SD-WAN Routen in Richtung Transit 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 Dropdownliste aus und wählen Sie dann **BGP**aus. Klicken Sie auf den Abschnitt **Nachbarn** und klicken Sie auf **+** Option.

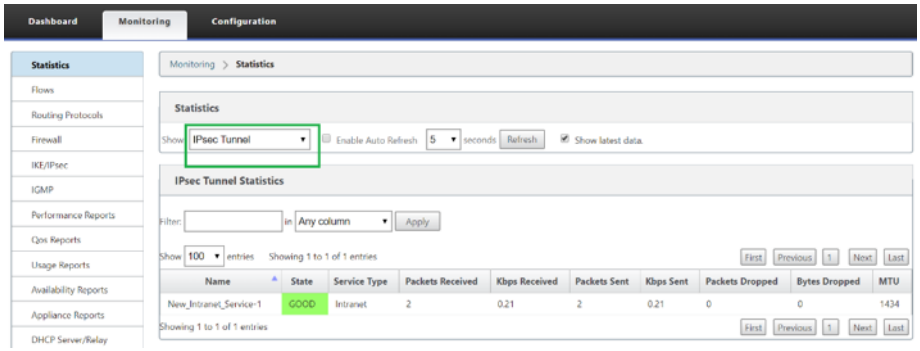
Verwenden Sie **Neighbor IP Address** und **Virtual Private Gateway ASN** aus den BGP-Konfigurationsoptionen, während Sie Nachbarn hinzufügen. Die **Quell-IP** muss mit der IP-Adresse des **Kunden-Gateways** (Konfiguriert als virtuelle IP-Adresse auf SD-WAN) aus der heruntergeladenen Konfigurationsdatei von AWS übereinstimmen. Fügen Sie BGP Neighbor mit aktiviertem **Multi-Hop** für SD-WAN hinzu.

11. Um **Importfilter** zum Importieren von BGP-Routen in SD-WAN hinzuzufügen, navigieren Sie zu **Verbindungen**, wählen Sie die Site aus der Dropdownliste 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.

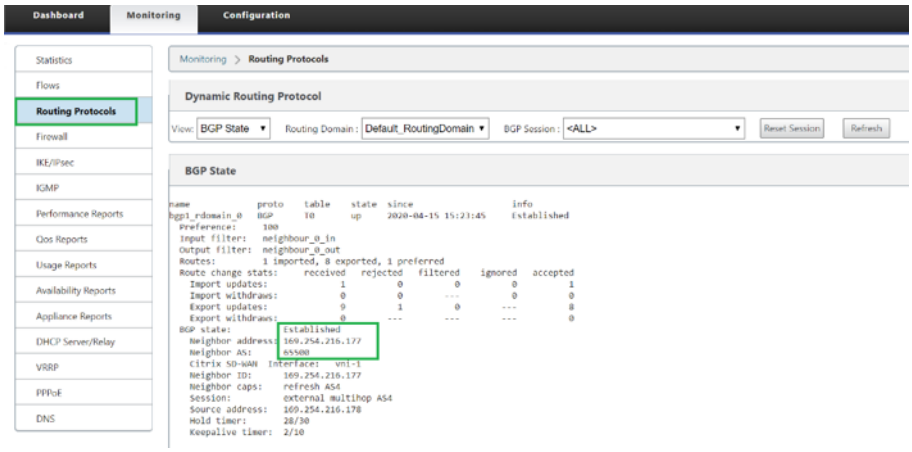


Überwachung und Fehlerbehebung auf SD-WAN

1. 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.

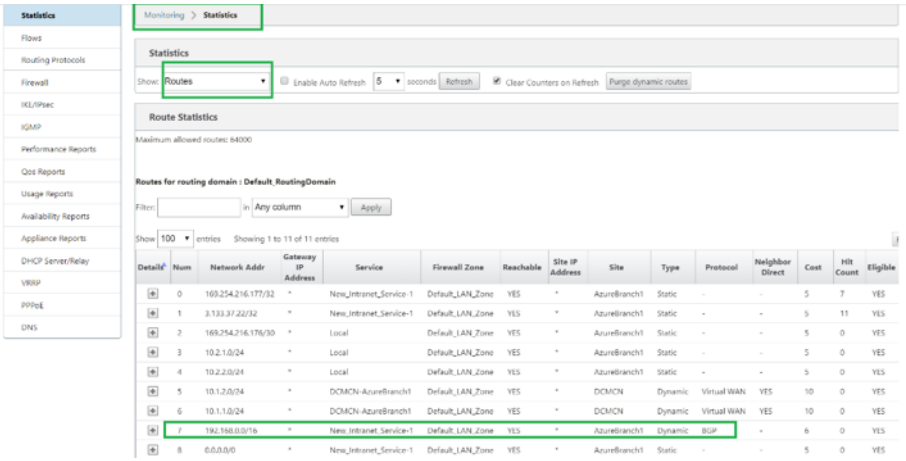


2. Um den **BGP Peering-Status** auf SD-WAN zu überprüfen, navigieren Sie zu **Monitoring > Routing Protocols** und wählen Sie **BGP State**aus. Sie können sehen, dass der BGP-Status als **Etabliert** gemeldet wurde und die **Nachbar-IP-Adresse** und die **Nachbar-ASN** den AWS BGP-Nachbardetails entsprechen. 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.

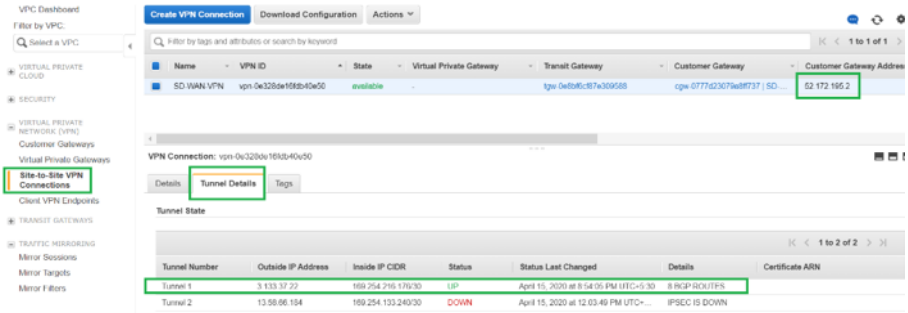
3. Um die BGP-Routeninstallation auf SD-WAN zu überprüfen, navigieren Sie zu **Monitoring > Statistics > Routes** und suchen Sie nach dem Netzwerk 192.168.0.0/16, das als BGP-Route mit Servicetyp als Intranet installiert wurde. Dies bedeutet, dass Sie die Netzwerke lernen können, die mit AWS Transit Gateway verbunden sind, und können mit diesen Netzwerken über IPsec-Tunnel kommunizieren.



Überwachung und Fehlerbehebung in AWS

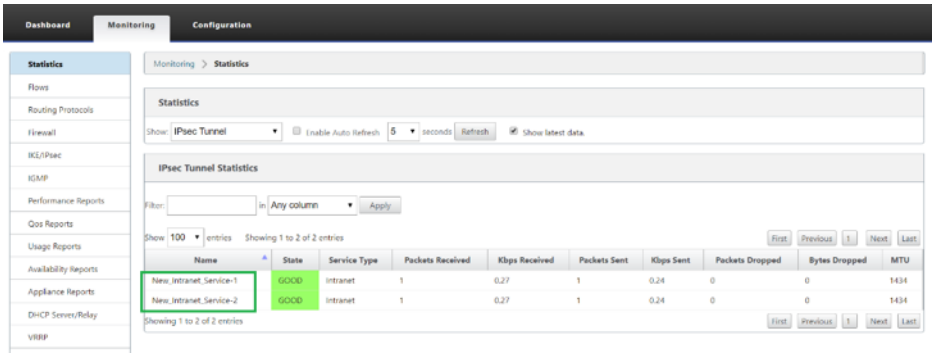
1. Um den Status der IPsec-Tunneleinrichtung auf AWS zu überprüfen, navigieren Sie zu **VIRTUAL PRIVATE NETWORK (VPN) > Site-to-Site VPN-Verbindungen** Im folgenden Screenshot können Sie beobachten, dass die Customer Gateway-Adresse SD-WAN Link öffentliche IP-Adresse darstellt, mit der Sie Tunnel eingerichtet 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.

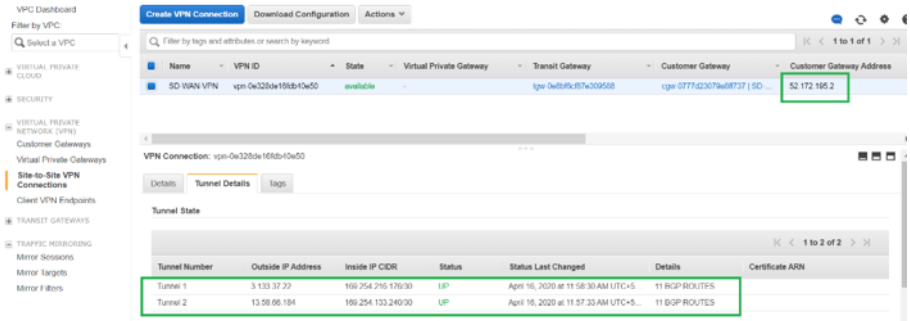


2. Konfigurieren Sie IPsec- und BGP-Details im Zusammenhang mit dem zweiten Tunnel basierend auf der heruntergeladenen Konfigurationsdatei auf SD-WAN.

   Der Status, der sich auf beide Tunnel bezieht, kann auf SD-WAN wie folgt überwacht werden:



3. Der Status, der sich auf beide Tunnel bezieht, kann in AWS wie folgt überwacht werden:

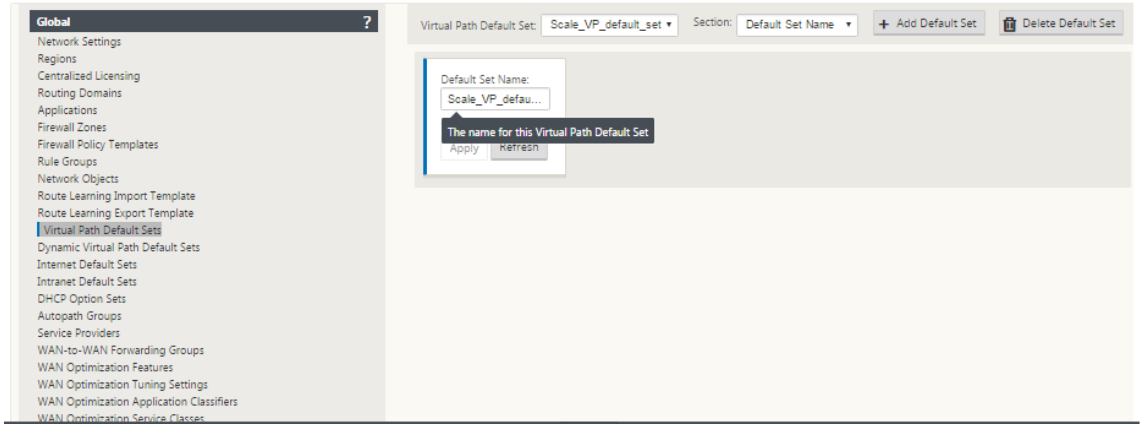


Konfigurieren von IPsec-Tunneln für virtuelle und dynamische Pfade

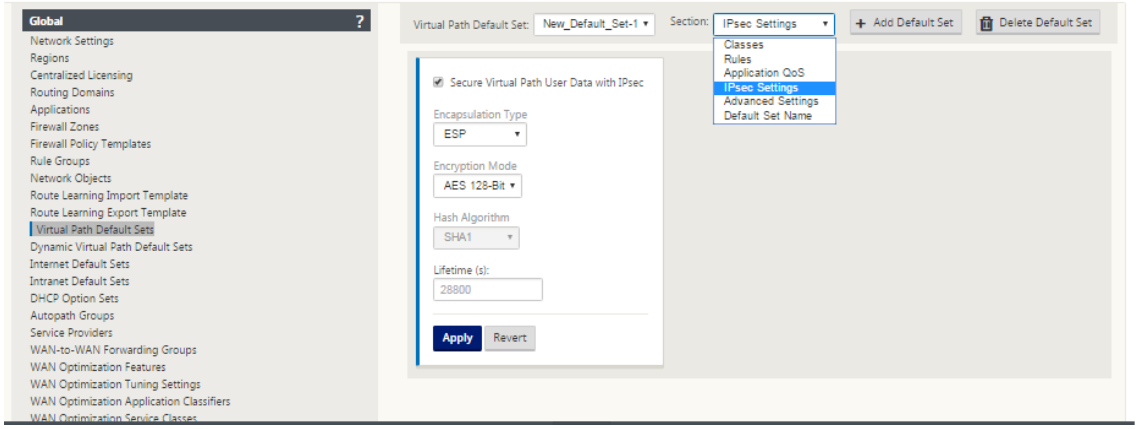
October 28, 2021

So konfigurieren Sie IPsec-Tunnel für virtuelle und dynamische virtuelle Pfade zwischen Citrix 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 das erstellte 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.

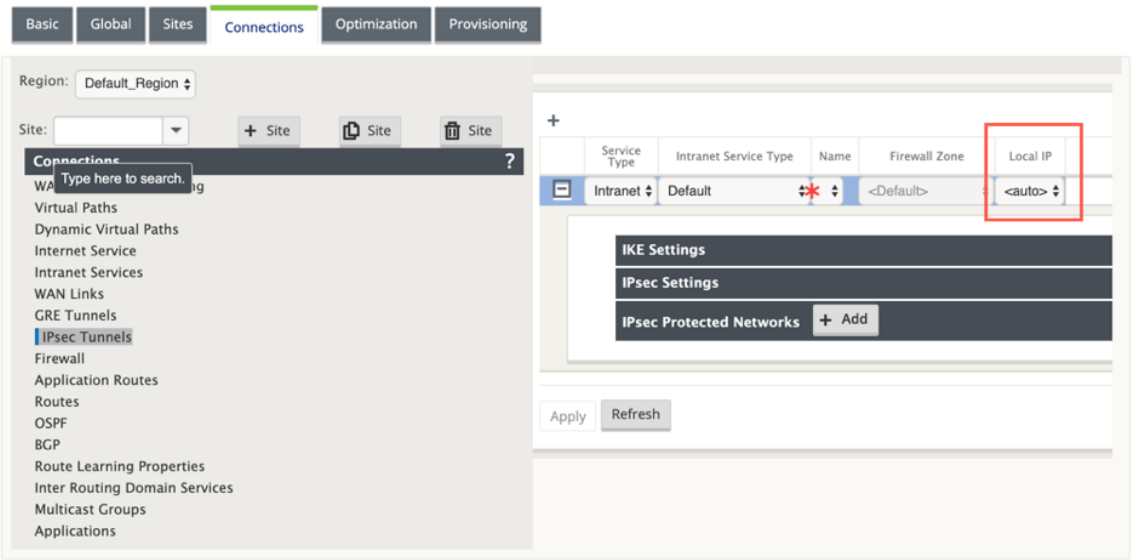


Konfigurieren des IPsec-Tunnels zwischen SD-WAN und Drittanbieter-Geräten

October 28, 2021

So konfigurieren Sie den IPsec-Tunnel für Intranet- oder LAN-Dienst:

1. Navigieren Sie im **Konfigurationseditor**zu **Verbindungen**> **Site anzeigen**> **[Standortname]**> **IPsec-Tunnel**. Wählen Sie einen **Servicetyp** (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.

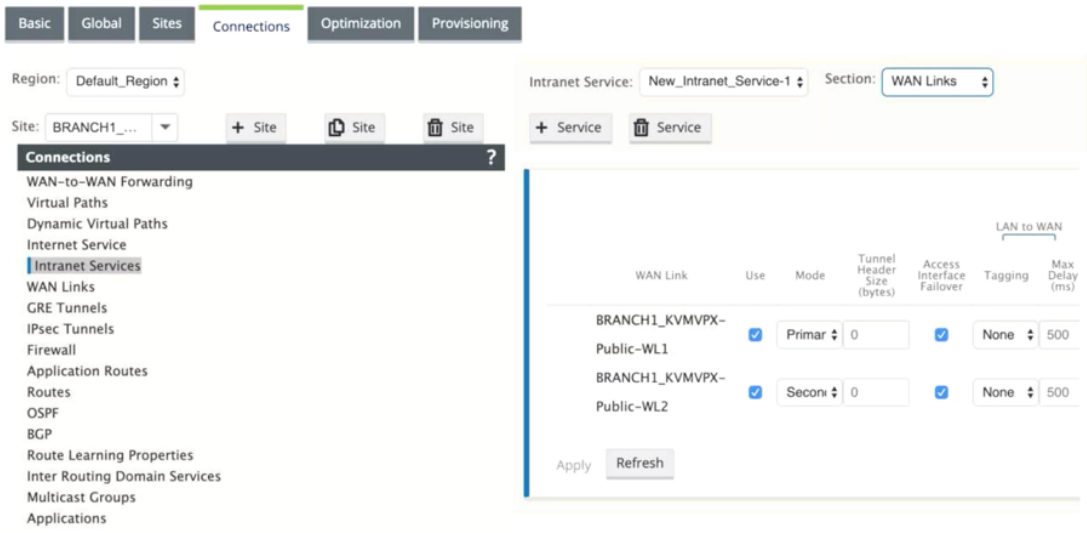
Wenn die lokale IP auf **Auto**festgelegt ist, kann sie die IP-Adresse übernehmen, die für die Zugriffsschnittstelle auf dieser WAN-Verbindung integriert ist. Diese WAN-Link-Zugriffsschnittstelle erhält möglicherweise die IP entweder statisch oder von DHCP. Der IPsec-Tunnel wird standardmäßig mit der 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.

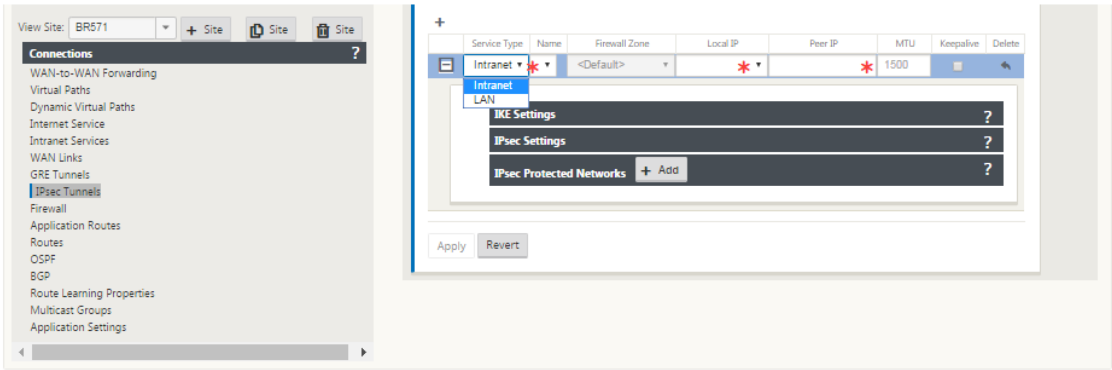
Ab Version 11.1.0 können Sie zwei WAN-Verbindungen verwenden, um IPsec-Tunnel einzurichten, um Zweigumgebungen vor Zeiten von Service-Unterbrechungen zu schützen. Wenn die primäre Verbindung heruntergeht, schaltet sich die sekundäre Verbindung innerhalb von Millisekunden aktiv/nach oben.

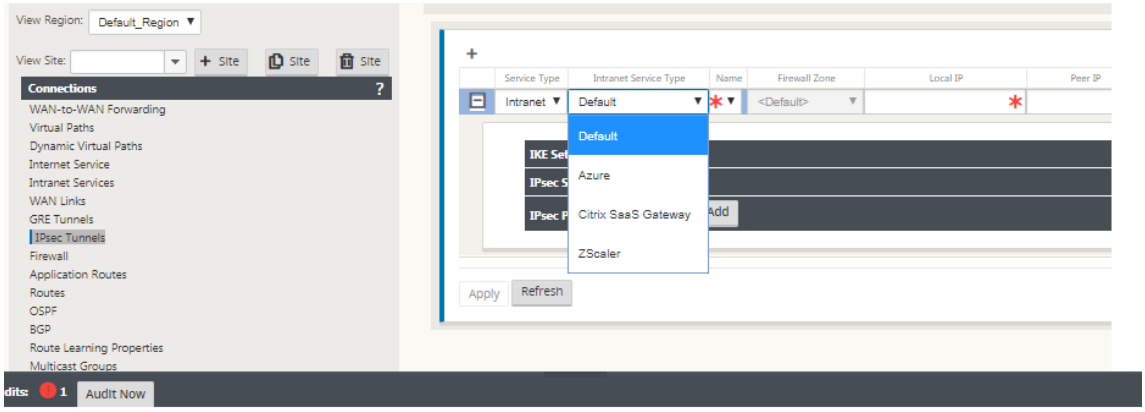
> **Hinweis**

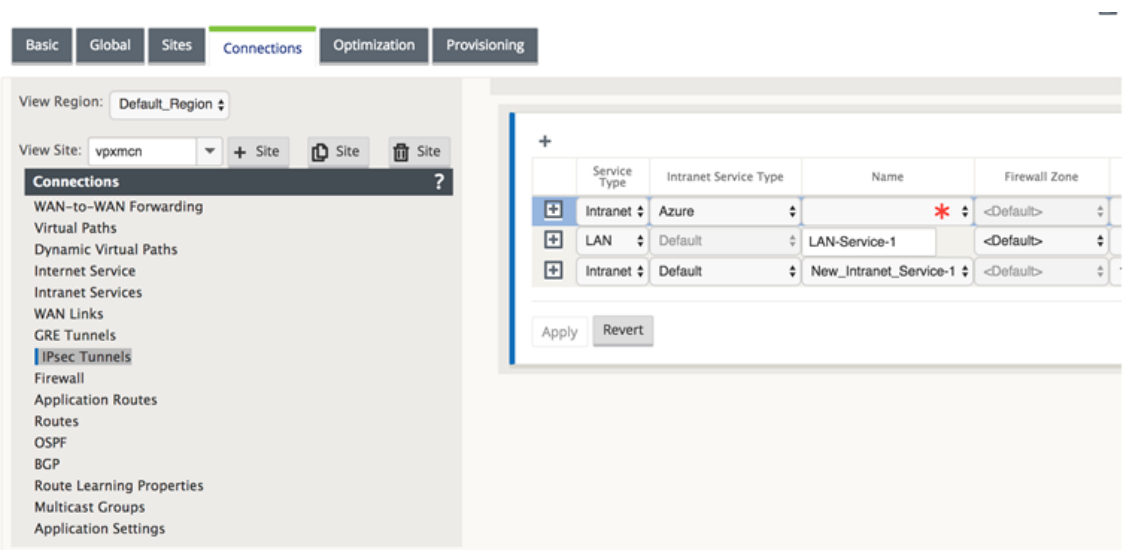
> Wenn die Option <**Auto**> ausgewählt ist, wird der IPsec-Tunnel über die primäre WAN-Link-Zugriffsschnittstelle eingerichtet. Wenn die primäre WAN-Verbindung ausfällt, wird der IPsec-Tunnel über die sekundäre WAN-Link-Zugriffsschnittstelle eingerichtet.



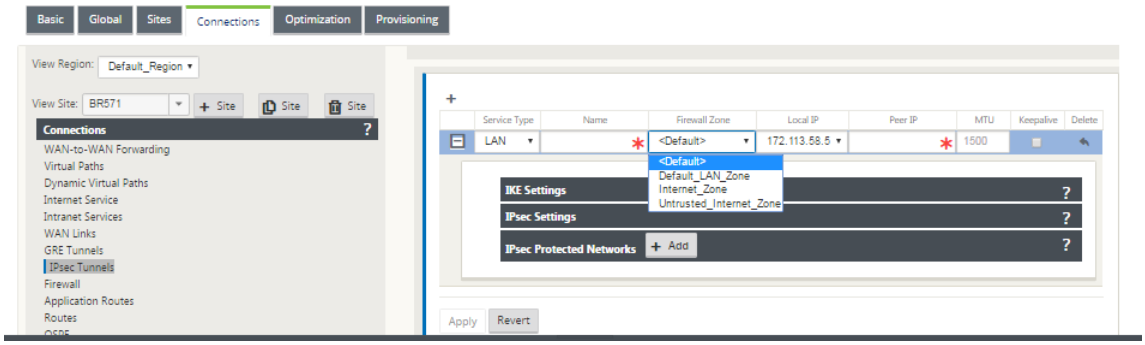
3. Wählen Sie die verfügbare **lokale IP-Adresse** aus und geben Sie die **Peer-IP-Adresse** des IPsec-Tunnels ein.







> **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.

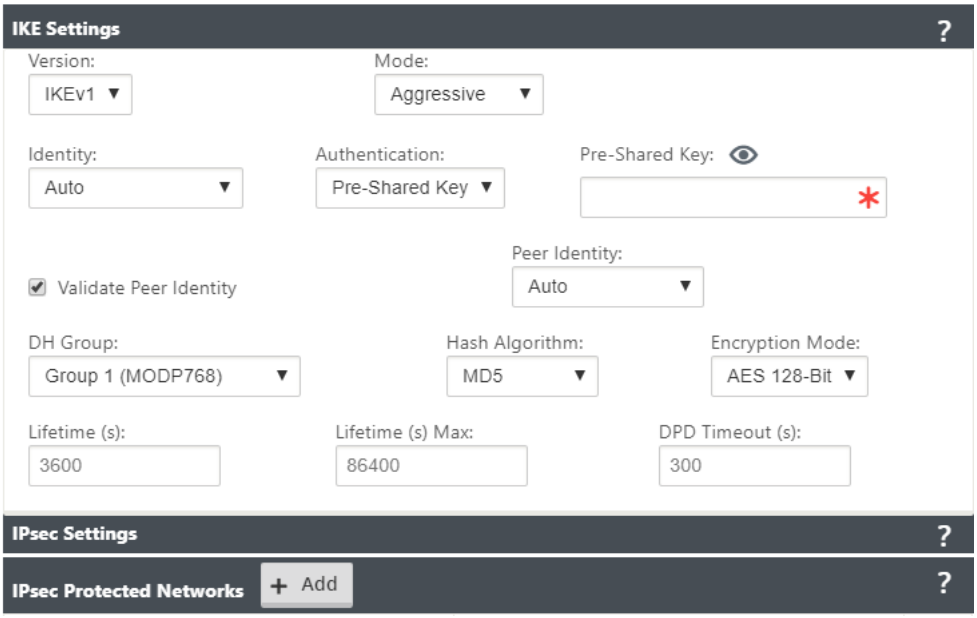
Feld	Beschreibung	Wert
Servicetyp	Wählen Sie einen Servicetyp aus dem Dropdownmenü	Intranet, LAN
Name	Wenn der Diensttyp Intranet ist, wählen Sie aus der Liste der konfigurierten Intranetdienste im Dropdownmenü aus. Wenn der Diensttyp LAN ist, geben Sie einen eindeutigen Namen ein	Textzeichenfolge

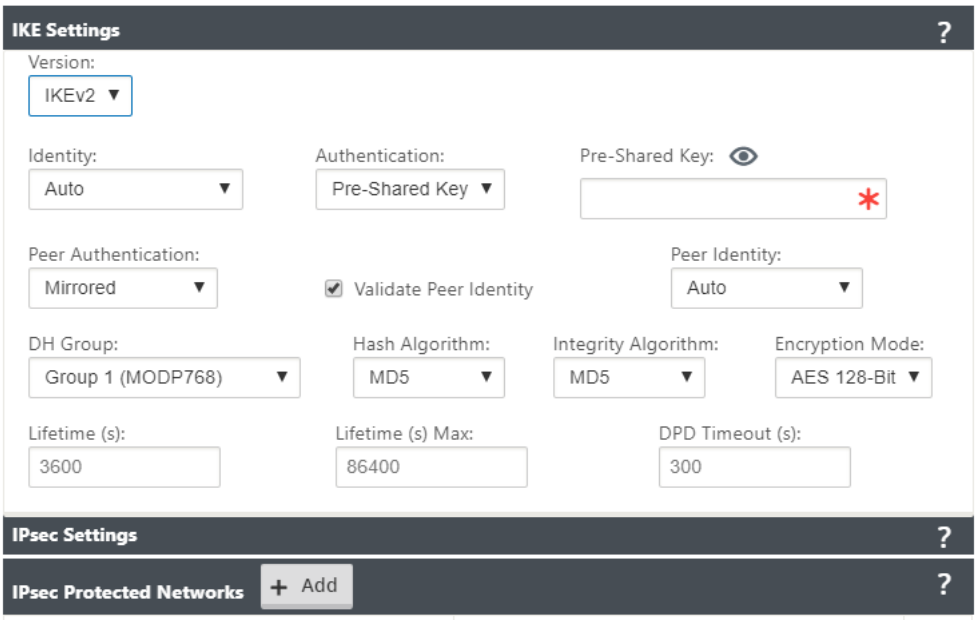
Feld	Beschreibung	Wert
Lokale IP	Wählen Sie die lokale IP-Adresse des IPsec-Tunnels aus dem Dropdownmenü der verfügbaren virtuellen IP-Adressen, die an diesem Standort konfiguriert sind.	IP-Adresse
Peer-IP	Geben Sie die Peer-IP-Adresse des IPsec-Tunnels ein	IP-Adresse
MTU	Geben Sie die **MTU** zum Fragmentieren 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
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	–

Feld	Beschreibung	Wert
DH-Gruppe	Wählen Sie die Diffie-Hellman-Gruppe für die IKE-Schlüsselgenerierung aus dem Dropdownmenü	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 aus, um IKE-Nachrichten zu authentifizieren	Nicht FIPS-konform: MD5 FIPS-konform: SHA1 SHA-256
Verschlüsselungsmodus	Wählen Sie den **Verschlüsselungsmodus** für IKE-Nachrichten aus dem Dropdownmenü	AES 128-Bit-AES 192-Bit-AES 256-Bit
Lebensdauer (s)	Geben Sie die bevorzugte Dauer in Sekunden ein, damit eine IKE-Sicherheitszuordnung existiert	3600 Sekunden (Standard)
Lebenszeit (n) Max	Geben Sie die bevorzugte Höchstdauer in Sekunden ein, damit eine IKE-Sicherheitszuordnung existieren kann	86400 Sekunden (Standard)
DPD Timeout (s)	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 Dropdownmenü	Gespiegeltes Pre-Shared-Key-Zertifikat
IKE2 - Vorab geteilter Schlüssel	Peer-Pre-Shared Key: Fügen Sie den vorab geteilten IKEv2-Peer-Schlüssel zur Authentifizierung in dieses Feld ein. Klicken Sie auf das Augensymbol (), um den Pre-Shared Key anzuzeigen	Textzeichenfolge

Feld	Beschreibung	Wert
Integrität Algorithmus	Wählen Sie im Dropdownmenü einen Algorithmus als Hashing-Algorithmus aus, der für die HMAC-Überprüfung 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**.

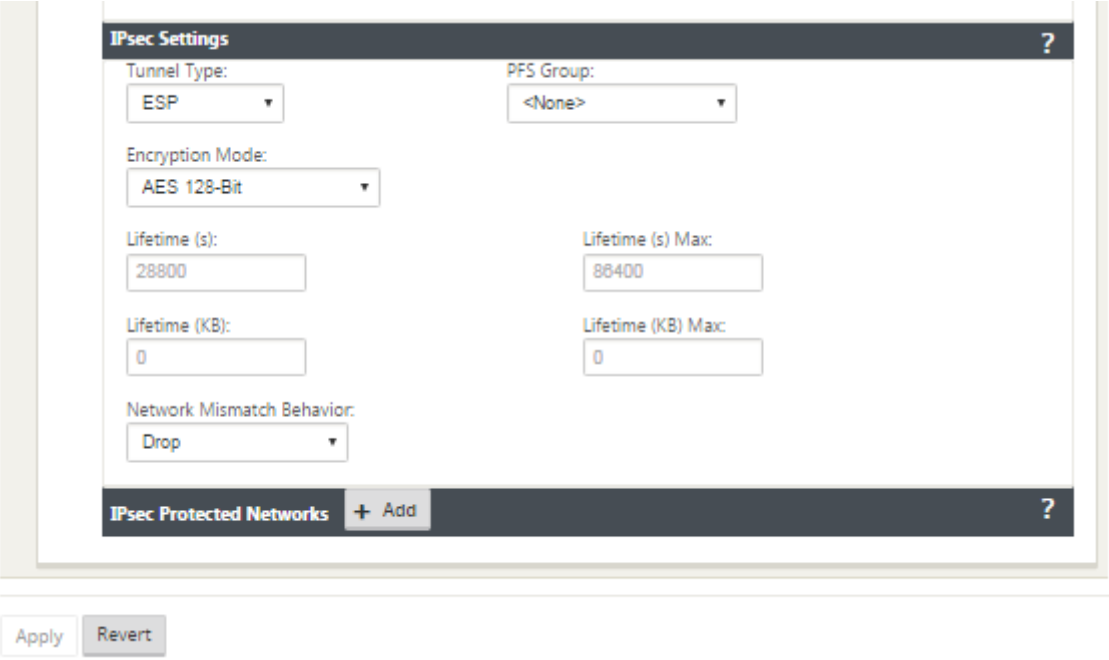




IPsec- und IPsec-geschützte Netzwerkeinstellungen:

Feld	Beschreibung	Wert (e)
Tunnel-Typ	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 Dropdownmenü	Keine Gruppe 1 Gruppe 2 Gruppe 5 Gruppe 14 Gruppe 15 Gruppe 16 Gruppe 19 Gruppe 20 Gruppe 21
Verschlüsselungsmodus	Wählen Sie den **Verschlüsselungsmodus** für IPsec-Nachrichten aus dem Dropdownmenü	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.

Feld	Beschreibung	Wert (e)
Lebensdauer (s)	Geben Sie die Zeit in Sekunden ein, um eine IPsec-Sicherheitszuordnung zu ermöglichen.	28800 Sekunden (Standard)
Lebenszeit Max (s)	Geben Sie die maximale Zeit in Sekunden ein, um eine IPsec-Sicherheitszuordnung zu ermöglichen.	86400 Sekunden (Standard)
Lebenszeit (KB)	Geben Sie die Datenmenge in Kilobyte ein, für die eine IPsec-Sicherheitszuordnung vorhanden sein soll.	Kilobyte
Lebensdauer (KB) maximal	Geben Sie die maximale Datenmenge in Kilobyte ein, um eine IPsec-Sicherheitszuordnung zu ermöglichen.	Kilobyte
Verhalten bei Netzwerk-Nichtübereinstimmung	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
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



Überwachung von IPsec-Tunneln

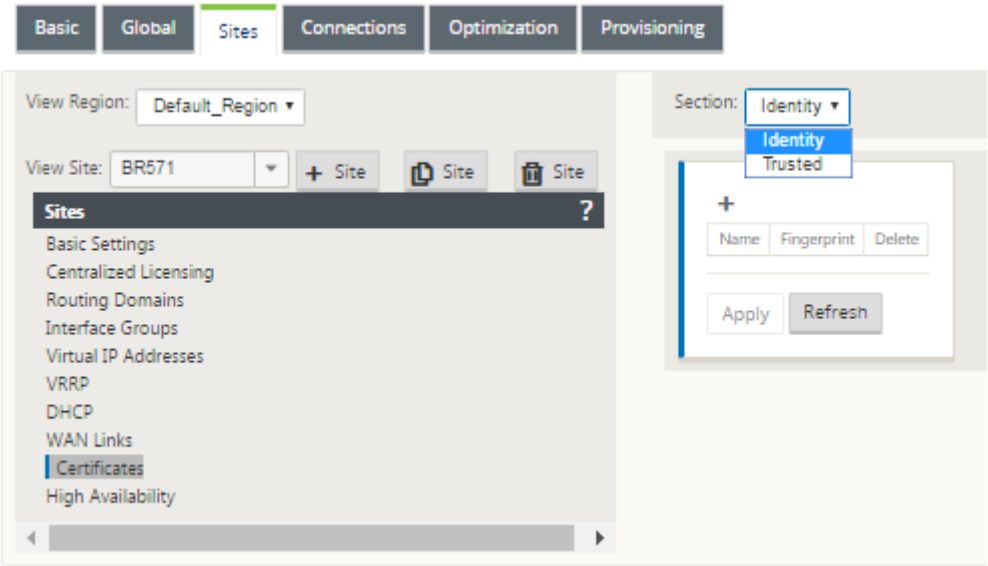
Navigieren Sie zu **Monitoring>IKE/IPsec** in der Benutzeroberfläche der SD-WAN-Appliance, um die IPsec-Tunnelkonfiguration anzuzeigen und zu überwachen.

Hinzufügen von IKE-Zertifikaten

October 28, 2021

So implementieren Sie Zertifikate für IKE-Verhandlungen:

1. Navigieren Sie zu **Sites** > **Zertifikate** und fügen Sie alle erforderlichen Zertifikate hinzu.

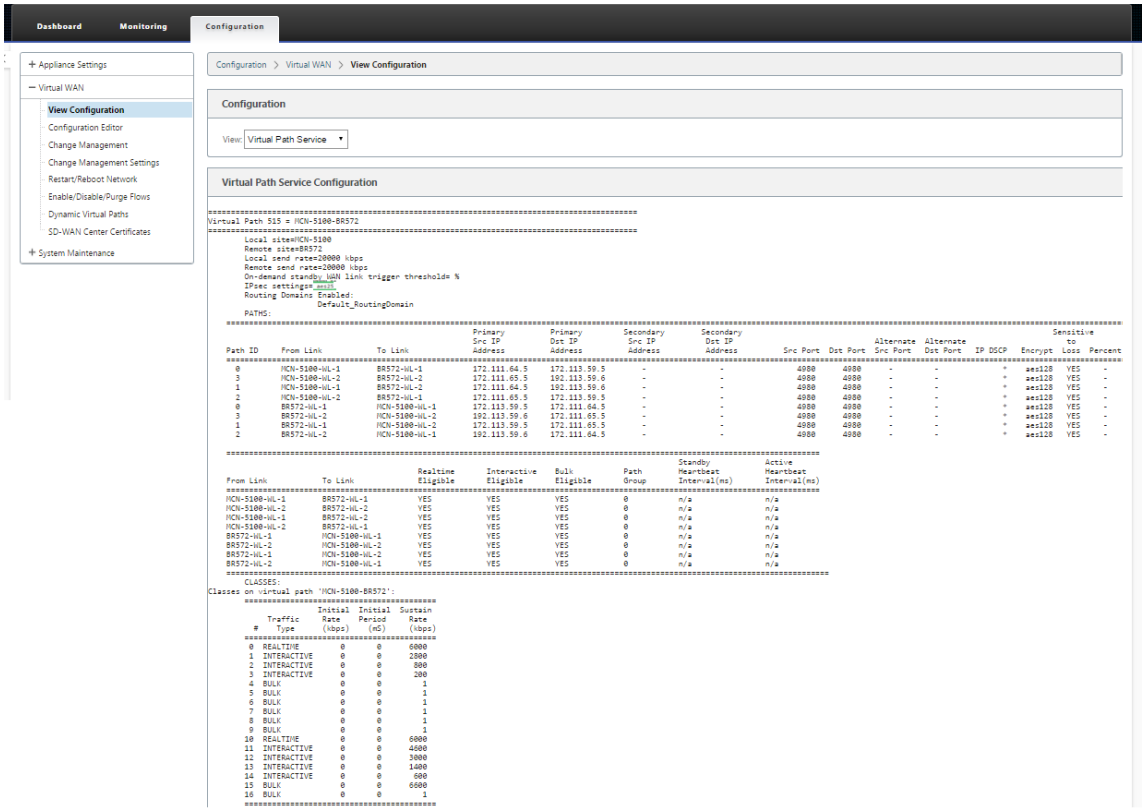


So zeigen Sie die IPsec-Tunnelkonfiguration an

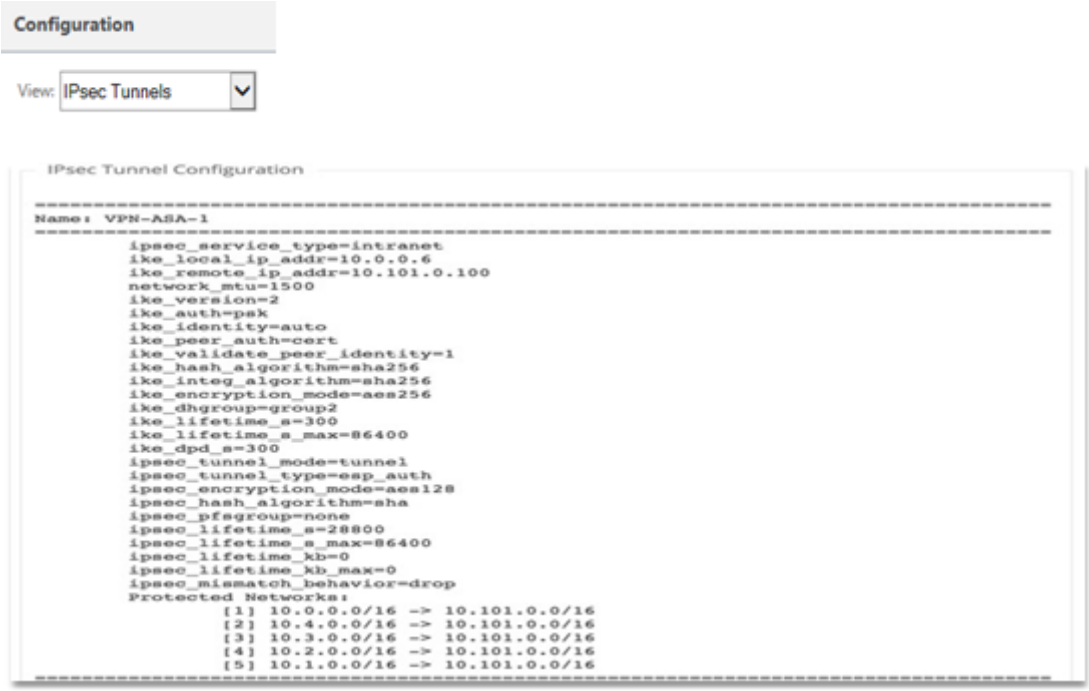
October 28, 2021

So zeigen Sie IPsec-Tunnelkonfiguration an:

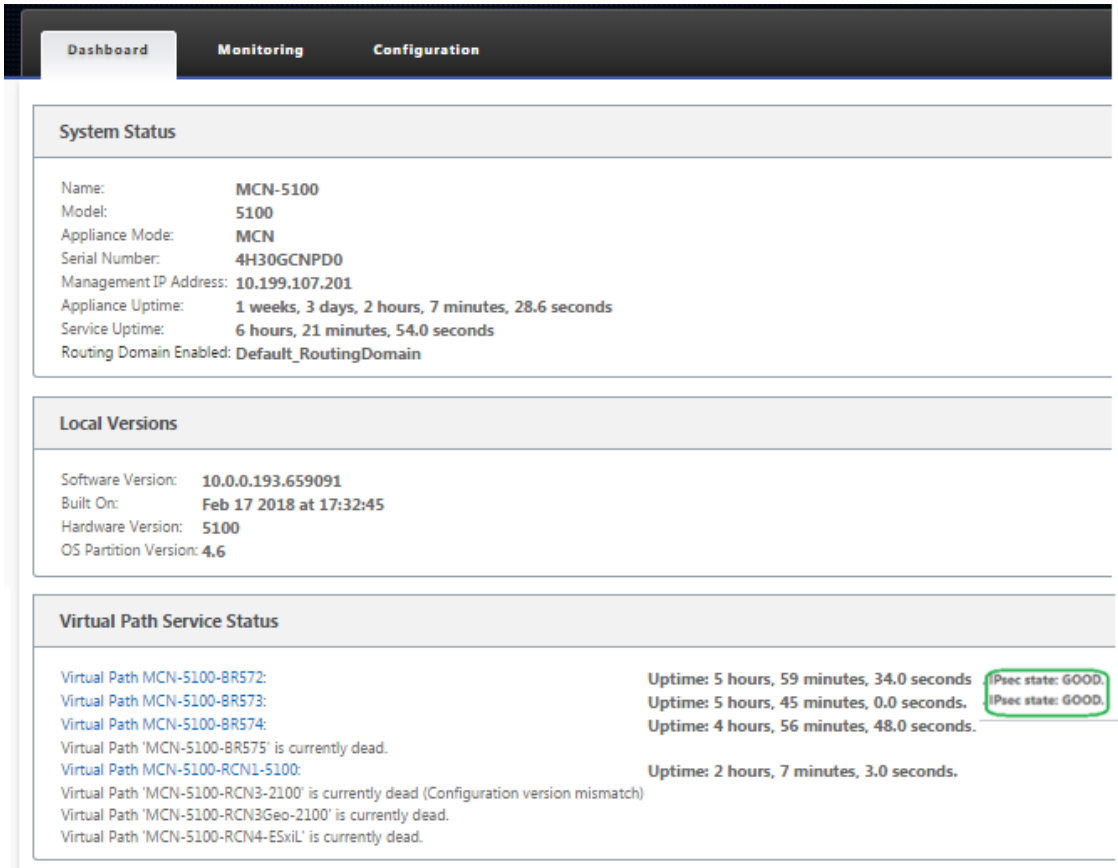
1. Navigieren Sie zu **Konfiguration > Virtuelles WAN** > **Konfiguration anzeigen**.
2. Wählen Sie im Dropdownmenü **Virtueller Pfaddienst** aus. Die IPsec-Einstellungen werden nur angezeigt, wenn IPsec im Konfigurationseditor aktiviert ist.



3. Wählen Sie **IPsec-Tunnel** aus dem Dropdownmenü, um die IPsec-Tunnelkonfiguration anzuzeigen.



4. Jeder virtuelle Pfad zeigt seinen eigenen IPsec-Tunnelstatus, wie unten gezeigt.

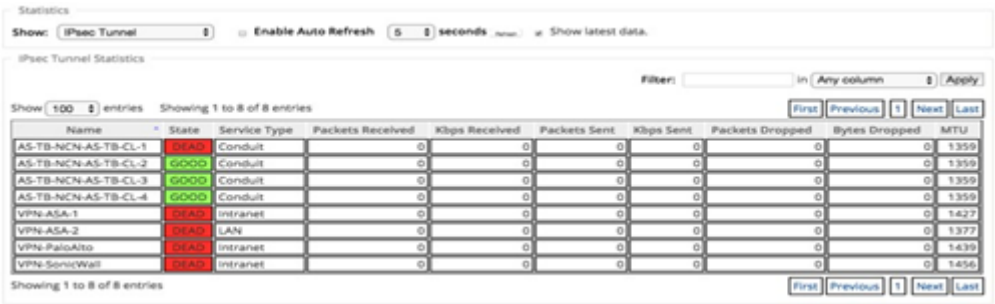


IPsec-Überwachung und -Protokollierung

October 28, 2021

So überwachen Sie IPsec-Tunnelstatistiken:

1. Navigieren Sie zu **Monitor > Statistiken**. Wählen Sie **IPsec-Tunnel** aus dem Dropdownmenü **Anzeigen**, wie unten dargestellt:



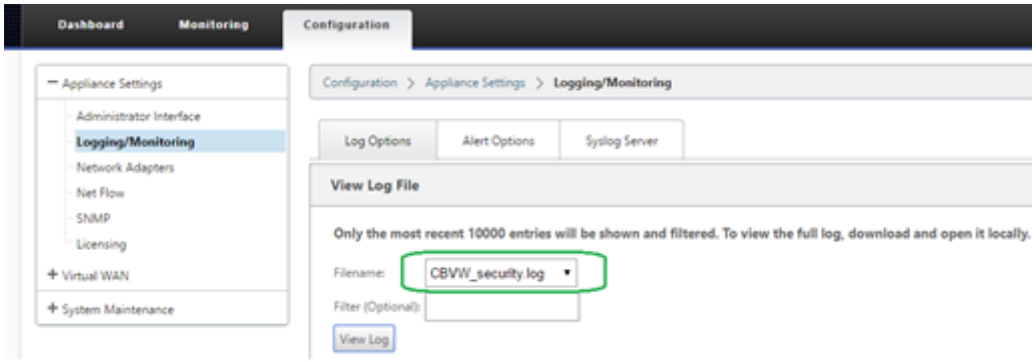
2. Navigieren Sie zu **Monitor** > **IKE/IPSec**. Beachten Sie die konfigurierten IPsec-Tunnel, die IKE-

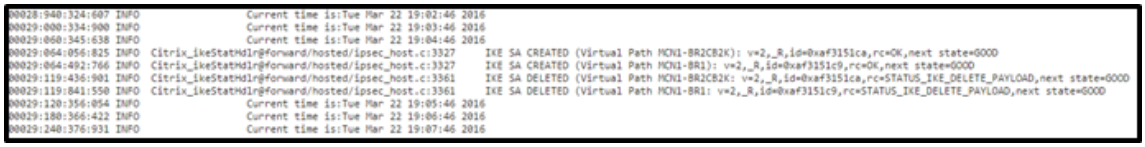
und IPsec-Dienstzuordnungen zwischen zwei oder Modus-VPN-Endpunkten, die im SD-WAN-Netzwerk konfiguriert sind.

Wie überwacht man IPec-Protokolle

1. Navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Protokollierung/Überwachung**. Wählen Sie im Dropdownmenü **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

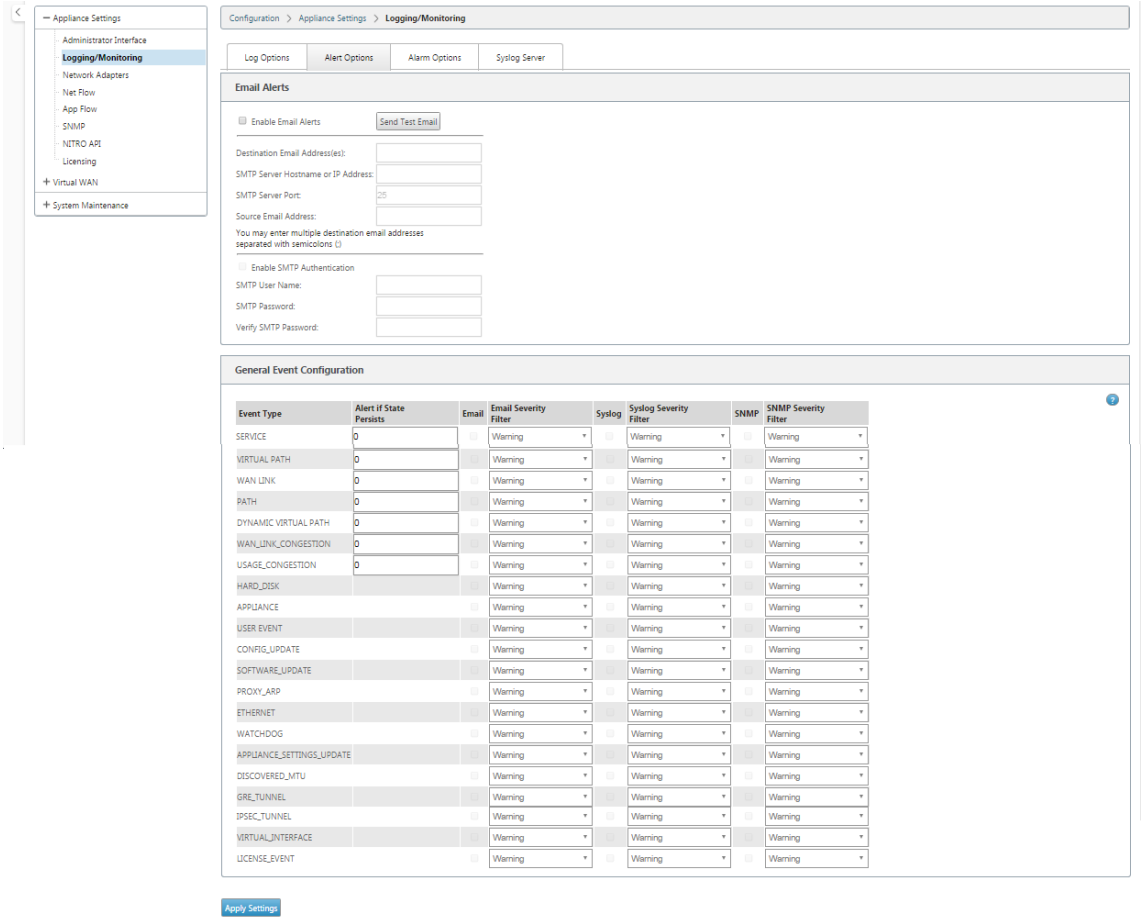




So zeigen Sie IPsec-Tunnelwarnungen an

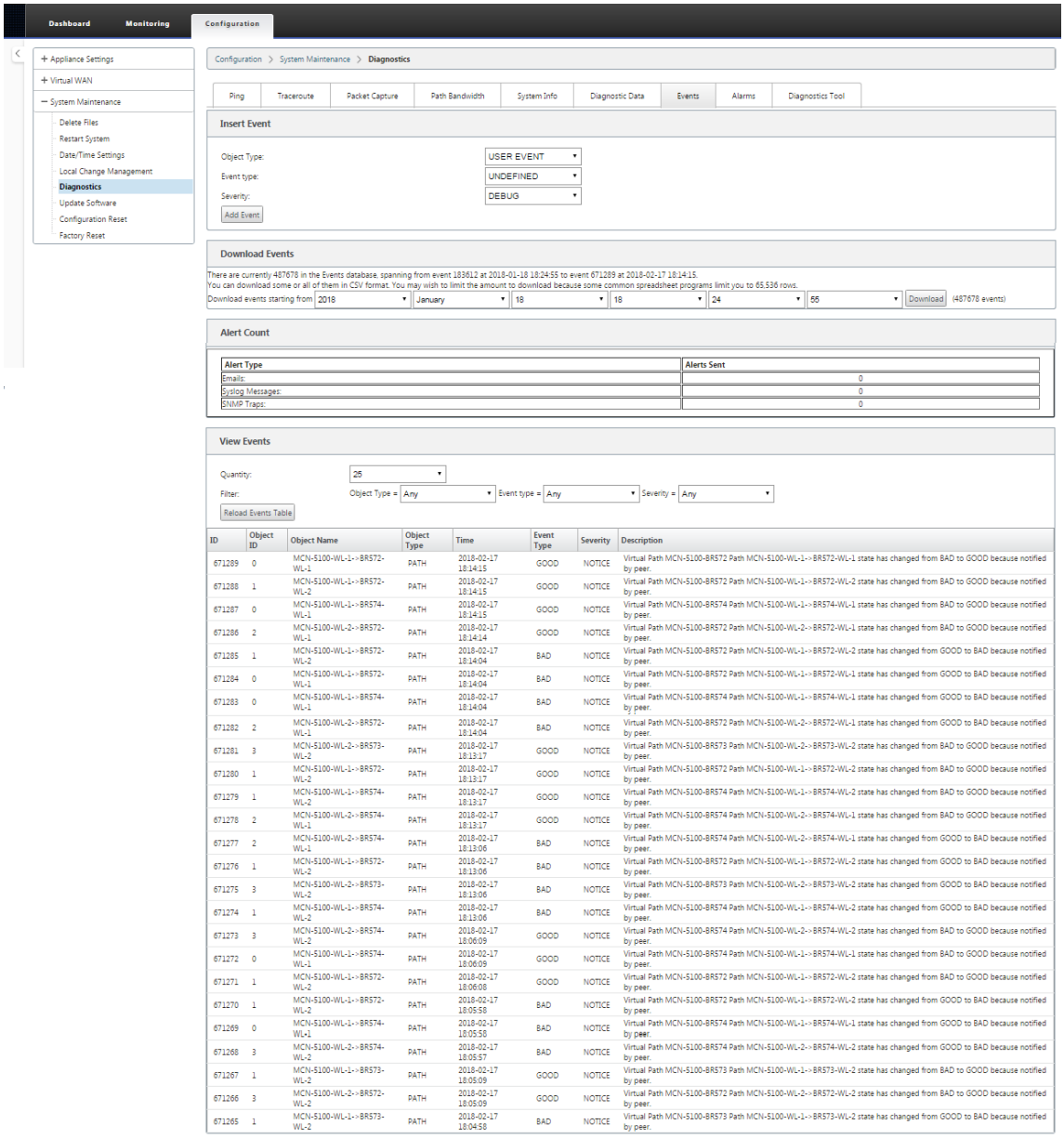
1. Navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Protokollierung/Überwachung** > **Warnoptionen**.
2. Erstellen Sie E-Mail- und Syslog-Warnungen für IPsec-Tunnelzustandsberichte.

   - Unterstützt IPSEC_TUNNEL als einer der Ereignistypen, mit denen Sie E-Mail- und Syslog-Schweregradfilter konfigurieren können.



Wie überwacht man IPsec-Tunnelereignisse

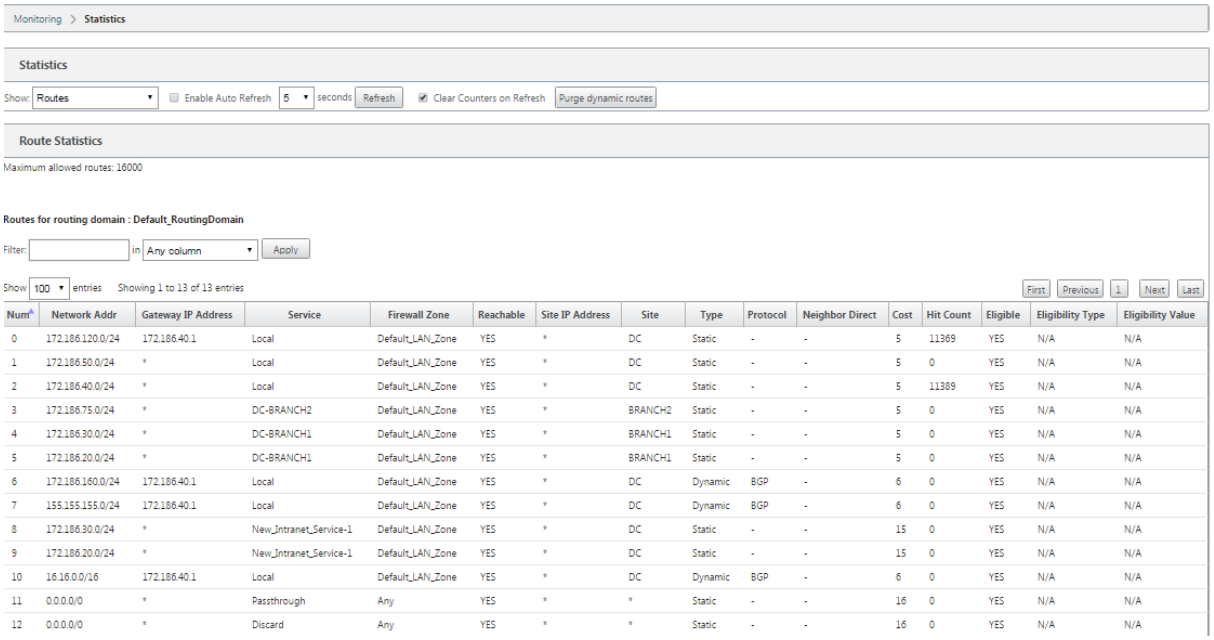
1. Navigieren Sie zu **Konfiguration > Systemwartung** > **Diagnose** > **Ereignisse**.
2. Fügen Sie Ereignisse basierend auf dem Objekttyp **IPSEC_TUNNEL** hinzu. Erstellen Sie Filter für alle IPsec-bezogenen Ereignisse.



Berechtigung für nicht-virtuelle IPsec-Pfadrouten

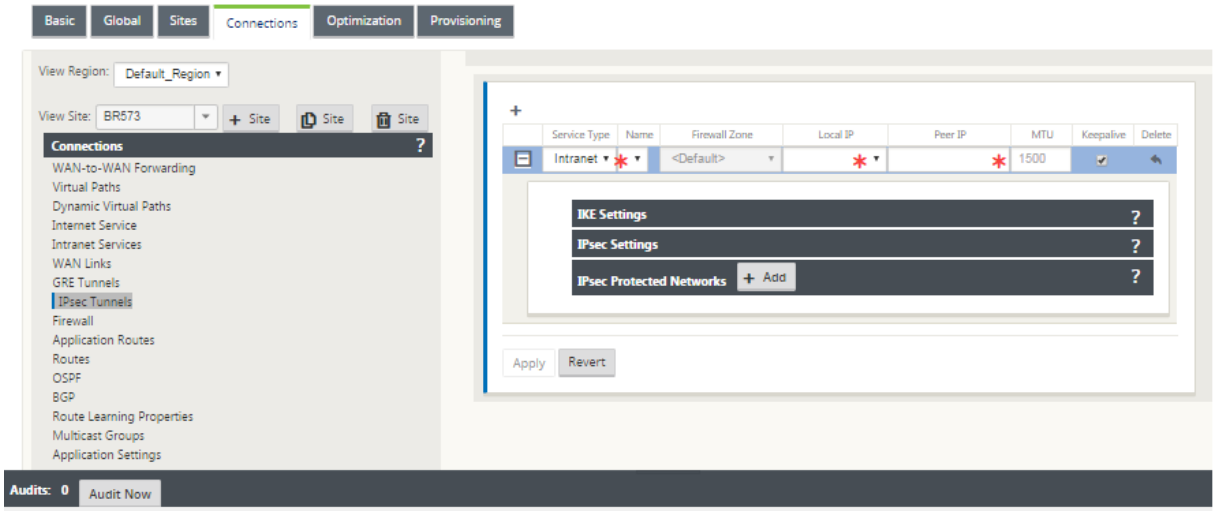
October 28, 2021

In früheren Versionen blieben ipsec-Tunnelrouten in der Routentabelle, selbst wenn der Tunnel nicht verfügbar wäre.



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

Die Verwendung der Keepalive-Option unter **Verbindungen** > [Site-Name] > **IPSec-Tunnel** verbessert dieses Verhalten, sodass die nicht-virtuellen IPSec-Pfadrouten jetzt als nicht förderfähig betrachtet 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.



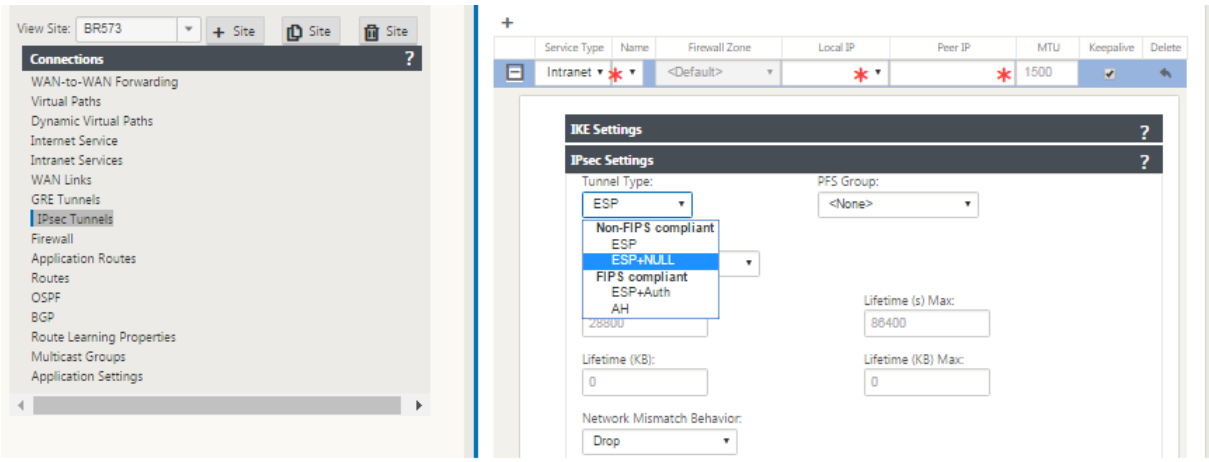
IPsec-Null-Verschlüsselung

October 28, 2021

In früheren Versionen wurde der Tunneltyp ESP+NULL eingeführt. Bei Verwendung des IPSec ESP-Protokolls wird der Datenverkehr normalerweise verschlüsselt und authentifiziert. Sie können sich je-

doch dafür entscheiden, keine Verschlüsselung zu verwenden, indem Sie die Nullverschlüsselung verwenden. Beim 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

October 28, 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 Audit-Fehler für FIPS-basierte Lebensdauereinstellungen durch

So aktivieren Sie die FIPS-Konformität mit der Citrix SD-WAN GUI:

1. Gehen Sie zu **Konfiguration** > **Virtuelles WAN** > **Konfigurationseditor** > **Global**und wählen Sie **FIPS-Modus aktivieren**aus.

Das Aktivieren des FIPS-Modus erzwingt Überprüfungen während der Konfiguration, um sicherzustellen, dass alle IPSec-bezogenen Konfigurationsparameter den FIPS-Standards entsprechen. Sie werden durch Audit-Fehler und Warnungen zur Konfiguration von IPsec aufgefordert.

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:

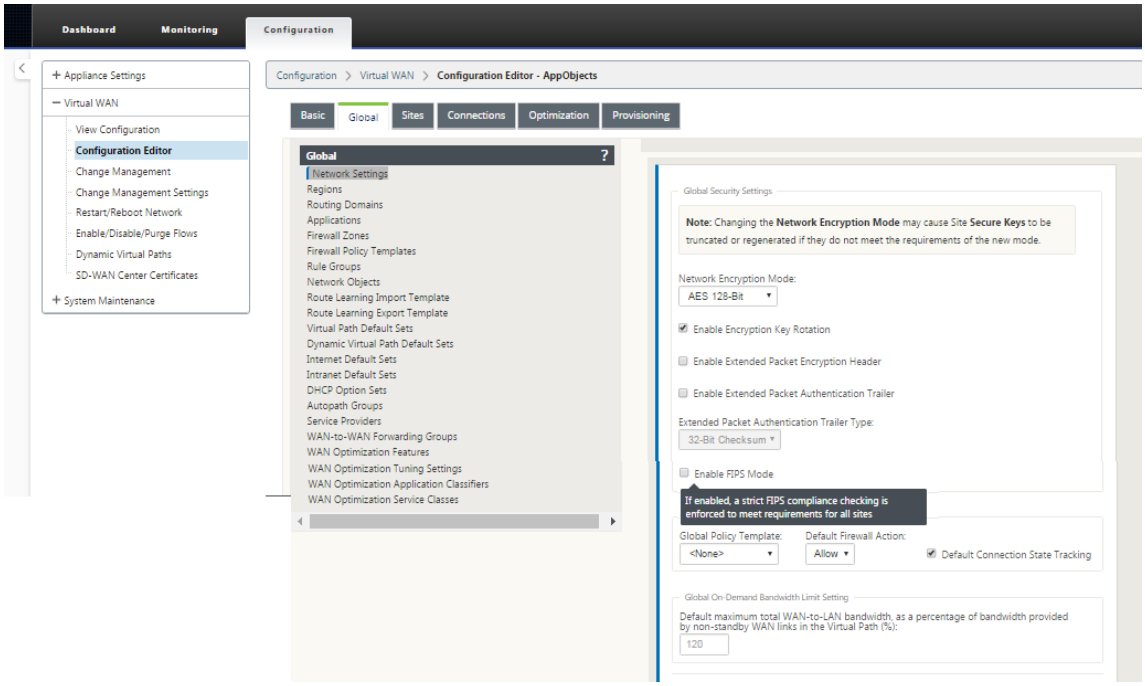
- DH Gruppe 19: ECP256 (256-Bit Elliptische Kurve) für Schlüsselaushandlung
- 256-Bit-AES-CBC-Verschlüsselung
- SHA256-Hashing für die Nachrichtenauthentifizierung
- SHA256-Hashing für Nachrichtenintegrität
- DH Gruppe 2: MODP-1024 für perfekte Vorwärtsgeheimnis

Verwenden Sie die folgenden Einstellungen, um IPsec-Tunnel für einen Drittanbieter zu konfigurieren:

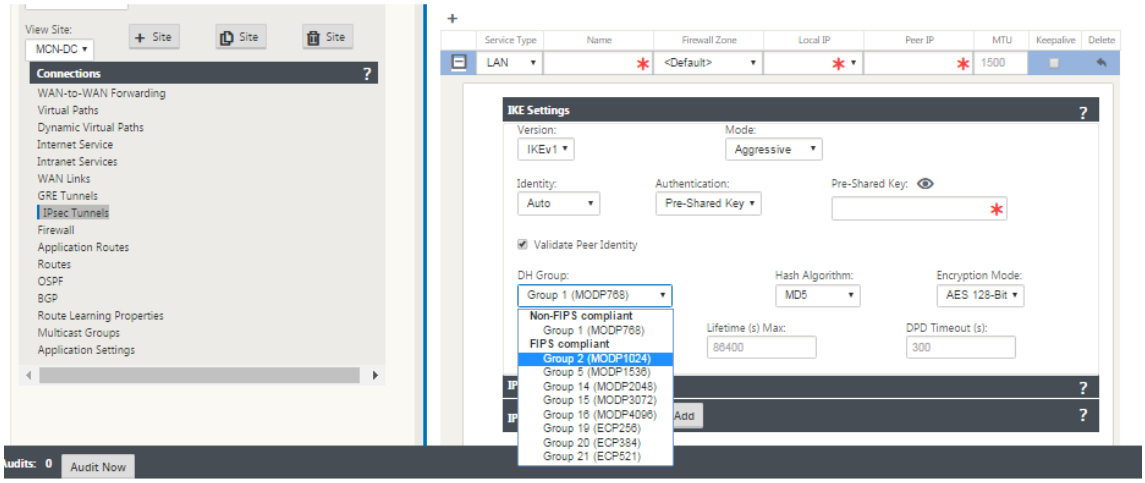
1. Konfigurieren Sie die FIPS-genehmigte DH-Gruppe Die Gruppen 2 und 5 sind unter FIPS zulässig, jedoch werden Gruppen 14 und höher dringend empfohlen.
2. Konfigurieren Sie die FIPS-genehmigte Hash-Funktion. SHA1 wird von FIPS akzeptiert, jedoch wird SHA256 dringend empfohlen.
3. Konfigurieren Sie bei Verwendung von IKEv2 eine FIPS-zugelassene 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 eine maximale Lebensdauer von nicht mehr als acht Stunden (28.800 Sekunden).

So konfigurieren Sie IPsec-Tunnel:

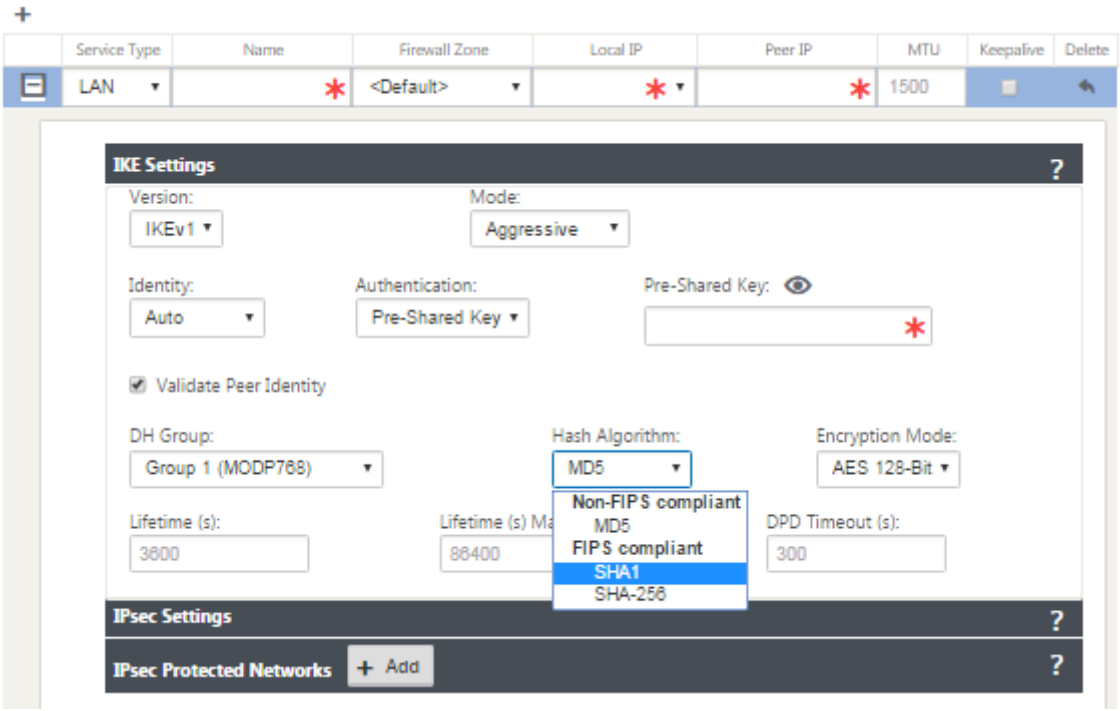
1. Wechseln Sie auf der MCN-Appliance zu **Konfiguration** > **Virtuelles WAN** > **Konfigurationseditor**. Öffnen Sie ein vorhandenes Konfigurationspaket. Gehen Sie zu **Verbindungen** > **IPSec-Tunnel**.



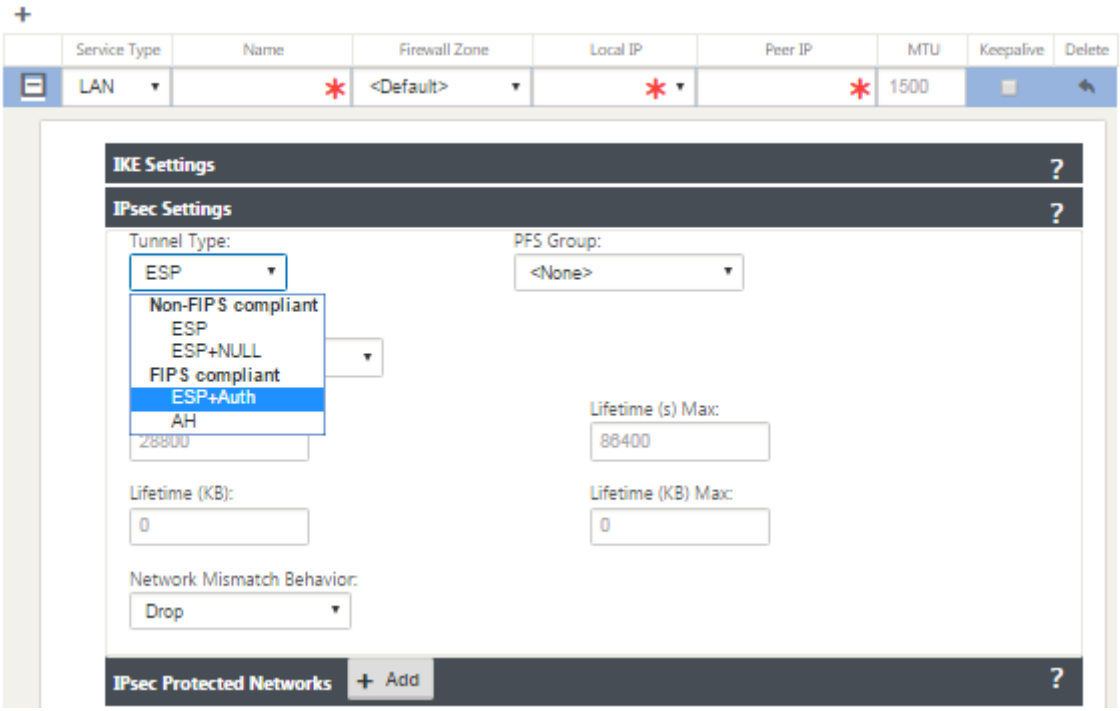
2. Gehen Sie zu **Verbindungen** > **IPsec-Tunnel**. Bei Auswahl des **LAN** - oder **Intranet-Tunnels** unterscheidet der Bildschirm die FIPS-konformen Gruppen in den IKE-Einstellungen von denen, die nicht konform sind, sodass Sie die FIPS-Konformität einfach konfigurieren können.



Der Bildschirm zeigt auch an, ob der Hash-Algorithmus FIPS-konform ist, wie in der folgenden Abbildung gezeigt.



FIPS-Konformitätsoptionen für IPsec-Einstellungen:



Wenn die IPsec-Konfiguration bei Aktivierung nicht den FIPS-Standards entspricht, kann ein Überwachungsfehler ausgelöst werden. Im Folgenden sind die Arten von Audit-Fehlern aufgeführt, die in der GUI angezeigt werden.

- Wenn der FIPS-Modus aktiviert ist und die nicht FIPS-konforme 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 Standardsatz des virtuellen Pfads ebenfalls aktiviert ist und der falsche Tunnelmodus ausgewählt ist (ESP vs ESP_Auth/AH).
- Wenn der FIPS-Modus aktiviert ist, werden die IPsec-Einstellungen für den Standardsatz des virtuellen Pfads ebenfalls aktiviert und ein falscher Lebenszeitwert wird eingegeben.

Secure Web Gateway für Citrix SD-WAN

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 auf den Sites aufrechtzuerhalten. Und wenn Sie viele Zweigstellen haben, wird das Kostenmanagement unpraktisch.

Zscaler:

Die ideale Lösung zur Durchsetzung der Sicherheit ohne zusätzliche Kosten, Komplexität oder Latenz besteht darin, den gesamten Internetverkehr der Zweigstelle von der Citrix SD-WAN Appliance an die Zscaler Cloud Security Platform zu leiten. Sie können dann eine zentrale Zscaler-Konsole verwenden, um granulare 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 Cloud-basiert ist, müssen Sie dem Netzwerk keine weiteren Sicherheitsgeräte hinzufügen.

FIPS-Konformität:

Das Nationale Institut für Standards und Technologie (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 Schutz sensibler Informationen.

FIPS legt die Sicherheitsanforderungen für ein kryptografisches Modul fest, das in Sicherheitssystemen verwendet wird. Um diese Sicherheitsstandards auf die von einer Citrix SD-WAN-Appliance durchgeführte Verarbeitung anzuwenden, konfigurieren Sie den FIPS-Modus.

Forcepoint:

Mithilfe von Citrix SD-WAN können Sie die Firewall-Umleitung (transparenter Proxy von Destination NAT) verwenden, um den Internetverkehr (HTTP und HTTPS) von einer SD-WAN-Appliance am Unternehmens-Edge auf das Cloud-gehostete 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-Proxyservers 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.

