



Citrix SD-WAN 11.5

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 für Citrix SD-WAN 11.5	6
Neue Benutzeroberfläche für SD-WAN-Appliances	9
Auswirkungen auf das Citrix SD-WAN 11.5-Release-Upgrade	42
Systemanforderungen	42
SD-WAN-Plattformmodelle	44
Upgradepfad	45
Konfiguration	46
Konfigurieren der LTE-Funktionalität auf 210 SE LTE-Appliance	76
Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Appliance	89
Konfigurieren eines externen USB-LTE-Modems	100
Bereitstellungen	104
Checkliste und Bereitstellung	105
Bewährte Methoden	106
Gateway-Modus	113
Inlinemodus	122
Virtueller Inline-Modus	123
Erstellen eines SD-WAN-Netzwerks	124
Hohe Verfügbarkeit	126
Hochverfügbarkeit des Edge-Modus mit Glasfaser-Y-Kabel aktivieren	132
Keine Berührung	134
AWS	139
Azure	140
Bereitstellung in einer Region	141

Bereitstellung in mehreren Regionen	142
Konfigurationshandbuch für Citrix Virtual Apps and Desktops s-Workloads	143
Domänennamensystem	156
DHCP	158
Dynamische PAC-Dateianpassung	162
GRE Tunnel	165
In-Band- und Backup-Management	165
Internetzugriff	171
Gehostete Firewalls	176
Verknüpfungsaggregationsgruppen	184
Verknüpfen Zustandspropagierung	187
Mess- und Standby-WAN-Verbindungen	188
Office 365-Optimierung	197
Optimierung von Citrix Cloud und Gateway Service	206
PPPoE-Sitzungen	211
Qualität der Dienstleistung	216
Berichterstellung	238
Routing	247
SD-WAN-Überlagerungsrouting	249
Routingdomäne	270
Routingdomäne konfigurieren	271
Verwenden von CLI für den Zugriff auf Routing	272
Dynamisches Routing	272
OSPF	276

BGP	282
iBGP	285
eBGP	285
Anwendungsrouten	286
Routenfilterung	288
Routenzusammenfassung	289
Protokollpräferenz	291
Multicast-Routing	291
Routenkosten für virtuelle Pfade konfigurieren	295
Konfigurieren des Virtual Router-Redundanzprotokolls	297
Routing-Unterstützung für die LAN-Segmentierung	301
Domänendienst für den übergreifenden Routing	302
ECMP Load Balancing	303
Sicherheit	304
IPsec-Tunnelterminierung	305
Citrix SD-WAN Integration mit AWS Transit Gateway	306
So zeigen Sie die IPsec-Tunnelkonfiguration an	312
IPsec-Überwachung und -Protokollierung	314
Berechtigung für nicht-virtuelle IPsec-Pfadrouten	317
FIPS-Konformität	318
Secure Web Gateway für Citrix SD-WAN	318
Zscaler Integration mit GRE-Tunneln und IPsec-Tunneln	320
Unterstützung der Firewall-Verkehrsumleitung mithilfe von Forcepoint in Citrix SD-WAN	324
Palo Alto Integration mit IPsec-Tunneln	327

Stateful Firewall und NAT-Unterstützung	328
Globale Firewall-Einstellungen	329
Erweiterte Firewall-Einstellungen	329
Zonen	329
Richtlinien	331
Netzwerkadressübersetzung (NAT)	331
Statische NAT	332
Dynamische NAT	338
Konfigurieren des virtuellen WAN-Dienstes	343
Konfigurieren der Firewall-Segmentierung	344
Zertifikatauthentifizierung	348
AppFlow und IPFIX	349
SNMP	357
Administrative Schnittstelle	360
NDP-Router-Werbung und Präfix-Delegationsgruppe	365
Anleitungen	366
Konfiguration der Zugriffsschnittstelle	367
Virtuelle IP-Adressen konfigurieren	367
GRE Tunnel konfigurieren	368
Dynamische Pfade für Zweigkommunikation einrichten	368
WAN-zu-WAN-Weiterleitung	370
Überwachung und Fehlerbehebung	370
Virtuelles WAN überwachen	371
Statistische Informationen anzeigen	372

Anzeigen von Flussinformationen	375
Anzeigen von Berichten	379
Firewall-Statistiken anzeigen	386
Diagnose	389
Verbesserte Pfadzuordnung und Bandbreitennutzung	406
Fehlerbehebung bei Management-IP	411
Sitzungsbasierte HTTP-Benachrichtigungen	413
Aktive Bandbreitentests	419
Adaptive Bandbreitenerkennung	421
Bewährte Methoden	422
Sicherheit	423
Routing	430
QoS	431
WAN-Links	431
FAQ	433
Referenzmaterial	442

Versionshinweise für Citrix SD-WAN 11.5

November 16, 2022

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für Citrix SD-WAN 11.5 bestehen.

Hinweise

Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisories finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Verbesserungen und Änderungen, die in SD-WAN 11.5 verfügbar sind.

Sonstiges

[Spezifikationen für Citrix SD-WAN 11.5](#)

- Citrix SD-WAN 11.5.0 ist eine Version mit eingeschränkter Verfügbarkeit, die nur für bestimmte Kunden-/Produktionsbereitstellungen empfohlen und unterstützt wird.
- SD-WAN 11.5.0 unterstützt keine Bereitstellungen für Advanced Edition (AE), Premium Edition (PE) und WAN-Optimierung.
- SD-WAN 11.5.0 unterstützt nur die in [SD-WAN-Plattformmodellen und Softwarepaketen](#) genannten Plattformen.
- SD-WAN 11.5.0 unterstützt Citrix SD-WAN Center oder Citrix SD-WAN Orchestrator nicht für on-premises.
- SD-WAN 11.5.0-Firmware ist auf der Seite Citrix Downloads nicht verfügbar.
- SD-WAN 11.5.0 ist nur über den Citrix SD-WAN Orchestrator Service und nur für ausgewählte geografische POPs verfügbar.
- Stellen Sie sicher, dass Sie die erforderlichen Genehmigungen und Anleitungen von Citrix Product Management/Citrix Support einholen, bevor Sie 11.5.0 in einem Produktionsnetzwerk bereitstellen.

[NSSDW-38486]

Der Citrix SD-WAN Orchestrator Service ersetzt den SD-WAN-Konfigurationseditor:

Ab Version Citrix SD-WAN 11.5 werden SD-WAN-Konfigurationseditor und SD-WAN Center durch den Citrix SD-WAN Orchestrator Service ersetzt. Der Citrix SD-WAN Orchestrator Service unterstützt alle Konfigurationen, die derzeit über den SD-WAN-Konfigurationseditor ausgeführt werden. Weitere Informationen zum Citrix SD-WAN Orchestrator Service finden Sie unter [Citrix SD-WAN Orchestrator Service](#).

[NSSDW-33528]

IPv6-Unterstützung:

Ab Version Citrix SD-WAN 11.5.0 unterstützen die folgenden Datenebenenfunktionen von Citrix SD-WAN-Appliances die IPv6-Adresse:

- [Anwendungsrouten](#)
- [Optimierung von Citrix Cloud und Gateway Service](#)
- [Domännennamenbasierte Anwendungsklassifizierung](#)
- [Dynamische PAC-Dateianpassung](#)
- [Dynamisches Routing](#)
- [Firewall-StandardEinstellungen](#)
- [Multicast](#)
- [Office 365-Optimierung](#)
- [PPPoE](#)
- [Site-Berichte —Routing-Protokolle](#)
- [VRRP](#)

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

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

Verbesserungen bei der Überwachung:

Die folgenden Monitoring-Dashboards wurden verbessert und sind auf der neuen Appliance-Benutzeroberfläche verfügbar:

- [Transparente DNS-Weiterleitung](#)
- [Firewall-Verbindungen, Firewallfilter, Firewall NAT](#)
- [IGMP, IGMP-Proxy, IGMP-Statistik](#)
- [IKE, IPsec](#)

- [Multicastgruppe, Multicastgruppenquelle, Multicastgruppenziel](#)
- [PPPoE-Sitzungen](#)
- [VRRP](#)

[NSSDW-33763]

Plattform und Systeme

[Referenzmaterial - Signaturbibliothek der Anwendung](#)

Die Signaturbibliothek der DPI-Anwendung wurde aktualisiert.

[NSSDW-38209]

Behobene Probleme

Die Probleme, die in SD-WAN 11.5 behoben werden.

Sonstiges

Der Status der Verwaltungsschnittstelle einiger SD-WAN-Appliances wurde auf der Seite **Ethernet-Schnittstelleneinstellungen der Benutzeroberfläche** als Heruntergefahren angezeigt. Dieses Problem trat auf, als bei einigen Appliances, die In-Band-Verwaltung unterstützt hatten, die Option zur Verwendung von Out-of-Band verfügbar war. Daher verwendeten die Appliances eine Out-of-Band-Verwaltungsschnittstelle, um auf den SD-WAN Orchestrator Service zuzugreifen.

[NSSDW-37028]

Bekannte Probleme

Die Probleme, die in SD-WAN 11.5 Version bestehen.

Im Falle einer skalierten Bereitstellung bei Konfigurationsänderungen an einem Standort oder einer WAN-Verbindung führt der Neustart der Routing-Engine dazu, dass BGP-Sitzungen flackern.

[SDWANHELP-2594]

Eine SD-WAN-Apliance ist unerwartet abgestürzt. Dieses Problem trat in folgenden Fällen auf:

- Während eines Software-Upgrades floss IPv6-Multicast-Datenverkehr.
- IPv6-Multicast-Datenverkehr wurde über einen Intranet-GRE-Tunnel bezogen und mithilfe der MLDv2-Proxykonfiguration auf mehrere Zweige über den virtuellen Pfad repliziert.

Problemumgehung: Deaktivieren Sie den IPv6-Multicast-Verkehr während des Software-Upgrades und aktivieren Sie ihn, sobald das Upgrade erfolgreich ist

[NSSDW-38495]

Neue Benutzeroberfläche für SD-WAN-Appliances

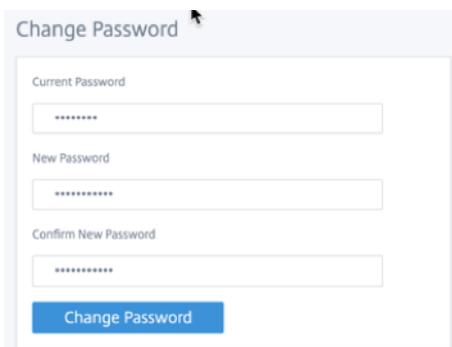
August 29, 2022

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.

Ab der Citrix SD-WAN 11.4-Version ist die Neue Benutzeroberfläche standardmäßig auf allen Citrix SD-WAN Appliances aktiviert, die als Clients konfiguriert sind.

Hinweis

- Durch die Provisioning der Citrix SD-WAN Appliances 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.



The screenshot shows a web-based form titled "Change Password". It contains three text input fields, each with a masked password field (represented by asterisks). The fields are labeled "Current Password", "New Password", and "Confirm New Password". Below the fields is a blue button labeled "Change Password".

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

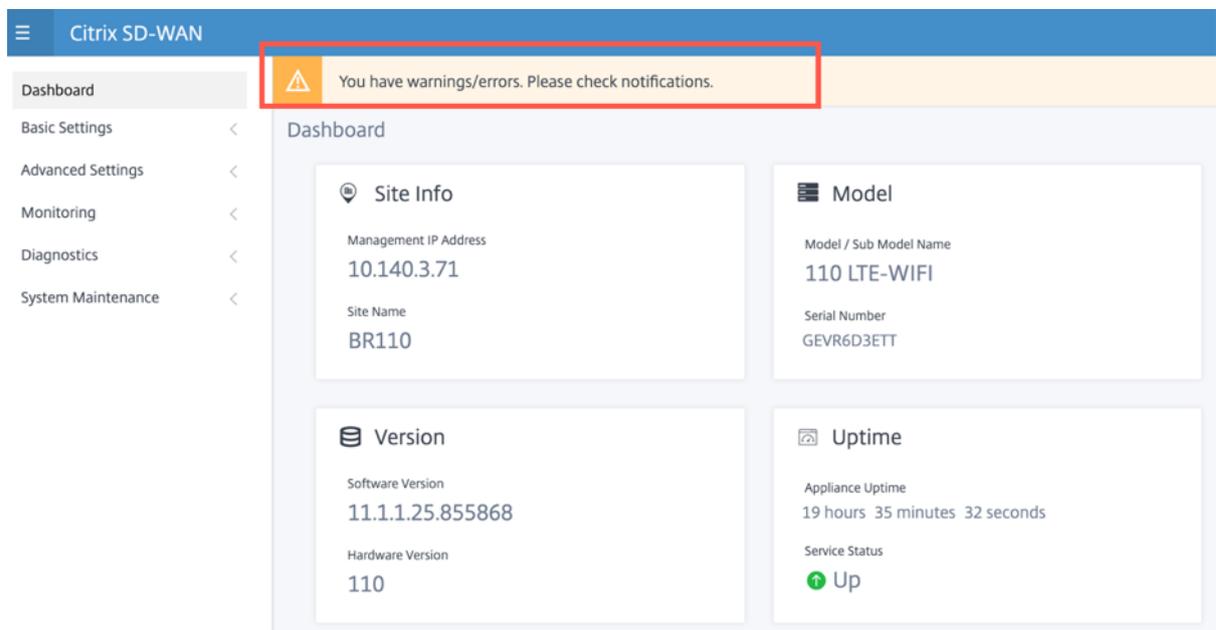
In dem Szenario, in dem das In-Band-Management aktiviert ist, kann die IP-Adresse der Schnittstelle bereitgestellt werden, < **management-ip** > um auf die neue Benutzeroberfläche zuzugreifen. Die In-Band-Verwaltung kann auf mehreren vertrauenswürdigen Schnittstellen aktiviert werden, die für IP-Dienste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



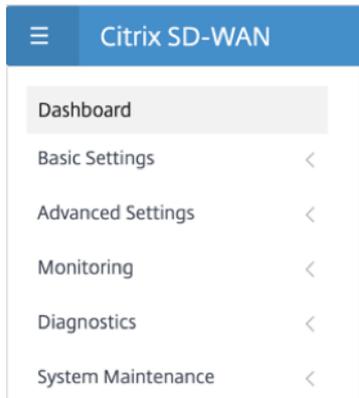
Sobald Sie sich erfolgreich angemeldet haben, können Sie sehen, dass sich das Navigationsfeld auf der linken Seite befindet. Außerdem können Sie ein Benachrichtigungsbanner auf dem Dashboard sehen, wenn Warnungen oder Fehler vorliegen.



Navigation

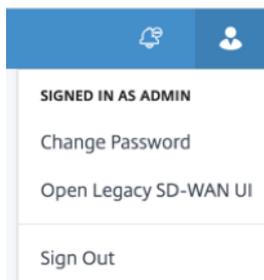
Die linke Navigations-Sidebar kann beim Klick auf das Hamburger-Symbol ausgeblendet oder sichtbar gemacht werden. Das Hamburger-Symbol in der oberen linken Ecke bietet Links zum Dashboard,

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



Menüleiste

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



Dashboard

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

- **Site** — Zeigt die Site-Informationen mit der **Verwaltungs-IP-Adresse** und dem **Site-Namen an**
- **Modell** — Zeigt den **Modell-/Untersmodellnamen** und die **Seriennummer an**
- **Version** — Zeigt **Software-** und **Hardwareversion an**
- **Betriebszeit** - Zeigt **Appliance-Betriebszeit, 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.
- **Orchestrator-Konnektivität** —Zeigt den Konnektivitätsstatus der Appliance mit dem Citrix SD-WAN Orchestrator Service an. Die folgenden Statusinformationen werden angezeigt:
 - **Online-Status**—Zeigt den Verbindungsstatus zwischen der Appliance und dem Citrix SD-WAN Orchestrator Service an. Periodische Heartbeat-Signale werden von der Appliance an den Citrix SD-WAN Orchestrator Service gesendet, um den Verbindungsstatus als Gut oder Schlecht zu identifizieren.
 - **Service State**- Zeigt die HTTPS-Erreichbarkeit der Appliance für alle erforderlichen SD-WAN Orchestrator-Dienste wie Download, Home, Protokollierung und Statistiken an. Wenn der Dienststatus schlecht ist, bedeutet dies, dass die Verbindung hergestellt wurde, aber alle oder einige der Dienste nicht erreichbar sind. Der nicht erreichbare Dienstname wird angezeigt.
 - **DNS-Status**—Zeigt den Status der FQDN-DNS-Auflösung an. Wenn der DNS-Status schlecht ist, bedeutet dies, dass die DNS-Auflösung eines der FQDNs fehlschlägt. Der Name des nicht aufgelösten FQDN wird angezeigt.
 - **Local Gateway State**—Zeigt den Standard-Gateway-Status an. Für eine Out-of-Band-Verbindung wird der Gateway-Status durch Pingen des Standard-Gateways bestimmt. Für eine In-Band-Verbindung wird der Gateway-Status bestimmt, indem die IP-Adresse der Inband-Ethernet-Schnittstelle angepingt wird.
 - **Verbunden durch**—Zeigt an, wie die Appliance den Citrix SD-WAN Orchestrator Service erreicht. Entweder über Out-Of-Band, was die Standardkonfiguration ist, oder über In-Band, wenn die In-Band-Verwaltung konfiguriert ist.
 - **Grund für Fehler:** Grund für den Fehler beim Herstellen einer Verbindung zum SD-WAN Orchestrator Service.

The screenshot displays the 'Dashboard' for a Citrix SD-WAN appliance. It is divided into four main sections:

- Site Info:** Management IP Address: 10.140.3.71; Site Name: BR110.
- Model:** Model / Sub Model Name: 110 LTE-WIFI; Serial Number: GEVR6D3ETT.
- Version:** Software Version: 11.1.1.24.855394; Hardware Version: 110.
- Uptime:** Appliance Uptime: 16 hours 20 minutes 27 seconds; Service Status: Up (indicated by a green arrow icon).

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
- LACP LAG Gruppe
- 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

The screenshot displays the Citrix SD-WAN management interface. The left sidebar contains a navigation menu with the following items: Dashboard, Basic Settings (expanded), Management & DNS (selected), Interface Settings, Date & Time, Advanced Settings, Monitoring, Diagnostics, and System Maintenance. The main content area is titled 'Network Adapters' and contains three sections: 'Management Interface IP', 'DNS Settings', and 'Current DNS'. The 'Management Interface IP' section includes a checked 'Enable DHCP' checkbox and three input fields for 'IP Address', 'Subnet Mask', and 'Gateway IP Address'. The 'DNS Settings' section has two input fields for 'Primary DNS' and 'Secondary DNS', and a 'Clear' button. The 'Current DNS' section shows the current 'Primary DNS' and 'Secondary DNS' values. A blue 'Save' button is located at the bottom of the form.

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.

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

LACP LAG Gruppe

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 Citrix SD-WAN 11.3 werden die protokollbasierten Verhandlungen des 802.3AD Link Aggregation Control Protocol (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 können Sie mit dem Active-Backupmodus auch den vollständigen LACP-Active-Active-Modus aus der SD-WAN-Benutzeroberfläche auswählen.

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 2100 SE/PE
- Citrix SD-WAN 4100 und 5100 SE

- Citrix SD-WAN 6100 SE

Hinweis

Die LAG-Funktionalität wird auf VPX/VPXL-Plattformen nicht unterstützt.

Sie können maximal 4 LAGs mit maximal 4 Ports erstellen, die in jeder LAG auf den Citrix SD-WAN Appliances gruppiert sind.

Für die Citrix SD-WAN 210- und 410-Geräte können maximal 3 LAGs und für die Citrix SD-WAN 110-Appliance maximal 2 LAGs erstellt werden.

Sie können LAG nur mit der [Legacy-Benutzeroberfläche](#) oder dem [SD-WAN Orchestrator](#) erstellen. In der neuen Benutzeroberfläche können Sie nur die Details der erstellten LAG anzeigen.