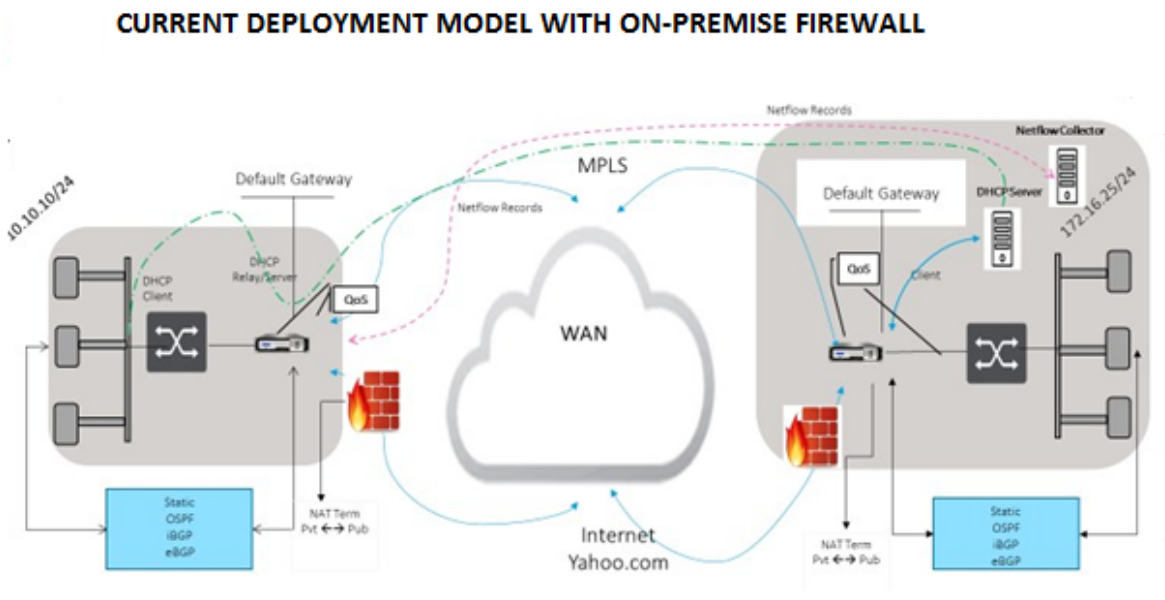
Citrix SD-WAN-Appliances können über GRE-Tunnel am Standort des Kunden eine Verbindung zu einem Zscaler-Cloud-Netzwerk herstellen. Eine Zscaler-Bereitstellung mit SD-WAN-Appliances unterstützt die folgenden Funktionen:

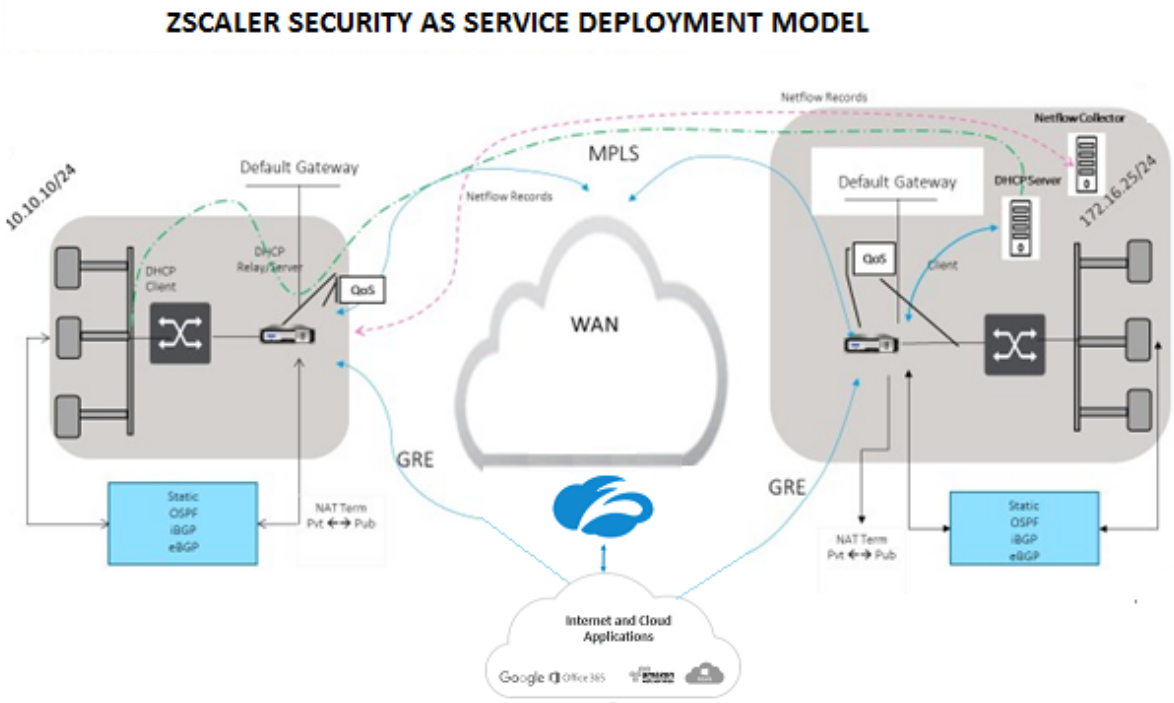
- Weiterleiten des gesamten GRE-Datenverkehrs an Zscaler, wodurch ein direktes Internetbreakout möglich ist.
- Direkter Internetzugang (DIA) mit Zscaler pro Kundenstandort.
  - Auf einigen Websites möchten Sie DIA möglicherweise on-premises Sicherheitsausrüstung zur Verfügung stellen und Zscaler nicht 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

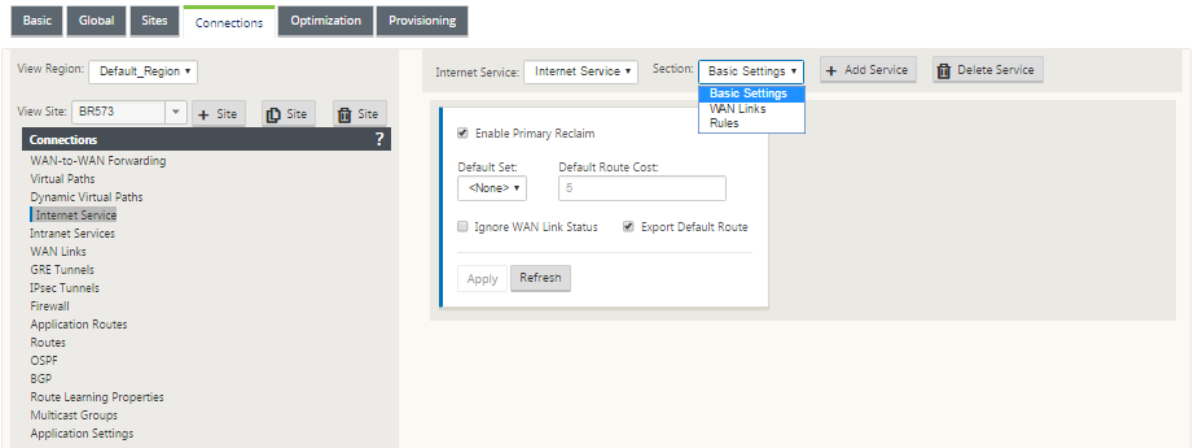
- WAN-Links
- Regeln

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:

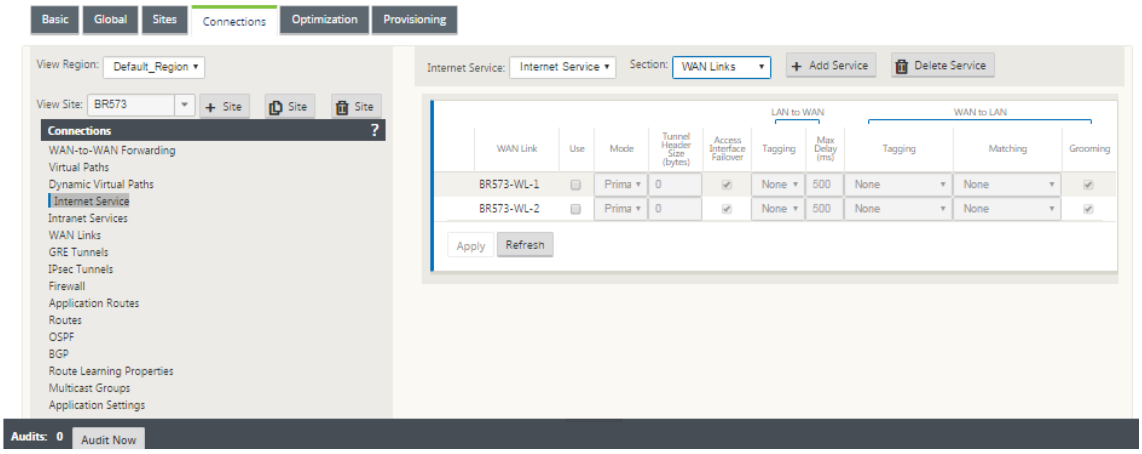
- **Benutzen**: Erlauben Sie dem Dienst, diesen WAN-Link zu verwenden. Wenn Verwenden deaktiviert ist, sind alle anderen Optionen nicht verfügbar.
- **Modus**: Der Modus des Dienstes —Primär, Sekundär oder Balance, für Verkehrsredundanz oder Lastausgleich.
- **Tunnelkopfgröße (Byte)**: Die Größe des 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

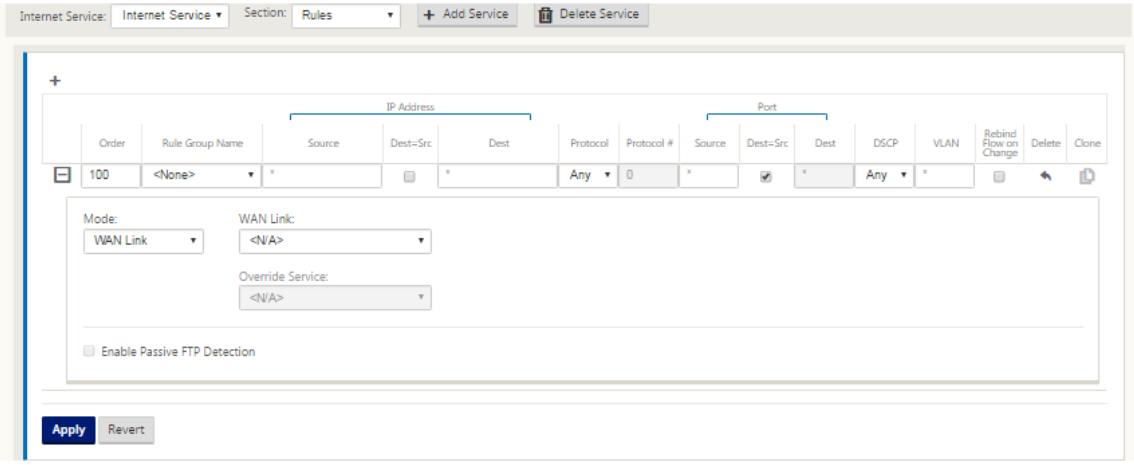
Der Internetverkehr wird anhand der definierten Regeln identifiziert. Eine Regeldefinition wird verwendet, um einen bestimmten Verkehrsfluss abzugleichen. Nach dem Abgleich müssen Sie die Aktion definieren, um den Verkehrsfluss zu beantragen.

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:

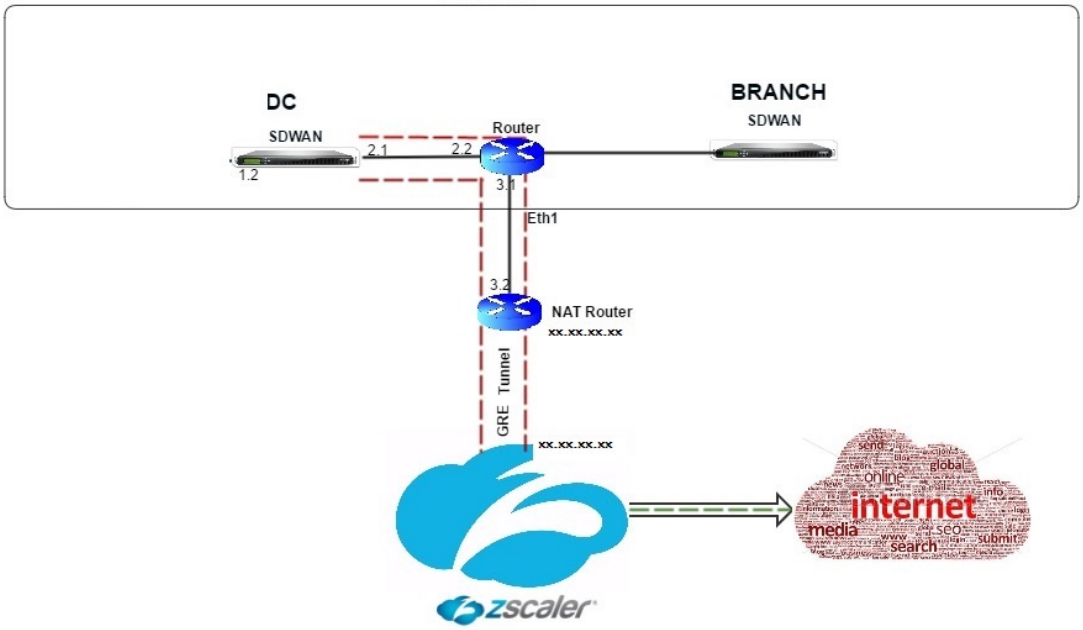
- **WAN-Verbindung**: Die WAN-Verbindung, die von Flows verwendet wird, die der Regel entsprechen, wenn der Internet-Lastausgleich aktiviert ist.
- **Dienst überschreiben**: Der Zieldienst für Flows, die der Regel entsprechen.
  - **Verwerfen**: Lass den Verkehr fallen.
  - **Passthrough**: Ordnen Sie den Fluss dem Passthrough zu und lassen Sie den Datenverkehr unverändert durch die Appliance fließen.



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.

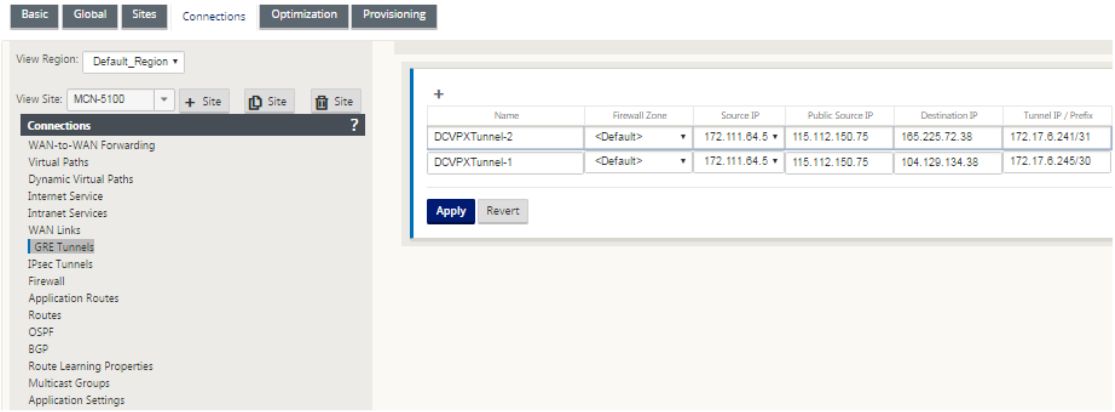
3. Die Quell-IP-Adresse und die Ziel-IP-Adresse sind die GRE-Header des Routers, wenn die ursprüngliche Nutzlast gekapselt ist.
4. Tunnel-IP-Adresse und Präfix sind die IP-Adressierung im GRE-Tunnel selbst. Dies ist nützlich, um den Verkehr über den GRE-Tunnel zu leiten. Der Verkehr benötigt diese IP-Adresse 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.



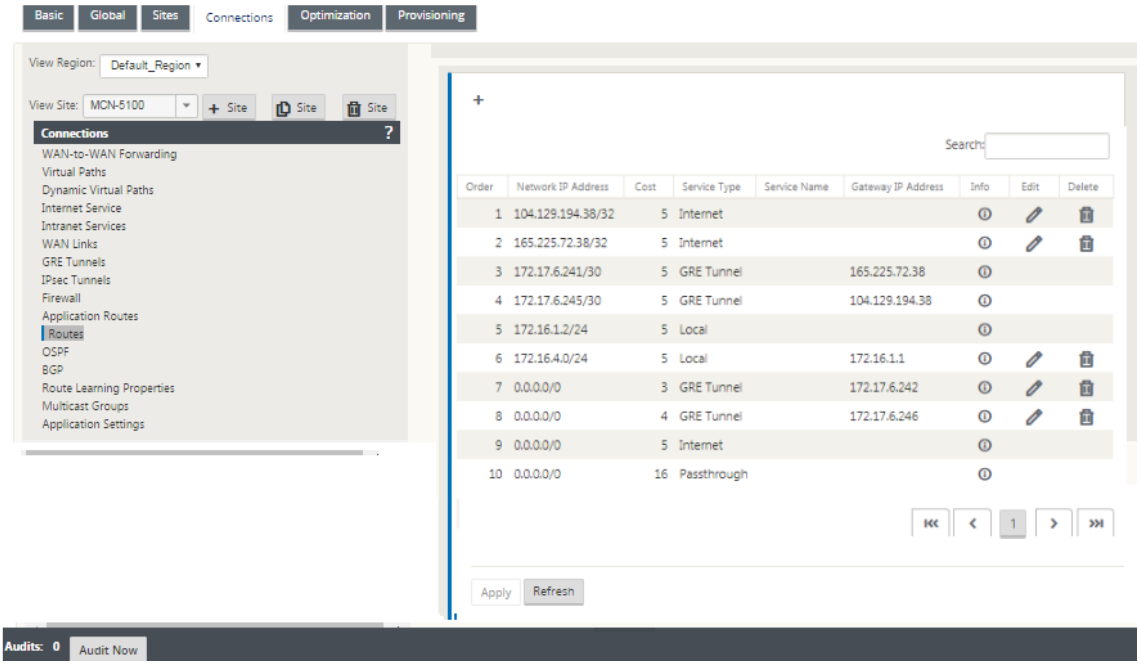
Konfigurieren von Routen für GRE-Tunnel

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.



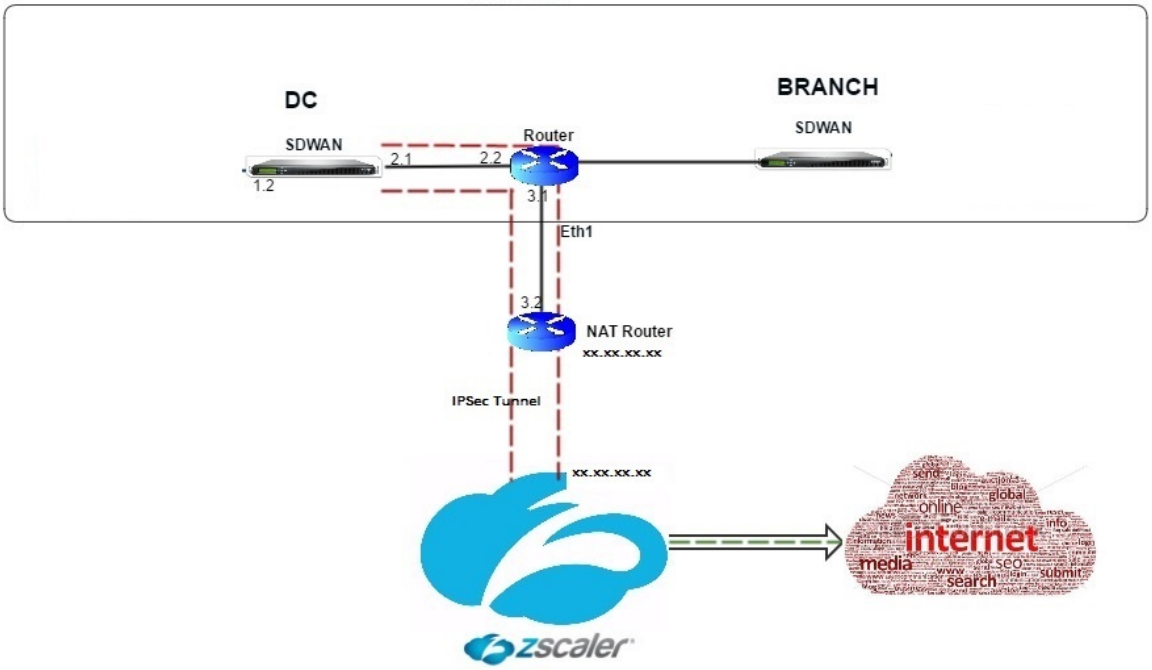
> **Hinweis**
>
> Wenn Sie keine spezifischen Routen für die Zscaler-IP-Adresse haben, konfigurieren Sie das Routenpräfix 0.0.0.0/0 so, dass es mit der ZEN-IP-Adresse übereinstimmt, und leiten Sie es durch eine GRE-Tunnelkapselungsschleife. Diese Konfiguration verwendet die Tunnel in einem Aktiv-Backupmodus. Mit den in der obigen Abbildung dargestellten Werten wech-

> selt 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 Internetzugriff 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

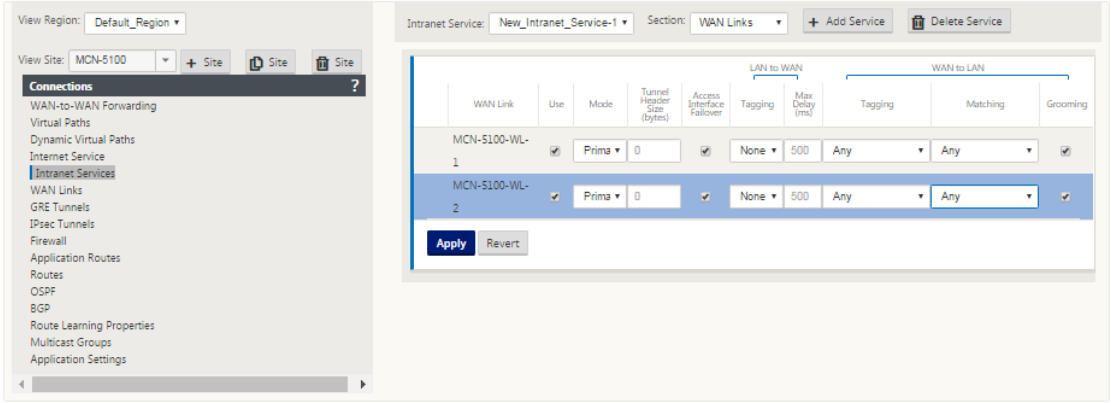
- Mehrere VRF-Bereitstellungen werden nicht unterstützt.
- Primäre Backup-GRE-Tunnel werden nur für einen Entwurfsmodus mit hoher Verfügbarkeit unterstützt.

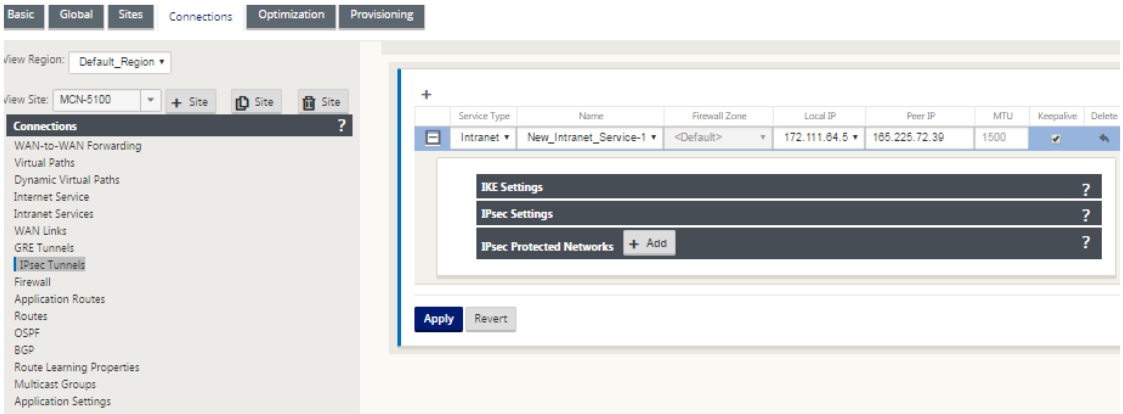
Konfigurieren von IPsec-Tunnels



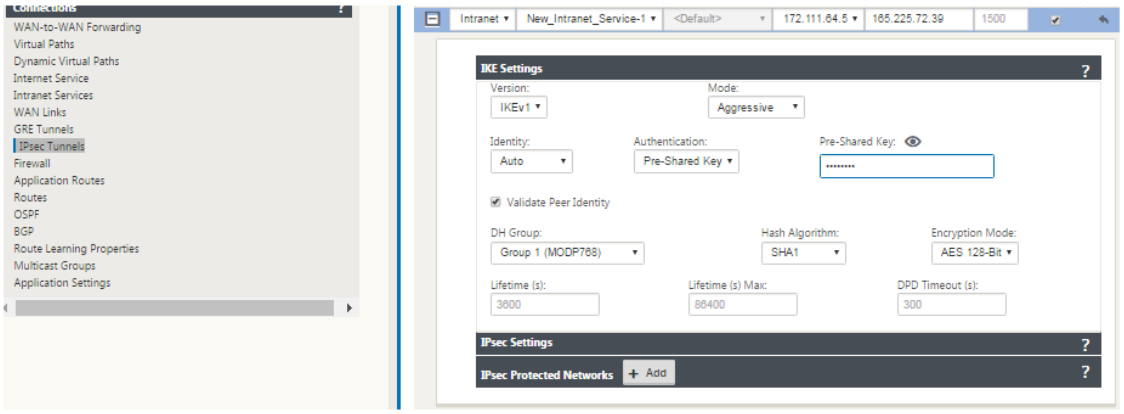
So konfigurieren Sie IPsec-Tunnel für Intranet- oder LAN-Dienste in der Benutzeroberfläche der Citrix SD-WAN Appliance:

1. Navigieren Sie im Konfigurationseditor zu **Verbindungen** > <**SiteName**> > **IPsec-Tunnel** und wählen Sie einen 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.
3. Wählen Sie die verfügbare lokale IP-Adresse aus und geben Sie die Peer-IP-Adresse für den virtuellen Pfad zum Remote-Peer ein.





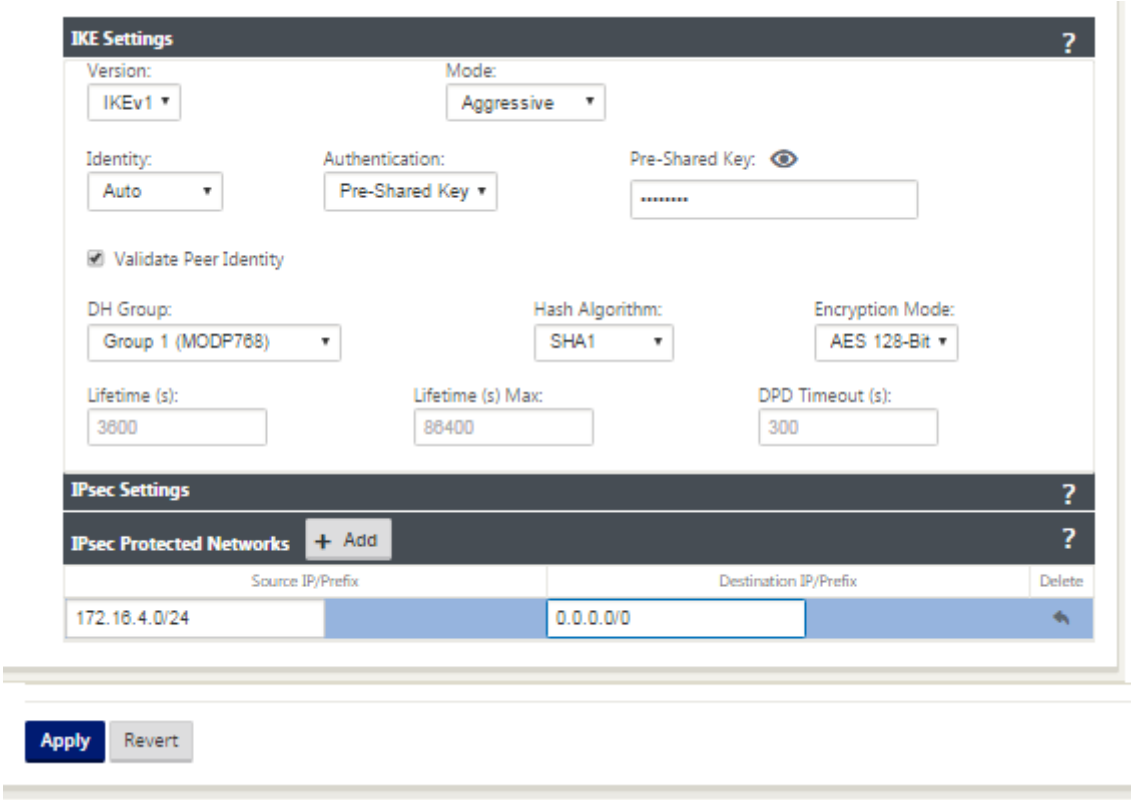
4. Wählen Sie **IKEv1** für **IKE-Einstellungen**. Zscaler unterstützt nur IKEv1.



5. Wählen Sie unter IPsec-Einstellungen **ESP-NULL** für **Tunneltyp** aus, um den Datenverkehr über

den IPsec-Tunnel nach Zscaler umzuleiten. Der IPsec-Tunnel verschlüsselt den Datenverkehr nicht.

6. Da der Internetverkehr umgeleitet wird, kann die Ziel-IP/das Präfix eine beliebige IP-Adresse sein.

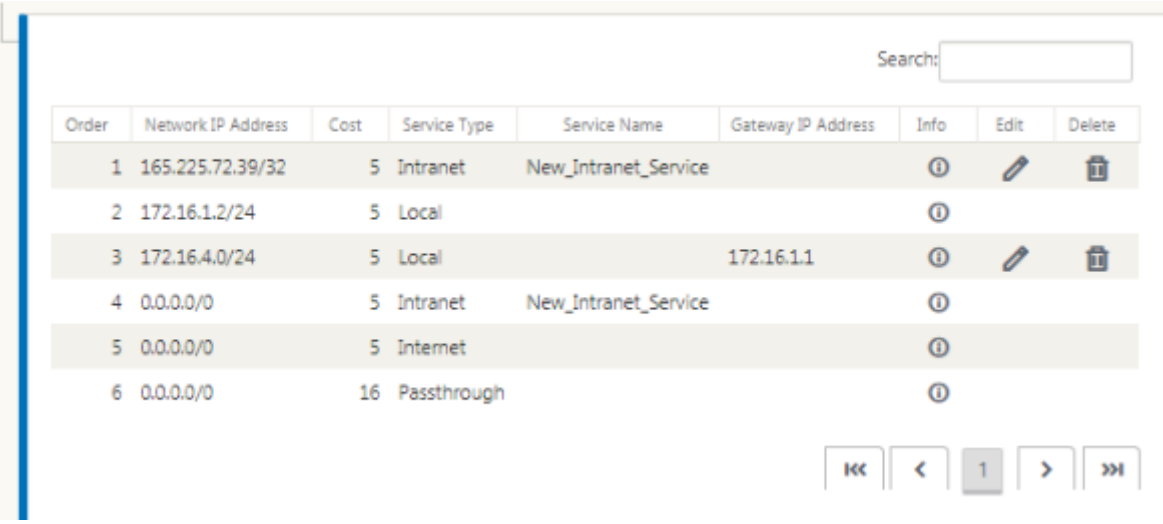


Weitere Informationen zum Konfigurieren von IPSec-Tunneln mit der Citrix SD-WAN-Weboberfläche finden Sie unter IPSec-Tunnel.

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.



So überwachen Sie GRE- und IPsec-Tunnelstatistiken:

Navigieren Sie im SD-WAN-Webinterface zu **Überwachung** > **Statistiken** > [**GRE-Tunnel** **IPsec-Tunnel**].

Weitere Informationen finden Sie unter Überwachung von IPSec-Tunneln und GRE-Tunneln.

Unterstützung der Firewall-Verkehrsumleitung mithilfe von Forcepoint in Citrix SD-WAN

October 28, 2021

Forcepoint unterstützt die folgenden Funktionen, obwohl SD-WAN nur die Firewall-Umleitungsfunktion unterstützt:

- IPSec mit PKI
- IPSec mit PSK
- Proxy-Verkettung mithilfe der PAC-Dateikonfiguration
- Proxy-Verkettung mit Standardüberschriften
- Proxy-Chaining mit proprietären Headern macht die Konfiguration des IP-Bereichs des Clients überflüssig - Partnerschaft/Entwicklung
- Firewall-Umleitung (transparenter Proxy von Destination NAT)

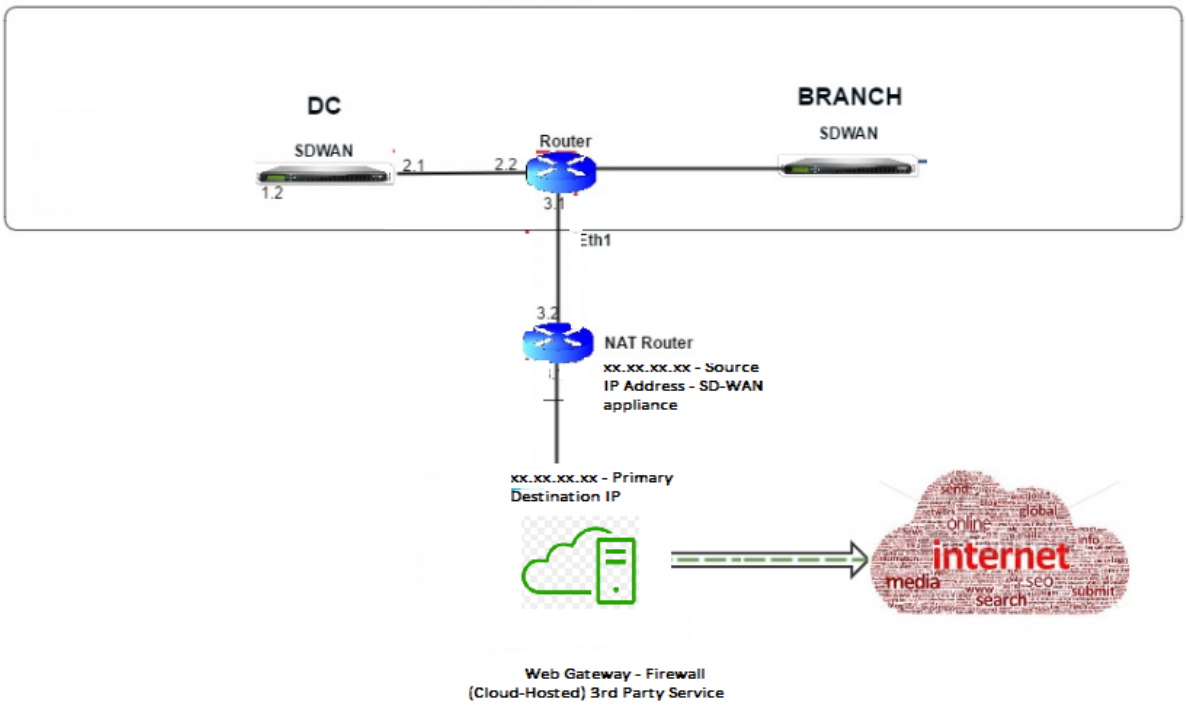
Die Ziel-NAT-Richtlinie ermöglicht es Unternehmen, den Internetverkehr mithilfe von ForcePoint über einen in der Cloud gehosteten Sicherheitsdienst weiterzuleiten.

Lesen Sie den folgenden Anwendungsfall, um zu verstehen, wie Sie Ziel-NAT in SD-WAN-Appliances konfigurieren und den Internetverkehr über einen sicheren Cloud-basierten Firewall-Dienst umleiten.

Voraussetzungen:

1. Melden Sie sich auf der Forcepoint-Portalseitean. Erstellen Sie eine Richtlinie, indem Sie die öffentliche Enterprise-IP-Adresse angeben, über die der Internetverkehr an Forcepoint umgeleitet werden muss. Besorgen Sie sich die primären und sekundären IP-Adressen, auf 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 mit WAN-Verbindungen verknüpft ist.
3. Die Ziel-NAT wird unter Verwendung der Ziel-IP-Adresse des Internetverkehrs durchgeführt. Diese Zieladresse wird in die öffentliche IP-Adresse von Forcepoint 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 an die primäre Ziel-IP-Adresse des Cloud-basierten Firewall-Gateways mit externen Ports 8081 (http) bzw. 8443 (https) umgeleitet/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 Konfigurieren von NAT



Konfigurieren von Ziel-NAT (DNAT)

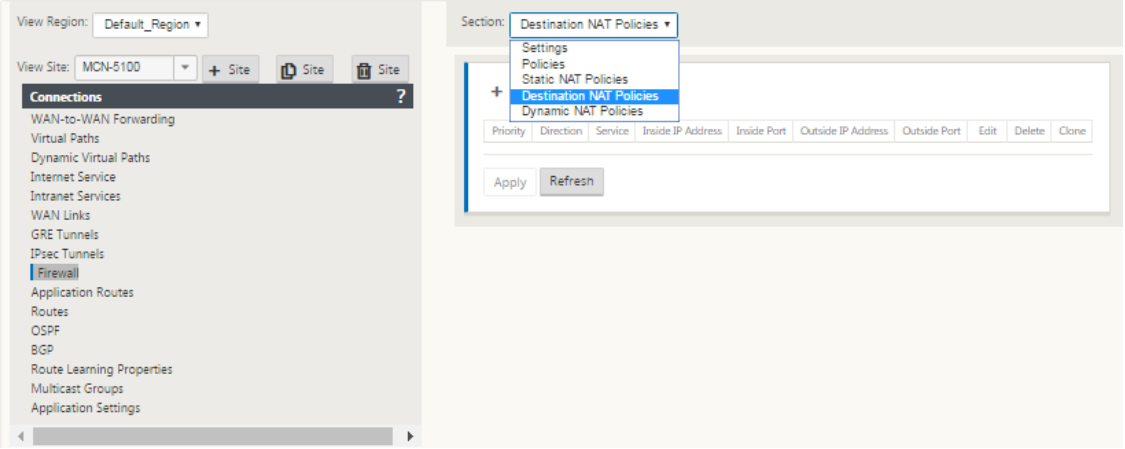
Verwenden Sie die Citrix SD-WAN GUI, um Destination NAT (DNAT) zu konfigurieren. Fügen Sie in der Konfiguration eine oder mehrere DNAT-Richtlinien hinzu, die den Datenverkehr umleiten, der einer bestimmten Ziel-IP-Adresse und einem bestimmten Zielport entspricht.

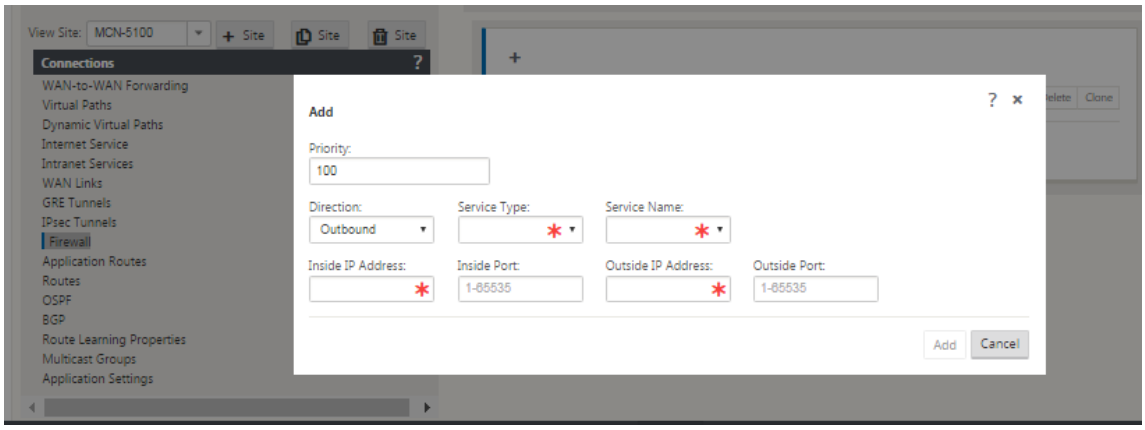
So konfigurieren Sie Destination NAT:

Wechseln Sie in der SD-WAN SE/VPX GUI zu **Konfiguration** -> **Virtual WAN** -> Konfigurationseditor. Klicken Sie auf **Öffnen**, um ein vorhandenes Paket zu öffnen. Wählen Sie ein gespeichertes Konfigurationspaket. Sie können auch DNAT-Regeln erstellen, während Sie die Netzwerkkonfiguration erstellen.

1. Konfigurieren Sie im DC (MCN) den Internetdienst. Gehe 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
    - Dienstname
    - Innen-IP-Adresse
    - Innen-Port

- Außen-IP-Adresse
- Außen-Port





4. Bereitstellung von Ziel-NAT-Regeln für die Weiterleitung des Firewall-Datenverkehrs, ähnlich wie bei statischer NAT.
5. Geben Sie die übereinstimmenden Kriterien und die Ziel-IP/Port ein, für die NAT angewendet werden soll.
6. Führen Sie den Verbindungsabgleich der DNAT-Regel mit Statistiken durch.
7. Entfernen oder aktualisieren Sie DNAT Regeln während des Konfigurationsupdates.

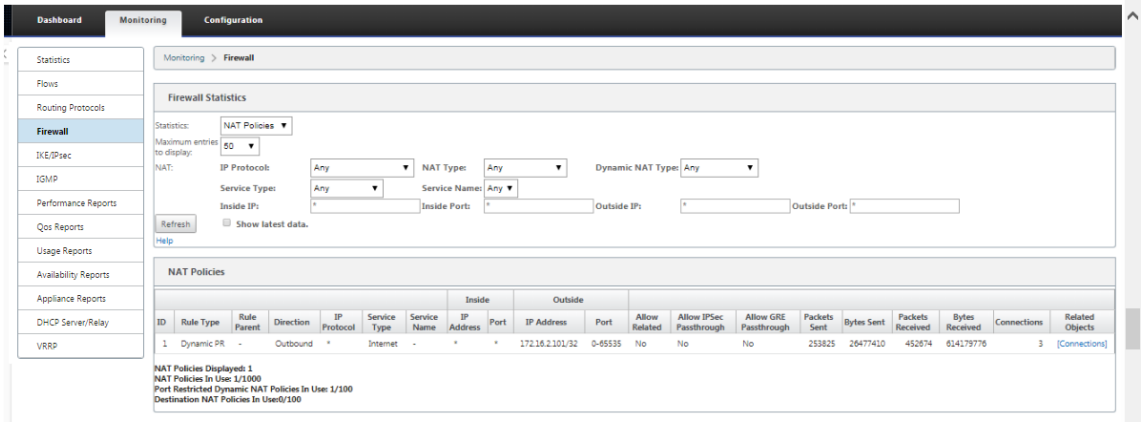
Überwachen einer Ziel-NAT-Richtlinie (Firewall)

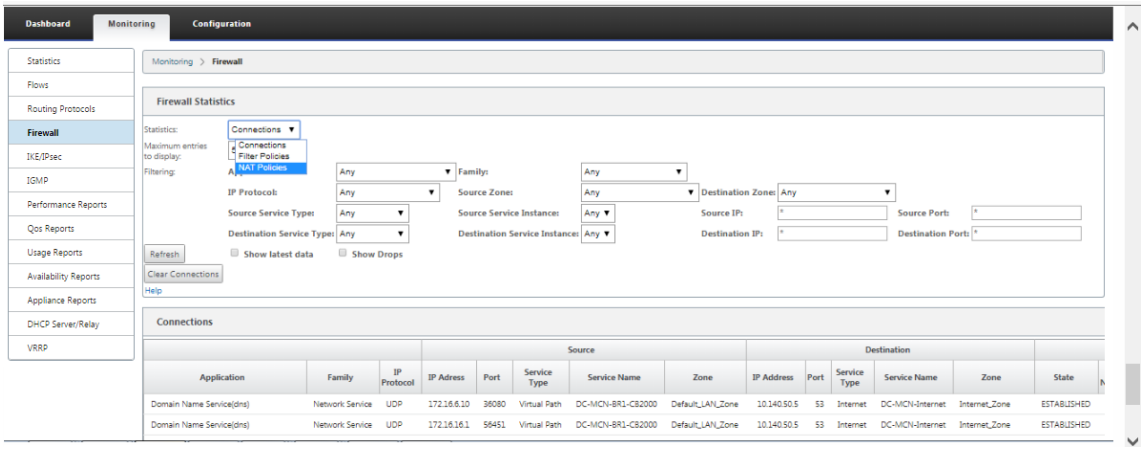
Sie können auch die Citrix SD-WAN GUI verwenden, um die aktuelle DNAT-Richtlinienkonfiguration zu überwachen.

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 aus, die die Statistiken enthält, die Sie überwachen möchten.





Palo Alto Integration mit IPsec-Tunneln

October 28, 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 Remotestandort. 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 bieten und gleichzeitig die Einführung eines teuren Sicherheitsstapels in jeder Filiale 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 im Citrix SD-WAN Center konfigurieren.

Bevor Sie mit der Konfiguration des Prisma Access Service für Remote-Netzwerke beginnen, stellen Sie sicher, dass Sie über die folgende Konfiguration verfügen, um sicherzustellen, dass Sie den Dienst erfolgreich aktivieren und Richtlinien für Benutzer an Ihren Remote-Netzwerkstandorten durchsetzen können:

1. **Service-Verbindung**—Wenn Ihre Remote-Netzwerkstandorte Zugriff auf die Infrastruktur in Ihrer Unternehmenszentrale benötigen, um Benutzer zu authentifizieren oder den Zugriff auf kritische Netzwerkressourcen zu ermöglichen, müssen Sie den Zugriff auf Ihr Unternehmensnetzwerk so einrichten, dass sich der Hauptsitz und die Remote-Netzwerkstandorte befinden verbunden.

Wenn der Remote-Netzwerkstandort autonom ist und an anderen Standorten keinen Zugriff auf die Infrastruktur benötigt, 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 Vorlage auf oberster Ebene (Remote_Network_Template) für den Prisma Access-Dienst für Remote-Netzwerke. Um den Prisma Access Service für Remote-Netzwerke zu konfigurieren, konfigurieren Sie die Vorlage auf oberster Ebene 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, zum 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 weiterleiten kann, müssen Sie Routing-Informationen 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. Während es praktisch sein kann, statische Routen zu verwenden, wenn Sie nur wenige Teilnetze an Ihren Remote-Netzwerkstandorten haben, ermöglicht Ihnen BGP in einer großen Bereitstellung mit vielen Remote-Netzwerken mit überlappenden Subnetzen eine einfachere Skalierung.

Netzwerk Palo Alto in SD-WAN Center

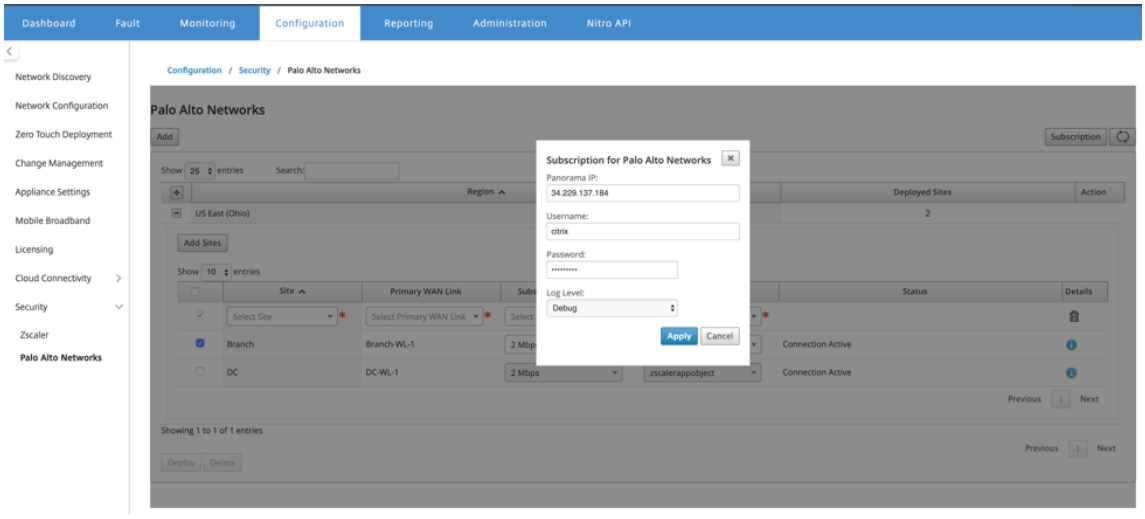
Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Beziehen Sie die Panorama-IP-Adresse vom PRISMA ACCESS-Dienst.
- 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 eingebunden ist, die bereits eine andere Site mit anderen ike/ipsec-Profilen als Citrix-IKE-Crypto-Default/Citrix-IPSec-Crypto-Standard konfiguriert hat.
- Stellen Sie sicher, dass die Prisma Access-Konfiguration nicht manuell geändert wird, wenn die Konfiguration von 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.

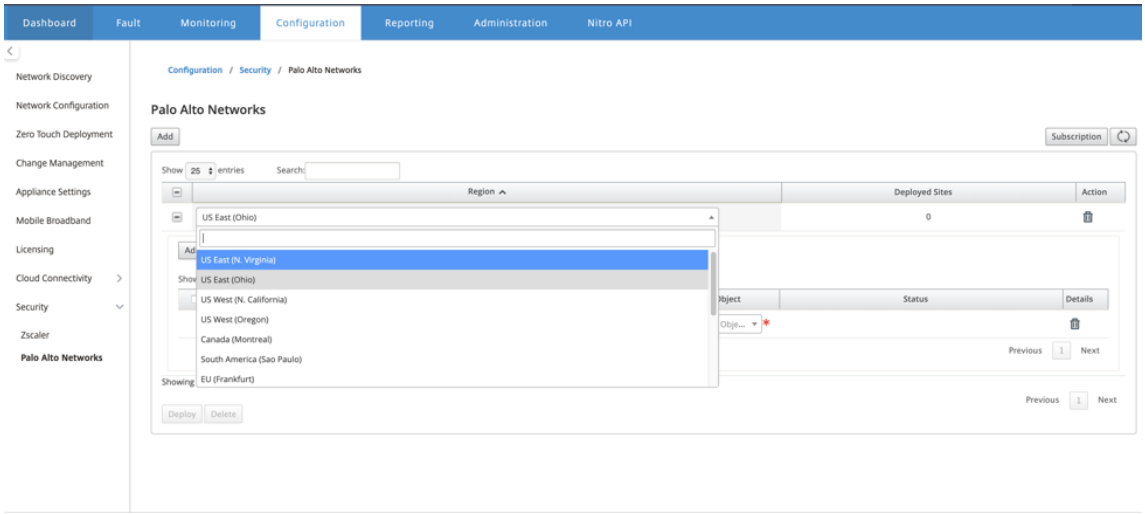


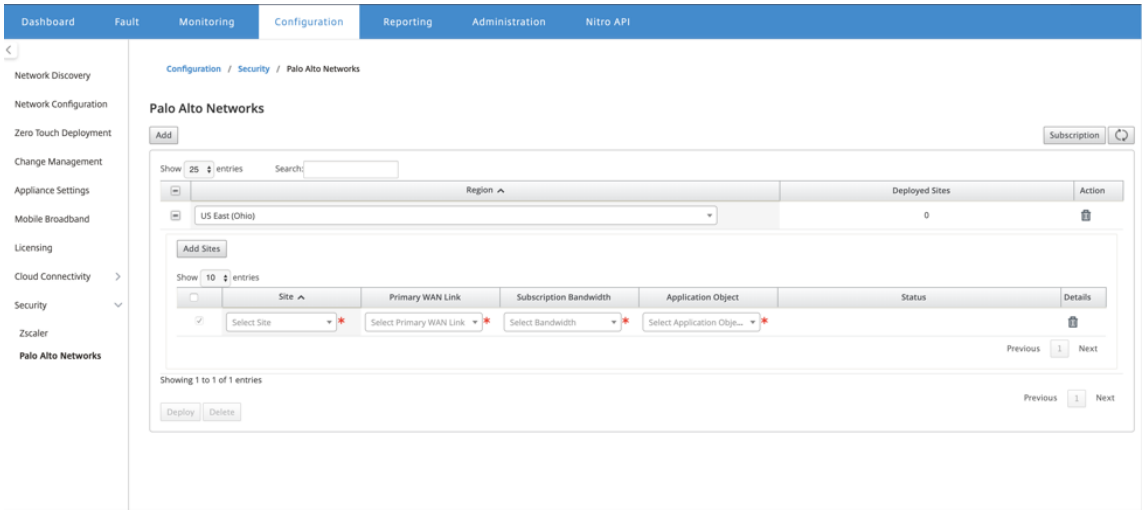
Hinzufügen und Bereitstellen von Sites

1. Um die Sites bereitzustellen, wählen Sie die PRISMA ACCESS-Netzwerkregion und den SD-WAN-Site aus, die für die Prisma Access-Region konfiguriert werden sollen, und wählen Sie dann die Standort-WAN-Verbindung, die Bandbreite und das Anwendungsobjekt für die Verkehrsauswahl aus.

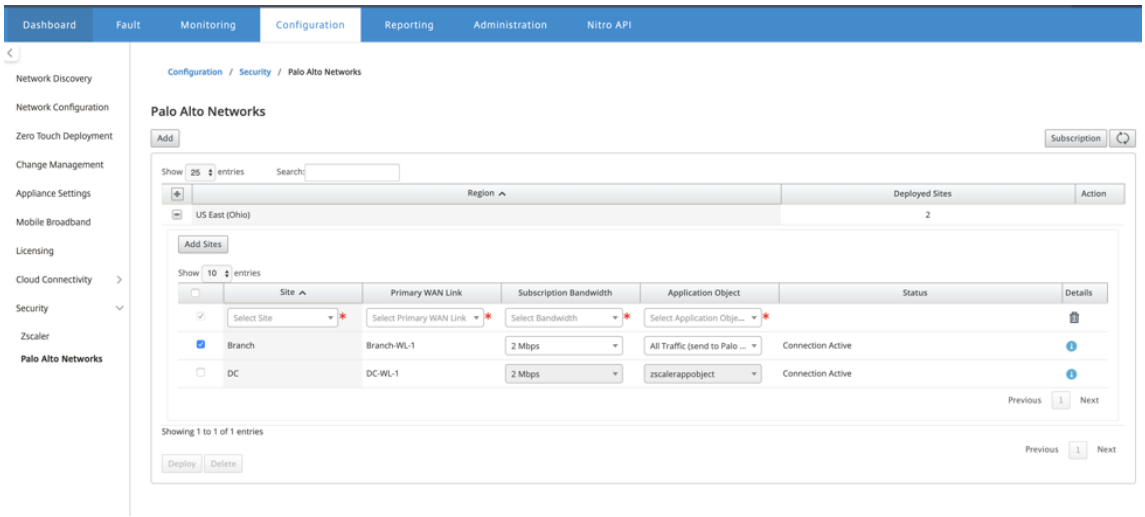
> **Hinweis:**
>
> Der Verkehrsfluss wird beeinträchtigt, wenn die gewählte Bandbreite den verfügbaren Bandbreitenbereich überschreitet.
>
> Sie können den gesamten internetgebundenen Datenverkehr an den PRISMA ACCESS-Dienst umleiten, indem Sie unter der Auswahl des Anwendungsobjekts die Option

> Gesamter **Verkehr** auswählen.

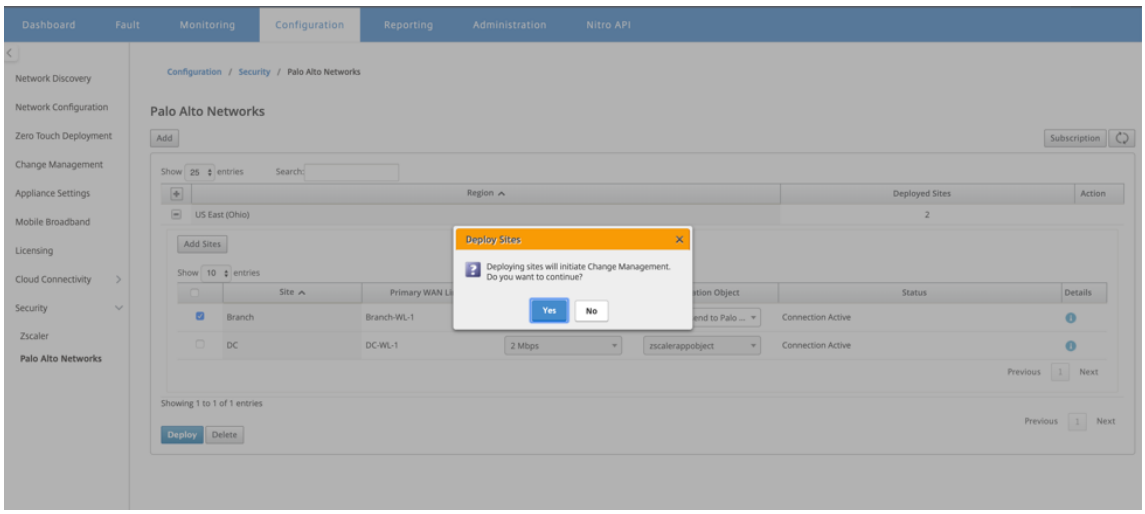




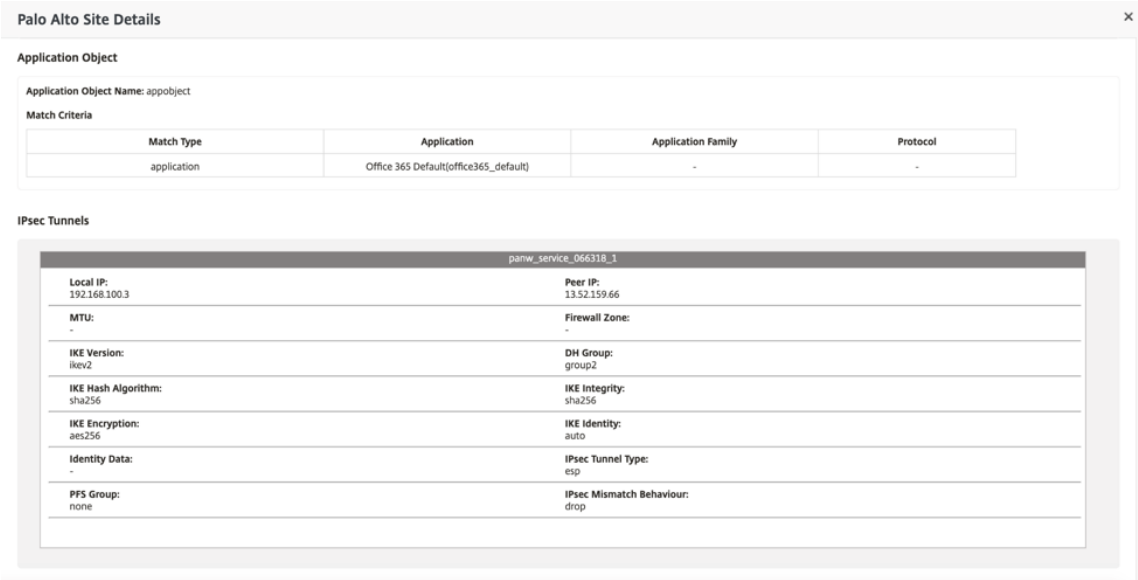
2. Sie können nach Bedarf weitere SD-WAN-Zweigstellen hinzufügen.



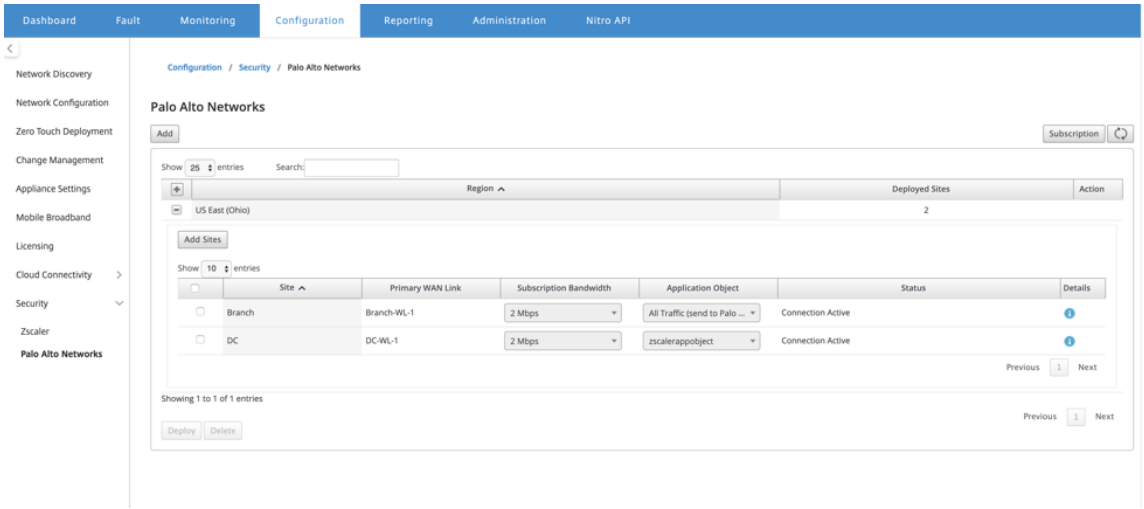
3. Klicken Sie auf **Bereitstellen**. Der Change-Management-Prozess wird eingeleitet. Klicken Sie auf **Ja** um fortzufahren.



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.
- Stellen Sie sicher, dass die Sicherheitsrichtlinie von Palo Alto auf den Verkehr auf der Registerkarte Überwachung angewendet wird.
- Überprüfen Sie, ob die Antwort von Internet zu Host in einem Zweig durchläuft.

Stateful Firewall und NAT-Unterstützung

October 28, 2021

Diese Funktion bietet eine in die SD-WAN-Anwendung integrierte Firewall. Die Firewall ermöglicht Richtlinien zwischen Diensten und Zonen und unterstützt Static NAT, Dynamic NAT (PAT) und Dynamic NAT mit Portweiterleitung. Zu den weiteren Firewall-Funktionen gehören:

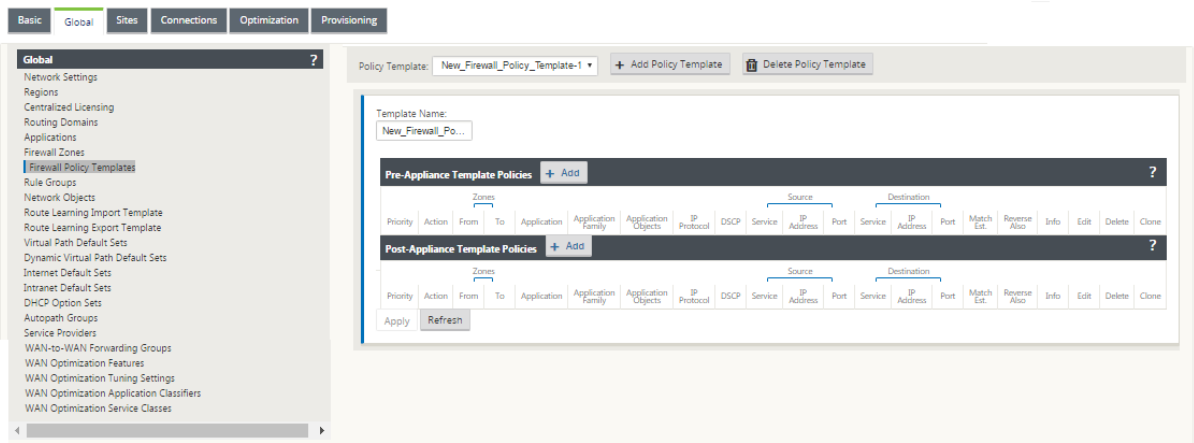
- Bieten Sie Sicherheit für den Benutzerverkehr innerhalb des SD-WAN-Netzwerks (Enterprise and Service Provider)
- (Mögliche) Reduzierung von externen Geräten (Unternehmen und Dienstleister)
- Verwendung des gleichen IP-Adressraums für mehrere Kunden: NAT Capability (Service Provider)
- Wenden Sie mehrere Firewalls aus einer globalen Perspektive an (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 Ablehnen von Flows
- Verfolgung des Flussstatus für ausgewählte Flüsse
- Anwenden von Vorlagen für globale Richtlinien
- Unterstützung für Port Address Translation für Datenverkehr ins Internet auf einem nicht vertrauenswürdigen Port sowie Port-Weiterleitung eingehender und ausgehender Port-Weiterleitung
- Bereitstellung einer statischen Netzwerkadressübersetzung (statische NAT)
- Bereitstellung einer dynamischen Netzwerkadressübersetzung (Dynamic NAT)
- Portadressübersetzung (PAT)
- Port-Weiterleitung

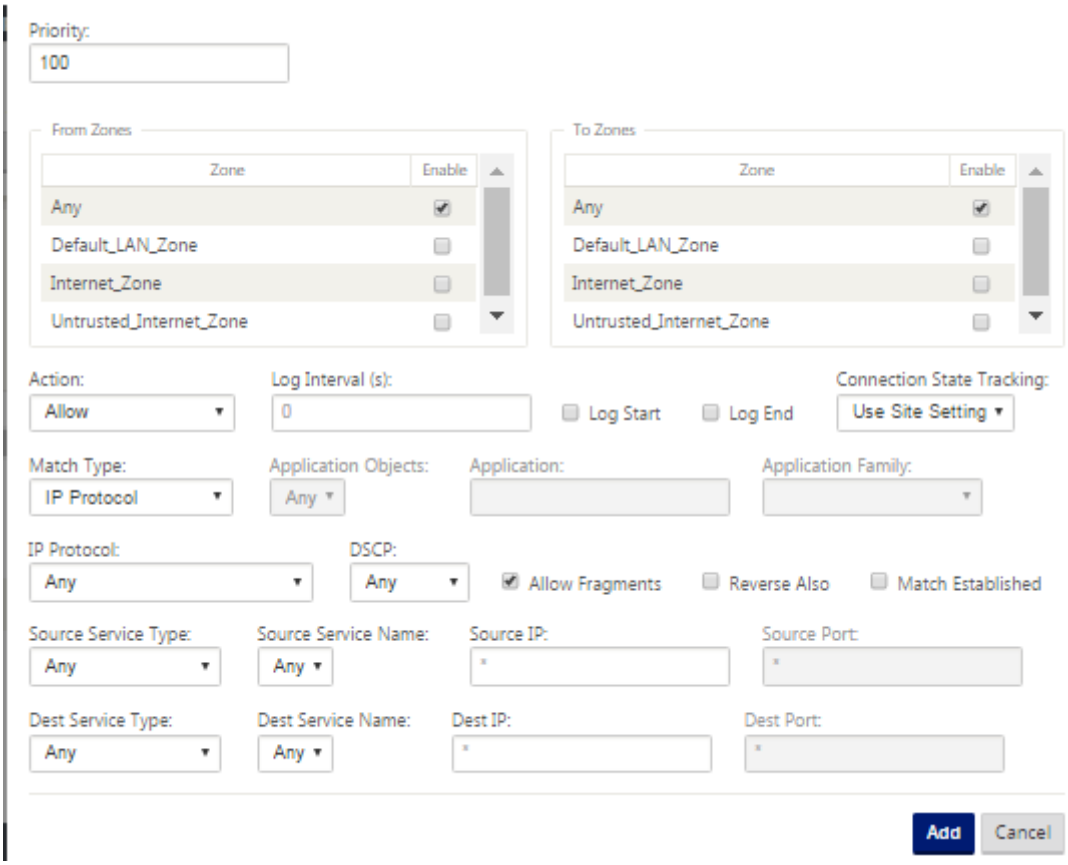
Um den Konfigurationsprozess zu vereinfachen, werden Firewall-Richtlinien auf der Ebene der globalen Konfiguration erstellt. Diese globale Konfiguration besteht aus Site-Richtlinienvorlagen vor und nach der Appliance, die auf alle Standorte innerhalb des SD-WAN-Netzwerks angewendet werden können.

> **Hinweis**
>
> Es wird aus Sicherheitsgründen nicht empfohlen, die Firewall im Fail-to-Wire-Inline-Modus zu verwenden.

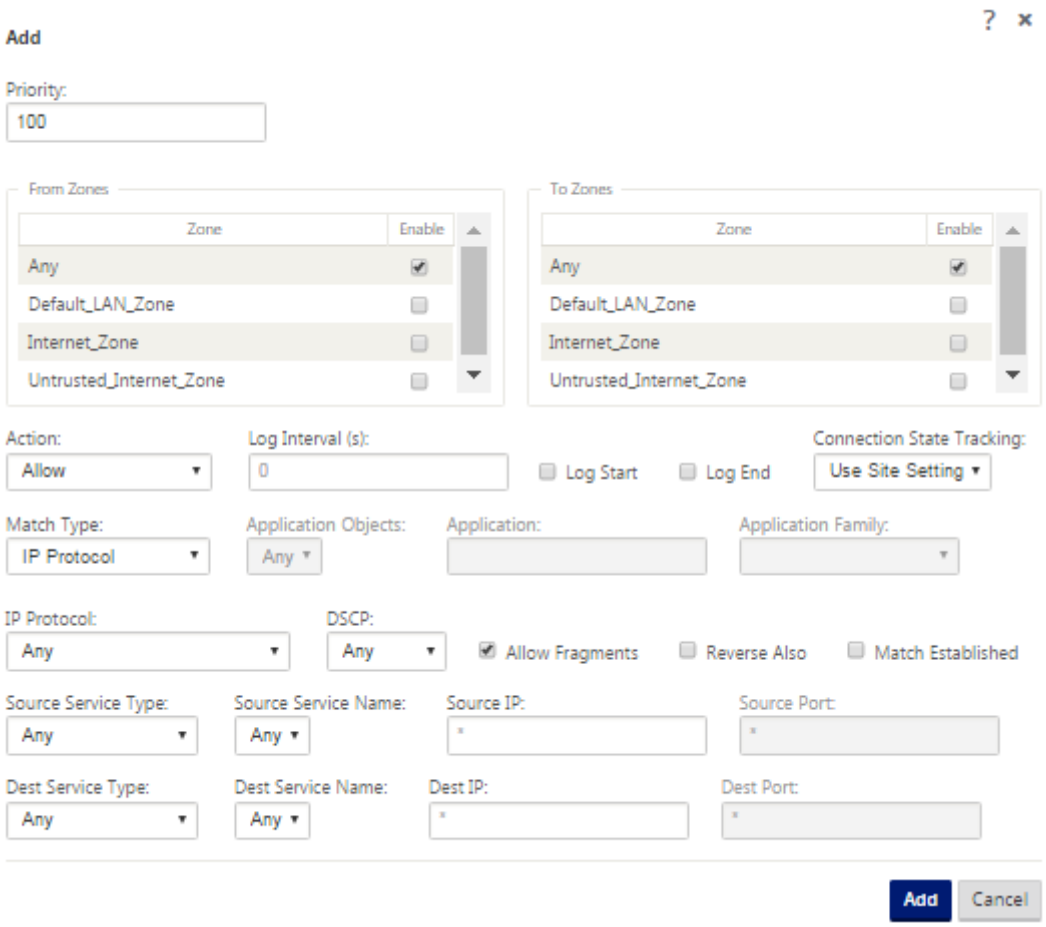
Vorlagen für globale Richtlinien



Vorlage für Vorabrichtlinien



Policy-Vorlage



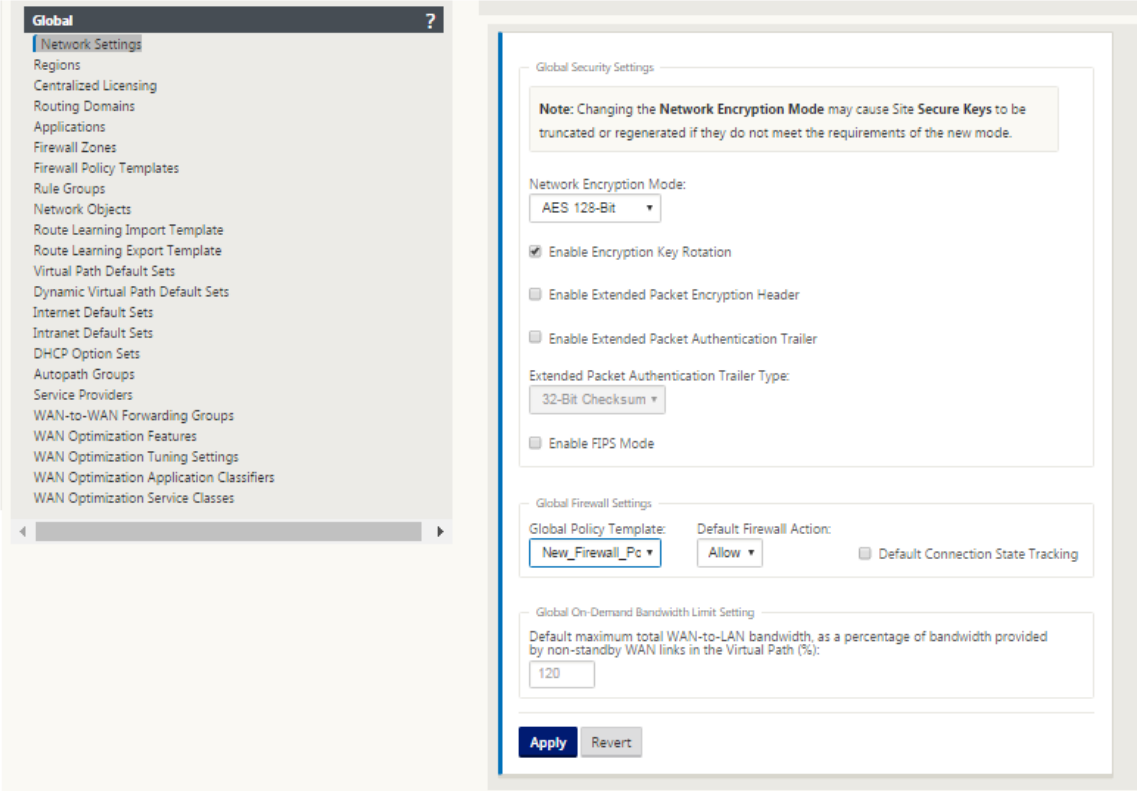
Globale Firewalleinstellungen

October 28, 2021

Nachdem Sie die Vorlagen für Firewall-Richtlinien erstellt haben, können Sie diese Richtlinie verwenden, um Firewall-Einstellungen für NetScaler SD-WAN Network zu konfigurieren. Mit den globalen Firewalleinstellungen können Sie die globalen Firewallparameter konfigurieren. Diese Einstellungen werden auf alle Sites im virtuellen WAN-Netzwerk angewendet.

So konfigurieren Sie globale Firewalleinstellungen:

1. Navigieren Sie im **Konfigurationseditor**zu **Global** > **Netzwerkeinstellungen** und klicken Sie auf das Bearbeitungssymbol.



2. Wählen Sie im Abschnitt **Globale Firewall-Einstellungen** Werte für die folgenden Optionen aus:
   - **Vorlage für globale Richtlinien** - Wählen Sie eine Firewall-Richtlinienvorlage aus, die auf alle Appliances im SD-WAN-Netzwerk angewendet werden soll, **Standard-Firewall-Aktionen** - Wählen Sie Zulassen aus, um Pakete zuzulassen stimmt nicht mit der Filterrichtlinie überein. Wählen Sie Drop, um die Pakete zu löschen, die nicht mit der Filterrichtlinie übereinstimmen, **Standardverbindungsstatusverfolgung** - Dies ermöglicht die Verfolgung des direktionalen Verbindungszustands 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 **Apply**.

> **Hinweis**
>
> Sie können diese Einstellungen auch auf Standortebene konfigurieren. Dadurch wird die globale Einstellung außer Kraft gesetzt.

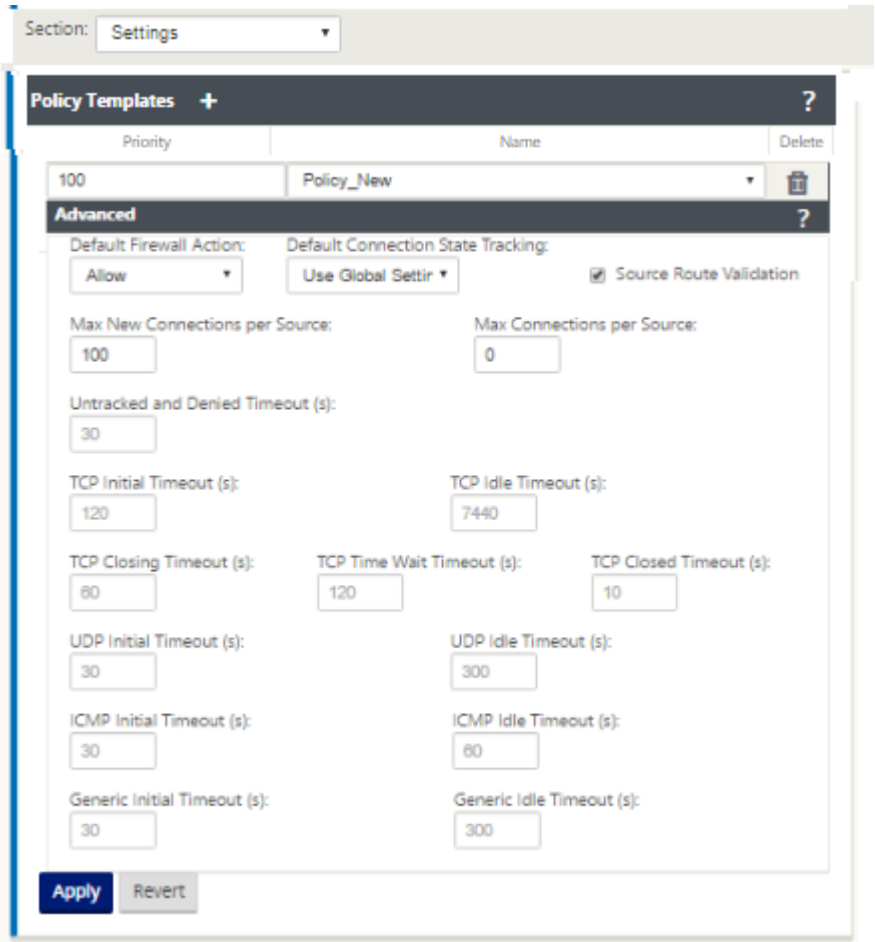
Erweiterte Firewalleinstellungen

October 28, 2021

Sie können die erweiterten Firewall-Einstellungen für jede Site einzeln konfigurieren. Dadurch werden die globalen Einstellungen außer Kraft gesetzt.

So konfigurieren Sie erweiterte Firewall-Einstellungen:

1. Navigieren Sie im **Konfigurationseditor** zu **Verbindungen** > **Site anzeigen** > **Firewall** > **Einstellungen**.



2. Klicken Sie im Abschnitt **Richtlinienvorlage** auf **Hinzufügen**. Geben Sie Werte für die folgenden Parameter ein.

   - **Priorität** - Die Reihenfolge, in der die Richtlinie auf der Website angewendet wird.
   - **Name** —Der Name der Richtlinienvorlage, die auf der Website 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 Sie die in den NetScaler SD-WAN-Einstellungen konfigurierte globale Einstellung
  - **Zulassen**- Pakete, die keiner Filterrichtlinie entsprechen, sind zulässig.
  - **Drop**- Pakete, die keiner Filterrichtlinie entsprechen, werden verworfen.
- **Standard-Verbindungsstatus-Tracking** —Wählen Sie eine der folgenden Optionen aus.
  - **Globale Einstellung verwenden**- Verwenden Sie die in den NetScaler SD-WAN-Einstellungen konfigurierte globale Einstellung
  - **Keine Verfolgung** - Bidirektionale Verbindungsstatusverfolgung wird nicht für Pakete durchgeführt, die keiner Filterrichtlinie entsprechen
  - **Track** - Bidirektionale Verbindungsstatusverfolgung wird für TCP-, UDP- und ICMP-Pakete durchgeführt, die keiner Filterrichtlinie oder NAT-Regel entsprechen. Dadurch wird der asymmetrische Fluss blockiert, selbst wenn keine Firewall-Richtlinien definiert sind.
- **Quell-Route-Validierung**: Wenn diese Option aktiviert ist, werden Pakete verworfen, 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.
- **Maximal 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 pro Quell-IP-Adresse. 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

October 28, 2021

Sie können Zonen im Netzwerk konfigurieren und Richtlinien definieren, um zu steuern, wie der Verkehr in Zonen ein- und aussteigt. Standardmäßig werden die folgenden Zonen erstellt:

- Internet_Zone

  - Gilt für den Verkehr zu oder von einem Internetdienst mit einer vertrauenswürdigen Schnittstelle.

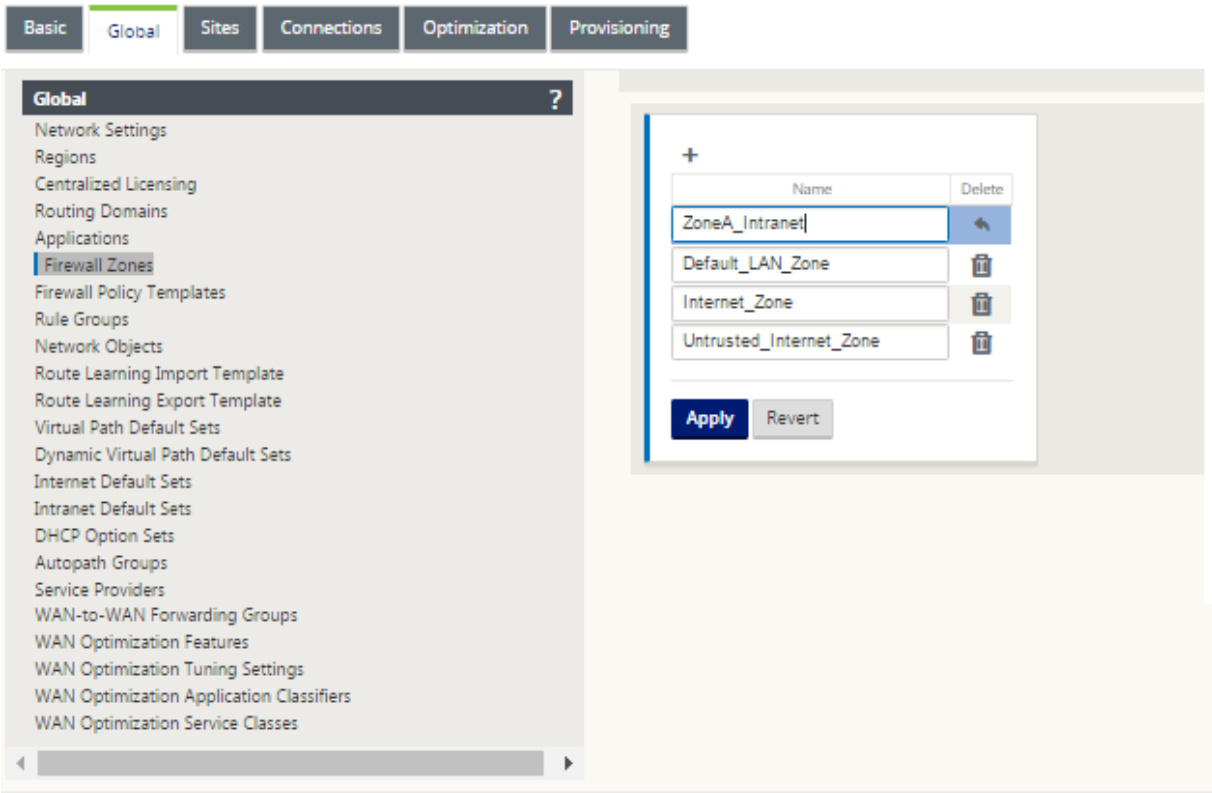
- Untrusted_Internet_Zone
  - Gilt für den Verkehr zu oder von einem Internetdienst über eine nicht vertrauenswürdige Schnittstelle.

- Default_LAN_Zone
  - Gilt für den Verkehr zu oder von einem Objekt mit einer konfigurierbaren Zone, in der die Zone nicht festgelegt wurde.

Sie können Ihre eigenen Zonen erstellen und folgenden Objekttypen zuweisen:

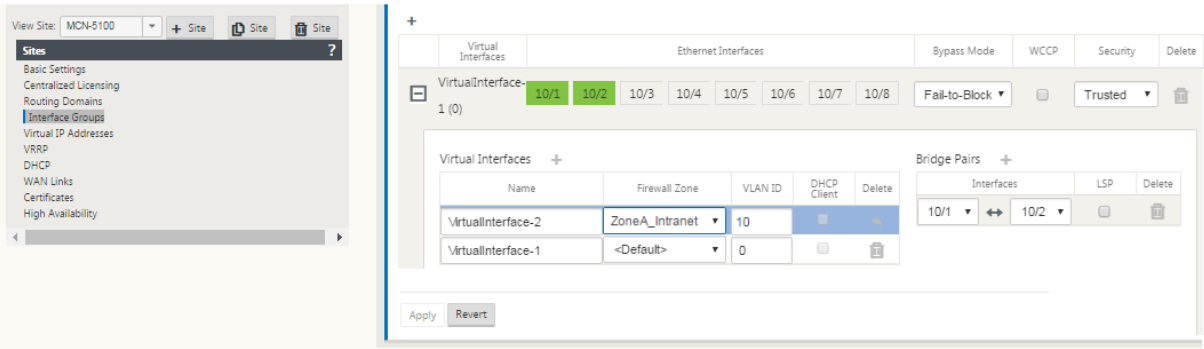
- Virtuelle Netzwerkschnittstellen (VNI)
- Intranetdienste
- GRE Tunnel
- LAN IPsec-Tunnel

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, aus der der Verkehr stammt, und diese Quellzone wird durch den virtuellen Pfad getragen. Auf diese Weise kann das empfangende Ende des virtuellen Pfades eine Richtlinienentscheidung basierend auf der ursprünglichen Quellzone treffen, bevor es in den virtuellen Pfad eintritt.

Beispielsweise möchte ein Netzwerkadministrator möglicherweise Richtlinien definieren, sodass nur Datenverkehr von VLAN 30 an Standort A an Standort B in VLAN 10 gelangen darf. Der Administrator kann jedem VLAN eine Zone zuweisen und Richtlinien erstellen, die den Verkehr zwischen diesen Zonen zulassen und den Verkehr 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.



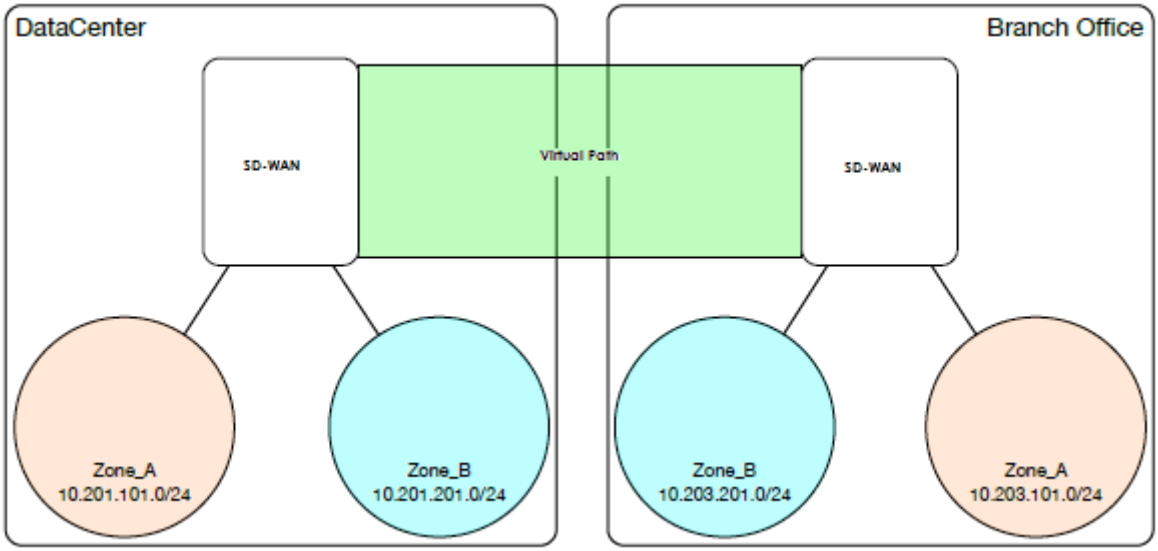
Die Zielzone eines Pakets wird basierend auf der Übereinstimmung der Zielroute bestimmt. Wenn eine SD-WAN-Appliance das Zielsubnetz in der Routentabelle nachschaut, stimmt das Paket mit einer Route überein, der eine Zone zugewiesen ist.

- Quellzone
  - Nicht-virtueller Pfad: Bestimmt durch das Virtual Network Interface Paket wurde am empfangen.
  - Virtueller Pfad: Wird durch das Quellzonenfeld im Paketfluss-Header bestimmt.
  - Virtuelle Netzwerkschnittstelle - Das Paket wurde am Quellstandort empfangen.
- Zielzone
  - Bestimmt durch die Suche nach der Zielroute des Pakets.

Routen, die mit Remotestandorten im SD-WAN geteilt werden, speichern Informationen über die Zielzone, einschließlich Routen, die durch das dynamische Routing-Protokoll (BGP, OSPF) erlernt wurden. Mit diesem Mechanismus gewinnen Zonen im SD-WAN-Netzwerk an globaler Bedeutung und ermöglichen eine Ende-zu-Ende-Filterung innerhalb des Netzwerks. Die Verwendung von Zonen bi-

etet einem Netzwerkadministrator eine effiziente Möglichkeit, den Netzwerkverkehr basierend auf Kunden, Geschäftsbereich oder Abteilung zu segmentieren.

Die Fähigkeit der SD-WAN-Firewall ermöglicht es dem Benutzer, den Datenverkehr zwischen Diensten innerhalb einer einzelnen Zone zu filtern oder Richtlinien zu erstellen, die zwischen Diensten in verschiedenen Zonen angewendet werden können, wie in der Abbildung unten gezeigt. Im Beispiel unten haben wir Zone_A und Zone_B, von denen jede über eine virtuelle LAN-Netzwerkschnittstelle verfügt.



Ein Screenshot unten zeigt die Vererbung der Zone für eine virtuelle IP (VIP) von der zugewiesenen virtuellen Netzwerkschnittstelle (VNI) an.

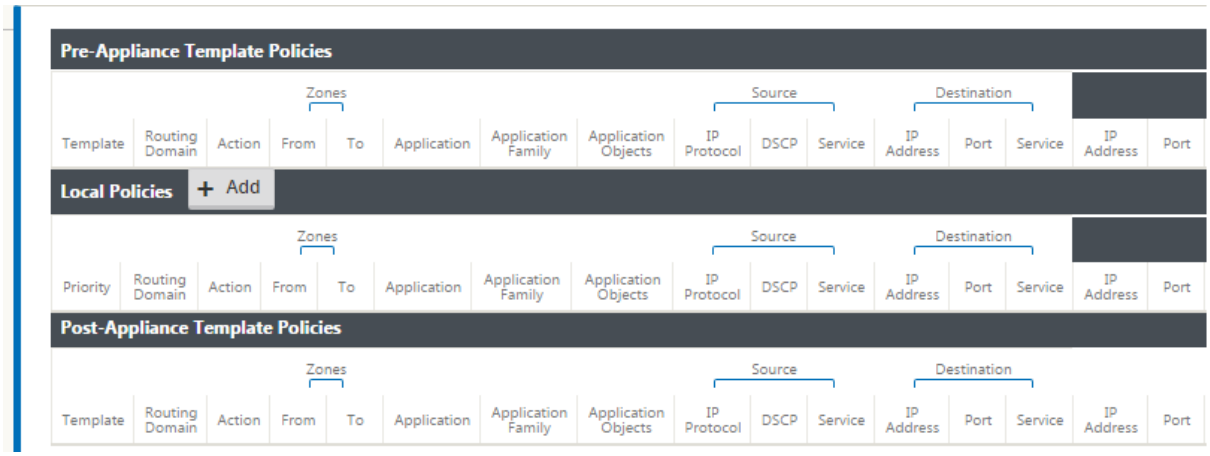
IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	✔		Trusted	🗑
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone			Trusted	

Richtlinien

October 28, 2021

Richtlinien bieten die Möglichkeit, bestimmte Verkehrsströme zuzulassen, abzulehnen oder zu zählen und fortzusetzen. Die individuelle 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 Richtlinien für Vorlagen vor der Appliance oder als Post-Appliance-Vorlagenrichtlinien angeordnet. Sowohl netzwerkweite Vorbereitungs- als auch Post-Appliance-Vorlagenrichtlinien werden auf globaler Ebene konfiguriert. Lokale Richtlinien werden auf Standortebene unter Verbindungen konfiguriert und gelten nur für diesen bestimmten Standort.



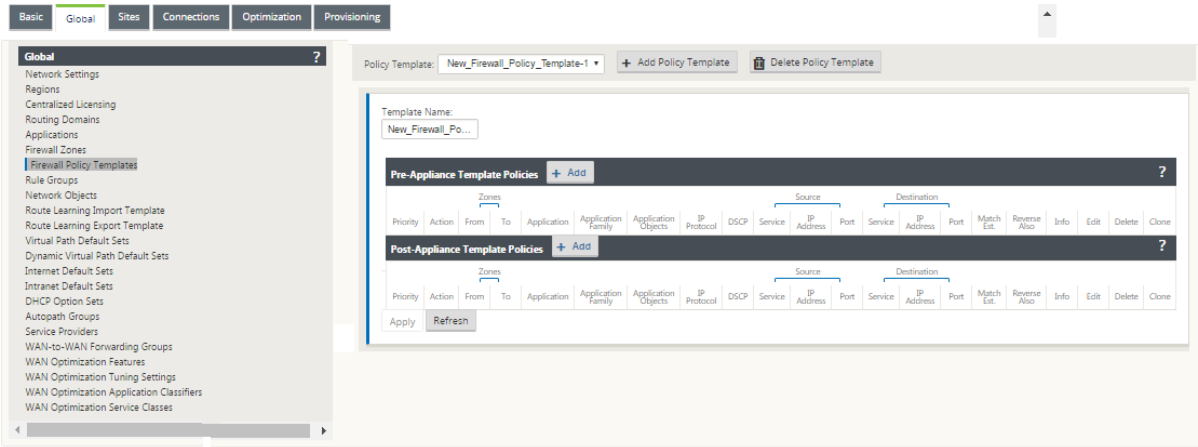
Vorlagenrichtlinien vor der Appliance werden vor allen lokalen Site-Richtlinien angewendet. Als Nächstes werden lokale Site-Richtlinien angewendet, gefolgt von Richtlinien für Post-Appliance-Vorlagen. Ziel ist es, den Konfigurationsprozess zu vereinfachen, indem Sie globale Richtlinien anwenden können und gleichzeitig die Flexibilität beibehalten, standortspezifische Richtlinien anzuwenden.

Filterrichtlinienauswertungsreihenfolge

1. Pre-Templates —kompilierte Richtlinien aus allen Abschnitten “PRE”für Vorlagen.
2. Vorglobal —zusammengestellte Richtlinien aus dem Abschnitt “Vor”Global.
3. Lokal —Richtlinien auf Appliance-Ebene.
4. Lokal automatisch generiert —automatisch lokal generierte Richtlinien.
5. Post-Templates —kompilierte Richtlinien aus allen Abschnitten “POST”der Vorlage.
6. Post-Global —zusammengestellte Richtlinien aus dem Abschnitt Global “POST”.

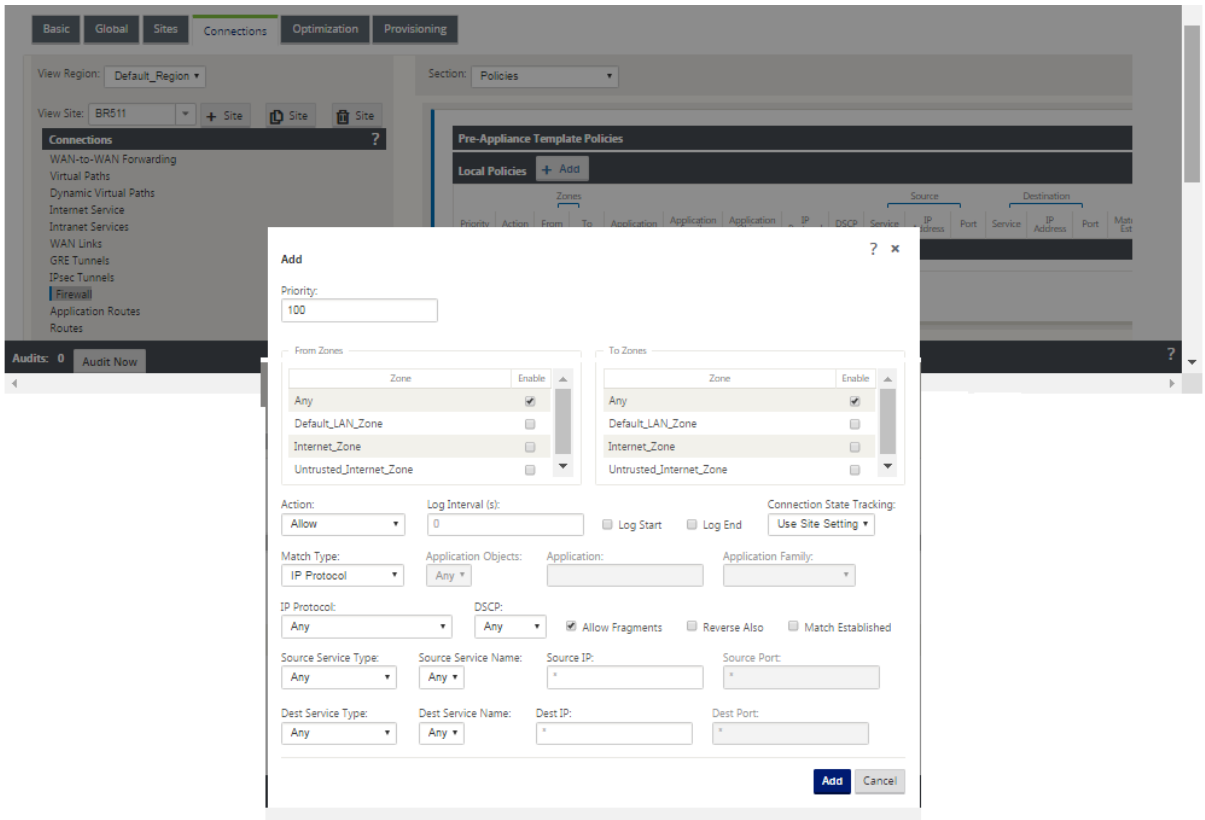
Richtliniendefinitionen - Global und Local (Site)

Sie können Richtlinien für Pre-Appliance- und Post-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 Sites 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 gleich.



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** —Flüsse haben eine Quell- und Zielzone.
  - **Aus Zone** —Quellzone für die Richtlinie.
  - **Zur Zone** —Zielzone für die Richtlinie.
- **Aktion** —**Aktion**, die bei einem übereinstimmenden Fluss ausgeführt werden soll.
  - **Erlauben** —**erlauben** Sie den Fluss durch die Firewall.
  - **Drop** —verweigern Sie den Fluss durch die Firewall, indem Sie die Pakete fallen lassen.
  - **Ablehnen** —verweigern Sie den Fluss durch die Firewall und senden Sie eine protokollspezifische Antwort. TCP sendet einen Reset, ICMP sendet eine Fehlermeldung.
  - **Zählen und fortfahren** —zählen Sie die Anzahl der Pakete und Byte für diesen Fluss und fahren Sie dann in der Richtlinienliste fort.
- **Protokollintervall** —Zeit in Sekunden zwischen der Protokollierung der Anzahl der Pakete, die der Richtlinie entsprechen, mit der Firewall-Protokolldatei oder dem Syslog-Server, falls diese konfiguriert ist.
  - **Start protokollieren** —wenn diese Option ausgewählt ist, wird ein Protokolleintrag für den neuen Flow erstellt.
  - **Log End** —protokolliert die Daten für einen Flow, wenn der Flow gelöscht wird.

> **Hinweis**
>
> Der Standardwert für Protokollintervall 0 bedeutet keine Protokollierung.

- **Track** —ermöglicht 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. Siehe die Tabelle für die Statusverfolgung basierend auf dem Protokoll unten. Verwenden Sie die auf Site-Ebene unter **Firewall** > **Einstellungen** > **Erweitert** > **Standardverfolgung**definierte Einstellung.
  - **Kein Track** —Flow-Status ist nicht aktiviert.
  - **Track** —Zeigt den aktuellen Status des Flows an (der dieser Richtlinie entspricht).
- **Übereinstimmungstyp** —wählen Sie einen der folgenden Übereinstimmungstypen aus

- **IP-Protokoll** —Wenn dieser Übereinstimmungstyp ausgewählt ist, wählen Sie ein IP-Protokoll aus, mit dem der Filter übereinstimmt. Zu den Optionen gehören ANY, TCP, UDP, ICMP usw.
- **Anwendung** —Wenn dieser Übereinstimmungstyp ausgewählt ist, geben Sie die Anwendung an, die als Übereinstimmungskriterium 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 Übereinstimmungskriterium für diesen Filter verwendet wird.

Weitere Informationen zu Anwendung, Anwendungsfamilie und Anwendungsobjekt finden Sie unter Anwendungsklassifizierung.

- **DSCP** —ermöglicht dem Benutzer die Übereinstimmung mit einer DSCP-Tag-Einstellung.
- **Fragmente** zulassen —erlaubt IP-Fragmente, die dieser Filterrichtlinie entsprechen.

> **Hinweis**
>
> Die Firewall fügt fragmentierte Frames nicht wieder ein.

- **Umkehren auch** —fügt automatisch eine Kopie dieser Filterrichtlinie hinzu, wobei die Quell- und Zieleinstellungen umgekehrt sind.
- **Match Etabliert** —stimmt eingehende Pakete für eine Verbindung zu, zu der ausgehende Pakete erlaubt waren.
- **Quelldiensttyp** - in Bezug auf einen SD-WAN-Dienst - Lokal (zur Appliance), virtueller Pfad, Intranet, IPHost oder Internet sind Beispiele für Diensttypen.
- **IPHost-Option** - Dies ist ein neuer Diensttyp für die Firewall und wird für Pakete verwendet, die von der SD-WAN-Anwendung generiert werden. Beispielsweise führt das Ausführen eines Pings über die Webbenutzeroberfläche des SD-WAN zu einem Paket, das von einer virtuellen SD-WAN-IP-Adresse bezogen wird. Beim Erstellen einer Richtlinie für diese IP-Adresse muss der Benutzer die Option IPHost auswählen.
- **Quelldienstname** —Name eines an den Diensttyp gebundenen Dienstes. Wenn beispielsweise virtueller 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, die der Filter verwendet, um abzugleichen.
- **Quellport** —Quellport, den die spezifische Anwendung verwenden wird.

- **Zieldiensttyp** - in Bezug auf einen SD-WAN-Dienst - Lokal (zur Appliance), Virtual Path, 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, die der Filter verwendet, um abzugleichen.
- **Zielport** —Zielport, den die spezifische Anwendung verwendet (d. h. den HTTP-Zielport 80 für das TCP-Protokoll).

Die Gleisoption bietet viel mehr Details über einen Fluss. Die in den Statustabellen verfolgten Zustandsinformationen sind unten aufgeführt.

Status-Tabelle für die Track-Option

Es gibt nur wenige Status, die konsistent sind:

- **INIT**-Verbindung wurde erstellt, aber das ursprüngliche Paket war ungültig.
- **O_DENIED**-Pakete, die die Verbindung hergestellt haben, werden von einer Filterrichtlinie verweigert.
- **R_DENIED**-Pakete vom Responder werden durch eine Filterrichtlinie verweigert.
- **NOT_TRACKED-** Die Verbindung wird nicht zustandslos verfolgt, ist aber anderweitig zulässig.
- **CLOSED-** Die Verbindung ist abgelaufenen oder wurde durch das Protokoll auf andere Weise geschlossen.
- **DELETED-** Die Verbindung wird gerade entfernt. Der Status DELETED wird fast nie gesehen werden.

Alle anderen Zustände sind protokollspezifisch und erfordern die Aktivierung der Statusverfolgung.

TCP kann die folgenden Zustände melden:

- **SYN_SENT** - erste TCP-SYN-Meldung wurde gesehen.
- **SYN_SENT2** - SYN-Meldung in beide Richtungen gesehen, kein SYN+ACK (AKA gleichzeitig geöffnet).
- **SYN_ACK_RCVD** - SYN+ACK erhalten.
- **ESTABLISHED-** zweites ACK erhalten, Verbindung ist vollständig hergestellt.
- **FIN_WAIT** - erste FIN-Nachricht gesehen.
- **CLOSE_WAIT** - FIN-Meldung in beide Richtungen gesehen.

- **TIME_WAIT** - letzte ACK in beide Richtungen gesehen. Die Verbindung ist jetzt geschlossen und wartet auf eine erneute Öffnung.

Alle anderen IP-Protokolle (insbesondere ICMP und UDP) haben die folgenden Zustände:

- **NEW** - Pakete in eine Richtung gesehen.
- **ESTABLISHED** - Pakete in beide Richtungen gesehen.

Netzwerkadressübersetzung (NAT)

October 28, 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-Adressübersetzung)
- Dynamisches NAT mit Port-Forwarding-Regeln

> **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

October 28, 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.

- 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. 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 für den 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

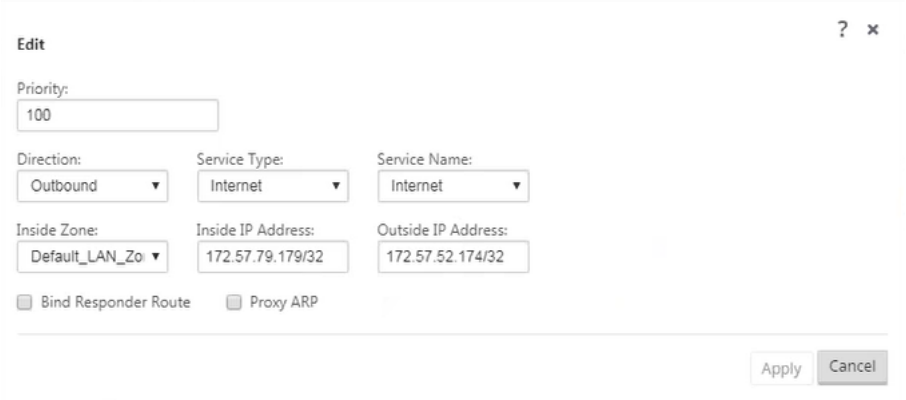
Die Quell- und Ziel-Firewallzonen für den eingehenden oder ausgehenden Datenverkehr sollten nicht identisch sein. Wenn sowohl die Quell- als auch die Ziel-Firewallzonen identisch sind, wird NAT nicht für den Datenverkehr ausgeführt.

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

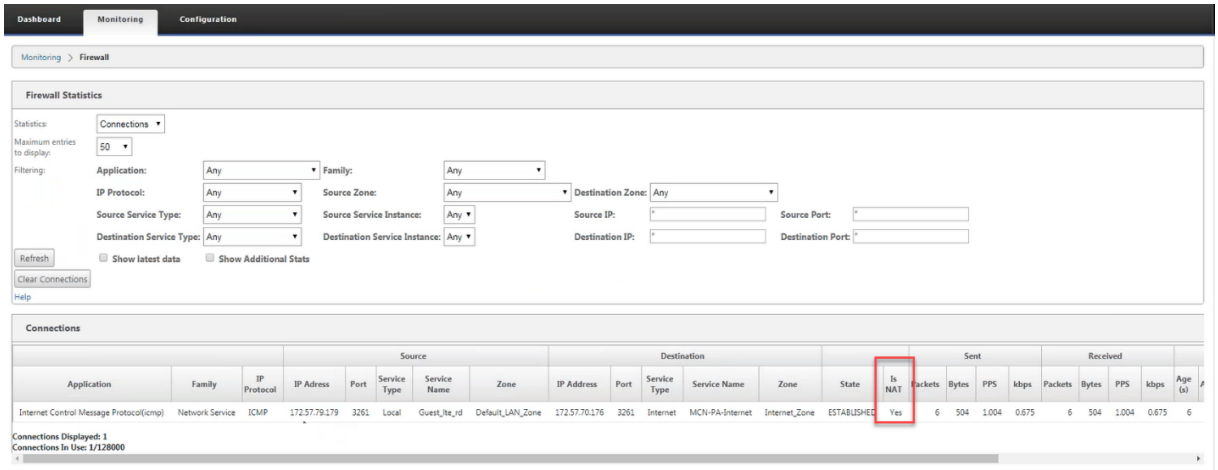
Um statische NAT-Richtlinien zu konfigurieren, navigieren Sie im Konfigurationseditor zu **Verbindungen** > **Firewall** > **Static NAT Policies**.



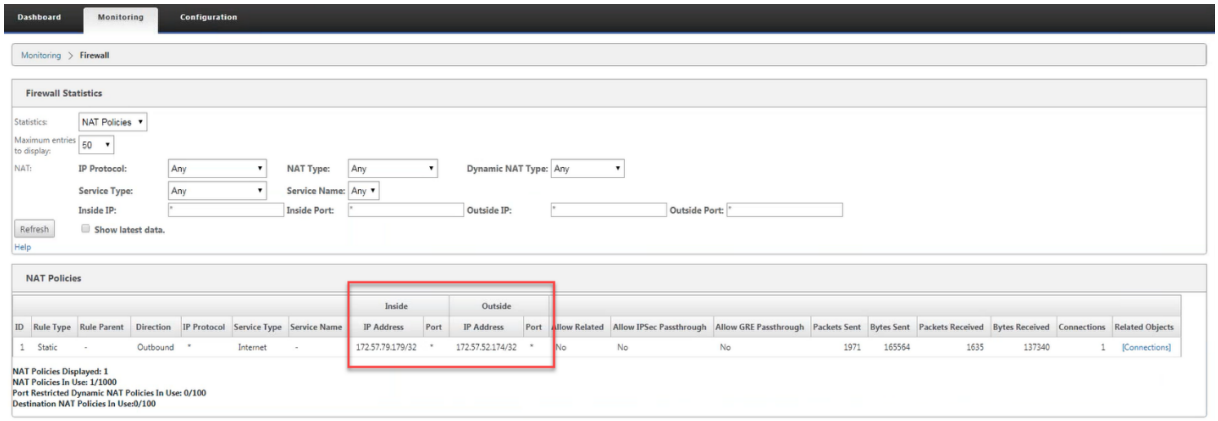
- **Priorität**: Die Reihenfolge, in der die Richtlinie innerhalb aller definierten Richtlinien angewendet wird. Richtlinien mit niedrigerer Priorität werden vor Richtlinien mit höherer Priorität angewendet.
- **Richtung**: Die Richtung, in die der Verkehr fließt, aus der Perspektive der virtuellen Schnittstelle 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.

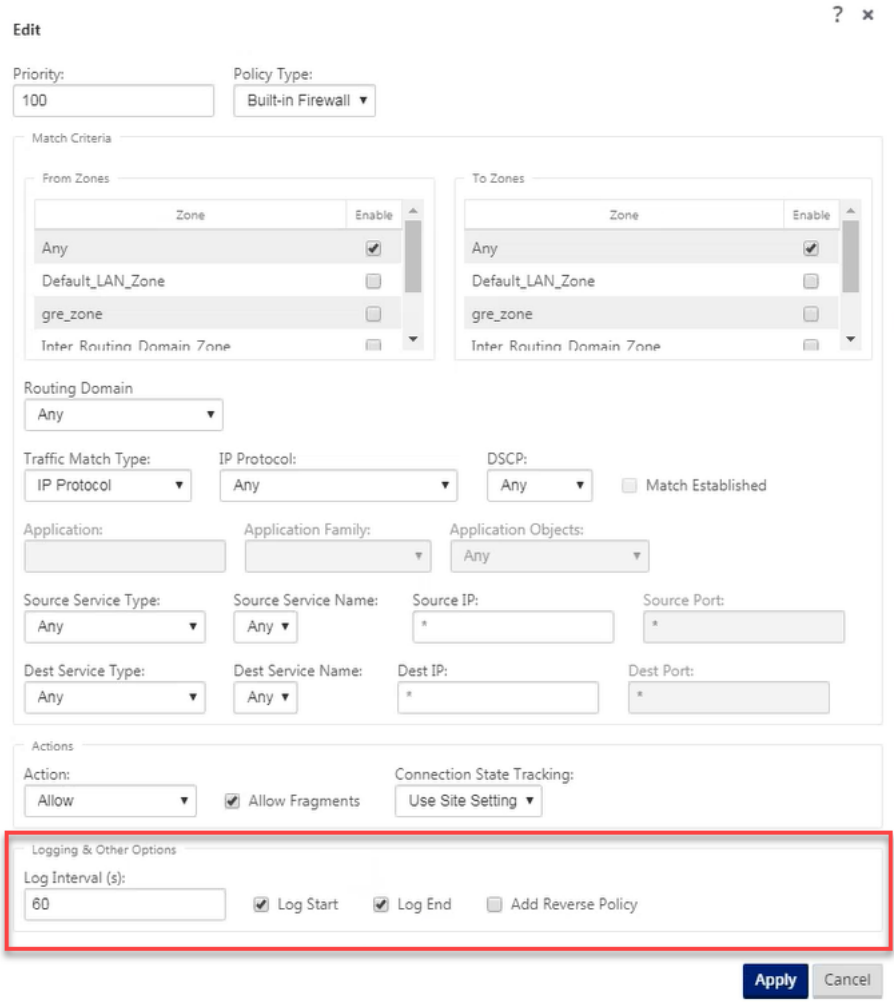


Um die innere IP-Adresse zur externen IP-Adresszuordnung zu sehen, klicken Sie unter **Zugehörige Objekte** auf **NAT nach dem Routing** oder navigieren Sie zu **Monitoring** > **Firewall-Statistiken** > **NAT-Richtlinien**.

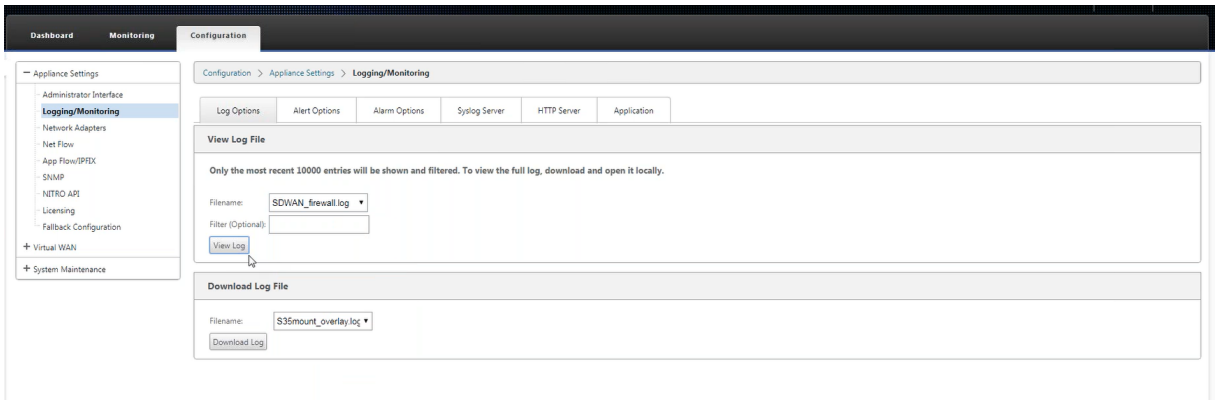


Protokolle

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.



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/firewall/connection.c:8704:      Removed 1 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

October 28, 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

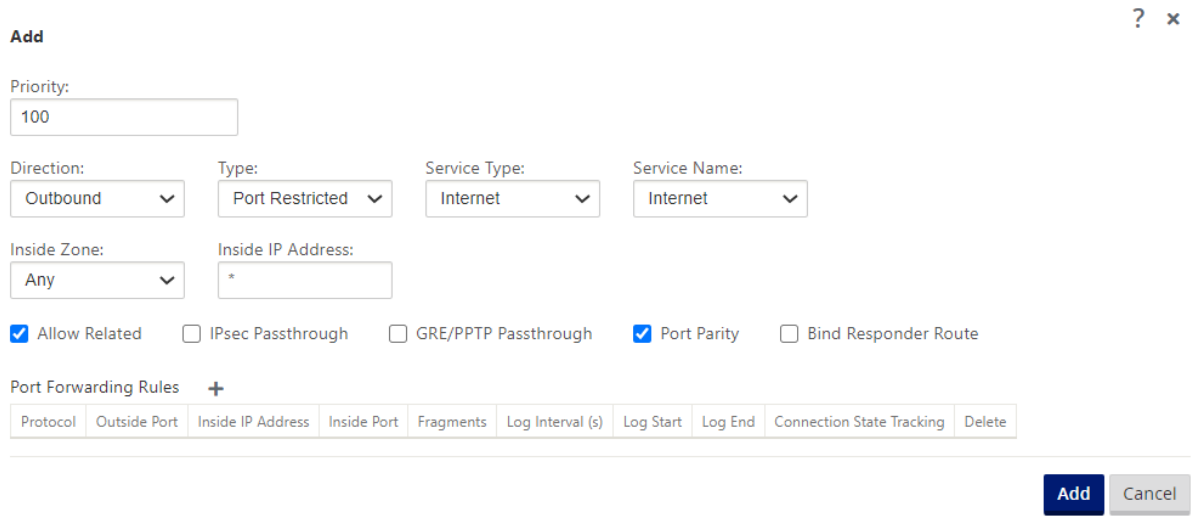
Die Richtung für eine Verbindung kann entweder von innen nach außen oder von außen nach innen sein. Wenn eine NAT-Regel erstellt wird, wird sie je nach Richtungsübereinstimmungstyp auf beide

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 Konfigurationseditor zu **Verbindungen** > **Firewall** > **Dynamische NAT-Richtlinien**.



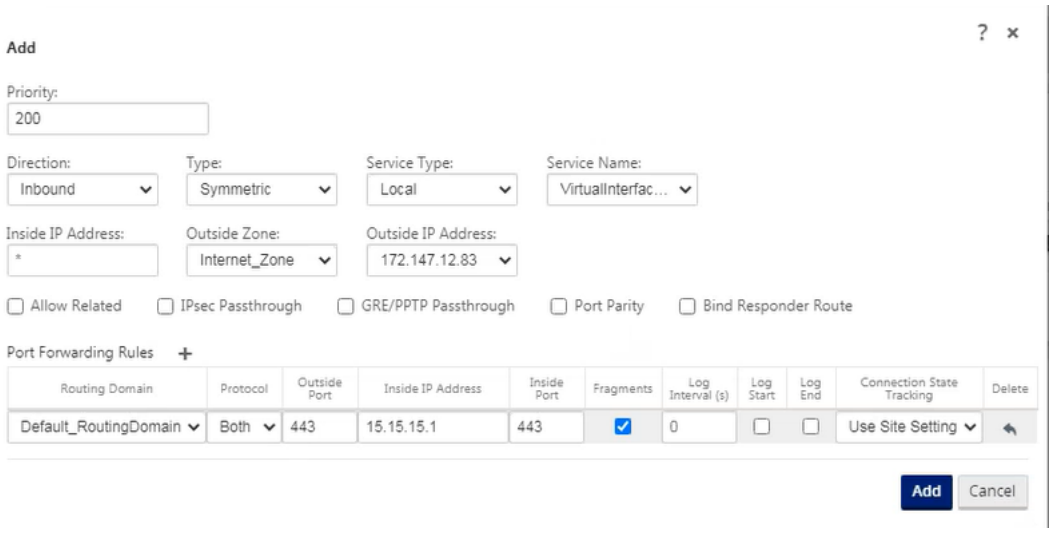
- **Priorität**: Die Reihenfolge, in der die Richtlinie innerhalb aller definierten Richtlinien angewendet wird. Richtlinien mit niedrigerer Priorität werden vor Richtlinien mit höherer Priorität angewendet.

- **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 übereinstimmte, 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).
- **Responder-Route binden**: Stellt sicher, dass der Antwortverkehr über denselben Dienst gesendet wird, auf dem er empfangen wird, um 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. Dy-

namische NAT-Portweiterleitung wird normalerweise verwendet, um Remotehosts die Verbindung zu einem Host oder Server in Ihrem privaten Netzwerk zu ermöglichen. Für einen detaillierteren Anwendungsfall siehe Citrix SD-WAN Dynamic NAT erklärt.



- **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.

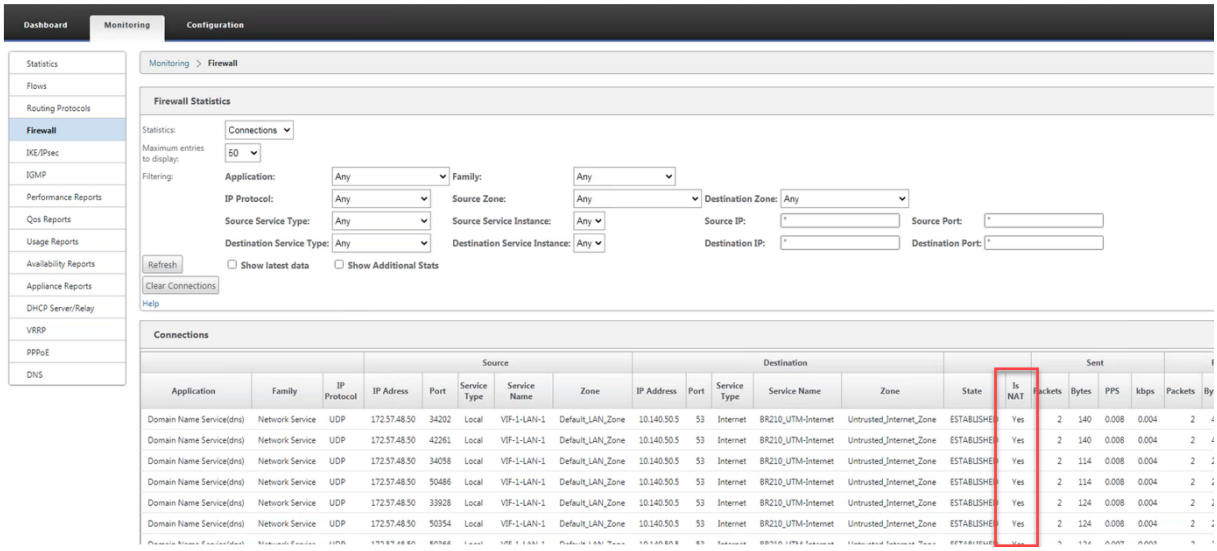
Automatisch erstellte dynamische NAT-Richtlinien

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 Einzelheiten finden Sie unter Konfigurieren der Firewall-Segmentierung.
- Konfigurieren von DNS-Weiterleitungen oder DNS-Proxy auf SD-WAN. Weitere Einzelheiten finden Sie unter Domainnamensystem.

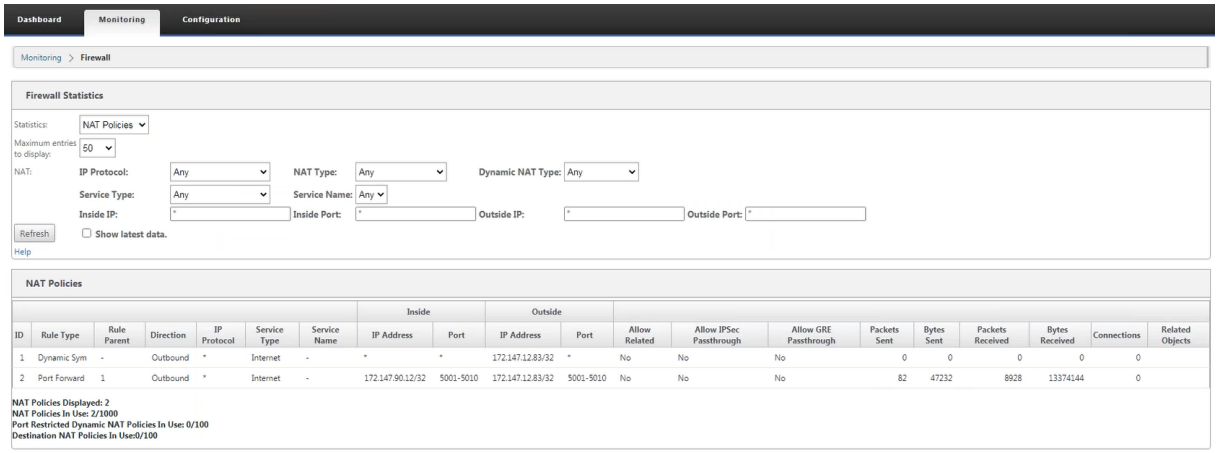
Überwachen

Um dynamische NAT zu überwachen, navigieren Sie zu **Monitoring** > **Firewall-Statistiken** > **Verbindungen**. Für eine Verbindung können Sie sehen, ob NAT fertig ist oder nicht.

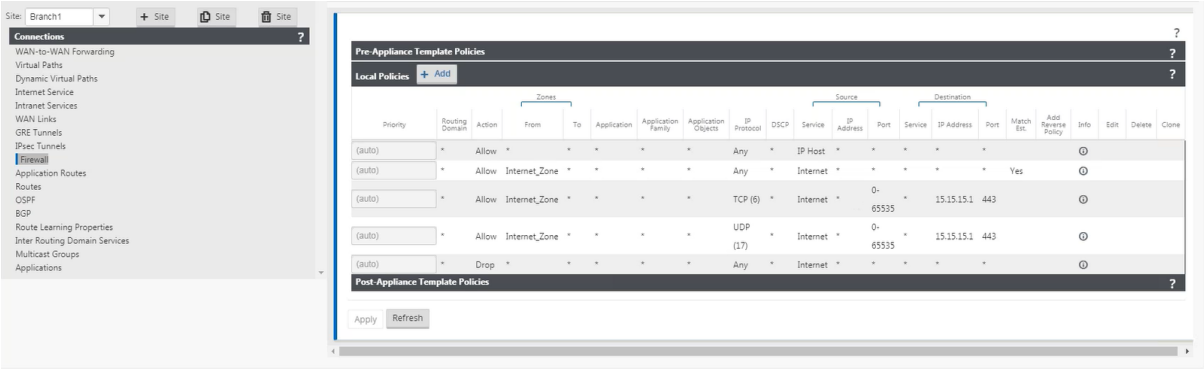


Um die innere IP-Adresse zur Zuordnung von externen IP-Adressen weiter zu sehen, klicken Sie unter **Verwandte Objekte** auf **NAT vor** der **Route oder NAT nach** der Route oder navigieren Sie zu **Überwachung** > **Firewall-Statistiken** > **NAT-Richtlinien**.

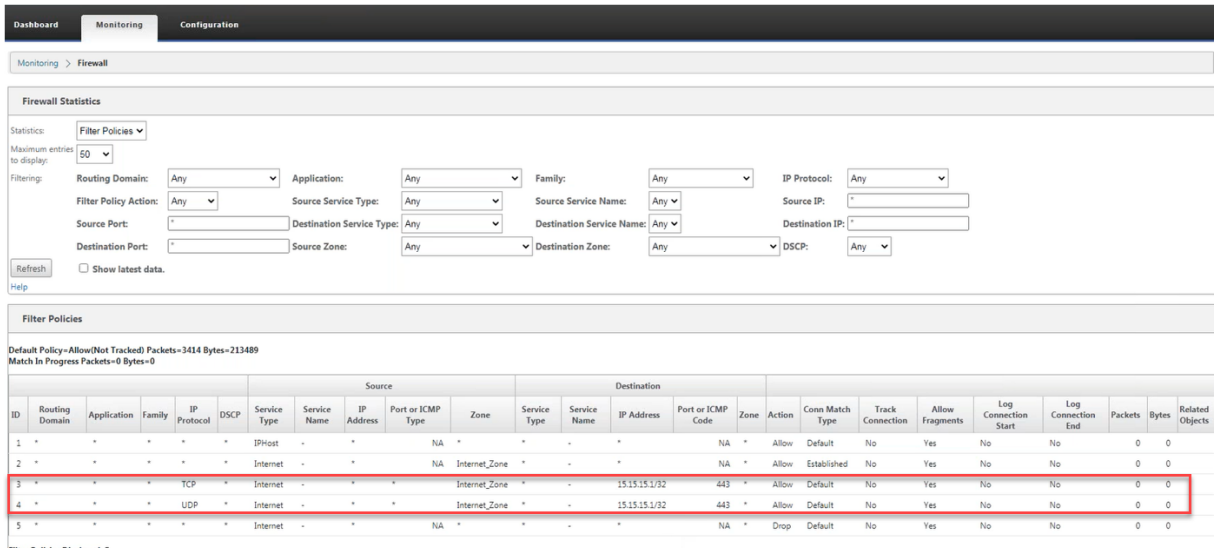
Der folgende Screenshot zeigt die Statistiken für die dynamische NAT-Regel vom Typ symmetrisch und die entsprechende Portweiterleitungsregel.



Wenn eine Portweiterleitungsregel erstellt wird, wird auch eine entsprechende Firewallregel erstellt.

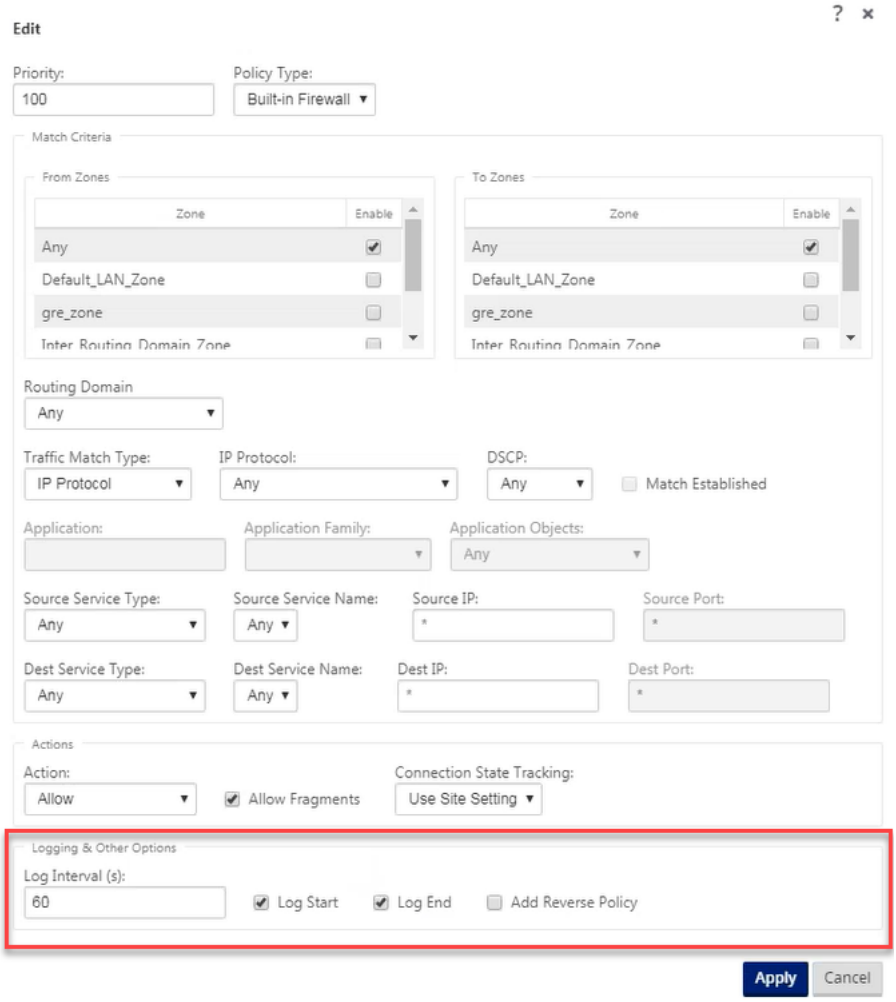


Sie können die Statistiken der Filterrichtlinie anzeigen, indem Sie zu **Überwachung** > **Firewall-Statistiken** > **Filterrichtlinien**navigieren.

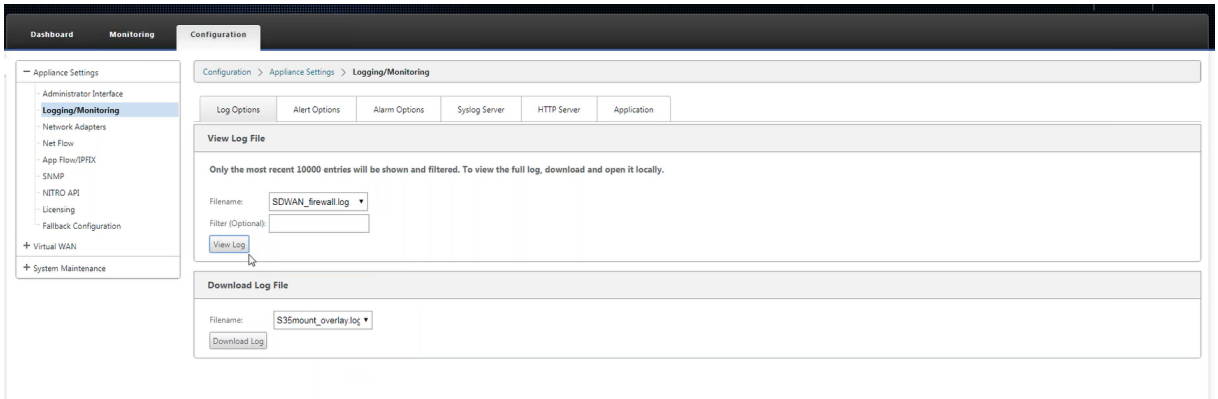


Protokolle

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.