Um Details von LAG anzuzeigen, navigieren Sie zu **Grundeinstellungen > LACP LAG Group**.

Sie können Details zu LACP LAG wie den aktuellen Status, das System und die Portpriorität von aktiven Ports und Partnerports anzeigen.

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

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

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](#).

The screenshot displays the Citrix SD-WAN configuration interface. The left sidebar contains a navigation menu with the following items: Dashboard, Basic Settings (expanded), Management & DNS, Interface Settings, Date & Time (selected), Advanced Settings, Monitoring, Diagnostics, and System Maintenance. The main content area is titled 'Date/Time Settings' and contains three sections:

- NTP Settings:** A warning message states, 'If the Appliance date/time is turned back due to NTP or manual changes, reporting artifacts may occur.' Below this, the 'Use NTP Server' checkbox is checked. The 'Server Address' field contains the text '0.pool.ntp.org;1.pool.ntp.org;2.pool.ntp.org;3.pool.ntp.org'. A 'Save' button is located below the field.
- Date/Time Settings:** The date and time are set to 'May 6, 2020 1:55 PM'. A 'Save' button is located below the field.
- Timezone Settings:** A warning message states, 'After changing the timezone setting, a reboot will be necessary for the timezone changes to take full effect. Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.' Below this, the 'Timezone' dropdown menu is set to 'UTC'. A 'Save' button is located below the dropdown.

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**.

RADIUS Server

Server Settings

Enable RADIUS

Server 1 IP Address *

Authentication Port

1812

Server 2 IP Address

Authentication Port

Server 3 IP Address

Authentication Port

Server Key

Confirm Server Key

Timeout(seconds)

Save

Test RADIUS Server Connection

User Name

Password

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**.

TACACS+ Server

Settings

Enable TACACS+

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

Authentication Type PAP ASCII

Server Key

Confirm Server Key

Timeout(seconds)

Test TACACS+ Server Connection

User Name

Password

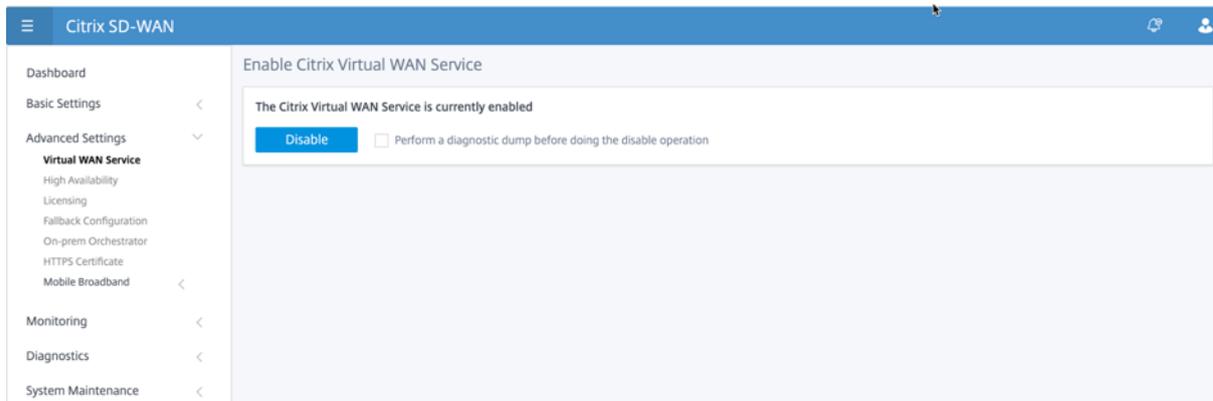
Erweiterte Einstellungen

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

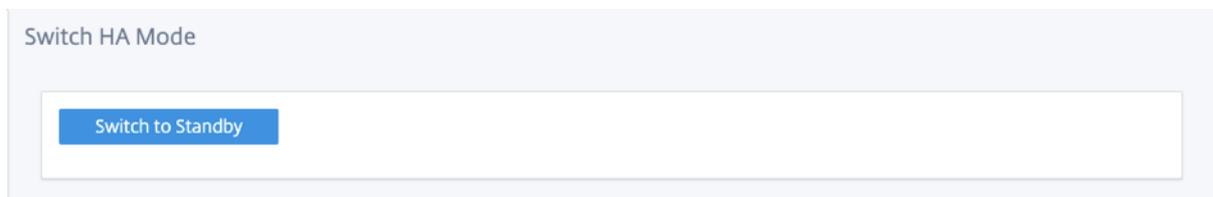
Citrix Virtual WAN-Dienst

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 **Autog**ändert 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.

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

Im Folgenden finden Sie einige nützliche Statusinformationen:

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

- **Betriebsart:** Zeigt den Modemstatus an.
- **SIM-Funktionen:** Zeigt an, ob die SIM unterstützt wird oder nicht.
- **Modell:** Zeigt den Namen des Moduls für mobiles Breitband an

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

Geräteinformationen für externes CDC Ethernet-Modem.

The screenshot shows the 'Mobile Broadband Status' interface. At the top, there are two dropdown menus: 'Modem Type' set to 'External Modem' and 'Status Of' set to 'Device'. Below these is a table with the following data:

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

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

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

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

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

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 SIM-Karten** angeschlossen sind, verwendet das LTE-Modem beim Booten 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.

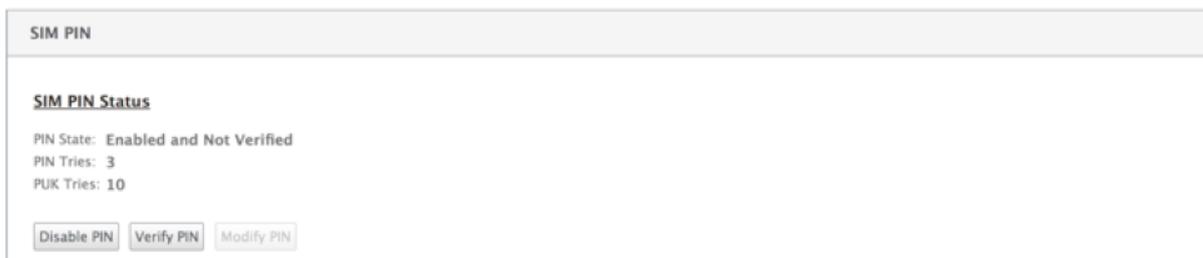
Hinweis

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**.



SIM PIN

SIM PIN Status

PIN State: Enabled and Not Verified
PIN Tries: 3
PUK Tries: 10

Disable PIN Verify PIN Modify PIN

Sie können die folgenden Vorgänge ausführen:

- **SIM-PIN überprüfen:** Klicken Sie auf **Überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Verifizieren**. Der Status ändert sich in **Aktiviert und Verifiziert**.
- **SIM-PIN aktivieren:** Sie können die SIM-PIN für eine SIM-PIN aktivieren, bei der die SIM-PIN klicken Sie auf **Aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**. Wenn sich der SIM-PIN-Status in **Aktiviert und Nicht überprüft** ändert, bedeutet dies, dass die PIN nicht überprüft wird und Sie erst dann LTE-bezogene Vorgänge ausführen können, wenn die PIN überprüft wurde. Klicken Sie auf **Verify**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Verifizieren**.
- **SIM-PIN deaktivieren:** Sie können die SIM-PIN-Funktion für eine SIM-PIN deaktivieren, für die die SIM-PIN aktiviert und verifiziert ist. Klicken Sie auf **Deaktivieren**. Geben Sie die SIM-PIN ein und klicken Sie auf **Deaktivieren**.
- **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 Mobilfunkansichters 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. 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

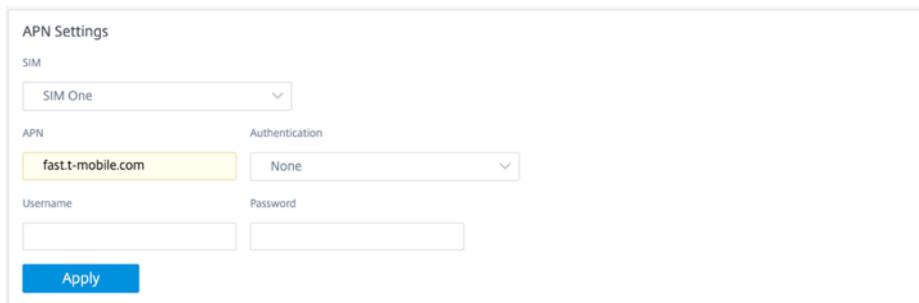
Rufen Sie die APN-Informationen vom Mobilfunkanbieter ab.

2. Wählen Sie die SIM-Karte aus, 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

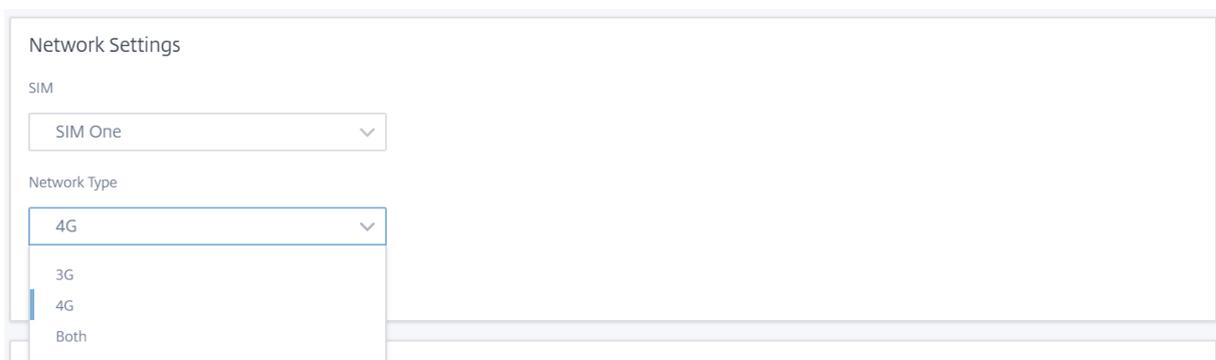
Alle diese Felder sind optional.

3. Klicken Sie auf **Anwenden**.



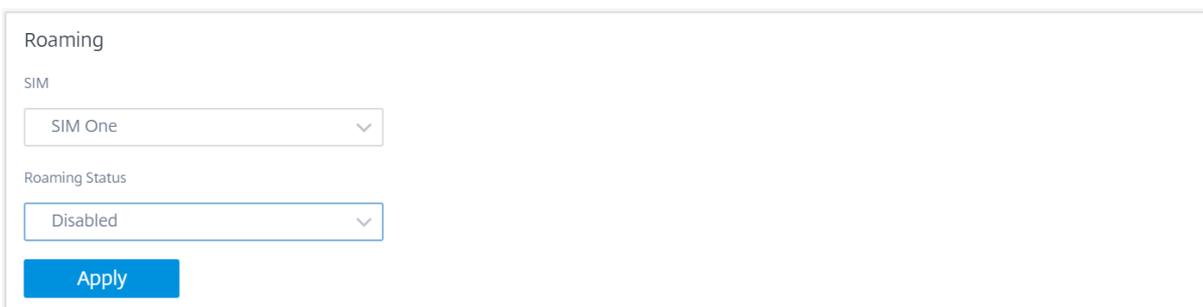
The screenshot shows the 'APN Settings' configuration window. It includes a 'SIM' dropdown menu set to 'SIM One'. Below this are two columns: 'APN' with a text input field containing 'fast.t-mobile.com', and 'Authentication' with a dropdown menu set to 'None'. At the bottom of these columns are 'Username' and 'Password' text input fields. A blue 'Apply' button is located at the bottom left of the form.

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



The screenshot shows the 'Network Settings' configuration window. It features a 'SIM' dropdown menu set to 'SIM One'. Below it is the 'Network Type' dropdown menu, which is currently open, showing options for '4G', '3G', '4G', and 'Both'. The '4G' option is selected and highlighted.

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



Roaming

SIM

SIM One

Roaming Status

Disabled

Apply

Firmware verwalten

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

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



Enable/Disable Modem

Enable

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



Reboot Modem

Reboot

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.



SIM Card (SIM Two)

Refresh SIM

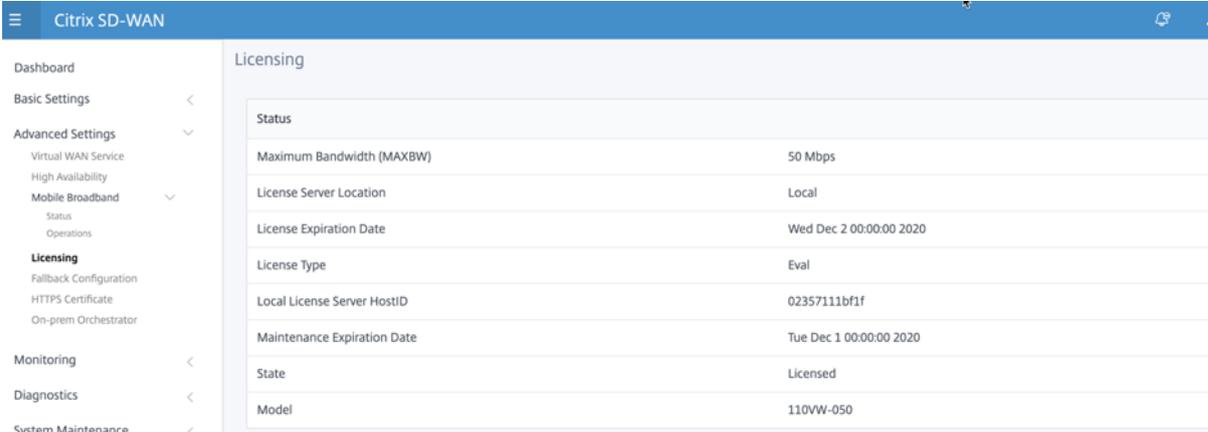
Mit dem Citrix SD-WAN Center können Sie alle LTE-Sites in Ihrem Netzwerk remote anzeigen und verwalten. Weitere Informationen finden Sie unter [Remote-LTE-Standortverwaltung](#).

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

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

Lizenzierung

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



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

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**.

Fallback Configuration

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

Enable Fallback Configuration [Reset](#)

WAN Settings

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

LAN Settings

VLAN ID: IP Address:

Enable DHCP Server

DHCP Start: DHCP End:

Dynamic DNS Servers

DNS Server: Alt DNS Server:

Internet Access

Port Settings

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

Unassigned Port Bypass Mode:

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](#).

The screenshot displays the 'HTTPS Certificate' configuration page in the Citrix SD-WAN management console. The interface is divided into several sections:

- Navigation Menu (Left):** Includes Dashboard, Basic Settings, Advanced Settings (with sub-items like Virtual WAN Service, High Availability, Mobile Broadband, Status, Operations, Licensing, Fallback Configuration, HTTPS Certificate, and On-prem Orchestrator), Monitoring, Diagnostics, and System Maintenance.
- Installed Certificate:** Shows two columns of information:

Issuer		Issued To	
Country:	US	Country:	US
State/Province:	California	State/Province:	California
Locality:	San Jose	Locality:	San Jose
Organization:	Citrix Systems, Inc.	Organization:	Citrix Systems, Inc.
Organizational Unit:	Engineering	Organizational Unit:	Engineering
Common Name:	Citrix	Common Name:	Citrix
Email:	support@citrix.com	Email:	support@citrix.com
- Certificate Details:**

Certificate Fingerprint:	9D:FA:53:C0:55:0C:28:6C:E3:FB:24:60:60:D2:82:C0:17:00:34:88
Start Date:	Apr 16 12:15:31 2020 GMT
End Date:	Apr 14 12:15:31 2030 GMT
Serial Number:	F22786ABF41CC86D
- Upload Certificate:** Contains instructions to upload a certificate that secures the Management HTTPS connection. It includes a note: "NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance." Below the instructions are two dashed boxes for file uploads:
 - Upload Certificate:** "Click to select or drag n drop file here. Allowed file types are .crt"
 - Upload Key:** "Click to select or drag n drop file here. Allowed file types are .key"
 An "Upload" button is located at the bottom of this section.
- Regenerate Certificate:** Contains instructions to regenerate the certificate, with a note: "NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance."

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 der SD-WAN-Appliance ist derzeit nicht verfügbar. Es ist für eine zukünftige Veröffentlichung 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.

The screenshot shows the 'On-Prem SD-WAN Orchestrator Identity' configuration page in the Citrix SD-WAN GUI. The page has a blue header with the title 'Citrix SD-WAN'. On the left is a navigation menu with options like Dashboard, Basic Settings, Advanced Settings, and Identity. The main content area contains a note: 'Note: This section is applicable only to On-prem SD-WAN Orchestrator managed networks, and not Cloud Orchestrator or SD-WAN Center managed networks.' Below the note are two checked checkboxes: 'Enable On-Prem SD-WAN Orchestrator connectivity' and 'Advanced Configuration'. There are three rows of input fields for IP addresses and domains for the On-prem SD-WAN Orchestrator, Download Management Service, and Statistics Management Service. An 'Apply' button is at the bottom.

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

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

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

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

Im Falle einer erweiterten Konfiguration:

Beispiel: Wenn die On-prem Orchestrator-Domäne als **citrix.com** konfiguriert ist, wird die Download Management Service Domain als **download.citrix.com** konfiguriert, und die 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/Domain:** Stellen Sie die IP-Adresse/Domäne bereit, die die Erfassung und Verwaltung von SD-WAN-Statistiken von Geräten auf eine unabhängige Serverinstanz auslagert, um eine bessere Skalierbarkeit für große Netzwerke zu ermöglichen.

4. Klicken Sie auf **Anwenden**.

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

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

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

Beim Deaktivieren des **Authentifizierungstyps** in On-prem Orchestrator vom Enable-Status wird vorhandene Geräte im Einweg-Authentifizierungsmodus in den Status "Getrennt" versetzt. Kunden müssen den Authentifizierungstyp der Appliance in Zwei-Wege-Authentifizierung ändern und das SD-WAN-Appliance-Zertifikat in den On-Prem Orchestrator hochladen, um es zu verbinden.

Hinweis

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

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

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

Secure Connectivity

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

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

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

Authentication Type

No Authentication

Apply

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

Secure Connectivity

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

Authentication Type

One-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

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

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

Upload

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

Secure Connectivity

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

Authentication Type
Two-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

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

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

Upload

SD-WAN Appliance Certificate

Certificate Details:

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

Regenerate Download

Hinweis

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

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

Upgrade und Downgrade

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

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

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

Überwachen

Im Abschnitt Monitoring können Sie die Statistiken **Address Resolution Protocol (ARP)**, **Route**, **Ethernet**, **Ethernet-MAC** zusammen mit **WAN Links für DHCP-Clients**, **SLAAC WAN-Verbindungen**, **DHCP Server/Relay**, **Firewall Connections**, **Flows** und **DNS Statistics** 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-Link-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](#).
- **SLAAC WAN-Links:** Die SLAAC WAN-Linkseite enthält Details zu den IPv6-Adressen, die SLAAC den virtuellen Schnittstellen zuordnet. Sie können auch **Release Renew** auswählen, damit SLAAC dem IPv6-Client eine neue IP-Adresse oder dieselbe IP-Adresse mit einem neuen Leasing zuweisen kann.
- **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 selben 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](#).
- **DNS-Proxy-Statistiken:** Diese Seite enthält Details zu den konfigurierten DNS-Proxys. Klicken Sie auf **Aktualisieren**, um die aktuellen Daten zu erhalten. Weitere Informationen finden Sie unter [Domainnamensystem](#).

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.