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/firewall/connection.c:8704        Removed 1 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)
```

Konfigurieren des virtuellen WAN-Dienstes

October 28, 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 dazu den Konfigurationseditor im Citrix SD-WAN Management-Webinterface 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-Chiffern (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 Konfigurationseditor im Management-Webinterface auf dem Management Control Node (MCN) verwenden. Sie benötigen Administratorzugriff auf den MCN, um die Konfiguration zu ändern und Ihre Änderungen über das SD-WAN-Netzwerk zu verteilen. Sobald der MCN gesichert ist, sind auch die Verschlüsselungseinstellungen und ihre Verteilung sicher.

Die Authentifizierung zwischen Standorten funktioniert mit der Virtual WAN-Konfiguration.
Die Netzwerkkonfiguration hat einen geheimen Schlüssel für jeden Standort. Für jeden virtuellen Pfad generiert die Netzwerkkonfiguration einen Schlüssel, indem die geheimen Schlüssel von den Sites an jedem Ende des virtuellen Pfades kombiniert werden. Der anfängliche Schlüsselaustausch, der nach der ersten Einrichtung eines virtuellen Pfades stattfindet, hängt von der Fähigkeit ab, Pakete mit diesem kombinierten Schlüssel zu verschlüsseln und zu entschlüsseln.

Virtuellen WAN-Dienst aktivieren

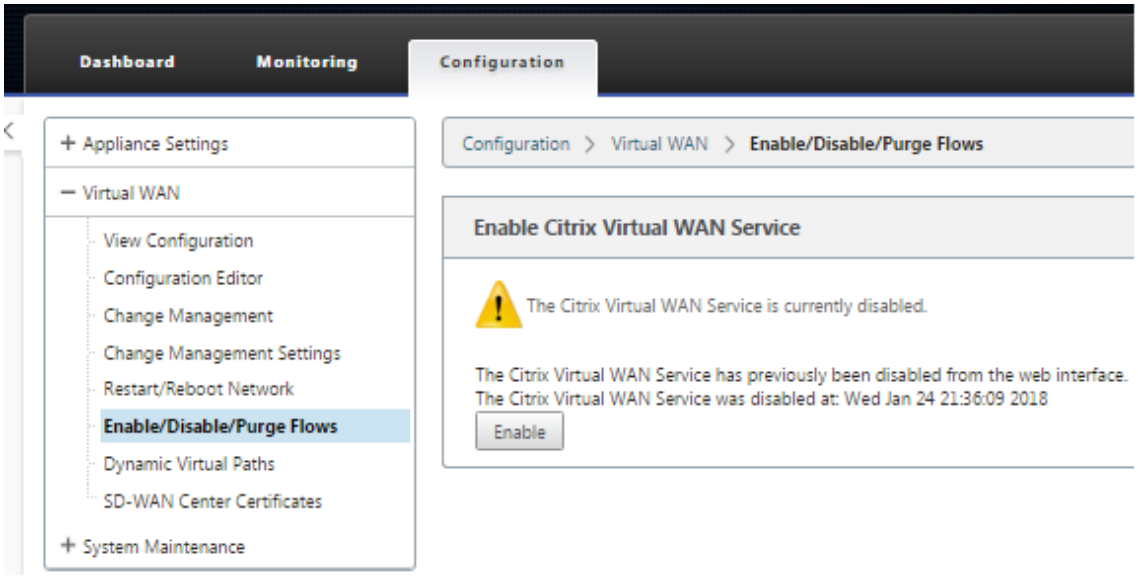
Wenn es sich um eine Erstinstallation und Konfiguration handelt, müssen Sie als letzten Schritt den virtuellen WAN-Dienst auf jeder SD-WAN-Appliance in Ihrem Netzwerk manuell aktivieren. Durch die Aktivierung des Dienstes wird der Virtual WAN-Daemon aktiviert und gestartet.

> **Hinweis**
>
> Wenn Sie eine vorhandene Bereitstellung neu konfigurieren, aktiviert der MCN den Dienst automatisch, wenn er die aktualisierten Appliance-Pakete an die Clientsites verteilt. In diesem Fall können Sie diesen letzten Schritt überspringen.

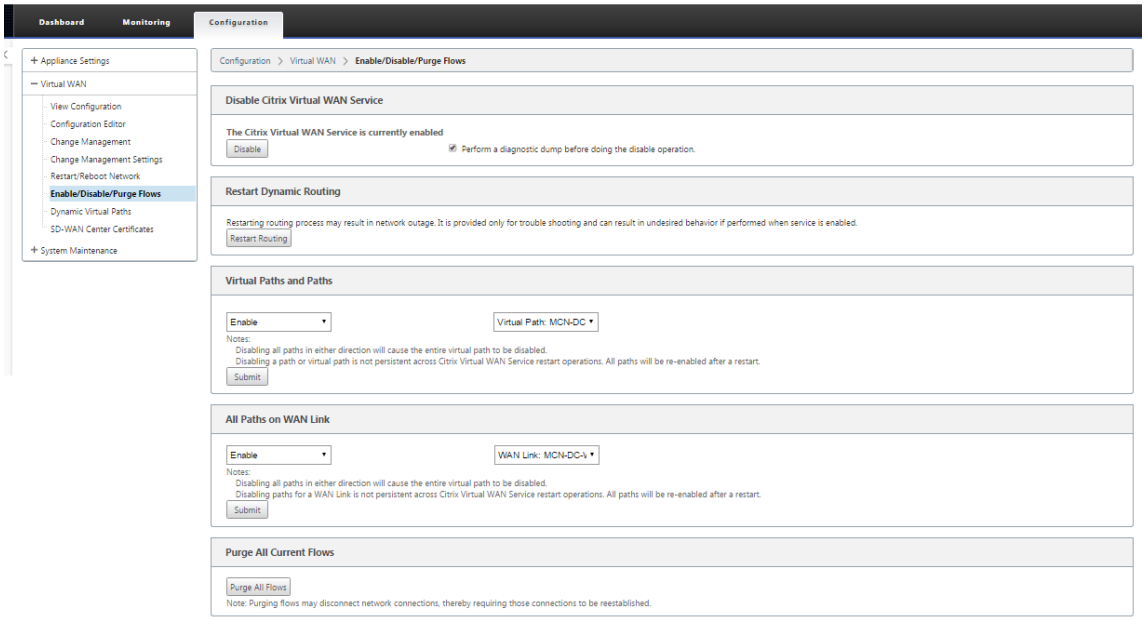
Gehen Sie wie folgt vor, um den Virtual WAN-Dienst auf einer Appliance manuell zu aktivieren:

1. Melden Sie sich bei der Managementoberfläche der Appliance an, die Sie aktivieren möchten.
2. Wählen Sie die Registerkarte **Konfiguration**.
3. Öffnen Sie im Navigationsbereich den Zweig Virtual WAN und wählen Sie **Flows aktivieren/deaktivieren/löschen**aus.

   Wenn der Virtual WAN-Dienst deaktiviert ist, wird die Seite “Virtuellen WAN-Dienst aktivieren” angezeigt, wie unten dargestellt. Wenn der Service bereits aktiviert ist, wird die Seite “Flows aktivieren/deaktivieren/löschen”angezeigt.



4. Klicken Sie auf **Aktivieren**. Dadurch wird der Dienst aktiviert und die Seite "**Flows aktivieren/deaktivieren/löschen** "angezeigt.



Wenn der Virtual WAN-Dienst aktiviert ist, wird im oberen Bereich der Seite eine entsprechende Statusmeldung angezeigt.

> **Hinweis**
>
> Auf dieser Seite werden auch Optionen zum Aktivieren/Deaktivieren bestimmter Pfade und virtueller Pfade in Ihrem Netzwerk sowie eine Option zum Bereinigen aller Flows vorgestellt.

Damit ist die Installation und Aktivierung des SD-WAN auf den MCN- und Zweigstandort-Client-

Appliances abgeschlossen. Sie können jetzt die Überwachungsseiten verwenden, um die Aktivierung zu überprüfen und vorhandene oder potenzielle Konfigurationsprobleme zu diagnostizieren.

Konfigurieren der Firewall-Segmentierung

October 28, 2021

Die Firewallsegmentierung von Virtual Route Forwarding (VRF) bietet mehrere Routingdomänen Zugriff auf das Internet über eine gemeinsame Schnittstelle, wobei der Datenverkehr jeder Domäne von dem der anderen isoliert ist. Beispielsweise können Mitarbeiter und Gäste über dieselbe Schnittstelle auf das Internet zugreifen, ohne auf den Verkehr des anderen zugreifen zu müssen.

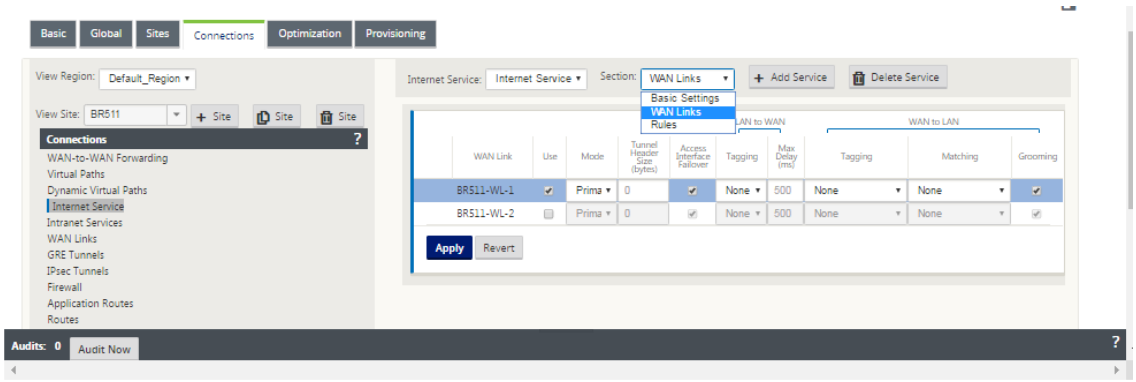
- Internet-Zugang für lokale Gastbenutzer
- Internetzugriff für Mitarbeiter/Benutzer für definierte Anwendungen
- Mitarbeiter-Benutzer können weiterhin den gesamten anderen Traffic zum MCN abstecken
- Erlauben Sie dem Benutzer, bestimmte Routen für bestimmte Routingdomänen hinzuzufügen.
- Wenn diese Option 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, die für jede Benutzergruppe erforderlich ist.

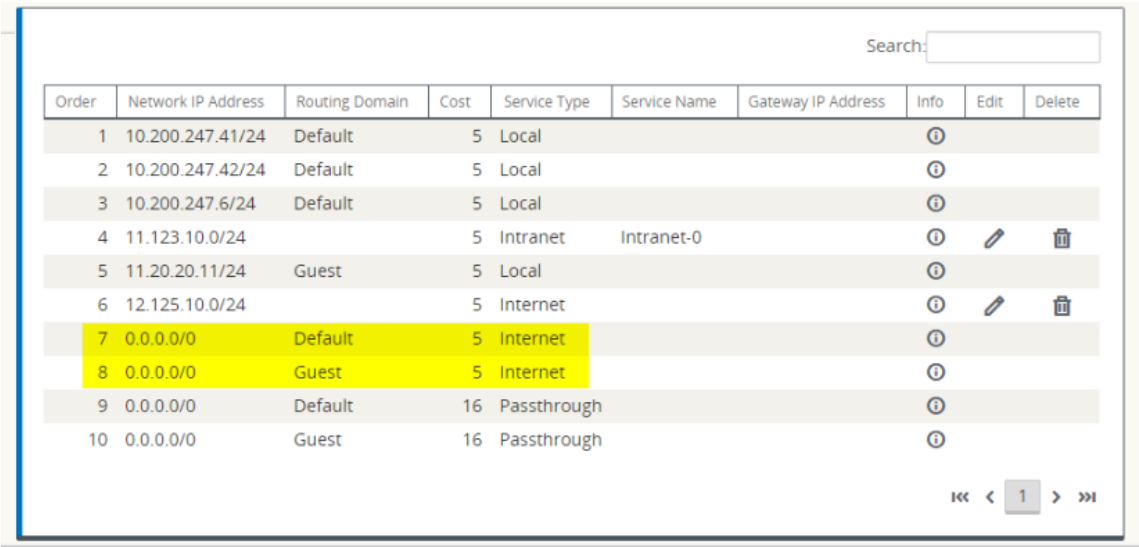
> **Hinweis**
>
> Weitere Informationen finden Sie unter So konfigurieren Sie VRFs.

So konfigurieren Sie Internetdienste für alle Routingdomänen:

1. Erstellen Sie Internetdienst für eine Site. Navigieren Sie zu **Verbindungen** > **Region anzeigen** > **Site anzeigen** > [Sitename] > **Internetdienst > Abschnitt > WAN-Links**, und aktivieren Sie unter WAN-Links das Kontrollkästchen **Verwenden**.



> **Hinweis**
>
> Sie sollten sehen, dass 0.0.0.0/0 Routen hinzugefügt wurden, eine pro Routingdomäne, unter **Verbindungen** > **Region anzeigen** > **Site anzeigen** >[Sitename] > **Routen**.



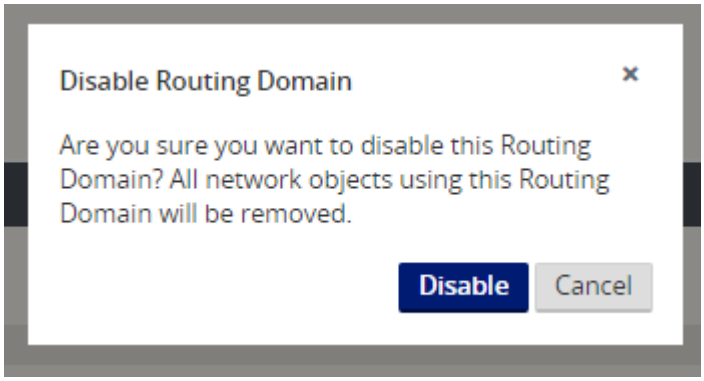
Search:

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 am 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**überprüfen.

Flows Data

Toggle Columns

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
Guest	11.20.20.20	12.125.10.20	WAN Ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Guest	12.125.10.20	11.20.20.20	WAN Egress	0	18456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

4. Sie können auch die Routing-Tabelle für jede Routingdomäne unter **Monitor** > **Statistiken** > **Routen**überprüfen.

Routes for routing domain : Guest

Filter: in Any column Apply

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

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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

Anwendungsfälle

In früheren Citrix SD-WAN-Releases hatten virtuelles Routing und Weiterleitung die folgenden Probleme, die behoben wurden.

- Kunden haben mehrere Routingdomänen an einem Zweigstandort, ohne dass alle Domänen im Rechenzentrum (MCN) einbezogen werden müssen. Sie müssen in der Lage sein, den Datenverkehr verschiedener Kunden auf sichere Weise zu isolieren
- Kunden müssen über eine einzige zugängliche öffentliche IP-Adresse mit Firewall verfügen, damit mehrere Routingdomänen an einem Standort auf das Internet zugreifen können (über VRF Lite hinaus).
- Kunden benötigen eine Internetroute für jede Routingdomäne, die verschiedene Dienste unterstützt.
- Mehrere Routingdomänen an einem Zweigstandort.
- Internetzugang für verschiedene Routingdomänen.

Mehrere Routingdomänen an einem Zweigstandort

Mit den Verbesserungen der Segmentierung der Virtual Forwarding und Routing Firewall können Sie:

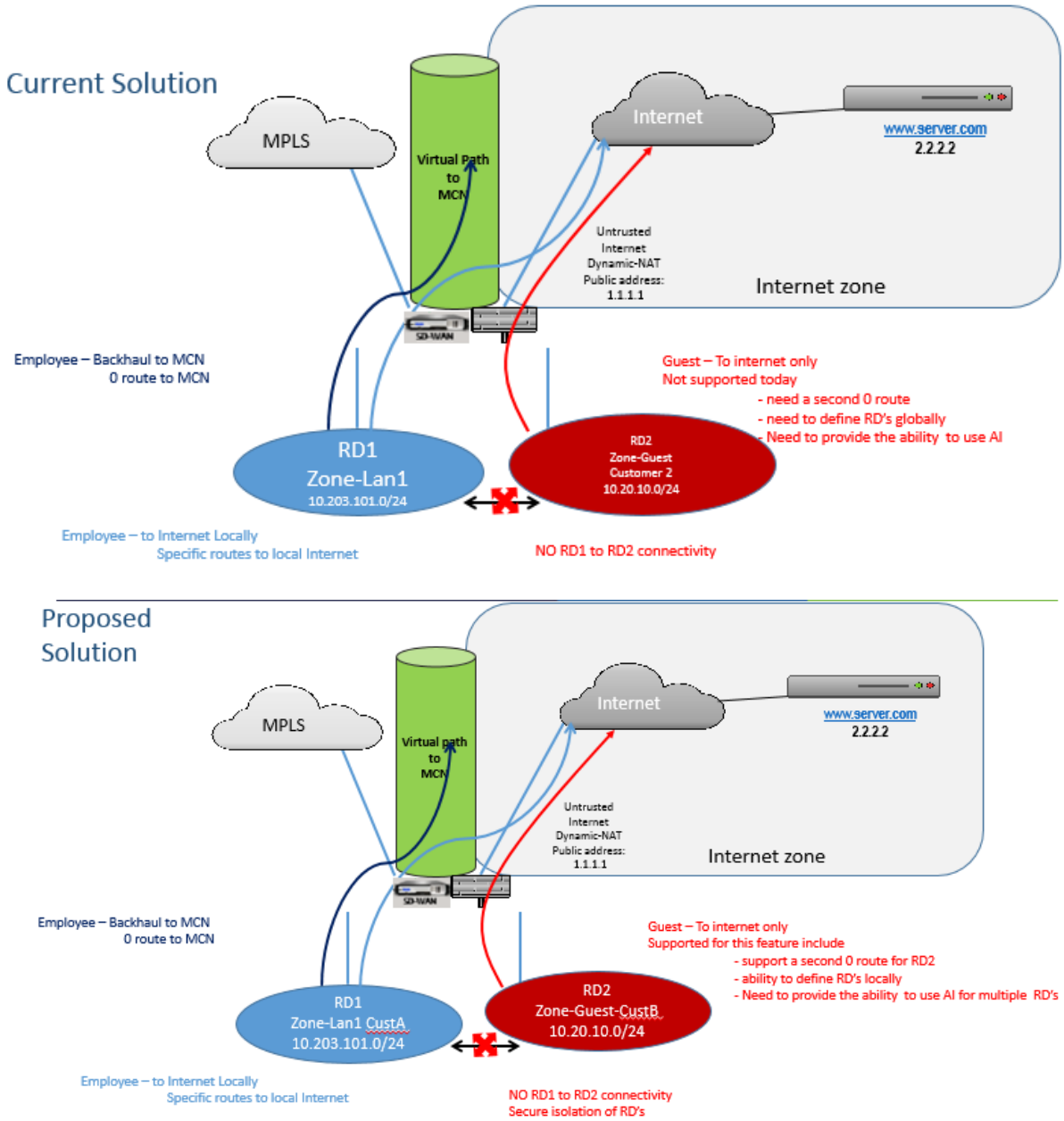
- Stellen Sie am Zweigstandort eine Infrastruktur bereit, die sichere Konnektivität für mindestens zwei Benutzergruppen wie Mitarbeiter und Gäste unterstützt. Die Infrastruktur kann bis zu 16 Routingdomänen unterstützen.
- Isolieren Sie den Traffic jeder Routingdomäne vom Traffic einer anderen Routingdomäne.

- Bereitstellung eines Internetzugangs für jede Routing-Domäne,
  - Ein gemeinsames Access Interface ist erforderlich und akzeptabel
  - Ein Access Interface für jede Gruppe mit separaten öffentlichen IP-Adressen
- Der Verkehr für den Mitarbeiter kann direkt ins lokale Internet geleitet werden (bestimmte Anwendungen)
- Der Verkehr für den Mitarbeiter kann zur umfassenden Filterung zum MCN weitergeleitet oder zurücktransportiert werden (0-Route)
- Der Verkehr für die Routing-Domäne kann direkt ins lokale Internet geleitet werden (0-Route)
- Unterstützt bei Bedarf bestimmte Routen pro Routingdomäne
- Routingdomänen sind VLAN-basiert
- Entfernt die Anforderung, dass der RD im MCN wohnen muss
- Routingdomäne kann jetzt nur an einem Zweigstandort konfiguriert werden
- Ermöglicht es Ihnen, einer Zugriffsschnittstelle mehrere RD zuzuweisen (sobald aktiviert)
- Jeder RD wird eine 0.0.0.0-Route zugewiesen
- Ermöglicht das Hinzufügen bestimmter Routen für eine RD
- Ermöglicht dem Datenverkehr von verschiedenen RD, über dieselbe Zugriffsschnittstelle ins Internet zu gelangen
- Ermöglicht die Konfiguration einer anderen Zugriffsschnittstelle für jede RD
- Muss eindeutige Subnetze sein (RD wird einem VLAN zugewiesen)
- Jeder RD kann dieselbe FW-Standardzone verwenden
- Der Verkehr wird durch die Routing-Domäne isoliert
- Ausgehende Flows haben den RD als Komponente des Flow-Headers. Ermöglicht SD-WAN, Rückflüsse der korrekten Routing-Domäne zuzuordnen.

Voraussetzungen für die Konfiguration mehrerer Routingdomänen:

- Der Internetzugang ist konfiguriert und einem WAN-Link zugewiesen.
- Für NAT konfigurierte Firewall und korrekte Richtlinien wurden angewendet.
- Zweite Routing-Domäne wurde 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 zum WAN-Link hinzugefügt werden, bevor Sie den Internetzugang für alle Routingdomänen aktivieren können. (Bis Sie dies tun, ist das Kontrollkästchen zum Aktivieren dieser Option ausgegraut).

  Nachdem Sie den Internetzugang für alle Routingdomänen aktiviert haben, fügen Sie automatisch eine Dynamic-NAT-Regel hinzu.

- Bis zu 16 Routing-Domains pro Standort.
- Zugriffsschnittstelle (KI): Einzelne KI pro Subnetz.
- Für mehrere KIs ist ein separates VLAN für jede KI erforderlich.
- Wenn Sie zwei Routingdomänen an einem Standort haben und über einen einzigen WAN-Link verfügen, verwenden beide Domänen dieselbe öffentliche IP-Adresse.
- Wenn der Internetzugang für alle Routingdomänen aktiviert ist, können alle Websites zum Internet weiterleiten. (Wenn eine Routing-Domäne keinen Internetzugang benötigt, können Sie die Firewall verwenden, um den Datenverkehr zu blockieren.)
- Keine Unterstützung für dasselbe Subnetz in mehreren Routingdomänen.
- Es gibt keine Audit-Funktion
- Die WAN-Verbindungen werden für den Internetzugang freigegeben.
- Kein QOS pro Routingdomäne; First come first serve.

Zertifikatauthentifizierung

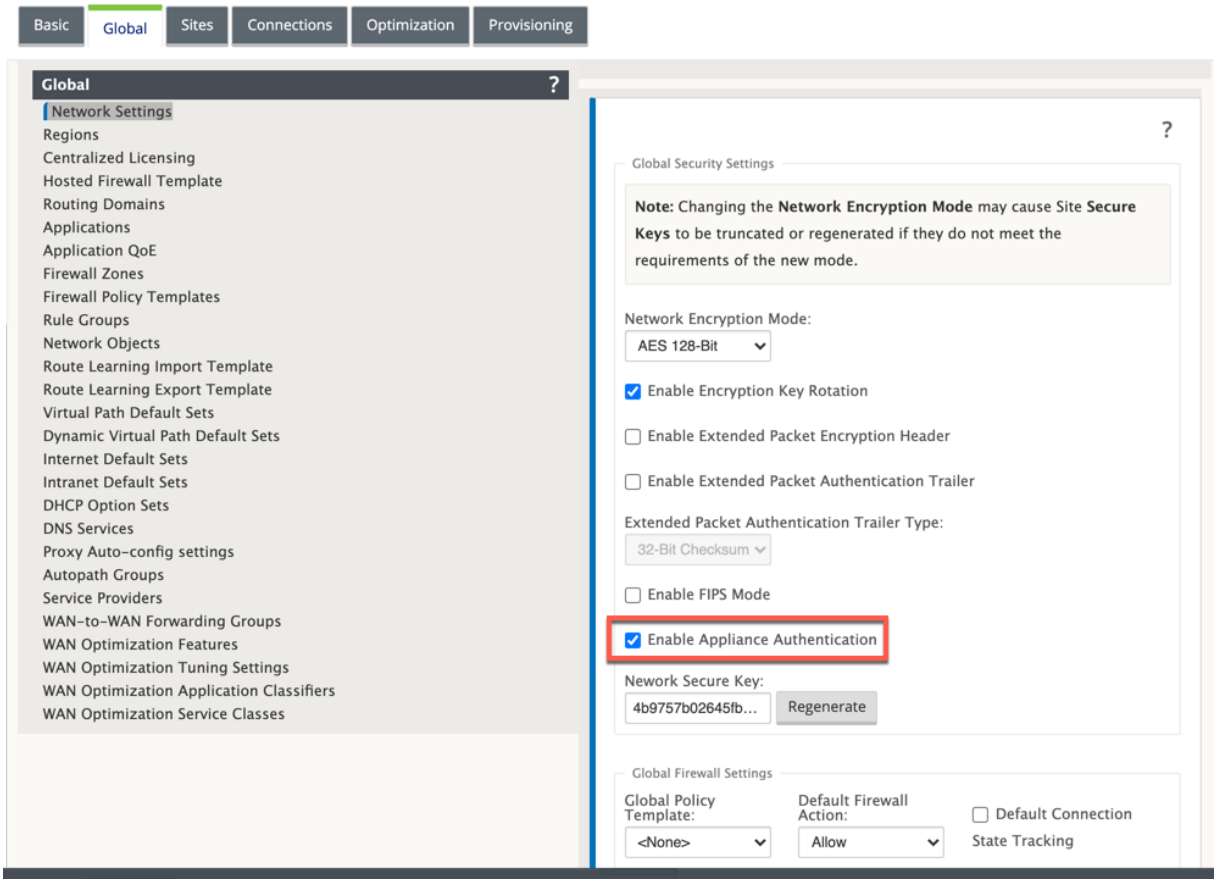
October 28, 2021

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 zertifikatbasierte Authentifizierung in Citrix SD-WAN 11.0.2 eingeführt.

Mit der Zertifikatauthentifizierung können Unternehmen Zertifikate verwenden, die von ihrer privaten Zertifizierungsstelle (CA) ausgestellt wurden, um Appliances zu authentifizieren. Die Appliances werden authentifiziert, bevor die virtuellen Pfade eingerichtet werden. Wenn beispielsweise eine Zweigeinheit versucht, eine Verbindung zum Rechenzentrum herzustellen, und das Zertifikat von der Zweigstelle nicht mit dem vom Rechenzentrum erwarteten Zertifikat übereinstimmt, wird der virtuelle Pfad nicht eingerichtet.

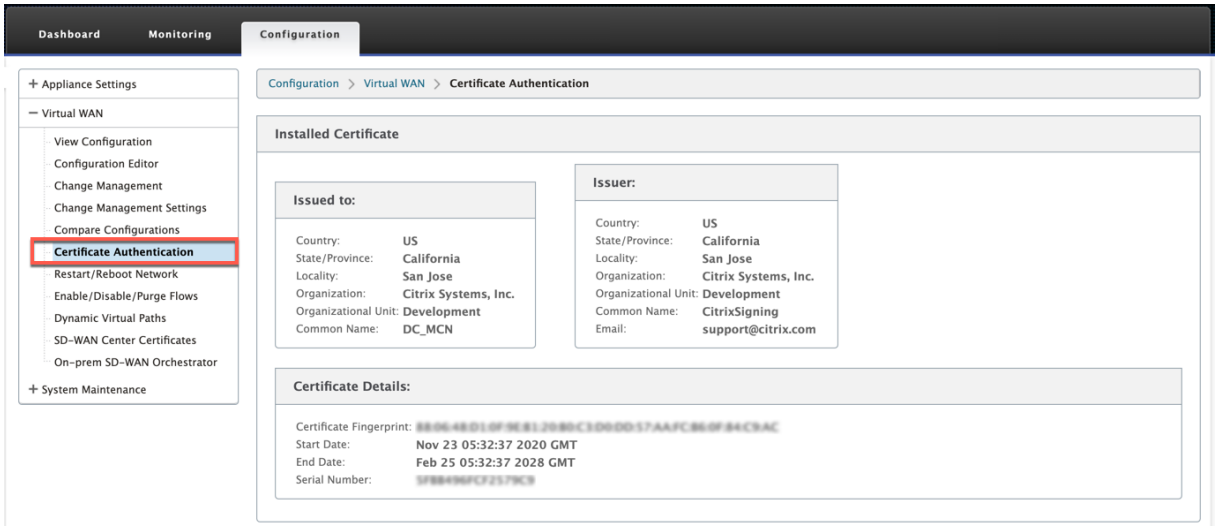
Das von der CA ausgestellte Zertifikat bindet einen öffentlichen Schlüssel an den Namen der Appliance. Der öffentliche Schlüssel arbeitet mit dem entsprechenden privaten Schlüssel, der im Besitz der durch das Zertifikat identifizierten Appliance ist.

Um die Appliance-Authentifizierung zu aktivieren, navigieren Sie im Konfigurationseditor zu **Global** > **Netzwerkeinstellungen** und wählen Sie **Einheitenauthentifizierung aktivieren** aus.



Nachdem die Konfiguration vorgenommen und angewendet wurde, wird eine neue Option für die **Zertifikatauthentifizierung** unter **Konfiguration** > **Virtuelles WAN**aufgeführt.

Sie können alle Zertifikate, die für die Authentifizierung virtueller Pfade verwendet werden, auf der Seite **Zertifikatauthentifizierung** verwalten.

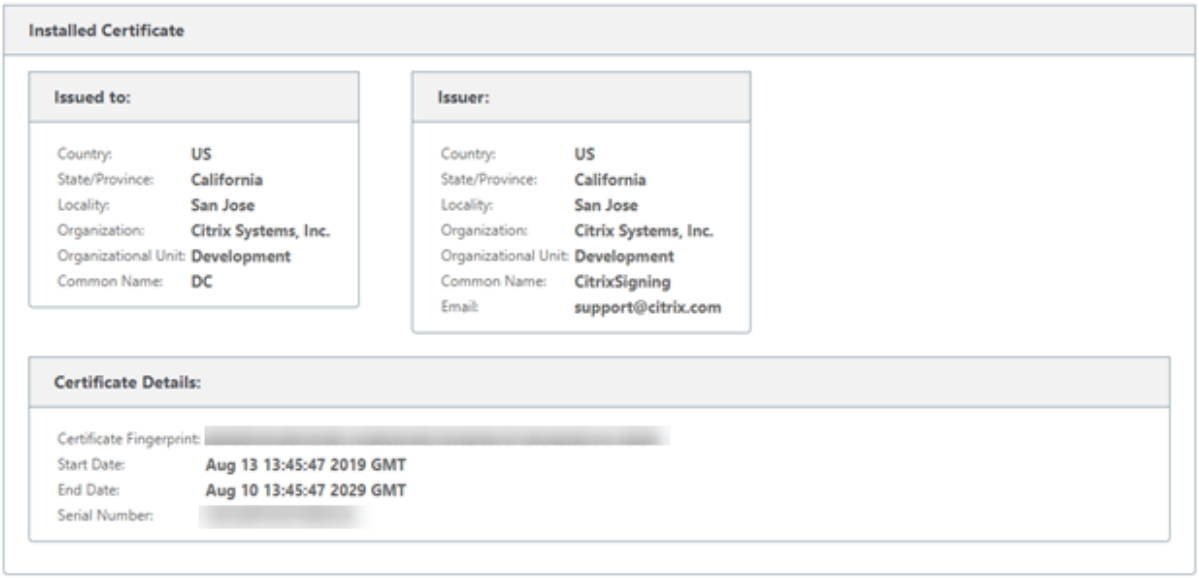


> **Hinweis**
>
> Wenn Sie die Appliance-Software von SD-WAN Version 11.0 auf Version 11.1 oder höher aktualisieren, deaktivieren Sie die Option **“Appliance-Authentifizierung aktivieren** “und führen Sie das Software-Upgrade durch. Sobald der Upgradevorgang abgeschlossen ist, wählen Sie die Option “**Appliance-Authentifizierung aktivieren** “.

Installiertes Zertifikat

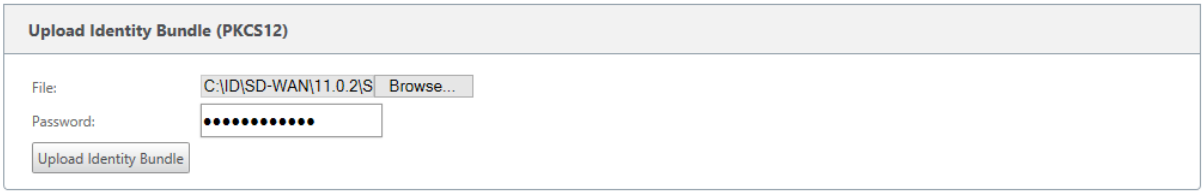
Der Abschnitt **Installiertes Zertifikat** enthält eine Zusammenfassung des auf der Appliance installierten Zertifikats. Die Appliance verwendet dieses Zertifikat, um sich im Netzwerk zu identifizieren.

Der Abschnitt **Ausgestellt** für enthält Einzelheiten 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 Zertifizierungsstelle, die das Zertifikat unterzeichnet hat. Zu den Zertifikatsdetails gehören der Fingerabdruck des Zertifikats, die Seriennummer und die Gültigkeitsdauer des Zertifikats.



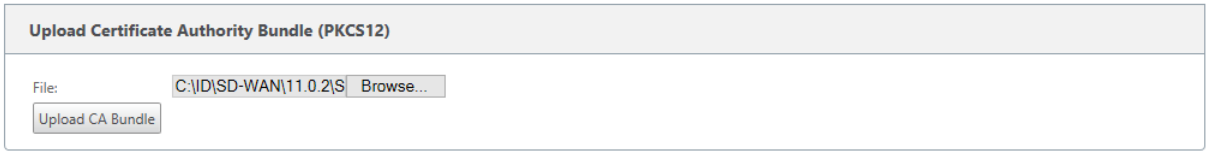
Identitätsbündel hochladen

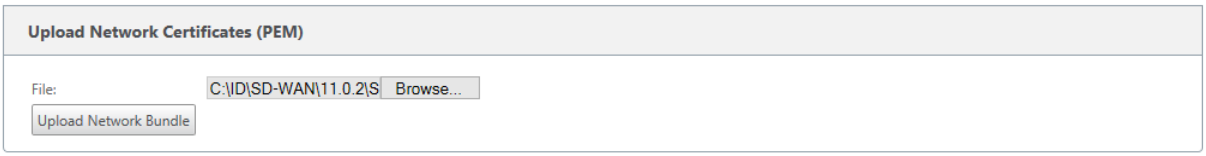
Das Identity-Paket enthält einen privaten Schlüssel und das dem privaten Schlüssel zugeordnete Zertifikat. Sie können das von der CA ausgestellte Appliance-Zertifikat in die Appliance hochladen. Das Zertifikatspaket ist eine PKCS 12-Datei mit der Erweiterung.p12. Sie können es mit einem Kennwort schützen. Wenn Sie das Kennwortfeld leer lassen, wird es als kein Kennwortschutz behandelt.



Laden Sie das Paket der Zertifizierungsstelle hoch

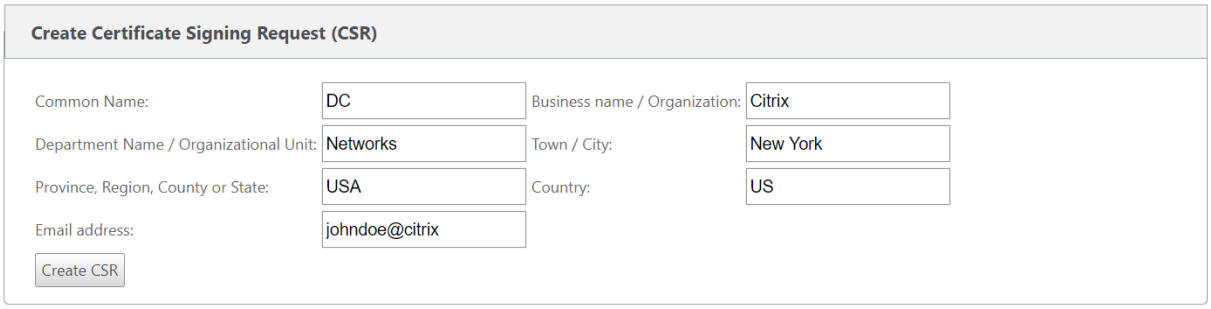
Laden Sie das PKCS 12-Bundle hoch, das der Zertifizierungsstelle entspricht. Das Paket der Zertifizierungsstelle enthält die komplette Signaturkette, das Stammverzeichnis und die gesamte zwischenunterzeichnende Behörde.





Erstellen einer Signaturanfrage für

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, die Organisationsdetails und die Adresse der Appliance an.

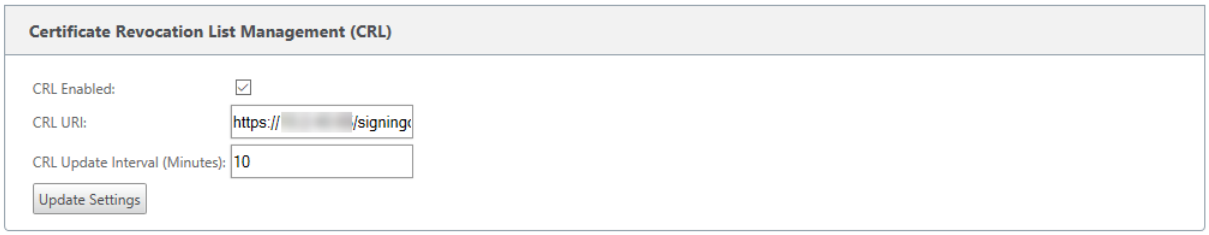


Listenmanager für Zertifikatsperrung

Eine Certificate Revocation List (CRL) ist eine veröffentlichte Liste von Zertifikatseriennummern, 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, überprüft der Responder die Zertifikatsperrliste, um zu sehen, ob das Initiatorenzertifikat bereits gesperrt wurde. Citrix SD-WAN unterstützt derzeit CRLs der Version 1 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 zum Überprüfen und Herunterladen der CRL-Datei an. Der Bereich beträgt 1—1440 Minuten.



> **Hinweis**
>
> Der Zeitraum für die erneute Authentifizierung für einen virtua1-Pfad kann zwischen 10—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, mit denen Anwendungs- und Transaktionsdaten in der Netzwerkinfrastruktur identifiziert und gesammelt werden. Diese Daten geben eine bessere Einsicht in die Auslastung und Leistung des Anwendungsdatenverkehrs.

Die gesammelten Daten, Flussaufzeichnungen genannt, werden an einen oder mehrere IPv4-Sammler übertragen. Die Kollektoren aggregieren die Flow-Datensätze und generieren Echtzeit- oder historische Berichte.

AppFlow

AppFlow exportiert Flow-Level-Daten nur für HDX/ICA-Verbindungen. Sie können entweder TCP nur für HDX-Dataset-Vorlage oder die HDX-Dataset-Vorlage aktivieren. Der TCP nur für HDX-Datensatz liefert Multi-Hop-Daten. Der HDX-Datensatz liefert HDX-Einblickdaten.

> **Hinweis**
>
> Die HDX-Vorlage ist nur für Citrix SD-WAN PE Edition und Zwei-Box-Appliances verfügbar. Es sollte auf der Rechenzentrums-Appliance aktiviert sein.

AppFlow Collectors wie Splunk und Citrix ADM verfügen über Dashboards zur Interpretation und Präsentation dieser Vorlagen.

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	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP-Protokollnummer	protocoldentifier,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 flow0x01: egress flowWAN-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	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP-Protokollnummer	protocoldentifier,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 flow0x01: egress flowWAN-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	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	

Einschränkungen

- Das Exportintervall für Net Flow wird von 15 Sekunden auf 60 Sekunden erhöht.

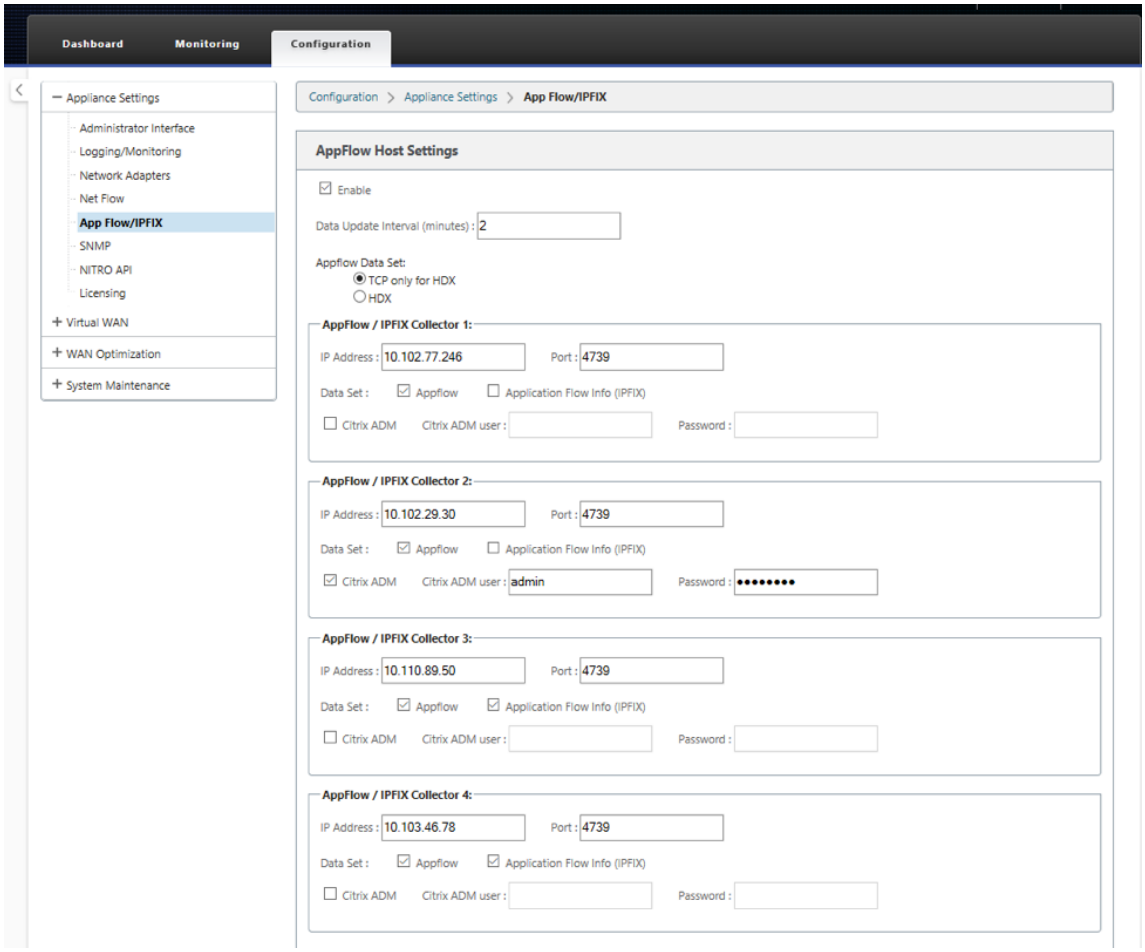
- AppFlow/IPFIX Flows werden über UDP übertragen, bei Verbindungsverlust werden nicht alle Daten erneut übertragen. Wenn das Exportintervall auf X Minuten eingestellt ist, speichert die Appliance nur X Minuten Daten. Welches wird nach X Minuten Verbindungsverlust erneut übertragen.
- In Citrix SD-WAN, Version 10 Version 2, werden die **AppFlow-Einstellungen** lokal für jede Appliance vorgenommen, während es sich in den vorherigen Versionen um eine globale Einstellung handelte. Wenn die SD-WAN-Softwareversion auf eine der vorherigen Versionen heruntergestuft wird und AppFlow auf einer der Appliances konfiguriert ist, wird es 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 an 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**.



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-Datensatzvorlage** aus, Sie können eine der folgenden Datensatzvorlagen wählen:

   - **TCP nur für HDX (AppFlow)**: Die AppFlow-Datensatzvorlage zum Sammeln und Senden von Multi-Hop-Daten von ICA-Verbindungen an den AppFlow-Kollektor.
   - **HDX (AppFlow)**: Die AppFlow-Datensatzvorlage zum Sammeln und Senden von HDX-Insight-Daten von ICA-Verbindungen an den AppFlow-Sammler.

   > **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-Collector-Systems.

- **Port**: Die Portnummer, auf der das externe AppFlow/IPFIX-Collector-System lauscht. 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 unterstützt keine IPv6-Adressen für AppFlow und IPFIX.

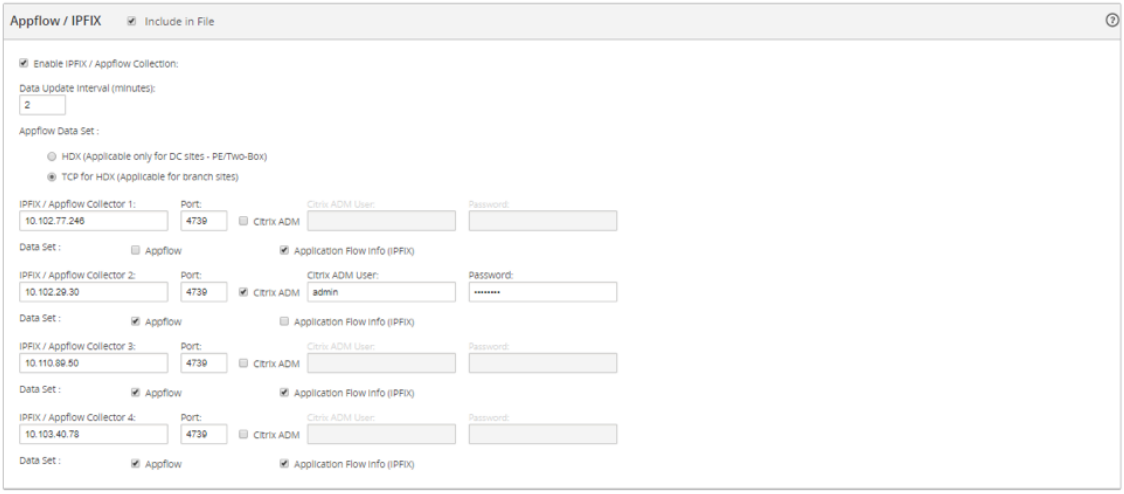
- **Citrix ADM Benutzer**: Benutzername des Citrix ADM -Kollektors
- **Kennwort**: Citrix ADM Collector-Kennwort.

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 den **AppFlow/IPFIX-Collector** mithilfe von Citrix SD-WAN Center:

1. Navigieren Sie in der Citrix SD-WAN Center-Verwaltungsoberfläche 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**.



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-Datensatzvorlage** aus, Sie können eine der folgenden Datensatzvorlagen wählen:
   - **TCP nur für HDX**: Die AppFlow-Datensatzvorlage zum Sammeln und Senden von Multi-Hop-Daten von ICA-Verbindungen an den AppFlow-Collector.
   - **HDX**: Die AppFlow-Datensatzvorlage zum Sammeln und Senden von HDX-Insight-Daten von ICA-Verbindungen an den AppFlow-Sammler.

   > **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-Collector-Systems.
   - **Port**: Die Portnummer, auf der das externe AppFlow/IPFIX-Collector-System lauscht. 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-Collectors.
   - **Kennwort**: Citrix ADM Collector-Kennwort.

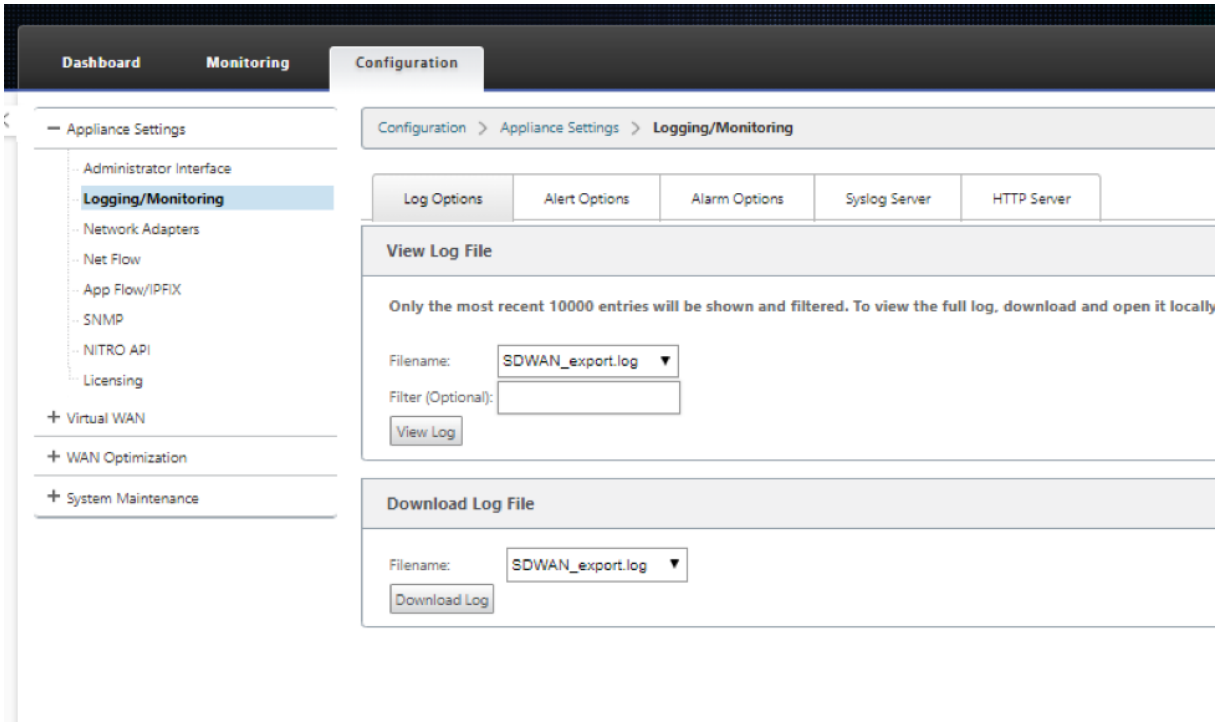
     Der Benutzername und das Kennwort werden verwendet, um sich nahtlos bei Citrix ADM anzumelden und Flussdaten zu speichern.

7. **Speichern** und **exportieren** Sie die Konfiguration in die verwalteten Appliances.

> **Hinweis**
>
> Wenn die SD-WAN Center-Version niedriger als 10.2 ist und die SD-WAN-Appliance-Version 10.2 und höher ist, können Sie die folgenden Bedingungen beachten.
>
> - Wenn lokale Collectors auf den Appliances aktiviert sind, wirkt sich die vom SD-WAN-Center übermittelte AppFlow/IPFIX-Konfiguration 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 Dateien SDWAN_export.log anzeigen und herunterladen. Navigieren Sie zu **Konfiguration > Protokollierung/Überwachung** und wählen Sie die Dateien **SDWAN_export.log** aus.



SNMP

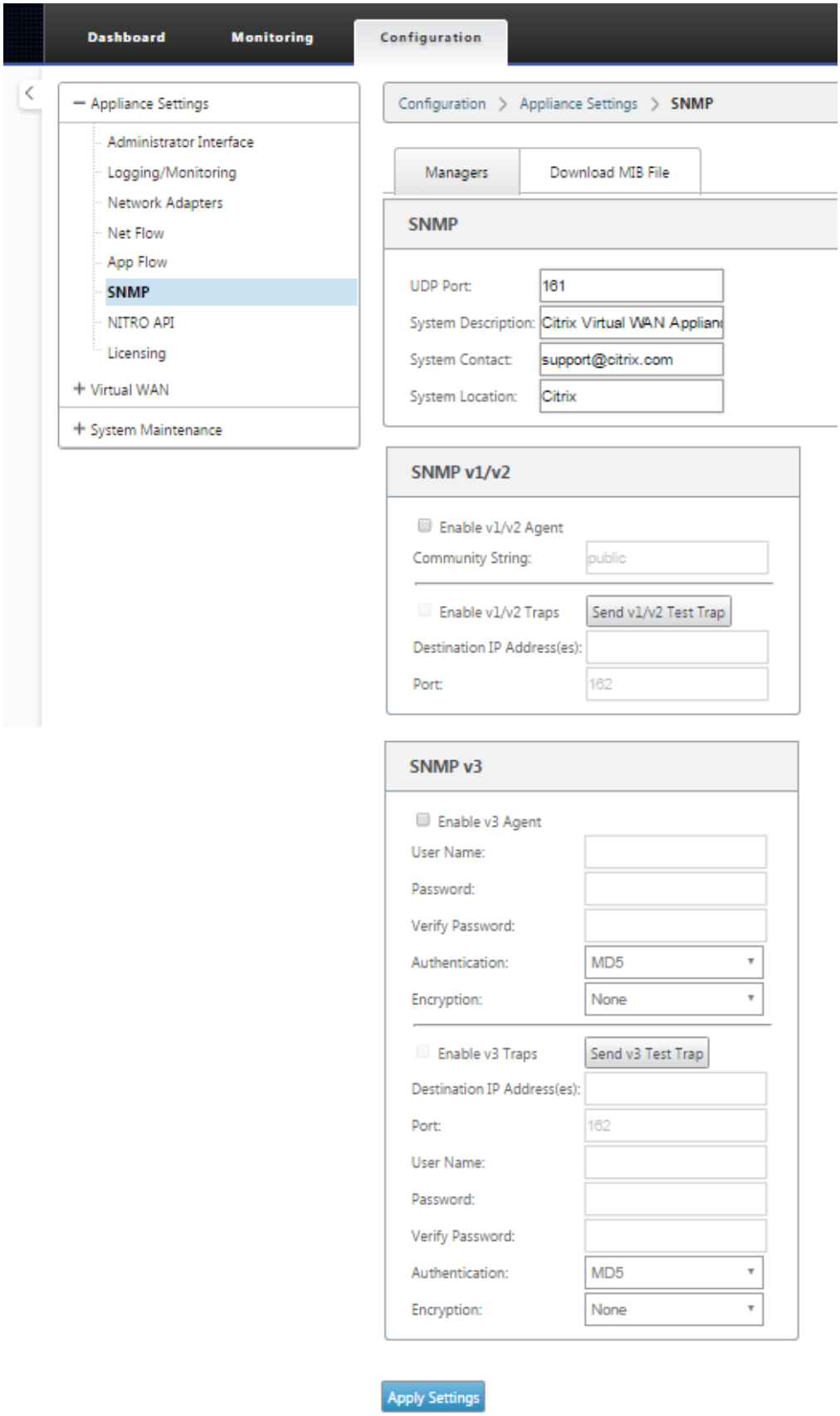
November 16, 2022

Citrix SD-WAN unterstützt die Fähigkeit SNMPV1/V2 und nur ein einziges 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.

> **HINWEIS**
>
> Um eine IPv6-Adresse zu konfigurieren, stellen Sie sicher, dass der SNMP-Server auch mit einer IPv6-Adresse konfiguriert ist.



Standard MIB Support

Die folgenden Standard-MIBs werden von den SD-WAN Appliances unterstützt.

MIB	RFC (Definitionslink)
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 (Partial)	https://www.ietf.org/rfc/rfc4293.txt
Q-BRIDGE-MIB (Partial)	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

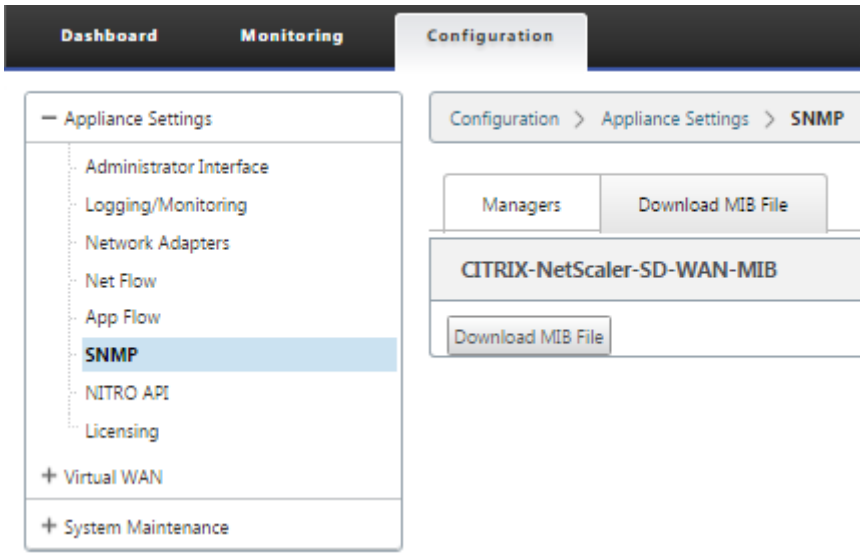
Sie müssen die folgenden SNMP-Dateien herunterladen, bevor Sie mit der Überwachung einer Citrix SD-WAN-Appliance beginnen können:

- 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-Listenern verwendet. Die Dateien enthalten die SD-WAN-Appliance Enterprise MIBs, die SD-WAN-spezifische Ereignisse bereitstellen. So laden Sie MIB-Dateien in der SD-WAN-Webverwaltungsschnittstelle herunter:

1. Navigieren Sie zur Seite **Konfiguration** > **Appliance-Einstellungen** > **SNMP** > **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**
>
> - Unterstützung für diese MIBs wird standardmäßig vom **net-snmp snmpd-Daemon-Prozess** auf Linux-Systemen bereitgestellt. Die MIBs bieten die Grundlage für die Unterstützung von Netzwerkmanagement-Anwendungen.
> - Das Ethernet-Port-Paket und die Byte-Zähler befinden sich in der **IF-MIB** innerhalb der **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 des SNMP-Managers, zum Konfigurieren von SNMP View/Alarm und zum Hinzufügen eines SNMP-Servers finden Sie in der CloudBridge 7.4-Dokumentation unter: CloudBridge

Administrative Schnittstelle

October 28, 2021

Sie können Ihre Citrix SD-WAN-Appliances mithilfe der folgenden Verwaltungsoptionen verwalten und warten:

- Benutzerkonten
- RADIUS-Server
- TACACS+ Server
- HTTPS Cert
- HTTPS-Einstellungen
- Sonstiges

Benutzerkonten

Sie können neue Benutzerkonten hinzufügen und die vorhandenen Benutzerkonten verwalten unter **Konfiguration > Appliance-Einstellungen > Seite Administratorschnittstelle > Registerkarte Benutzerkonten**.

Sie können die neu hinzugefügten Benutzerkonten entweder lokal von der SD-WAN-Appliance oder remote authentifizieren. Benutzerkonten, die remote authentifiziert werden, werden über RADIUS- oder TACACS+-Authentifizierungsserver authentifiziert.

User-Rollen

Die folgenden Benutzerrollen werden unterstützt:

- **Viewer**: Viewer-Konto ist ein schreibgeschütztes Konto mit Zugriff auf **Dashboard**, **Reporting** und **Monitoring**-Seiten.
- **Admin**: Das Admin-Konto verfügt über die Administratorrechte und den Lese-/Schreibzugriff auf alle Abschnitte.

  Ein Superadministrator (admin) hat die folgenden Berechtigungen:

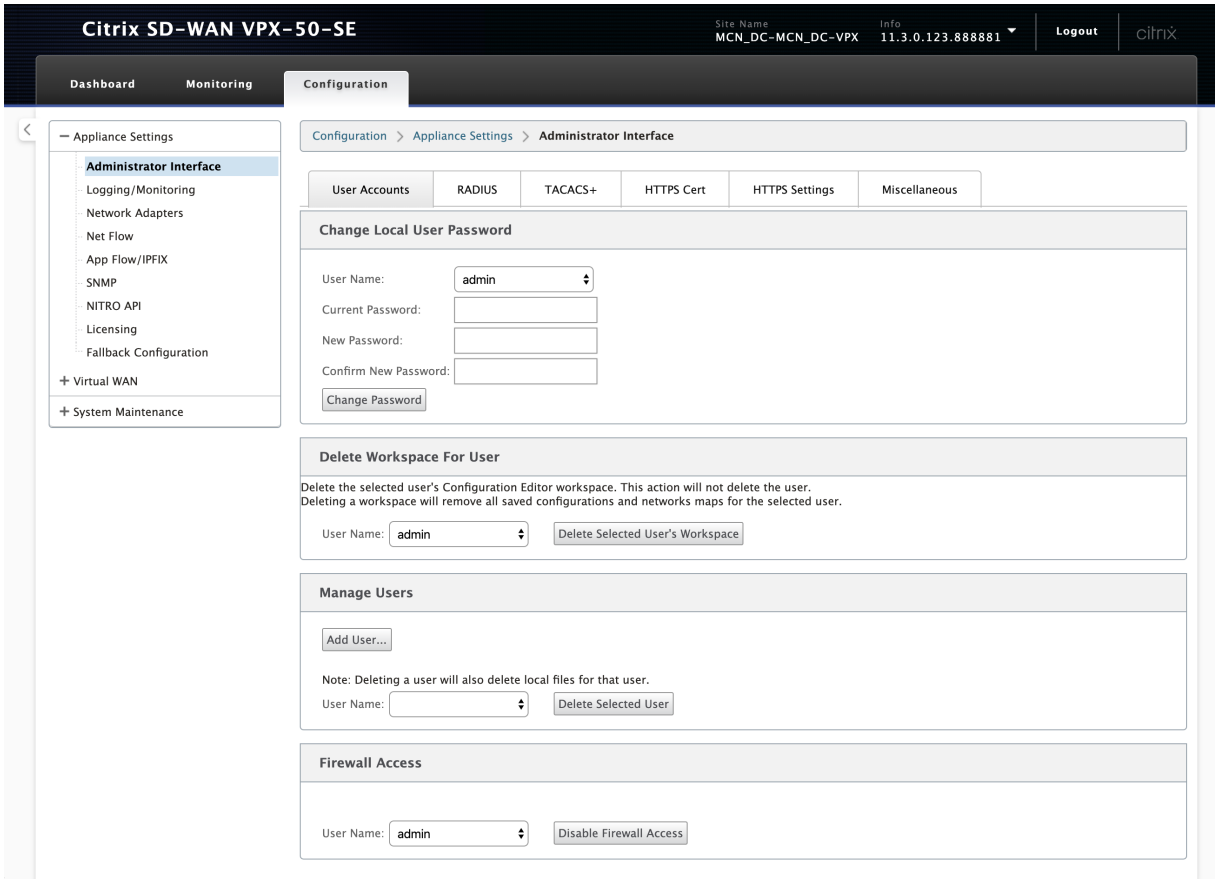
  - Kann die Konfiguration in den Posteingang zur Änderungsverwaltung exportieren, um eine Konfiguration und ein Softwareupdate im Netzwerk durchzuführen.
  - Kann auch den Lese-/Schreibzugriff der Netzwerk- und Sicherheits-Admins umschalten.
  - Behält sowohl Netzwerk- als auch sicherheitsbezogene Einstellungen bei.
- **Sicherheitsadministrator**: Ein Sicherheitsadministrator hat den Lese-/Schreibzugriff nur für die Firewall- und sicherheitsbezogenen Einstellungen im **Konfigurationseditor**, während er

schreibgeschützten Zugriff auf die übrigen Abschnitte hat. Der Sicherheitsadministrator hat auch die Möglichkeit, den Schreibzugriff auf die Firewall für andere Benutzer außer dem Superadministrator (Admin) zu aktivieren oder zu deaktivieren.

- **Netzwerkadministrator**: Ein Netzwerkadministrator hat Lese- und Schreibberechtigungen für alle Abschnitte und kann einen Zweig mit Ausnahme der Firewall- und sicherheitsbezogenen Einstellungen im **Konfigurationseditor**vollständig bereitstellen. Der gehostete Firewallknoten ist für den Netzwerkadministrator nicht verfügbar. In diesem Fall muss der Netzwerkadministrator eine neue Konfiguration importieren.

Sowohl der Netzwerkadministrator als auch der Sicherheitsadministrator können Änderungen an der Konfiguration vornehmen und diese auch im Netzwerk bereitstellen.

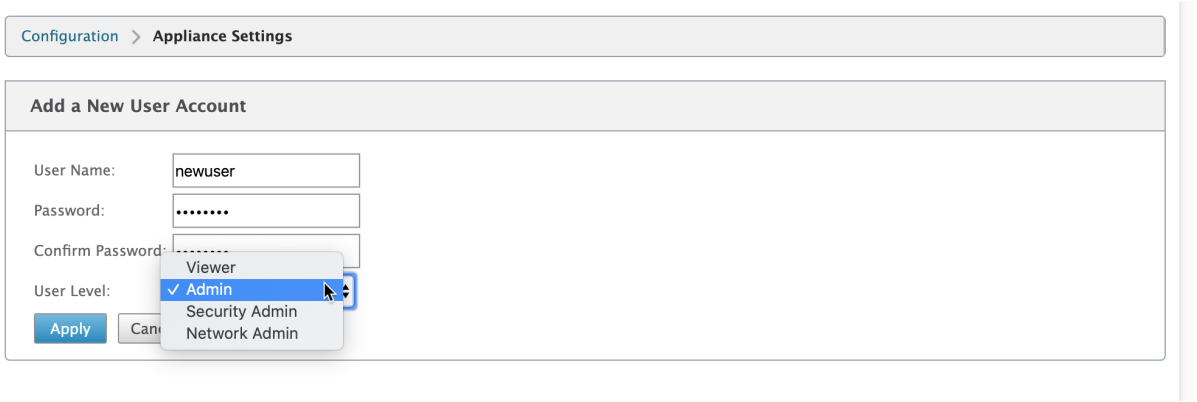
> **HINWEIS**
>
> Der Netzwerkadministrator und Sicherheitsadministrator können keine Benutzerkonten hinzufügen oder löschen. Sie können nur die Kennwörter ihrer eigenen Konten bearbeiten.



Benutzer hinzufügen

Um einen Benutzer hinzuzufügen, klicken Sie im Abschnitt **Benutzer**verwalten auf Benutzer**hinzufügen**. Geben Sie den **Benutzernamen** und das **Kennwort ein**. Wählen Sie die Benutzerrolle aus der Dropdownliste **Benutzerebene** aus und klicken Sie auf **Übernehmen**.

Sie können bei Bedarf auch ein Benutzerkonto löschen. Durch das Löschen eines Benutzers werden auch die lokalen Dateien gelöscht, die diesem Benutzer gehören. Um zu löschen, wählen Sie im Abschnitt **Benutzer verwalten** den Benutzer aus der Dropdownliste **Benutzername** aus und klicken Sie auf **Ausgewählten Benutzer löschen**.



Kennwort eines Benutzers ändern

Die Administratorrolle kann das Kennwort eines Benutzerkontos ändern, das lokal von der SD-WAN-Appliance authentifiziert wird.

Um das Kennwort zu ändern, wählen Sie im Abschnitt **Lokales Benutzerkennwort** ändern den Benutzer aus der Dropdownliste **Benutzername** aus. Geben Sie das aktuelle Kennwort und das neue Kennwort ein. Klicken Sie auf **Kennwort ändern**.

Arbeitsbereich für einen Benutzer löschen

Sie können den Workspace des **Konfigurationseditors** für einen Benutzer löschen. Durch das Löschen des Workspace wird das Benutzerkonto nicht gelöscht. Es werden alle gespeicherten Konfigurationen und Netzwerkkarten für den ausgewählten Benutzer entfernt.

Um den Workspace für einen Benutzer zu **löschen, wählen Sie im Abschnitt Workspace für Benutzer** löschen den Benutzer aus der Dropdownliste **Benutzername** aus. Klicken Sie auf **Arbeitsbereich des ausgewählten Benutzers löschen**.

Deaktivieren Sie den Zugriff auf Firewall

Sie können den Firewallzugriff auf ein Benutzerkonto deaktivieren. Um dies zu deaktivieren, wählen Sie den Benutzer aus der Dropdownliste **Benutzername** aus und klicken Sie auf **Firewallzugriff deaktivieren**.

RADIUS-Server

Sie können eine SD-WAN-Appliance so konfigurieren, dass der Benutzerzugriff bei einem oder maximal drei RADIUS-Servern authentifiziert wird. Der Standardport ist 1812.

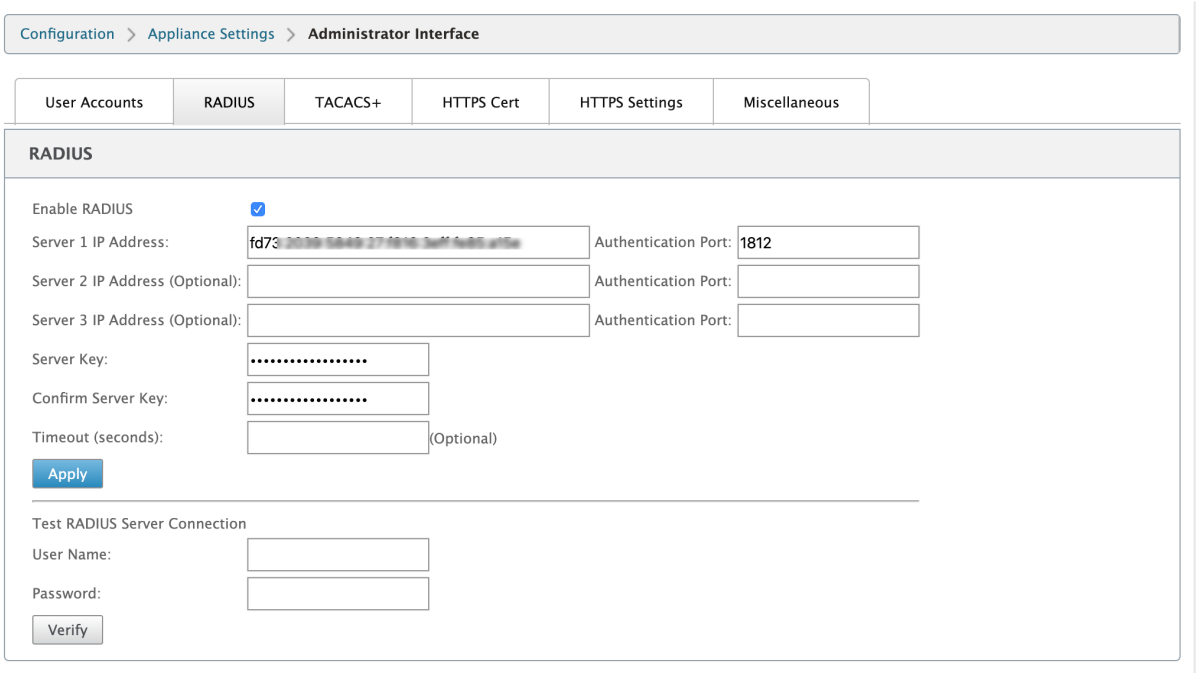
So konfigurieren Sie den RADIUS-Server:

1. Navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Administratorschnittstelle > RADIUS**.
2. Aktivieren Sie das Kontrollkästchen **Radius aktivieren**.
3. Geben Sie die **Server-IP-Adresse** und den **Authentifizierungsport** ein. Es können maximal drei Server-IP-Adressen konfiguriert werden.

   > **HINWEIS**
   >
   > Um eine IPv6-Adresse zu konfigurieren, stellen Sie sicher, dass der RADIUS-Server auch mit einer IPv6-Adresse konfiguriert ist.

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



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. Navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Administratorschnittstelle > TACACS+**.
2. **Aktivieren Sie das Kontrollkästchen Enable TACACS+**.
3. Geben Sie die **Server-IP-Adresse** und den **Authentifizierungsport** ein. Es können maximal drei Server-IP-Adressen konfiguriert werden.

   > **HINWEIS**
   >
   > Um eine IPv6-Adresse zu konfigurieren, stellen Sie sicher, dass der TACACS+-Server auch mit einer IPv6-Adresse konfiguriert ist.

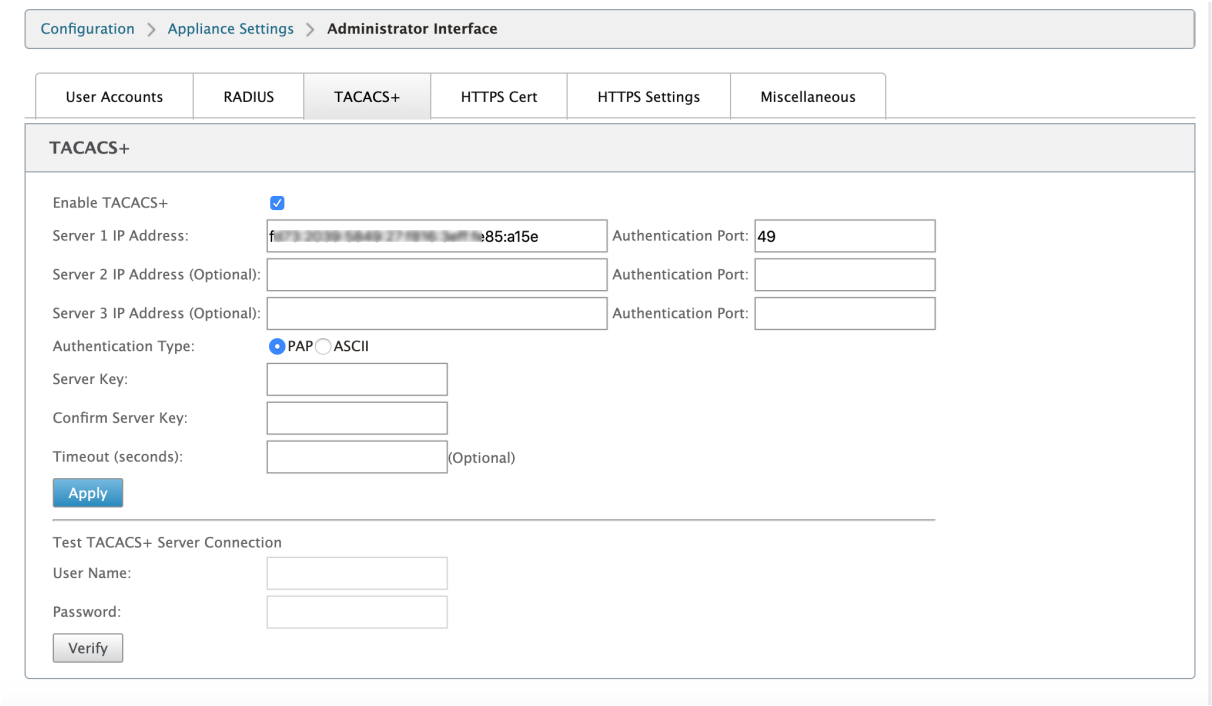
4. Wählen Sie **PAP** oder **ASCII** als Authentifizierungstyp aus.

   - PAP: Verwendet PAP (Password Authentication Protocol), um die Benutzerauthentifizierung zu stärken, indem dem TACACS+-Server ein starkes gemeinsames Geheimnis zugewiesen wird.

- ASCII: Verwendet den ASCII-Zeichensatz, um die Benutzerauthentifizierung zu stärken, indem dem TACACS+-Server ein starkes gemeinsames Geheimnis zugewiesen wird.

5. Geben Sie den **Server-Schlüssel** ein und bestätigen Sie.
6. Geben Sie den **Timeout-Wert** in Sekunden ein.
7. Klicken Sie auf **Speichern**.

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



NDP-Router-Werbung und Präfix-Delegationsgruppe

October 28, 2021

NDP-Router-Werbung

In einem IPv6-Netzwerk findet regelmäßig ein Multicasting durch die SD-WAN-Appliance von Router Advertisement (RA)-Nachrichten statt, um ihre Verfügbarkeit anzukündigen und Informationen an die benachbarten Appliances im SD-WAN-Netzwerk zu übermitteln. Die Router-Anzeigen enthalten die IPv6-Präfix-Informationen. Das Neighbor Discovery-Protokoll (NDP), das auf SD-WAN-Appliances ausgeführt wird, verwendet diese Router-Anzeigen, um die benachbarten Geräte auf demselben Link zu

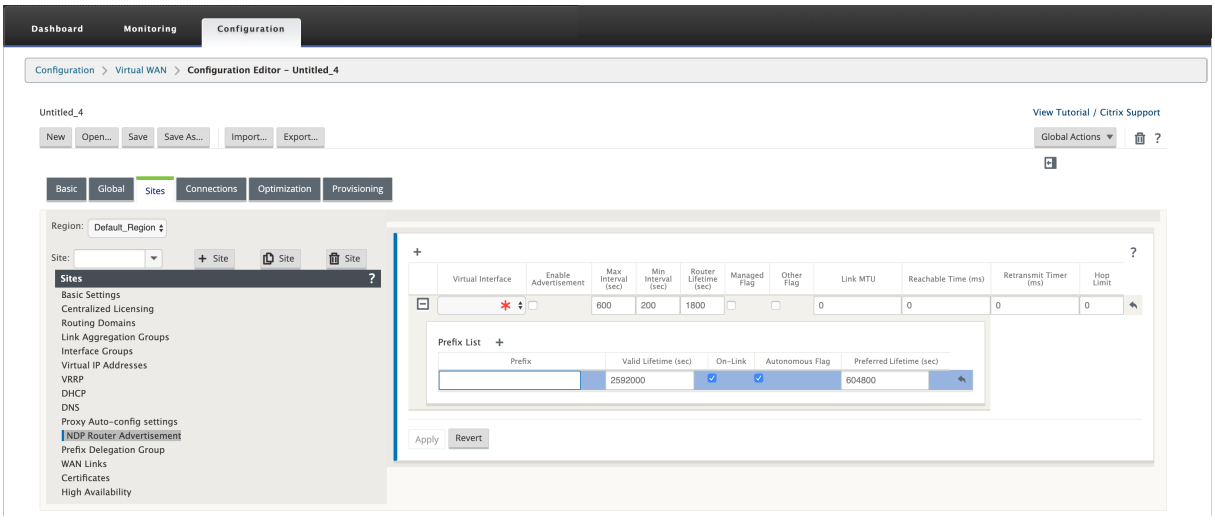
ermitteln. Es bestimmt auch die Link-Layer-Adressen des anderen, findet Nachbarn und verwaltet Informationen zur Erreichbarkeit der Erreichbarkeit über die Wege zu aktiven Nachbarn.

Um die NDP-Router-Werbung zu konfigurieren,

1. Navigieren Sie im Konfigurationseditor zu **Sites > NDP Router Advertisement**.
2. Klicken Sie auf **+** und wählen Sie eine der konfigurierten virtuellen Schnittstellen aus der Dropdownliste **Virtuelle Schnittstelle** aus.
3. Aktivieren Sie das Kontrollkästchen **Werbung aktivieren**, um das Senden von periodischen Router-Advertisements und das Reagieren auf Router Solicitations für die ausgewählte virtuelle Schnittstelle zu ermöglichen.
4. Geben Sie die maximalen, minimalen und Router-Lebenszeitintervalle an.
   - **Maximales Intervall**: Die maximal zulässige Zeit (in Sekunden) zwischen dem Senden periodischer unerwünschter Multicast-Router-Werbung.
   - **Mindestintervall**: Die Mindestdauer (in Sekunden), die zwischen dem Senden periodischer unerwünschter Multicast-Router-Werbung zulässig ist.
   - **Router Lifetime**: Die Zeit (in Sekunden), die der Router von den Hosts als gültig betrachtet wird. 0 gibt an, dass der Router nicht als Standard-Router verwendet werden kann.
5. Aktivieren Sie das Kontrollkästchen **Managed Flag**, wenn IP-Adressen über das DHCPv6-Protokoll verfügbar sind.
6. Aktivieren Sie das Kontrollkästchen **Anderes Flag**, wenn die Konfigurationsinformationen (außer den IP-Adressen) über das DHCPv6-Protokoll verfügbar sind.
7. Geben Sie die folgenden Werte für die ausgewählte Schnittstelle an.
   - **Link MTU**: Die empfohlene Maximum Transmission Unit (MTU) für die Schnittstelle.
   - **Erreichbare Zeit**: Die Zeit (in Millisekunden), die das NDP-Protokoll im Status "**Reachable** "verbleibt.
   - **Retransmit-Timer**: Die Zeit (in Millisekunden) zwischen der erneuten Übertragung von Neighbor Solicitation Nachrichten beim Auflösen einer IP-Adresse oder der Untersuchung eines Nachbarn.
   - **Hop-Limit**: Die maximale Anzahl von Hops, die in die Router-Werbung aufgenommen werden sollen.
8. Geben Sie die mit dem Präfix verknüpften Details ein.
   - **Präfix**: Die Präfix- und Präfixlänge in der Cassless Inter-Domain Routing (CIDR) -Notation.
   - **Gültige Lebensdauer**: Die Zeit in Sekunden, bis zu der das Präfix gültig ist. -1 steht für unendlich, was bedeutet, dass das Präfix für immer erhalten bleibt.
   - **On-Link**: Wenn diese Option ausgewählt ist, wird das Präfix als lokal für das Netzwerk betrachtet.

- **Autonomes Flag**: Wenn diese Option aktiviert ist, wird das Präfix von der Stateless Address Autoconfiguration (SLAAC) des Hosts verwendet, um die IP-Adresse zu generieren.
- **Präfix-Lebensdauer**: Die Zeit (in Sekunden), bis zu der das Präfix als bevorzugt gilt.

9. Klicken Sie auf **Apply**.
10. Um weitere virtuelle Schnittstellen für NDP-Router-Werbung zu konfigurieren, klicken Sie auf **+**.



Präfix-Delegierungsgruppe

> **HINWEIS**
>
> Die Präfixdelegierung wird in der Citrix SD-WAN 11.3-Version nicht unterstützt.

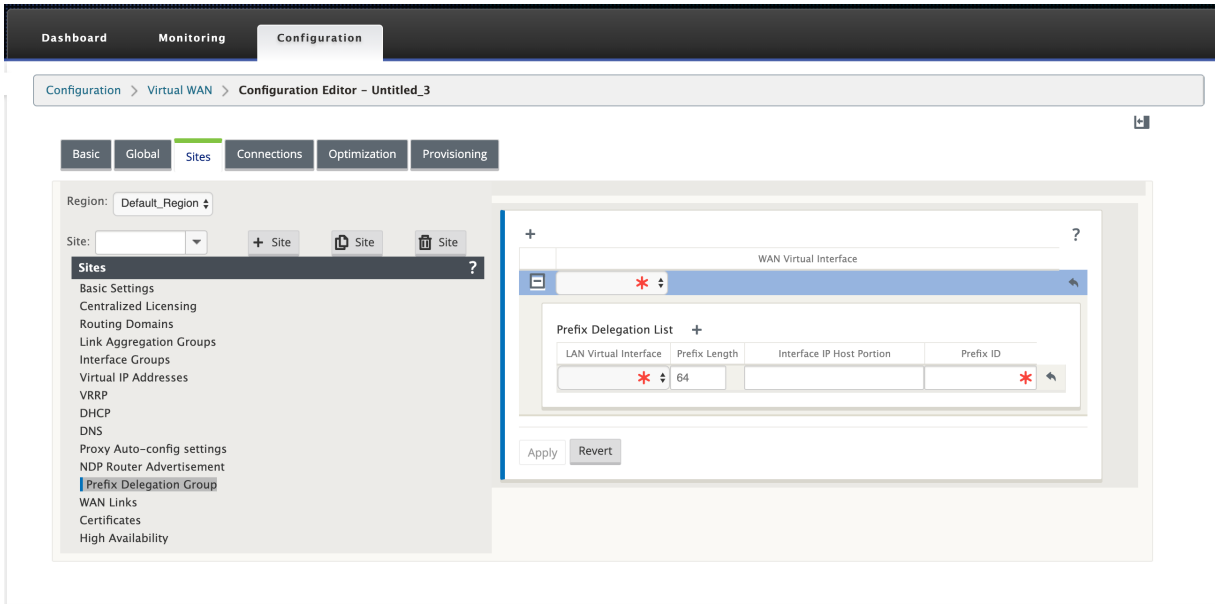
Citrix SD-WAN Appliances können als DHCPv6-Client konfiguriert werden, um ein Präfix vom ISP über den konfigurierten WAN-Port anzufordern. Sobald die Citrix SD-WAN Appliance das Präfix erhält, verwendet sie das Präfix, um einen Pool von IP-Adressen zu erstellen, um die LAN-Clients zu bedienen. Die Citrix SD-WAN Appliance verhält sich dann wie ein DHCP-Server und kündigt das Präfix auf den LAN-Ports an die LAN-Clients an.

Um die Präfixdelegierung zu konfigurieren,

1. Navigieren Sie im Konfigurationseditor zu **Sites > Präfix Delegierungsgruppe**.
2. Klicken Sie auf **+** und wählen Sie ein konfiguriertes WAN Virtual Interface aus, auf dem das Präfix vom ISP angefordert wird.
3. Geben Sie die folgenden Details an:
   - **LAN Virtual Interface**: Wählen Sie eine der konfigurierten virtuellen LAN-Schnittstellen aus, für die das Präfix angefordert wird.

- **Präfixlänge**: Die Anzahl der Bits einer Global Unicast IPv6-Adresse, die Teil des Präfixes sind.
- **Interface-IP-Hostteil**: Der Host-Teil, der für die IP-Adresse der Schnittstelle verwendet werden soll.
- **Präfix-ID**: Eine eindeutige Kennung zur Identifizierung der Präfix-Delegierungsanforderungen für die LAN-Schnittstelle.

4. Klicken Sie auf **Apply**.
5. Um weitere virtuelle WAN-Schnittstellen als Teil der Präfix-Delegierungsgruppe zu konfigurieren, klicken Sie auf **+**.



WAN-Optimierung

October 28, 2021

Die Citrix SD-WAN WANOP-Appliance optimiert WANOP-Verbindungen und sorgt so für maximale Reaktionsfähigkeit und Durchsatz. Die Citrix SD-WAN WANOP-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
- Verkehrs-Management

- Anwendungs-Beschleunigung
- Citrix XenApp/XenDesktop (HDX) -Beschleunigung
- Integration
- Monitoring und Management

Informationen zur Installation, Bereitstellung und Funktionskonfiguration von Citrix SD-WAN WANOP 10.2 finden Sie in der Citrix SD-WAN WANOP-Dokumentation. 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

October 28, 2021

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 des Abschnitts **Optimierung** im **Konfigurationseditor** im Web Management Interface auf dem MCN.

> **Hinweis**
>
> Sie müssen eine SD-WAN Premium (Enterprise) Edition-Lizenz installiert haben, um auf WAN-Optimierungsfunktionen in Ihrem virtuellen WAN zugreifen, diese aktivieren, konfigurieren und aktivieren zu können. 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 lauten wie folgt und in der Reihenfolge der Abhängigkeit aufgeführt:

1. Aktivieren Sie die WAN-Optimierung und passen Sie die **Standardkonfiguration** an oder akzeptieren Sie die Standardeinstellungen.

   Die **Standardkonfiguration** wird als **Basisoptimierungskonfiguration** für alle Standorte verwendet, die für die WAN-Optimierung in Frage kommen. Die **Standardkonfiguration** ist vorkonfiguriert und kann angepasst werden.

> **Hinweis**
>
> Anweisungen finden Sie unter Optimierung aktivieren und Standardeinstellungen konfigurieren.

2. (Optional) Passen Sie die WAN-Optimierungskonfiguration für jeden einzelnen Zweigstandorte an, oder akzeptieren Sie die **Standardsätze und -einstellungen für jeden.**

   Standardmäßig wird die **Standardkonfiguration** anfänglich auf jeden Zweigstandort angewendet, der für die WAN-Optimierung geeignet ist. Die 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 eine beliebige 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 Sets und Einstellungen enthalten:
     - **Standardfunktionen**
     - **Standard-Tuning-Einstellungen**
     - **Standardwerte Anwendungsklassifizierer (Satz)**
     - **Standard-Serviceklassen** (eingestellt)
   - **** <Client Site Name>—Die Konfigurationsstruktur des **Optimierungsabschnitts** enthält einen Zweig für jeden Clientknoten (Zweigstandort), der die WAN-Optimierung unterstützt. Wenn ein Clientknoten ein nicht unterstütztes Appliance-Modell ist, 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 zum Konfigurieren ihrer jeweiligen Sets und Einstellungen enthalten:
     - **Standardfunktionen**
     - **Standard-Tuning-Einstellungen**
     - **Standardwerte Anwendungsklassifizierer** (eingestellt)
     - **Standard-Serviceklassen** (eingestellt)

     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

October 28, 2021

Das Aktivieren der WAN-Optimierung in Ihrem virtuellen WAN umfasst die folgenden Verfahren:

1. Aktivieren Sie die WAN-Optimierung in den **Featureseinstellungen** des **Abschnitts Optimierung.**

   Anweisungen für diesen Teil des Prozesses finden Sie in diesem Abschnitt.

2. Konfigurieren Sie die Richtlinieneinstellung **Beschleunigung** für jede anwendbare Serviceklasse in der Tabelle **Serviceklassen**.

   Dieser Vorgang erfolgt weiter, nachdem Sie den Rest der **Optimierungskonfiguration** abgeschlossen haben. Anweisungen finden Sie im Abschnitt Konfigurieren von Standarddienstklassen 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 die WAN-Optimierung in Ihrem virtuellen 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, ein Staging durchführen und aktivieren, wie in den folgenden Kapiteln dieser Dokumentation beschrieben.

   Gehen Sie wie folgt vor, um die WAN-Optimierung zu aktivieren und den Abschnitt **Standardeinstellungen** unter **Features** zu konfigurieren:

   a) Melden Sie sich bei Bedarf wieder beim Management-Webinterface an und öffnen Sie den **Konfigurationseditor**.

      Gehen Sie wie folgt vor, um den **Konfigurationseditor** zu öffnen:

      i. Wählen Sie oben auf der Seite die Registerkarte **Konfiguration**, um den **Konfigurations-Navigationsbaum** (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 **Konfigurationseditor** 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 **Konfigurationseditor** geladen und zur Bearbeitung geöffnet.
      Wenn Sie über eine gültige und aktuelle Lizenz verfügen, die WAN-Optimierungsfunktionen enthält, ist der Abschnitt **Optimierung** im **Konfigurationseditor**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.

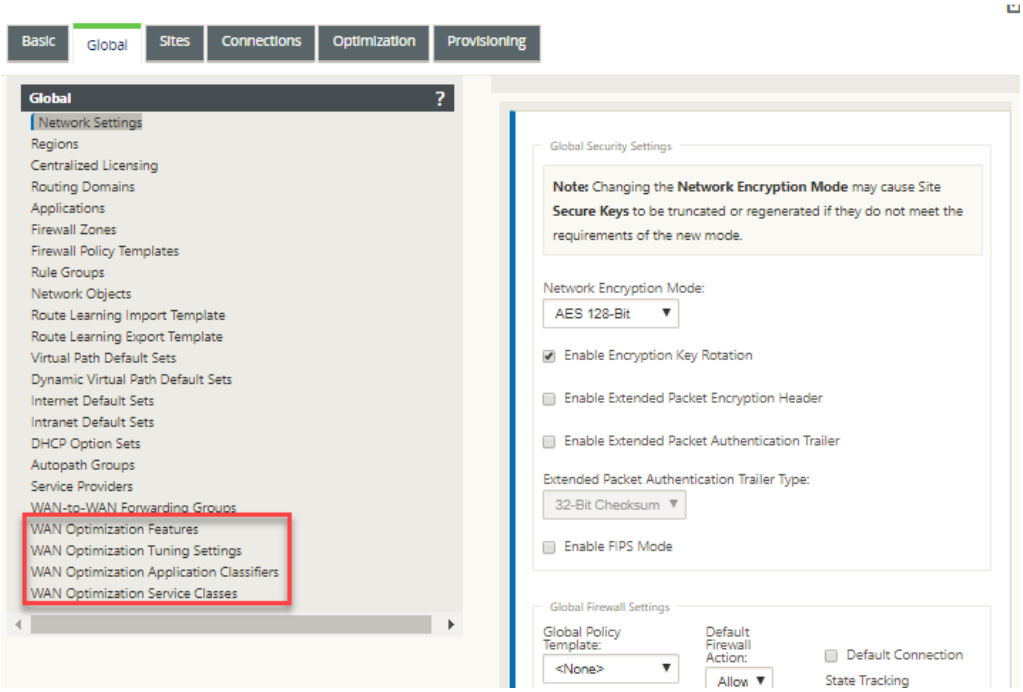
Einzelheiten und Anweisungen finden Sie in den folgenden Abschnitten:

- Die SD-WAN-Editionen
- Lizenzierung

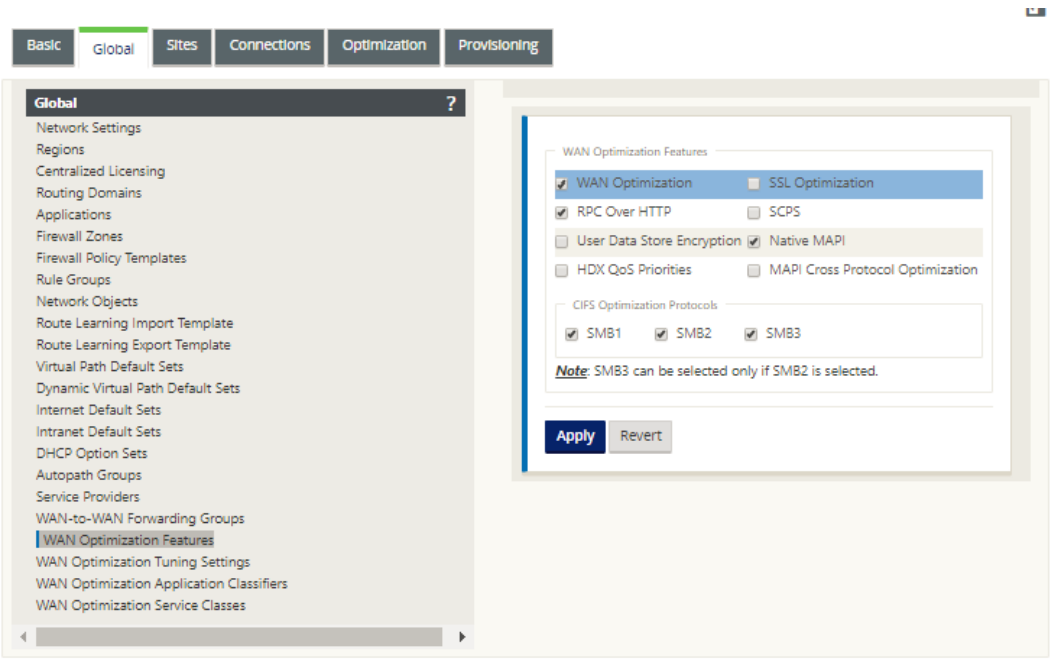
c) Klicken Sie auf die Registerkarte **Global**.

Auf der Registerkarte **Global** können Sie die folgenden Standardeinstellungen für die WAN-Optimierung 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 **Featues-Konfiguration** abgeschlossen haben. Darüber hinaus müssen Sie auch die **Beschleunigungseinstellung** für jede anwendbare Serviceklasse in der Tabelle Serviceklassen konfigurieren, wie weiter im **Optimierungskonfigurationsprozess** beschrieben. (Anweisungen finden Sie im Abschnitt Konfigurieren von Standarddienstklassenfür die Optimierung.) Schließlich wird die WAN-Optimierung in Ihrem virtuellen WAN erst aktiviert und aktiviert, wenn Sie die gesamte Virtual WAN-Konfiguration abgeschlossen und dann die Virtuelle WAN-Appliance-Pakete auf den berechtigten Sites in Ihrem virtuellen WAN.

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 Konfigurieren der Optimierung für einen Zweigstandortbeschrieben.

Das **Features-Konfigurationsformular** 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.

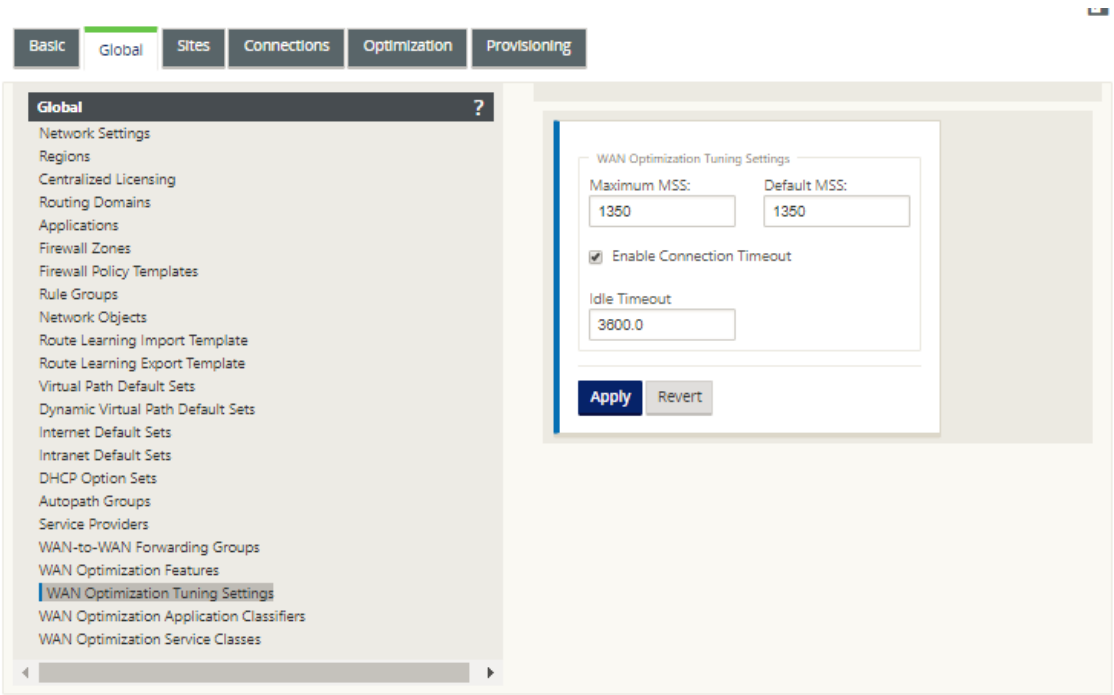
Konfigurieren der Standardoptimierungseinstellungen für die Optimierung

October 28, 2021

Sie können die Standardeinstellungen für die WAN-Optimierung auf der Registerkarte **Global** konfigurieren.

Gehen Sie wie folgt vor, um die standardmäßigen **Tuning-Einstellungen für**die WAN-Optimierung zu konfigurieren:

1. Klicken Sie auf der Registerkarte **Global** auf **WAN-Optimierungseinstellungen**.



2. Wählen und konfigurieren Sie die **Tuning-Einstellungen**.

   Die Optionen für **die Tuning-Einstellungen** lauten wie folgt:

   - **Maximum 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 das MSS für TCP-Segmente ein.
   - **Verbindungs-Timeout aktivieren** —Wählen Sie diese Option, um die automatische Beendigung einer Verbindung zu ermöglichen, wenn der Leerlaufschwellenwert überschritten wird.
   - **Leerlauf-Timeout** —Geben Sie einen Schwellenwert (in Sekunden) ein, um die zulässige Dauer des Leerlaufs festzulegen, bevor eine Verbindung im Leerlauf beendet wird. Sie müssen zuerst **Verbindungs-Timeout aktivieren** auswählen, bevor dieses Feld konfiguriert werden kann.

3. Klicken Sie auf **Apply**.

   Dies wendet die geänderten **Tuning-Einstellungen** auf die globale Konfiguration an.

   Der nächste Schritt besteht darin, den Standardsatz von WAN Optimization Application Classifiers zu konfigurieren.

Konfigurieren von Standardanwendungsklassifizierern für die Optimierung

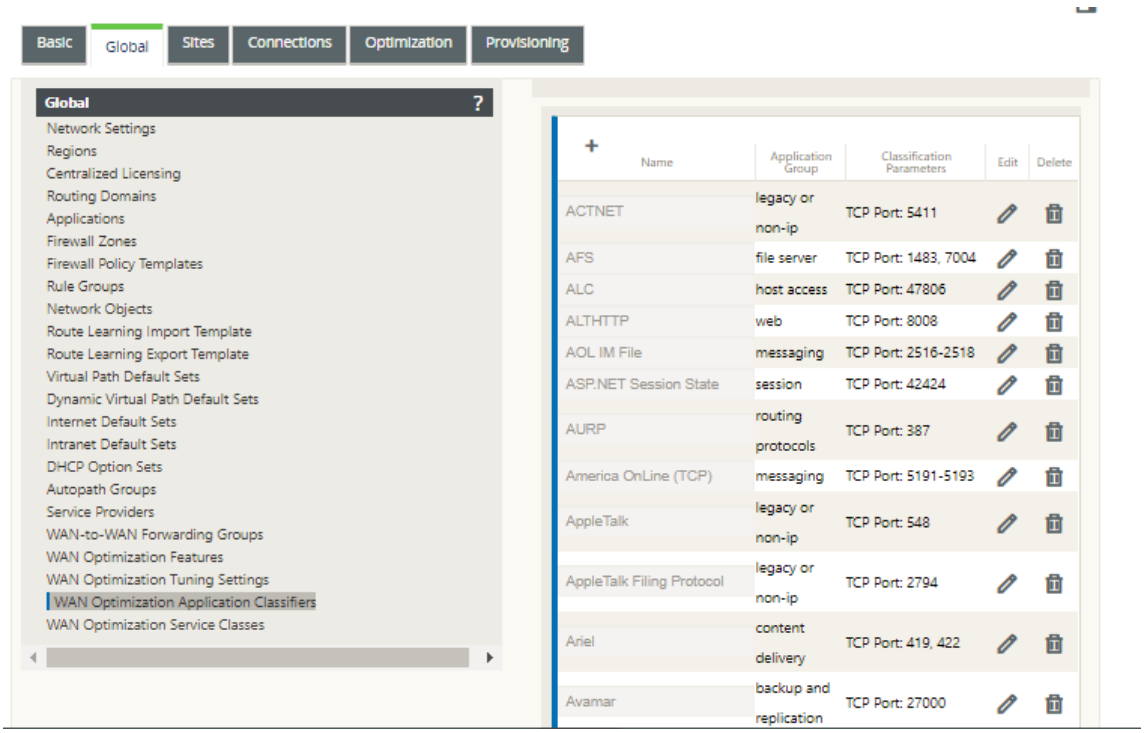
October 28, 2021

Sie können die standardmäßigen Anwendungsklassifiziereinstellungen 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 **Application Classifiers** geöffnet, in der der Standardsatz von Anwendungsklassifizierern angezeigt wird.

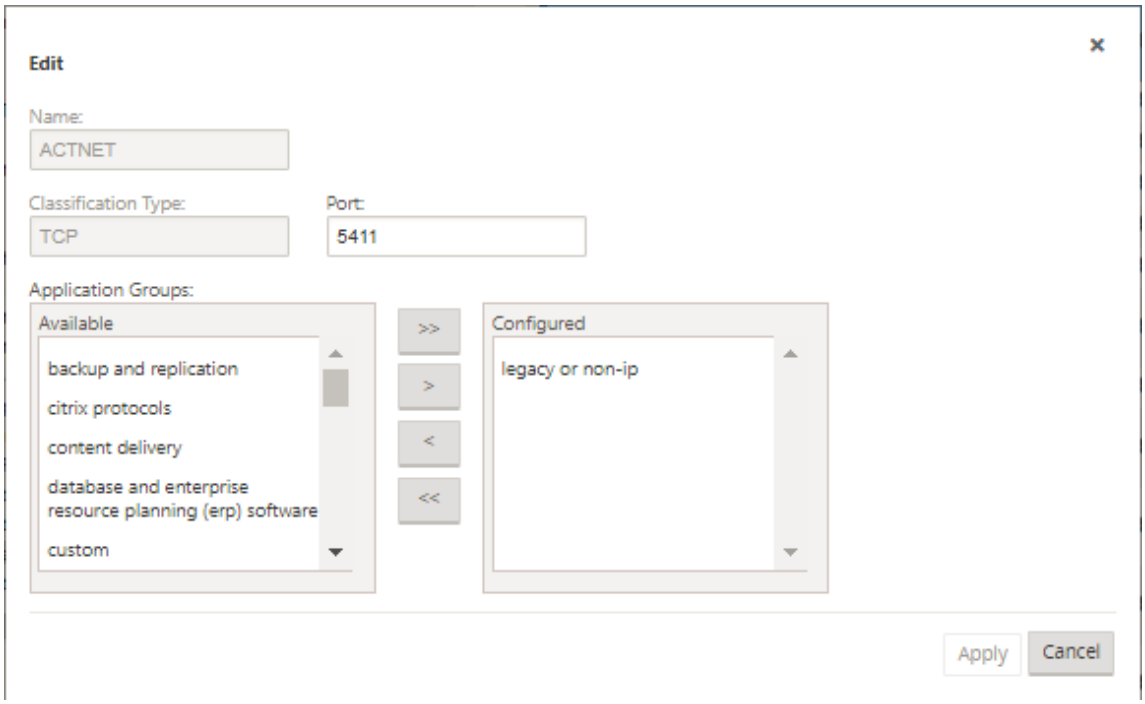


   Diese Tabelle ist auch ein Konfigurationsformular. Mit diesem Formular können Sie Anwendungsklassifizierer konfigurieren (bearbeiten), löschen und hinzufügen, um einen benutzerdefinierten Standardsatz zu erstellen. Der geänderte standardmäßige **Anwendungsklassifizierersatz** und die einzelnen Application Classifier-Einstellungen, die Sie konfigurieren, werden automatisch als Standardeinstellungen auf alle Zweigstellen angewendet, die in der Abschnittsstruktur **Optimierung** enthalten sind.

> **Hinweis**
>
> Sie können auch das Set und die Einstellungen für **Anwendungsklassifizierer** für jeden bestimmten Zweigstandort anpassen. Anweisungen hierzu finden Sie im Abschnitt Konfigurieren der Optimierung für einen Zweigstandort.

2. Um einen vorhandenen Application Classifier zu konfigurieren, klicken Sie auf Bearbeiten (Bleistiftsymbol) in der Spalte **Bearbeiten** dieses Klassifikatoreintrags.

   Dadurch wird ein Popup-Formular Einstellungen **bearbeiten** geöffnet, um den ausgewählten Anwendungsklassifizierer zu konfigurieren.



3. Geben Sie im Feld **Port** die Portnummer für den Application Classifier ein oder akzeptieren Sie den Standardwert.

4. Fügen Sie Anwendungsgruppen in der Liste **Konfiguriert** hinzu oder entfernen Sie diese oder akzeptieren 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 zur 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** auf einmal aus der Liste zu entfernen, klicken Sie auf den doppelten Linkspfeil Alle entfernen («).

5. Klicken Sie auf **Apply**.

   Dadurch werden Ihre Änderungen auf den Application Classifier angewendet und das Formular Konfiguration **bearbeiten** geschlossen.

6. (Optional) Passen Sie den standardmäßigen **Anwendungsklassifizierersatz** an.

   Sie können Anwendungsklassifizierer hinzufügen oder löschen, um den Standardsatz wie folgt anzupassen:

   - **So entfernen Sie einen Application Classifier 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 Application Classifier hinzu:**

     a) Klicken Sie auf **+** rechts neben dem **Application Classifier**-Zweiglabel.

        Dadurch wird das Formular Konfiguration **hinzufügen** angezeigt.

     b) Geben Sie den Namen und die Portnummer für den Application Classifier in die Felder **Name** bzw. **Port** ein.

     c) Fügen Sie Anwendungsgruppen in der Liste **Konfiguriert** hinzu oder entfernen Sie sie.

        So fügen Sie der Liste eine Anwendungsgruppehinzu: 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 zur 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** auf einmal aus der Liste zu entfernen, klicken Sie auf den doppelten Linkspfeil Alle entfernen («).

     d) Klicken Sie auf **Apply**.

        Dadurch wird der neue Application Classifier zum Satz hinzugefügt und das Formular Konfiguration **hinzufügen** geschlossen.

        Der nächste Schritt besteht darin, den Standardsatz der WAN-Optimierungsdienstklassen zu konfigurieren.

Konfigurieren von Standardserviceklassen für die Optimierung

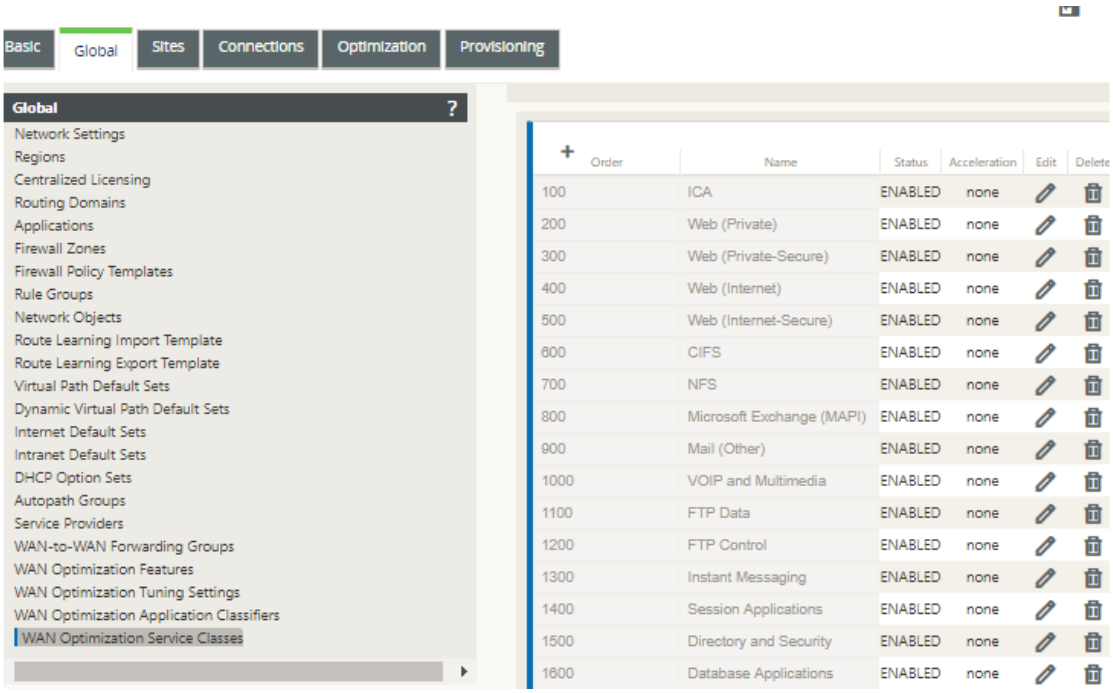
October 28, 2021

Sie können die Standard-Serviceklasseneinstellungen 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 **Serviceklassen** geöffnet, in der der Standardsatz von Serviceklassen angezeigt wird.



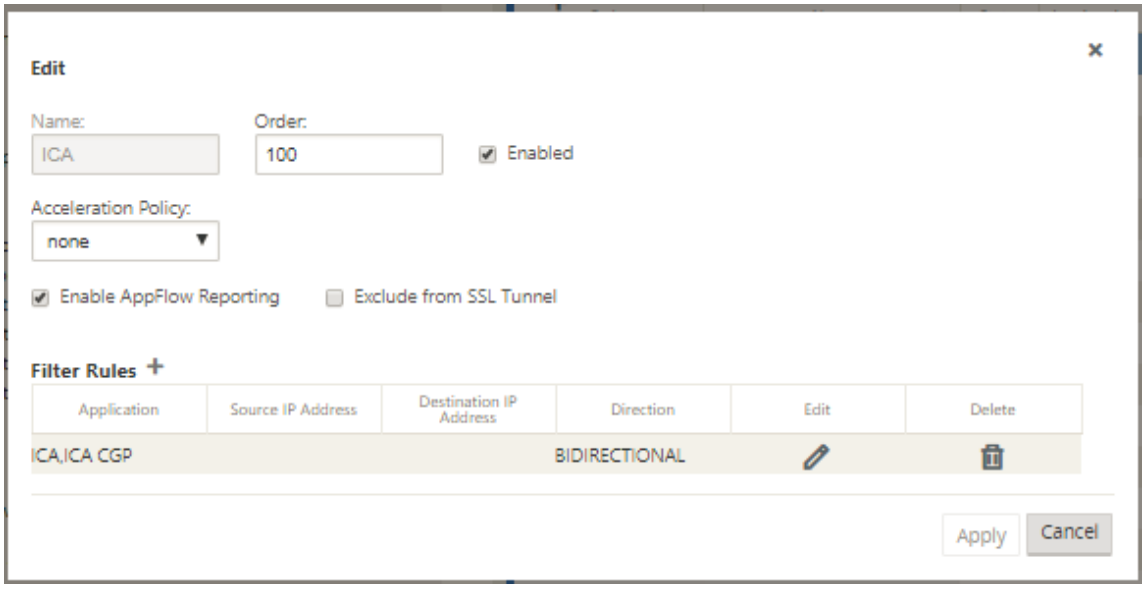
   Diese Tabelle ist auch ein Konfigurationsformular. Sie können dieses Formular verwenden, um Serviceklassen zu konfigurieren (bearbeiten), zu löschen und hinzuzufügen, um einen benutzerdefinierten Standardsatz zu erstellen. Der geänderte Standardsatz von **Serviceklassen** und die einzelnen Serviceklasseneinstellungen, die Sie konfigurieren, werden automatisch als Standardeinstellungen auf jeden Zweigstandort angewendet, der in der Abschnittsstruktur **Optimierung** enthalten ist.

   > **Hinweis**
   >
   > Sie können auch den Satz und die Einstellungen der **Serviceklassen** für jeden bestimmten Zweigstandort anpassen. Anweisungen zum Anpassen der **Optimierungskonfiguration**

> für einen Zweigstandort finden Sie im Abschnitt Konfigurieren der Optimierung für einen Zweigstandort.

2. Um eine vorhandene Serviceklasse zu konfigurieren, klicken Sie in der Spalte **Bearbeiten** dieses Klasseneintrags in der Tabelle Serviceklassen auf Bearbeiten (Bleistiftsymbol).

   Dadurch wird ein Popup-Formular Einstellungen **bearbeiten** geöffnet, um die ausgewählte Serviceklasse zu konfigurieren.



3. Konfigurieren Sie die Grundeinstellungen für die Serviceklasse.

   Die Grundeinstellungen lauten wie folgt:

   - **Aktiviert** —Wählen Sie diese Option aus, um die neue Serviceklasse 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 Appliancedatenträger als Speicherort für das Speichern des für die Komprimierung verwendeten Datenverkehrshistorie anzugeben. Dadurch wird die DBC-Richtlinie (Disk Based Compression) für diese Serviceklasse aktiviert. Im Allgemeinen ist eine **Datenträgerrichtlinie** normalerweise die beste Wahl, da die Appliance automatisch **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 **none** wird im Allgemeinen nur für unkomprimierbaren verschlüsselten Datenverkehr und Echtzeitvideo 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.
  - **memory** —Wählen Sie diese Richtlinie aus, um Speicher als Speicherort für die Speicherung des für die Komprimierung verwendeten Verkehrsverlaufs anzugeben.

- **AppFlow Reporting aktivieren** —Wählen Sie diese Option aus, um AppFlow-Berichte für diese Serviceklasse 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 Collector erhält mithilfe des offenen AppFlow-Standards (`http://www.appflow.org`) detaillierte Informationen von der Appliance.

  Weitere Informationen zu AppFlow finden Sie in der Citrix CloudBridge 7.4-Produktdokumentation, die im Citrix Dokumentationsportal verfügbar ist `http://docs.citrix.com/`.

  > **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. Siehe auch Überwachung des virtuellen WAN.

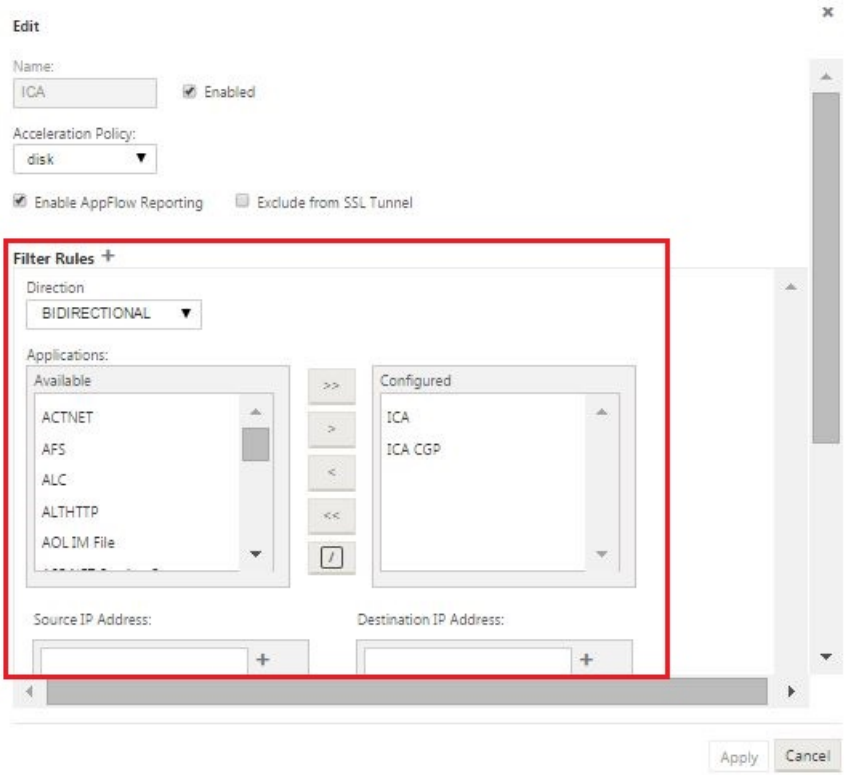
- **Aus dem SSL-Tunnel ausschließen** —Wählen Sie diese Option, um den mit der Serviceklasse verknüpften Datenverkehr vom SSL-Tunneling auszuschließen.

4. Konfigurieren Sie die **Filterregeln** für die Serviceklasse.

   Gehen Sie wie folgt vor, um eine bestehende 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 (Stiftsymbol).

      Dadurch werden die Einstellungen für die Filterregeln für die ausgewählte Filterregel angezeigt.



b) Wählen Sie die Filterrichtung aus dem Dropdownmenü Richtung aus.

Wählen Sie eine der folgenden Optionen:

- **BIDIRECTIONAL**
- **UNIDIRECTIONAL**

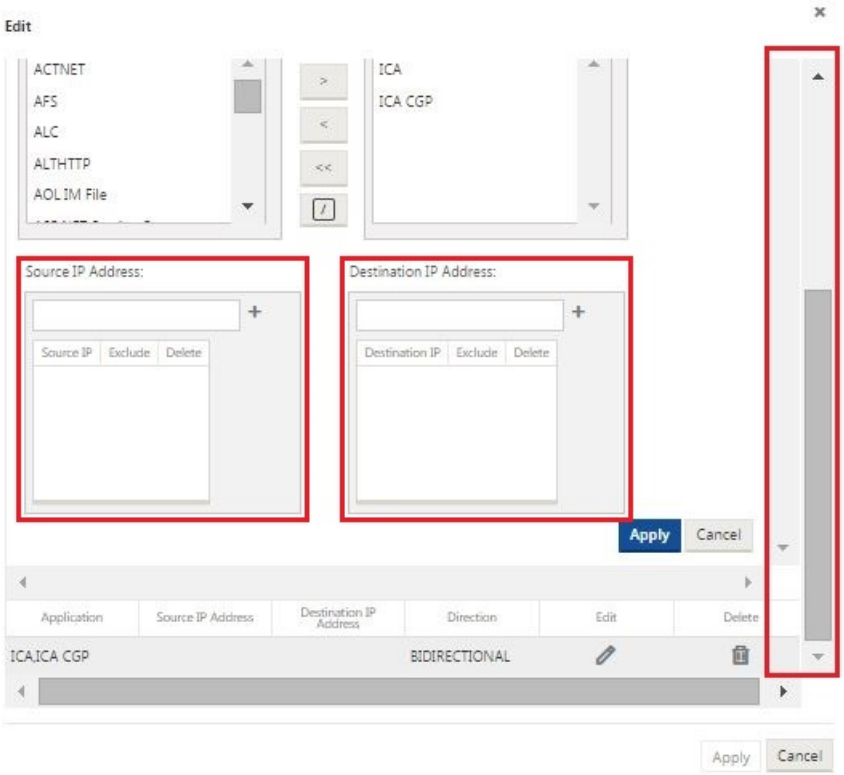
c) Fügen Sie Anwendungen in der Liste **Konfiguriert** hinzu oder entfernen Sie sie.

So fügen Sie eine Anwendung zur Listehinzu: 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 zur 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** auf einmal aus der Liste zu entfernen, klicken Sie auf den doppelten Linkspfeil Alle entfernen (**«**).

d) Scrollen Sie nach unten, um den abgeschnittenen Teil des Formulars anzuzeigen.

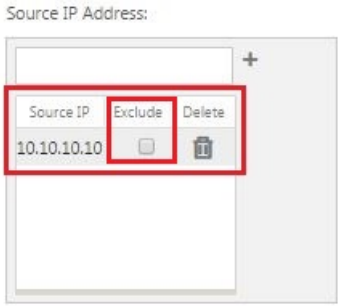
Der Abschnitt Einstellungen **für Filterregeln** ist etwas lang, daher müssen Sie die Bildlaufleisten verwenden, um den abgeschnittenen Teil des Formulars anzuzeigen.



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.



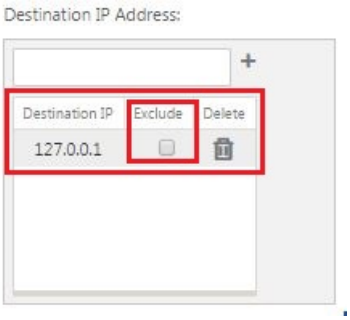
g) Geben Sie an, ob die Quell-IP-Adresse für diese Filterregel eingeschlossen oder ausgeschlossen werden soll.

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 auf **+** rechts neben der Ziel-IP-Adresse, die Sie gerade eingegeben haben.

Dadurch wird die angegebene IP-Adresse zur Tabelle **Quell-IP-Adresse** hinzugefügt.



j) Geben Sie an, ob die Ziel-IP-Adresse für diese Filterregel ein- 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 **Apply**.

   Dies wendet Ihre Änderungen an der Regel an und blendet den Abschnitt **Einstellungen für Filterregeln** aus.

5. (Optional) Passen Sie die **Standard-Serviceklassen** an.

   Sie können Service Classes wie folgt hinzufügen oder löschen, um den Standardsatz anzupassen:

   - **So entfernen Sie eine Serviceklasse aus dem Set:**

     Klicken Sie auf das Mülleimer-Symbol in der Spalte **Löschen** eines Eintrags der Serviceklasse in der Tabelle, um diesen Eintrag zu entfernen.

   - **So fügen Sie dem Set eine Serviceklasse**hinzu:

     a) Klicken Sie auf **+** rechts neben dem Etikett der Zweigstelle **Service Class**.

        Dadurch 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 Serviceklasse.

        Die Schritte zum Konfigurieren einer neuen Serviceklasse sind dieselben wie für das Ändern einer vorhandenen Serviceklasse. Anweisungen finden Sie in den folgenden Schritten zu Beginn dieses Abschnitts:

        "3. Konfigurieren Sie die Grundeinstellungen für die Serviceklasse. "

        "4. Konfigurieren Sie die Filterregeln für die Serviceklasse. "

d) Klicken Sie auf **Hinzufügen**, um die neue Serviceklasse zum Standardsatz hinzuzufügen und das Formular Konfiguration **hinzufügen** zu schließen.

6. (Optional, empfohlen) **Speichern** Sie das Konfigurationspaket.

   Sie haben jetzt die Konfiguration der globalen WAN-Optimierung abgeschlossen und können mit der Konfiguration der **Optimierungssätze** und -einstellungen für die Zweigstellen beginnen.

Konfigurieren der Optimierung für einen Zweigstandort

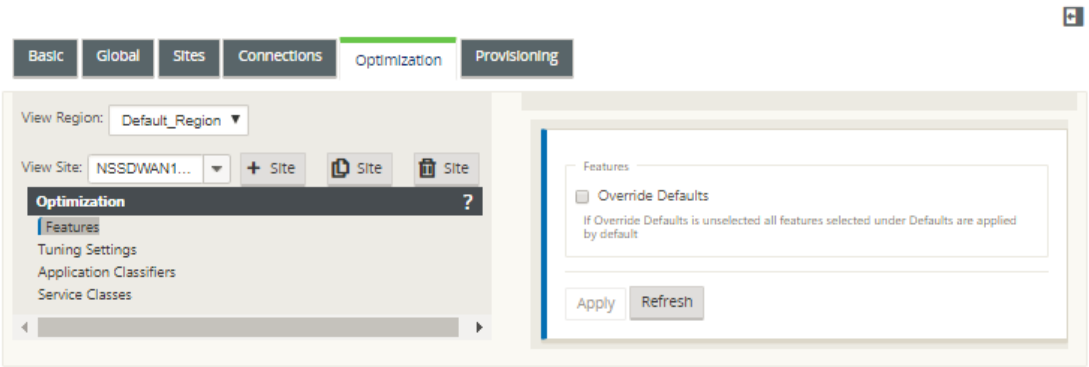
October 28, 2021

Nachdem Sie die globale Standardkonfiguration abgeschlossen haben, haben Sie die Möglichkeit, die Sets und Einstellungen für jeden Zweigstandort anzupassen.

Die globalen Einstellungen, die Sie gerade konfiguriert haben, 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 für die Konfiguration der globalen Standardeinstellungen, mit einigen geringfügigen Unterschieden.

Gehen Sie wie folgt vor, um die **Optimierungskonfiguration** für einen Zweigstandort anzupassen:

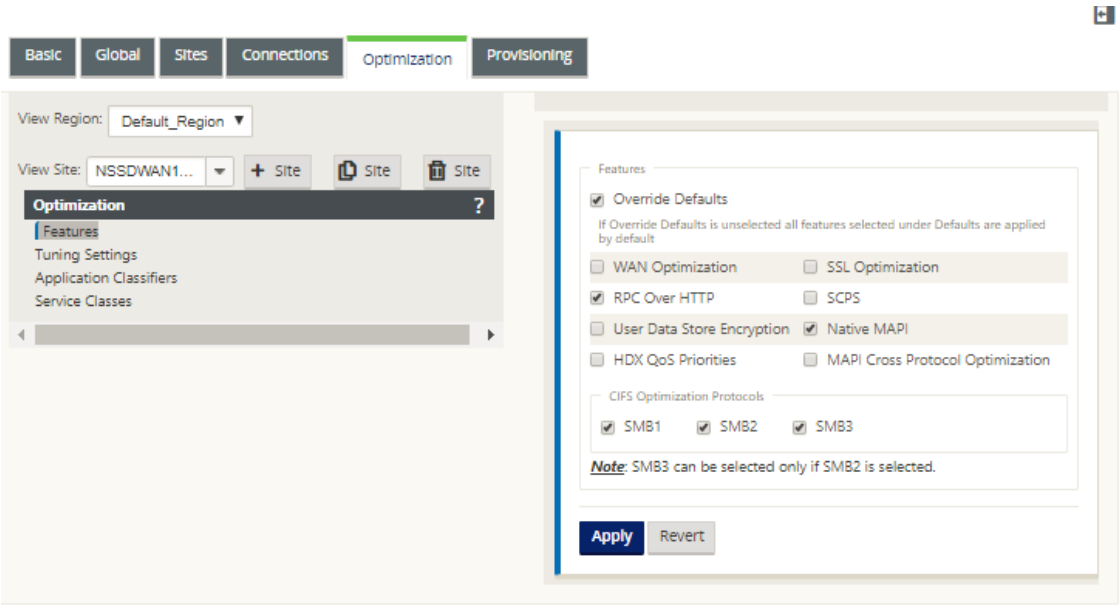
1. Klicken Sie auf die Registerkarte **Optimierung**, wählen Sie im Feld Site anzeigen eine Site aus.



2. Aktivieren Sie das Kontrollkästchen **Standardeinstellungen überschreiben**.

   Dadurch wird das Konfigurationsformular der obersten Ebene für diese Konfigurationskategorie angezeigt und zur Bearbeitung geöffnet.

   Das folgende Bild zeigt ein Beispiel für ein Konfigurationsformular für Einstellungen auf oberster Ebene, in diesem Fall für den **Features**-Satz.



3. Geben Sie Ihre Konfigurationsänderungen ein.

   Ab diesem Zeitpunkt ist der Konfigurationsprozess für jede Kategorie der **Zweigstandort-Optimierung** derselbe 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 dieOptimierung.
   - Konfigurieren von Optimierungs-Standardanwendungsklassifikatoren.
   - Konfigurieren von Standard-Serviceklassen 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-Profile konfigurieren

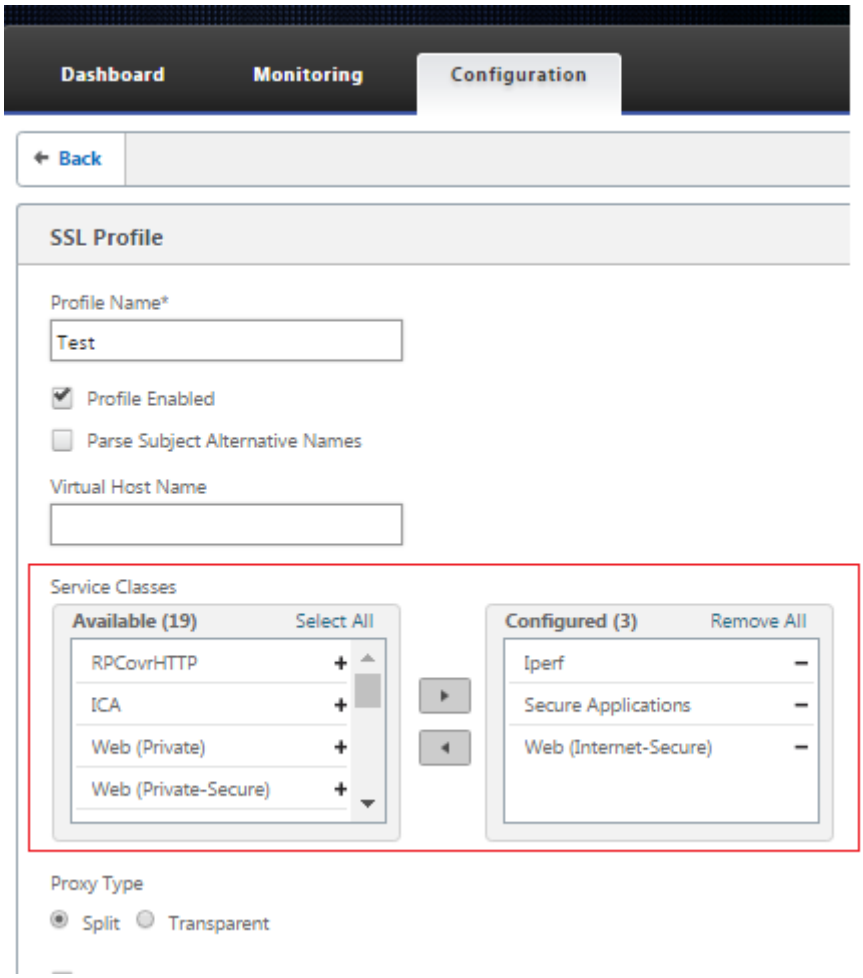
October 28, 2021

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.

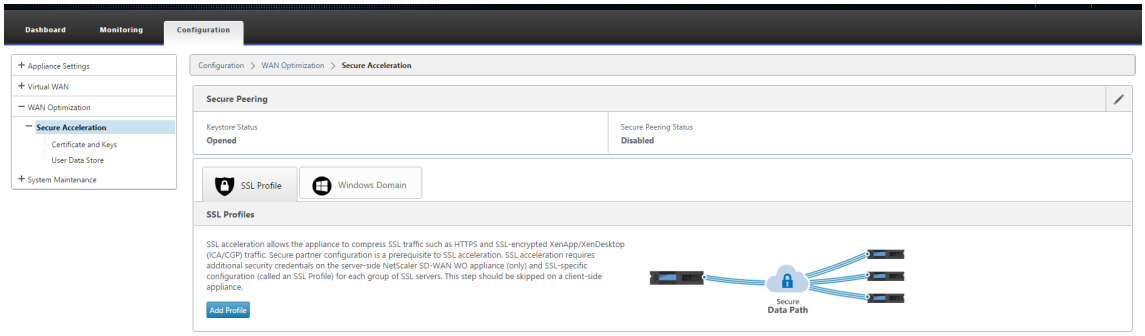
Eine der Einschränkungen besteht darin, dass das SSL-Profil an alle Regeln in einer Serviceklasse angehängt wird. Wenn Sie das SSL-Profil selektiv an eine bestimmte Regel anhängen müssen, wird die Konfiguration der Serviceklasse in detaillierte Regeln für die weitere Auswahl aufgeteilt.

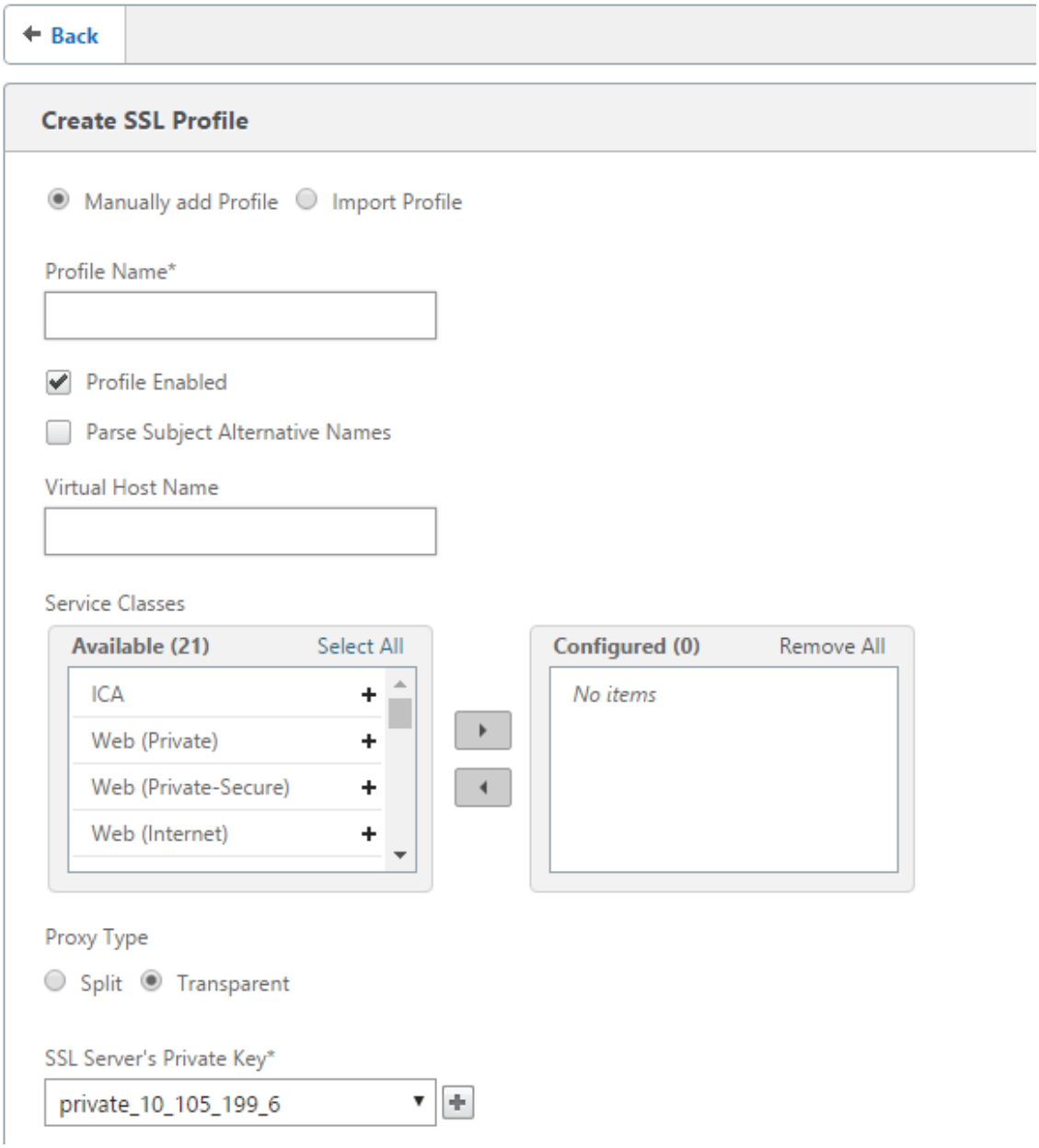
> **Hinweis**
>
> SSL-Profilen können nur die Dienstklassen zugeordnet werden, deren Filterregeln auf unidirektional festgelegt sind.



So erstellen Sie SSL-Profil auf der neuen Premium (Enterprise) Edition-Appliance im Rechenzentrum:

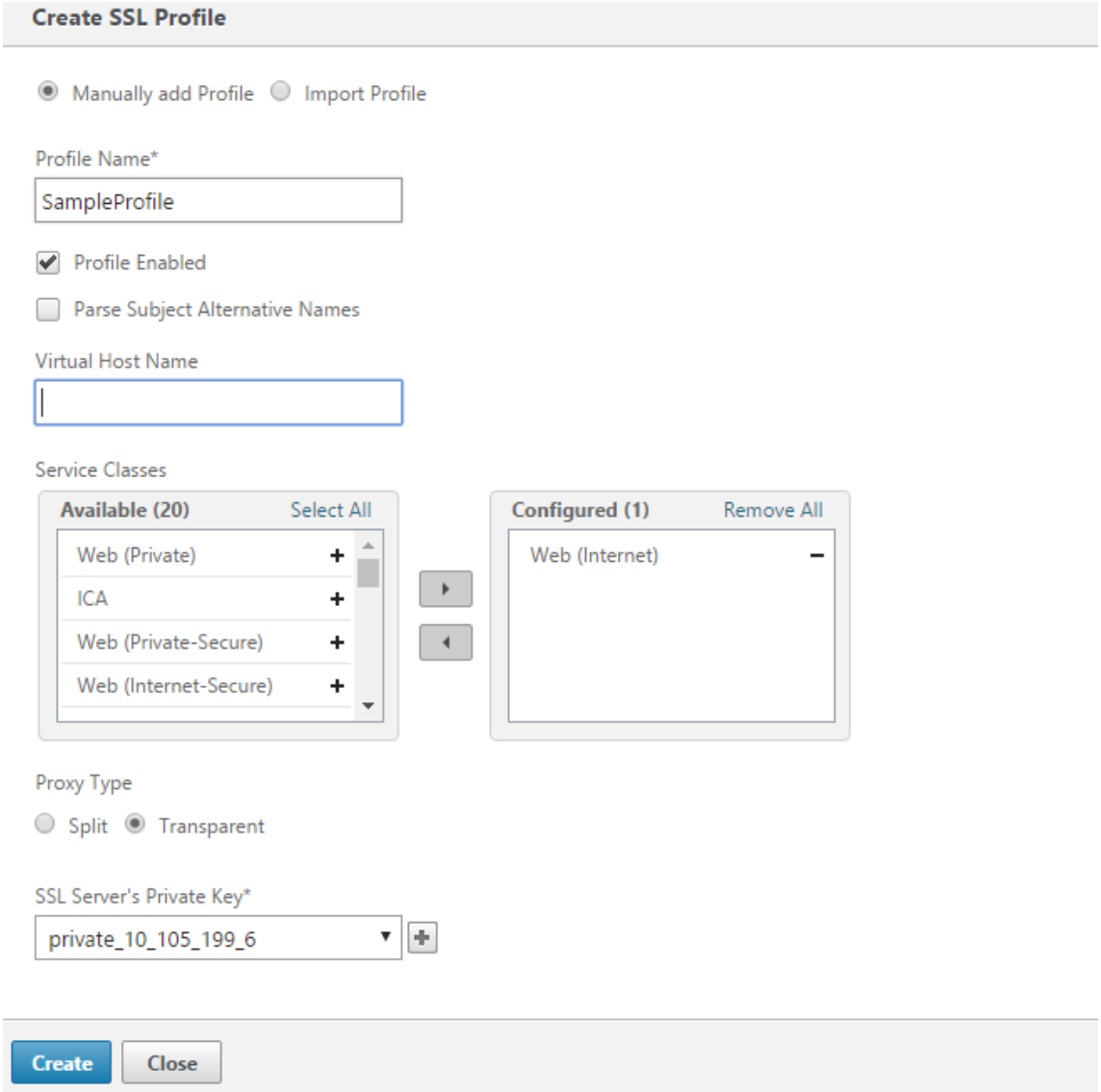
1. Wechseln Sie in der SD-WAN-Web-GUI zur Seite **Konfiguration** > **Sichere Beschleunigung**. Klicken Sie auf **Profil hinzufügen**. Erstellen Sie das **SSL-Profil**.



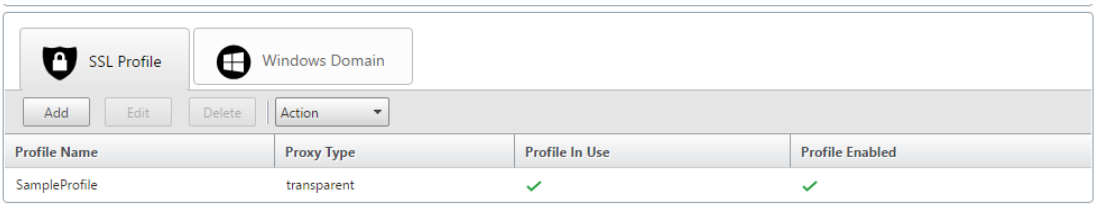


2. Geben Sie auf der Seite **SSL-Profil erstellen** einen Profilnamen an und wählen Sie **Serviceklassen** aus, die diesem Profil zugeordnet werden. Wählen Sie **Proxy-Typ**, geben Sie

relevante Daten ein und klicken Sie auf **Erstellen**.



3. Nachdem das SSL-Profil erfolgreich erstellt und die Serviceklasse zugeordnet wurde, zeigen Sie die SSL-Profilinformationen wie unten gezeigt an.



Citrix WAN-Optimierungs-Client-Plug-In

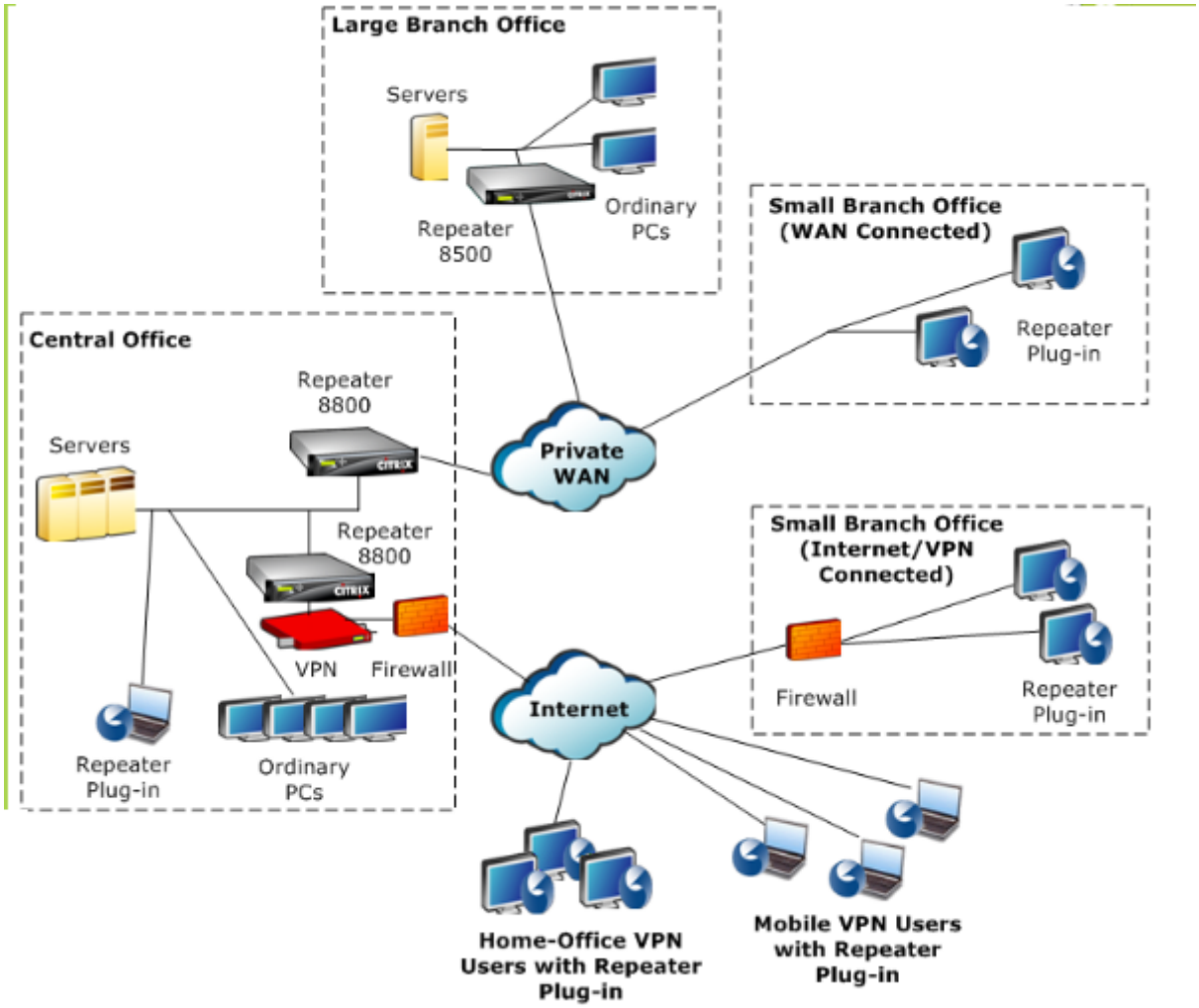
October 28, 2021

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

October 28, 2021

Auf der Clientseite der beschleunigten Verbindung wird das
WANOP Client Plug-in auf Windows-Desktop- und Laptop-Systemen unterstützt, jedoch 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

October 28, 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. An Ihren Routingtabellen, Netzwerkeinstellungen, Clientanwendungen oder Serveranwendungen sind keine Änderungen erforderlich.

Citrix Access Gateway-VPNs erfordern eine geringe Menge an WANOP Client-Plug-In-spezifischen Konfigurationen.

Es gibt zwei Varianten der Art und Weise, wie Verbindungen durch das Plug-in und die Appliance gehandhabt werden: *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-to-Appliance ist der Beschleunigung von Gerät zu Gerät 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 fungiert der transparente Modus als transparenter Proxy, wobei die Quell- und Ziel-IP-Adresse und die Portnummern von einem Ende der Verbindung zum anderen erhalten werden.
- Der**Redirector-Modus** (nicht empfohlen) verwendet einen expliziten Proxy. Das Plug-in liest ausgehende Pakete an die Redirector-IP-Adresse der Appliance um. Die Appliance wiederum adressiert die Pakete an den Server, während sie die Rücksendeadresse so ändert, dass sie auf sich selbst anstelle des Plug-Ins zeigt. In diesem Modus muss die Appliance nicht physisch mit dem Pfad zwischen der WAN-Schnittstelle und dem Server übereinstimmt (obwohl dies die ideale Bereitstellung ist).

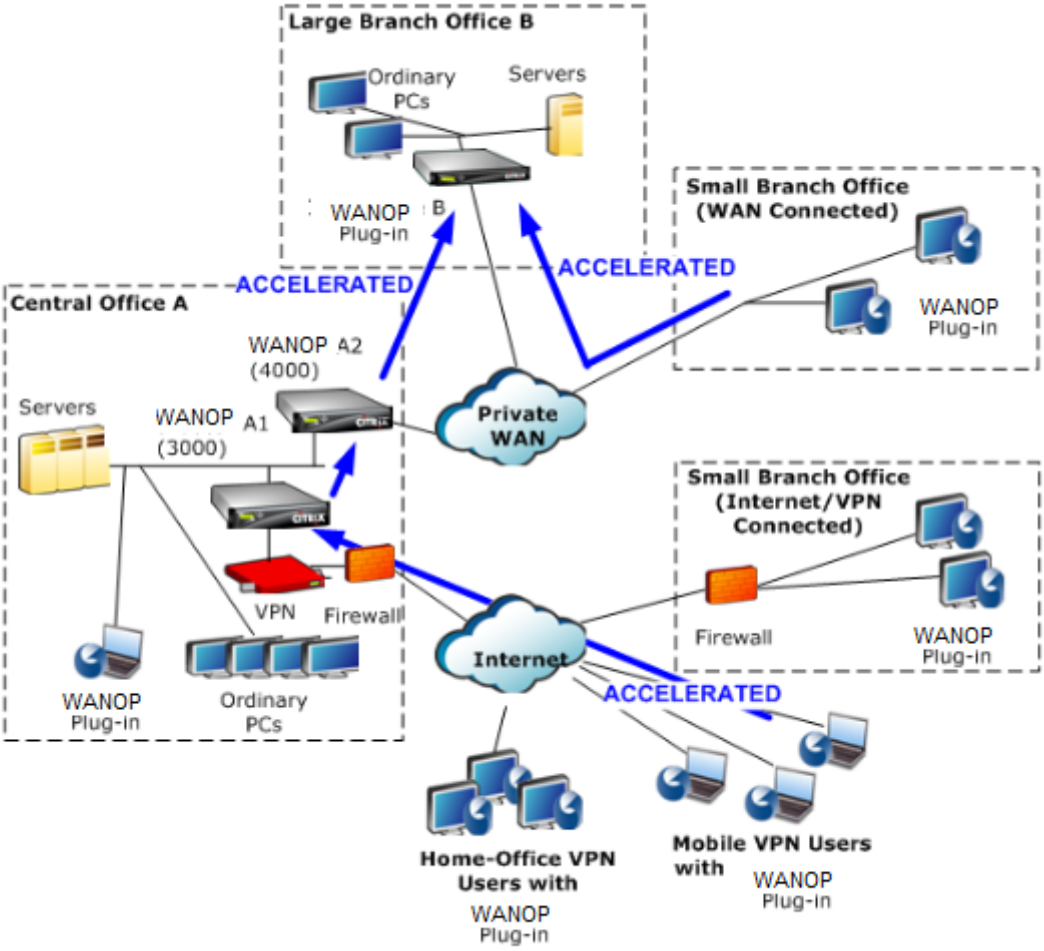
  Best Practice: Verwenden Sie den transparenten Modus, wenn Sie können, und den Redirector-Modus, wenn Sie müssen.

Transparenter Modus

Im transparenten Modus müssen die Pakete für beschleunigte Verbindungen die Ziel-Appliance passieren, ähnlich wie bei der Appliance-zu-Appliance-Beschleunigung.

Das Plug-in ist mit einer Liste von Appliances konfiguriert, die für die Beschleunigung verfügbar sind. Es versucht, jedes Gerät zu kontaktieren und eine Signalverbindung zu öffnen. Wenn die Signalisierungsverbindung 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. In dem Diagramm wird der Verkehr von Home-Office- und mobilen VPN-Benutzern, der für große Zweigstellen B bestimmt ist, durch Repeater B beschleunigt, damit dies funktioniert, müssen die Repeater A1 und A2 die Daisy-Chaining 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 ursprüngliche Paket in der Verbindung (das SYN-Paket) angehängt 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.

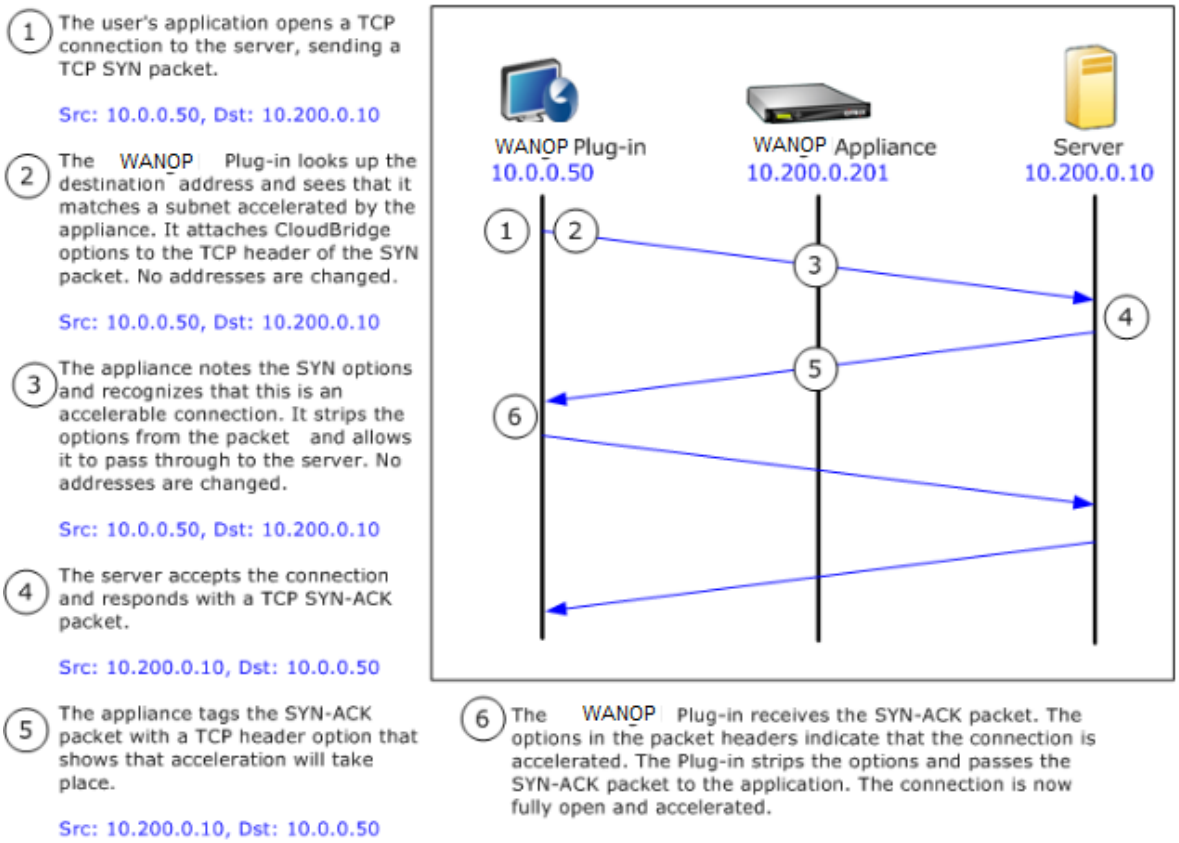
Der transparente Modus ähnelt der Beschleunigung von Gerät zu Gerät, ist jedoch nicht identisch damit. Die Unterschiede sind:

- 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-zu-Appliance-Beschleunigung hingegen funktioniert unabhängig davon, auf welcher Seite der Client und welcher 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 Gerät zu Gerät erfordert keine Signalverbindung, außer für sichere Peer-Beziehungen, die standardmäßig deaktiviert sind. Wenn das Plug-in keine Signalverbindung öffnen kann, versucht es nicht, Verbindungen über das Gerät zu beschleunigen.
- Daisy-Chaining —Für eine Appliance, die sich im Pfad zwischen einem Plug-In und der ausgewählten Ziel-Appliance befindet, müssen Sie die Daisy-Chaining im Menü **Konfiguration: Tuning** 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 Gerät zu Gerät, mit der Ausnahme, dass die Entscheidung, ob versucht werden soll, die Verbindung zu beschleunigen oder nicht, auf Beschleunigungsregeln basiert, die über die Signalverbindung heruntergeladen wurden.

Abbildung 2. Paketfluss im transparenten Modus



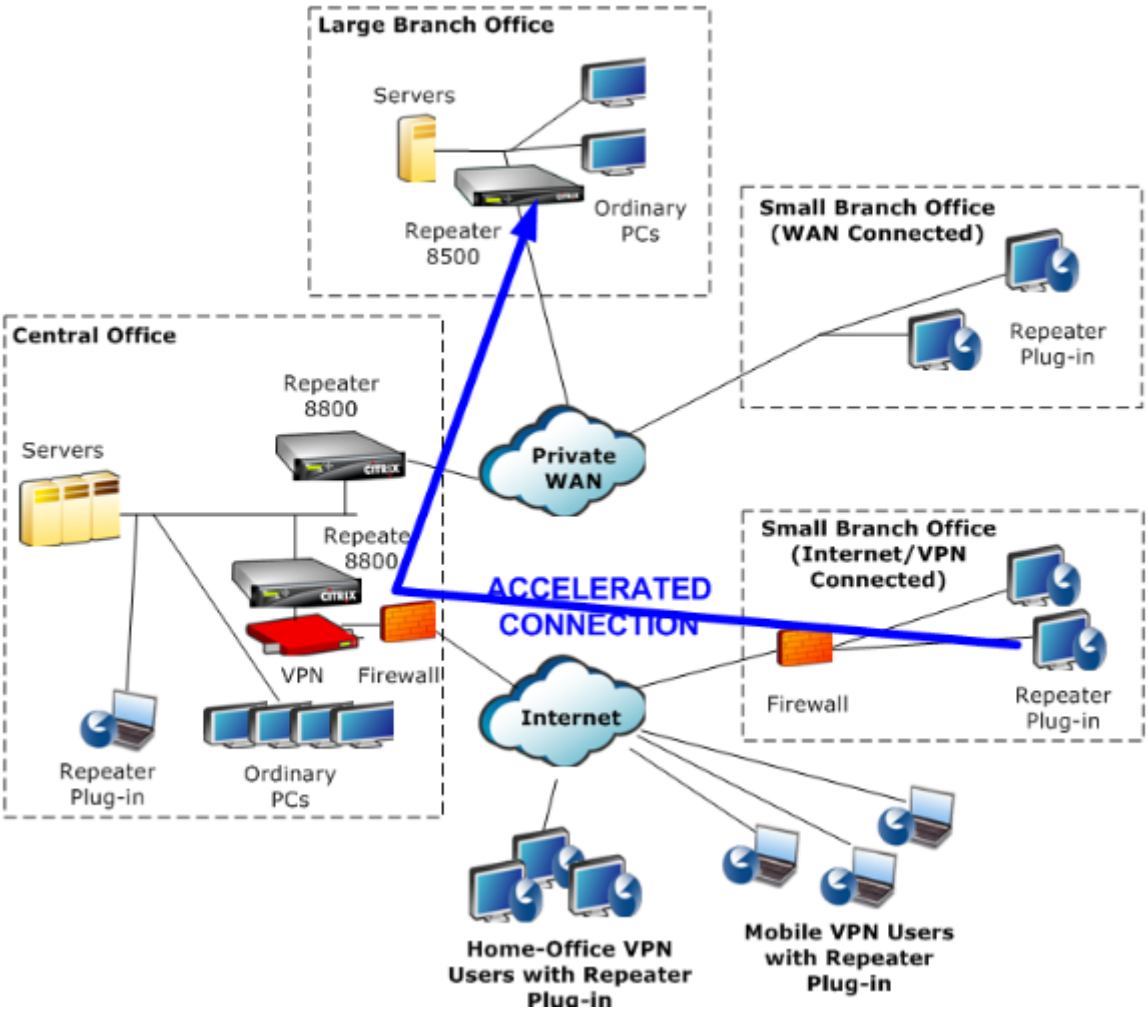
Umleitungsmodus

Der Redirector-Modus 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 Appliance im Umleitungsmodus nicht den gesamten WAN-Link-Verkehr 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 und ersetzt die Quell-IP-Adresse in den Paketen durch ihre eigene Adresse. Aus Sicht des Servers stammt die Verbindung von der Appliance.
- Der Rückgabeverkehr vom Server wird an die Appliance gerichtet, die Optimierungen in Rückgaberichtung durchführt und die Ausgabepakete an das Plug-in weiterleitet.
- Die Zielportnummern werden nicht geändert, sodass Netzwerküberwachungsanwendungen den Verkehr weiterhin klassifizieren können.

Die folgende Abbildung zeigt, wie der Redirector-Modus funktioniert.

Abbildung 1. Umleitungsmodus



Die folgende Abbildung zeigt den Paketfluss und die Adresszuordnung 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

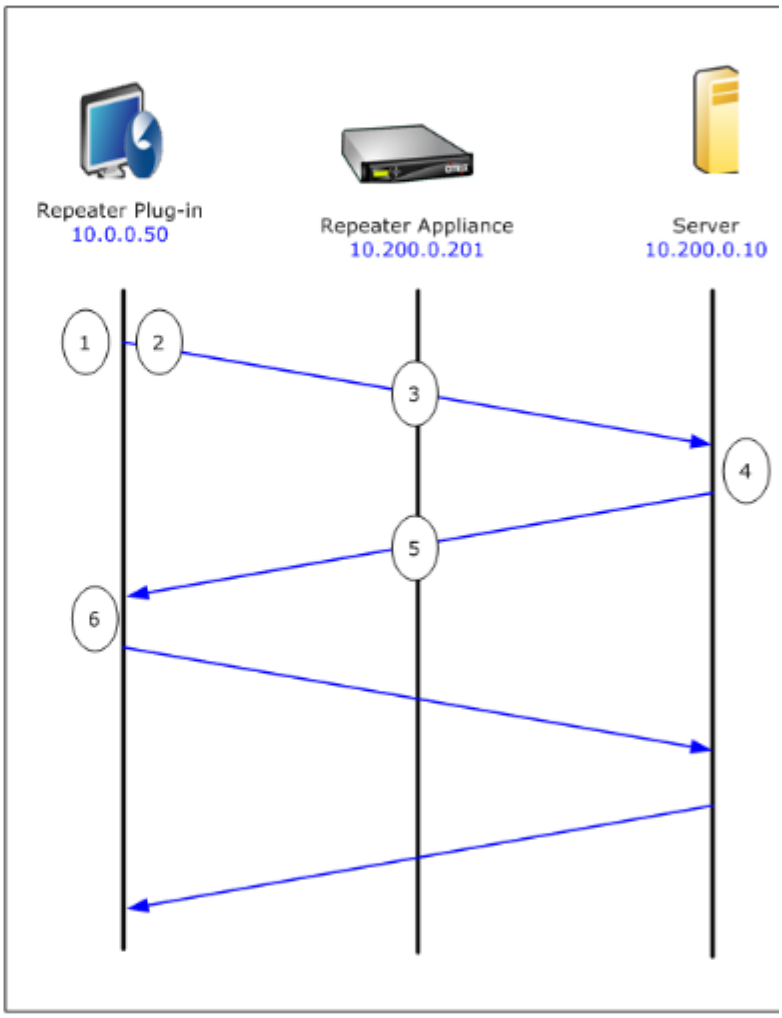
5. The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

   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 von Appliances konfiguriert, die es kontaktieren kann, um eine beschleunigte Verbindung anzufordern.

Die Appliances verfügen jeweils über eine Liste von *Beschleunigungsregeln*, bei der es sich um eine Liste von Zieladressen oder Ports handelt, zu denen die Appliance beschleunigte Verbindungen herstellen kann. Das Plug-in lädt diese Regeln von den Appliances herunter und stimmt die Zieladresse und den Port jeder Verbindung mit dem Regelsatz jeder Appliance ab. Wenn nur ein Gerät anbietet, eine bestimmte Verbindung zu beschleunigen, ist die Auswahl einfach. Wenn mehr als ein Gerät anbietet, die Verbindung zu beschleunigen, muss das Plug-in eines der Geräte auswählen.

Die Regeln für die Geräteauswahl lauten wie folgt:

- Wenn alle Geräte, die zur Beschleunigung der Verbindung anbieten, Geräte im Umleitungsmodus sind, wird die Appliance ganz links in der Appliance-Liste des Plug-ins ausgewählt. (Wenn die Appliances als DNS-Adressen angegeben wurden und der DNS-Datensatz mehrere IP-Adressen hat, 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 dem ansprechenden Gerät verfügen, sonst findet keine Beschleunigung statt.
- Einige Konfigurationsinformationen werden als global angesehen. 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

October 28, 2021

Die Clientbeschleunigung erfordert eine spezielle Konfiguration auf der WANOP Client-Plug-In-Appliance. Andere Überlegungen umfassen die Platzierung der Geräte. Plug-Ins werden typischer-

weise für VPN-Verbindungen eingesetzt.

Verwenden Sie nach Möglichkeit ein dediziertes Gerät

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 Remotesites 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.

Verwenden Sie nach Möglichkeit den Inline-Modus

Eine Appliance sollte am selben Standort wie die VPN-Einheit bereitgestellt werden, die sie unterstützt. Typischerweise stehen die beiden Einheiten in einer Linie zueinander. Eine Inline-Bereitstellung bietet die einfachste Konfiguration, die meisten Funktionen und die höchste Leistung. Um beste Ergebnisse zu erzielen, sollte die Appliance direkt mit der VPN-Einheit in Einklang stehen.

Appliances können jedoch jeden Bereitstellungsmodus verwenden, mit Ausnahme des Gruppenmodus oder des Hochverfügbarkeitsmodus. Diese Modi eignen sich sowohl für die Beschleunigung von Gerät zu Gerät als auch für die Client-zu-Gerät-Beschleunigung. Sie können alleine (*transparenter Modus*) oder in Kombination mit dem Redirector-Modus verwendet werden.

Platzieren Sie die Geräte in einem sicheren Teil Ihres Netzwerks

Eine Appliance hängt genauso von Ihrer vorhandenen Sicherheitsinfrastruktur ab wie Ihre Server. Es sollte auf derselben Seite der Firewall (und der VPN-Einheit, falls verwendet) wie die Server platziert werden.

Vermeiden Sie NAT-Probleme

Network Address Translation (NAT) auf der Plug-In-Seite wird transparent behandelt und ist kein Problem. Auf der Geräteseite kann NAT problematisch sein. Wenden Sie die folgenden Richtlinien an, um eine reibungslose Bereitstellung zu gewährleisten:

- Legen Sie die Appliance in denselben Adressraum wie die Server, damit alle Adressänderungen, die verwendet werden, um die Server zu erreichen, auch auf die Appliance angewendet werden.
- Greifen Sie niemals mit einer Adresse auf die Appliance zu, 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.

Wählen Sie den Softboost-Modus

Wählen Sie auf der Seite Einstellungen konfigurieren: Bandbreitenmanagement den Softboost-Modus aus. 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 führt eine Liste von Beschleunigungsregeln, die den Clients mitteilen, welcher Datenverkehr beschleunigt werden soll. Jede Regel gibt eine Adresse oder ein Subnetz und einen Portbereich an, den die Appliance beschleunigen kann.

Was beschleunigt werden soll-Die Wahl des zu beschleunigenden Datenverkehrs hängt von der Verwendung ab, für die die Appliance verwendet wird:

- VPN-Beschleuniger - Wenn die Appliance als VPN-Beschleuniger verwendet wird und der gesamte VPN-Verkehr durch die Appliance fließt, sollte der gesamte TCP-Verkehr 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. Eine 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 herstellt. Daher empfiehlt Citrix, Beschleunigungsregeln so zu konfigurieren, dass eine bestimmte Appliance nur ihre eigene Site beschleunigen kann.

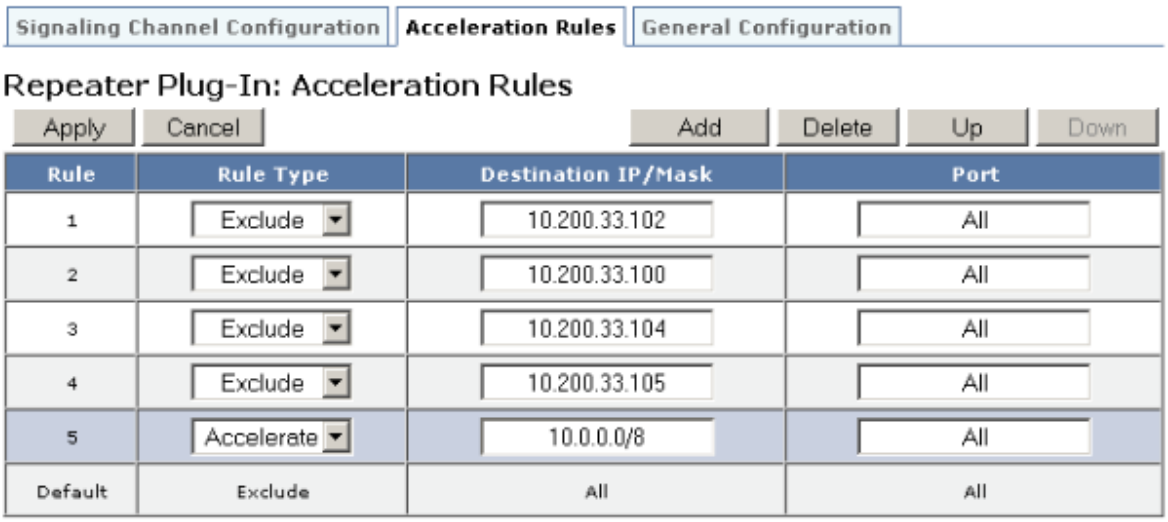
- Sonstige Verwendung - Wenn das Plug-In weder als VPN-Beschleuniger noch im Redirector-Modus verwendet wird, sollten die Beschleunigungsregeln Adressen enthalten, die remote zu den Benutzern und lokal in Rechenzentren sind.

Definieren Sie die Regeln - Definieren Sie Beschleunigungsregeln für die Appliance 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. Festlegen von Beschleunigungsregeln



1. Auf der Registerkarte Konfiguration: WANOP Plug-In: Beschleunigungsregeln:
   - Fügen Sie eine beschleunigte Regel für jedes lokale LAN-Subnetz hinzu, das von der Appliance erreicht werden kann. 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 über der Beschleunigungsregel für 10.217.1.0/24.
3. Wenn Sie die 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 spez-

ifische 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 **Apply**. 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 unterhält einen Dialog mit der Appliance über eine Signalverbindung, die standardmäßig auf Port 443 (HTTPS) liegt, was durch die meisten Firewalls zulässig ist.
- **Für die Kommunikation mit Servern verwendete Ports**—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 über Port 80 eine Verbindung zur Appliance her. Die Appliance wiederum kontaktiert den Server über Port 80.

  Im Redirector-Modus wird nur der bekannte Port (d. h. der Zielport des TCP-SYN-Pakets) beibehalten. Der vergängliche Port ist nicht erhalten. Im transparenten Modus bleiben beide Anschlüsse erhalten.