Nicht unterstützte Plattformen

Die neue Benutzeroberfläche unterstützt die folgenden SD-WAN-Appliances nicht:

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

Auswirkungen auf das Citrix SD-WAN 11.5-Release-Upgrade

August 29, 2022

- Citrix SD-WAN 11.5.0 ist eine Version mit eingeschränkter Verfügbarkeit, die nur für bestimmte Kunden-/Produktionsbereitstellungen empfohlen und unterstützt wird.
- SD-WAN 11.5.0 unterstützt keine Bereitstellungen für Advanced Edition (AE), Premium Edition (PE) und WAN-Optimierung.
- SD-WAN 11.5.0 unterstützt nur die in [SD-WAN-Plattformmodellen und Softwarepaketen](#) genannten Plattformen.
- SD-WAN 11.5.0 unterstützt Citrix SD-WAN Center oder Citrix SD-WAN Orchestrator nicht für on-premises.
- SD-WAN 11.5.0-Firmware ist auf der Seite Citrix Downloads nicht verfügbar.
- SD-WAN 11.5.0 ist nur über den Citrix SD-WAN Orchestrator Service und nur für ausgewählte geografische POPs verfügbar.
- Stellen Sie sicher, dass Sie die erforderlichen Genehmigungen und Anleitungen von Citrix Product Management/Citrix Support einholen, bevor Sie 11.5.0 in einem Produktionsnetzwerk bereitstellen.

Systemanforderungen

August 29, 2022

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 11.4 ausgeführt wird. Für weitere Informationen wenden Sie sich bitte an das Citrix Support-Team.

Softwareanforderungen

Ab SD-WAN 11.5-Version wird die SD-WAN-Appliance-Lizenzierung über den Citrix SD-WAN Orchestrator Service verwaltet. 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 Edge 13+

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

September 26, 2023

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
1100-SE	Appliance für große Zweigstellen
2100-SE	Appliance für große Zweigstellen
4100-SE	Rechenzentrum —Master Control Node (MCN) -Appliance
5100-SE	Rechenzentrum —Master Control Node (MCN) -Appliance
6100-SE	Rechenzentrum —Master Control Node (MCN) -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.

Upgradepfad

August 29, 2022

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 ignoriert 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.

Konfiguration

September 26, 2023

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.

Ersteinrichtung

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.

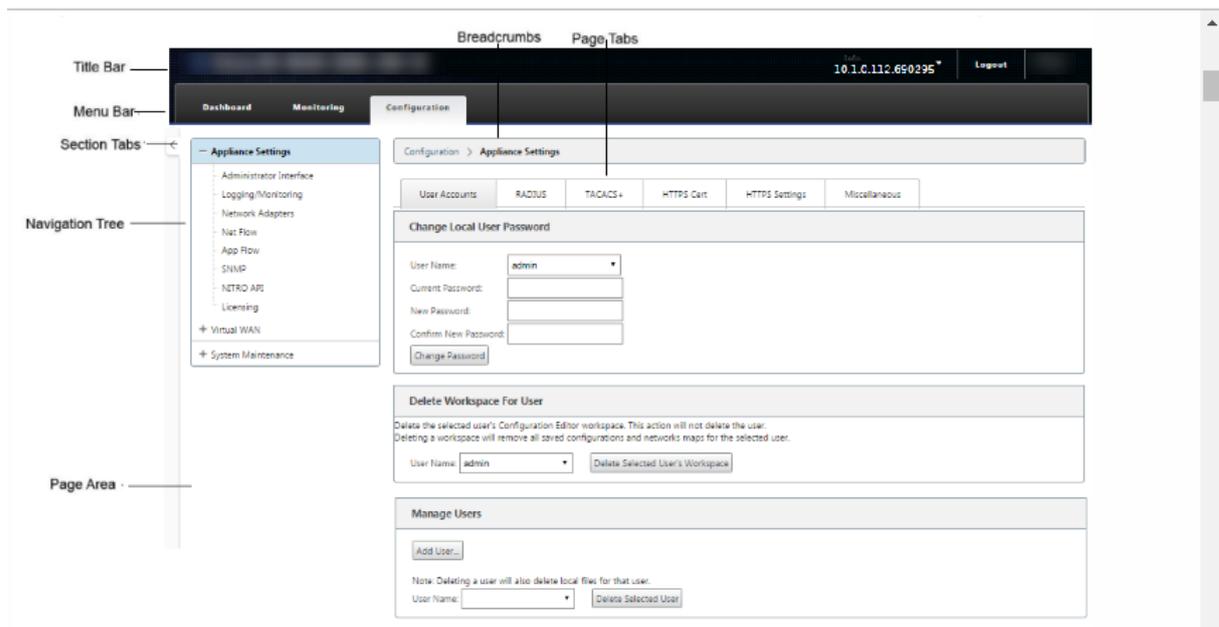
Anweisungen zum Installieren einer virtuellen SD-WAN Appliance (SD-WAN VPX) finden Sie in den folgenden Abschnitten:

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

Übersicht über das Layout des Web Interface (UI)

Dieser Abschnitt enthält grundlegende Navigationsanweisungen und eine Navigations-Roadmap der Seitenhierarchie der SD-WAN-Webverwaltungs Oberfläche. <! —Außerdem werden spezifische Navigationsanweisungen für den **Konfigurations-Editor** und den Assistenten für die **Änderungsverwaltung 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.

The screenshot shows the 'Dashboard' tab selected in a navigation bar with 'Monitoring' and 'Configuration' options. The main content area is titled 'System Status' and contains the following information:

Name:	MCN_23
Model:	VPX
Sub-Model:	BASE
Appliance Mode:	MCN
Serial Number:	67e0772c-5190-a2ee-d183-9244189b30a0
Management IP Address:	10.102.78.154
Appliance Uptime:	1 days, 10 hours, 49 minutes, 48.5 seconds
Service Uptime:	1 days, 10 hours, 42 minutes, 20.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Below this, the 'Local Versions' section shows:

Software Version:	10.1.0.111.690027
Built On:	Jun 21 2018 at 23:42:30
Hardware Version:	VPX
OS Partition Version:	4.6

The 'Virtual Path Service Status' section shows:

Virtual Path MCN_23-Site1: Uptime: 1 days, 10 hours, 39 minutes, 19.0 seconds.

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

The screenshot shows the 'Dashboard' tab selected in a navigation bar with 'Monitoring' and 'Configuration' options. The main content area is titled 'System Status' and contains the following information:

Name:	DC2-201
Model:	5100
Appliance Mode:	Client
Management IP Address:	10.199.107.201
Appliance Uptime:	2 weeks, 36 minutes, 52.5 seconds
Service Uptime:	2 weeks, 8 minutes, 26.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Below this, the 'Virtual Path Service Status' section shows:

Virtual Path DC-BR: Uptime: 4 days, 5 hours, 31 minutes, 39.0 seconds.

Einrichten der Appliance-Hardware

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 Managementport 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-Managementport mit dem Standard-Ethernetport 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-SE](#) beschrieben.

Die virtuelle SD-WAN VPX-SE Appliance ist eine virtuelle Maschine, daher gibt es keinen physischen Verwaltungs-Port. Wenn Sie jedoch die Verwaltungs-IP-Adresse für 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-SE](#) beschrieben.

Konfigurieren der Verwaltungs-IP-Adresse

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 zulässig.
- Um eine IPv6-Adresse zu konfigurieren, benötigen Sie einen Router im Netzwerk, der die IPv6-Adresse ankündigt.

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 Managementport der Appliance und das andere Ende an den Standard-Ethernetport 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: *Passwort*

Hinweis

Es wird empfohlen, das Standardkennwort zu ändern. Achten Sie darauf, das Kennwort an einem sicheren Ort aufzuzeichnen, da die Wiederherstellung des Kennworts möglicher-

weise ein Zurücksetzen der Konfiguration erfordert.

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



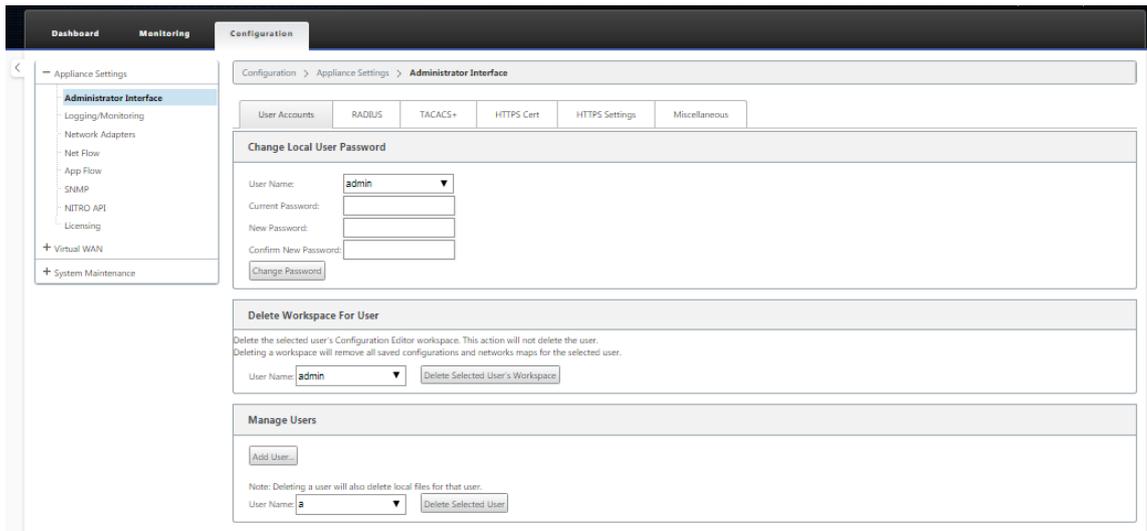
Wenn Sie sich zum ersten Mal bei der Management-Weboberfläche einer Appliance anmelden, zeigt das **Dashboard** ein Warnsymbol (Goldenrod Delta) und eine Warnmeldung an, die angibt, dass der SD-WAN-Dienst deaktiviert ist und die Lizenz nicht installiert wurde. Im Moment können Sie diese Warnung ignorieren.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



- 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.

Configuration > Appliance Settings > Network Adapters

IP Address Ethernet Mobile Broadband

Management Interface IP

DHCP

Enable DHCP

Manual

IP Address:

Subnet Mask:

Gateway IP Address:

DNS Settings

Primary DNS:

Secondary DNS:

Management Interface Whitelist

An empty Whitelist allows Management Interface to be accessed from all networks.

Allowed Network:

Add Network(s):

Management Interface DHCP Server

If you plan to use the DHCP Server or DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead to duplicate IP addresses on the defined management network.

When HA switches from the Active to the Standby Citrix Appliance, the DHCP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working.

The Management Interface DHCP Server will use the current Management Interface IP settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server IP range, defined by Start and End IP Address, must be valid in the Management Interface subnet.

DHCP Server Status: stopped

Enable DHCP Server

Lease Time (minutes):

Domain Name:

Start IP Address:

End IP Address:

Management Interface DHCP Relay

Enable DHCP Relay

DHCP Server IP Address:

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
- Präfix

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.
- Wenn die Verwaltungsschnittstelle als DHCP-Client fungiert, wird der Hostname in DHCP-Clientnachrichten als Option 12 verwendet. Ab Citrix SD-WAN Version 11.2.3 und bis Version 11.4.1 wurde der Hostname als **sdwan** festgelegt. Ab Citrix SD-WAN Version 11.4.1 entspricht der Hostname dem Site-Namen.

Wenn der Site-Name zum ersten Mal geändert oder konfiguriert wird, wird der alte Site-Name oder **sdwan**, bis das Konfigurationsupdate abgeschlossen ist und der virtuelle WAN-Dienst verfügbar ist, der alte Site-Name oder **sdwan** als Hostname in DHCP-Clientnachrichten verwendet. Nachdem das Konfigurationsupdate abgeschlossen ist und der virtuelle WAN-Dienst verfügbar ist, verwenden die nachfolgenden DHCP-Clientnachrichten den neuen Standortnamen.

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.

Management Interface Whitelist

An empty Whitelist allows Management Interface to be accessed from all networks.
V4 networks can be added/removed only from a V4 network.
V6 networks can be added/removed only from a V6 network.

Add Network(s):

Datum und Uhrzeit festlegen

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

Hinweis

- Sie müssen diesen Vorgang für jede Appliance wiederholen, die Sie Ihrem Netzwerk hinzufügen möchten.
- Wenn die aktuelle Zeit entweder manuell oder über den NTP-Server geändert wird und die neu eingestellte Zeit mehr als der Timer für das Sitzungstimeout ist, wird die UI-Sitzung abgemeldet.

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.

- 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.

- 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 Zeitzonenuodate abgeschlossen ist, werden im oberen Bereich der Seite ein Symbol für eine Erfolgsalarmierung (grünes Häkchen) und eine Statusmeldung angezeigt.
- (Optional) Aktivieren Sie den NTP-Serverdienst.
 - Wählen Sie **NTP-Server verwenden**.
 - Geben Sie die Serveradresse in das Feld **Serveradresse** ein.
 - Klicken Sie auf **Change Settings**.
Ein Erfolgswarnsymbol (grünes Häkchen) und eine Statusmeldung werden angezeigt, wenn das Update abgeschlossen ist.
- 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 während der Arbeit an der Konfiguration vorzeitig beendet wird, 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-Softwarelizenzdatei](#) fortfahren.

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.

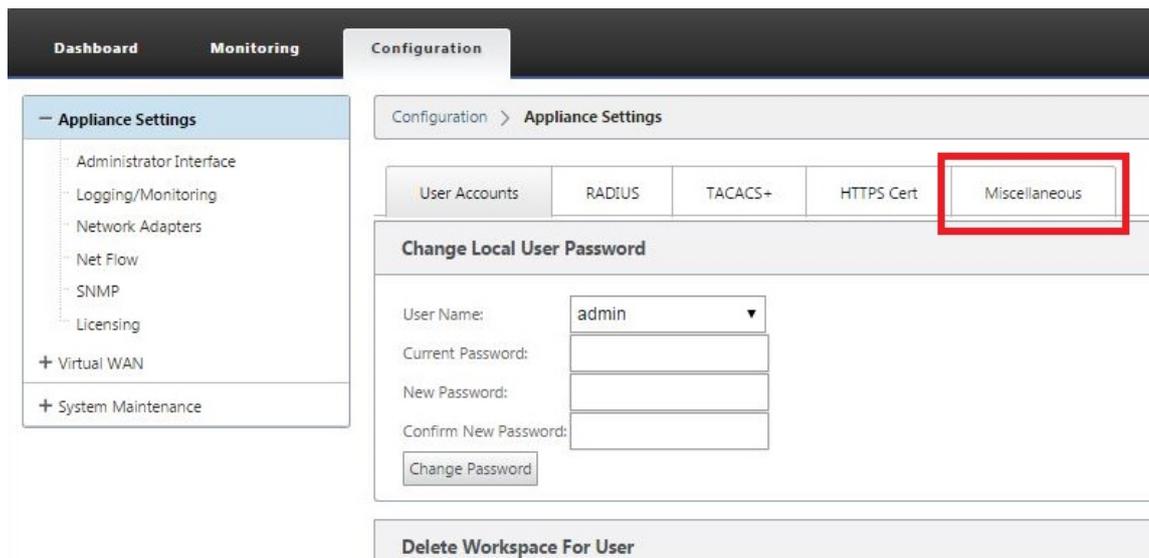
Sitzungstimeout

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

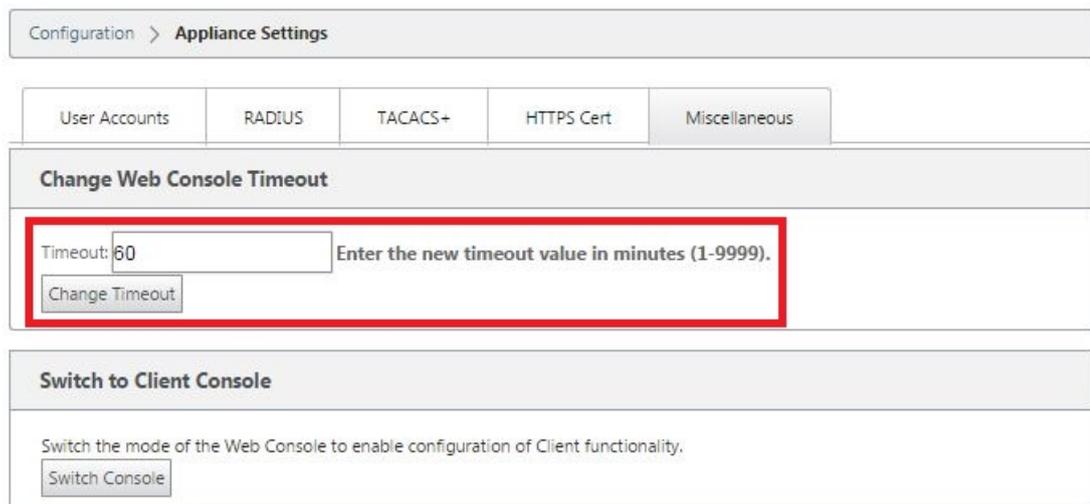
1. Wählen Sie die Registerkarte **Konfiguration** aus, und wählen Sie dann den Zweig **Appliance-Einstellungen** in der Navigationsstruktur aus.

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.

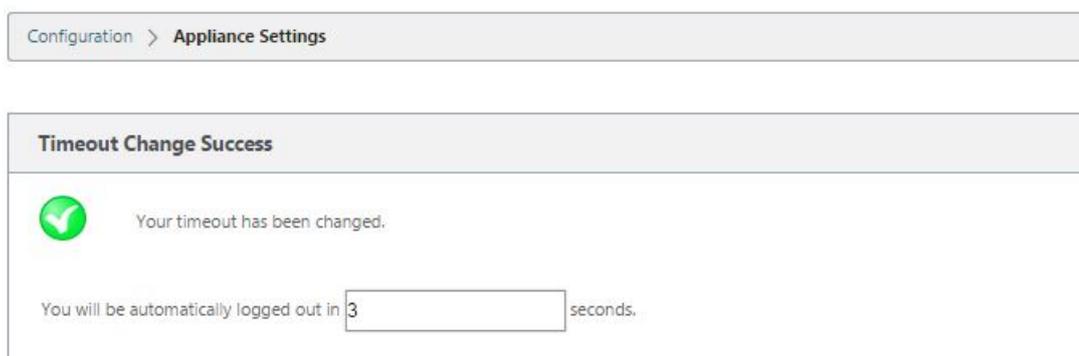
Geben Sie im Feld **Timeout** des Abschnitts **Timeout der Webkonsole ändern** einen höheren Wert (in Minuten) bis zum Maximalwert von 9999 ein. Der Standardwert ist 60, was für eine erste Konfigurationssitzung viel zu kurz ist.

Hinweis

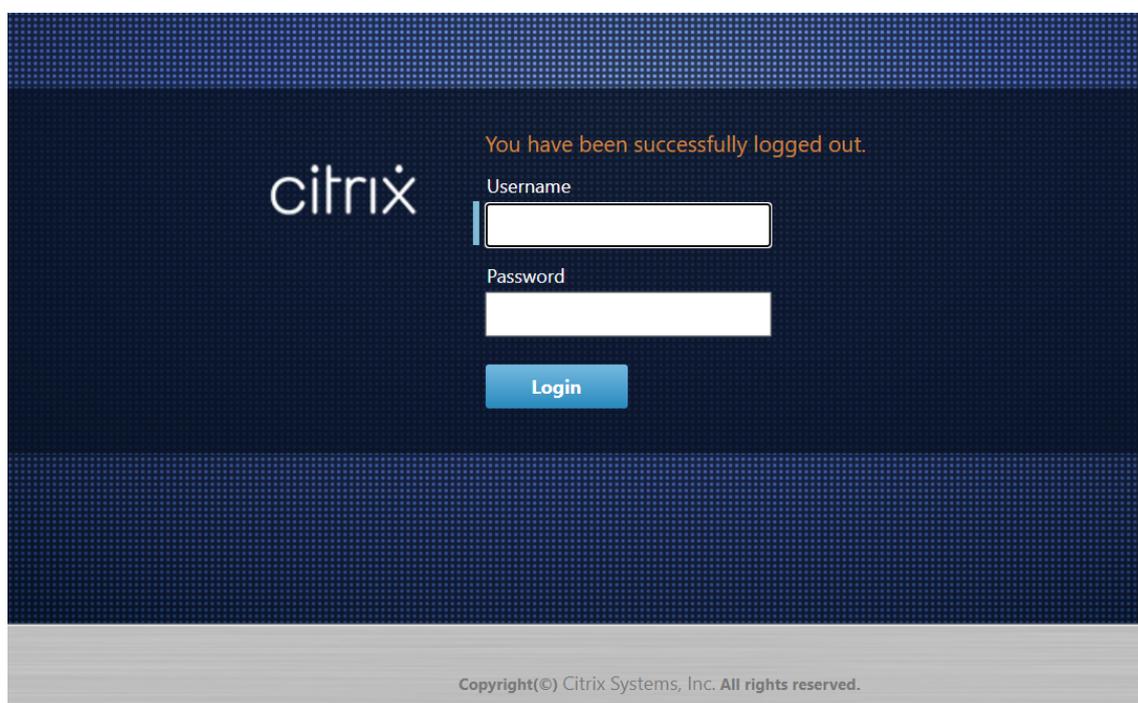
Stellen Sie aus Sicherheitsgründen sicher, dass Sie diesen Wert nach Abschluss der Konfiguration und Bereitstellung auf ein niedrigeres Intervall zurücksetzen.