  Die Appliance geht davon aus, dass sie an jedem vom Client angeforderten Port mit dem Server kommunizieren kann, und der Client geht davon aus, dass er an jedem gewünschten Port mit der Appliance kommunizieren kann. Dies funktioniert gut, wenn die Appliance denselben Firewall-Regeln unterliegt wie die Server. 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 vorkommen und sind garantiert in den SYN- und SYN-ACK-Paketen vorhanden, die die Verbindung herstellen.

Ihre Firewall darf TCP-Optionen im Bereich von 24-31 (Dezimal) nicht blockieren, sonst kann keine Beschleunigung stattfinden. 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

October 28, 2021

Sie können Parameter in der
WANOP Client Plug-in-Distributionsdatei ändern, die im Standardformat von Microsoft Installer (MSI) vorliegt. Die Anpassung erfordert die Verwendung eines MSI-Editors.

> **Hinweis**
>
> Die geänderten Parameter in Ihrem bearbeiteten. MSI-Datei gilt nur für Neuinstallationen. 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.

Bewährte Methoden:

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 eine Appliance haben. 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 das Ändern dieser einzelnen DNS-Definition auf Ihrem DNS-Server die Appliance-Liste in Ihren Plug-Ins automatisch aktualisiert.

Sie können den DNS-Eintrag auch für mehrere Appliances auflösen lassen, dies ist jedoch unerwünscht, es sei denn, alle Appliances sind identisch konfiguriert, da das Plug-in einige seiner Eigenschaften von der Appliance ganz links in der Liste übernimmt und sie global anwendet (einschließlich SSL-Komprimierungseigenschaften). 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.

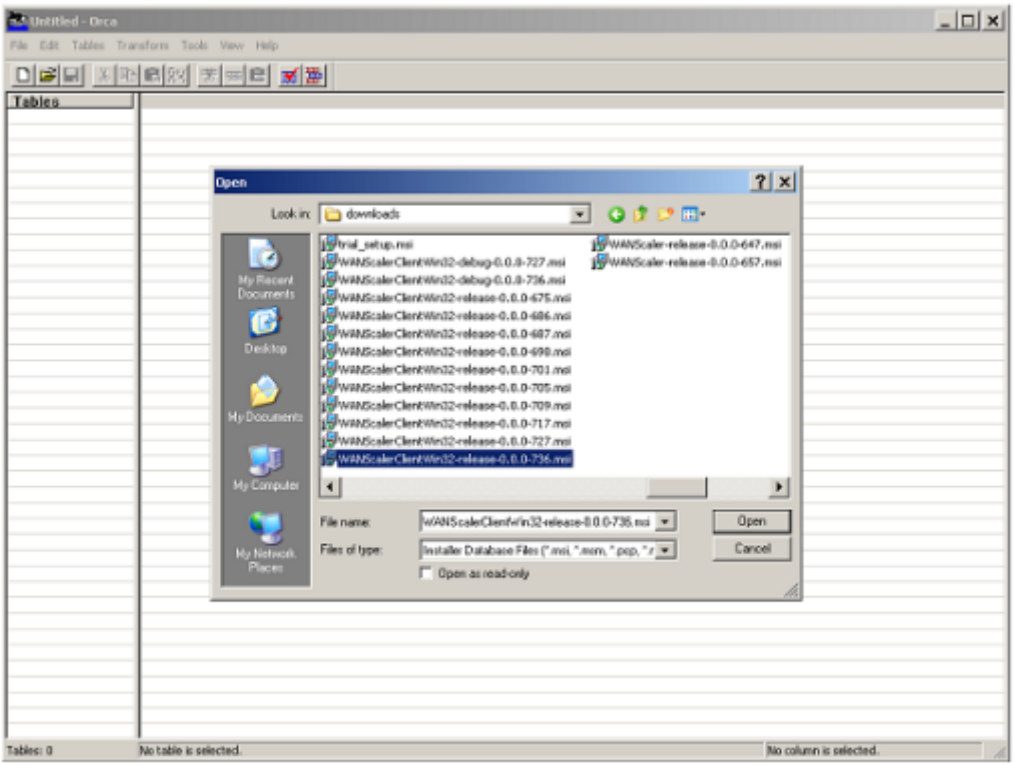
- So installieren Sie den Orca MSI Editor
    1. Laden Sie die PSDK-x86.exe Version des SDK herunter und führen Sie es aus. Folgen Sie den Installationsanweisungen.

2. Sobald das SDK installiert ist, muss der Orca-Editor installiert werden. Es wird unter Microsoft Platform SDK\ Bin\ Orca.Msi sein. 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. Starte Orca mit **Start > Alle Programme > Orca.** Wenn ein leeres Orca-Fenster angezeigt wird, öffnen Sie die MSI-Datei des WANOP Client Plug-in 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	Anmerkungen
WSAPPLIANCES	Liste der Appliances	–	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 für die Signalisierung von Verbindungen verwendete Port vom Standard unterscheidet (443), geben Sie den Port in der Form an Appliance1:Port_Number.
DBCMINSIZE	Minimum des Speicherplatz, der für die Komprimierung verwendet werden soll, in Megabyte	250	Eine Änderung auf einen größeren Wert (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	Anmerkungen
EKEYPEM	Privater Schlüssel für das Plug-In. Teil des Zertifikat-/Schlüsselpaars, das für die SSL-Komprimierung verwendet wird	–	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	–	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	Zertifizierungsstellenzertifikat für das Plug-in. Wird mit SSL-Komprimierung verwendet		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

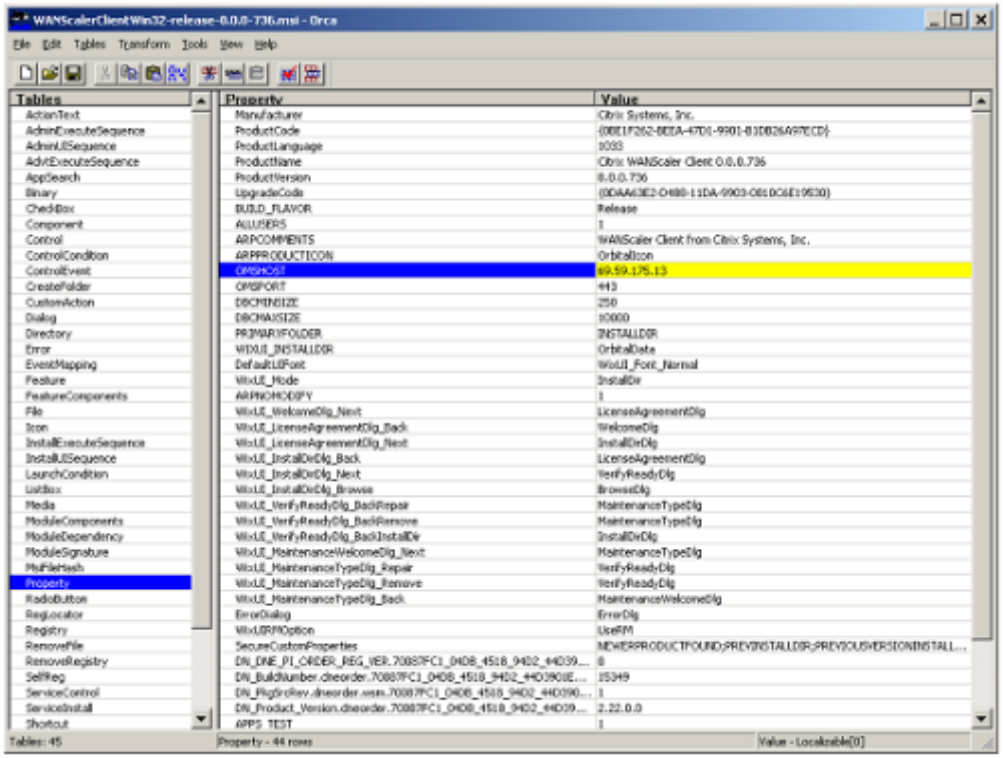
den neuen Wert ein und drücken Sie die **Eingabetaste**.

Parameter	Beschreibung	Standard	Anmerkungen
WSAPPLIANCES	Liste der Appliances	–	Geben Sie hier die IP- oder DNS-Adressen Ihrer WANOP-Client-Plug-in-Appliances in einer durch Kommas getrennten Liste in Form von *{Appliance1, Appliance2, Appliance3}* ein. Wenn sich der für die Signalisierung von Verbindungen verwendete Port vom Standard unterscheidet (443), geben Sie den Port in der Form an *Appliance1:Port_Number*.
DBCMINSIZE	Minimum des Speicherplatz, der für die Komprimierung verwendet werden soll, in Megabyte	250	Eine Änderung auf einen größeren Wert (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	Anmerkungen
PRIVATEKEYPEM	Privater Schlüssel für das Plug-In. Teil des Zertifikat-/Schlüsselpaars, das für die SSL-Komprimierung verwendet wird	–	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	–	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	Zertifizierungsstellenzertifikat für das Plug-in. Wird mit SSL-Komprimierung verwendet		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 Ihre 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 Ihre 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. Prüfen Sie die Größe der gespeicherten Datei. Wenn es 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

October 28, 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 -Site ab.

> **Hinweis:**
>
> Die WANOP Client Plug-in-Benutzeroberfläche 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 durch Kommas getrennten Liste von IP- oder DNS-Adressen bestehen. Die beiden Formen können gemischt werden. Sie können die Distributionsdatei 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 geeignete Appliance gesendet, und der gesamte andere Datenverkehr wird direkt an den Server gesendet. Die Benutzeranwendung ist sich nicht bewusst, dass dies geschieht.

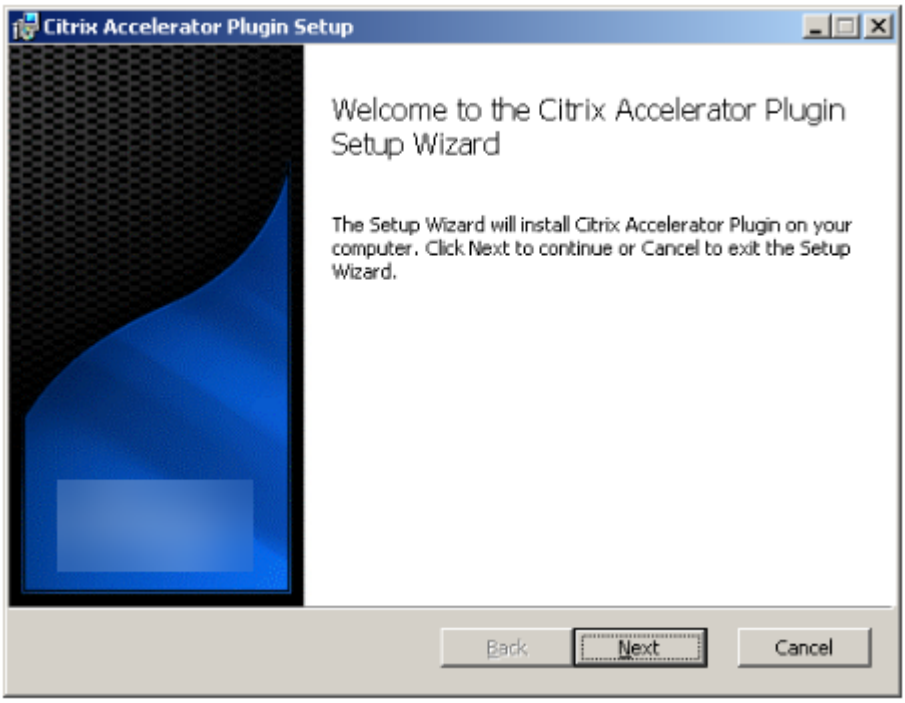
Installation

> **Voraussetzungen:**
>
> Für Windows 10 müssen alle Treiber über eine gültige digitale Signatur verfügen, um die Installation fehlerfrei durchführen zu können.

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. Erstinstallationsbildschirm:



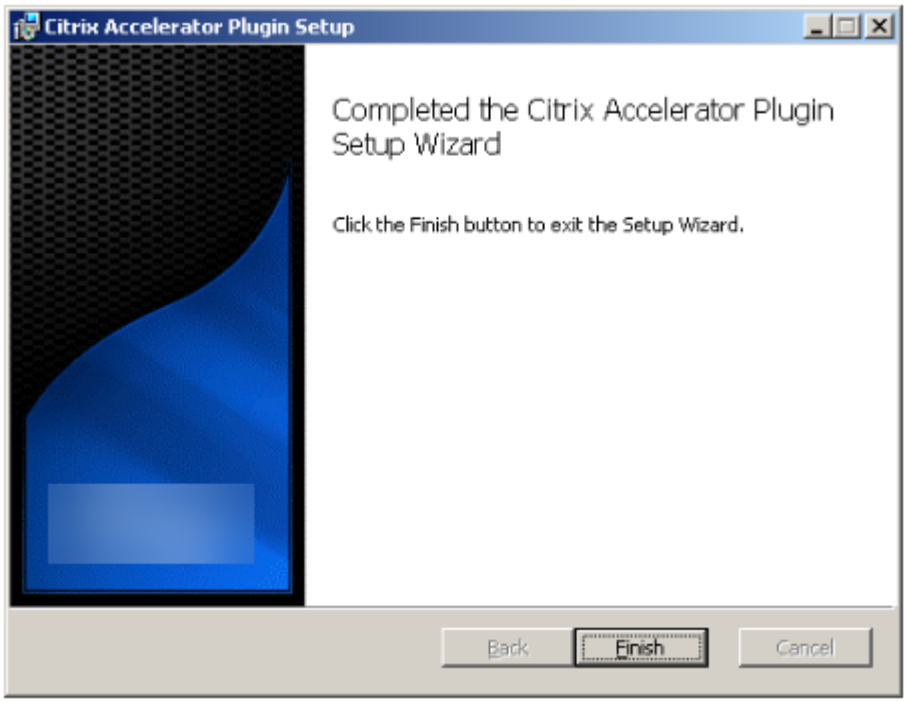
Die folgenden Schritte sind für eine interaktive Installation. Eine unbeaufsichtigte Installation kann mit dem Befehl durchgeführt werden:

"**msiexec /i client_msi_file /qn**"

2. Das Installationsprogramm fragt nach dem Speicherort, an dem die Software installiert werden soll. Das von Ihnen angegebene Verzeichnis wird sowohl für die Clientsoftware als auch für den datenträgerbasierten Komprimierungsverlauf verwendet. Zusammen benötigen sie mindestens 500 MB Speicherplatz.

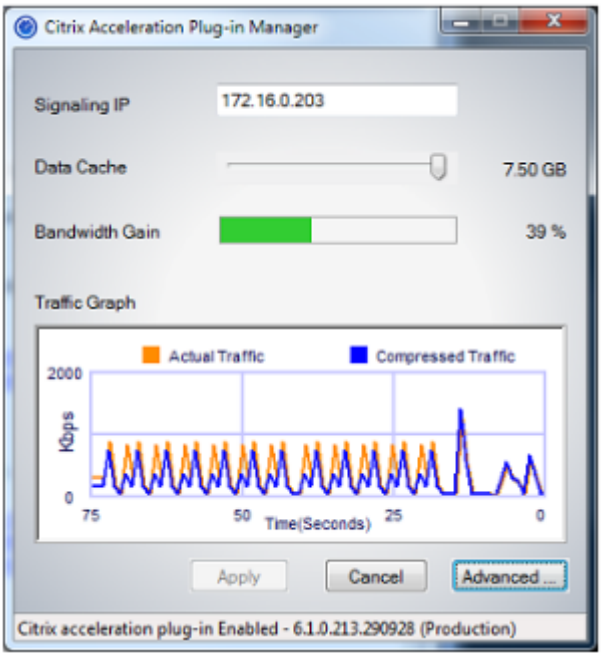
3. Wenn das Installationsprogramm abgeschlossen ist, werden Sie möglicherweise aufgefordert, das System neu zu starten. Nach einem Neustart startet das WANOP Client Plug-In Plug-In automatisch.

Abbildung 2. Letzter Installationsbildschirm



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: Signaling Addresses die Signalisierungs-IP-Adresse Ihrer

Appliance 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 mit dem Schieberegler "Data Cache"die Menge an Speicherplatz aus, die 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 die Liste Beschleunigungsregeln jede Appliance als Verbunden und die beschleunigten Subnetze jeder Appliance als beschleunigt anzeigen. Wenn nicht, überprüfen Sie das IP-Feld Signalisierungsadressen und Ihre Netzwerkkonnektivität im Allgemeinen.

Problembehandlung bei Plug-Ins

Die Plug-In-Installation verläuft in der Regel reibungslos. Wenn nicht, suchen Sie nach folgenden Problemen:

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 Ausfall der Beschleunigung (keine beschleunigten Verbindungen auf der Registerkarte **Diagnose** aufgeführt) weist normalerweise darauf hin, dass etwas die Kommunikation mit der Appliance verhindert. 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 läuft nicht 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 Netzwerkverbesserungs-Sperrfehler

In seltenen Fällen wird nach der Installation des Plug-Ins und dem Neustart des Computers die folgende Fehlermeldung zweimal angezeigt:

Die Installation von Deterministic Network Enhancer erfordert zuerst einen Neustart, um gesperrte Ressourcen freizugeben. Bitte führen Sie diese Installation nach dem Neustart des Computers erneut aus.

Sie umgehen das Problem wie folgt:

1. Gehen Sie zu **Software hinzufügen/entfernen** und entfernen Sie das WANOP Client-Plug-in, falls vorhanden.
2. Wechseln Sie zu **Systemsteuerung** > **Netzwerkadapter** > **Lokale 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:\windows\inf (oder das entsprechende Verzeichnis, wenn Sie Windows an einem nicht standardmäßigen Speicherort installiert haben).
4. Geben Sie den folgenden Befehl ein:

   finde "dne2000.cat"oem*.inf
5. Suchen Sie die OEM*.inf-Datei mit der höchsten Nummer, die eine übereinstimmende Zeile zurückgegeben hat (die übereinstimmende Zeile ist CatalogFile= dne2000.cat) und bearbeiten Sie sie. Beispiel:

   Notizblock oem13.inf
6. Lösche alles außer den drei Zeilen oben, die mit Semikola beginnen, und speichere dann die Datei. Dadurch werden alle unangemessenen oder veralteten Einstellungen gelöscht und bei der nächsten Installation werden Standardwerte verwendet.
7. Versuchen Sie die Installation erneut.

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, versuchen Sie die folgenden Schritte:

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 vorübergehend alle Firewall- und Antivirensoftware.
4. Wenn einiges 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

October 28, 2021

Die GUI des WANOP Client Plug-ins wird angezeigt, wenn Sie mit der rechten Maustaste auf das **Citrix Accelerator Plug-in-Symbol** klicken und **Beschleunigung verwalten**auswählen. Das Basic-Display der GUI erscheint zuerst. Es gibt auch ein Advanced-Display, das auf Wunsch verwendet werden kann.

Grundlegendes Display

Auf der Seite Basic können Sie zwei Parameter einstellen:

- Das Feld Signalisierungsadressen gibt die IP-Adresse jeder Appliance an, mit der sich das Plug-in verbinden kann. Citrix empfiehlt, nur eine Appliance aufzulisten, aber Sie können eine durch Kommas getrennte Liste erstellen. Dies ist eine geordnete Liste, wobei die Geräte ganz links Vorrang vor den anderen haben. Die Beschleunigung wird mit dem Gerät ganz links versucht, für das eine Signalverbindung hergestellt werden kann. Sie können sowohl DNS-Adressen als auch IP-Adressen verwenden.

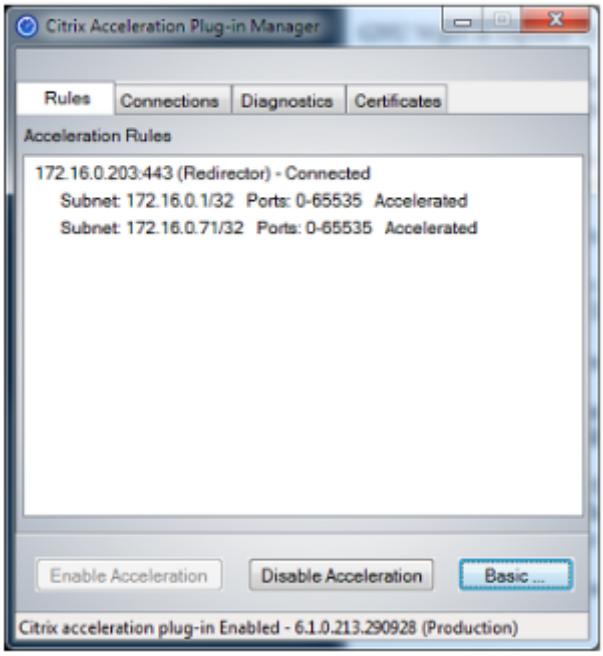
  Beispiele: 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

- Der Data Cache-Schieberegler passt den Speicherplatz an, der dem datenträgerbasierten Komprimierungsverlauf des Plug-Ins zugewiesen ist. Mehr ist besser.

  Zusätzlich gibt es eine Taste, um zum erweiterten Display zu wechseln.

Erweitertes Display

Die Seite “Erweitert”enthält vier Registerkarten: Regeln, Verbindungen, Diagnose und Zertifikate.



Am unteren Rand des Displays befinden sich Schaltflächen, mit denen Sie die Beschleunigung aktivieren, die Beschleunigung deaktivieren und zur Seite Basic zurückkehren können.

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”

Auf der Registerkarte **Verbindungen** wird die Anzahl der offenen Verbindungen verschiedener Typen aufgeführt:

- **Beschleunigte Verbindungen**—Die Anzahl der offenen Verbindungen zwischen dem WANOP Client Plug-in Plug-in und Appliances. Diese Nummer beinhaltet eine Signalverbindung pro Gerät, jedoch keine beschleunigten CIFS-Verbindungen. Wenn Sie auf Mehr klicken, wird ein Fenster mit einer kurzen Zusammenfassung jeder Verbindung geöffnet. (Mit allen Schaltflächen “Mehr”können Sie die Informationen im Fenster in die Zwischenablage kopieren, falls Sie sie mit dem Support teilen möchten.)
- **Beschleunigte CIFS-Verbindungen**—Die Anzahl offener, beschleunigter Verbindungen mit CIFS-Servern (Windows-Dateisystem). Dies entspricht normalerweise der Anzahl der eingehängten Netzwerkdateisysteme. Wenn Sie auf Mehr klicken, werden dieselben Informationen

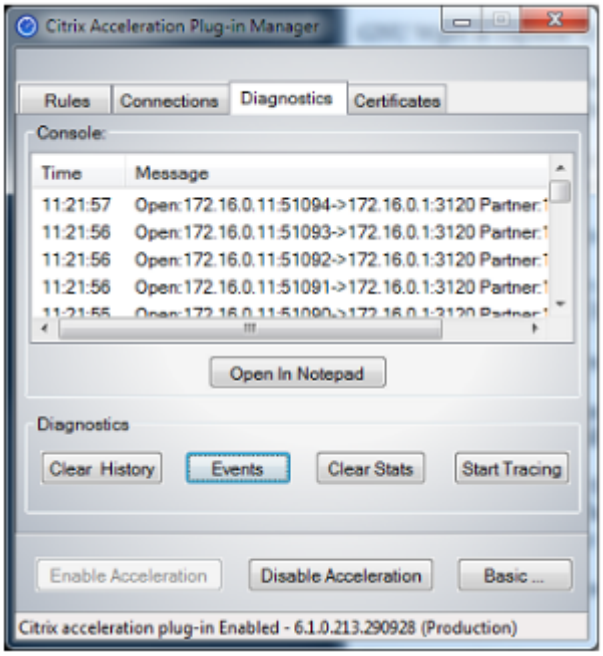
angezeigt wie bei beschleunigten Verbindungen sowie ein Statusfeld, das Aktiv meldet, wenn die CIFS-Verbindung mit den speziellen CIFS-Optimierungen des WANOP Client-Plug-Ins ausgeführt wird.

- **Beschleunigte MAPI-Verbindungen**—Die Anzahl offener, beschleunigter Outlook/Exchange-Verbindungen.
- **Beschleunigte ICA-Verbindungen**—Die Anzahl der offenen, beschleunigten XenApp- und XenDesktop-Verbindungen, die die ICA- oder CGP-Protokolle verwenden.
- **Unbeschleunigte Verbindungen**—Öffnet Verbindungen, die nicht beschleunigt werden. Sie können auf Mehr klicken, um eine kurze Beschreibung anzuzeigen, warum die Verbindung nicht beschleunigt wurde. In der Regel liegt der Grund darin, dass keine Appliance die Zieladresse beschleunigt, die als Servicerichtlinienregel gemeldet wird.
- **Öffnen/Schließen von Verbindungen**—Verbindungen, die nicht vollständig geöffnet sind, aber gerade geöffnet oder geschlossen werden (TCP-Verbindungen "halboffen"oder "halb geschlossen"). Die Schaltfläche "Mehr"zeigt einige zusätzliche Informationen zu diesen Verbindungen an.

Registerkarte "Diagnose"

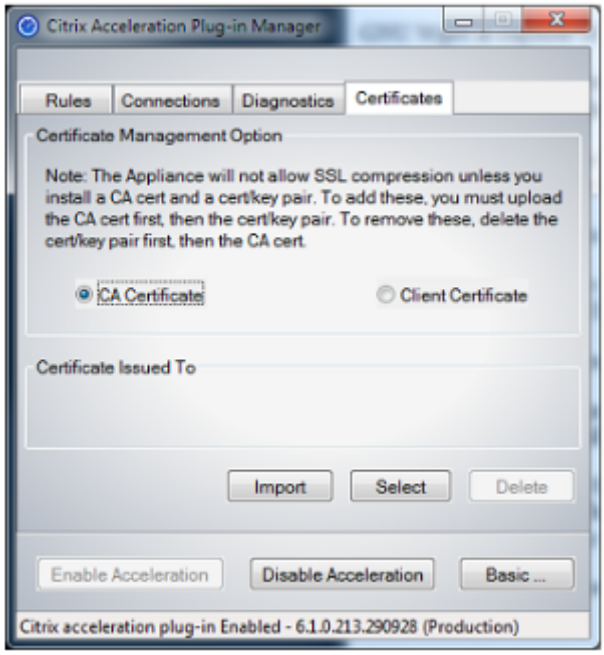
Auf der Seite Diagnose werden die Anzahl der Verbindungen in verschiedenen Kategorien und andere nützliche Informationen angegeben.

- **Tracing starten/Tracing beenden**—Wenn Sie ein Problem melden, fordert Ihr Citrix Vertreter Sie möglicherweise auf, eine Verbindungsverfolgung durchzuführen, um Probleme zu lokalisieren. Dieser Knopf startet und stoppt den Trace. Wenn Sie die Verfolgung beenden, zeigt ein Popup-Fenster die Trace-Dateien an. Senden Sie sie auf die von ihm empfohlenen Mittel an Ihren Citrix Vertreter.
- **Verlauf löschen**—Diese Funktion sollte nicht verwendet werden.
- **Statistiken löschen**—Durch Drücken dieser Schaltfläche werden die Statistiken auf der Registerkarte Leistung gelöscht.
- **Konsole**—Ein scrollbares Fenster mit aktuellen Statusmeldungen, hauptsächlich Meldungen zum Öffnen und Schließen der Verbindung, aber auch Fehler und verschiedenen Statusmeldungen.



Registerkarte “Zertifikate”

Auf der Registerkarte Zertifikate können Sie Sicherheitsanmeldeinformationen für die optionale Funktion für sicheres Peering installieren. Der Zweck dieser Sicherheitsanmeldeinformationen besteht darin, der Appliance zu ermöglichen, zu überprüfen, ob das Plug-in ein vertrauenswürdiger Client ist oder nicht.



So laden Sie das CA-Zertifikat und das Zertifikatschlüsselpaar hoch:

1. Wählen Sie CA **Certificate Management**.
2. Klicken Sie auf **Importieren**.
3. Laden Sie ein Zertifizierungsstellenzertifikat hoch. Die Zertifikatsdatei muss einen der unterstützten Dateitypen (.pem, .crt., .cer oder .spc) verwenden. Möglicherweise wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, den zu verwendenden Zertifikatspeicher auszuwählen und Ihnen eine Liste von Schlüsselwörtern anzuzeigen. Wählen Sie das erste Schlüsselwort in der Liste aus.
4. Wählen Sie **Clientzertifikatverwaltung**.
5. Klicken Sie auf **Importieren**.
6. Wählen Sie das Format des Zertifikatschlüsselpaars (PKCS12 oder PEM/DER).
7. Klicken Sie auf **Absenden**.

> **Hinweis**
>
> Im Fall von PEM/DER gibt es separate Upload-Felder 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

October 28, 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

October 28, 2021

- **Problem**: Ich habe Probleme mit der Konnektivität des Signalkanals. Wie kann ich diese Probleme lösen?

  Lösung: Führen Sie die folgenden Schritte zur Fehlerbehebung durch, um Probleme mit der Signalkanalkonnektivität zu beheben:

  - 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 des Signalkanalquellenfilters 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**: Auf 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**: Wenn Sie mithilfe des WANOP-Plug-Ins eine Verbindung zur WANOP-Appliance herstellen, wird der folgende Fehlermeldungseintrag auf der Registerkarte Warnungen protokolliert:

  Mehr WANOP-Plug-Ins als das aktuelle Limit von <Number> haben versucht, eine Verbindung mit dieser Appliance herzustellen.

  Ursache: Die Anzahl der Verbindungen zur WANOP-Appliance hat das Limit für lizenzierte Benutzer überschritten.

  Auflösung: Warten Sie entweder, bis ein Benutzer die Verbindung trennt oder beendet.

- **Problem**: Eine 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: Führen Sie die folgenden Schritte zur Fehlerbehebung durch, um dieses Problem zu beheben:

  - Stellen Sie sicher, dass die 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-Verbindung

October 28, 2021

Das Server Message Block (SMB) -Protokoll ist ein Netzwerk-Filesharing-Protokoll. Die Nachrichtenpakete, die eine bestimmte Version des Protokolls definieren, werden als Dialekt bezeichnet. Das Common Internet File System (CIFS) -Protokoll 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.

Das 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 Verkehr das WANOP-Modul durchläuft:

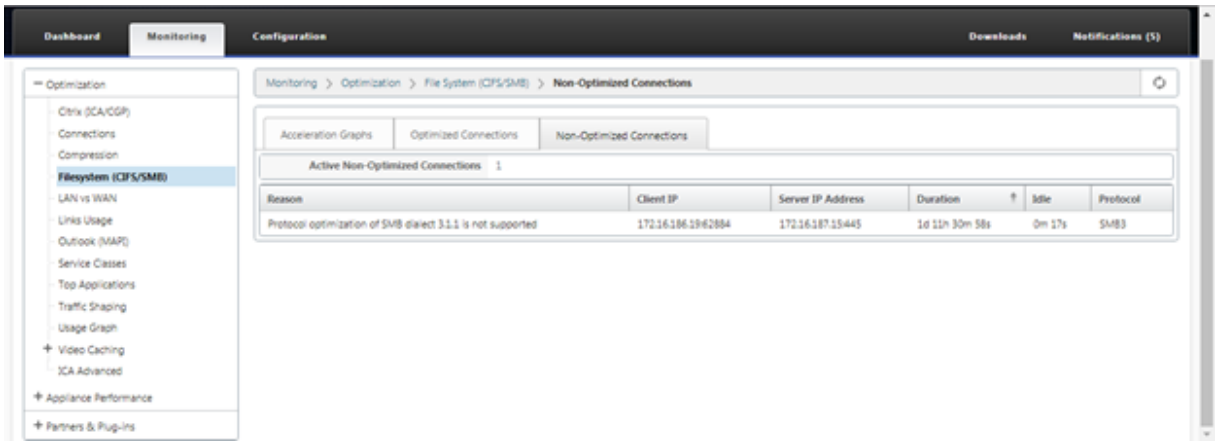
- Es ist gezählt/sichtbar als Teil von SMB 3.1 CIFS unoptimierten Verbindungen
- Die folgende Trace-Meldung wird angezeigt: “Diese Verbindung durchlaufen, da SMB 3.1.1 nicht unterstützt wird”.

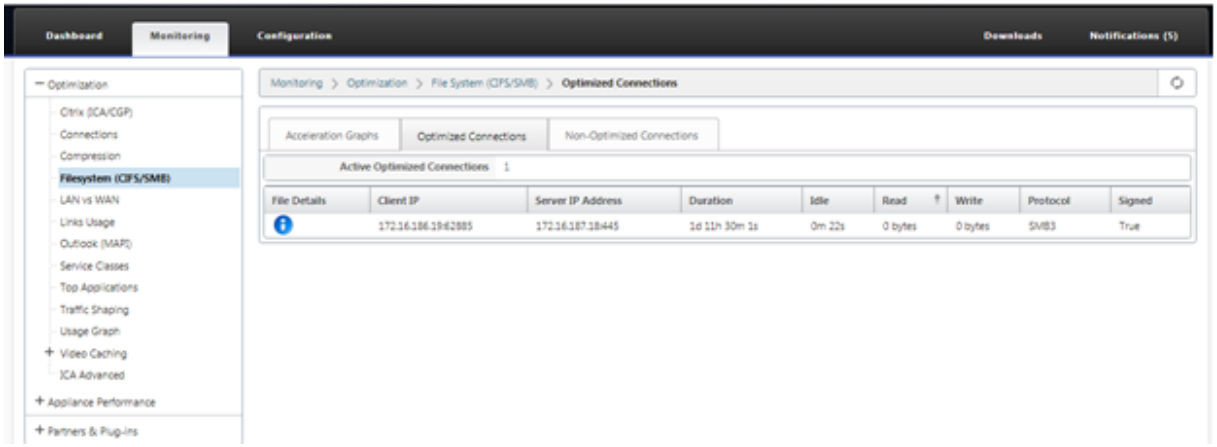
Client	Server	SMB-Ausführung
Windows 10	Gewinnen Sie 2016, 2012R2	SMB 3.1.1, 3.0.2
Windows 8.1	SMB 3.0	SMB 3.0

Client	Server	SMB-Ausführung
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 GUI der Citrix SD-WAN WANOP Appliance zu **Überwachung** > **Dateisystem (CIFS/SMB)**. Klicken Sie auf die Registerkarte **Nicht optimierte Verbindungen**, die folgende Meldung wird angezeigt: Die *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

August 29, 2022

In den “How-to-Articles”wird das Verfahren zur Konfiguration der unterstützten Funktionen von Citrix SD-WAN beschrieben. Diese Artikel enthalten Informationen zu einigen der folgenden wichtigen Funktionen:

Klicken Sie unten auf einen Feature-Namen, um die Liste der Artikel mit Anleitungen für diese Funktion anzuzeigen.

- Virtuelles Routing und Weiterleitung
- RED für QoS Fairness aktivieren
- Konfiguration
- Dynamisches Routing
- DHCP-Server und DHCP-Relay
- Routen-Filter
- IPSec-Kündigung und Überwachung
- Secure Web Gateway
- QoS
- FIPS-konformer Betrieb —IPsec-Tunnel
- Dynamische NAT-Konfiguration
- Adaptive Bandbreitenerkennung
- Aktive Bandbreitentests
- BGP Erweiterungen
- Service Class Assoziation mit SSL-Profilen
- Sicheres Peering und manuelles sicheres Peering
- Zero-Touch-Bereitstellung
- Bereitstellung im Zwei-Box-Modus

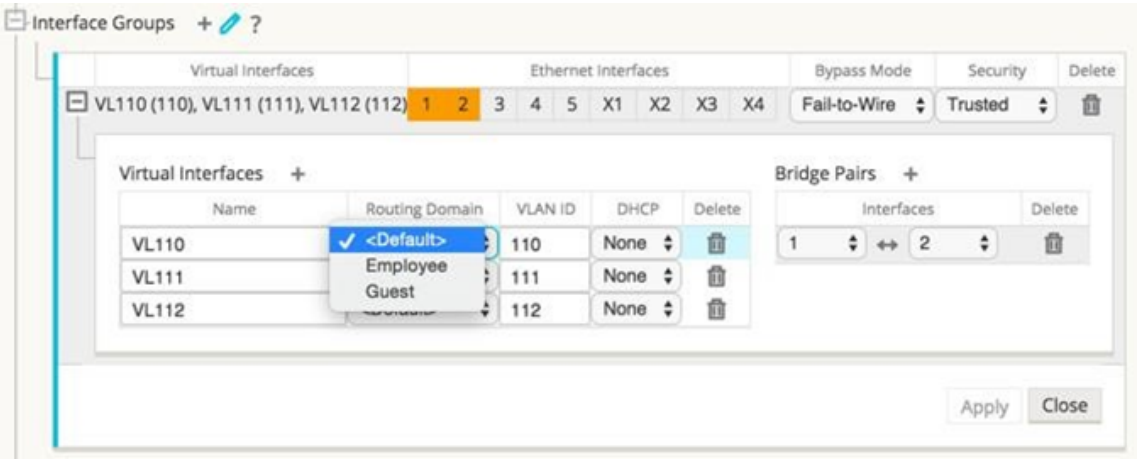
Schnittstellengruppen

October 28, 2021

So konfigurieren Sie Schnittstellengruppen:

1. Navigieren Sie im **Konfigurationseditor**zu **Sites** > **[Client-Site-Name]** > **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 wurden, sind nur diese Schnittstellen verfügbar, wenn diese Routingdomäne verwendet wird.



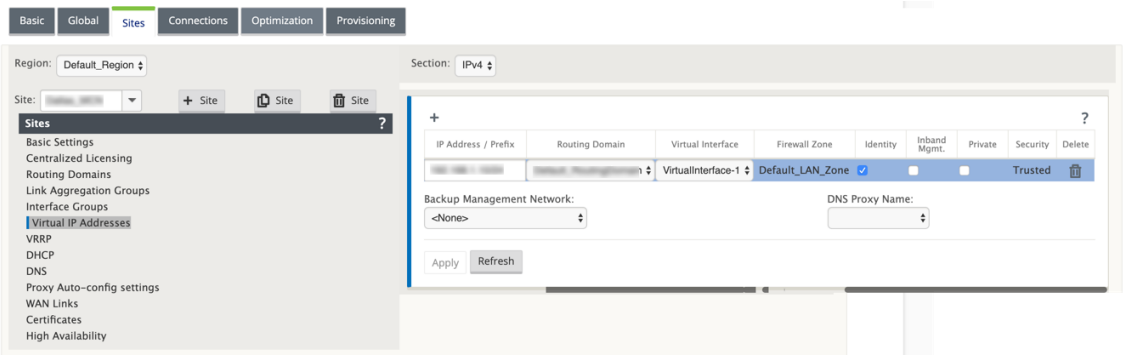
Konfigurieren der Identität virtueller IP-Adresse

October 28, 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 **Konfigurationseditor**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.



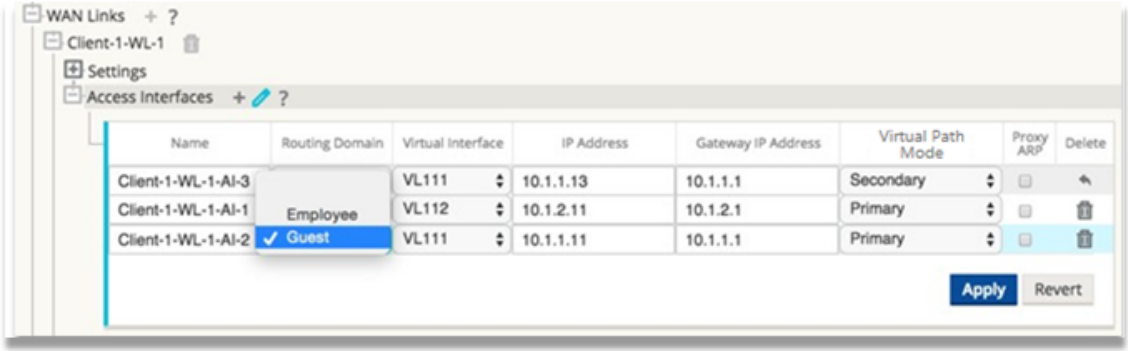
Konfiguration der Zugriffsschnittstelle

September 26, 2023

So konfigurieren Sie die Zugriffsoberfläche:

1. Navigieren Sie im **Konfigurationseditor**zu **Sites** > **[Client-Site-Name]** > **WAN-Links** > **[WAN-Linkname]** > **Zugriffsschnittstellen**.
2. Wählen Sie eine **Routingdomäne** aus dem Dropdownmenü aus, wenn Sie ein Access Interface konfigurieren.

   Ausführliche Anweisungen finden Sie im Abschnitt **Konfigurieren der Zugriffsschnittstelle** unter MCN konfigurieren.



Virtuelle IP-Adressen konfigurieren

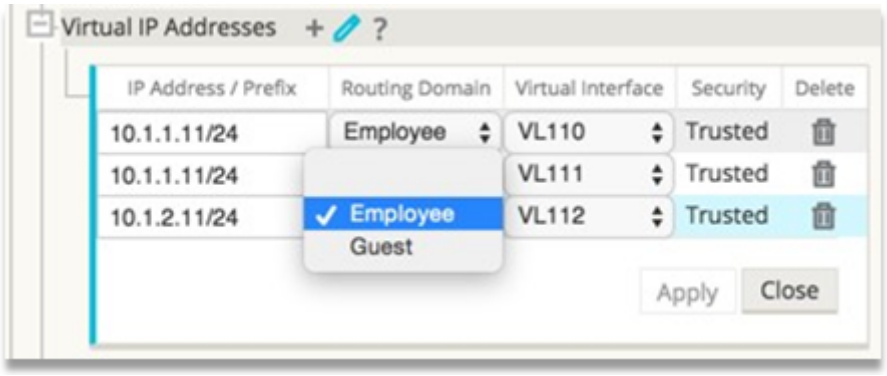
October 28, 2021

So konfigurieren Sie virtuelle IP-Adressen:

1. Navigieren Sie im **Konfigurationseditor**zu **Sites > [Client-Site-Name] > Virtuelle IP-Adressen**.
2. Wählen Sie eine **Routingdomäne** aus dem Dropdownmenü aus, wenn Sie virtuelle IP-Adressen konfigurieren.

   Ausführliche Anweisungen finden Sie unter Konfigurieren virtueller IP-Adressen.

Die von Ihnen gewählte Routingdomäne legt fest, welche virtuellen Schnittstellen im Dropdownmenü verfügbar sind.



GRE Tunnel konfigurieren

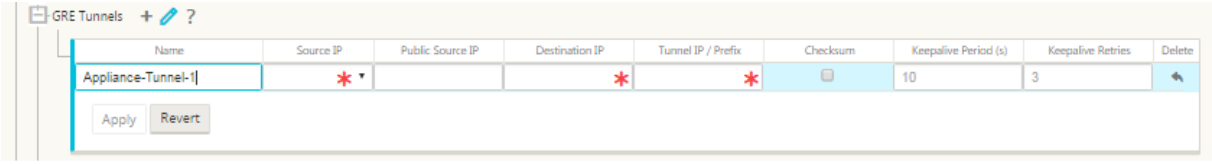
October 28, 2021

So konfigurieren Sie GRE-Tunnel:

1. Navigieren Sie im Konfigurationseditor 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 im Dropdownmenü verfügbare **Quell-IP-Adresse** aus. Die Routingdomäne legt im Dropdownmenü fest, welche Quell-IP-Adressen verfügbar sind.
4. (Optional) Wählen Sie die **Public Source-IP**aus. Dieses Feld kann leer sein, wenn diese Adresse der Quell-IP entspricht.
5. Geben Sie die **Ziel-IP-Adresse** des GRE-Tunnels ein.
6. Geben Sie die **IP/Präfix-Adresse des Tunnels** des GRE-Tunnels ein.
7. Klicken Sie auf **Prüfsumme**, wenn Sie die Prüfsumme im GRE-Tunnelkopf verwenden möchten.

8. Geben Sie einen Wert für den **Keepalive-Zeitraum** in Sekunden ein. Wenn Sie 0 konfigurieren, wird kein Keepalive-Paket übertragen, aber der GRE-Tunnel ist aktiv.
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 in den Konfigurieren von GRE-Tunneln auf der MCN-Website.



Weitere Hinweise zur Sicherung des Web-Gateways mithilfe von GRE-Tunneln finden Sie unter; Secure Web Gateway

Dynamische Pfade für Zweigkommunikation einrichten

October 28, 2021

Angesichts der Nachfrage nach VoIP und Videokonferenzen bewegt sich der Verkehr zunehmend zwischen Büros. Es ist ineffizient, Vollmaschenverbindungen über Rechenzentren einzurichten, was zeitaufwändig sein kann.

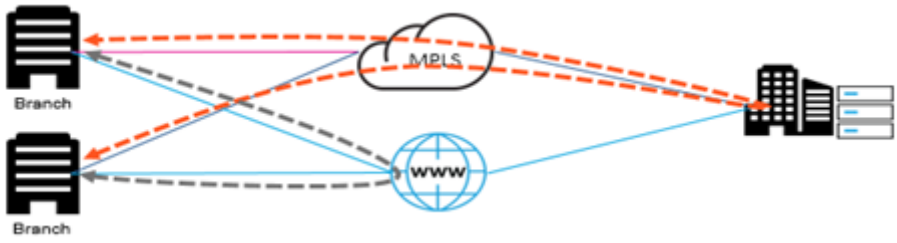
Mit Citrix SD-WAN müssen Sie keine Pfade zwischen jedem Büro konfigurieren. Sie können die Funktion “Dynamic Path”aktivieren, und die SD-WAN-Lösung erstellt bei Bedarf automatisch Pfade zwischen Büros. Die Sitzung verwendet anfänglich einen vorhandenen festen Pfad. Und wenn die Bandbreite und der Zeitschwellenwert erreicht sind, wird dynamisch ein Pfad erstellt, wenn dieser neue Pfad bessere Leistungseigenschaften als der feste Pfad aufweist. Der Sitzungsverkehr wird über den neuen Pfad übertragen. Dies führt zu einer effizienten Ressourcennutzung. Pfade existieren nur, wenn sie benötigt werden, und reduzieren den Datenverkehr, der zum und vom Rechenzentrum übertragen wird.

Zusätzliche Vorteile des SD-WAN-Netzwerks sind:

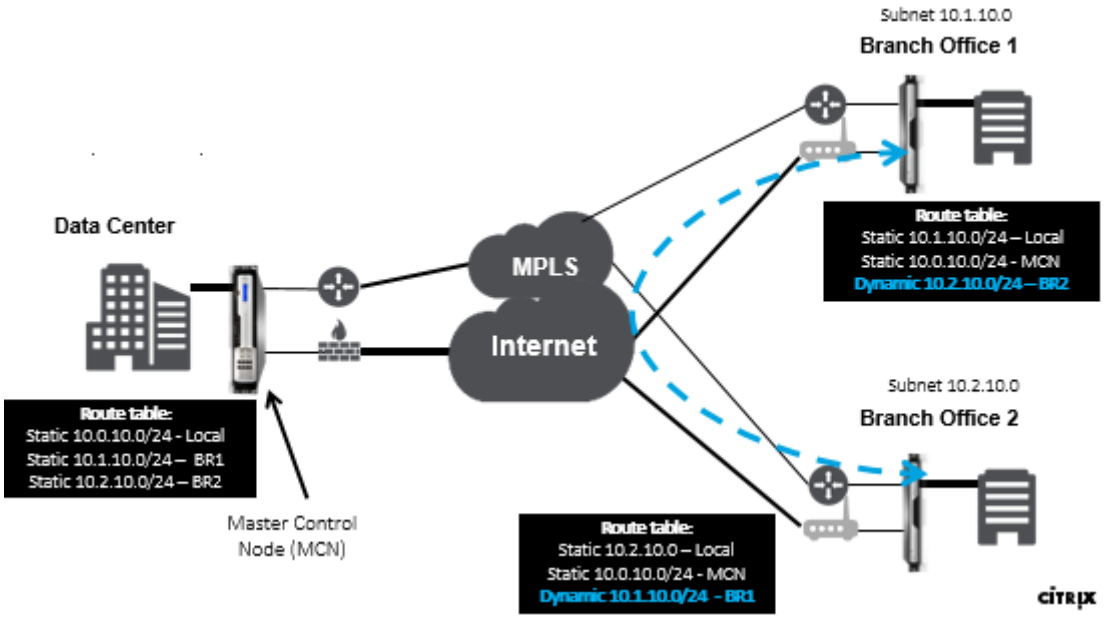
- Bandbreiten- und PPS-Schwellenwerte, um Zweig-zu-Zweig-Verbindungen zu ermöglichen
- Reduzieren Sie die Bandbreitenanforderungen innerhalb und außerhalb des Rechenzentrums und minimieren Sie gleichzeitig die Latenz
- Auf Nachfrage erstellte Pfade hängen von festgelegten Schwellenwerten ab
- Geben Sie Netzwerkressourcen dynamisch frei, wenn dies nicht erforderlich

- Reduzieren Sie die Belastung des Master Control Node und die Latenz

Kommunikation von Verzweigung zu Zweig über dynamische virtuelle Pfade:



SD-WAN-Netzwerk mit dynamischem Pfad:

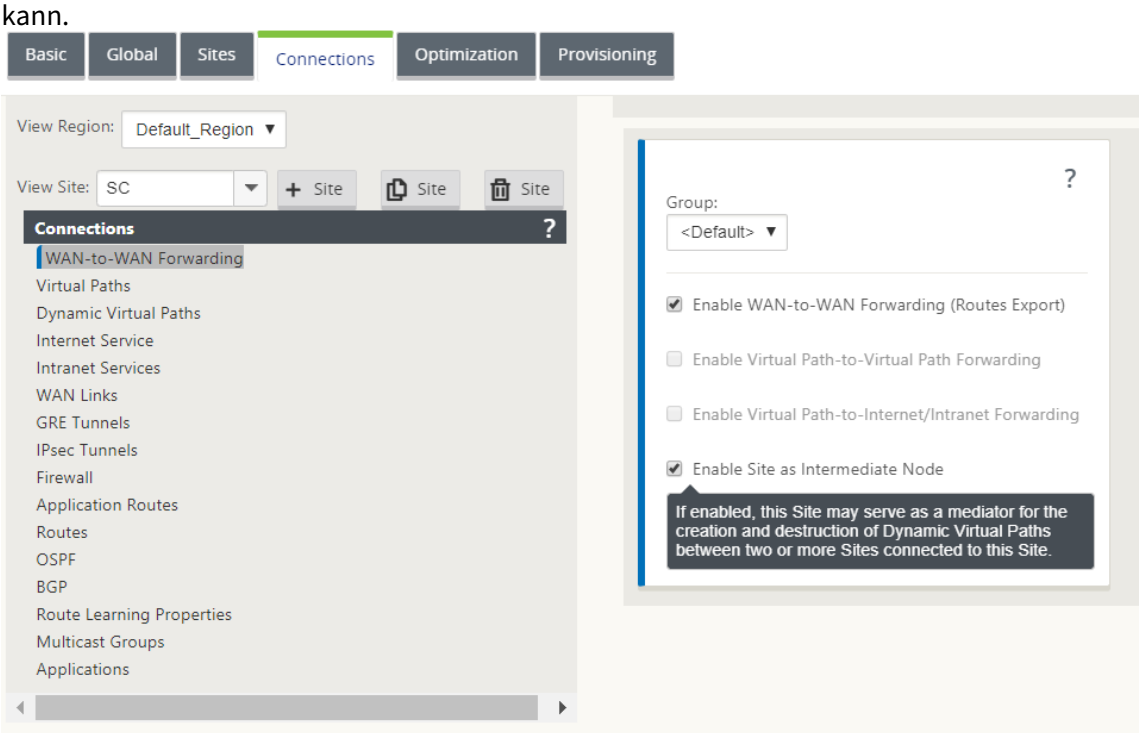


- Dynamische virtuelle Pfade werden für umfangreiche Bereitstellungen wie Unternehmen verwendet
- Kleinere Bereitstellungen verwenden statische virtuelle Pfade und virtuelle Pfade
- Verwenden Sie immer statische virtuelle Pfade zwischen zwei Rechenzentren (DC bis DC)
- Nicht alle WAN-Pfade müssen für die Verwendung des dynamischen virtuellen Pfades konfiguriert werden
- Jede SD-WAN-Appliance verfügt über eine begrenzte Anzahl dynamischer virtueller Pfade (8 dynamische unterste Grenze, 8 statische unterste Grenze = insgesamt 16), die konfiguriert werden können.

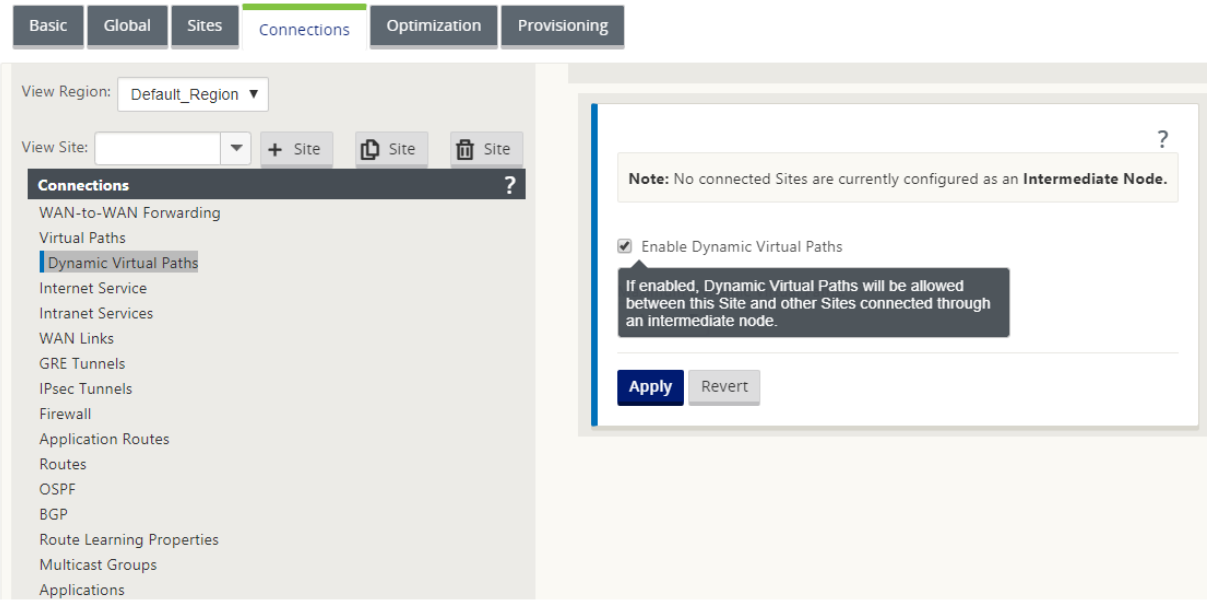
So aktivieren Sie dynamischen virtuellen Pfad in der SD-WAN GUI

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-Site-Name] > WAN zu WAN-Weiterleitung**.
3. Aktivieren Sie **WAN to WAN Forwarding**, damit die Site als Proxy für die Multi-Hop-Site dienen kann.
4. Aktivieren Sie **Site as Intermediate Node**
5. Navigieren Sie zu **Verbindungen > Remotestandort > WAN zu WAN-Weiterleitung**.
6. Aktivieren Sie WAN to WAN Forwarding, damit die Site als Proxy für die Multi-Hop-Site dienen kann.

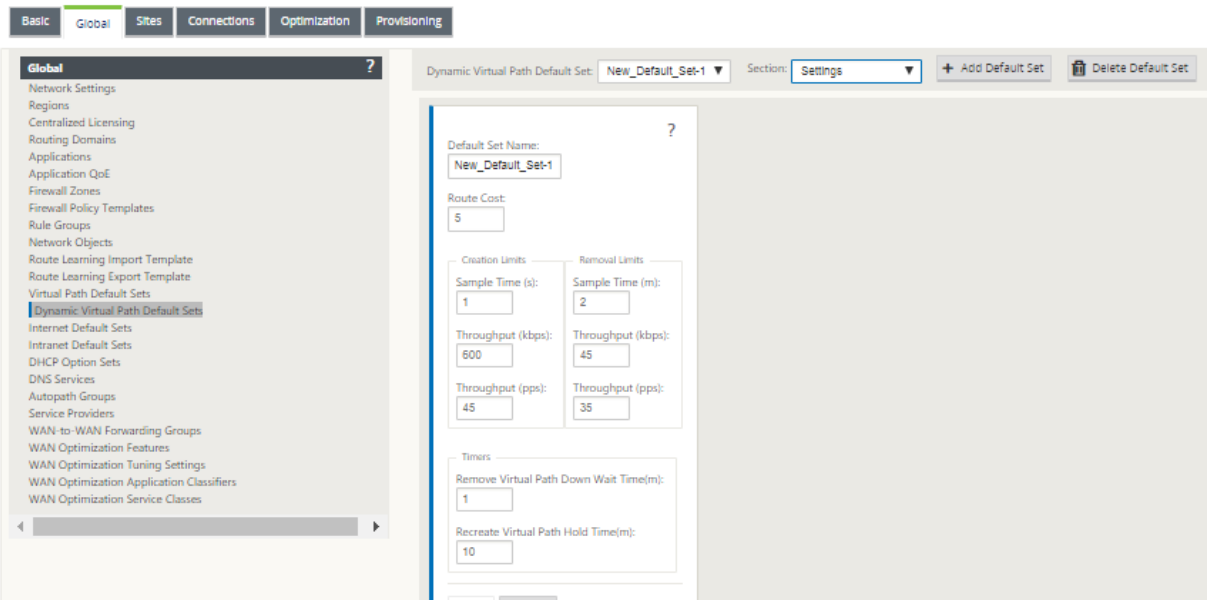


7. Navigieren Sie zu **Verbindungen > Remotestandort > Virtueller Pfad > Dynamischer virtueller Pfad**.
8. Aktivieren Sie **dynamische virtuelle Pfade**.
9. Stellen Sie die maximale Anzahl dynamischer Pfade ein.



So erstellen Sie einen dynamischen virtuellen Pfad

- Die Konfiguration bestimmt, wann ein dynamischer virtueller Pfad aktiv oder ausgefallen ist.
- Konfigurieren Sie die Anzahl der Sample-Pakete (pps) oder die Bandbreite (kbps) innerhalb eines Zeitraums.
- Kann global oder mit WAN Link eingestellt werden, der am Zwischenknoten konfiguriert ist.



WAN-zu-WAN-Weiterleitung

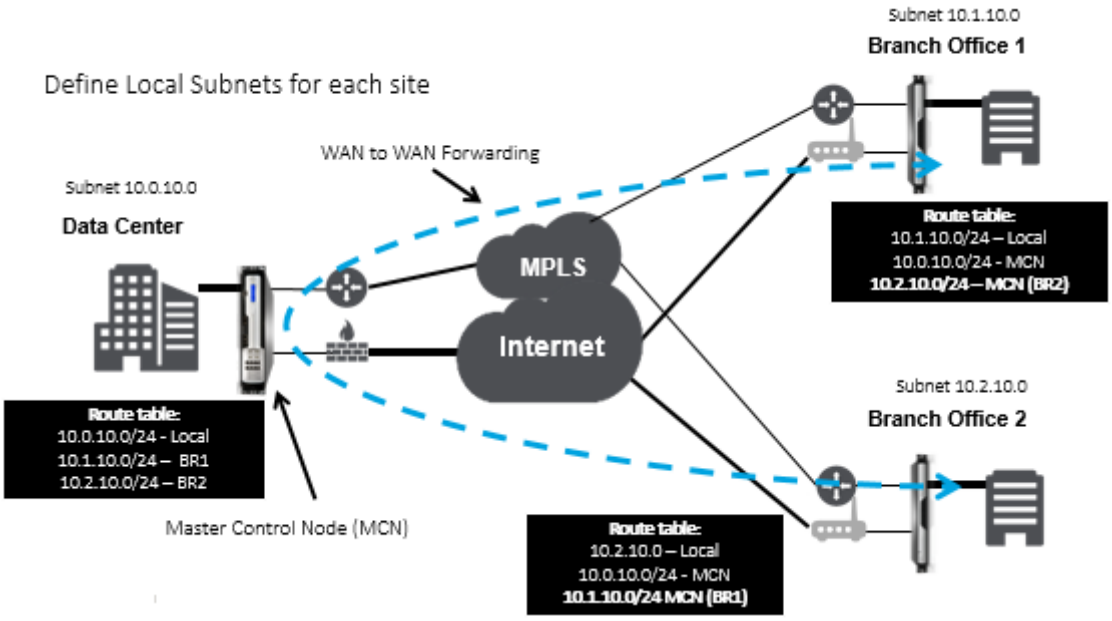
October 28, 2021

Das Aktivieren der WAN-zu-WAN-Weiterleitung auf dem MCN ermöglicht es dem MCN, Routen für Remotestandorte 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

October 28, 2021

Sie können die Webverwaltungsoberfläche der Citrix SD-WAN Appliance verwenden, um unterstützte Funktionen zu überwachen und zu beheben. Nachfolgend finden Sie die Links zu Themen zur Überwachung und Fehlerbehebung, die für Citrix SD-WAN-Appliances gelten.

Virtuelles WAN überwachen

October 28, 2021

Anzeigen grundlegender Informationen für eine Appliance

Verwenden Sie einen Browser, um eine Verbindung zum Management-Webinterface 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.
- **Appliance-Modus** —Dies zeigt an, ob diese Appliance als primärer oder sekundärer MCN oder als Client-Appliance konfiguriert wurde.
- **Management-IP-Adresse** — Dies ist die Management-IP-Adresse für die Appliance.
- **Appliance Uptime** — Dies gibt die Dauer an, für die die Appliance seit dem letzten Neustart ausgeführt wurde.

- **Dienstverfügbarkeit** —Dies gibt die Dauer an, für die der Virtual WAN-Dienst seit dem letzten Neustart ausgeführt wurde.

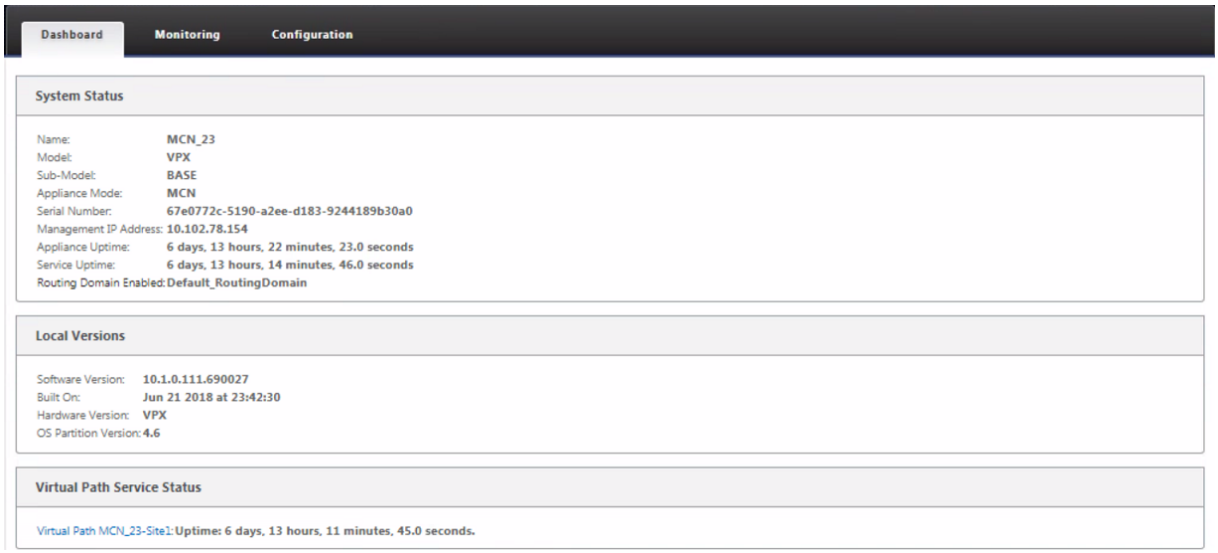
Status des virtuellen Pfaddienstes:

[Site-Name des]virtuellen Pfads —Dies 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 Virtual WAN-Dienst deaktiviert ist, werden anstelle dieses Abschnitts ein Warnsymbol (Goldrutendelta) und eine entsprechende Warnmeldung angezeigt.

Lokale Versionsinformationen:

- **Softwareversion** — Dies ist die Version des CloudBridge Virtual Path Softwarepakets, das derzeit auf der Appliance aktiviert ist.
- **Aufbauen auf** —Dies ist das Erstellungsdatum für die Produktversion, die derzeit auf der lokalen Appliance ausgeführt wird.
- **Hardwareversion** —Dies ist die Hardwaremodellnummer und -version der Appliance.
- **Betriebssystempartitionsversion** — Dies ist die Version der Betriebssystempartition, die derzeit auf der Appliance aktiv ist.

Die folgende Abbildung zeigt eine Beispiel-Dashboard-Seite.



Statistische Informationen anzeigen

October 28, 2021

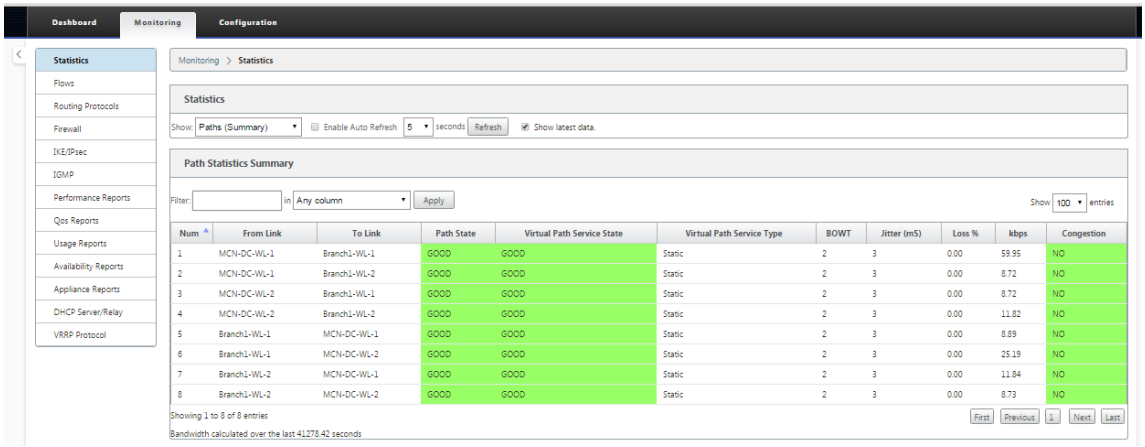
Dieser Abschnitt enthält grundlegende Anweisungen zum Anzeigen von Virtual WAN-Statistikinformationen.

1. Melden Sie sich beim Management Web Interface für den MCN an.

2. Wählen Sie die Registerkarte **Überwachung**.

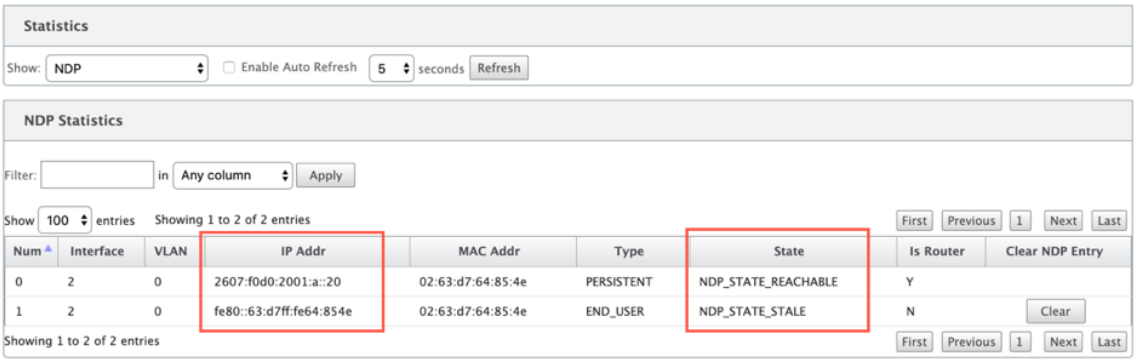
   Dadurch wird der **Monitoring-Navigationsbaum** im linken Bereich geöffnet. Standardmäßig zeigt dies auch die Seite **Statistiken** mit vorausgewählten **Pfaden** im Feld **Anzeigen** an. Dies enthält eine ausführliche Tabelle mit Pfadstatistiken.

   > **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.

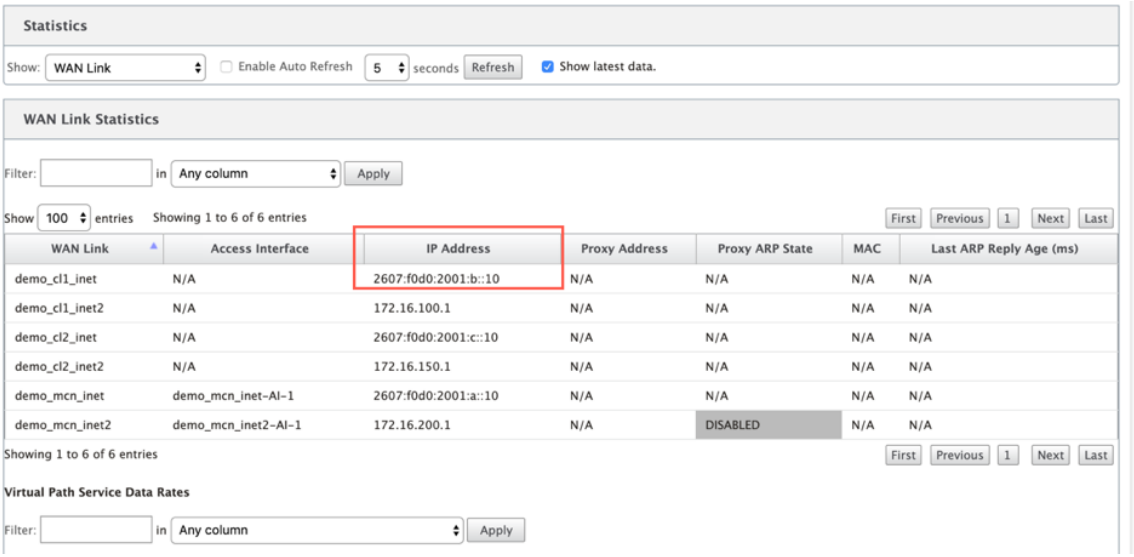


Mit Version 11.1.0 wird die NDP-Option (Neighbor Discovery Protocol) zum Debuggen von Neighbor Discovery-Problemen hinzugefügt.

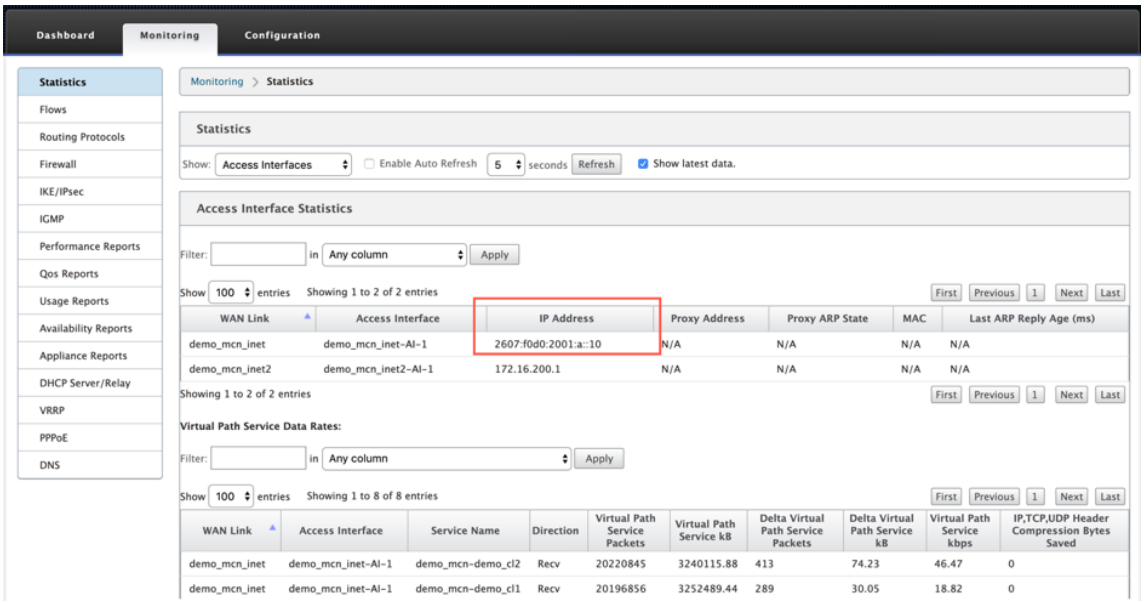
1. Wählen Sie die NDP-Option aus dem Dropdownmenü Anzeigen aus, und Sie können den Status von NDP zusammen mit den IPv6-Adressen anzeigen.



2. Wählen Sie WAN-Link aus dem Dropdownmenü. Sie können die IPv6-Adresse auch anzeigen, wenn Sie auf der Registerkarte IP-Adresse konfiguriert haben.

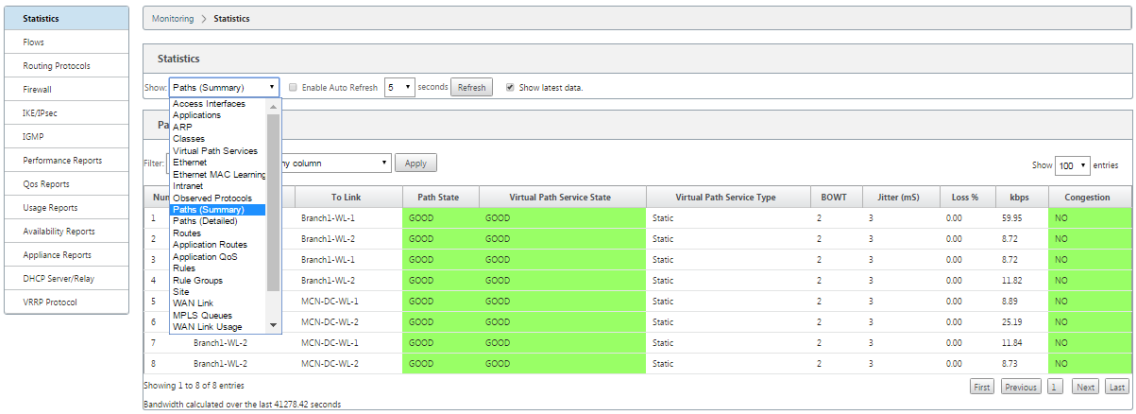


3. Sie können auch die Access Interface-Statistiken anzeigen.



4. Öffnen Sie das Drop-down-Menü **Anzeigen**.

   Neben den **Statistiken**Pfade, NDP, Access Interface**und WAN-Links**bietet das Menü **Anzeigen** auch mehrere weitere Optionen zum Filtern und Anzeigen statistischer Informationen.



Wählen Sie im Menü **Anzeigen** einen Filter aus, um eine Tabelle mit statistischen Informationen für dieses Thema anzuzeigen.

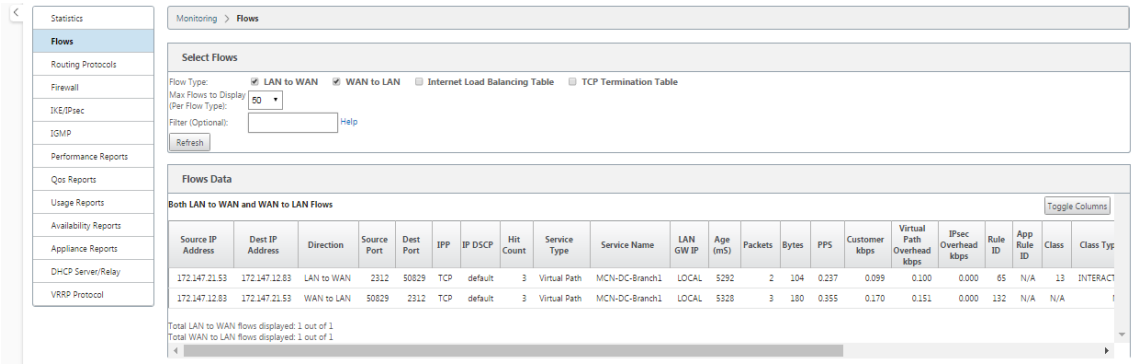
Anzeigen von Flussinformationen

October 28, 2021

Dieser Abschnitt enthält grundlegende Anweisungen zum Anzeigen von Virtual WAN-Flow-Informationen.

Gehen Sie wie folgt vor, um Flow-Informationen 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.

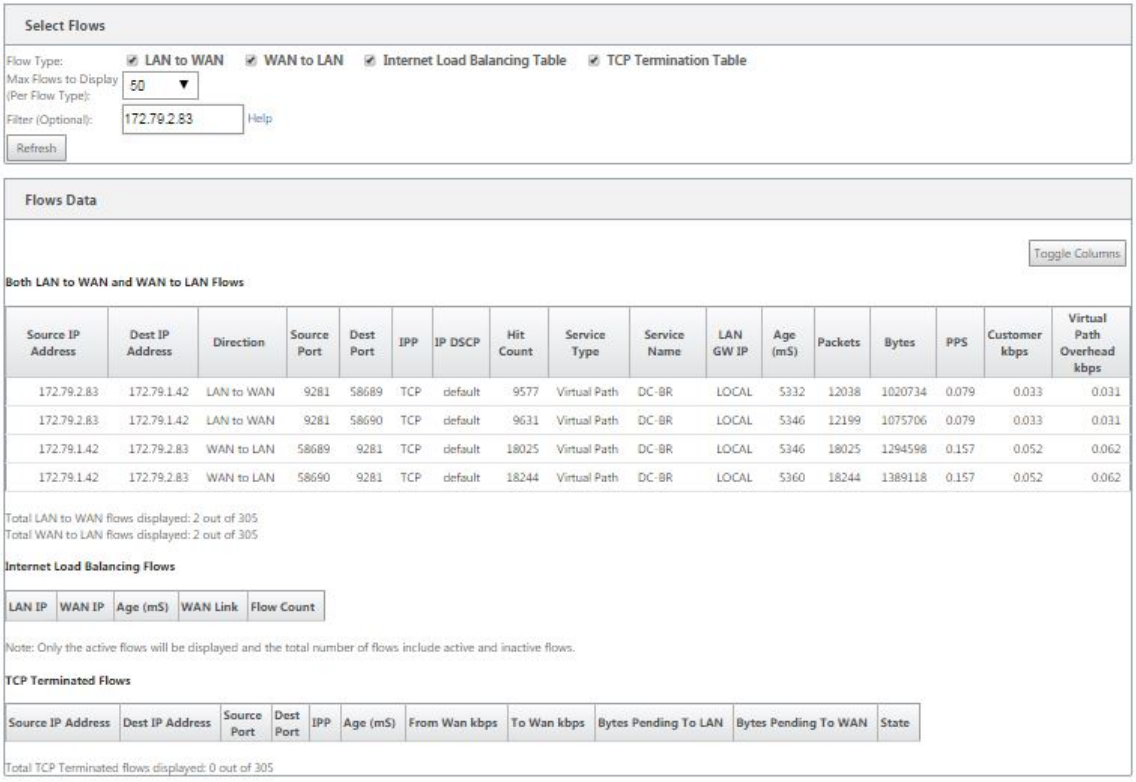


3. Wählen Sie den **Flow-Typ**aus. Das Feld **Flow-Art** befindet sich im Abschnitt **Flows auswählen** oben auf der Seite **Flows**. Neben dem Feld "**Flow-Typ** "befindet sich eine Reihe von Kontrollkästchens zur Auswahl der Flussinformationen, die Sie anzeigen möchten. Sie können ein oder mehrere Kontrollkästchen 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 zur Verfeinerung der Ergebnisse von **Flow-Tabellen** anzuzeigen, klicken Sie rechts neben dem Feld **Filter** auf **Hilfe**. Um die Hilfeanzeige zu schließen, klicken Sie in der unteren linken Ecke des Abschnitts **Flows auswählen** auf **Aktualisieren**.

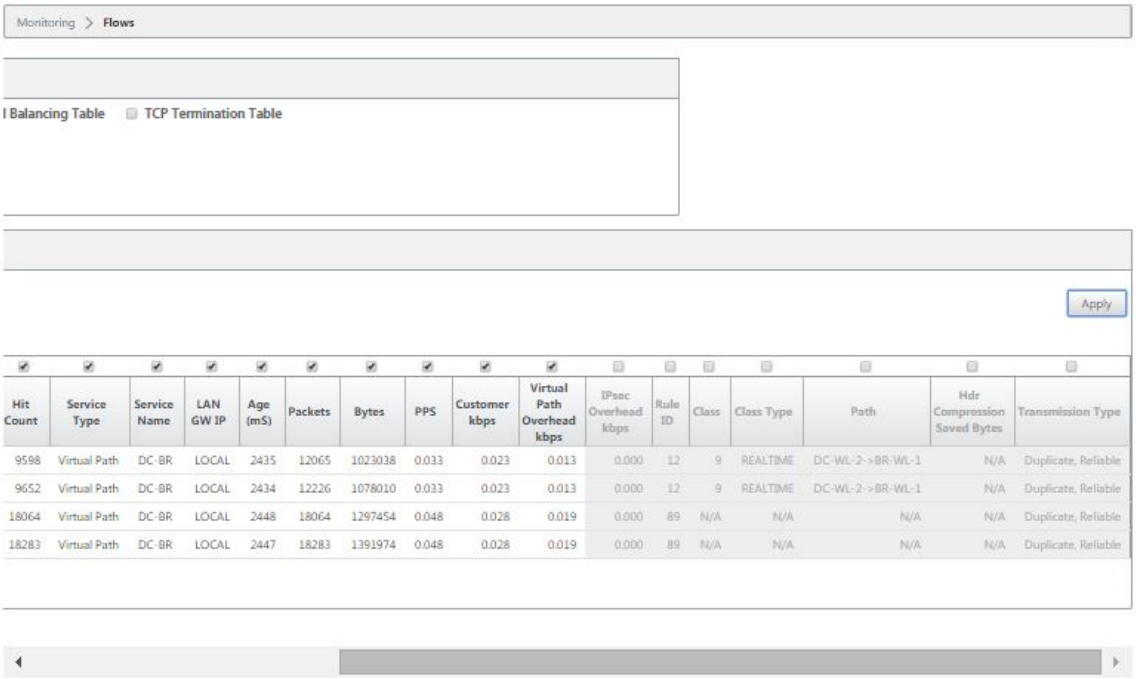
7. Klicken Sie auf **Aktualisieren**, um die Filterergebnisse anzuzeigen. Die Abbildung zeigt eine gefilterte Beispielanzeige der **Flows-Seite** mit allen ausgewählten Flow-Typen.



8. (Optional) Wählen Sie die Spalten aus, die in die Tabelle aufgenommen werden sollen. Führen Sie folgende Schritte aus:
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

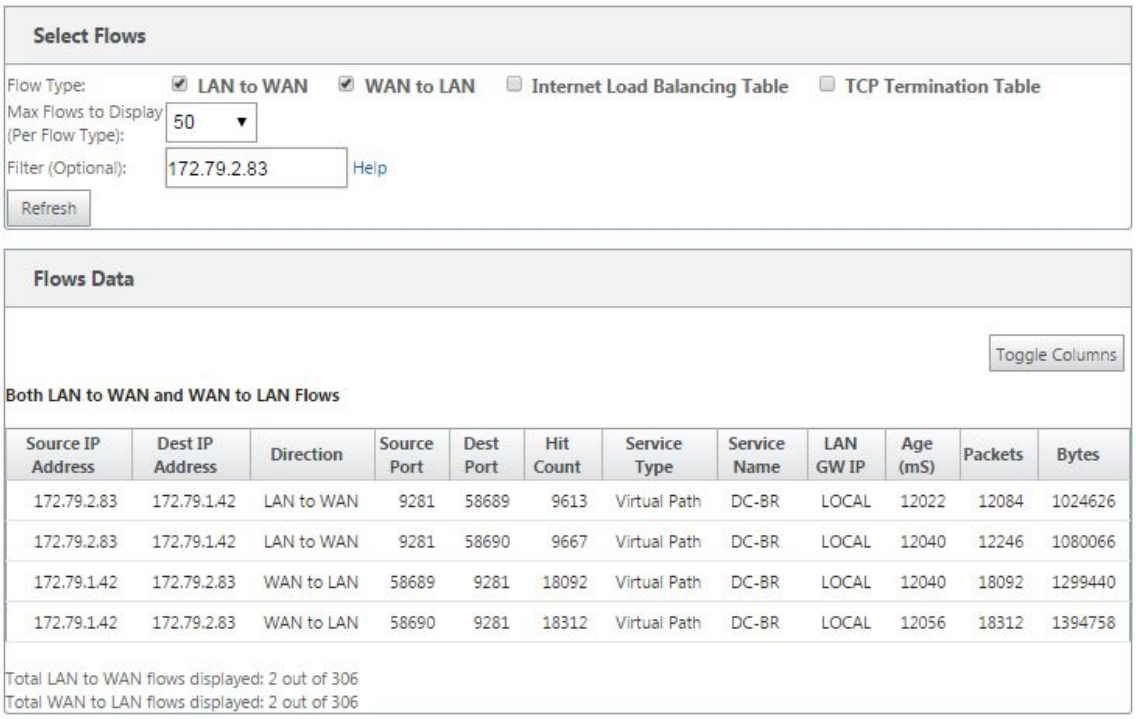
an und öffnet ein Kontrollkästchen über jeder Spalte, um diese Spalte auszuwählen oder zu deaktivieren. Deaktivierte Spalten werden ausgegraut angezeigt, wie in der Abbildung gezeigt.

> **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.



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.



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

DPI-Anwendungen im SD-WAN Center

In früheren Versionen können rund 4.000 Anwendungen identifiziert und mit 800 Diensten (550 virtuelle Pfade, 256 Intranetdienste) konfiguriert werden. 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.

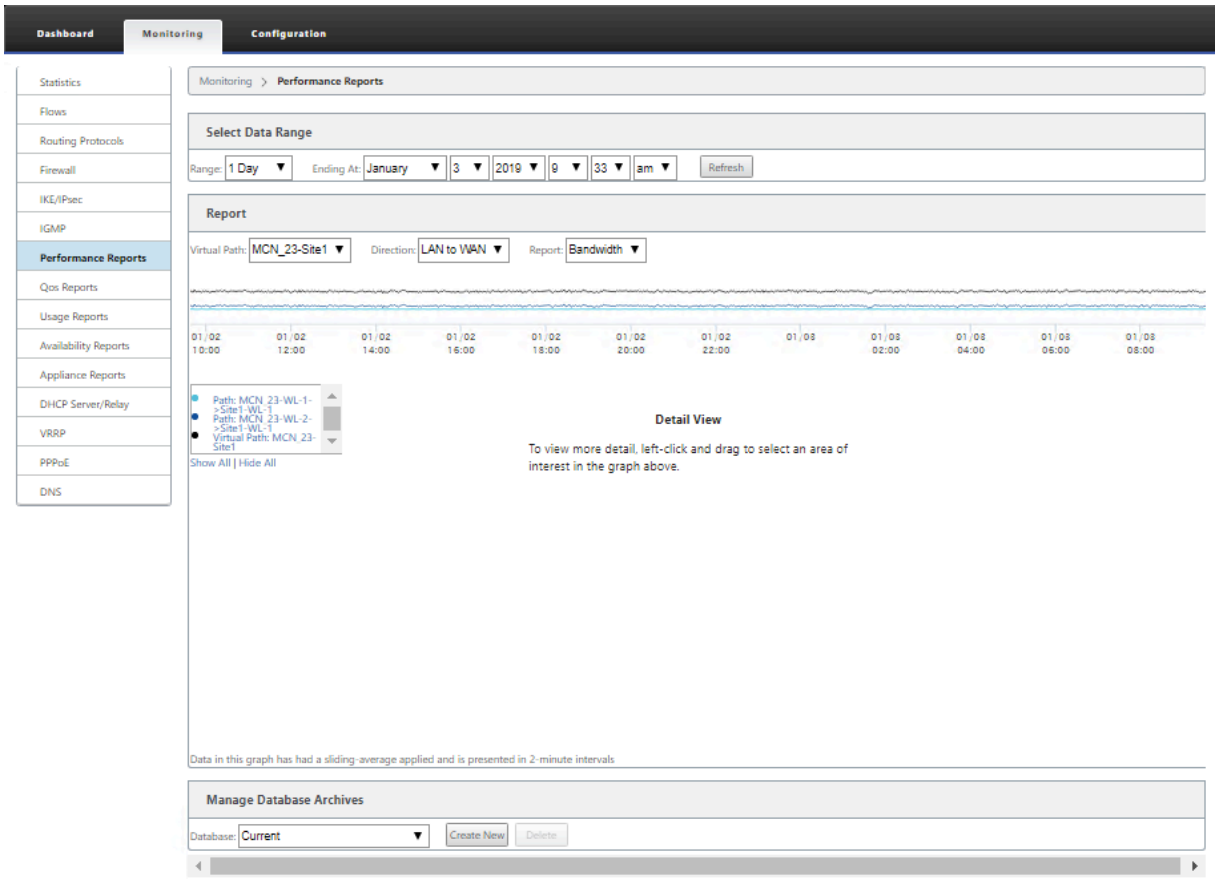
Während der Datenpfad Informationen über jede Anwendung in einer Minute gesammelt, die pro Minute Statistiken Berichterstattung bestimmt die Top 100 Anwendungen und Bericht über das Aggregat aller anderen Anwendungen als andere. Wenn es eine große Vielfalt an verfolgbaren Anwendungen in ihrem Netzwerk 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

October 28, 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**
>
> Auf dem Management-Webinterface generierte Berichte gelten nur für die lokale Appliance. Verwenden Sie das Virtual WAN Center Webinterface, um Berichte für das virtuelle WAN zu erstellen und anzuzeigen.

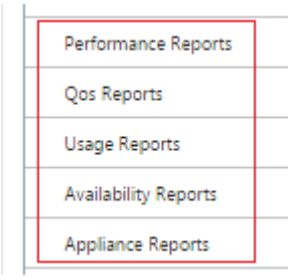
Gehen Sie wie folgt vor, um Virtual WAN-Berichte zu generieren und anzuzeigen:

1. Melden Sie sich am Management-Webinterface für den MCN an und wählen Sie die Registerkarte **Überwachung** aus.

   Dadurch wird der **Monitoring-Navigationsbaum** im linken Bereich 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:

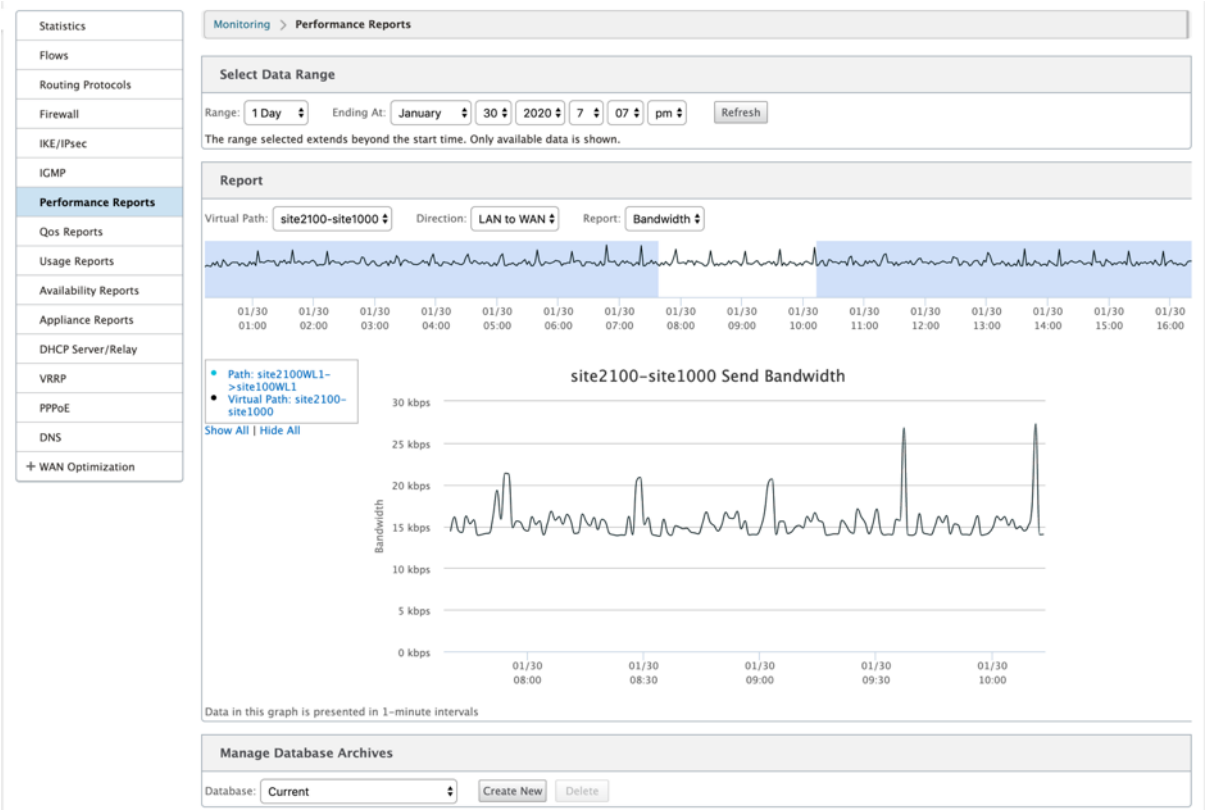
- **Performance-Berichte**
- **QoS-Berichte**
- **Nutzungs-Berichte**
- **Verfügbarkeitsberichte**
- **Appliance-Berichte**

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.

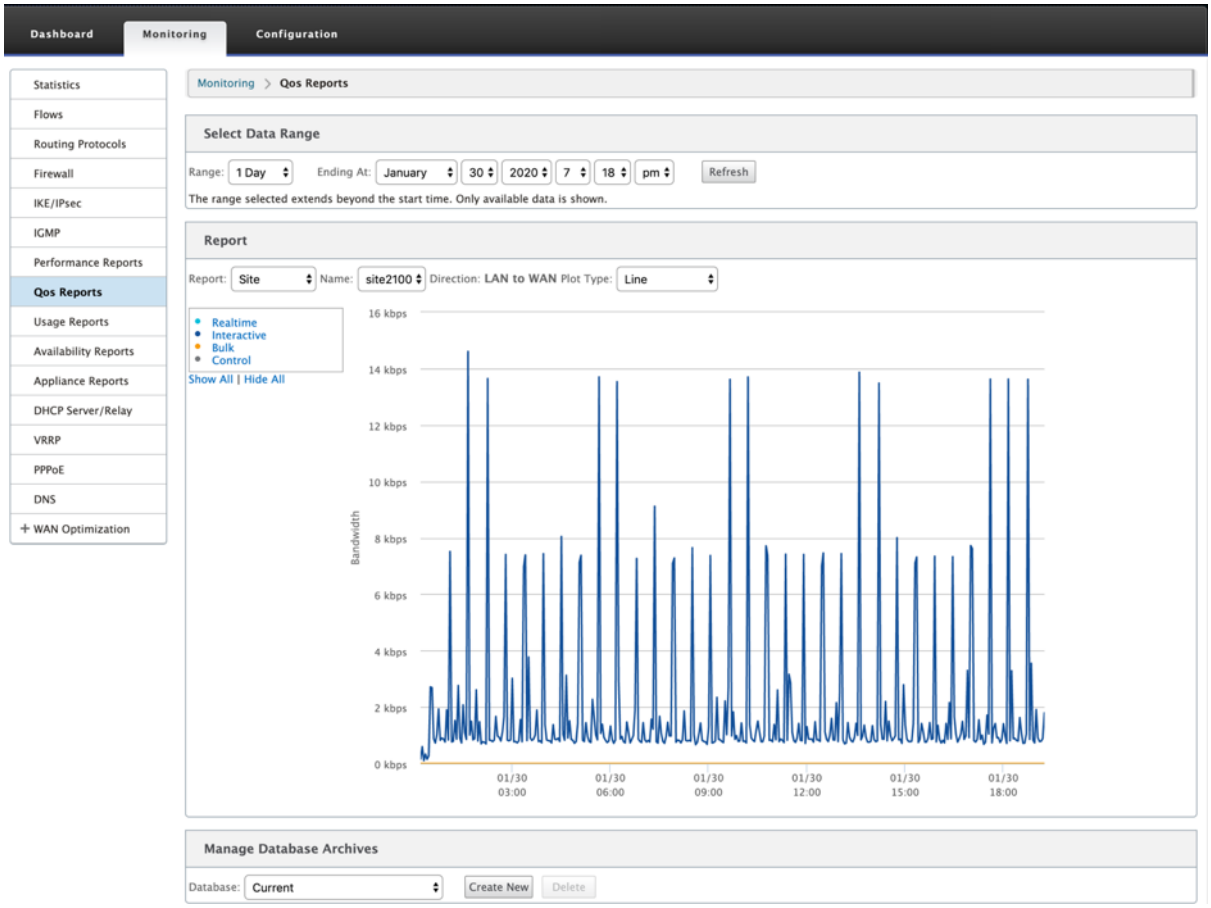


Sie können den Datenbereich nach Bedarf mit den folgenden Feldern auswählen, um den Leistungsbericht anzuzeigen:

- **Virtueller Pfad:** Wählen Sie den virtuellen Pfad aus der Dropdownliste 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.

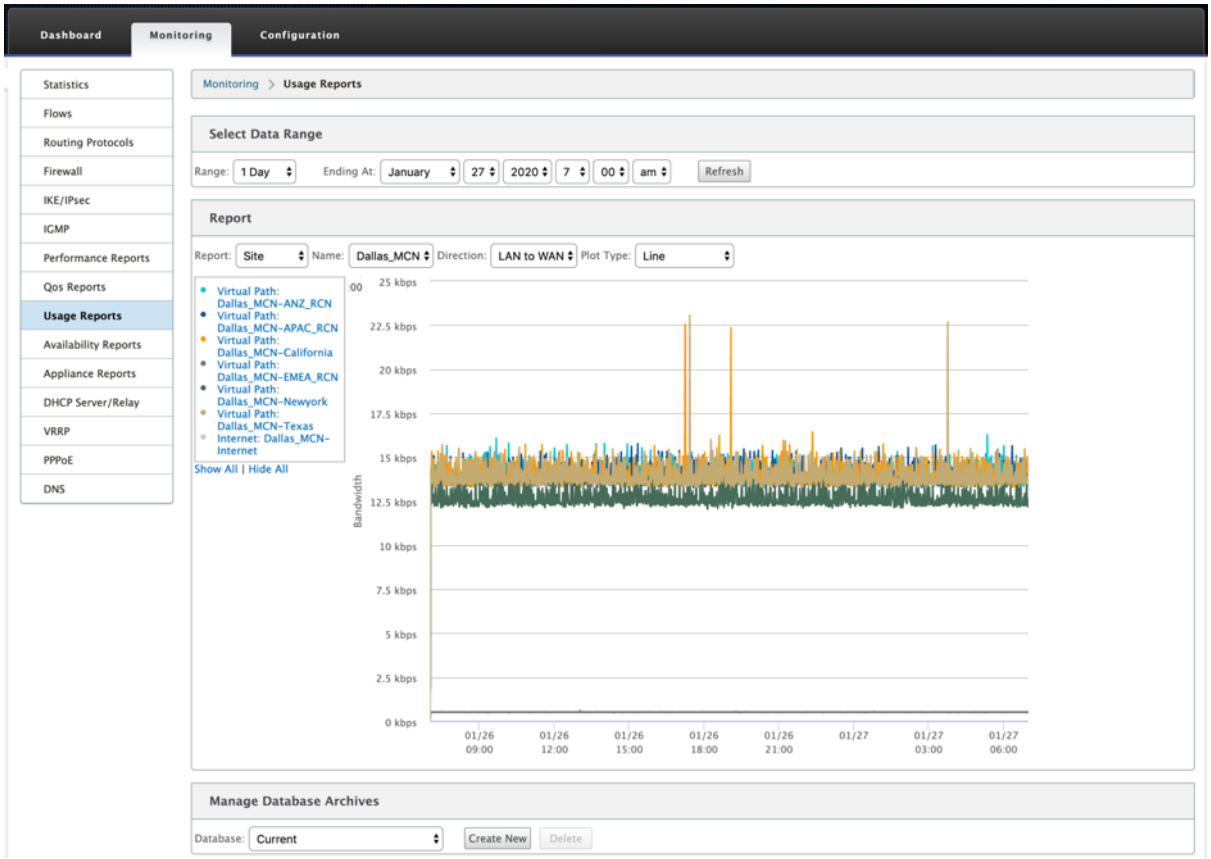


Sie können die folgenden Metriken anzeigen:

- **Echtzeit:** Bandbreite, die von Anwendungen verbraucht wird, die zum Echtzeit-Klassentyp in der Citrix SD-WAN-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-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-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

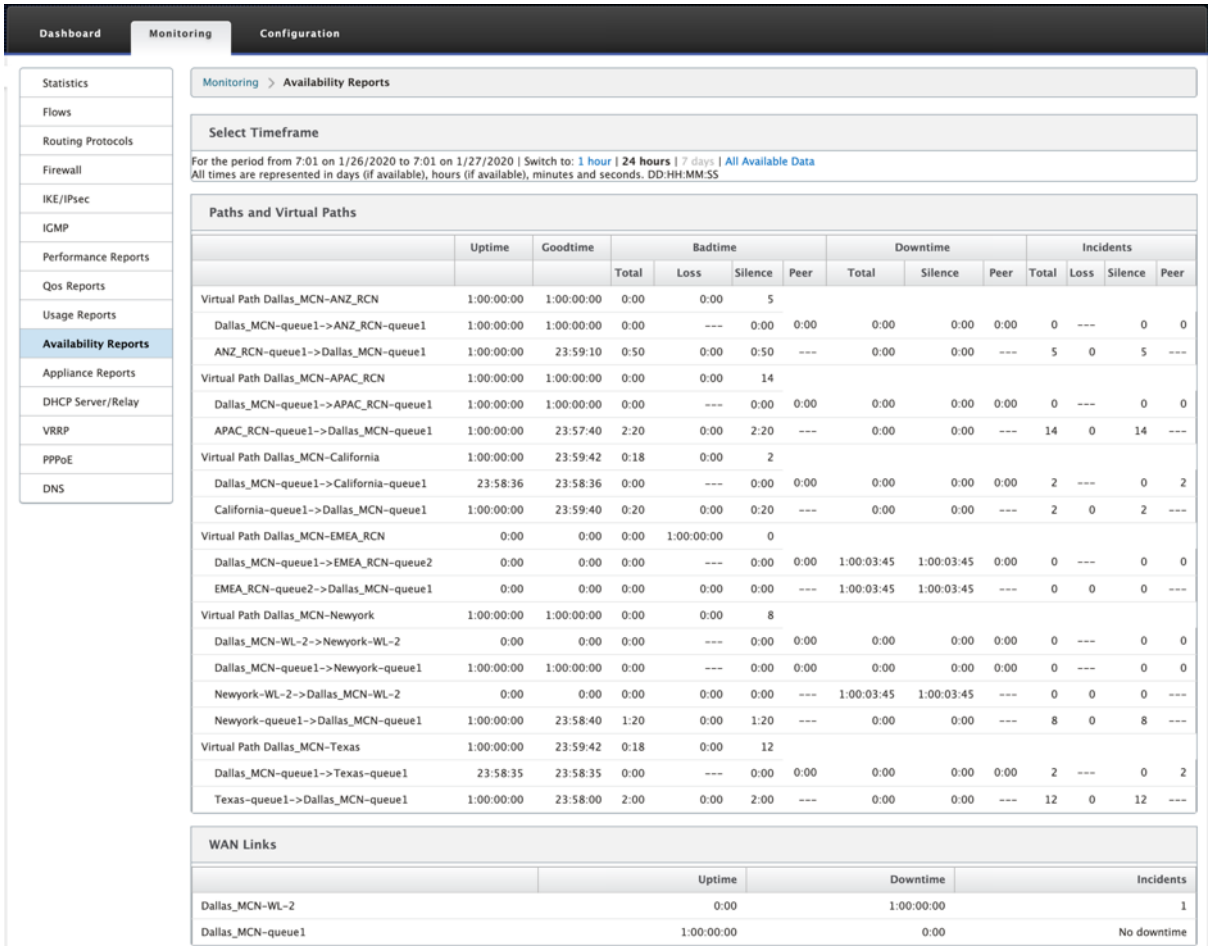
Die Verwendungsberichte liefern die Informationen zur Verwendung virtueller Pfade.



- **Bericht:** Wählen Sie **Site** oder **WAN-Link** aus der Dropdownliste aus, um den Bericht anzuzeigen.
- **Name:** Wählen Sie den Namen der Site oder des WAN-Link aus der Dropdownliste aus.
- **Richtung:** Wählen Sie die Richtung nach Bedarf aus (LAN zu WAN oder WAN to LAN).
- **Plottyp:** Wählen Sie den Plottyp aus der Dropdownliste (Linie oder Fläche) aus.

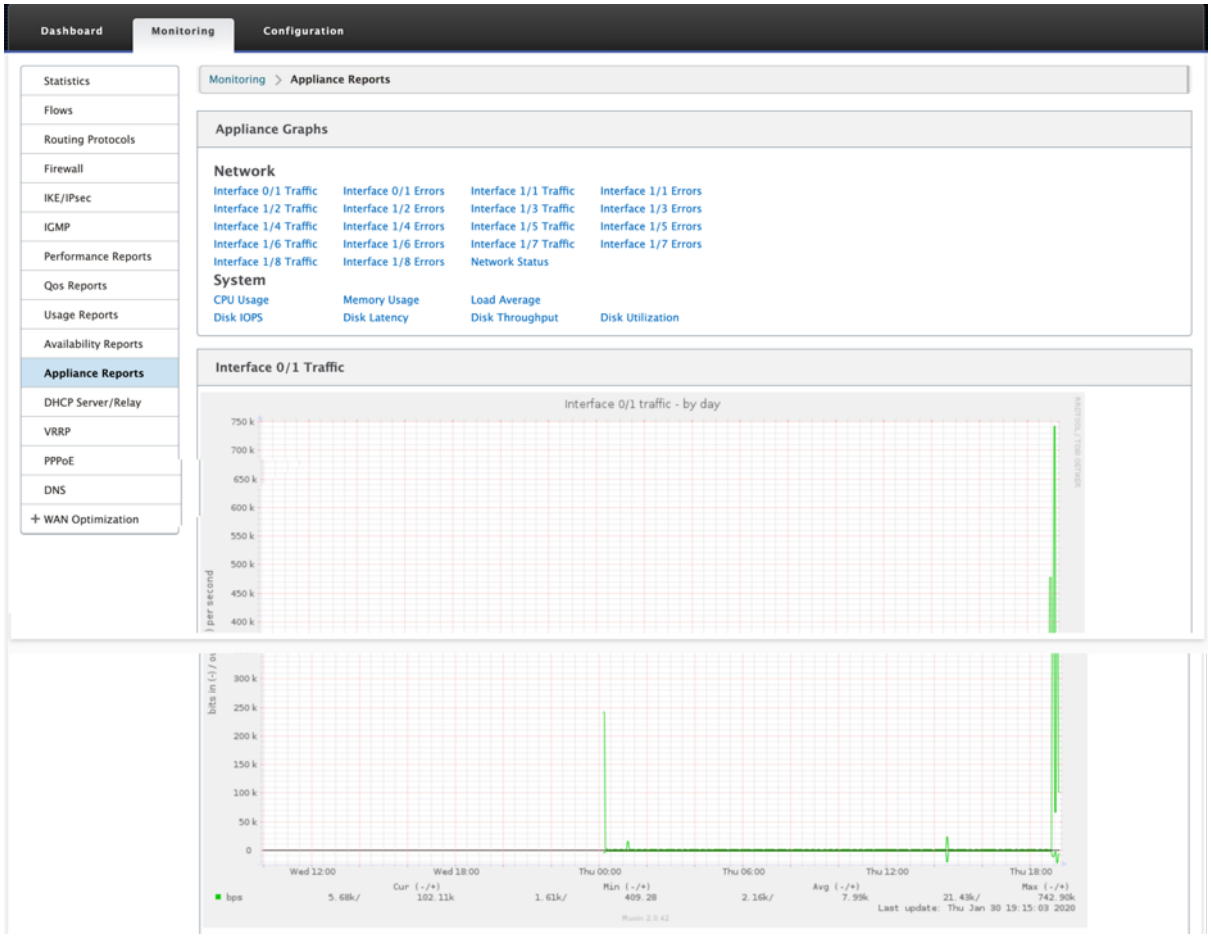
Verfügbarkeitsberichte

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.



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

October 28, 2021

Sobald 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.

Informationen zur Konfiguration von Firewall- und NAT-Richtlinien finden Sie unter Stateful Firewall und NAT-Support.

Verbindungen

Sie können die Statistiken für Anwendungen für die Firewall-Richtlinie überprüfen. Auf diese Weise können Sie alle Verbindungen sehen, die mit der ausgewählten Anwendung übereinstimmen, woher

sie kommen, wohin sie gehen und wie viel Traffic sie erzeugen. Sie können sehen, wie die Firewall-Richtlinien auf den Datenverkehr für jede Anwendung wirken.

Sie können die Verbindungsstatistiken mithilfe der folgenden Parameter filtern:

- Anwendung - Die Anwendung, die als Filterkriterium für die Verbindung verwendet wird.
- Familie —Die Anwendungsfamilie, die als Filterkriterium 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, aus der der antwortende Verkehr stammt.
- Quelldiensttyp - Der Dienst, von dem die Verbindung stammt.
- Source Service Instance - 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 Port-Bereich, von dem die Verbindung stammt. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Zieldiensttyp - Der Dienst, von dem der antwortende Verkehr stammt.
- Destination Service Instance - Die Instanz des Dienstes, von der der antwortende Datenverkehr stammt.
- Ziel-IP - Die IP-Adresse des antwortenden Geräts, Eingabe in punktierter Dezimalnotation mit optionaler Subnetzmaske.
- Zielport - Der Port oder Port-Bereich, der vom antwortenden Gerät verwendet wird. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.

Richtlinien filtern

Mithilfe von Richtlinien können Sie Aktionen für Verkehrsflüsse festlegen. Gruppe von Firewallfiltern werden mithilfe von Firewall-Richtlinienvorlagen erstellt und können auf alle Sites im Netzwerk oder nur auf bestimmte Sites angewendet werden.

Sie können den Statistikbericht für alle Filterrichtlinien anzeigen und mithilfe der folgenden Parameter filtern.

- Anwendungsobjekt - Das in der Firewall-Richtlinie als Filterkriterium verwendete Application-Objekt.
- Anwendung - Die Anwendung, die als Filterkriterien in der Firewall-Richtlinie verwendet wird
- Familie —Die Anwendungsfamilie, die als Filterkriterium in der Firewall-Richtlinie verwendet wird.
- IP-Protokoll - Das IP-Protokoll, mit dem die Filterrichtlinie übereinstimmt.
- DSCP: Das DSCP-Tag, mit dem die Filterrichtlinie übereinstimmt.
- 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 Port-Bereich, von dem die Verbindung stammt. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Zieldiensttyp - Der Dienst, für den der antwortende Verkehr bestimmt ist.
- Name des Zieldienstes - Falls zutreffend, der Dienst, für den der antwortende Verkehr bestimmt ist.
- Ziel-IP - Die IP-Adresse des antwortenden Geräts, Eingabe in punktierter Dezimalnotation mit optionaler Subnetzmaske.
- Zielport - Der Port oder Port-Bereich, der vom antwortenden Gerät verwendet wird. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Quellzone —Die mit der Filterrichtlinie übereinstimmende Ursprungszone.
- Zielzone —Die antwortende Zone, die mit der Filterrichtlinie übereinstimmt.

NAT-Richtlinien

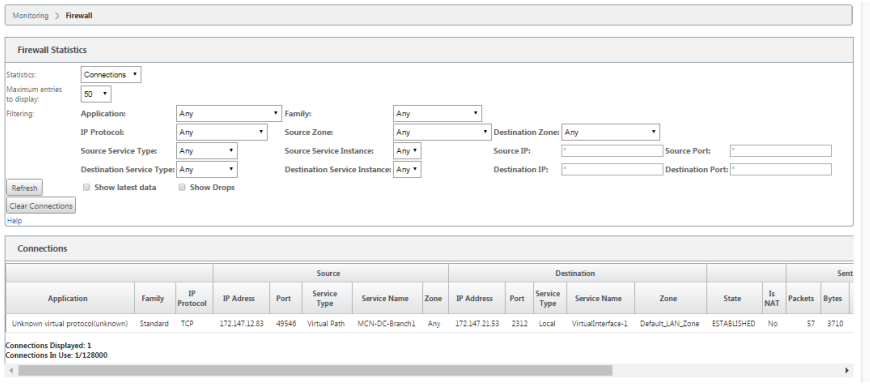
Sie können die Statistiken aller Richtlinien für die Netzwerkadressübersetzung (NAT) anzeigen und den Bericht mithilfe der folgenden Parameter filtern.

- 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 des dynamischen NAT, der von der NAT-Richtlinie verwendet wird.
- Servicetyp —Der von der NAT-Richtlinie verwendete Diensttyp.
- Dienstname —Die Instanz des von der NAT-Richtlinie verwendeten Dienstes.
- Innen-IP - Die innere IP-Adresse, die in gepunkteter Dezimalschreibweise mit einer optionalen Subnetzmaske eingegeben wird.
- Inside Port- Der von der NAT-Richtlinie verwendete innere Portbereich. Ein einzelner Port oder ein Bereich von Ports mit dem Zeichen - wird akzeptiert.
- Außen-IP - Die äußere IP-Adresse, die in gepunkteter Dezimalschreibweise mit einer optionalen Subnetzmaske eingegeben wird.
- Außenport - 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 **Monitoring** > **Firewall.**
2. Wählen Sie im Feld Statistik je nach Bedarf **Verbindungen**, **Filterrichtlinien oder NAT-Richtlinien** aus.

3. Legen Sie die Filterkriterien nach Bedarf fest.



4. Klicken Sie auf **Aktualisieren**.

Diagnose

February 7, 2022

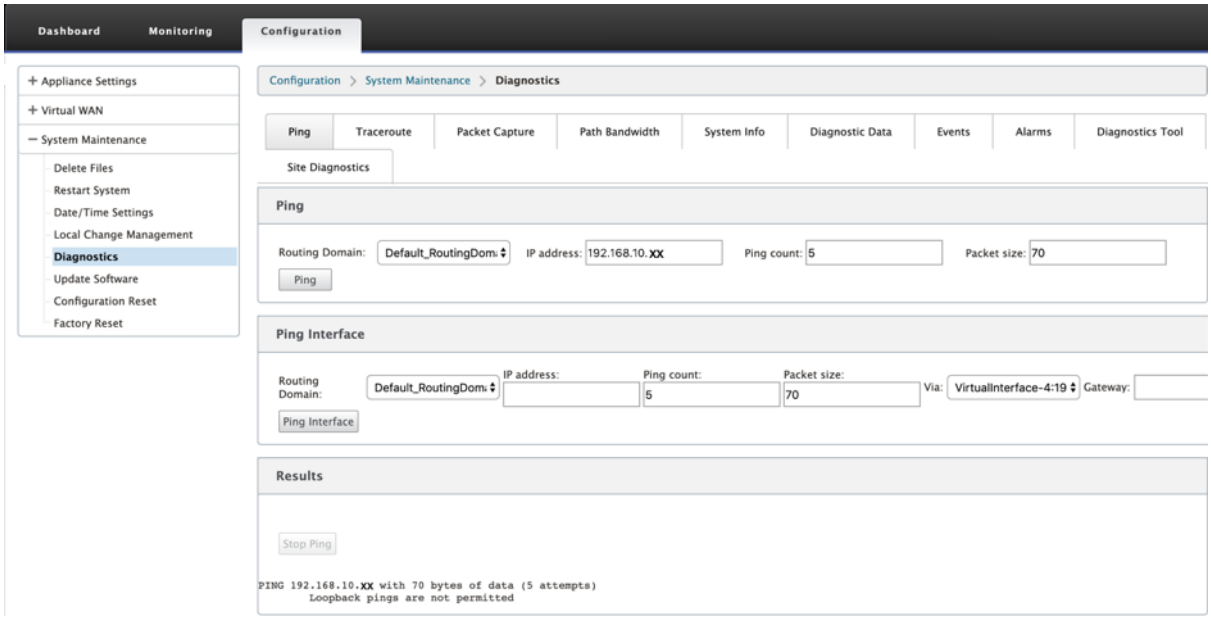
Citrix SD-WAN Diagnostics-Dienstprogramme bieten die folgenden Optionen zum Testen und Untersuchen von Konnektivitätsproblemen:

- 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.

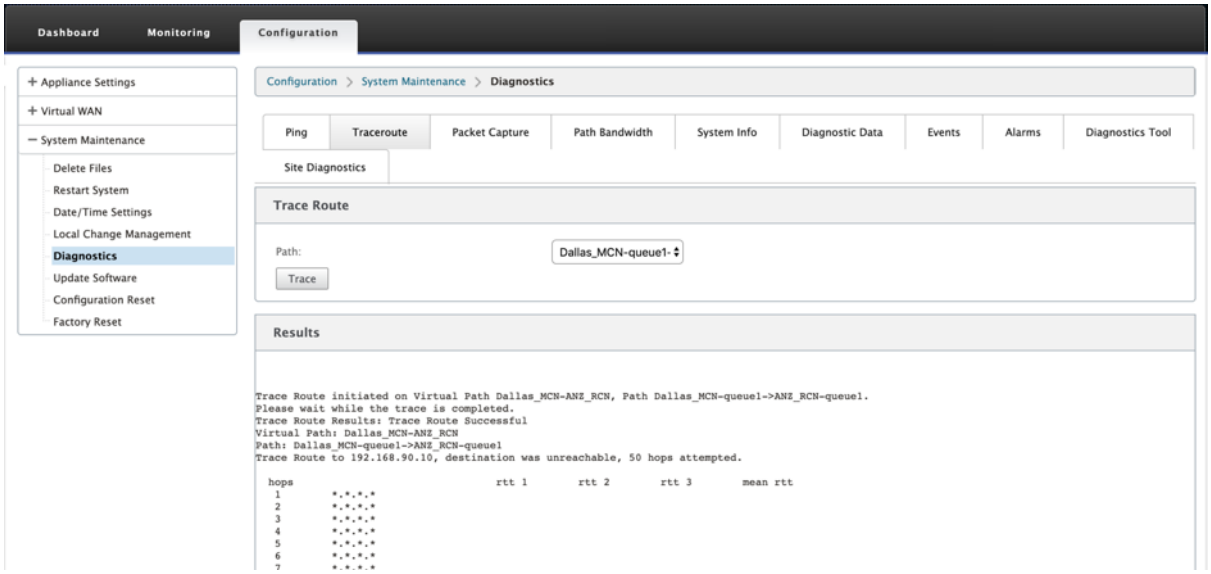


Wählen Sie die Routing-Domäne aus. Geben Sie eine gültige IP-Adresse, die Anzahl der Ping-Zähler (Anzahl der Ping-Anfragen zu senden) und die Paketgröße (Anzahl der Datenbytes) an. Klicken Sie auf **Ping stoppen**, um eine laufende Ping-Suche

Sie können über eine bestimmte Oberfläche pingen. Wählen Sie die Routingdomäne aus und geben Sie die IP-Adresse mit Ping-Anzahl, Paketgröße an, und wählen Sie die virtuelle Schnittstelle aus der Dropdownliste aus.

Traceroute

Um die Option **Traceroute** zu verwenden, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Traceroute**aus.

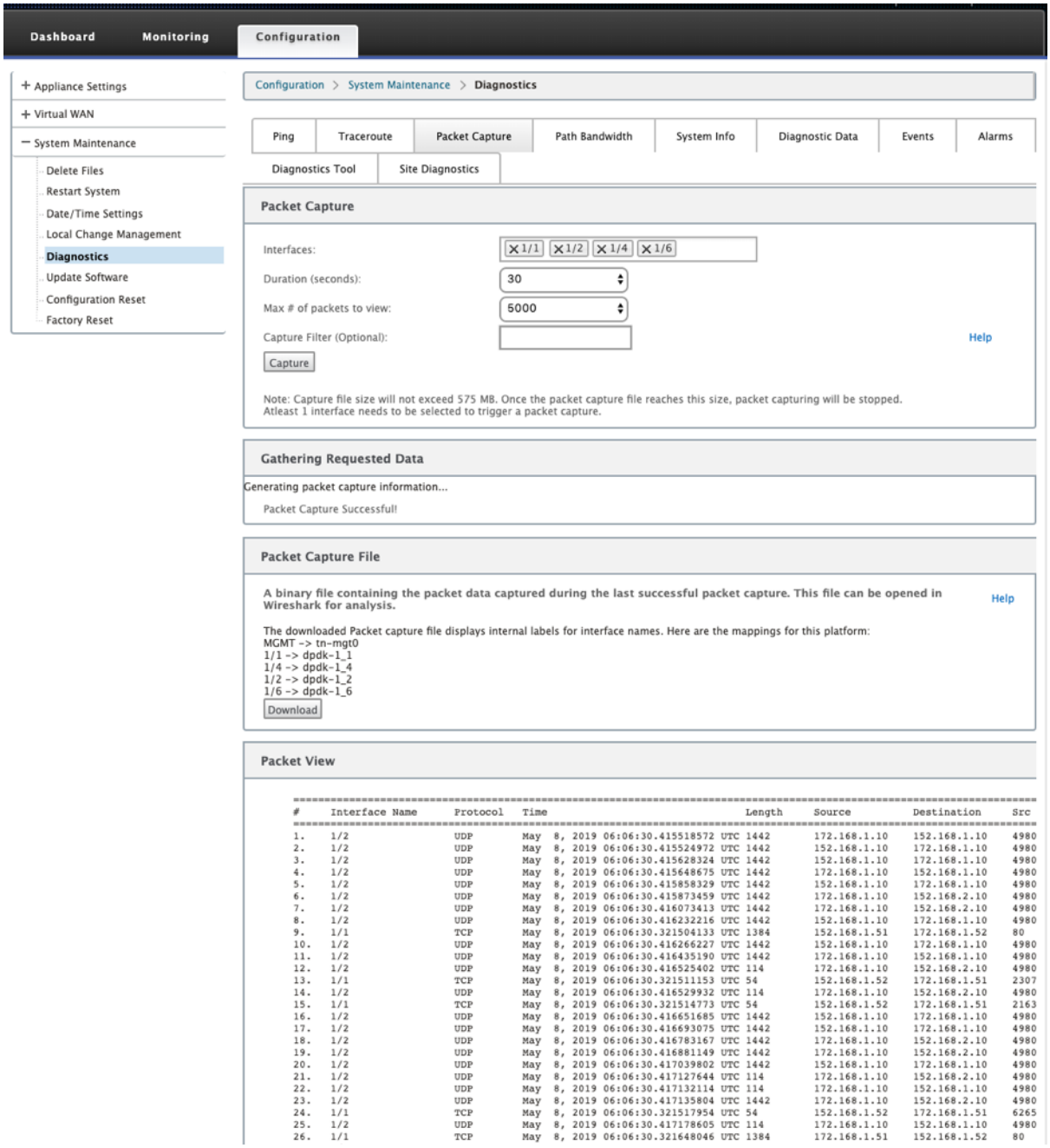


Traceroute hilft dabei, den Pfad oder die Route zu einem Remoteserver zu erkennen und anzuzeigen. Verwenden Sie die Option **Traceroute** als Debugging-Tool, um die Fehlerpunkte in einem Netzwerk zu erkennen.

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.



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 Dropdown-liste 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.

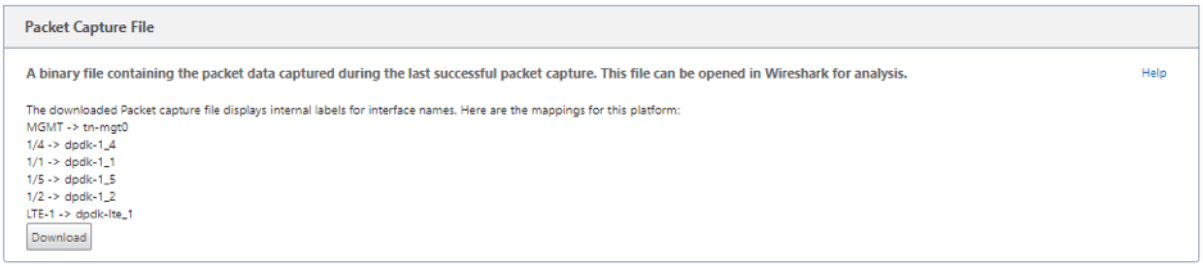
Sammeln angeforderter Daten

In dieser Tabelle sehen Sie den Status der Generierung von Paketerfassungsinformationen (ob die Paketerfassung erfolgreich ist oder keine Paketerfassung ist).

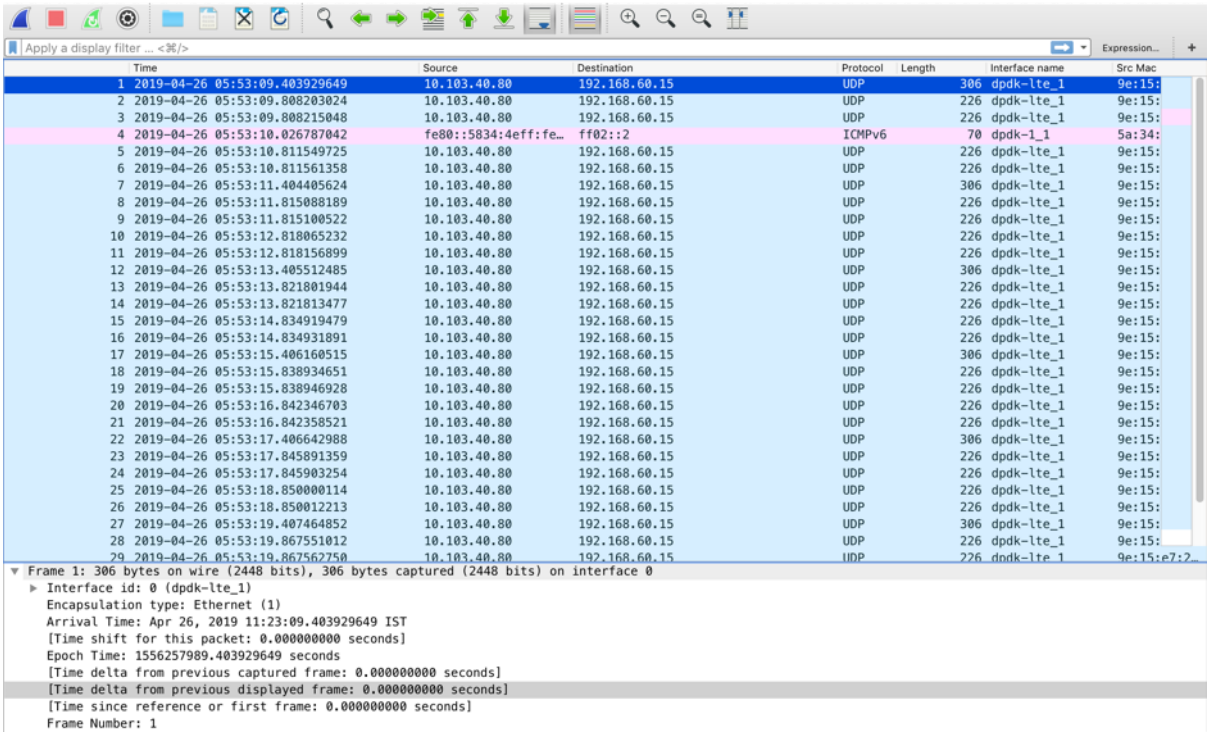
Paket-Capture-Datei

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.



Sie benötigen **Wireshark** Software 2.4.13 Version oder höher, um die Binärdatei zu öffnen und zu lesen.

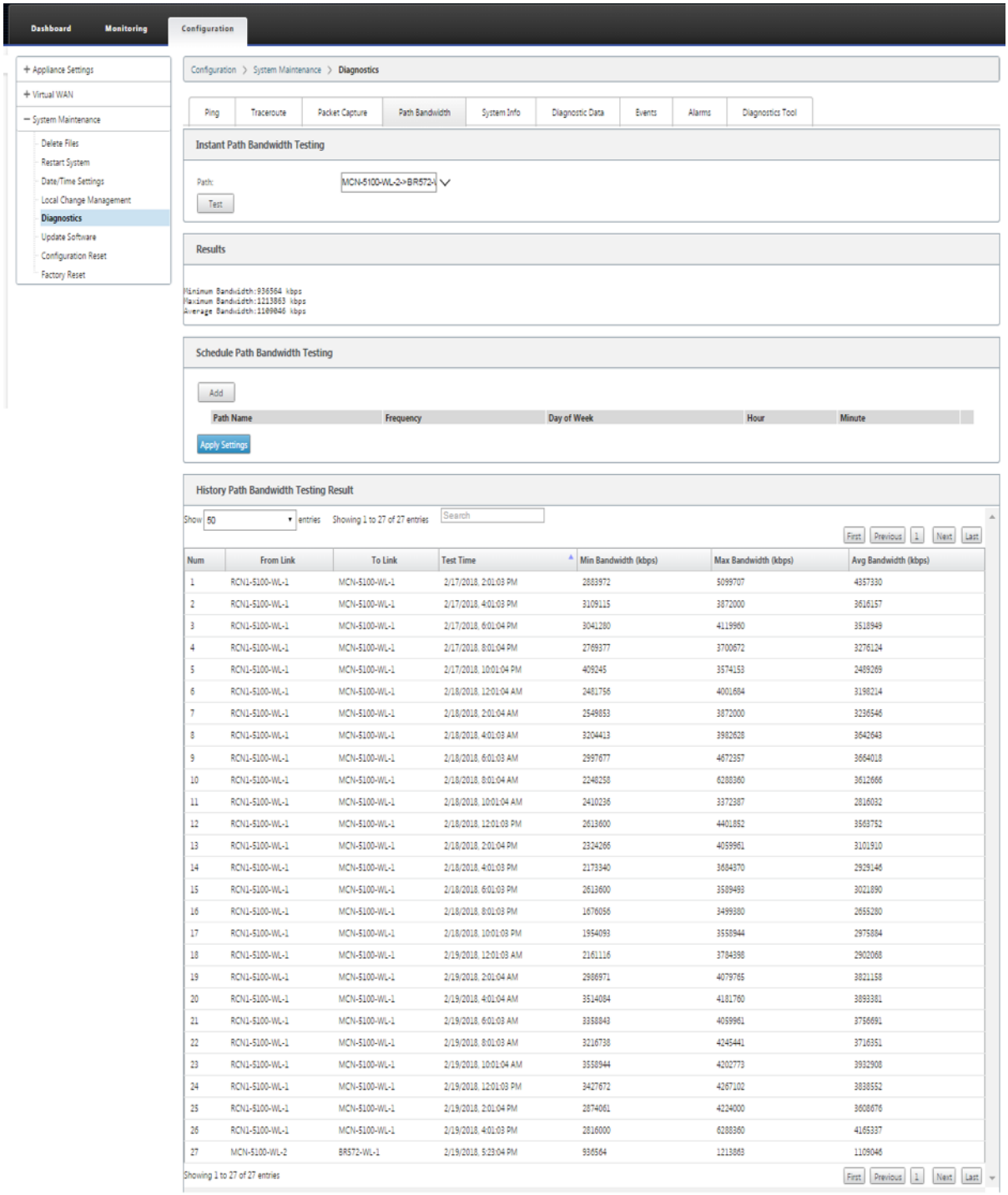


Paket-Ansicht

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 **Wireshark** 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.



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.

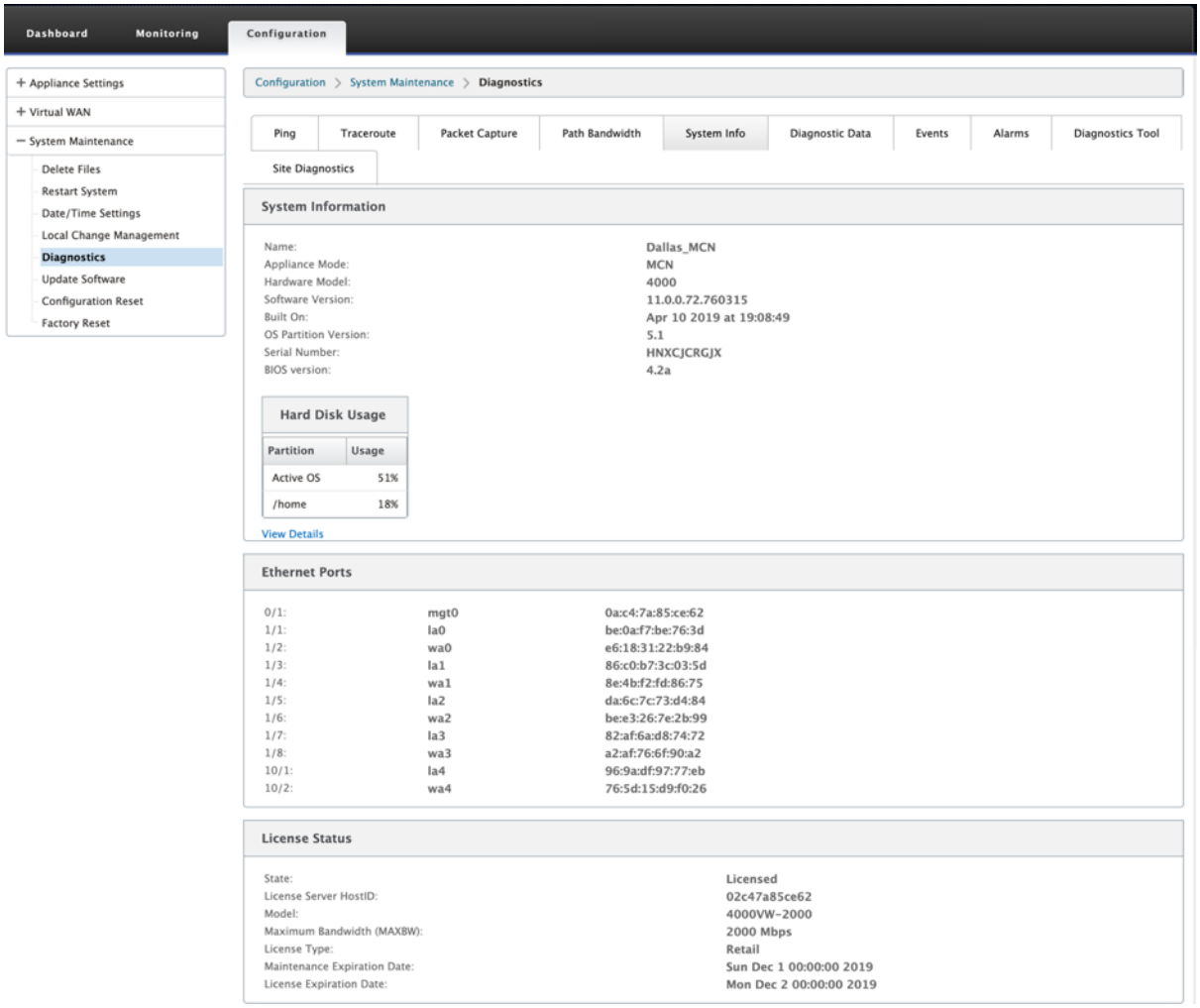
Die **Pfadbandbreitenfunktion** ist nützlich, um zu demonstrieren, wie viel Bandbreite zwischen zwei Standorten während neuer und vorhandener Installationen verfügbar ist. Die Werte aus der Pfad-

bandbreite geben die maximale Bandbreite an. Um eine genaue zulässige Bandbreite zu erhalten, navigieren Sie zu **Konfiguration** > **Systemwartung** > **Diagnose** > **Standortdiagnose** > **Bandbreitentest**. 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**.

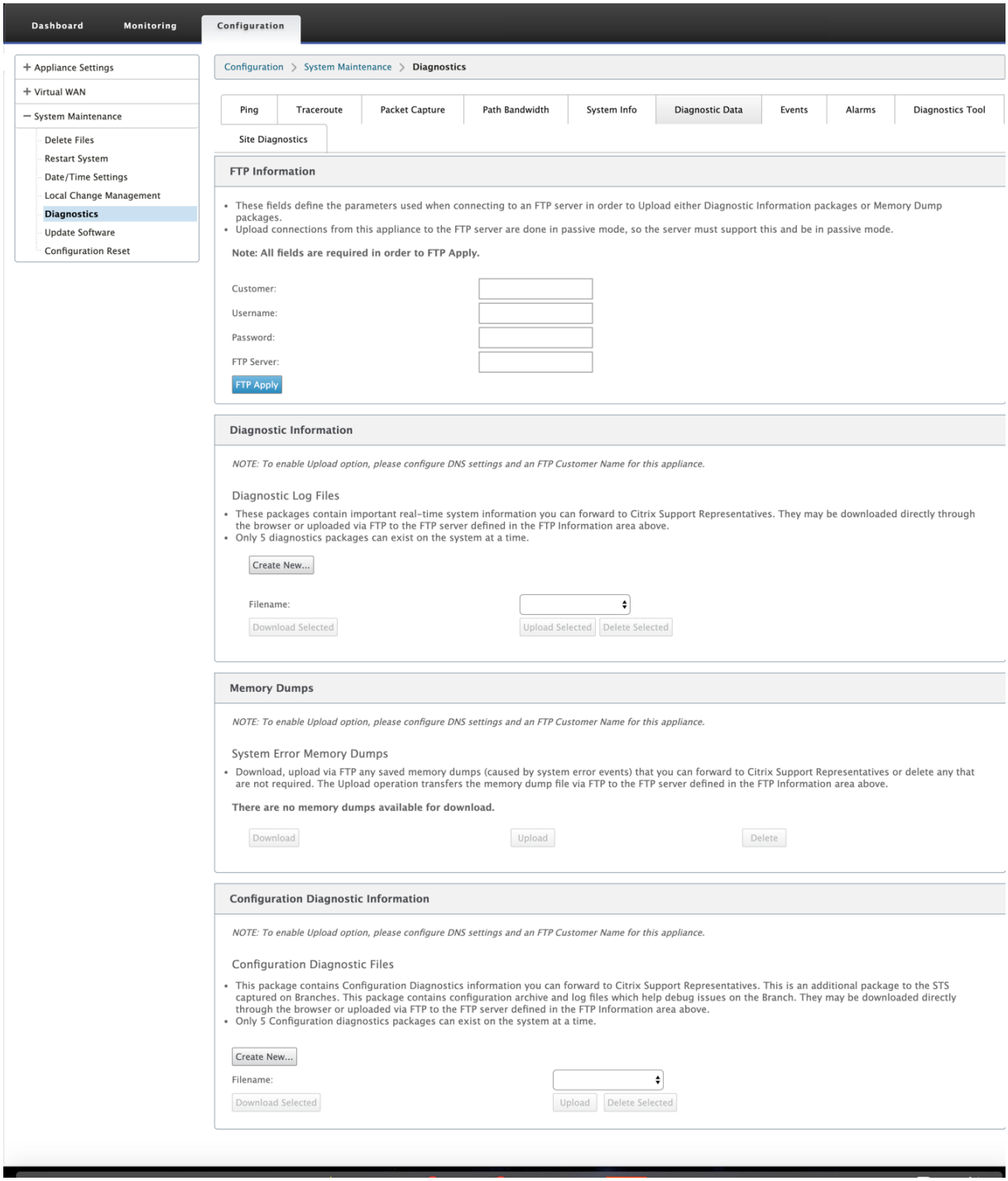


In den **Systeminformationen** werden alle Parameter aufgeführt, die nicht auf ihre Standardwerte eingestellt sind. Diese Informationen sind schreibgeschützt. Es wird vom Support verwendet, wenn eine Art von Fehlkonfiguration vermutet wird. Wenn Sie ein Problem melden, werden Sie möglicherweise aufgefordert, einen oder mehrere Werte auf dieser Seite zu überprüfen.

Diagnosedaten

Mit**Diagnosedaten** können Sie ein Diagnosedatenpaket zur Analyse durch das Citrix Support-Team erstellen. Sie können das **Diagnostics Log Files** Paket herunterladen und für das Citrix Support-Team freigeben.

Um die **Diagnosedaten**anzuzeigen, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Diagnosedaten**.



Die **Diagnosedaten** beinhalten:

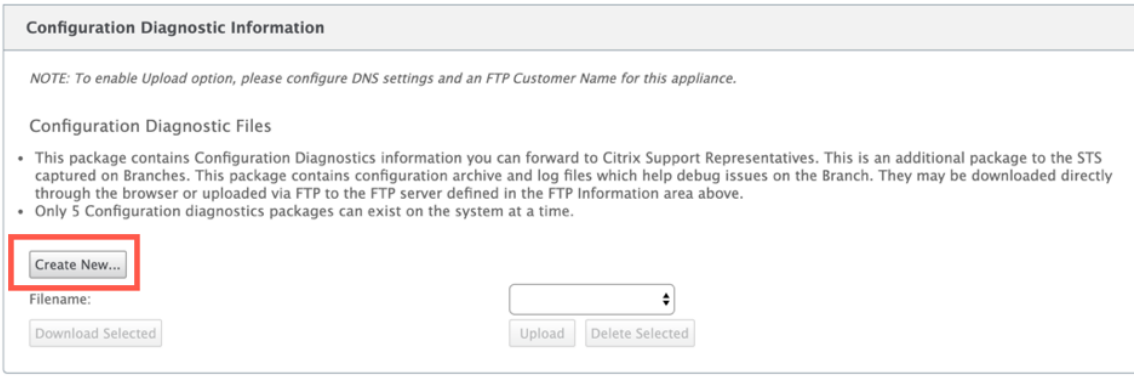
- **FTP-Informationen** —Geben Sie die Details der FTP-Parameter an und klicken Sie auf **FTP Übernehmen**. Die FTP-Informationen, die erforderlich sind, um einen FTP-Server anzuschließen, um ein Diagnoseinformation hochzuladen.
- **Diagnoseinformationen** —Das Diagnoseprotokolldateipaket enthält Systeminformationen 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 der Verzweigung und die Konfigurationsdiagnoseinformationen von dem 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.

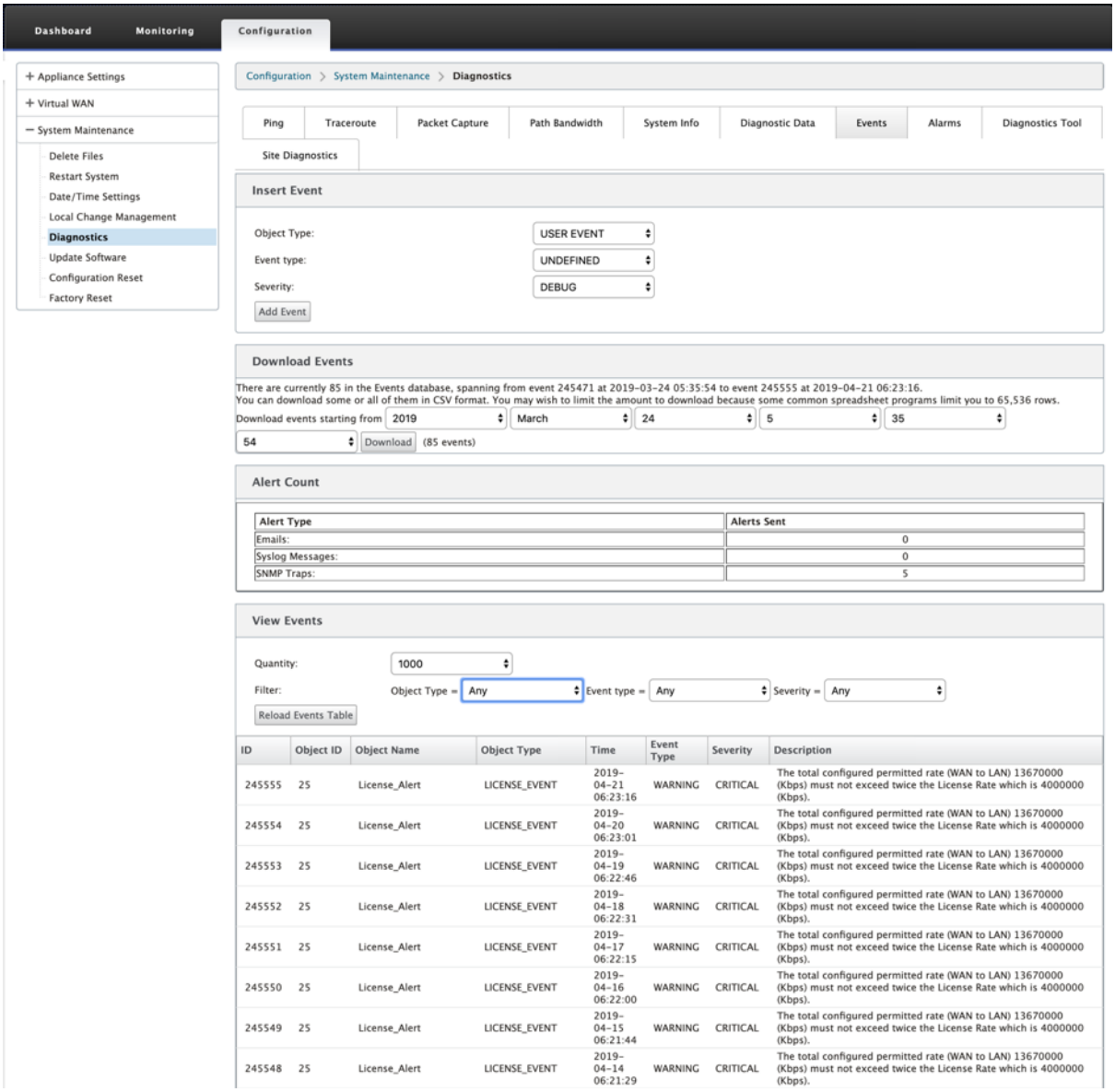
> **HINWEIS:**
>
> Standardmäßig befindet sich die Option **Hochladen** im deaktivierten Modus. Um es zu aktivieren, konfigurieren Sie **DNS-Einstellungen** und einen **FTP-Kundennamen** für diese Appliance.

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 Dropdownliste aus und klicken Sie auf **Ereignis hinzufügen**.

Um **Ereignisse** anzuzeigen, navigieren Sie zu **Konfiguration** erweitern Sie **Systemwartung > Diagnose** und wählen Sie **Ereignisse** aus.



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.

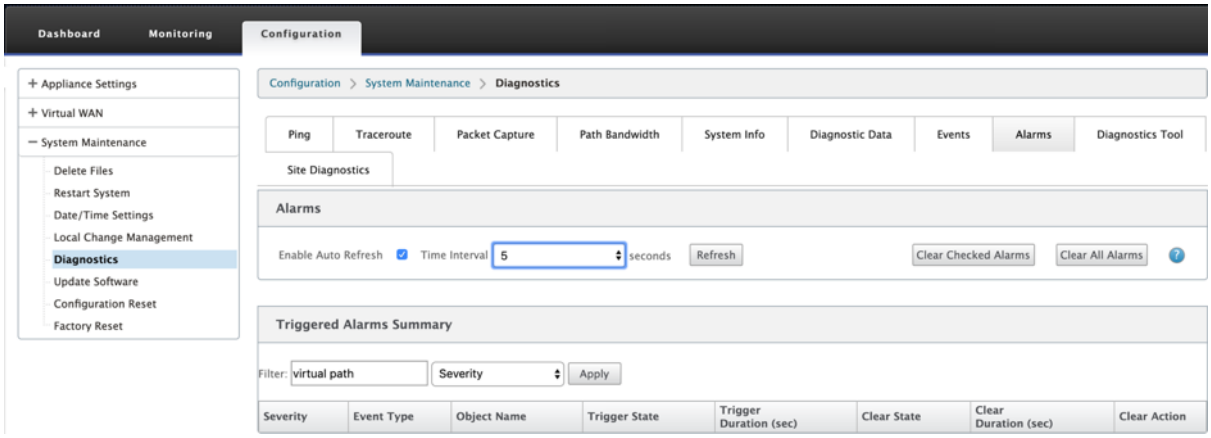
Benachrichtigungen werden für Ereignisse generiert, die dem angegebenen Schweregrad für den Ereignistyp entsprechen oder darüber liegen.

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 Alarmelöschen 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:

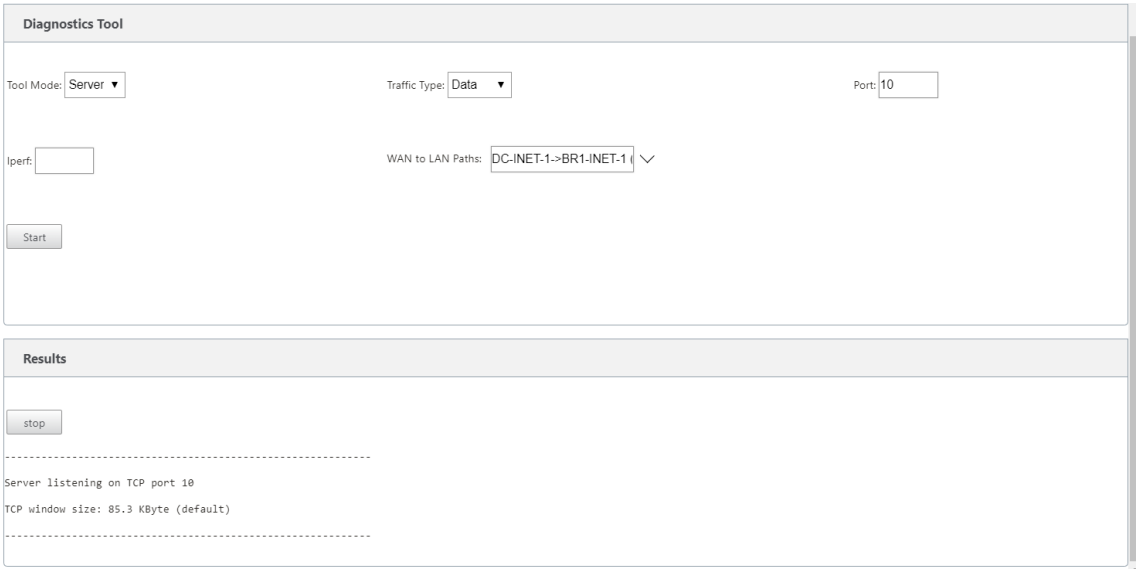
- **Steuerung**: Generiert Traffic ohne QoS/Scheduling auf die Pakete angewendet. Infolgedessen werden die Pakete über den in der Benutzeroberfläche ausgewählten Pfad gesendet, auch wenn der Pfad zu diesem Zeitpunkt nicht der beste ist. Dieser Verkehr wird verwendet, um bestimmte Pfade zu testen und 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**.



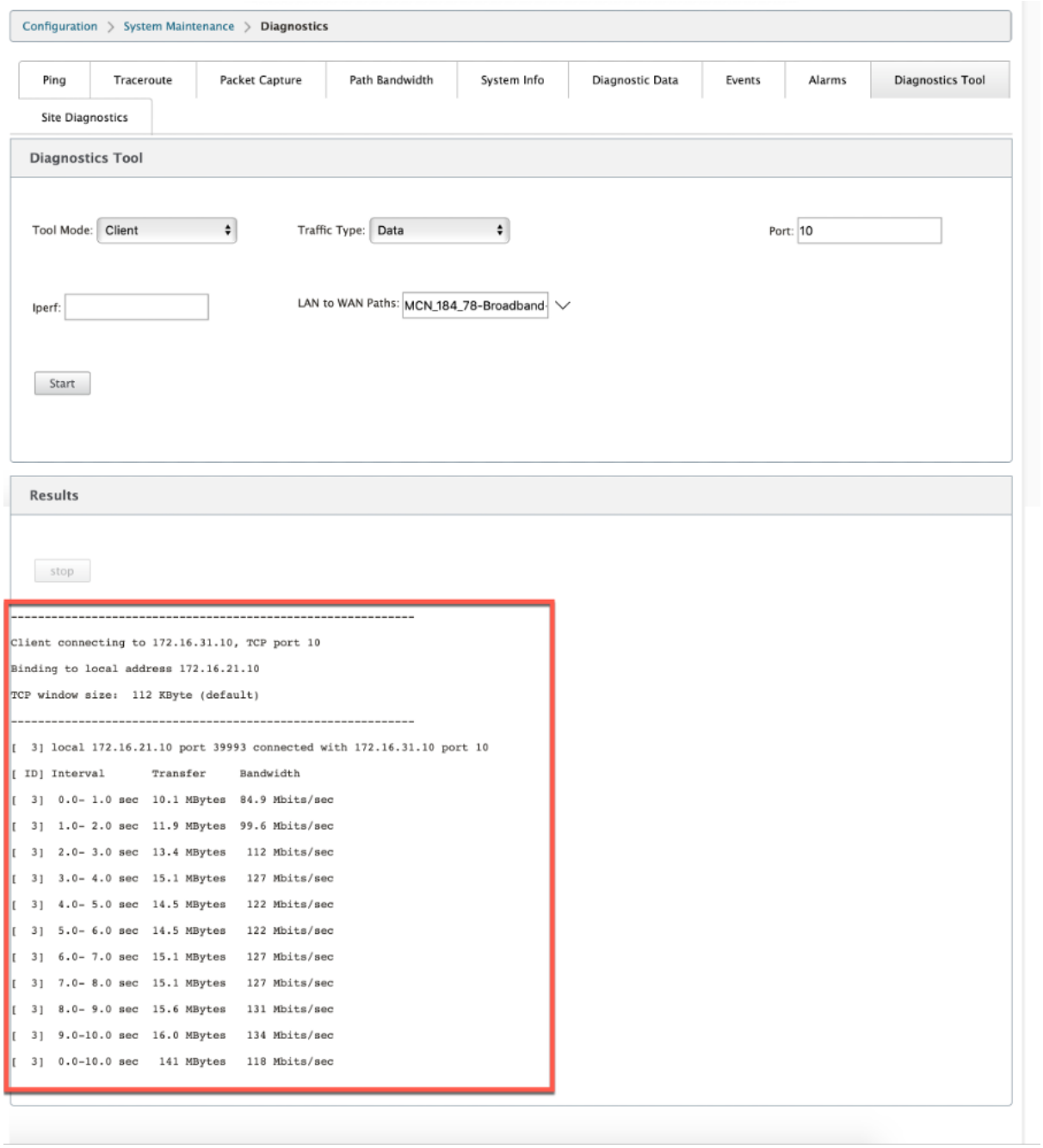
2. Wählen Sie im Feld **Toolmodus** die Option **Server** auf einer Appliance aus und wählen Sie **Client** auf der Appliance aus, die sich am Remote-Ende des ausgewählten Pfads befindet.
3. Wählen Sie im Feld **Traffic Type** die Art des Diagnoseverkehrs aus, entweder **Steuerung** oder **Daten**. Wählen 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**.

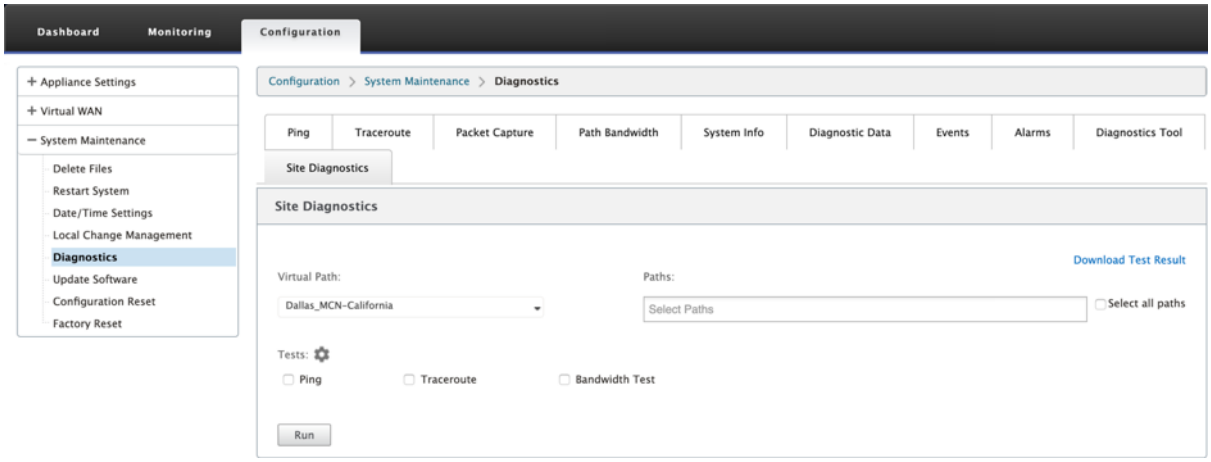
Das Ergebnis zeigt den Modus (Client oder Server) der ausgewählten Appliance und den TCP- oder UDP-Port an, auf dem der Test ausgeführt wird. Es zeigt regelmäßig die übertragenen Daten und die Bandbreite an, die für das angegebene Intervall genutzt wurde, bis die Gesamtdauer des Tests erreicht ist.



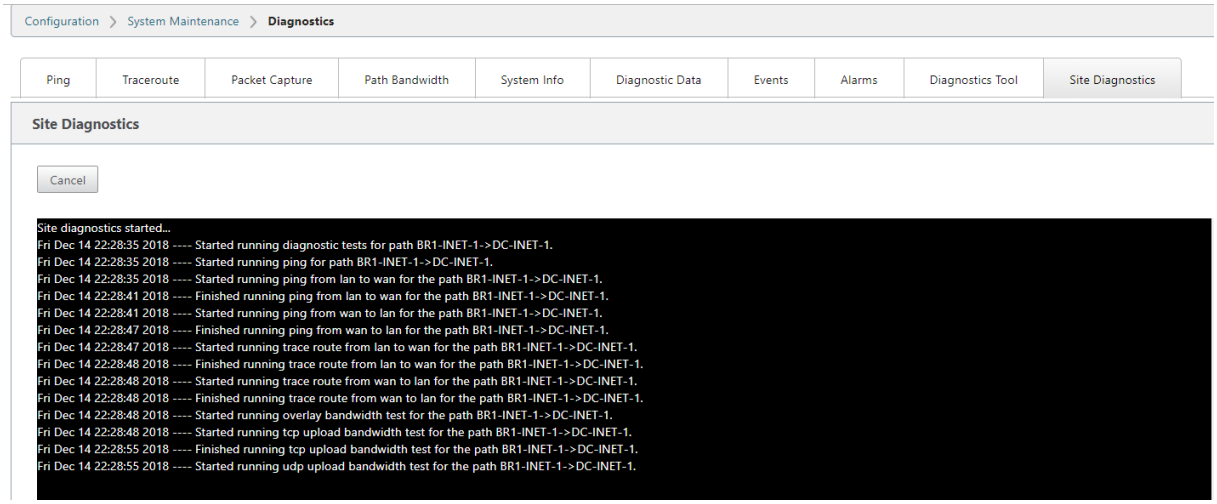
Site-Diagnose

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 bietet 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

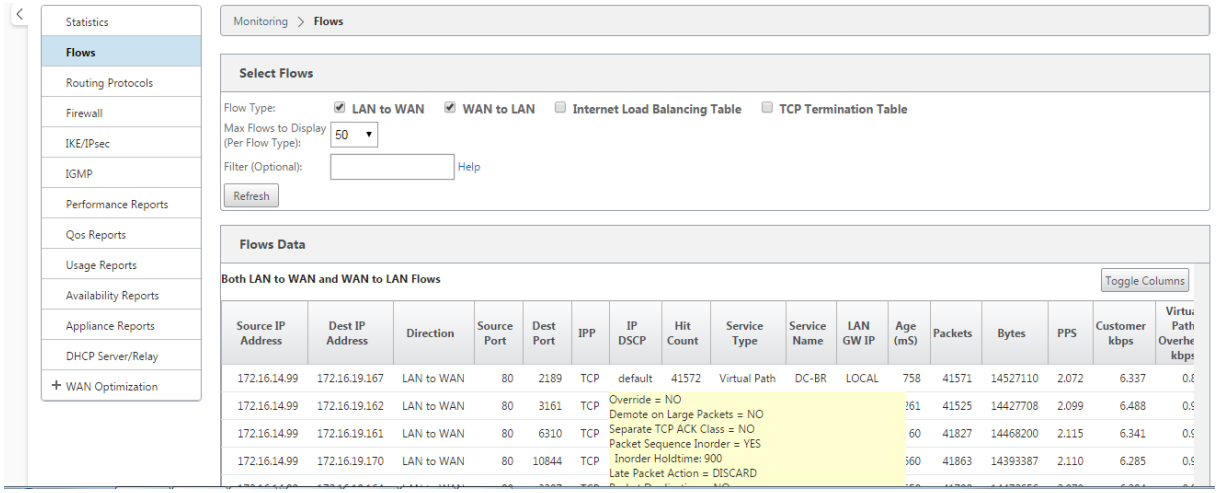
October 28, 2021

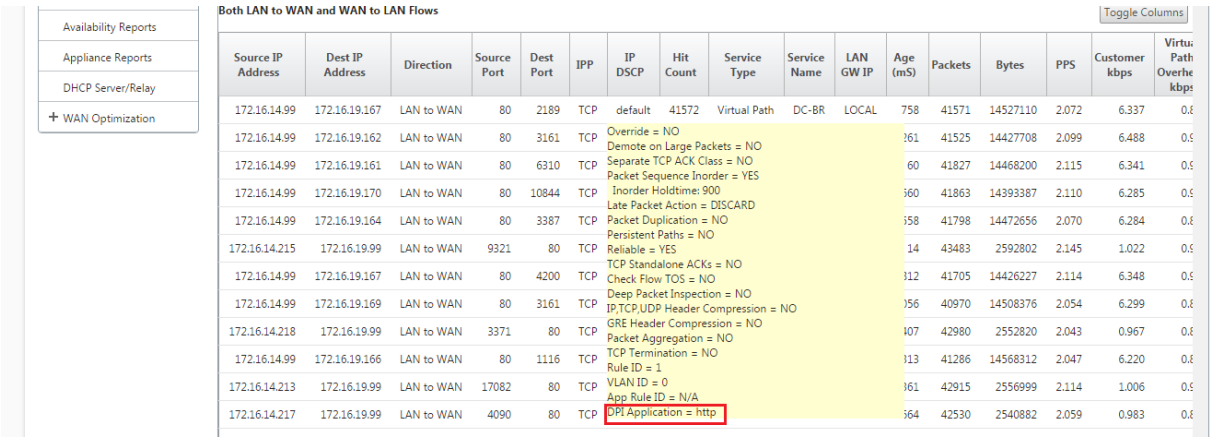
Pfadzuordnung und Verbesserungen der Bandbreitennutzung werden auf der Registerkarte Überwachung implementiert, um Verkehrsflüsse anzuzeigen. Wenn beispielsweise nur ein virtueller Pfad eine Netzwerkverbindung bedient und dieser virtuelle Pfad inaktiv wird, wird ein neuer bester Pfad gewählt und der ursprüngliche 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 bedient, sehen Sie einen aktuell besten Pfad und den nächstbesten Pfad, falls verfügbar. Wenn nur ein Pfad zur Verarbeitung des Datenverkehrs existiert, vorausgesetzt, es gibt mehr als zwei Pfade, die den Datenverkehr verarbeiten, 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 kommaseparaten Pfad als letzten besten Pfad an. Dieses Szenario wird implementiert, wenn mehr Pfade mit Bedarf an Bandbreite benötigt werden.

Überwachen von DPI-Anwendungsinformationen in SD-WAN GUI

Der Name des DPI-Anwendungsobjekts im Monitoring-Ablauf wird auf der Seite SD-WAN GUI **Monitoring** -> **Flows** gespeichert und angezeigt. Ein Tooltip wird angezeigt, um die DPI-Anwendung zu identifizieren.





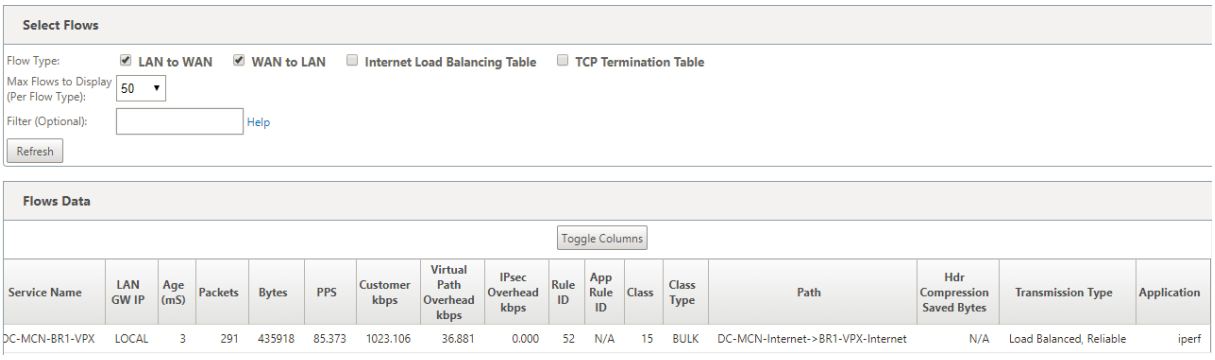
Überwachung von Pfadinformationen für den Verkehrsfluss in SD-WAN GUI

Es ist möglich, dass basierend auf der eingehenden Verkehrsrate, die Bandbreite erfordert, ein oder mehrere Pfade erforderlich sind, um den Verkehr zu verarbeiten.

Sehen Sie sich die folgenden Szenarien an, um zu bestimmen, wie Pfadzuordnung durchgeführt wird:

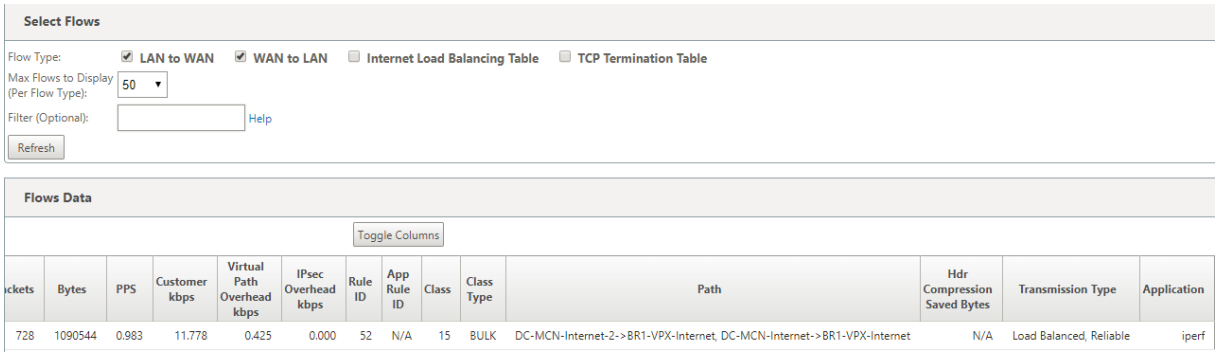
Lastausbalancierter Übertragungsmodus:

Die folgende Abbildung zeigt das Szenario, in dem der Verkehr initiiert wird und alle Pfade gut sind. Ein bester 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 ist und der Übertragungstyp als **Load Balanced angezeigt wird.**



Die folgende Abbildung zeigt, wann der Verkehr fließt und die WAN-Attribute des Pfades verschlechtert sind. Sie stellen fest, dass ein neuer Pfad für die Verarbeitung des Datenverkehrs ohne Unterbrechung gewählt wird. In diesem Fall können Sie mit der Pfadzuordnungsfunktion angeben, dass der derzeit beste Pfad zur Verarbeitung des Datenverkehrs **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.

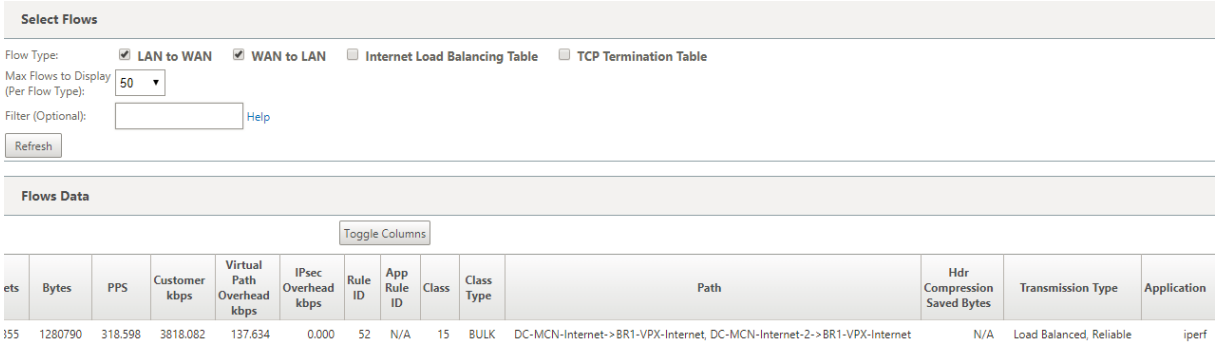


ckets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
728	1090544	0.983	11.778	0.425	0.000	52	N/A	15	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

Die folgende Abbildung zeigt, dass bei laufendem Datenverkehr und der Auswahl von mehr als einem Pfad für die Datenverkehrsverarbeitung aufgrund des Bandbreitenbedarfs, 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 auch den Verkehr bedienen, aber in der GUI werden nur die beiden besten Pfade angezeigt, die derzeit den Verkehr bedienen.

Beachten Sie, dass **DC-MCN-Internet-> BR1-VPX-Internet**, **DC-MCN-Internet2-> BR1-VPX-Internet** die beiden Pfade sind, die in der Tabelle **Flows Data** angezeigt werden.

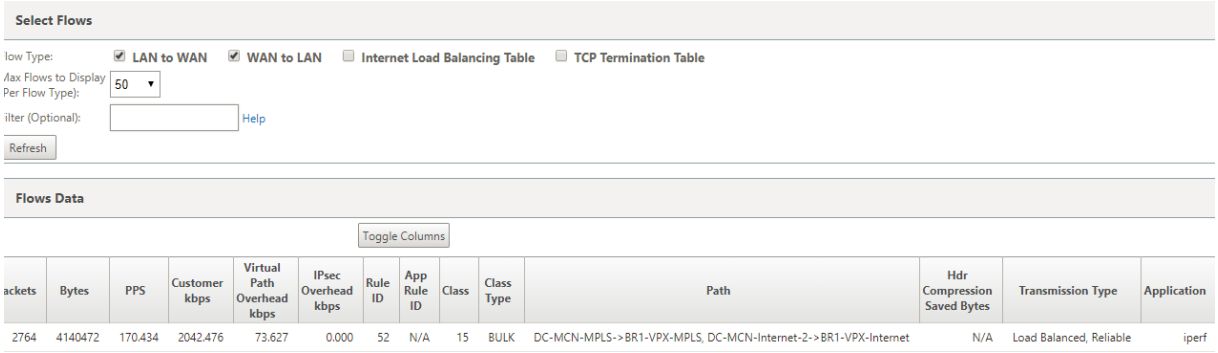
> **Hinweis**
>
> Wie angegeben, werden nur maximal zwei Pfade in der Flow-Tabelle angezeigt.



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
355	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 Verkehr noch fließt und der derzeit beste Pfad, der **DC-MCN-Internet-> BR1-VPX-Internet** ist, in WAN-Attributen nicht verfügbar/inaktiv/verschlechtert ist, der aktuell gewählte beste Pfad zuerst im Pfadabschnitt der Tabelle **Flows Data** angezeigt wird gefolgt auf dem letzten besten Weg, der den Verkehr bedient.

Da das **DC-MCN-Internet-> BR1-VPX-Internet** nicht mehr das beste war, wurde vom System ein neuer aktueller bester Pfad als **DC-MCN-MPLS->BR1-VPX-MPLS**gewählt, und der letzte beste Pfad, der die Verbindung zusammen mit dem aktuell besten Pfad aktiv bedient, ist **DC-MCN-Internet2-> BR1-VPX-Internet** da beide für den aktuellen Traffic-Bedarf an Bandbreite benötigt werden.



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

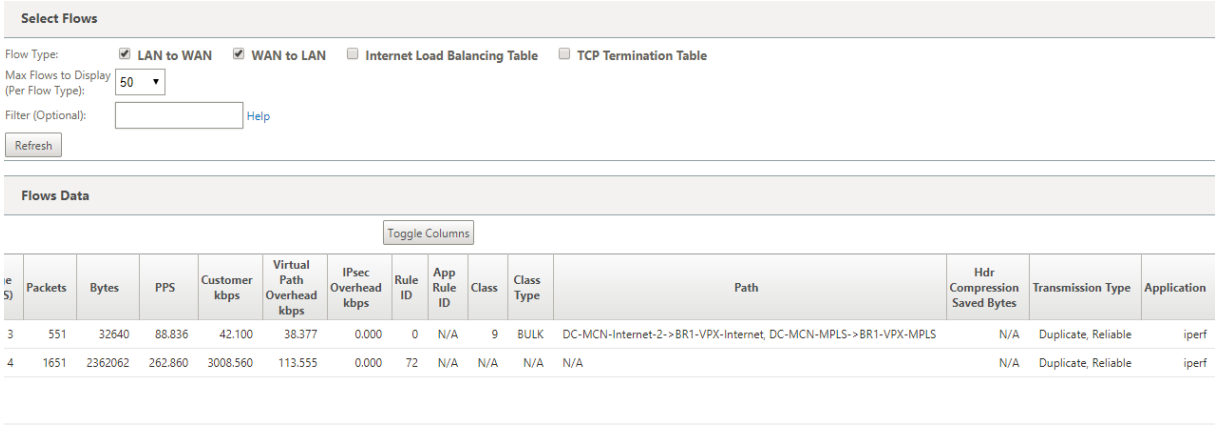
Übertragungsmodus duplizieren

Der allgemeine Paketduplizierungsmodus stellt sicher, dass anfänglich zwei Pfade für die Verarbeitung von Paketen derselben Verbindung verwendet werden, um eine zuverlässige Zustellung zu gewährleisten, indem Pakete über zwei separate Pfade dupliziert werden.

Beim Pfad-Mapping stellen Sie fest, dass im Pfadabschnitt der Flow-Tabelle zwei Pfade belegt werden, solange zwei Pfade existieren, um Flows durch Duplizieren zu verarbeiten.

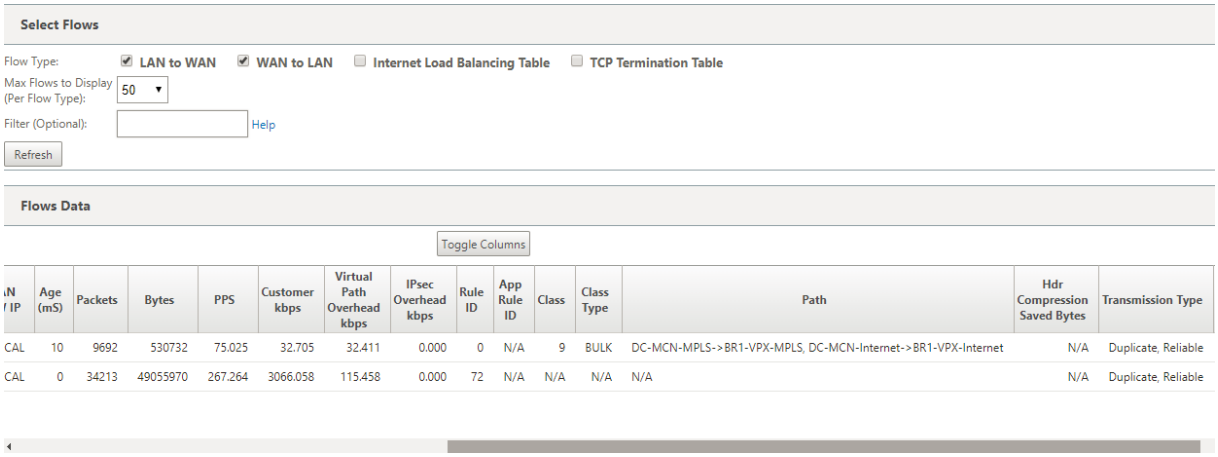
Die folgende Abbildung zeigt, dass bei fließendem Verkehr festgestellt werden kann, dass zwei Pfade den Verkehr verarbeiten. Im Gegensatz zu jedem anderen Modus dupliziert dieser Modus immer den Datenverkehr über zwei Pfade, selbst wenn der Verkehr weniger Bandbreite erfordert, die von nur einem Pfad bereitgestellt werden kann, für eine zuverlässige Anwendungsbereitstellung.

In der folgenden Abbildung sehen Sie zwei Pfade im Pfadabschnitt der Tabelle **Flows Data** ; **DC-MCN-Internet2-> BR-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS**.



ie S)	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 bei fließendem Datenverkehr, wenn einer der aktuellen besten Pfade inaktiv wird, ein anderer Pfad gewählt wird und es immer noch zwei Pfade als Teil des Pfadabschnitts in der Tabelle **Flows Data** gibt.

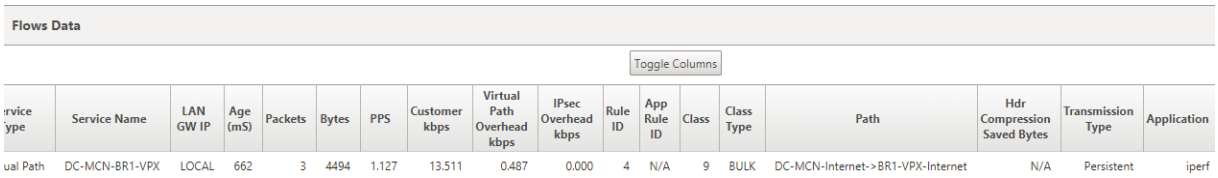


N / IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
CAL	10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	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

Persistenter Pfadübertragungsmodus

Der persistente Pfadübertragungsmodus hilft dabei, Pakete eines Flusses basierend auf der Pfadlatenzimpedanz beizubehalten.

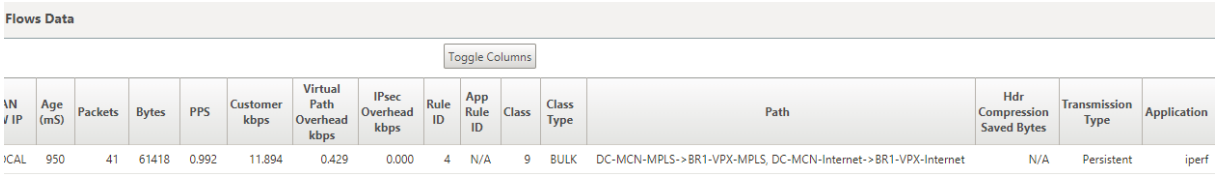
Die folgende Abbildung zeigt nur einen Pfad, der der beste Pfad ist, der derzeit die Flüsse und ihre Pakete verarbeitet. Es besteht kein Bedarf an Bandbreite und ein Pfad bietet alles. Derzeit gibt es nur einen besten Pfad, nämlich **DC-MCN-Internet-> BR1-VPX-Internet.**



rvice ype	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
ual 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 ein neuer Pfad wirksam wird und der aktuelle Pfad **DC-MCN-Internet-> BR1-VPX-Internet** zum letzten besten Pfad wird.

Der neue Pfadabschnitt zeigt also **DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-> BR1-VPX-Internet**.



N / IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
CAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

Im persistenten Modus kann mehr als ein Pfad zur Verarbeitung des Datenverkehrs ausgewählt werden. In diesem Fall zeigt die GUI sowohl die Pfade mit den besten als auch den nächstbesten im Pfadabschnitt der Flusstabelle vom Beginn 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 eingenommenen

Pfade werden wie folgt 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	N/A	Persistent	iperf

Angenommen, einer der besten Pfade **DC-MCN-Internet** geht in eine hohe Latenz oder ist deaktiviert. Dies lässt einen neuen Pfad erscheinen 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	N/A	Persistent	iperf

Fehlerbehebung bei Management-IP

October 28, 2021

Im Folgenden sind die möglichen Szenarien aufgeführt, die bei der Konfiguration 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 Hardwaremodelle von SD-WAN-Appliances werden mit einer werkseitigen Standardverwaltungs-IP-Adresse ausgeliefert. Stellen Sie sicher, dass Sie während des Einrichtungsvorgangs die erforderliche DHCP-IP-Adresse für die Appliance konfigurieren.
>
> Allen virtuellen Modellen von SD-WAN-Appliances (VPX-Modelle) und Appliances, die in einer AWS-Umgebung bereitgestellt werden können, ist keine werkseitig standardmäßige IP-Adresse zugewiesen.

Geräte werden eingeschaltet, ohne dass DHCP-Server erreichbar sind:

- Verursacht:
  - Ethernet-Managementkabel ist getrennt

  - Der DHCP-Dienst ist für das verbundene Netzwerk ausgefallen

- Erwartetes Verhalten
  - Appliances mit aktiviertem DHCP-Dienst versuchen die DHCP-Anforderung alle 300 Sekunden erneut (Standardwert). Das tatsächliche Intervall beträgt ungefähr 7 Minuten.
  - Daher erhalten Appliances mit aktiviertem DHCP-Dienst DHCP-Adressen innerhalb von 7 Minuten nach der Verfügbarkeit von DHCP-Servern DHCP-Adressen. Die Verzögerung reicht von 0 bis 7 Minuten

Die zugewiesene DHCP-Adresse läuft ab:

- Erwartetes Verhalten:
  - Appliances mit aktiviertem DHCP-Dienst versuchen, das Leasing zu verlängern, bevor die Adresse abläuft
  - Appliances beginnen mit einer neuen DHCP-Erkennung, wenn die Verlängerung fehlschlägt

Appliances mit aktiviertem DHCP-Dienst wechseln von einem DHCP-fähigen Subnetz in ein anderes Subnetz:

- Ursachen: Appliances wechseln von einem zugewiesenen DHCP-Subnetz in ein anderes DHCP-Subnetz
- Erwartetes Verhalten:
  - Bei einer permanenten Lease-DHCP-IP-Adresszuweisung müssen die Appliances möglicherweise neu gestartet werden, um eine IP-Adresse vom neuen DHCP-Server zu erhalten.
  - Nach Ablauf des DHCP-Leases initiieren Appliances möglicherweise das DHCP-Discovery-Protokoll erneut, 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 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

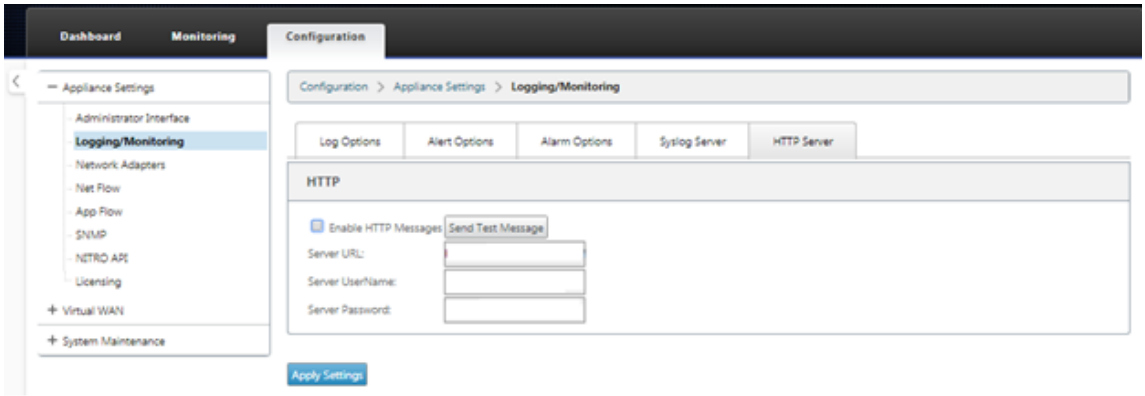
October 28, 2021

Sie können jetzt Ereignis- und Alarmberichte für generische HTTP-POST-API-Dienstanforderungen in der Benutzeroberfläche der Citrix SD-WAN Appliance konfigurieren. Die Konfiguration von HTTP-Alarm- und Ereignisbenachrichtigungen ähnelt den E-Mail- und SNMP-Ereignissen für Ereignisse und Alarme, die in SD-WAN unterstützt werden.

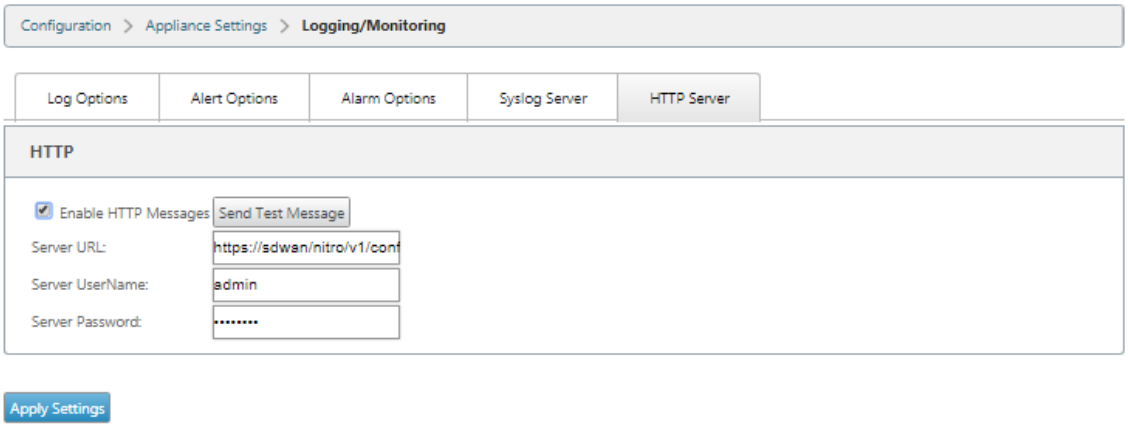
Die sitzungsbasierte HTTP-Post-Benachrichtigung wird an einen externen Dienst wie Service Now gesendet. Die Ereignisbenachrichtigungen für den HTTP-Server können in der Benutzeroberfläche der Citrix SD-WAN Appliance und im Citrix SD-WAN Center konfiguriert werden.

So konfigurieren Sie HTTP POST-Benachrichtigungen in der Benutzeroberfläche der Citrix SD-WAN Appliance:

1. Navigieren Sie zu **Konfiguration** > **Protokollierung/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**.

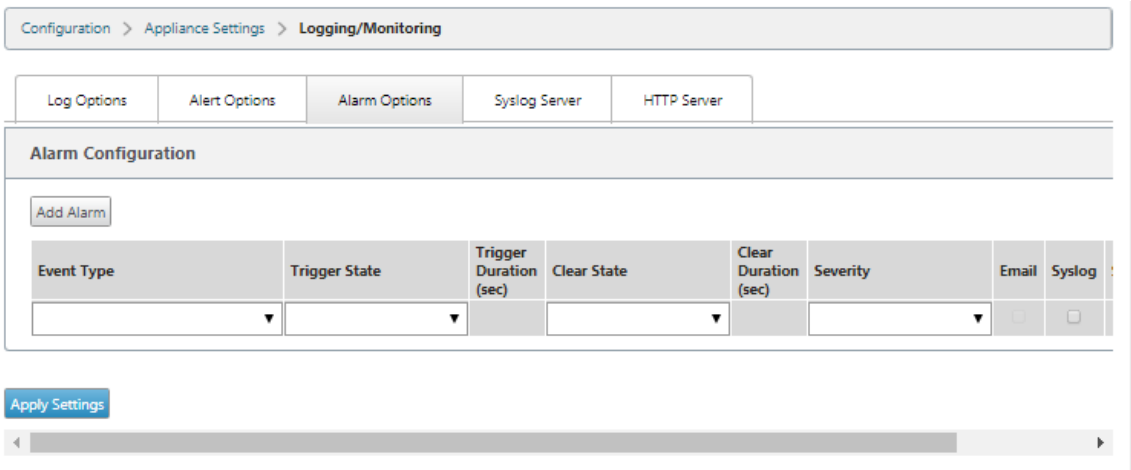


4. Klicken Sie auf **Einstellungen anwenden**. Die Seite wird aktualisiert, nachdem die Einstellungen für Benachrichtigungen des HTTP-Servers angewendet wurden.

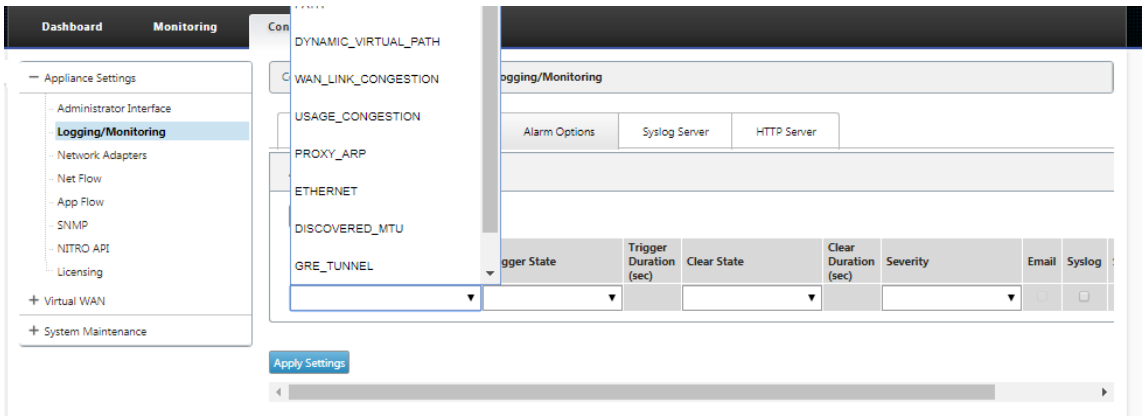
> **Hinweis**
>
> Verwenden Sie die Option **Testnachricht senden**, um zu überprüfen, ob die HTTP-Serververbindung erfolgreich ist.

So fügen Sie eine Alarmbenachrichtigung für die HTTP-Server

1. Wechseln Sie auf der Seite **Protokollierung/Überwachung** zur Registerkarte **Alarmoptionen**.
2. Klicken Sie auf **Alarm hinzufügen**.

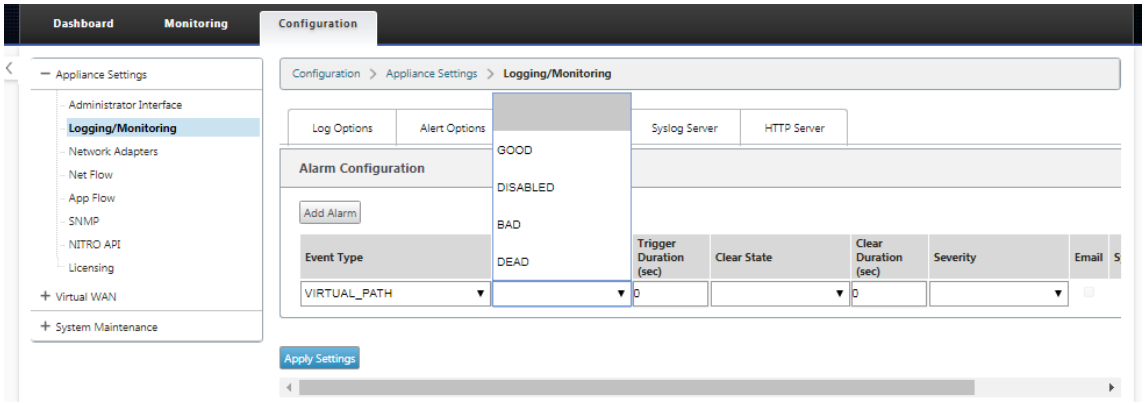


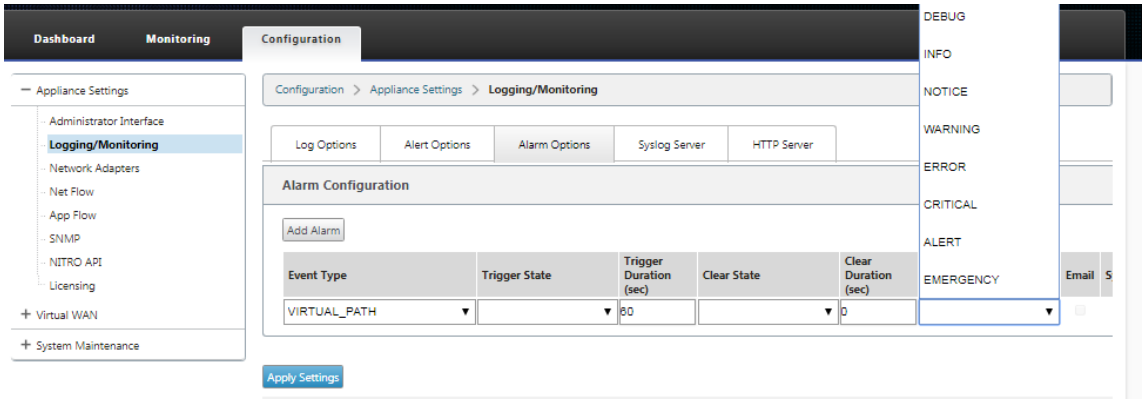
3. Wählen Sie in der Dropdownliste einen **Ereignistyp** aus.



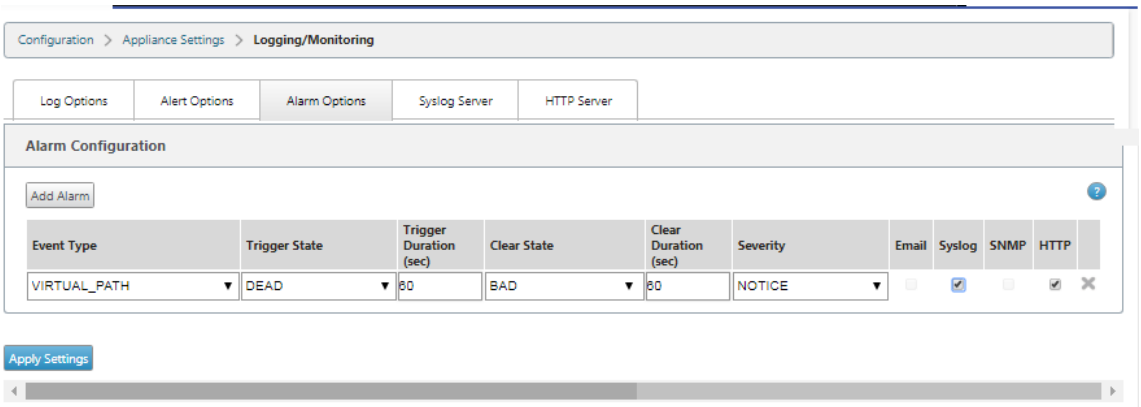
4. Wählen Sie die folgenden Alarmbenachrichtigungszustände für die gewählte **Ereignisart**. Der Triggerstatus und der Löschzustand ändern sich entsprechend dem ausgewählten Ereignistyp.

   - Trigger State –GOOD, DISABLED, BAD, DEAD
   - Triggerdauer —Zeit in Sekunden
   - Clear State - GOOD, DISABLED, BAD, DEAD
   - Dauer löschen —Zeit in Sekunden
   - Severity –DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, EVENT, EMERGENCY





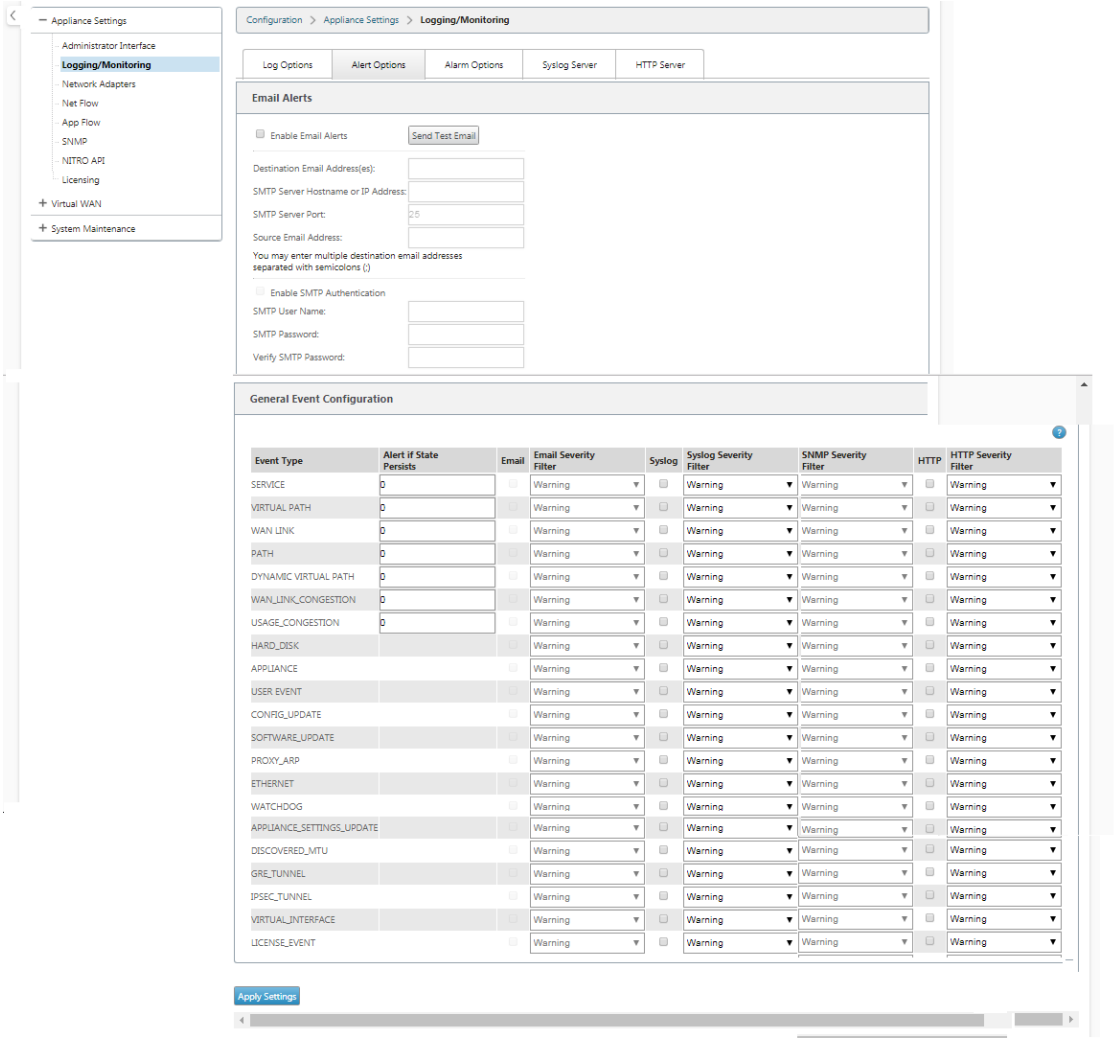
5. Aktivieren Sie die Kontrollkästchen **Syslog** und **HTTP**, um Benachrichtigungen zu den Syslog- und HTTP-Serverereignissen zu erhalten. Klicken Sie auf **Einstellungen anwenden**.



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**.

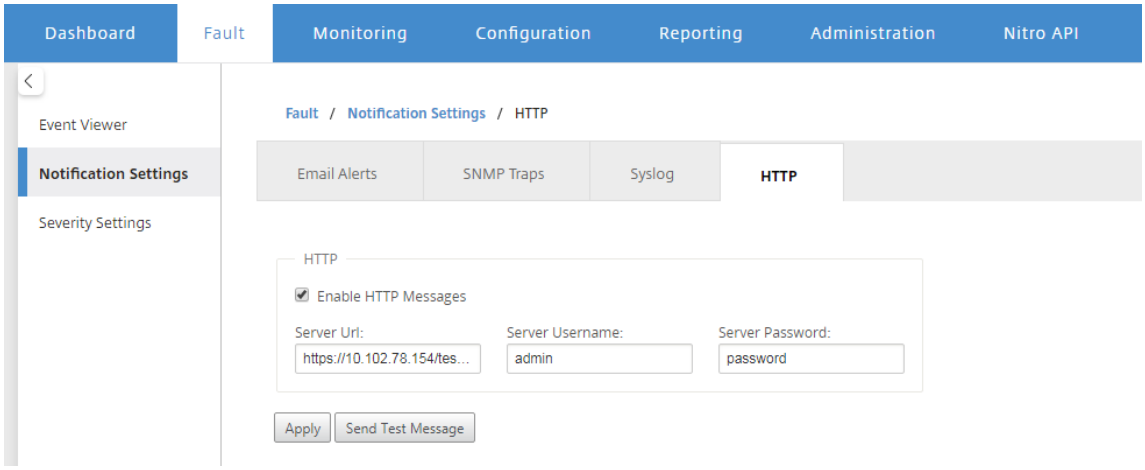
- HTTP
- HTTP-Schweregradfilter



Konfigurieren von HTTP-Benachrichtigungen in Citrix SD-WAN Center

So konfigurieren Sie HTTP-Benachrichtigungen:

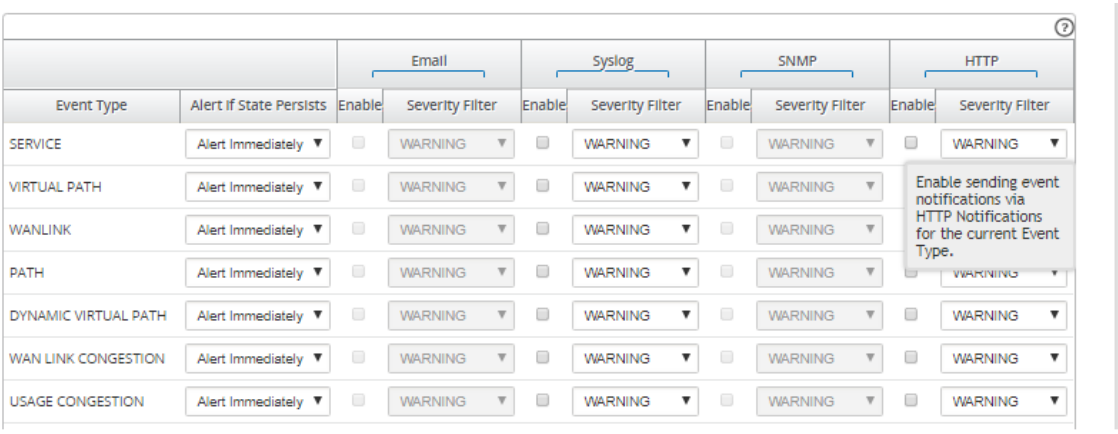
1. Navigieren Sie zu **Fehler** > **Benachrichtigungseinstellungen** > **HTTP**.



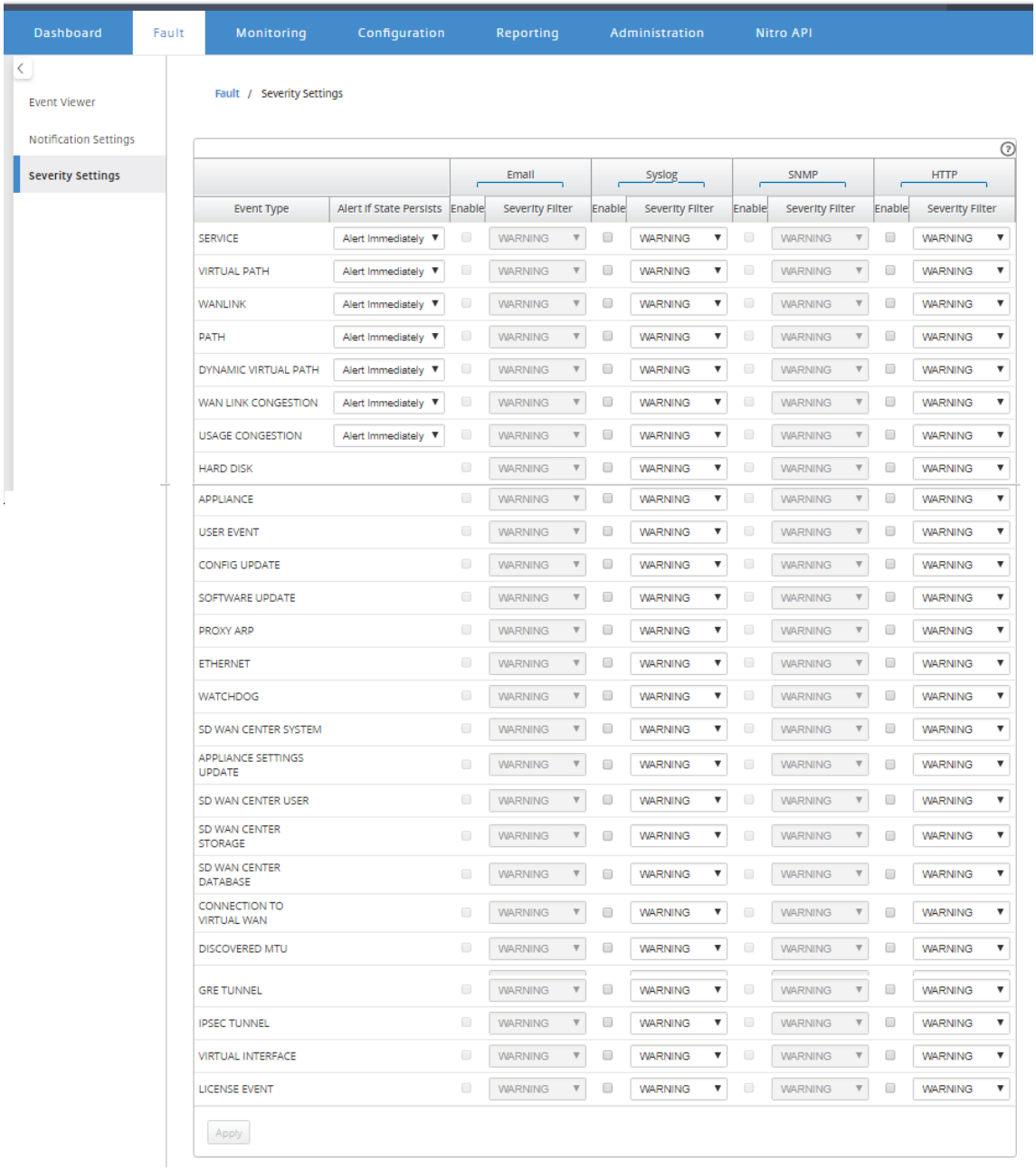
2. Geben Sie die **Server-URL**, den **Server-Benutzernamen** und das **Serverkennwort** für den HTTP-Server ein.
3. Klicken Sie auf **Anwenden**

So konfigurieren Sie Schweregradeinstellungen:

1. Wechseln Sie zur Seite **Schweregradeinstellungen**. Klicken Sie auf **Aktivieren**, um HTTP-Benachrichtigungen für einen ausgewählten Ereignistyp zu überwachen.



2. Sie können E-Mail-, Syslog-, SNMP- und HTTP-Ereignisbenachrichtigungen für die folgenden Ereignistypen überwachen. Klicken Sie auf **Apply**.



Aktive Bandbreitentests

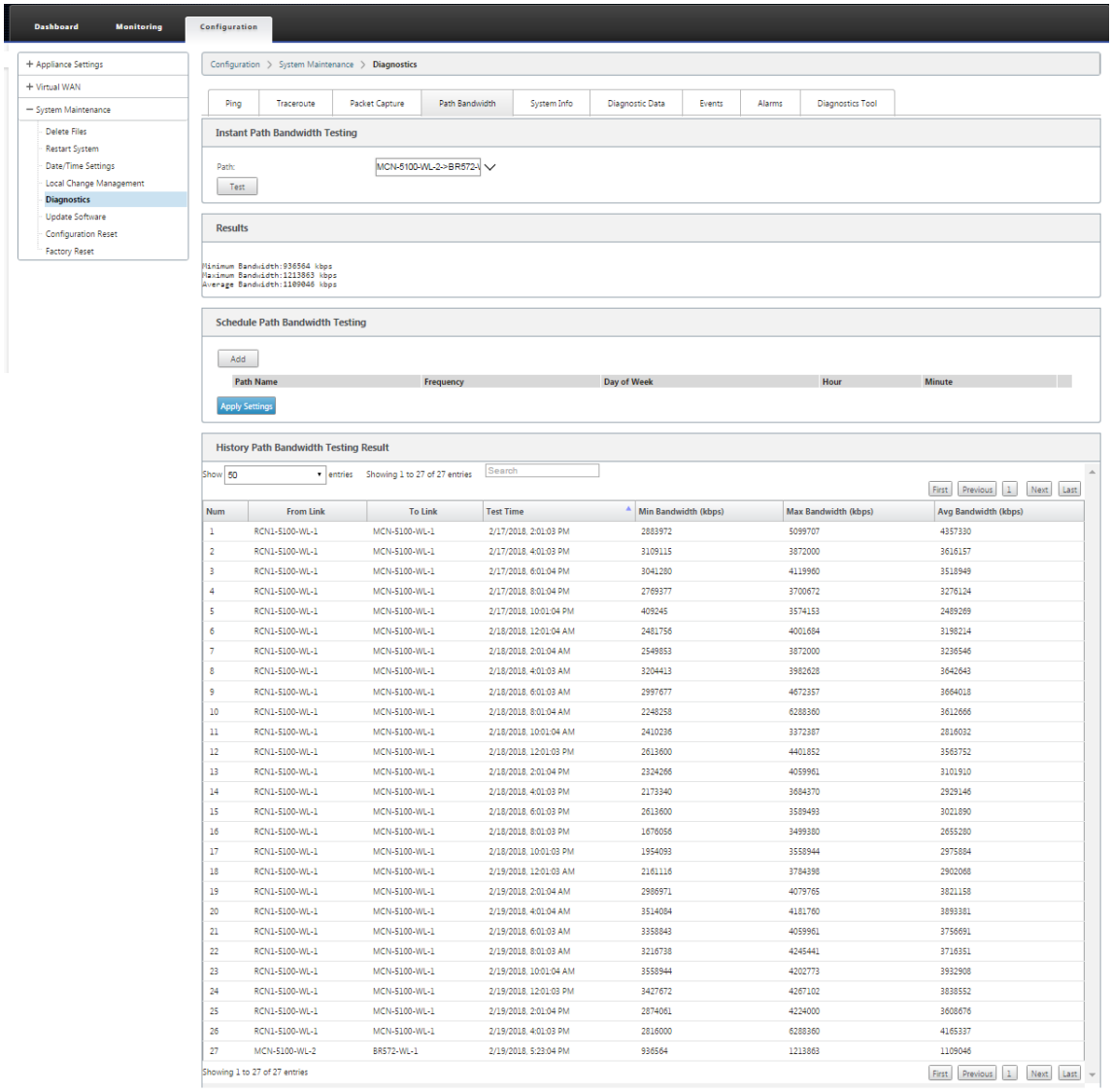
October 28, 2021

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 vorhandener Installationen verfügbar ist, auch um Pfade zu testen, um das Ergebnis von Einstellungs- und Bestätigungsänderungen zu bestimmen, z. B. die Anpassung der DSCP-Tag-Einstellungen oder der zulässigen Bandbreitenraten.

So verwenden Sie die Funktion zum aktiven Bandbreitentest:

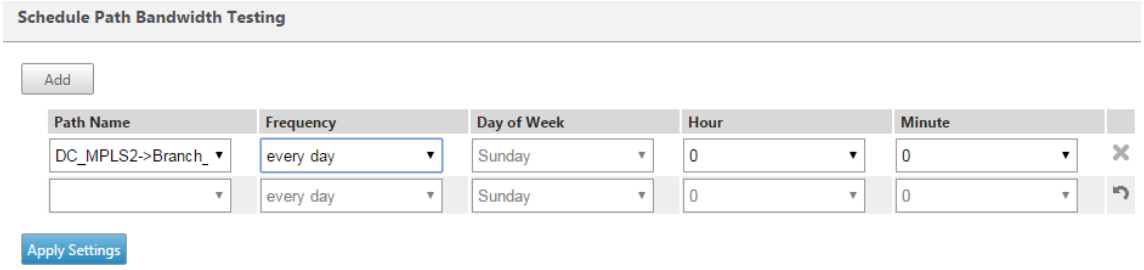
1. Navigieren Sie zu **Systemwartung** > **Diagnose** > **Pfadbandbreite**.
2. Wählen Sie den gewünschten **Pfad** aus und klicken Sie auf **Test**.



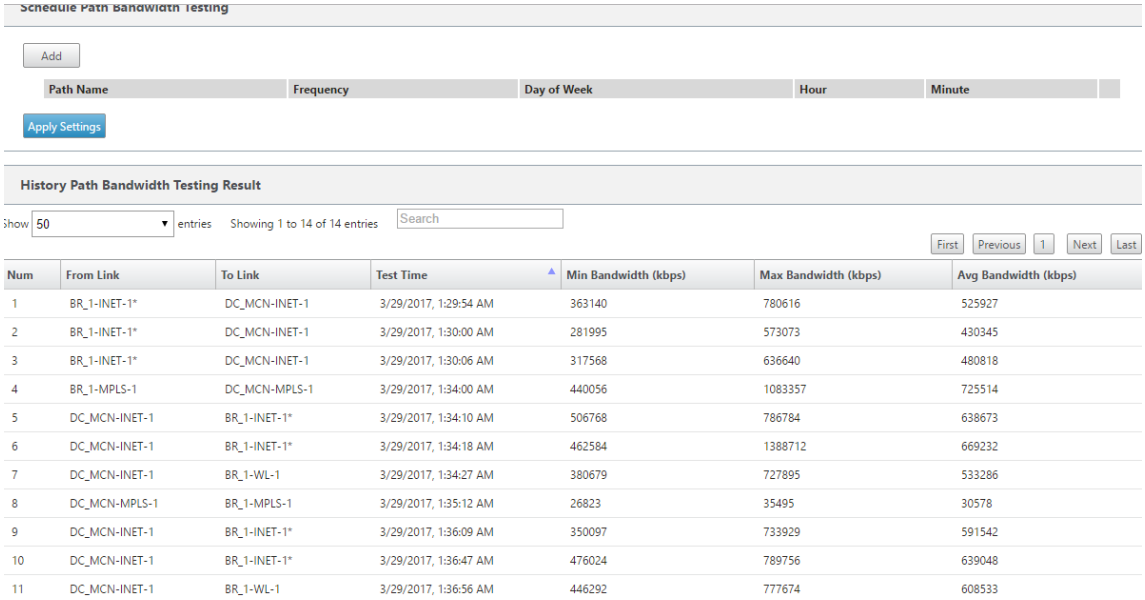
Die Ausgabe zeigt die durchschnittliche Bandbreite an, die als Wert verwendet wird, um als zulässige Rate für die Ergebnisse der minimalen und maximalen WAN-Link-Bandbreite des Tests festzulegen. Zusammen mit der Möglichkeit, die Bandbreite zu testen, können Sie nun die Konfigurationsdatei ändern, um die erlernte Bandbreite zu verwenden. Dies wird durch die Option Auto Learn unter **Standort > [Site-Name]** > **WAN-Links > [WAN-Link-Name]** > **Einstellungen**

erreicht und wenn aktiviert, verwendet das System die erlernte Bandbreite.

Sie können auch wiederkehrende Tests der Pfadbandbreite in wöchentlichen, täglichen oder stündlichen Intervallen planen.



> **Hinweis**
>
> Eine Historie der Ergebnisse der Pfadbandbreitentests wird unten auf dieser Seite angezeigt und die Ergebnisse werden alle sieben Tage archiviert.



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

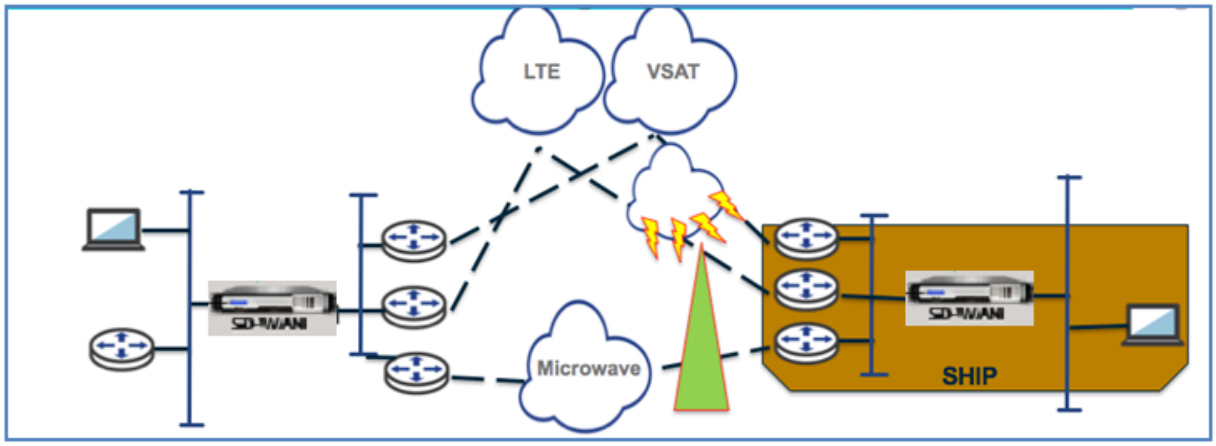
Adaptive Bandbreitenerkennung

October 28, 2021

Diese Funktion gilt für Netzwerke mit VSAT-, LOS-, Mikrowellen-, 3G/4G/LTE-WAN-Verbindungen, für die die verfügbare Bandbreite je nach Wetter- und Atmosphärenbedingungen, Standort und Standortbehinderung variiert. Es ermöglicht den SD-WAN-Appliances, die Bandbreitenrate auf dem WAN-Link

dynamisch basierend auf einem definierten Bandbreitenbereich (minimale und maximale WAN-Link-Rate) anzupassen, um die maximale Menge an verfügbarer Bandbreite zu nutzen, ohne die Pfade BAD zu markieren.

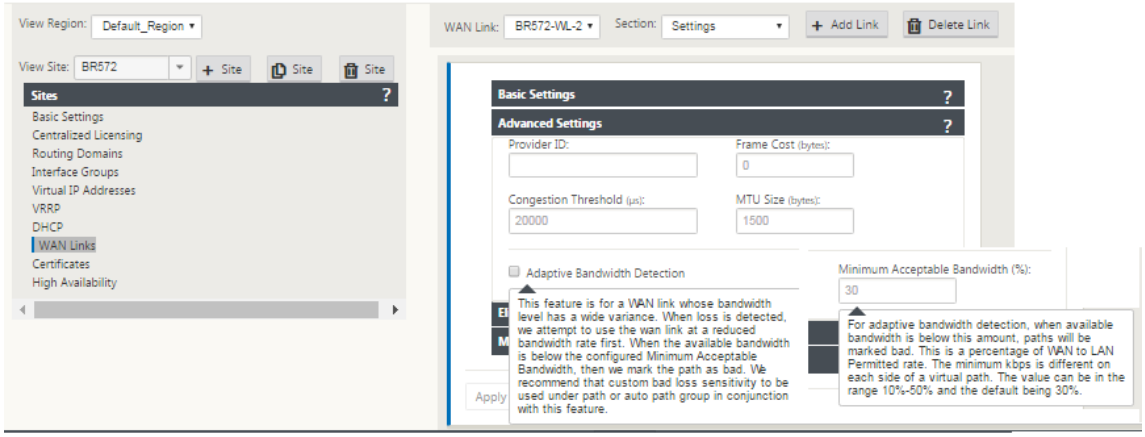
- Höhere Bandbreitenzuverlässigkeit (über VSAT, Mikrowelle, 3G/4G und LTE)
- Höhere Vorhersagbarkeit der adaptiven Bandbreite über vom Benutzer konfigurierte Einstellungen



So aktivieren Sie die adaptive Bandbreitenerkennung:

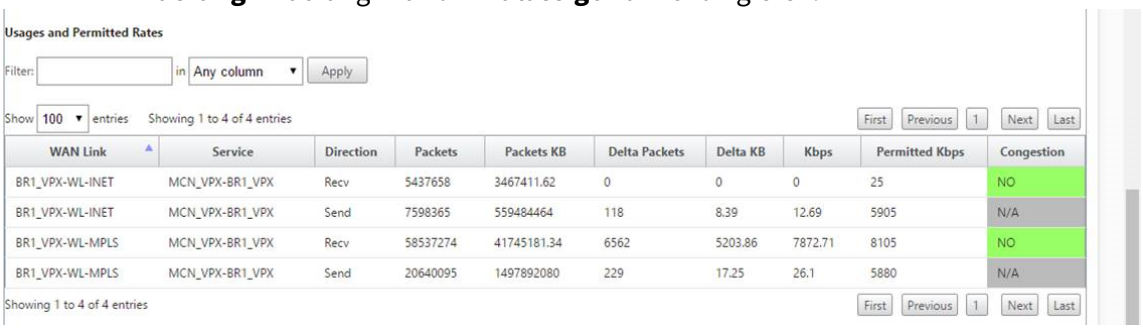
Für diese Funktion ist die Option Empfindlichkeit bei schlechten Verlusten erforderlich, um als Voraussetzung aktiviert (Standard/Benutzerdefiniert) zu sein. Sie können es unter **Global** >**Autopath-Gruppen > [**Autopath-Gruppenname**]** > **Bad Loss Sensitive**aktivieren.

1. Aktivieren Sie die **adaptive Bandbreitenerkennung** unter **Global** >**Autopath-Gruppen** >[**Autopath-Gruppenname**] >**Schadverlustempfindlich**.
2. Navigieren Sie zu **Konfigurationseditor** > **Sites**[**> Site-Name**] > **WAN-Links** > [**WAN-Linkname**] > **Einstellungen** > **Erweiterte Einstellungen**.



3. Aktivieren Sie das Kästchen **Adaptive Bandbreitenerkennung** und geben Sie einen Wert in das Feld **Minimale akzeptable Bandbreite** ein.

4. Zeigen Sie die Tabelle **Nutzung und zulässige Tarife** an, indem **Sie zu Monitor** > **Statistik** > **WAN-Link-Nutzung >**Nutzung**** und **zulässige Tarife**navigieren.



Usages and Permitted Rates

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

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 First Previous 1 Next Last

Bewährte Methoden

October 28, 2021

Die folgenden Themen enthalten die Best Practices, die bei der Planung, Planung und Ausführung der Citrix SD-WAN in Ihrem Netzwerk zu befolgen sind.

Sicherheit

Routing

QoS

WAN-Links

Sicherheit

October 28, 2021

In diesem Artikel werden bewährte Sicherheitsmethoden für die Citrix SD-WAN-Lösung beschrieben. Es bietet allgemeine Sicherheitsrichtlinien für Citrix SD-WAN-Bereitstellungen.

Citrix SD-WAN Bereitstellungsrichtlinien

Um die Sicherheit während des Bereitstellungslebenszyklus aufrechtzuerhalten, empfiehlt Citrix die folgenden Sicherheitsüberlegungen:

- Physische Sicherheit
- Gerätesicherheit

- Netzwerksicherheit
- Verwaltung und Verwaltung

Physische Sicherheit

Bereitstellen von Citrix SD-WAN Appliances in einem sicheren Serverraum - Die Appliance oder der Server, auf dem Citrix SD-WAN installiert ist, sollte in einem sicheren Serverraum oder einer eingeschränkten Rechenzentrumseinrichtung aufgestellt werden, die die Appliance vor unbefugtem Zugriff schützt. Der Zugang sollte mindestens über einen elektronischen Kartenleser gesteuert werden. Der Zugriff auf die Appliance wird von CCTV überwacht, die kontinuierlich alle Aktivitäten zu Prüfungszwecken aufzeichnet. Bei einem Einbruch sollte das elektronische Überwachungssystem dem Sicherheitspersonal einen Alarm zur sofortigen Reaktion senden.

Schützen Sie die Frontplatte und die Konsolenanschlüsse vor unbefugtem Zugriff - Sichern Sie das Gerät in einem großen Käfig oder Rack mit einer Zugangskontrolle mit physischem Schlüssel.

Netzteil schützen - Stellen Sie sicher, dass das Gerät mit einer unterbrechungsfreien Stromversorgung (USV) geschützt ist.

Gerätesicherheit

Schützen Sie aus Sicherheitsgründen das Betriebssystem eines Servers, auf dem eine virtuelle Citrix SD-WAN Appliance (VPX) gehostet wird, führen Sie Remote-Softwareupdates durch und befolgen Sie sichere Lebenszyklusverwaltungspraktiken:

- Sichern Sie das Betriebssystem des Servers, der eine Citrix SD-WAN VPX Appliance hostet - Eine Citrix SD-WAN VPX-Appliance wird als virtuelle Appliance auf einem Standardserver ausgeführt. Der Zugriff auf den Standardserver sollte durch eine rollenbasierte Zugriffskontrolle und eine starke Kennwortverwaltung geschützt werden. Außerdem empfiehlt Citrix regelmäßige Updates des Servers mit den neuesten Sicherheitspatches für das Betriebssystem und aktueller Antivirensoftware auf dem Server.
- Durchführen von Remote-Softwareupdates - Installieren Sie alle Sicherheitsupdates, um bekannte Probleme zu beheben Auf der Webseite Security Bulletins finden Sie Informationen, um sich anzumelden und aktuelle Sicherheitswarnungen zu erhalten.
- Befolgen Sie die Secure Lifecycle Management Practices - Um eine Appliance bei der erneuten Bereitstellung oder Initiierung von RMA und der Stilllegung sensibler Daten zu verwalten, schließen Sie die Gegenmaßnahmen zur Datenerinnerung ab, 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 routbare Verwaltungs-IP-Adresse der Appliance, konfigurieren Sie ein Hochverfügbarkeits-Setup und implementieren Sie gegebenenfalls Administrations- und Verwaltungssicherungen für die Bereitstellung.

- Verwenden Sie nicht das Standard-SSL-Zertifikat - Ein SSL-Zertifikat einer seriösen Zertifizierungsstelle vereinfacht die Benutzererfahrung für Internet-Webanwendungen. Im Gegensatz zu einem selbstsignierten Zertifikat oder einem Zertifikat der seriösen Zertifizierungsstelle müssen Benutzer in Webbrowsern das Zertifikat der seriösen Zertifizierungsstelle nicht installieren, um eine sichere Kommunikation mit dem Webserver zu initiieren.
- Verwenden Sie Transport Layer Security beim Zugriff auf die Administratorschnittstelle - Stellen Sie sicher, dass die Management-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 sichere Passwörter für Admin- und Betrachterkonten fest. Wenn Sie den Remote-Kontozugriff konfigurieren, sollten Sie die Konfiguration der extern authentifizierten administrativen Verwaltung von Konten mithilfe von RADIUS und TACAS in Betracht ziehen. Ändern Sie das Standardkennwort für die Admin-Benutzerkonten, konfigurieren Sie NTP, verwenden Sie den Standard-Sitzungstimeout-Wert, verwenden Sie SNMPv3 mit SHA-Authentifizierung und AES-Verschlüsselung.

Das Citrix SD-WAN-Overlay-Netzwerk schützt Daten, die das SD-WAN-Overlay-Netzwerk durchlaufen.

Sichere Administratoroberfläche

Ersetzen Sie für einen sicheren Zugriff auf die Webverwaltung Standardsystemzertifikate, indem Sie Zertifikate von einer seriösen Zertifizierungsstelle hochladen und installieren. Gehen Sie in der SD-WAN-Appliance-GUI zu **Konfiguration> Appliance-Einstellungen> Administratorschnittstelle**.

Benutzerkonten:

- Ändern Sie das lokale Benutzerkennwort
- Nutzer verwalten

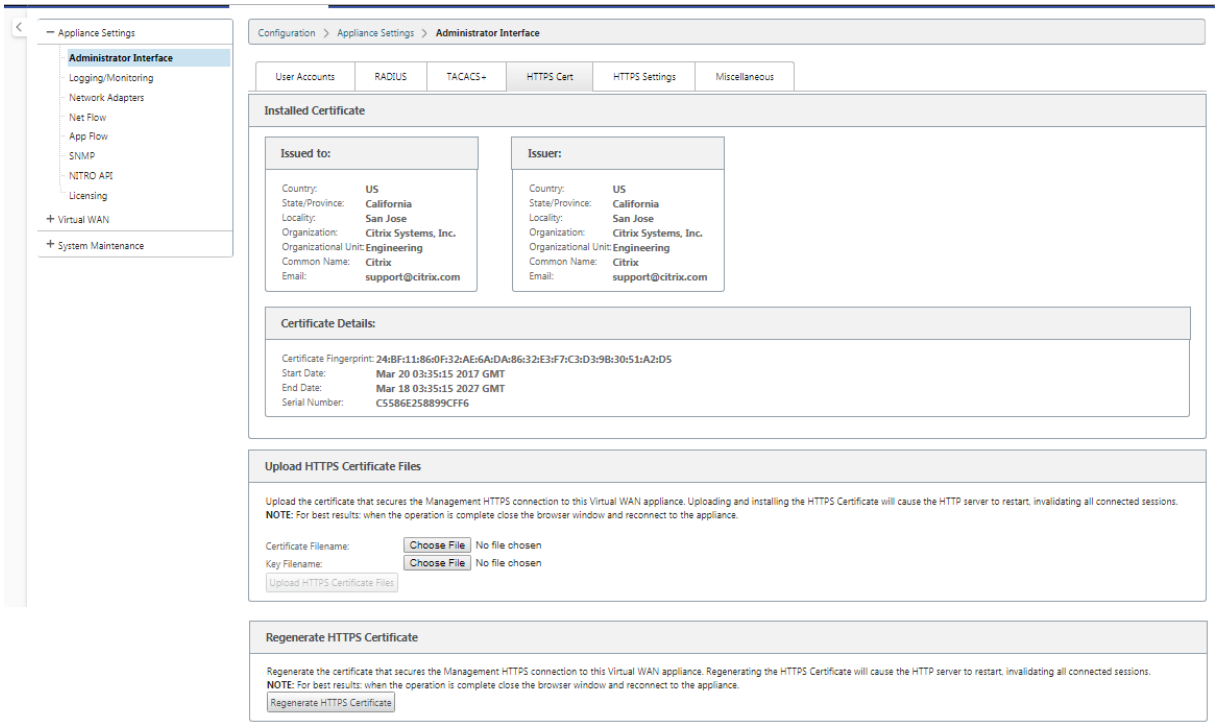
HTTPS Certs:

- Zertifikat

- Key

Sonstiges:

- Timeout der Webkonsole



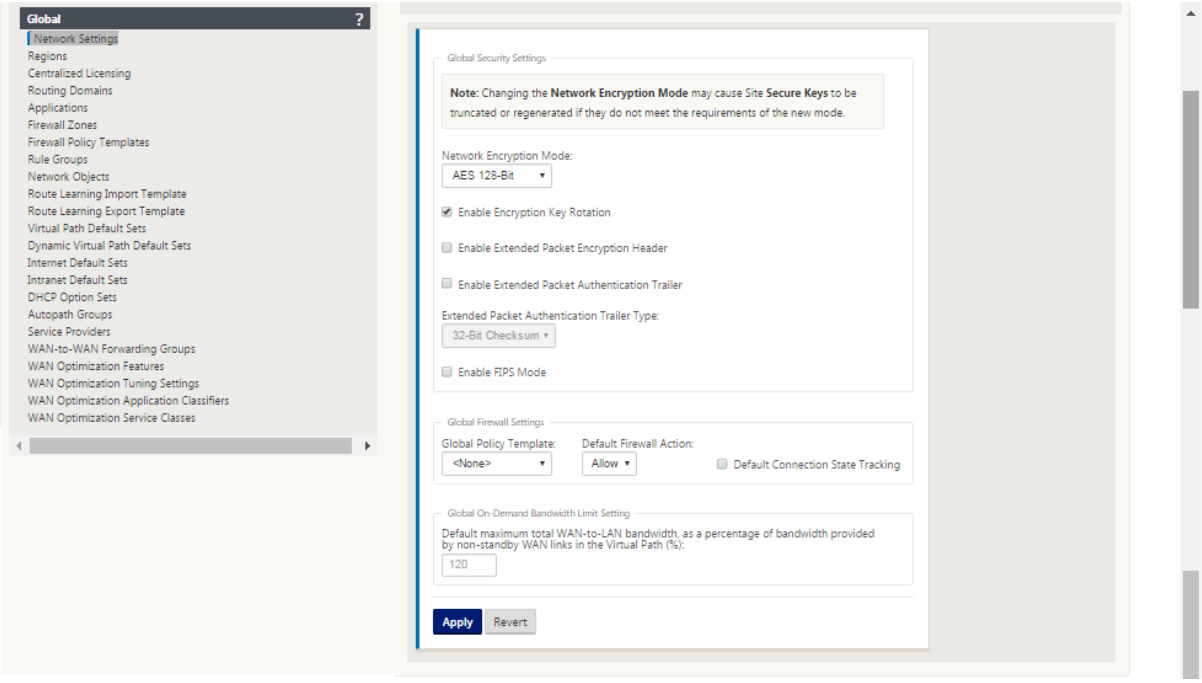
Konfigurationseditor > **Global** > **Netzwerkeinstellungen**

Globale Firewall-Einstellungen:

- Vorlage für globale Richtlinien
- Standard-Firewall-Aktionen
- Standard-Verbindungsstatus-Tracking

Globale Verschlüsselungseinstellungen für virtuelle Pfade:

- AES 128-Bit (Standard)
- Rotation des Verschlüsselungsschlüssels (Standard)
- Erweiterte Paketverschlüsselung Header
- Erweiterter Trailer zur Paketauthentifizierung



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 Schlüsselregeneration für jeden virtuellen Pfad mit aktivierter Verschlüsselung mithilfe eines Elliptic Curve Diffie-Hellman-Schlüsselaustauschs in Intervallen von 10-15 Minuten sichergestellt wird.

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, einen zufällig gesetzten Zähler dem Anfang jeder verschlüsselten Nachricht voranzustellen. Bei Verschlüsselung dient dieser Zähler als zufälliger Initialisierungsvektor, der nur mit dem Verschlüsselungsschlüssel deterministisch ist. Dies randomisiert die Ausgabe der Verschlüsselung und liefert eine starke Botschaft, die nicht zu unterscheiden ist. Beachten Sie, dass diese Option bei Aktivierung den Paketaufwand um 16 Byte erhöht
- Extended Packet Authentication Trailer hängt einen Authentifizierungscode an das Ende jeder verschlüsselten Nachricht an. Dieser Trailer ermöglicht die Überprüfung, dass Pakete während des Transports nicht modifiziert werden. Denken Sie daran, dass diese Option den Paketaufwand erhöht.

Firewall-Sicherheit

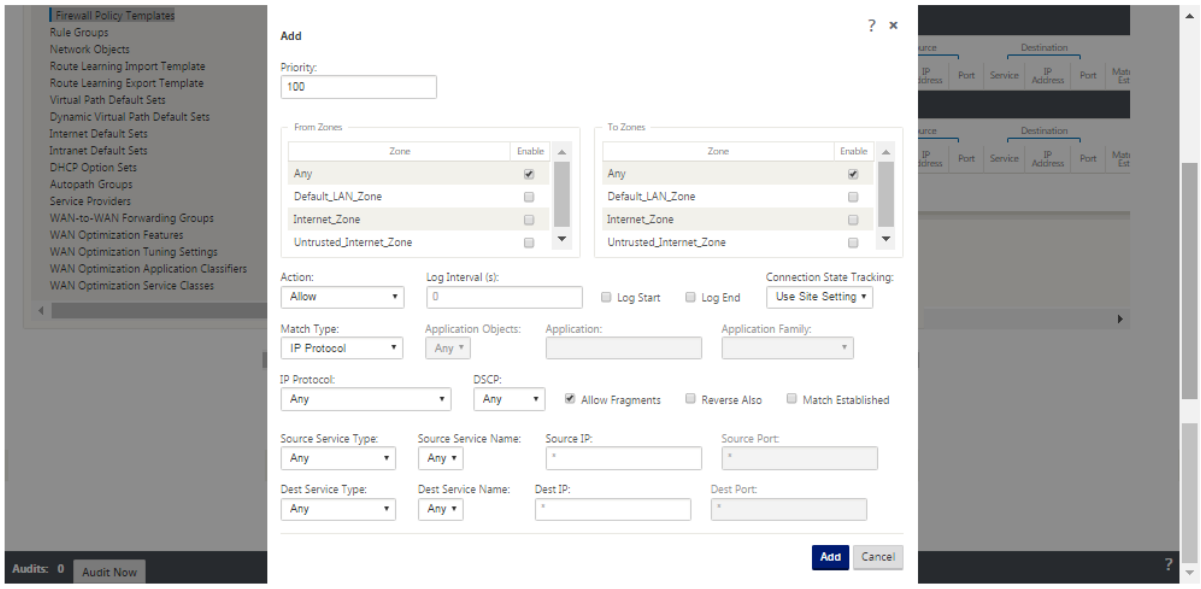
Die empfohlene Firewall-Konfiguration ist mit einer Standard-Firewall-Aktion, die zuerst alle verweigert und dann Ausnahmen hinzufügt. Dokumentieren und überprüfen Sie vor dem Hinzufügen von Regeln den Zweck der Firewall-Regel. Verwenden Sie nach Möglichkeit eine stateful Inspektion und Inspektion auf Anwendungsebene. Vereinfachen Sie die Regeln und eliminieren Sie redundante Regeln. Definieren und halten Sie einen Änderungsverwaltungsprozess ein, der Änderungen an den **Firewall-Einstellungen** verfolgt und überprüft. Richten Sie die Firewall für alle Appliances ein, um Verbindungen über die Appliance mithilfe der globalen Einstellungen zu verfolgen. Durch die Verfolgung von Verbindungen wird sichergestellt, dass Pakete ordnungsgemäß gebildet wurden und für den Verbindungsstatus geeignet sind. Erstellen Sie Zonen, die der logischen Hierarchie des Netzwerks oder der Funktionsbereiche der Organisation entsprechen. Denken Sie daran, dass Zonen global bedeutsam sind und es ermöglichen können, geografisch unterschiedliche Netzwerke als dieselbe Sicherheitszone zu behandeln. Erstellen Sie die spezifischsten Richtlinien, um das Risiko von Sicherheitslücken zu verringern, und vermeiden Sie die Verwendung von Any in Allow Regeln. Konfigurieren und pflegen Sie eine Vorlage für globale Richtlinien, um ein Basissicherheitsniveau für alle Appliances im Netzwerk zu schaffen. Definieren Sie Richtlinienvorlagen basierend auf den funktionalen Rollen von Appliances im Netzwerk und wenden Sie sie gegebenenfalls an. Definieren Sie Richtlinien an einzelnen Standorten nur bei Bedarf.

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. Deny ermöglicht, dass Pakete, die keiner Filterrichtlinie entsprechen, verworfen werden.

Standard-Verbindungsstatus-Tracking —Ermöglicht die bidirektionale Verfolgung des Verbindungsstatus für TCP-, UDP- und ICMP-Flows, die nicht mit einer Filterrichtlinie oder NAT-Regel übereinstimmen. Asymmetrische Flows werden blockiert, wenn dies 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 die Möglichkeit von asymmetrischen Flüssen an einem Standort besteht, wird empfohlen, dies auf Standort- oder Richtlinienebene und nicht global zu ermöglichen.

Zonen - Firewall-Zonen definieren die logische Sicherheitsgruppierung von Netzwerken, die mit dem Citrix SD-WAN verbunden sind. Zonen können auf virtuelle Schnittstellen, Intranetdienste, GRE Tunnel und LAN IPsec-Tunnel angewendet werden.



Sicherheitszone für WAN-Verbindungen

Nicht vertrauenswürdige Sicherheitszone sollte auf WAN-Verbindungen konfiguriert werden, die direkt mit einem öffentlichen (unsicheren) Netzwerk verbunden sind. Nicht vertrauenswürdig 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 der einzige andere zulässige Traffic-Typ. Diese Einstellung stellt auch sicher, dass nur verschlüsselter Datenverkehr von den Schnittstellen gesendet wird, die der Interfacegruppe zugeordnet sind.

Routing-Domänen

Routingdomänen sind Netzwerksysteme, die eine Reihe von Routern enthalten, die zur Segmentierung des Netzwerkverkehrs verwendet werden. Neu erstellte Vererben werden automatisch mit der standardmäßigen Routingdomäne verknüpft.

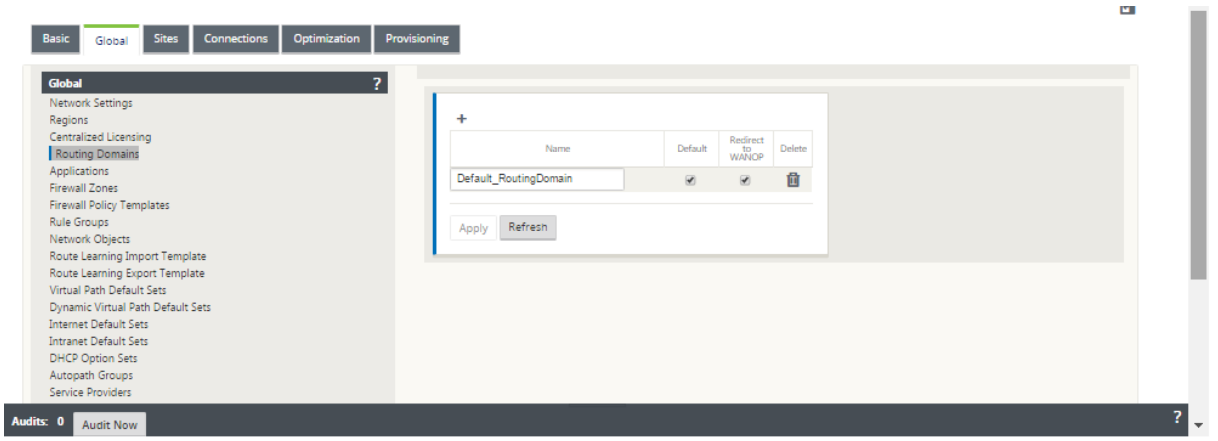
Konfigurationseditor > **Glob**

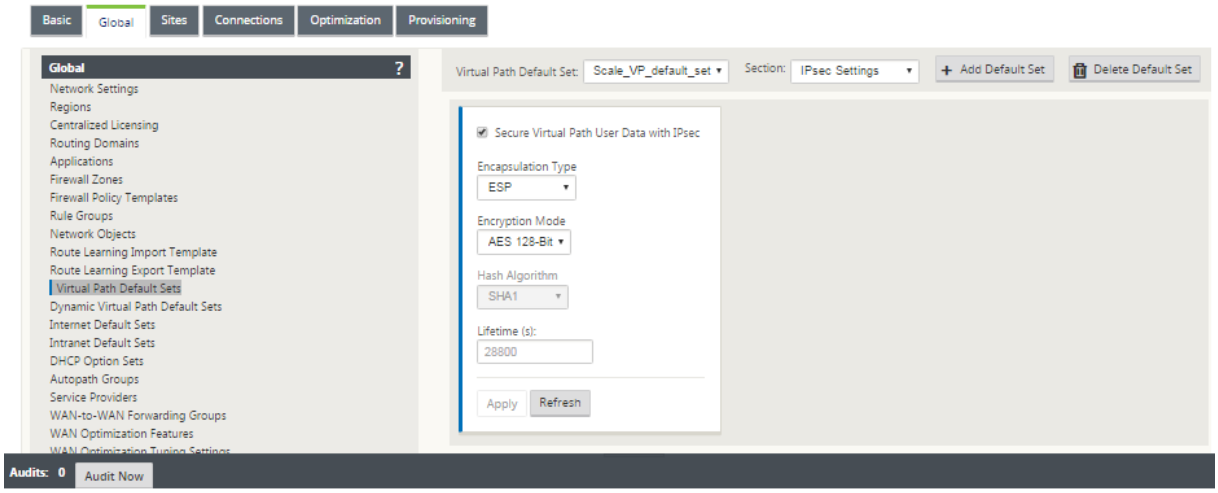
Domains weiterleiten

- Default_RoutingDomain

IPsec-Tunnel

- Standard-Sets
- 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.

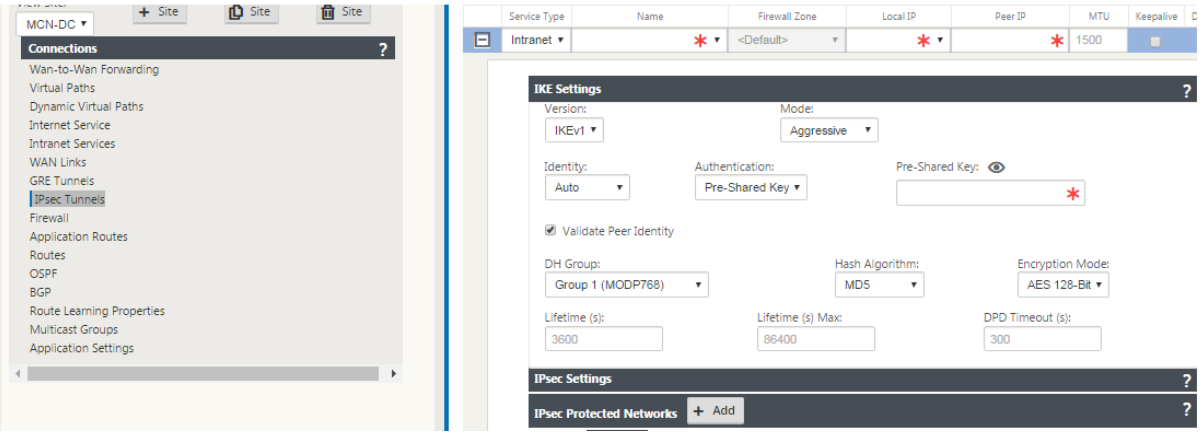
- Zu den Optionen für den Kapselungstyp gehören ESP - Daten werden gekapselt und verschlüsselt, ESP+Auth - Daten werden gekapselt, verschlüsselt und mit einem HMAC validiert, AH - Daten werden mit einem HMAC validiert.
- Der Verschlüsselungsmodus ist der Verschlüsselungsalgorithmus, der verwendet wird, 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 Aggressiv-Modus sein.
- Die Identität kann automatisch erfolgen, um Peer zu identifizieren, oder eine IP-Adresse kann verwendet werden, um die IP-Adresse des Peers manuell anzugeben.
- Die Authentifizierung ermöglicht die Pre-Shared Key-Authentifizierung oder das Zertifikat als Authentifizierungsmethode.
- Validate Peer Identity ermöglicht die Validierung der Peer-Identity 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.
- Der Hash-Algorithmus umfasst MD5, SHA1 und SHA-256. Für IKE-Nachrichten stehen Algorithmen zur Verfügung.
- Zu den Verschlüsselungsmodi gehören AES-128, AES-192 und AES-256-Verschlüsselungsmodi, die für IKE-Nachrichten verfügbar sind.
- Zu den IKEv2-Einstellungen gehören Peer-Authentifizierung und Integritätsalgorithmus.



Konfigurieren der Firewall

Die folgenden häufigen Probleme können durch Überprüfung der Upstream-Router- und Firewall-Konfiguration identifiziert werden:

- MPLS-Warteschlangen/QoS-Einstellungen: Stellen Sie sicher, dass der in UDP eingekapselte Datenverkehr zwischen virtuellen SD-WAN IP-Adressen aufgrund von **QoS-Einstellungen** auf den Zwischengeräten im Netzwerk nicht leidet.
- Der gesamte Datenverkehr auf den WAN-Verbindungen, die im SD-WAN-Netzwerk konfiguriert sind, 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 Bypass und dieselbe zugrunde liegende Verbindung verwenden muss, sollten ordnungsgemäße Bandbreitenreservierungen für SD-WAN-Verkehr auf dem Router vorgenommen werden. Außerdem sollte die Verbindungskapazität in der SD-WAN-Konfiguration entsprechend konfiguriert werden.
- Stellen Sie sicher, dass für den dazwischengeschalteten Router/die Firewall keine UDP-Flood- und/oder PPS-Grenzwerte durchgesetzt sind. Dadurch wird der Datenverkehr gedrosselt, wenn er über den virtuellen Pfad gesendet wird (UDP-gekapselt).

Routing

October 28, 2021

In diesem Artikel werden bewährte Routing für die Citrix SD-WAN-Lösung beschrieben.

Internet-/Intranet-Routingdienst

Wenn der Internetdienst nicht für internetgebundenen Datenverkehr konfiguriert ist und stattdessen entweder eine **lokale** Route oder eine **Passthrough-Route** konfiguriert ist, um den Gateway-Router zu 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 am MCN als **lokal** konfiguriert ist, wird sie von allen SD-WAN-Sites der Zweigstelle erlernt und standardmäßig als **Virtual Path Route** konfiguriert. Dies bedeutet, dass der internetgebundene Datenverkehr in der Zweige-Appliance über den virtuellen Pfad an MCN weitergeleitet wird.

Routing-Vorrang

Die Reihenfolge der Routing-Präzidenz:

- Präfixübereinstimmung: Die längsten Präfixe stimmen überein.
- Dienst: Lokal, Virtueller Pfaddienst, Internet, Intranet, Passthrough
- Kosten für die Route

Routing-Asymmetrie

Stellen Sie sicher, dass es keine Routing-Asymmetrie im Netzwerk gibt (die NetScaler SD-WAN-Appliance überträgt den Datenverkehr nur in eine Richtung). Dies führt zu Problemen mit der Firewall-Verbindungsverfolgung und Deep Packet Inspection.

QoS

October 28, 2021

Beachten Sie bei der Konfiguration von QoS Folgendes:

- Verstehen Sie Ihre Netzwerkverkehrsmuster und -anforderungen. Möglicherweise müssen Sie die **QoS-Klassenstatistiken**beobachten und die Warteschlangentiefe ändern und/oder den standardmäßigen Anteil an QoS-Klassen ändern, um Tail-Drops zu vermeiden, wie in den QoS-Statistiken gezeigt.
- Manchmal wird das gesamte Subnetz zur Vereinfachung der Konfiguration zu einer Regel hinzugefügt, 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

October 28, 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 beachten sollten:

- Konfigurieren Sie die **zulässige und physische** Rate als tatsächliche WAN-Verbindungsbandbreite. In Fällen, in denen die gesamte WAN-Link-Kapazität nicht von der SD-WAN-Appliance verwendet werden soll, ändern Sie die **zulässige** Rate entsprechend.
- Wenn Sie sich über die Bandbreite nicht sicher sind und die Verbindungen nicht zuverlässig sind, können Sie die **Auto Learn-Funktion** aktivieren. Die **Auto-Learn-Funktion lernt** nur die zugrunde liegende Linkkapazität 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 zur **adaptiven 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:
  - Verlust-Einstellungen
  - Deaktivieren Instabilität Sensitive
  - Zeit zum Schweigen
- Verwenden Sie **das Diagnose-Tool**, um die Gesundheit/Kapazität des Links zu überprüfen
- Wenn SD-WAN im **Einarmmodus** bereitgestellt wird, stellen Sie sicher, dass Sie die physische Kapazität der zugrunde liegenden Verbindung nicht überlaufen.

Überprüfung des ISP-Linkzustands

Für neue Bereitstellungen, vor der SD-WAN-Bereitstellung und beim Hinzufügen einer neuen ISP-Verbindung zur vorhandenen SD-WAN-Bereitstellung:

- Überprüfen Sie den Linktyp. Zum Beispiel; MPLS, ADSL, 4G.
- Eigenschaften des Netzwerks. Zum Beispiel - Bandbreite, Verlust, Latenz und Jitter.

Diese Informationen helfen bei der Konfiguration des SD-WAN-Netzwerks gemäß Ihren Anforderungen.

Netzwerktopologie

Es wird allgemein 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 Sichtbarkeit über die Link-Auslastung hat, besteht die Möglichkeit, dass SD-WAN die Verbindung überzeichnet, was zu Leistungs- und PATH-Problemen führt.

Provisioning

Punkte, die bei der Bereitstellung von SD-WAN zu beachten sind:

- Standardmäßig erhalten alle Zweigstellen 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.

FAQ

October 28, 2021

Hohe Verfügbarkeit

Was ist der Unterschied zwischen High Availability und Secondary (Geo) Appliance?

- Hochverfügbarkeit gewährleistet Fehlertoleranz. Sekundäre (Geo) Appliance ermöglicht Disaster Recovery.
- Hochverfügbarkeit kann für die MCN-, RCN- und Zweigstellen konfiguriert werden. Sekundäre (Geo) -Appliance kann nur für MCN und RCNs konfiguriert werden.
- Hochverfügbarkeits-Appliances werden am selben Standort oder an demselben geografischen Standort konfiguriert. Eine Zweigeinheit an einem anderen geografischen Standort ist als sekundäre (Geo) MCN/RCN-Appliance konfiguriert.
- Primäre und sekundäre Geräte mit hoher Verfügbarkeit sollten dieselben Plattformmodelle sein. Die sekundäre (Geo) -Appliance kann dasselbe Plattformmodell wie die primäre MCN/RCN sein oder nicht.
- Hochverfügbarkeit hat eine höhere Priorität gegenüber Sekundär (Geo). Wenn eine Appliance (MCN/RCN) mit Hochverfügbarkeit und sekundärer (Geo) -Appliance konfiguriert ist, wird die sekundäre Hochverfügbarkeits-Appliance aktiv, wenn die Appliance ausfällt. Wenn beide Hochverfügbarkeits-Appliances ausfallen oder der Rechenzentrumsstandort abstürzt, wird die sekundäre (Geo) -Appliance aktiv.
- Bei Hochverfügbarkeit erfolgt die primäre/sekundäre Umschaltung je nach Bereitstellung mit hoher Verfügbarkeit sofort oder innerhalb von 10-12 Sekunden. Die primäre Umschaltung von MCN/RCN zu Sekundär (Geo) MCN/RCN erfolgt nach 15 Sekunden, nachdem die primäre inaktiv ist.

- Mit der Hochverfügbarkeitskonfiguration können Sie die primäre Rückgewinnung konfigurieren. Sie können die primäre Rückgewinnungs für Secondary (Geo)-Appliance nicht konfigurieren, die primäre Rückgewinnung erfolgt automatisch, nachdem das primäre Gerät zurück ist und der Holdtimer abläuft.

Upgrade in einem Schritt

> **Hinweis**
>
> Die WANOP, SVM und XenServer Supplemental/HFS werden als Betriebssystemkomponenten angesehen.

Sollte ich *.tar.gz* oder ein einstufiges *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 betroffenen Plattformen, um die SD-WAN-Software auf 9.3.x zu aktualisieren. Nachdem die SD-WAN-Software auf Version 9.3.x aktualisiert wurde, führen Sie das Änderungsmanagement über das *ZIP*-Paket durch, um Softwarepakete für Betriebssystemkomponenten zu übertragen/ein Staging durchzuführen. Nach der Aktivierung überträgt der MCN Betriebssystemkomponenten für alle relevanten Zweige.

Nach dem Upgrade auf 9.3.0 mit einem einzigen Schritt Upgrade-Paket (.zip-Datei) muss ich ausführen.*Upg-Upgrade* auf jeder Appliance?

Nein, das Update/Upgrade der Betriebssystemsoftware wird durch das einstufige *Upgrade-.zip-Paket* übernommen und gemäß den Planungsdetails installiert, die Sie in den Änderungsverwaltungseinstellungen der jeweiligen Sites angegeben haben.

Warum sollte ich *.tar.gz* gefolgt vom *.zip-Paket* verwenden, um von früher als 9.3 auf 9.3.x zu aktualisieren, und warum nicht direkt das *.zip-Paket* von 9.3.x verwenden?

Das Single Step-Upgrade-Paket wird ab 9.3.0.161 unterstützt und in früheren Versionen (vor Version 9.3) wird dieses Paket nicht erkannt. Wenn das einstufige *Upgrade-ZIP-Paket* in den Posteingang des Änderungsmanagements hochgeladen wird, gibt das System einen Fehler aus, der besagt, dass das Paket nicht erkannt wird. Aktualisieren Sie daher zuerst die SD-WAN-Software auf Version 9.3 oder höher und führen Sie dann das Änderungsmanagement mithilfe des durch.*Zip-Paket*.

Wie werden die Betriebssystemkomponenten durch ein einstufiges Upgrade installiert, wenn.*Upg-Upgrade* wird nicht durchgeführt?

Der MCN führt eine Übertragung/ein Staging der Softwarepakete für Betriebssystemkomponenten basierend auf dem Appliance-Modell durch, nachdem das Änderungsmanagement mit dem einstufigen *Upgrade-ZIP-Paket* abgeschlossen wurde. Nach der Aktivierung beginnt der MCN mit der Übertragung/dem Staging der Softwarepakete der Betriebssystemkomponenten für die Zweige, die sie für das geplante Update/Upgrade benötigen.

Wie installiere ich Betriebssystemkomponenten, ohne für spätere Installationen zu planen?

Stellen Sie den Wert des **Wartungsfensters** für die sofortige Installation der Betriebssystemkomponenten auf **0** ein.

> **Hinweis**
>
> Die Installation beginnt erst, wenn die Appliance das gesamte Paket erhalten hat, das für den Standort benötigt wird, auch wenn der Wert des **Wartungsfensters** auf '**0**'festgelegt ist.

Was ist der Nutzen der Planungsinstallation? Kann ich die Zeitplananweisungen 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 einstufigen Upgrade müssen Sie sich nicht bei jeder Appliance anmelden, um ein Upgrade der Betriebssystemkomponenten durchzuführen, und 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 "Änderungsverwaltungseinstellungen"standardmäßig nach dem geplanten Datum angezeigt und was bedeutet dies?

Auf der Seite "**Änderungsverwaltungseinstellungen** "werden die standardmäßigen Planungsinformationen angezeigt, die *"Start": "2016-05-21 21:20:00", "Fenster": 1, "Wiederholung": 1, "Einheit" : "Tage"*"sind. Wenn das Datum ein vergangenes Datum ist, bedeutet dies, dass die geplante Installation auf der Uhrzeit und anderen Parametern wie Wartungsfenster, Wiederholungsfenster und Einheit und nicht auf dem Datum basiert.

Auf was ist das standardmäßige Installations-Datum/die Uhrzeit des Zeitplans eingestellt, ist es generisch oder von der lokalen

Standardmäßig sind die Planungsdetails *auf '2016-05-21 um 21:20:00 Uhr (Wartungsfenster von 1 Stunde und alle 1 Tag wiederholt)* 'festgelegt. Dieses Detail ist vom Standort der lokalen Appliance abhängig.

Wie kann ich OS Components sofort installieren, ohne auf das Wartung/das geplante Fenster zu warten?

Stellen Sie den Wert des **Wartungsfensters** auf der Seite **Änderungsverwaltungseinstellungen** auf **0** ein. Dadurch wird die geplante Installationszeit außer Kraft gesetzt.

Welches Paket sollte ich für ein Upgrade verwenden, wenn die aktuelle Softwareversion 9.3.x oder höher ist?

Verwenden Sie ein einstufiges Upgrade-*ZIP*-Paket, um auf höhere Versionen zu aktualisieren, wenn die aktuelle Softwareversion 9.3.x oder höher ist.

Wann findet das Übertragen/Staging der Betriebssystemkomponentendateien auf die Zweige statt?

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 Betriebssystemkomponentendateien, ist es plattformabhängig oder alle Zweige erhalten sie?

Appliances, die auf Hypervisor basieren, wie **SD-WAN - 400, 800, 1000, 2000 SE** und Bare Metal **SD-WAN - 2100**, die mit einer EE-Lizenz ausgeführt werden, erhalten Betriebssystemkomponenten zum Upgrade.

Wie funktioniert die Terminplanung?

Standardmäßig sind die Planungsdetails um *21:20:00 Uhr auf 2016-05-21 festgelegt (Wartungsfenster von 1 Stunde und wird alle 1 Tag wiederholt) und es bedeutet, dass das System jeden*Tag prüft, ob neue Software für die Installation verfügbar ist, da der Wiederholungswert auf **1 Tage** festgelegt ist und gewartet wird Fenster von **1 Stunde** und die Installation wird ab dem **21.05.2016** um **21:20:00 Uhr**(lokale Appliance-Zeit) ausgelöst/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 mit der Maus darüber fahren, 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 auf der Seite MCN **Change Management**-Einstellungen. Für RCN-Filialen müssen Sie sich bei den jeweiligen RCN anmelden und die Zeitplandetails festlegen.

Woher erhalte ich den Status der geplanten Installation?

Der Status der geplanten Installation für RCN kann auf der Seite MCN **Change Management-Einstellungen** abgerufen werden. Für RCN-Filialen müssen Sie sich bei den jeweiligen RCN anmelden, um den Status abzurufen.

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

Show 100 entries Search: Edit Selected Refresh

Site Name	Scheduling Information	Status	Edit
GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries Previous 1 Next

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 Datei *tar.gz* für ein Upgrade verwenden, dies 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 Appliance anmelden. Ab Version 9.3 Version 1 wird die Seite **Betriebssystemsoftware aktualisieren** abgeschrieben. Infolgedessen können Sie das Änderungsmanagement durchführen, indem Sie das *.zip-Paket* verwenden, um Betriebssystemkomponenten zu aktualisieren.

Wie können wir die aktuellen laufenden Versionen von Betriebssystemkomponenten validieren?

Jetzt können Sie die aktuell laufenden Versionen von Betriebssystemkomponenten nicht über die Benutzeroberfläche validieren. Sie können sich von jeder Konsole aus anmelden oder STS dazu bringen, diese Informationen anzuzeigen.

Welchen Unterschied würde es machen, wenn ich Bare-Metal-Geräte in meinem Netzwerk hätte? Hat die Planung Auswirkungen auf Bare-Metal-/Virtuelle Appliances?

Bare-Metal-Appliances wie **SD-WAN —410.2100.4100.5100 SD-WAN** führen nur SD-WAN-Software

aus. Bare Metal Appliances benötigen keine OS-Komponentenpakete. Diese Plattformen werden hinsichtlich des Softwarebedarfs auf Augenhöhe mit SD-WAN VPX-SE Appliances behandelt. Der MCN überträgt keine BS-Komponentenpakete auf diese Appliances. Das Festlegen von Planungsinformationen wird für diese Appliances nicht wirksam, da sie keine Betriebssystemkomponenten haben, die aktualisiert werden müssen.

Wie funktioniert SSU in einer Hochverfügbarkeitsumgebung/-bereitstellung?

Bei der Hochverfügbarkeitsbereitstellung bei MCN haben wir eine Einschränkung, bei der der aktive MCN-Switch die Rolle des primären MCN während des Change Managements und des Standby/Secondary MCN übernimmt. In diesem Fall können Sie das Änderungsmanagement erneut mit dem *ZIP-Paket* auf dem aktiven MCN für die Pakete durchführen oder zurück zum primären MCN wechseln, indem Sie die Rolle des aktiven MCN umschalten, sodass der ursprüngliche primäre MCN die Rolle übernehmen kann, damit für die BS-Komponentenpakete auf anderen Zweigen ein Staging durchgeführt wird.

Wie funktioniert ein einstufiges Upgrade in einer Hochverfügbarkeitsumgebung/Bereitstellung?

Bei der Durchführung eines einstufigen Upgrades bei der Bereitstellung mit hoher Verfügbarkeit wird die Rolle des primären MCN und des Standby-MCN umgeschaltet. Das ist eine Einschränkung. Führen Sie in diesem Fall das Änderungsmanagement erneut mit dem *.zip-Paket* auf dem aktiven MCN durch. Alternativ können Sie zum primären MCN zurückkehren, indem Sie die Rolle des aktiven MCN umschalten, sodass der ursprüngliche primäre MCN BS-Komponentenpakete in die Zweige stellen kann.

Unterstützt ein einstufiges Upgrade für die Zero-Touch-Bereitstellung, um die Appliances neu zu starten?

Ja, es kann verwendet werden.

Kann ich ein einstufiges Upgrade verwenden, um meine eigenständige WANOP-Appliance zu aktualisieren?

Nein.

Kann ich ein einstufiges Upgrade verwenden, um die eigenständige WANOP-Appliance im Zwei-Box-Modus zu aktualisieren?

Nein. Nur eine SD-WAN-Appliance, die Teil des Zwei-Box-Modus ist, wird aktualisiert und nicht die WANOP-Standalone-Appliance.

Welches Paket sollte ich verwenden, um auf ein mehrstufiges Netzwerk zu aktualisieren?

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 für RCN und das RCNS, das Softwarepaket für die jeweiligen Zweigstellen.

Nach dem Hochladen der Datei *ns-sdw-sw-<release-version>.zip* sehe ich nur ein Plattformmodell unter aktueller Software?

Ab Release 10.0 wird Unterstützung für Skalenarchitektur eingeführt, um die Verarbeitung von einstufigen Upgrades zu beschleunigen. Unter aktueller Software können Sie nur das MCN-Plattformmodell sehen. Andere Appliance-Pakete werden aufgelistet/angezeigt/verarbeitet, wenn Sie die Schaltfläche **Verify** oder **Stage Appliance** wählen.

Für welche Pakete wird bei VPX/VPXL/Bare-Metal-Appliances für RCN ein Staging durchgeführt?

Das Paket wird in RCNs bereitgestellt, da RCNs Branches von jedem Plattformmodell sein können. Daher brauchen sie alle Pakete.

Wie erhält meine Zweigstelle hinter dem RCN OS-Komponentenpakete, wenn RCN eine VPX-Appliance ist und Zweig eine Appliance ist, die diese Pakete benötigt?

RCN stellt das relevante Paket nach der Aktivierung des SD-WAN VW-Softwarepakets an den Zweig bereit, der die Betriebssystemkomponentenpakete benötigt.

Kann ich während des Stagings "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 **Unvollständig ignorieren** klicken. Dies aktiviert die Schaltfläche **Weiter** und der Fortschrittsbalken wird angezeigt. Diese Option wird für Szenarien bereitgestellt, in denen die Site nicht erreichbar ist und das Änderungsmanagement immer noch darauf wartet, dass das Staging für diese Site abgeschlossen ist, sodass Benutzer mit der nächsten Stufe fortfahren können, indem sie den Stagestatus ignorieren und mit der Aktivierung fortfahren. Nachdem die Site hochgekommen ist, führt MCN ein Staging des Pakets nach Abschluss der Aktivierung durch.

Teilweise Softwareupgrade

Was ist ein teilweises Site-Upgrade und wie kann ich es verwenden?

Ein teilweises Site-Software-Upgrade ist eine neue Funktion, die in Version 10.0 eingeführt wurde. Sie können für eine neuere Version von Version 10.x vom MCN aus ein Staging durchführen und die gestagte Softwareversion auf der Seite **Local Change Management** auf ausgewählten Standorten/Zweigen aktivieren. Stellen Sie vor der Aktivierung von bereitgestellter Software vor der Standort/Zweigstelle 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 sich dafür entscheiden, teilweise Site-Upgrades zuzulassen, 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.

Unten ist der Anwendungsfall/das Szenario, in dem ein teilweises Site-Software-Upgrade verwendet werden kann:

Überprüfen Sie, ob ein Software-Patch mit relevanten Änderungen kompatibel ist und für eine bestimmte Site funktioniert (wo 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 reparieren, 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 J
- 11.0.x bis 11.0.y
- Alle oben genannten

Ein partielles Site-Software-Upgrade ist nur anwendbar, wenn auf der Appliance Softwareversion 10.x und neuer ausgeführt wird und in derselben Hauptversion der Software verwendet werden kann. Es kann zwischen den Releases 10.0 bis 10.0.x/10.x verwendet werden. Nur im Rahmen eines teilweisen Standort-Software-Upgrades kann die Konfiguration nicht geändert werden.

Kann ich neue Funktionen testen, die im Rahmen eines partiellen Software-Upgrades getestet werden sollen, indem ich sie über die Konfiguration aktiviere?

Nein, ein teilweises Software-Upgrade erfordert, dass jetzt Active und Staged Config identisch sind. Nur die Softwareversion kann sich ändern.

Kann ich das partielle Software-Upgrade für RCN deaktivieren?

Nein, ein partielles Software-Upgrade kann nur von MCN aus aktiviert oder deaktiviert werden. Bei RCN befindet sich die Funktion im schreibgeschützten Modus.

Kann ich Partial Software Upgrade verwenden, wenn ich als 9.3.x und 10.0.x aktiv bin?

Nein, die Appliance sollte auf Version 10.0 als aktive Software laufen.

Was passiert, wenn die Option Partielle Software-Upgrades von MCN deaktiviert ist, während einige Zweige bereits über diese Funktion aktualisiert wurden?

MCN sendet eine Benachrichtigung an alle Appliances im Netzwerk, dass die Funktion des partiellen Software-Upgrades deaktiviert ist, und dann werden alle Appliances im Netzwerk von MCN automatisch korrigiert, um der aktiven und Staging-Version zu entsprechen. Beachten Sie jedoch, dass MCN erwartet, dass auf die Option "Staged aktivieren"auf der Aktivierungsseite von **Change Management**geklickt wird. Sie können das Netzwerk aktivieren, indem Sie auf die Schaltfläche "**Staged aktivieren** "klicken oder auf "**Vorbereitung ändern** "klicken, um den Status abzubrechen, indem Sie die Bestätigung akzeptieren.

Änderungsmanagement —Rollback

Was ist eine Rollback-Funktion im Change-Management-Prozess?

Ab Release 9.3 ermöglicht die Rollback-Funktion für die Änderungsverwaltung das Zurücksetzen 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. Wenn während dieses Intervalls die folgenden Bedingungen erfüllt sind (vorausgesetzt, der Benutzer hat die Funktion aktiviert), wird die Staged-Konfiguration aktiviert. Die Active Software wird auf Staged zurückgesetzt.

Was sind die Kriterien für den Neustart der Konfiguration?

Das Rollback tritt auf, wenn die folgenden Szenarien auftreten:

1. MCN - Wenn der Dienst t2_app nach einer Änderung der Konfigurations-/Software aufgrund eines Absturzes innerhalb eines 30-Minuten-Intervalls deaktiviert wird.
2. MCN - Nach Konfigurations-/Softwareänderung, wenn der Virtual Path-Dienst nach der Aktivierung 30 Minuten oder länger ausgefallen ist. Die Rollback-Funktion wird an den Standorten initiiert.
3. Site - Wenn die Site nach der Änderung der Konfiguration/Software ihre Kommunikation mit MCN verliert, wird die Rollback-Funktion initiiert.
4. Site - Nach dem Konfigurations-/Softwarewechsel wird der 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 darüber informiert, dass ein Rollback stattgefunden hat?

Ein gelbes Banner oben in der GUI, das besagt, dass Config aufgrund entsprechender Fehler zurückgesetzt wird, wird angezeigt. Außerdem können Sie sehen, dass es sich um eine Statustabelle für die Änderungsverwaltung Es zeigt **einen Konfigurationsfehler** oder **Softwarefehler** an, der der Site entspricht, für die ein Rollback aufgetreten ist.

Werden Config und Software beide zurückgerollt?

Ja, wenn ein Software-Upgrade zusammen mit der Konfiguration ebenfalls durchgeführt wird und ein Rollback-Szenario angetroffen wird, wird auch Software zurückgesetzt.

Was passiert, wenn es ein Problem in MCN gibt und es abstürzt oder die Konnektivität mit allen Standorten verliert?

Das gesamte Netzwerk wird mit Ausnahme von MCN zurückgesetzt. Die Benachrichtigung wird angezeigt, und alle Websites zeigen den Rollback-Status im Abschnitt Änderungsmanagement an. Sie können das Problem auf MCN manuell lösen.

Können wir diese Funktion deaktivieren?

Ja, wir können diese Funktion kurz vor der Aktivierung deaktivieren. Standardmäßig ist diese Funktion jedoch aktiviert.

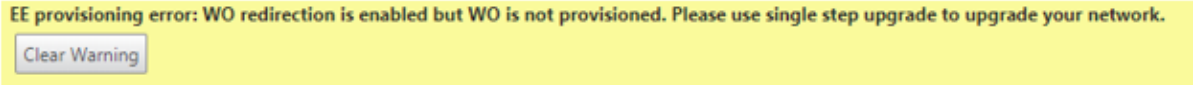
Wie interagiert Rollback mit partiellem Software-Upgrade, wenn ich ein mehrstufiges Netzwerk habe?

- Wenn ein teilweises Software-Upgrade deaktiviert ist und ein Standort in einer Region (oder dem RCN) zurückkehrt, wird die Region mit dem Problem zurückgesetzt, und nach Abschluss wird der Rollback an den MCN weitergegeben. Infolgedessen wurden 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 beim RCN nicht automatisch verwerfen kann.
- Wenn ein teilweises Software-Upgrade aktiviert ist und ein Standort in einer Region (oder dem RCN) zurückgesetzt wird, wird nur diese Region zurückgesetzt. Das Rollback-Ereignis wird nicht auf den MCN übertragen. Infolgedessen verlässt der MCN die Region. Der MCN zeigt kein Rollback-Banner an und rollt sich selbst oder das Netzwerk nicht zurück.

In beiden Szenarien zeigt der RCN das Rollback-Banner an, bis es entlassen wird. Weil es von MCN nicht automatisch abgewiesen werden kann.

2100 Premium (Enterprise) Edition

Was zeigt die folgende Meldung an, wenn eine 2100 EE-Appliance auf Release 10.0 aktualisiert wird?



Die Appliance hat eine EE-Lizenz oder die WANOP-Umleitung ist von MCN aktiviert. Sie können die Installation von WANOP-Komponenten planen, um die Provisioning von WANOP-Funktionen auf dieser Plattform zu starten.

Verwandte Informationen

- Zero Touch-Bereitstellung über LTE
- Konfigurieren des sekundären MCN in HA

Referenzmaterial

October 28, 2021

Anwendungssignaturbibliothek

Eine Liste der Anwendungen, die die Citrix SD-WAN Appliances mithilfe der Deep Packet Inspection identifizieren können.