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.

Alarmer konfigurieren

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.

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

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.
- **Löschdauer:** Die Dauer in Sekunden. Sie bestimmt, wie lange gewartet werden muss, bevor ein Alarm ausgelöst 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.

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

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.

Master-Kontrollknoten einrichten

Der **SD-WAN Master Control Node (MCN)** ist die Head End-Appliance im virtuellen WAN. In der Regel ist dies eine virtuelle WAN-Appliance, die im Rechenzentrum 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.

Ab Version Citrix SD-WAN 11.5 können Sie einen MCN über den Citrix SD-WAN Orchestrator Service einrichten. Weitere Informationen finden Sie unter [Bereitstellung](#) und [Sitekonfiguration](#).

Verbinden der Client-Appliances mit dem Netzwerk

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.

Zugriff auf den Shell-Befehl

Ab Version SD-WAN 11.4.1 können Benutzer des Administratorkontos den Shell-Befehl direkt von der SD-WAN CLI-Konsole aus ausführen, ohne nach den Anmeldeinformationen des statischen CBVWSSH-Kontos gefragt zu werden. Diese Funktion erhöht die Sicherheit Ihrer SD-WAN-Appliances, da das fest codierte Kennwort des CBVWSSH-Kontos entfernt und mithilfe einer sichereren Methode ersetzt wird. Um den Shell-Befehl auszuführen, melden Sie sich bei der SD-WAN CLI-Konsole an und geben Sie ein `shell`.

Hinweis

- Diese Funktion wird nur für Benutzer von Admin-Konten unterstützt. Sie wird nicht für Netzwerkadministratoren, Sicherheitsadministratoren oder Benutzer von Viewer-Konten unterstützt.
- Diese Funktion dient nur zur Fehlerbehebung. Alle systemspezifischen Änderungen, die über den Befehl `shell` vorgenommen werden, werden von Citrix überwacht.

Upgrade Wenn Sie Ihre SD-WAN-Appliance auf die Version 11.4.1 aktualisieren, wird das Kennwort des Standard-Administratorkontos mit dem CBVWSSH-Konto synchronisiert. Diese Synchronisierung zwischen dem CBVWSSH-Konto und dem Standard-Administratorkonto erfolgt jedes Mal, wenn Sie das Administratorkonto bearbeiten/aktualisieren.

Downgrade Wenn Sie Ihre SD-WAN-Appliance von 11.4.1 auf eine ältere Version herunterstufen, erhalten Sie die Option, das Kennwort des Standard-Administratorkontos zurückzusetzen. Das neue Kennwort wird jedoch nicht mit dem CBVWSSH-Konto synchronisiert. Um auch nach einem Downgrade auf den Befehl `shell` zugreifen zu können, müssen Sie sich daher das aktuelle Kennwort merken, bevor Sie Ihre Appliance herunterstufen.

Bereitstellen von Citrix SD-WAN Standard Edition in OpenStack mit CloudInit

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**.

The screenshot shows the 'Create Image' dialog box with the following fields and options:

- Image Name:** Text input field containing 'i'.
- Image Description:** Text input field.
- Image Source:** 'File' section with a 'Browse...' button.
- Format:** Dropdown menu.
- Image Requirements:**
 - Kernel:** Dropdown menu with 'Choose an image'.
 - Ramdisk:** Dropdown menu with 'Choose an image'.
 - Architecture:** Text input field.
 - Minimum Disk (GB):** Text input field with '0'.
 - Minimum RAM (MB):** Text input field with '0'.
- Image Sharing:**
 - Visibility:** Radio buttons for 'Public' and 'Private'.
 - Protected:** Radio buttons for 'Yes' and 'No'.

At the bottom of the dialog, there are buttons for 'Cancel', '< Back', 'Next >', and 'Create Image'.

- **Image name** - Geben Sie den Imagennamen an.
- **Imagebeschreibung** —Fügen Sie eine Bildbeschreibung hinzu.
- **Datei** - Suchen Sie von Ihrem lokalen Laufwerk nach der kvm.qcow2-Imagedatei und wählen Sie sie aus.
- **Format** —Wählen Sie das Datenträgerformat QCOW2 —QEMU Emulator aus der Dropdownliste aus.

Klicken Sie auf **Image erstellen**.

Sowohl Netzwerk- als auch Netzwerk-Port müssen zunächst erstellt und vordefiniert werden. So erstellen Sie einen Netzwerk-Port:

1. Wählen Sie unter **Netzwerk** die Option **Netzwerke** aus und gehen Sie zur Registerkarte **Port**.
2. Klicken Sie auf **Port erstellen**, geben Sie die erforderlichen Details an und klicken Sie auf Erstellen.

Create Port ✕

Info

Security Groups

Name

Enable Admin State

Device ID ?

Device Owner ?

Specify IP address or subnet ?

Fixed IP Address
▼

Fixed IP Address ?

10.106.36.xx
?

MAC Address ?

Port Security ?

VNIC Type ?

Normal
▼

Description:

You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.

Cancel

Create

Wenn Sie **Feste IP-Adresse** auswählen, müssen Sie die Subnetz-IP-Adresse für den neuen Port angeben.

Project

Project / Network / Networks / public

API Access

public

Edit Network ▼

Compute

Overview

Subnets

Ports

Volumes

Filter

+ Create Port

Delete Ports

Network

Displaying 12 items

□	Name	Fixed IPs	MAC Address	Attached Device	Status	Admin State	Actions
<input type="checkbox"/>	Mgt-Port	• 10.106.36.41	fa:16:3e:24:8a:8c	Detached	Down	UP	Edit Port ▼
<input type="checkbox"/>	(0b1273e8-1205)	• 10.106.36.31	fa:16:3e:c4:bc:eb	compute:compute1	Active	UP	Edit Port ▼
<input type="checkbox"/>	test1	• 10.106.36.36	fa:16:3e:52:2d:8b	compute:compute2	Active	UP	Edit Port ▼
<input type="checkbox"/>	tiny_mgmt	• 10.106.36.44	fa:16:3e:8d:83:04	Detached	Down	UP	Edit Port ▼

Der Port wird erstellt und da er nicht an ein Gerät angeschlossen ist, wird der aktuelle Status als Detached angezeigt.

Erstellen Sie OpenStack-Instanz, um config-drive zu aktivieren und die user_data zu übergeben.

3. Melden Sie sich bei OpenStack an und konfigurieren Sie Instanzen.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
router_image	test_linux	10.106.36.43	m1.medium	-	Active	compute1	None	Running	1 day, 5 hours	Create Snapshot
sdwan-11configdata	sdwan-finaltny	10.106.36.36	m1.large	-	Active	compute2	None	Running	1 week, 1 day	Create Snapshot
sdwan-release11	sdwan-finaltny	10.106.36.31	m1.large	-	Active	compute1	None	Running	1 week, 1 day	Create Snapshot
sdwan-sample	sdwan_priv	test_3 172.16.12.44 public 10.106.36.42 test_1 172.16.10.67	m1.large	-	Active	compute2	None	Running	1 week, 1 day	Create Snapshot

4. Laden Sie die **kvm.qcow2.gz-Datei** herunter und entpacken Sie sie.

5. Gehen Sie zu **Instances** und klicken Sie auf **Launch Instance**

HINWEIS

Sie können zu **Instances** zurückkehren und auf **Launch Instance** klicken oder im Bildschirm Images auf **Launch** klicken, sobald das Image erstellt wurde.

admin	sdwan-finaltny	Image	Active	Public	No	QCOW2	1.33 GB	Launch
admin	sdwan_mtu_check	Image	Active	Public	No	QCOW2	1.32 GB	Launch
admin	sdwan_priv	Image	Active	Public	No	QCOW2	1.29 GB	Launch

6. Geben Sie auf der Registerkarte **Details** die folgenden Informationen an:

- **Instanzname** —Geben Sie den Hostnamen für die 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**.

Launch Instance

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *
sdwan-openstack

Description

Availability Zone
Any Availability Zone

Count *
1

Total Instances (30 Max)
40%

11 Current Usage
1 Added
18 Remaining

Cancel < Back **Next >** Launch Instance

7. Wählen Sie auf der Registerkarte **Quelle** unter **Neues Volume erstellen** die Option **Nein** aus und klicken Sie auf **Weiter**. Instanzquelle ist die Vorlage, die zum Erstellen einer Instanz verwendet wird.

Launch Instance

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source: Image

Create New Volume: Yes No

Allocated

Name	Updated	Size	Type	Visibility
Select an item from Available items below				

Available 10

Click here for filters or full text search.

Name	Updated	Size	Type	Visibility
cirros	8/7/19 9:25 PM	12.65 MB	qcow2	Public
sdwan-finaltiny	11/7/19 10:42 AM	1.33 GB	qcow2	Public
sdwan_mtu_check	8/19/19 1:34 PM	1.32 GB	qcow2	Public
sdwan_priv	11/5/19 10:34 AM	1.29 GB	qcow2	Public
SDWAN_VPX_IMG_NEW	8/8/19 8:31 PM	1.31 GB	qcow2	Public
test_branch_1	10/4/19 10:07 AM	1.72 GB	qcow2	Public
test_brnach_2	10/4/19 10:08 AM	1.72 GB	qcow2	Public
test_dynamips	10/4/19 10:06 AM	1.72 GB	qcow2	Public
test_linux	10/4/19 10:07 AM	1.72 GB	qcow2	Public
test_mcn	10/4/19 10:08 AM	1.72 GB	qcow2	Public

Buttons: Cancel, < Back, **Next >**, Launch Instance

8. Wählen Sie **Flavour** für die Instanz aus und klicken Sie auf Weiter. Das für eine Instanz ausgewählte Flavour verwaltet die Menge an Rechen-, Speicher- und Speicherkapazität der Instanz.

HINWEIS:

Dem ausgewählten Flavour müssen genügend Ressourcen zugewiesen sein, um den Instanztyp zu unterstützen, den Sie erstellen möchten. Flavours, die nicht genügend Ressourcen für Ihre Instanz bereitstellen, werden in der verfügbaren Tabelle mit einem gelben Warnsymbol gekennzeichnet.

Administratoren sind für die Erstellung und Verwaltung von Geschmacksrichtungen verantwortlich. Klicken Sie auf den Pfeil (rechts), den Sie zuweisen möchten.

Launch Instance

Flavours manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> m1.large	4	8 GB	80 GB	80 GB	0 GB	Yes

Available 4 Select one

Click here for filters or full text search.

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> m1.tiny	1	512 MB	1 GB	1 GB	0 GB	Yes
> m1.small	1	2 GB	20 GB	20 GB	0 GB	Yes
> m1.medium	2	4 GB	40 GB	40 GB	0 GB	Yes
> m1.xlarge	8	16 GB	160 GB	160 GB	0 GB	Yes

9. Wählen Sie das Netzwerk aus und klicken Sie auf **Weiter**. Netzwerke stellen die Kommunikationskanäle für Instanzen bereit.

HINWEIS:

Ein Administrator wird die Provider-Netzwerke erstellt, und diese Netzwerke sind einem vorhandenen physischen Netzwerk im Rechenzentrum zugeordnet. Ähnlich werden Projekt-Netzwerke von Benutzern erstellt, und diese Netzwerke sind vollständig isoliert und projektspezifisch.

Launch Instance
✕

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud.

▼ **Allocated** 1 Select networks from those listed below.

Network	Subnets Associated	Shared	Admin State	Status
↕ 1 > public	public_subnet	Yes	Up	Active ↓

▼ **Available** 30 Select at least one network

Network	Subnets Associated	Shared	Admin State	Status
> 08c39ca9-c86e-4e80-8dd2-5b775497069c	09408ac1-6dfb-4381-bd2b-34c128f5280c	No	Up	Active ↑
> 0ce9e8b1-ad5d-4210-87dc-62917c827c17	76268f54-7faf-45ff-ae2a-b97fb72e3d6b	No	Up	Active ↑
> 26a6e41d-6f64-4f6b-b510-810938d9a669	c81c3a0e-e84e-46b1-9e29-3300b8e7323c	No	Up	Active ↑
> 272165f0-443b-4f81-9358-38a9e2ea0fa3	373b775b-9576-484d-abd8-9011362284da	No	Up	Active ↑
> test_4	subnet_4	No	Up	Active ↑
> 8b69e4a3-c47a-4821-bb17-09aca96a4fe9	ab3c53f6-ca4b-4958-aedf-7c444b21c257	No	Up	Active ↑
> test_1	subnet_1	No	Up	Active ↑
> Hw_provider3_vlan20	provider3_subnet	No	Up	Active ↑
> f1d4edbe-8272-400c-bba1-c350864eecd	366f5024-cf0a-4648-8053-c3fe946df958	No	Up	Active ↑
> f3158a09-c8dc-421a-9e8f-04814860b955	736e9da4-7526-4072-aa93-666071df24f8	No	Up	Active ↑
> test_3	subnet_3	No	Up	Active ↑
> network_ipv6	subnetwork_ipv6 ipv4_subnet	No	Up	Active ↑

✕ Cancel
< Back
Next >
Launch Instance

10. Wählen Sie einen Netzwerkport für die Instanz und klicken Sie auf **Weiter**. Netzwerkports stellen zusätzliche Kommunikationskanäle für die Instanzen bereit.

HINWEIS:

Sie können Ports anstelle von Netzwerken oder eine Mischung aus beiden auswählen.

Launch Instance

Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both.

Allocated 1 Select ports from those listed below.

Name	IP	Admin State	Status
tiny_mgmt	10.106.36.44 on subnet public_subnet	Up	Down

Available 31 Select one

Filter

Name	IP	Admin State	Status
3865f021-d8df-40a9-964a-7bb7f3728353	192.168.234.239 on subnet	Up	Down
3f7888d2-dd2b-487d-ad88-6cf3261ebf8b	192.168.234.113 on subnet	Up	Down
7847377d-6f82-4a7f-9e8d-26703bfc7b0b	192.168.234.240 on subnet	Up	Down
2bd26300-4af2-4503-8ec8-728ad5967c5f	192.168.237.88 on subnet	Up	Down
6ca1aeab-4b38-41f3-86cc-8973a3bfc3bd	192.168.240.223 on subnet	Up	Down
9dc0d02b-7933-4689-92a3-18c3177c7c0d	192.168.240.251 on subnet	Up	Down
c378ba39-0c61-4e35-8a2c-0419fa8c2989	192.168.240.4 on subnet	Up	Down
958ad235-94b0-4ccd-8f07-88539bc5b584	172.16.22.1 on subnet	Up	Down
Mgt-Port	10.106.36.41 on subnet public_subnet	Up	Down

Cancel < Back Next > Launch Instance

- 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.
- Aktivieren Sie das Kontrollkästchen **Konfigurationslaufwerk**. Wenn Sie das Konfigurationslaufwerk aktivieren, können Sie die Benutzermetadaten in das Image einfügen.

Launch Instance

You can customise your instance after it has launched using the options available here. "Customisation Script" is analogous to "User Data" in other systems.

Load Customisation Script from a file

Choose file No file chosen

Customisation Script (Modified) Content size: 213 bytes of 16.00 KB

```
#config
management_ip
address 10.106.36.43
netmask 255.255.255.0
gateway 10.106.36.1
dns
```

Disk Partition

Automatic

Configuration Drive

Cancel < Back Next > Launch Instance

13. Klicken Sie auf **Launch Instance**.

Konfigurieren der LTE-Funktionalität auf 210 SE LTE-Appliance

August 29, 2022

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. Informationen zum Konfigurieren und Verwalten von LTE-Sites in Ihrem Netzwerk finden Sie unter [LTE-Firmware-Upgrade](#).

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**.

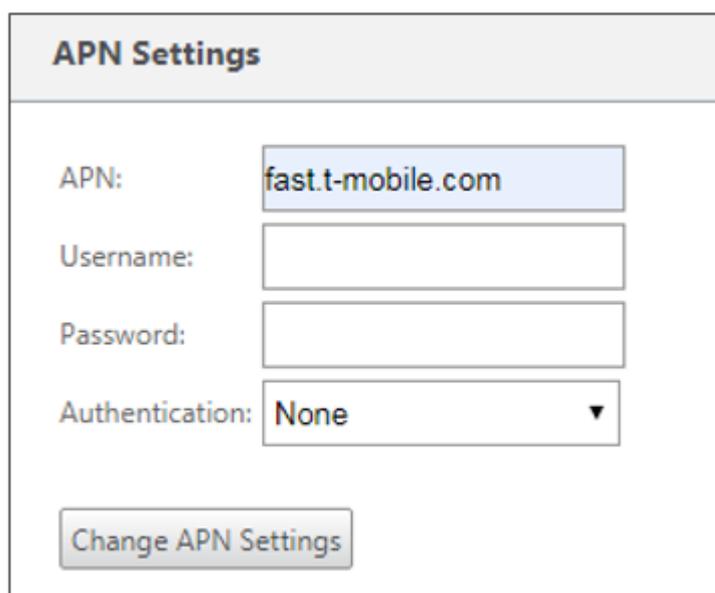


The screenshot shows a web interface for SIM Card configuration. At the top, there is a header 'SIM Card'. Below the header, there is a single button labeled 'Refresh SIM Card'.

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.



The screenshot shows the 'APN Settings' configuration page. The title is 'APN Settings'. The form contains the following fields:

- APN: fast.t-mobile.com
- Username: (empty text box)
- Password: (empty text box)
- Authentication: None (dropdown menu)

At the bottom of the form is a button labeled 'Change APN Settings'.

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.



Modem	Cellular network	Network
Type: 210-LTE-R1	Home Network: T-Mobile	IP Address/Gateway: 100.234.16.66/ 100.234.16.65
IMEI Number: 359073060554999	Radio Interface: LTE	Primary/Secondary DNS: 10.177.0.34/ 10.177.0.210
Status: Enabled	Signal Strength: Excellent	
Active Firmware: 02.24.05.06 GENERIC	Session State: CONNECTED	
IMEI Number: 310260186289688	APN Name: fast.t-mobile.com	
MS ISDN: 16692121835	Profile Name:	

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.

Status Info

Modem

Manufacture: Sierra Wireless, Incorporated
 Modem Type: 210-LTE-R1
 Modem Status: Enabled
 Active Firmware: 02.24.05.06_GENERIC
 Model Id: EM7455
 Firmware Revisions: SW09X30C_02.24.05.06_r7040_CARM-D-EV-FRMWR2_2017/05/19_06:23:09
 Boot Revisions: SW09X30C_02.24.05.06_r7040_CARM-D-EV-FRMWR2_2017/05/19_06:23:09
 PRL Revisions: 9907721.001.000_Generic-M2M
 PRL Version: 1
 PRL Preference: 0
 ICCID Number: 89012601837628968847
 ESN Number: 80BBAD37
 IMEI Number: 359073060554999
 MEID Number: 359073060554999
 IMSI Number: 310260186289688
 MSISDN: 16692121835
 Hardware Revision: 1.0
 Device State: READY

Cellular Network

Home Network: T-Mobile
 Roaming Status: Home
 Session State: CONNECTED
 Data Bearer: GPRS
 Dormancy Status: Traffic Channel Active
 LUJ Reject Cause: 0
 Card State: Ready

Call Statistics

Call Status: CONNECTED
 Bytes Transferred: 317984
 Bytes Received: 0

RF Information

Radio Interface: LTE
 Active Band Class: 123
 Active Channel: 2300
 Signal Strength: Excellent
 ECIO: 0
 IO: 0
 SINR: 0
 RSRQ: -19

Profile

POP Type: IPv4
 Authentication: 0
 Profile Name:
 APN Name: fast.t-mobile.com
 User Name:
 IP Address: 100.234.16.66
 Gateway Address: 100.234.16.65
 Primary DNS: 10.177.0.34
 Secondary DNS: 10.177.0.210

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**.

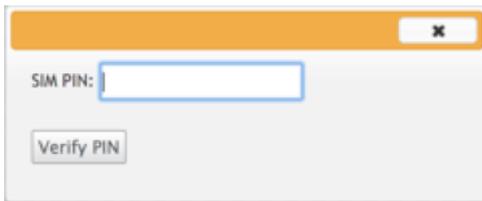
SIM PIN

SIM PIN Status

PIN State: Enabled and Not Verified
 PIN Tries: 3
 PUK Tries: 10

Disable PIN Verify PIN Modify PIN

Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.

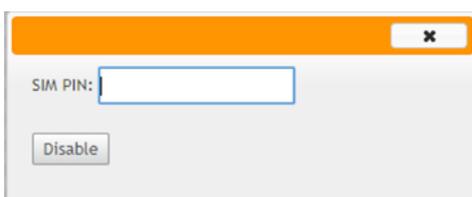


Der Status ändert sich in **Aktiviert und Verifiziert**.



SIM-PIN deaktivieren

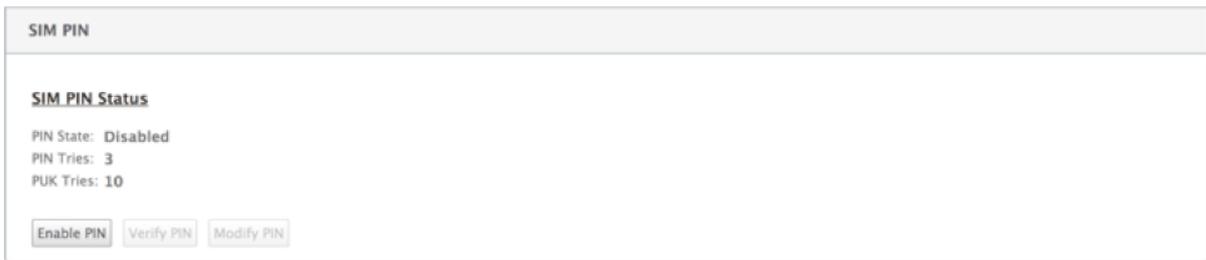
Sie können die SIM-PIN-Funktionalität für eine SIM-Karte deaktivieren, für die SIM-PIN aktiviert und verifiziert ist.



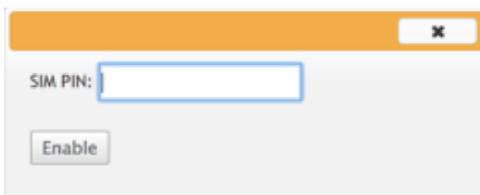
Klicken Sie auf **PIN deaktivieren**. Geben Sie die **SIM-PIN** ein und klicken Sie auf **Deaktivieren**.

SIM-PIN aktivieren

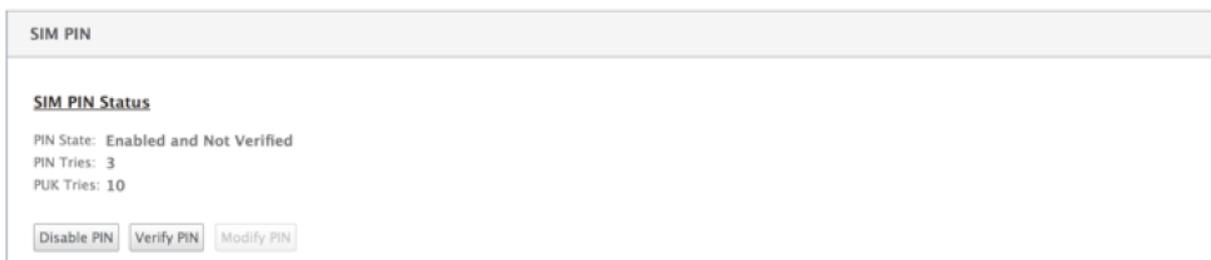
Die SIM-PIN kann für die SIM aktiviert werden, für die sie deaktiviert ist.



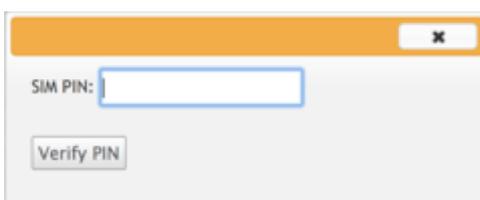
Klicken Sie auf **PIN aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**.



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.

SIM PIN

SIM PIN Status

PIN State: **Enabled and Verified**

PIN Tries Remaining: **3**

PUK Tries Remaining: **10**

Klicken Sie auf **PIN ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **PIN ändern**.

✕

Old SIM PIN:

New SIM PIN:

Confirm New SIM PIN:

SIM aufheben

Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe der vom Träger erhaltenen SIM-PUK zurücksetzen.

IP Address
Ethernet
Mobile Broadband

Status Info

This SIM Card is **Blocked**. Please contact the carrier service for a PUK code to unblock the SIM card.

PIN State: **Blocked**

PIN Tries: **3**

PUK Tries: **10**

Um die Blockierung einer SIM aufzuheben, klicken Sie auf **Sperre aufheben**. Geben Sie die **SIM-PIN** und die **SIM-PUK** ein, die Sie vom Mobilfunkanbieter erhalten haben, und klicken Sie auf **Sperre aufheben**.

✕

SIM PIN:

SIM PUK:

Hinweis:

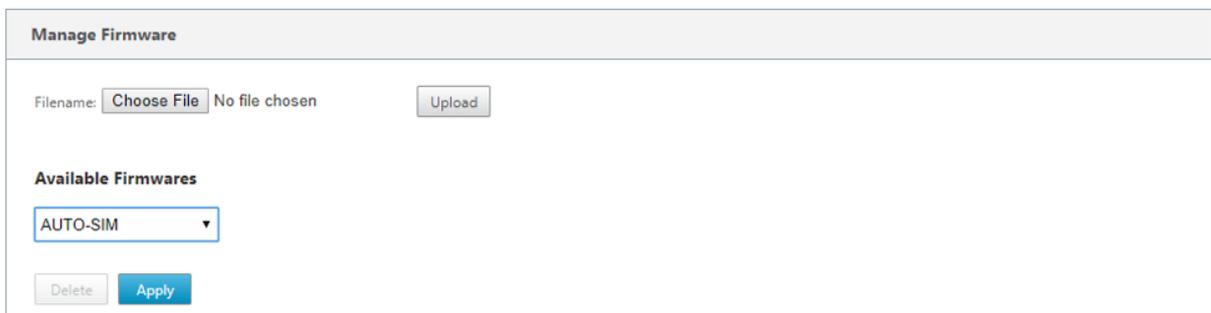
Die SIM-Karte wird mit 10 erfolglosen PUK-Versuchen dauerhaft blockiert, während die SIM-Karte entsperrt wird. Wenden Sie sich an den Mobilfunkanbieter, um eine neue SIM-Karte zu erhalten.



Firmware verwalten

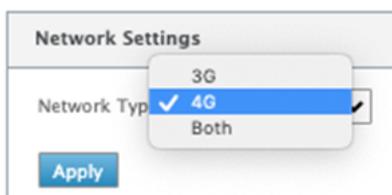
Jedes Gerät, das LTE aktiviert hat, verfügt über eine Reihe verfügbarer Firmware. Sie können aus der vorhandenen Firmware-Liste auswählen oder eine Firmware hochladen und anwenden.

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.



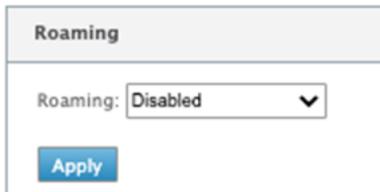
Netzwerkeinstellungen

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



Roaming

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



The screenshot shows a configuration panel titled "Roaming". Inside the panel, there is a label "Roaming:" followed by a dropdown menu currently showing "Disabled". Below the dropdown is a blue "Apply" button.

Modem aktivieren/deaktivieren

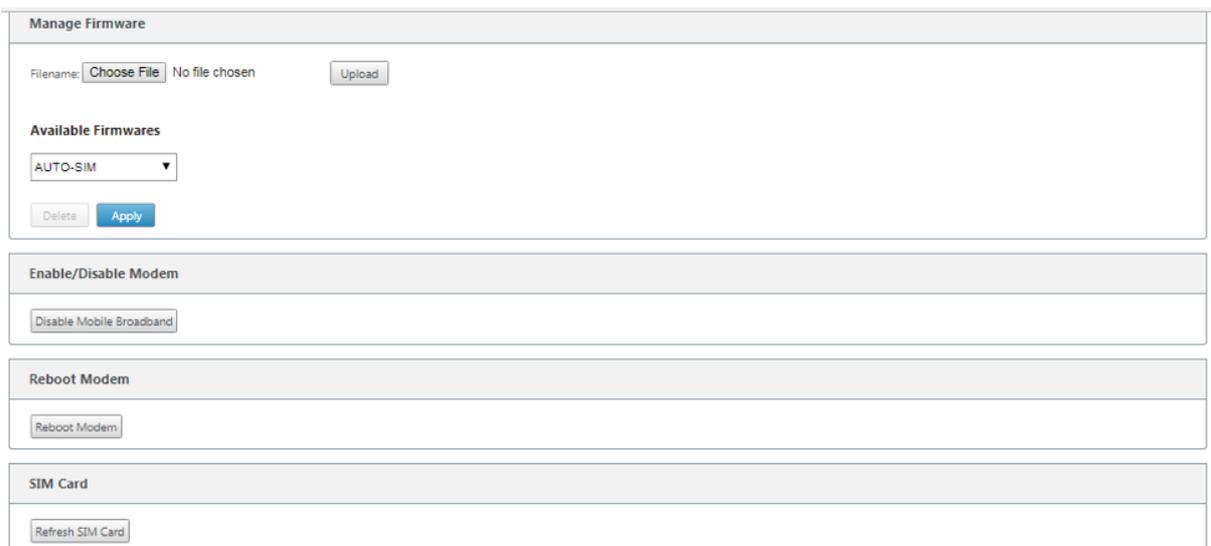
Aktivieren/deaktivieren Sie das Modem abhängig von Ihrer Absicht, die LTE-Funktionalität zu verwenden. Standardmäßig ist das LTE-Modem aktiviert.

Modem neu starten

Startet das Modem neu. Es kann bis zu 3-5 Minuten dauern, bis der Neustartvorgang abgeschlossen ist.

SIM aktualisieren

Verwenden Sie diese Option, wenn Sie die SIM-Karte per Hot-Swap austauschen, um die neue SIM-Karte durch das 210-SE LTE-Modem zu erkennen.



The screenshot displays a series of control panels. The first panel, "Manage Firmware", contains a "Filename:" field with a "Choose File" button and "No file chosen" text, and an "Upload" button. Below it is the "Available Firmwares" section with a dropdown menu set to "AUTO-SIM" and "Delete" and "Apply" buttons. The second panel, "Enable/Disable Modem", features a "Disable Mobile Broadband" button. The third panel, "Reboot Modem", has a "Reboot Modem" button. The fourth panel, "SIM Card", includes a "Refresh SIM Card" button.

Konfigurieren der LTE-Funktionalität mit CLI

Konfigurieren des 210-SE LTE-Modems mithilfe der CLI.

1. Melden Sie sich bei der Citrix SD-WAN Appliance-Konsole an.
2. Geben Sie an der Eingabeaufforderung den Benutzernamen und das Kennwort ein, um Zugriff auf die CLI-Schnittstelle zu erhalten.
3. Geben Sie an der Eingabeaufforderung den Befehl ein **lte**. Tippen Sie **>help**. Hier wird die Liste der für die Konfiguration verfügbaren LTE-Befehle angezeigt.

```

site210>lte
lte>help
status                # Show status
show                  # Show settings
disable               # Disable LTE modem
enable                # Enable LTE modem
apn <apn> [<user name> [<password> [<PAP|CHAP|PAPCHAP>]]] # Set APN
sim-power <off|on|reset> # Off, on, reset SIM card power
sim-pin <show>        # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin> # Modify SIM card PIN
sim-pin <unlock> <sim puk> <sim pin> # Unblock SIM card PIN
reboot                # Reboot modem
ping                  # Check if modem manager ready
list-fw               # List available firmware
apply-fw <fw>        # Apply the specified firmware

```

In der folgenden Tabelle sind die Beschreibungen des **LTE**-Befehls aufgeführt.

Befehl	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
Enable {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, SIM-Karte einschalten, SIM-Karte aktualisieren
SIM PIN {lte>sim-pin}	Schaltet die SIM-Karte aus, SIM-Karte einschalten, SIM-Karte aktualisieren
Reboot {lte>reboot}	Neustart des LTE-Modems
Ping {lte>ping}	Pings LTE-Modem

Befehl	Beschreibung
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

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 der Internetdienst für die LTE-Schnittstelle definiert ist.

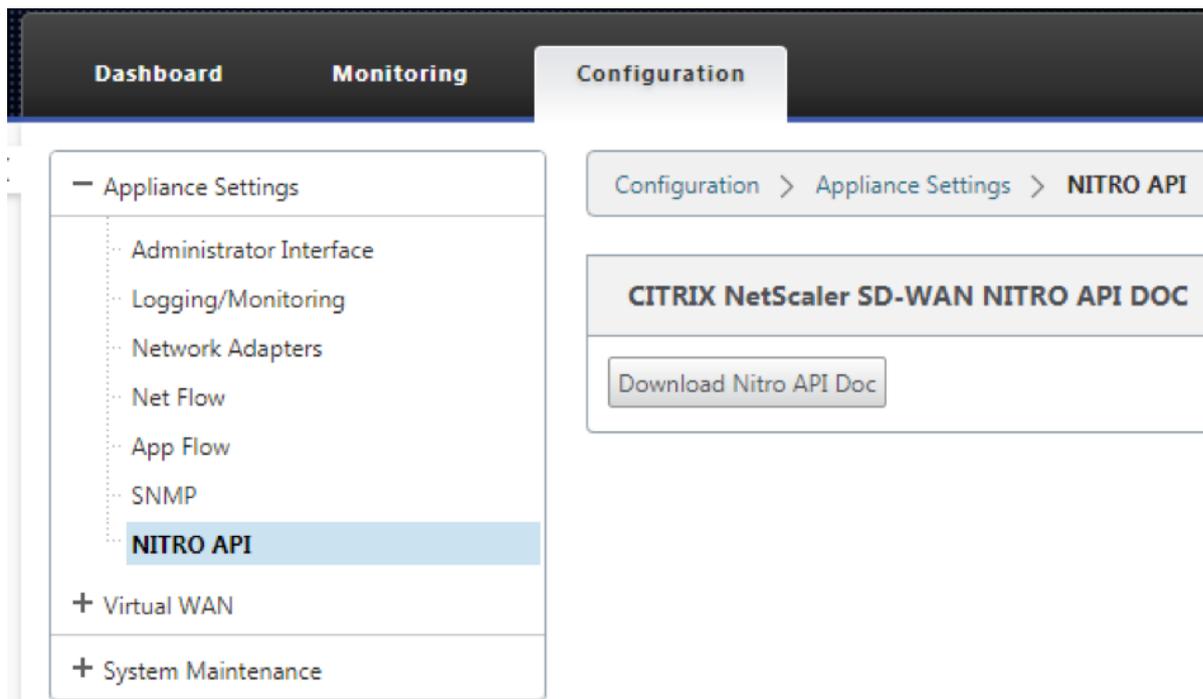
Wenn die Appliance eingeschaltet ist, verwendet der Zero-Touch-Bereitstellungsdienst den LTE-Port, um die neueste SD-WAN-Software und SD-WAN-Konfiguration nur dann abzurufen, wenn der Management-Port nicht angeschlossen wurde.

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

Um Informationen zur LTE-REST-API zu erhalten, navigieren Sie zur SD-WAN GUI und gehen Sie zu **Konfiguration > Appliance-Einstellungen > NITRO-API**. Klicken Sie auf **Nitro API Doc herunterladen**. Die REST-API für SIM-PIN-Funktionalität wird in Citrix SD-WAN 11.0 eingeführt.



AT-Befehle

AT-Befehle helfen bei der Überwachung und Fehlerbehebung der Konfiguration und des Status von LTE-Modem. AT ist die Abkürzung für **Attension**. Da jede Befehlszeile mit **at** beginnt, werden sie AT-Befehle genannt. Citrix SD-WAN-Plattformmodelle, die LTE unterstützen, unterstützen die Ausführung von AT-Befehlen. AT-Befehle sind modemspezifisch und daher variiert die Liste der AT-Befehle plattformübergreifend.

Führen Sie die folgenden Schritte aus, um AT-Befehle auszuführen:

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 **lte** ein.
4. Geben Sie **at** ein und geben Sie dann den AT-Befehl ein.

Ein Beispiel:

- **bei at+cpin** —Bietet SIM-Statusinformationen.

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
+CPIN: READY
OK
success
```

- **bei bei! gstatus** - Bietet Statusinformationen für LTE-Modem.

```
lte> at at!gstatus?
Running at!gstatus? command
AT command state: success
!GSTATUS:
Current Time: 1279298           Temperature: 62
Reset Counter: 1               Mode: ONLINE
System mode: LTE               PS state: Attached
LTE band: B5                   LTE bw: 10 MHz
LTE Rx chan: 2559             LTE Tx chan: 20559
LTE CA state: NOT ASSIGNED
EMM state: Registered          Normal Service
RRC state: RRC Connected
IMS reg state: Full Srv        IMS mode: Normal
PCC RxM RSSI: -73              RSRP (dBm): -112
PCC RxD RSSI: -73              RSRP (dBm): -107
Tx Power: --                   TAC: 1F00 (7936)
RSRQ (dB): -17.3               Cell ID: 00798912 (7964946)
SINR (dB): 0.2
OK
Success
```

- **bei bei! beeindrucken?** - Bietet Modem-Firmware und Netzwerkbetreiberinformationen.

```
lte> at at!impref?
Running at!impref? command
AT command state: success
!IMPREF:
preferred fw version: 00.00.00.00
preferred carrier name: AUTO-SIM
preferred config name: AUTO-SIM_000.000_000
preferred subpri index: 000
current fw version: 02.33.03.00
current carrier name: VERIZON
current config name: VERIZON_002.079_001
current subpri index: 000
OK
success
```

Konfigurieren der LTE-Funktionalität auf 110-LTE-WiFi-Appliance

August 29, 2022

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.
- Informationen zur Konfiguration und Verwaltung aller LTE-Sites in Ihrem Netzwerk finden Sie unter [LTE-Firmware-Vorlage](#).

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.

APN Settings

SIM:

APN:

Username:

Password:

Authentication:

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

Hinweis

Alle diese Felder sind optional.

6. Klicken Sie auf **APN-Einstellungen ändern**.
7. Navigieren Sie in der Benutzeroberfläche der **SD-WAN-Appliance** zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Mobiles Breitband**.

Sie können die Statusinformationen für mobile Breitbandeinstellungen anzeigen.

Status Info ?

<u>Modem</u>	<u>Cellular network</u>	<u>Network</u>
Operating Mode: online	Home Network: airtel	IP Address/Gateway: 100.105.88.189/100.105.88.190
IMEI Number: 867698040397609	Radio Interface: lte	Primary/Secondary DNS: 125.22.47.102/59.144.144.106
Active SIM: SIM One	Signal Strength: Excellent	
IMSI Number: 404450986042323	Session State: connected	
ICCID Number: 8991000902637718627f	APN Name:	
Card State (SIM One): present	Card State (SIM Two): absent	

Im Folgenden finden Sie einige nützliche Statusinformationen:

- **Betriebsart:** Zeigt den Modemstatus an.
- **Aktive SIM:** Zu einem bestimmten Zeitpunkt kann nur eine SIM aktiv sein. Die aktuell aktive SIM wird angezeigt.
- **Kartenstatus:** Vorhanden zeigt an, dass die SIM ordnungsgemäß eingelegt ist.
- **Signalstärke:** Qualität der Signalstärke - ausgezeichnet, gut, fair, schlecht oder kein Signal.
- **Heimnetzwerk:** Träger der eingelegten SIM-Karte.

- **APN-Name:** Der vom LTE-Modem verwendete Zugriffspunktname.
- **Sitzungsstatus:** Verbunden zeigt an, dass das Gerät dem Netzwerk beigetreten ist. Wenn der Sitzungsstatus getrennt ist, erkundigen Sie sich beim Mobilfunkanbieter, ob das Konto aktiviert ist und der Datenplan aktiviert ist.

SIM-Präferenz

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

- **SIM One bevorzugt:** Wenn zwei SIM-Karteneingesteckt 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 Preference

Preferred SIM: SIM One preferred ▼

Apply

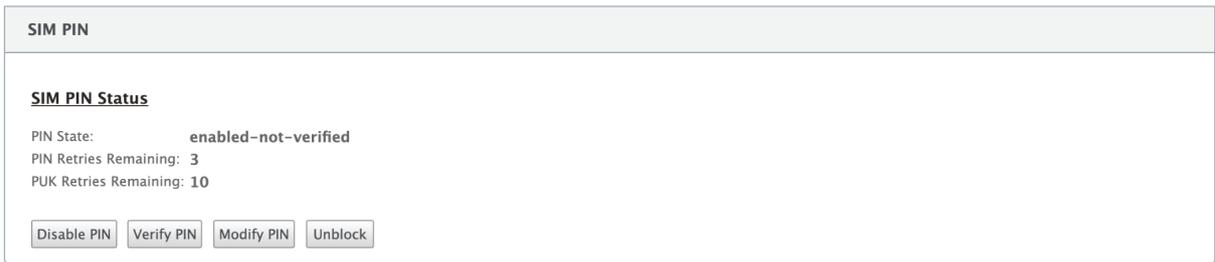
SIM-PIN

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

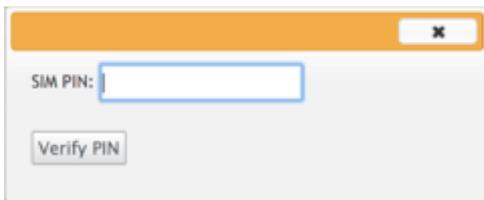
Hinweis

Die SIM-PIN-Vorgänge gelten nur für die aktive SIM.

Um SIM-PIN-Vorgänge durchzuführen, navigieren Sie zu **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Mobiles Breitband > SIM-PIN**.



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”**.

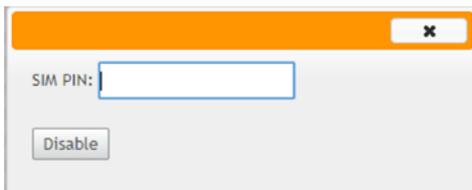


SIM-PIN deaktivieren

Sie können die SIM-PIN-Funktionalität für eine SIM-Karte deaktivieren, für die SIM-PIN aktiviert und verifiziert ist.

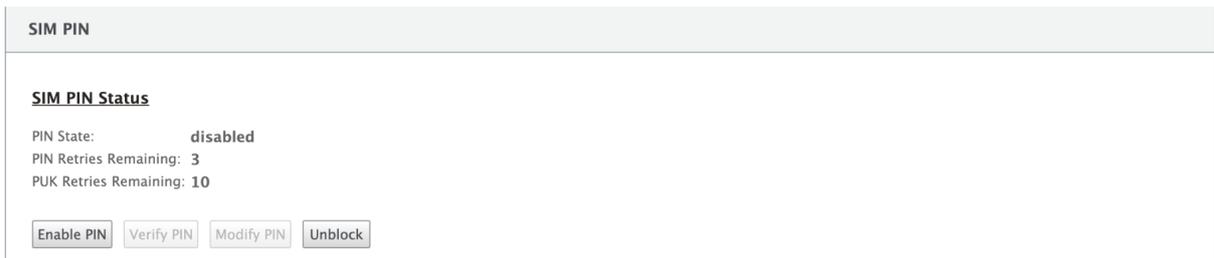


Klicken Sie auf **PIN deaktivieren**. Geben Sie die **SIM-PIN** ein und klicken Sie auf **Deaktivieren**.



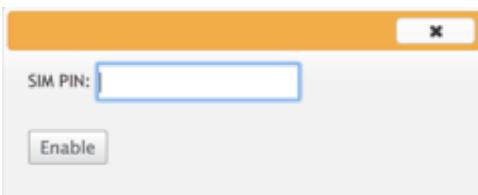
SIM-PIN aktivieren

Die SIM-PIN kann für die SIM aktiviert werden, für die sie deaktiviert ist.



The screenshot shows a web interface titled "SIM PIN". Under the heading "SIM PIN Status", the following information is displayed: "PIN State: disabled", "PIN Retries Remaining: 3", and "PUK Retries Remaining: 10". Below this information are four buttons: "Enable PIN", "Verify PIN", "Modify PIN", and "Unblock".

Klicken Sie auf **PIN aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**.



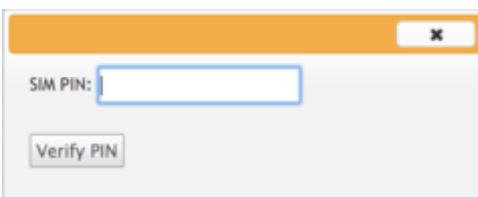
The screenshot shows a dialog box with a title bar. Inside, there is a label "SIM PIN:" followed by a text input field. Below the input field is an "Enable" button.

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.



The screenshot shows a web interface titled "SIM PIN". Under the heading "SIM PIN Status", the following information is displayed: "PIN State: enabled-not-verified", "PIN Retries Remaining: 3", and "PUK Retries Remaining: 10". Below this information are four buttons: "Disable PIN", "Verify PIN", "Modify PIN", and "Unblock".

Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.



The screenshot shows a dialog box with a title bar. Inside, there is a label "SIM PIN:" followed by a text input field. Below the input field is a "Verify PIN" button.

SIM-PIN ändern

Sobald sich die PIN im Status **“Aktiviert”** befindet, können Sie die PIN ändern.

SIM PIN

SIM PIN Status

PIN State: **enabled-verified**
 PIN Retries Remaining: 3
 PUK Retries Remaining: 10

Klicken Sie auf **PIN ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **PIN ändern**.

✕

Old SIM PIN:

New SIM PIN:

Confirm New SIM PIN:

SIM aufheben

Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe der vom Träger erhaltenen SIM-PUK zurücksetzen.

Status Info

This SIM Card is **Blocked**. Please contact the carrier service for a PUK code to unblock the SIM card.

PIN State: **Blocked**
 PIN Tries: 3
 PUK Tries: 10

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**.

✕

SIM PIN:

SIM PUK:

Hinweis:

Die SIM-Karte wird mit 10 erfolglosen PUK-Versuchen dauerhaft blockiert, während die SIM-Karte

entsperrt wird. Sie müssen sich an den Anbieter für eine neue SIM-Karte wenden.



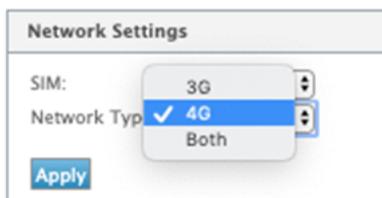
Netzwerkeinstellungen

Sie können das Mobilfunknetz auf den Citrix SD-WAN-Appliances auswählen, die interne LTE-Modems 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.



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 <unlock> <sim puk> <sim pin> # Unblock SIM card PIN
  reboot                # Reboot modem
  list-fw               # List available firmware
  upload-fw <fw file>  # Upload firmware file
  apply-fw <fw> [keep-AUTO-SIM] # Apply firmware
  delete-fw <fw>      # Delete firmware
  session <show|stop|start> # Show/stop/start data session
  exit|quit             # Exit LTE CLI

```

In der folgenden Tabelle sind die Beschreibungen des **LTE**-Befehls aufgeführt.

Befehl	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
Enable {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 [1 2] [1 2] {lte>select [1 2] [1 2]}	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-bezogenen Vorgänge werden auf der 110-LTE-WiFi-Appliance nicht unterstützt.

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 für die Konfiguration der 110-LTE-WiFi-Appliance der Internetdienst für die LTE-Schnittstelle definiert ist.

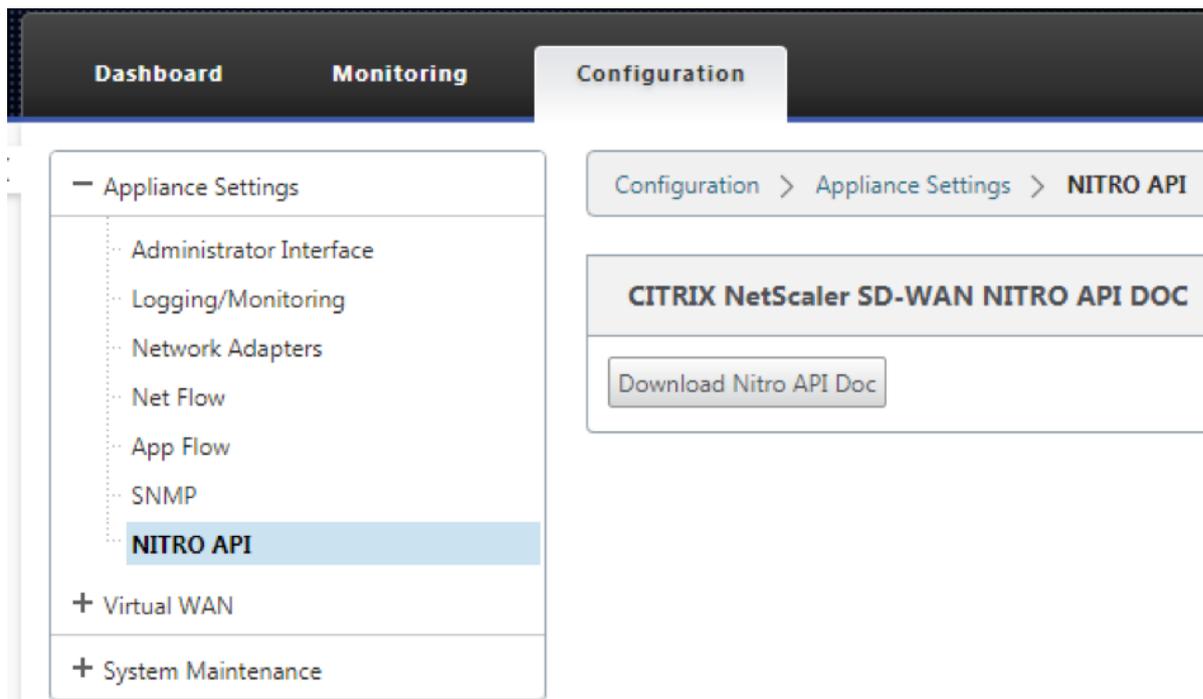
Wenn die Appliance eingeschaltet ist, verwendet der Zero-Touch-Bereitstellungsdienst den LTE-Port, um die neueste SD-WAN-Software und SD-WAN-Konfiguration zu erhalten.

Zero-Touch-Bereitstellung Service über Management-/Datenschnittstelle für 110-SE LTE Appliance

Verbinden Sie den Verwaltungs-/Datenport mit dem Internet und verwenden Sie das standardmäßige [Zero-Touch-Bereitstellungsverfahren](#), das auf allen anderen Nicht-LTE-Plattformen unterstützt wird.

LTE REST API

Um Informationen zur LTE-REST-API zu erhalten, navigieren Sie zur SD-WAN GUI und gehen Sie zu **Konfiguration > Appliance-Einstellungen > NITRO-API**. Klicken Sie auf **Nitro API Doc herunterladen**. Die REST-API für SIM-PIN-Funktionalität wird in Citrix SD-WAN 11.0 eingeführt.



AT-Befehle

AT-Befehle helfen bei der Überwachung und Fehlerbehebung der Konfiguration und des Status von LTE-Modem. AT ist die Abkürzung für **Attension**. Da jede Befehlszeile mit **at** beginnt, werden sie AT-Befehle genannt. Citrix SD-WAN-Plattformmodelle, die LTE unterstützen, unterstützen die Ausführung von AT-Befehlen. AT-Befehle sind modemspezifisch und daher variiert die Liste der AT-Befehle plattformübergreifend.

Führen Sie die folgenden Schritte aus, um AT-Befehle auszuführen:

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 **lte** ein.
4. Geben Sie **at** ein und geben Sie dann den AT-Befehl ein.

Ein Beispiel:

- **bei at+cpin** —Bietet SIM-Statusinformationen.

```
lte> at at+cpin?  
Running at+cpin? command  
AT command state: success  
+CPIN: READY  
OK  
success
```

Konfigurieren eines externen USB-LTE-Modems

August 29, 2022

Sie können ein externes 3G/4G-USB-Modem auf bestimmten Citrix SD-WAN Appliances anschließen. Die Appliances verwenden das 3G/4G-Netzwerk zusammen mit anderen Verbindungen, um ein virtuelles Netzwerk zu bilden, das Bandbreite aggregiert und Ausfallsicherheit bietet. Wenn auf den anderen Schnittstellen ein Verbindungsfehler auftritt, wird der Datenverkehr automatisch über das USB-LTE-Modem umgeleitet. Die folgenden Appliances unterstützen ein externes USB-Modem:

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 Wi-Fi SE
- Citrix SD-WAN 110 LTE Wi-Fi SE
- Citrix SD-WAN 1100 SE
- Citrix SD-WAN 2100 SE

Die [Citrix SD-WAN 210 SE LTE](#) und [Citrix SD-WAN 110 LTE Wi-Fi SE](#) Appliances verfügen über ein eingebautes LTE-Modem. Aktives Dual LTE wird auf diesen Geräten unterstützt.

CDC Ethernet, MBIM und NCM sind die drei unterstützten externen USB-Modems. Sie können die **APN-Einstellungen** und das Aktivieren/Deaktivieren des Modems auf MBIM- und NCM-USB-Modems konfigurieren. Mobile Breitbandvorgänge werden auf CDC Ethernet USB-Modems nicht unterstützt.

Hinweis

Die externen LTE-Dongles mit Modemtyp als MBIM funktionieren nicht auf der Citrix SD-WAN 2100-Plattform.

Anschließen des USB-Modems

Aktivieren und testen Sie das USB-Modem gemäß den Richtlinien Ihres Mobilfunkanbieter.

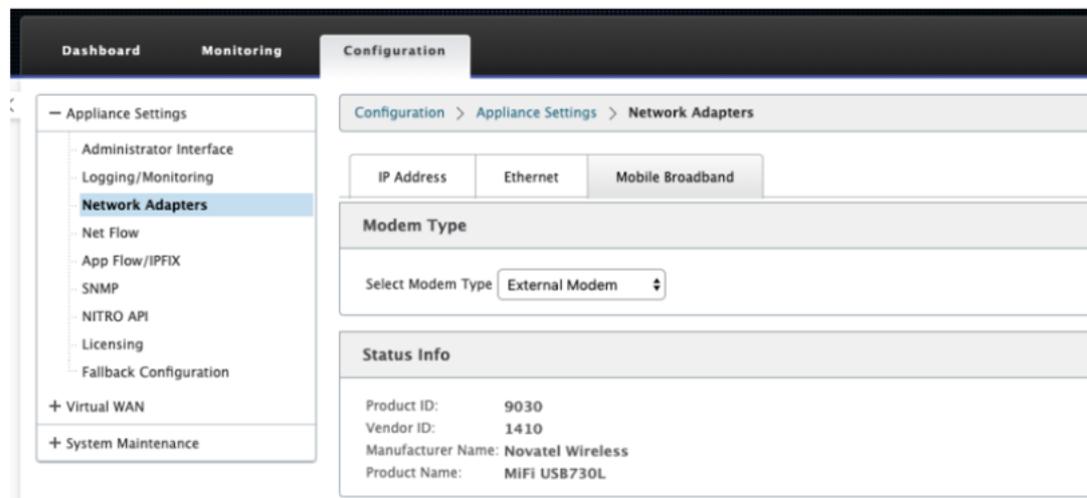
Perquisites für externes LTE-Modem:

- 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

Konfigurieren des externen USB-Modems

Sie können LTE-Sites mit einem externen USB-Modem über den Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [LTE-Firmware-Upgrade](#).

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 für die 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.

Informationen zur Zero-Touch-Bereitstellung über den SD-WAN Orchestrator Service 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

Region	Wireless Carrier/ Manufacturer	USB-Modem	Unterstützter Modemtyp	Schnittstellen
USA	AT&T	AT&T Globales Modem USB800	cdc_ether	Nur 4G

AT-Befehle

AT-Befehle helfen bei der Überwachung und Fehlerbehebung der Konfiguration und des Status von LTE-Modem. AT ist die Abkürzung für **Attension**. Da jede Befehlszeile mit **at** beginnt, werden sie AT-Befehle genannt. Citrix SD-WAN-Plattformmodelle, die LTE unterstützen, unterstützen die Ausführung von AT-Befehlen. AT-Befehle sind modemspezifisch und daher variiert die Liste der AT-Befehle plattformübergreifend.

Führen Sie die folgenden Schritte aus, um AT-Befehle auszuführen:

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 **lte** ein.
4. Geben Sie **at** ein und geben Sie dann den AT-Befehl ein.

Ein Beispiel:

bei at+cpin —Bietet SIM-Statusinformationen.

```
lte> at at+cpin?  
Running at+cpin? command  
AT command state: success  
+CPIN: READY  
OK  
success
```

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
- WAN-zu-WAN-Weiterleitung
- Aufbau eines SD-WAN-Netzwerks
- Routing für die LAN-Segmentierung
- Zero Touch-Bereitstellung
- Bereitstellung einer einzelnen Region
- Bereitstellung mit mehreren Regionen
- Hohe Verfügbarkeit

Checkliste und Bereitstellung

August 29, 2022

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 Editionen erforderlich sind.

Informationen zu einigen Anwendungsfällen 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
 - Sitenamen
 - Geräte Namen (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

August 29, 2022

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 gut, für ARP-Anfragen LAN-Next-Hop als Proxy zu verwenden, 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 befindetet, 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).

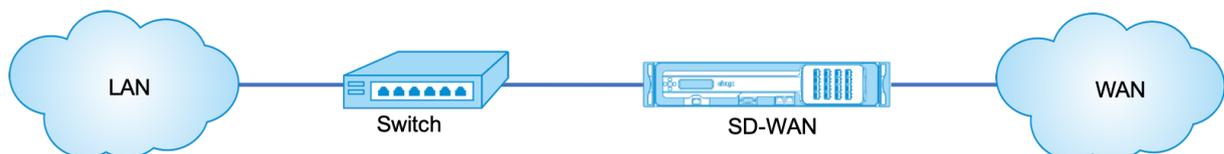
Gateway-Modus

August 29, 2022

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

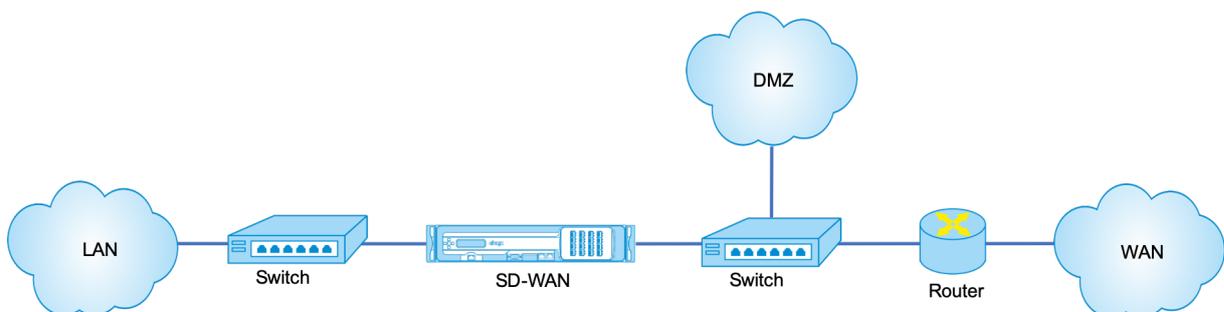
Der Gateway-Bereitstellungsmodus wird vom Citrix SD-WAN Orchestrator Service unterstützt. Weitere Informationen finden Sie unter [Schnittstellen](#).



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.

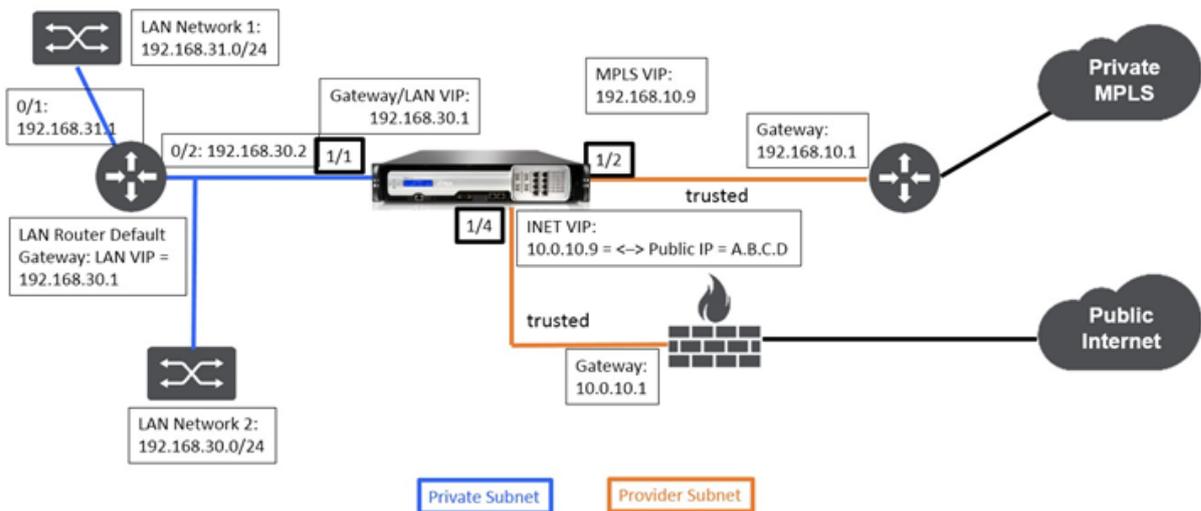


Dieser Artikel enthält schrittweise Verfahren zum Konfigurieren einer SD-WAN-Appliance im Gateway-Modus in einem Beispielnetzwerk-Setup. Die Inline-Bereitstellung wird auch für die Zweigseite beschrieben, um die Konfiguration abzuschließen. Ein Netzwerk kann weiterhin funktionieren, wenn ein Inline-Gerät entfernt wird, verliert jedoch jeglichen Zugriff, wenn das Gateway-Gerät entfernt wird.

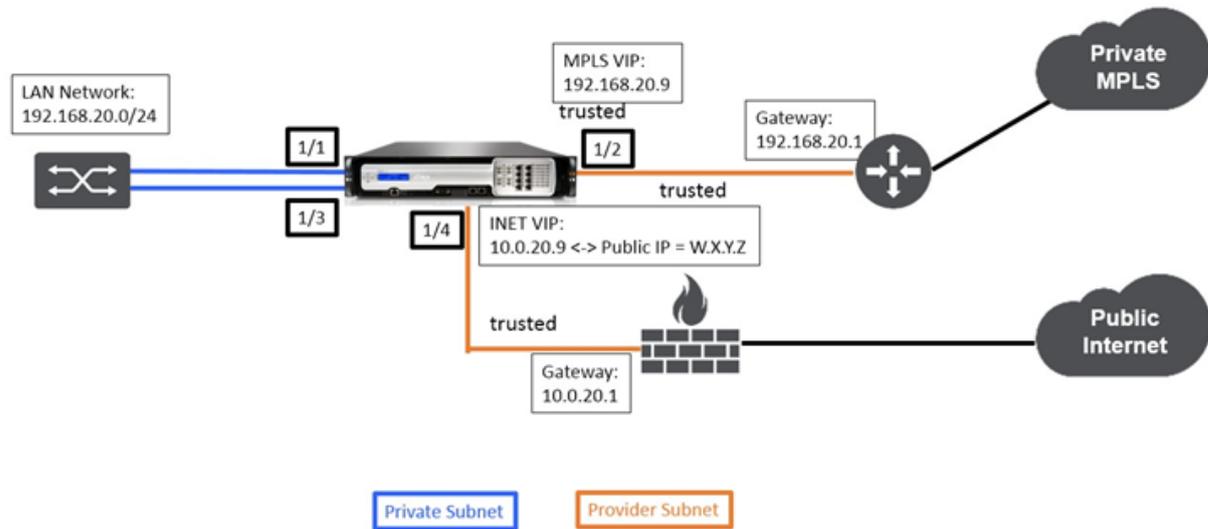
Topologie

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



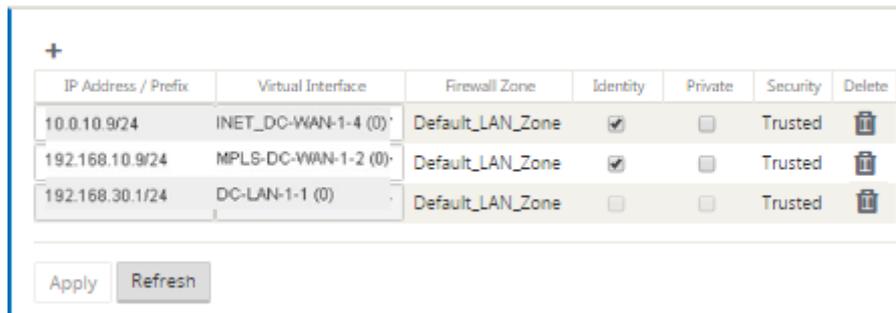
Konfiguration des Sitegatewaymodus für Rechenzentren

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 VIP-Adresse (Virtual IP) für jede virtuelle Schnittstelle

1. Erstellen Sie für jeden WAN-Link im entsprechenden Subnetz eine VIP. VIPs werden für die Kommunikation zwischen zwei SD-WAN-Appliances in der virtuellen WAN-Umgebung verwendet.
2. Erstellen Sie eine virtuelle IP-Adresse, die als Gateway-Adresse für das LAN-Netzwerk verwendet werden soll.



IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.0.10.9/24	INET_DC-WAN-1-4 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.10.9/24	MPLS-DC-WAN-1-2 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.30.1/24	DC-LAN-1-1 (0)	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply Refresh

So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten mithilfe des Internetlinks aus:

1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+ Link hinzufügen**, um einen WAN-Link für den Internet-Link hinzuzufügen.
2. Geben Sie Informationen zum Internetlink ein, einschließlich der angegebenen öffentlichen IP-Adresse, wie unten dargestellt. AutoDetect **Public IP** kann nicht für SD-WAN-Appliance ausgewählt werden, die als MCN konfiguriert ist.
3. Navigieren Sie im 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.

WAN Link: BR571-WL-1 Section: Settings + Add Link Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name: BR571-WL-1

Access Type: Public Internet WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

Set Permitted From Physical Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

Set Permitted From Physical Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_DC-INET-AI-1	INET_DC-WAN-1-4	10.0.10.9	10.0.10.1	Primary	<input type="checkbox"/>	

So erstellen Sie eine MPLS-Verbindung

1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+**, um einen WAN-Link für den MPLS-Link hinzuzufügen.
2. Füllen Sie MPLS-Link-Details wie unten gezeigt.
3. Navigieren Sie zu **Access Interfaces**, klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den MPLS-Link hinzuzufügen.
4. Füllen Sie das Access Interface für IP- und Gateway Adressen wie unten dargestellt aus.

Basic Settings
?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

Access Type: WAN Link Template:

LAN to WAN

Physical Rate (kbps):

Set Permitted From Physical

Permitted Rate (kbps):

WAN to LAN

Physical Rate (kbps):

Set Permitted From Physical

Permitted Rate (kbps):

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_DC-MPLS-...	MPLS-DC-WAN-1-2	192.168.10.9	192.168.10.1	Primary	<input type="checkbox"/>	

So füllen Sie Routen aus

Routen werden 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 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.



IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.0.20.9/24	INET_BR-3-4 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.20.9/24	MPLS_BR-1-2 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.113.58.8/24	VirtualInterface-2	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply Refresh

So füllen Sie WAN-Verbindungen basierend auf physischer Rate und nicht auf Burst-Geschwindigkeiten mithilfe des Internetlinks aus:

1. Navigieren Sie zu **WAN-Links**, klicken Sie auf die Schaltfläche **+**, um einen WAN-Link für den Internetlink hinzuzufügen.
2. Füllen Sie Details zum Internetlink, einschließlich der öffentlichen IP-Adresse Auto Detect, wie unten dargestellt.
3. Navigieren Sie zu **Access Interfaces**, klicken Sie auf die Schaltfläche **+**, um Schnittstellendetails für den Internetlink hinzuzufügen.
4. Fügen Sie das Access Interface für IP-Adresse und Gateway wie unten gezeigt ein.

WAN Link: BR571-WL-1 Section: Settings + Add Link Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name: BR571-WL-1

Access Type: Public Internet WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

Set Permitted From Physical Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

Set Permitted From Physical Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-INET-AI-1	INET_BR-3-4	10.0.20.9	10.0.20.1	Primary	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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 Schnittstellendetails für den MPLS-Link hinzuzufügen.
4. Fügen Sie das Access Interface für IP-Adresse und Gateway wie unten gezeigt ein.

Basic Settings
?

Note: Changing the access type of this **WAN Link** may cause automatically generated **Paths** to this link to be added or removed.

Link Name:

Access Type: Private MPLS WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps):

Set Permitted From Physical

Permitted Rate (kbps):

WAN to LAN

Physical Rate (kbps):

Set Permitted From Physical

Permitted Rate (kbps):

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-MPLS-...	MPLS_BR-1-2	192.168.20.9	192.168.20.1	Primary	<input checked="" type="checkbox"/>	

So füllen Sie Routen aus

Routen werden automatisch basierend auf der obigen Konfiguration erstellt. Falls es mehr Subnetze für diese Remote-Zweigstelle gibt, müssen bestimmte Routen hinzugefügt werden, die angeben, welches Gateway den Datenverkehr leitet, um diese Back-End-Subnetze zu erreichen.

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.0.20.9/24	5	Local					
2	192.168.20.9/24	5	Local	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5						
9	0.0.0.0/0	65535	Passthrough					

« < 1 > »

Beheben von Überwachungsfehlern

Nach Abschluss der Konfiguration für DC- und Zweigstandorte werden Sie benachrichtigt, um Überwachungsfehler auf DC- und BR-Standorten zu beheben.

Standardmäßig generiert das System Pfade für WAN-Links, die als Zugriffstyp Public Internet definiert sind. Sie müssen die Autopfad-Gruppenfunktion verwenden oder Pfade manuell für WAN-Links mit dem Zugriffstyp Privates Internet aktivieren. Pfade für MPLS-Links können durch Klicken auf Operator hinzufügen (im grünen Rechteck) aktiviert werden.

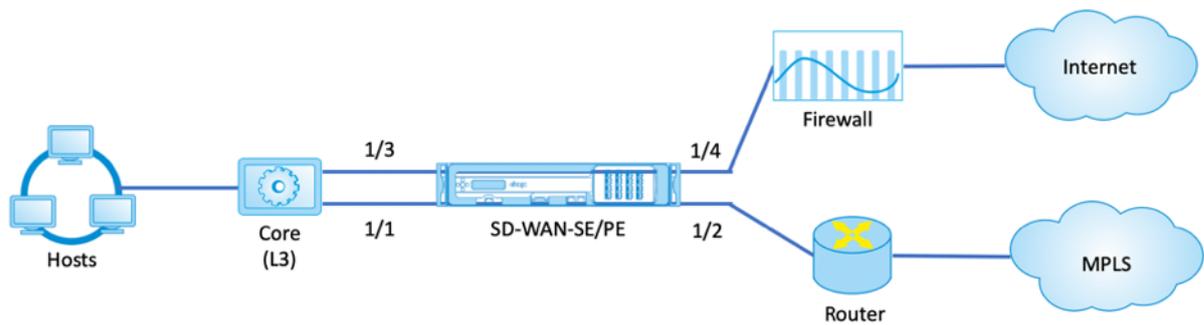
Nachdem Sie alle oben genannten Schritte ausgeführt haben, fahren Sie mit [Vorbereiten der SD-WAN-Appliance-Paket](#) fort. —>

Inlinemodus

August 29, 2022

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. Weitere Informationen zur dienstbasierten SD-WAN Orchestrator-Bereitstellung im Inlinemodus finden Sie unter [Schnittstellen](#).



Virtueller Inline-Modus

August 29, 2022

Im virtuellen Inlinemodus verwendet der Router ein Routing-Protokoll wie PBR, OSPF oder BGP, um eingehenden und ausgehenden WAN-Verkehr an die Appliance umzuleiten, und die Appliance leitet die verarbeiteten Pakete zurück an den Router.

Im folgenden Artikel wird die schrittweise Vorgehensweise zum Konfigurieren von zwei SD-WAN (SD-WAN SE) -Appliances beschrieben:

- Rechenzentrums-Appliance im virtuellen Inlinemodus
- Gerät im Inline-Modus verzweigen
- Das Routing-Protokoll muss entweder am Core-Switch oder weiter stromaufwärts am Router konfiguriert werden. Der Router muss den Zustand der SD-WAN-Appliance überwachen, damit die Appliance bei einem Ausfall umgangen werden kann.
- Im virtuellen Inlinemodus wird die SD-WAN-Appliance physisch aus dem Pfad versetzt (ein-armige Bereitstellung), dh es muss nur eine einzige Ethernet-Schnittstelle verwendet werden (Beispiel: Schnittstelle 1/5), wobei der Bypass-Modus auf Fail-to-Block (FTB) eingestellt ist. Die Citrix SD-WAN Appliance muss so konfiguriert sein, dass Datenverkehr an das richtige Gateway weitergeleitet wird. Der für den virtuellen Pfad vorgesehene Datenverkehr wird auf die SD-WAN-Appliance gerichtet und dann gekapselt und an die entsprechende WAN-Verbindung geleitet.

Sammeln Sie Informationen

Sammeln Sie die folgenden Informationen, die für die Konfiguration des virtuellen Inlinemodus erforderlich sind:

- Genaues Netzwerkschema Ihrer lokalen und Remotestandorte, einschließlich:

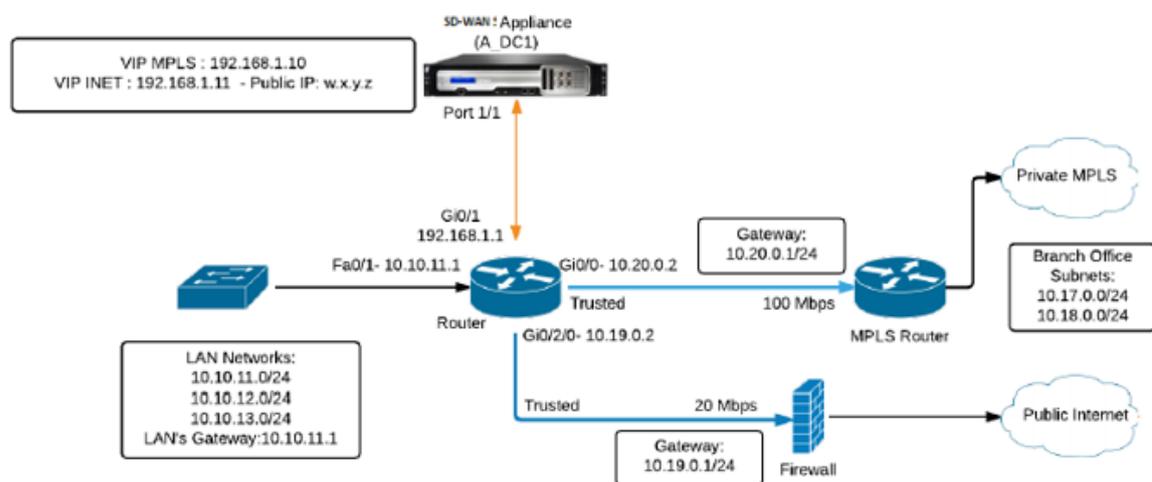
- Lokale und Remote-WAN-Verbindungen und ihre Bandbreiten in beide Richtungen, ihre Subnetze, virtuellen IP-Adressen und Gateways von jeder Verbindung, Routen und VLANs.

- Tabelle für die Bereitstellung

Informationen zur dienstbasierten SD-WAN Orchestrator-Bereitstellung im virtuellen Inline-Modus finden Sie unter [Schnittstellen](#).

Das Folgende ist ein Beispiel für ein Netzwerkschema und eine Bereitstellungstabelle:

Rechenzentrumstopologie — Virtueller Inline-Modus



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

August 29, 2022

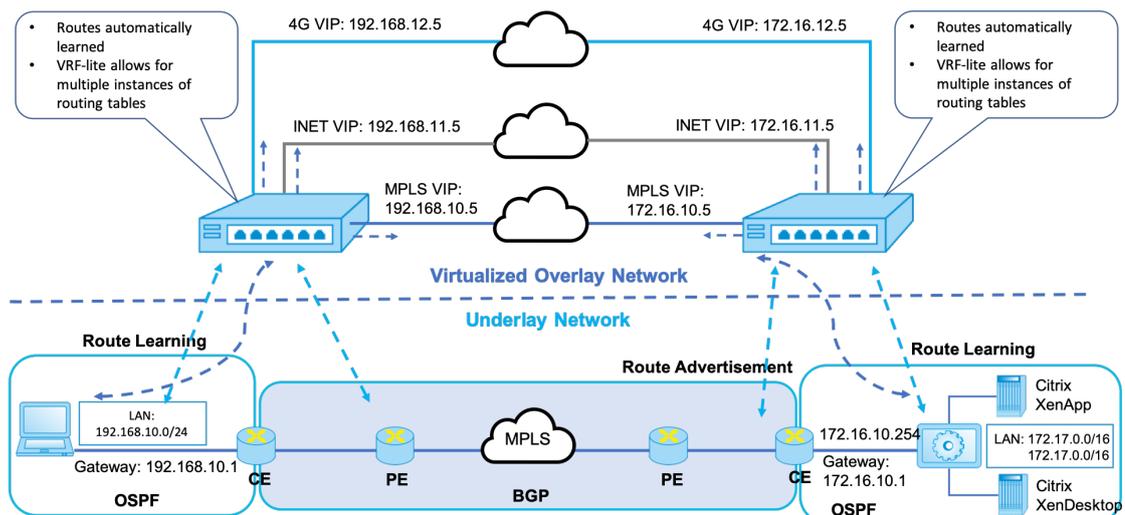
So erstellen Sie ein SD-WAN-Overlay-Netzwerk ohne die Notwendigkeit, SD-WAN-Overlay-Routentabellen zu erstellen:

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 kostenineffizient 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.

SD-WAN overlay dynamic network routing



Hohe Verfügbarkeit

August 29, 2022

In diesem Thema werden die Bereitstellungen und Konfigurationen mit hoher Verfügbarkeit (Hochverfügbarkeit) behandelt, die von SD-WAN-Appliances (Standard Edition) unterstützt werden.

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:**

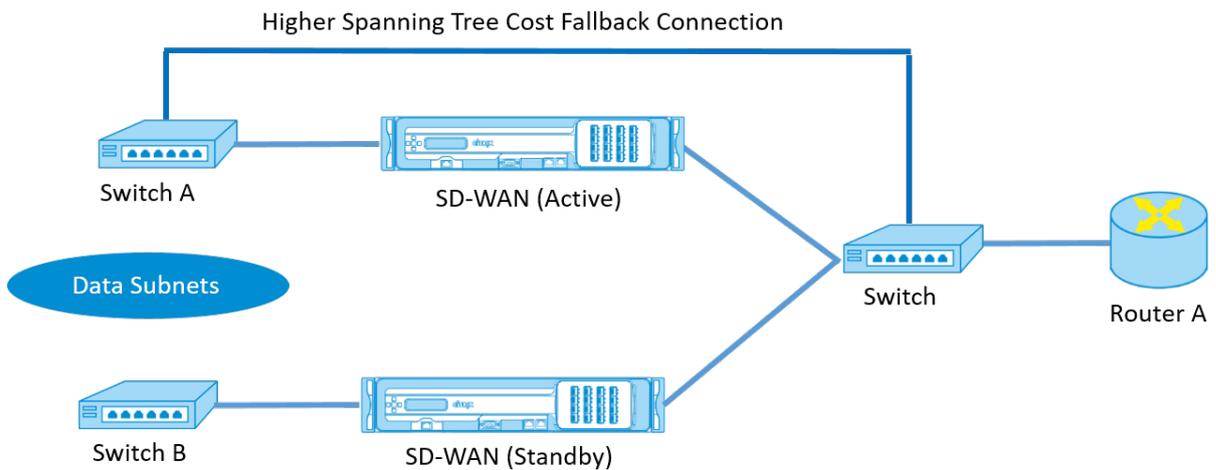
Der aktive Datenverkehr fließt auch dann, wenn der virtuelle Pfad ausgefallen ist, solange eine der SD-WAN-Appliances aktiv ist. Die SD-WAN-Appliance leitet den Datenverkehr als Intranetverkehr zurück an den Router um. Wenn jedoch beide aktive/Standby-SD-WAN-Appliances inaktiv werden, versucht der Router, 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:

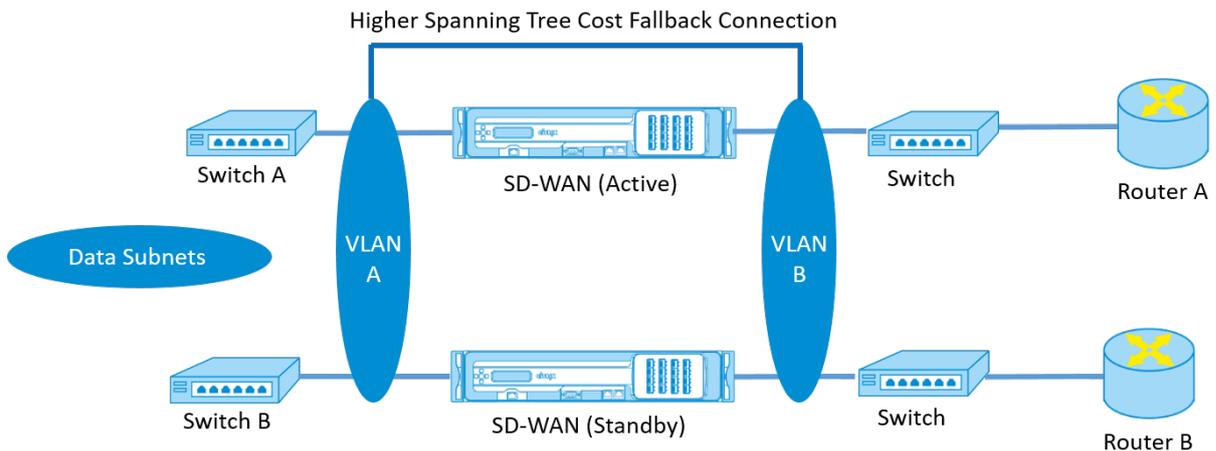
Im parallelen Inline-Hochverfügbarkeitsmodus werden die SD-WAN-Appliances inline mit dem Datenpfad nebeneinander bereitgestellt. Es wird nur ein Pfad durch die Active Appliance verwendet. Es ist wichtig zu beachten, dass Bypass-Schnittstellengruppen so konfiguriert sind, dass sie Failto-Block sind, um 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

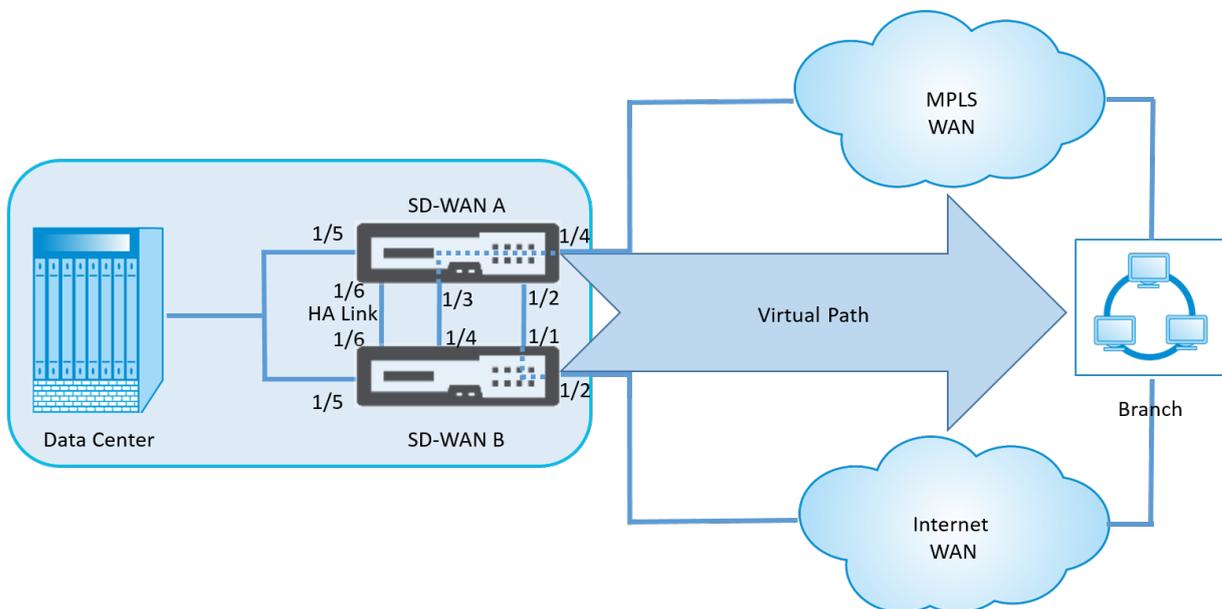
- Der Switchover mit hoher Verfügbarkeit im Fail-to-Wire-Modus dauert etwa 10 bis 12 Sekunden, da die Ports bei der Wiederherstellung aus dem Fail-to-Wire-Modus verzögert werden.
- Wenn die Hochverfügbarkeitsverbindung zwischen den Appliances fehlschlägt, wechseln beide Appliances in den Status Aktiv 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.

Weitere Informationen zur dienstbasierten SD-WAN Orchestrator-HA-Bereitstellung finden Sie unter [Gerätedetails](#).

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.

The screenshot displays the Citrix SD-WAN web management interface. At the top, there is a navigation bar with three tabs: **Dashboard** (selected), **Monitoring**, and **Configuration**. Below the navigation bar, the **System Status** section is visible, containing the following information:

Name:	BLR_DC-Appliance
Model:	4000
Appliance Mode:	MCN
Management IP Address:	10.105.58.172
Appliance Uptime:	3 days, 7 hours, 1 minutes, 43.0 seconds
Service Uptime:	3 days, 6 hours, 39 minutes, 51.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Below the System Status section, the **High Availability Status** section is visible, containing the following information:

Local Appliance:	Active
Peer Appliance:	Standby
Last Update Received:	0 seconds ago

Dashboard
Monitoring
Configuration

System Status

Name: **BLR_DC-BLR_DC_HA**
 Model: **4000**
 Appliance Mode: **MCN**
 Management IP Address: **10.105.58.142**
 Appliance Uptime: **1 weeks, 1 days, 12 hours, 41 minutes, 5.3 seconds**
 Service Uptime: **3 days, 6 hours, 50 minutes, 31.0 seconds**
 Routing Domain Enabled: **Default_RoutingDomain**

High Availability Status

Local Appliance: **Standby**
 Peer Appliance: **Active**
 Last Update Received: **0 seconds ago**

Informationen zu Netzwerkadapters zu Active und Standby-Hochverfügbarkeits-Appliances finden Sie unter **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Ethernet**.

Dashboard
Monitoring
Configuration

- Appliance Settings
 - Administrator Interface
 - Logging/Monitoring
 - Network Adapters**
 - Net Flow
 - SNMP
 - Licensing
- + Virtual WAN
- + System Maintenance

Configuration > Appliance Settings > **Network Adapters**

IP Address

Ethernet

Ethernet Interface Settings

For the CB4000 platform, settings for ports 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 10/1 and 10/2 will only take effect when the Citrix Virtual WAN Service is in the Citrix configuration.
The settings for the high speed port 10/1 cannot be changed.

0/1 : ● MAC Address: 0a:c4:7a:14:c9:d6	Autonegotiate: <input checked="" type="checkbox"/>	Speed: <input type="text" value="1000Mb/s"/>	Duplex: <input type="text" value="Full"/>
1/1 : ● MAC Address: 5a:4c:f8:f0:71:b2	Autonegotiate: <input checked="" type="checkbox"/>	Speed: <input type="text" value="Unknown"/>	Duplex: <input type="text" value="Unknown"/>
1/2 : ● MAC Address: d6:1e:72:d5:d1:18	Autonegotiate: <input checked="" type="checkbox"/>	Speed: <input type="text" value="1000Mb/s"/>	Duplex: <input type="text" value="Full"/>
1/3 : ● MAC Address: 66:4f:9d:c5:48:d2	Autonegotiate: <input checked="" type="checkbox"/>	Speed: <input type="text" value="Unknown"/>	Duplex: <input type="text" value="Unknown"/>
1/4 : ● MAC Address: 46:63:cb:5d:39:db	Autonegotiate: <input checked="" type="checkbox"/>	Speed: <input type="text" value="1000Mb/s"/>	Duplex: <input type="text" value="Full"/>
1/5 : ● MAC Address: 06:7b:ce:9a:c5:dd	Autonegotiate: <input checked="" type="checkbox"/>	Speed: <input type="text" value="1000Mb/s"/>	Duplex: <input type="text" value="Full"/>

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

131

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN management console. The left sidebar lists 'Appliance Settings' with sub-items: Administrator Interface, Logging/Monitoring, Network Adapters (selected), Net Flow, SNMP, and Licensing. Below this are 'Virtual WAN' and 'System Maintenance'. The main content area is titled 'Configuration > Appliance Settings > Network Adapters'. It has two tabs: 'IP Address' and 'Ethernet'. The 'Ethernet' tab is active, showing 'Ethernet Interface Settings'. A note states: 'For the CB4000 platform, settings for ports 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 10/1 and 10/2 will only take effect when the Citrix Virtual WAN Service is enabled and the port is included in the Citrix configuration. The settings for the high speed port 10/1 cannot be changed.' Below the note is a table of interface settings:

Port	MAC Address	Autonegotiate	Speed	Duplex
0/1	0a:25:90:c5:70:b4	<input checked="" type="checkbox"/>	1000Mb/s	Full
1/1	b2:1fd0:ab:70:ea	<input checked="" type="checkbox"/>	Unknown	Unknown
1/2	36:1f0e:02:91:03	<input checked="" type="checkbox"/>	Unknown	Unknown
1/3	aa:af:3e:1f:3b:2b	<input checked="" type="checkbox"/>	Unknown	Unknown
1/4	c2:3e:e5:22:93:05	<input checked="" type="checkbox"/>	Unknown	Unknown
1/5	ee:6fd3:aa:6b:bc	<input checked="" type="checkbox"/>	1000Mb/s	Full

Problembehandlung

Führen Sie die folgenden Schritte zur Fehlerbehebung durch, während Sie die SD-WAN-Appliance im Hochverfügbarkeitsmodus (HA) konfigurieren:

- 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.
- 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 **racpprotokolliert**.

- Sie können die portbezogenen Ereignisse in der Datei **SDWAN_common.log** überprüfen (z. B. gehen die HA-fähigen Ports aus oder nach oben).
- 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

August 29, 2022

Hinweis: In Version 10.2 Version 2 gilt diese Funktionalität nur für die 1100 SE Appliance.

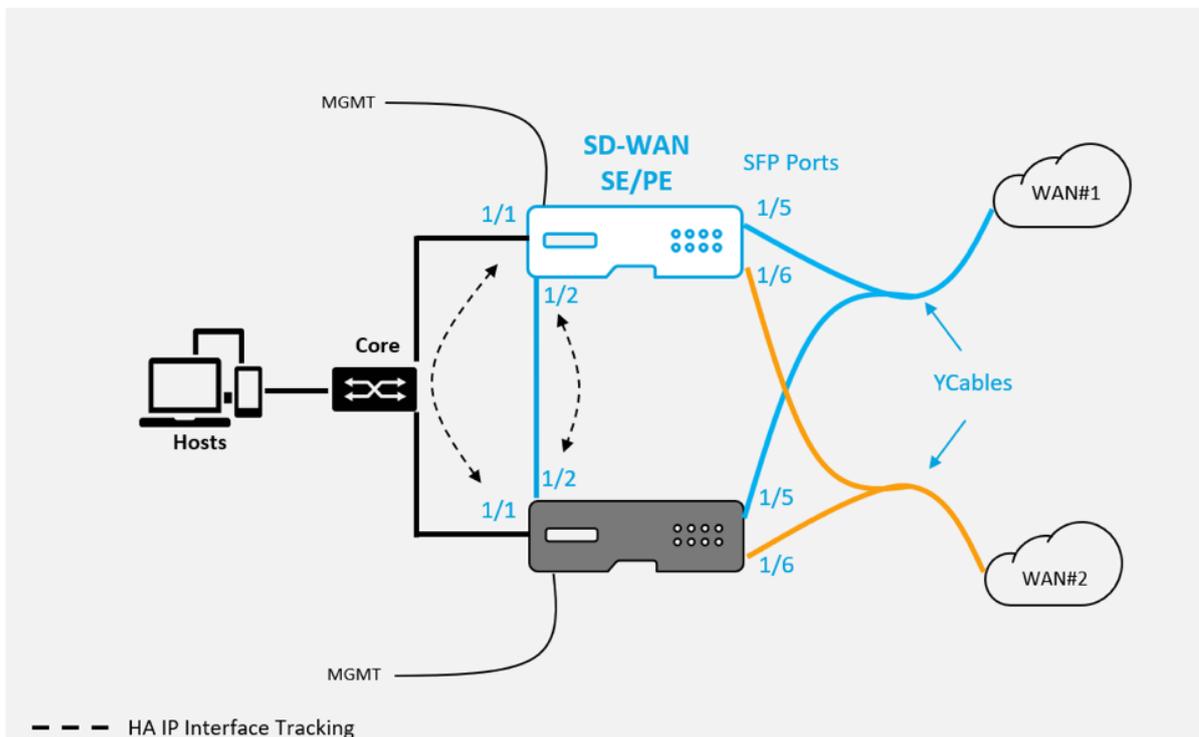
Im folgenden Verfahren werden die Schritte zum Aktivieren der Hochverfügbarkeit (HA) auf 1100 SE-Appliances beschrieben, die im Edge-Modus bereitgestellt werden, wobei die Übergaben von den WAN-Verbindungsdiensteanbietern Glasfaser sind.

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.

Bei der 1100 SE-Einheit wird das geteilte Ende des Splitterkabels mit Glasfaser-Ports von zwei 1.100-Einheiten verbunden, die als HA-Paar konfiguriert sind.

Das Glasfaser-Y-Kabel hat drei Enden. Ein Ende stellt eine Verbindung zur Glasfaserübergabe des Anbieters her und die anderen beiden Enden stellen eine Verbindung zu SFP-Ports her, die für diese WAN-Verbindung auf zwei 1100 SE-Appliances konfiguriert sind, die als HA-Paar bereitgestellt werden. Das Splitterkabel wird verwendet, um ein eingehendes Signal in mehrere Signale aufzuteilen.

Informationen zur auf dem SD-WAN Orchestrator-Dienst basierenden Edge-Modus-HA-Bereitstellung finden Sie unter [Gerätedetails](#).



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

August 29, 2022

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 1100 Standard Edition
- SD-WAN 2100 Standard Edition
- SD-WAN AWS VPX-Instanz

Zero-Touch-Bereitstellung Cloud Service ist ein von Citrix betriebener und verwalteter cloud-basierter Dienst, der die Erkennung neuer Appliances im Citrix SD-WAN-Netzwerk ermöglicht und sich hauptsächlich auf die Rationalisierung des Bereitstellungsprozesses für Citrix SD-WAN an Zweigstellen- oder Cloud-Servicebüros konzentriert. Der Zero-Touch-Bereitstellungs-Cloud-Service ist von jedem beliebigen Punkt im Netzwerk über den öffentlichen Internetzugang zugänglich. Auf den Zero-Touch-Bereitstellungs-Cloud-Dienst wird über das Secure Socket Layer (SSL)-Protokoll zugegriffen.

Die Zero-Touch-Bereitstellungs-Cloud-Services kommunizieren sicher mit den Back-End-Diensten von Citrix, die eine gespeicherte Identifizierung von Citrix-Kunden hosten, die Zero Touch-fähige Geräte (z. B. 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.

Weitere Informationen finden Sie im Thema [Zero-Touch-Bereitstellung](#) des Citrix SD-WAN Orchestrator Service.

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:

- Citrix Cloud Login, um den Zero Touch Deployment Service für die Bereitstellung neuer Standortknoten zu initiieren.

Netzwerkadministrator —Ein Benutzer, der für das Unternehmensnetzwerkmanagement verantwortlich ist (DHCP, DNS, Internet, Firewall usw.).

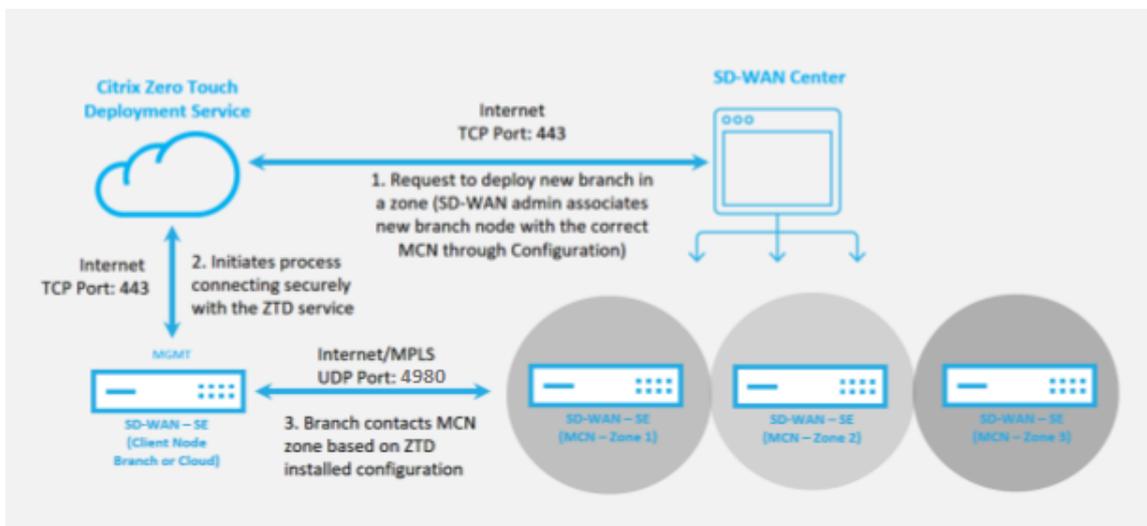
Remotestandort:

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.

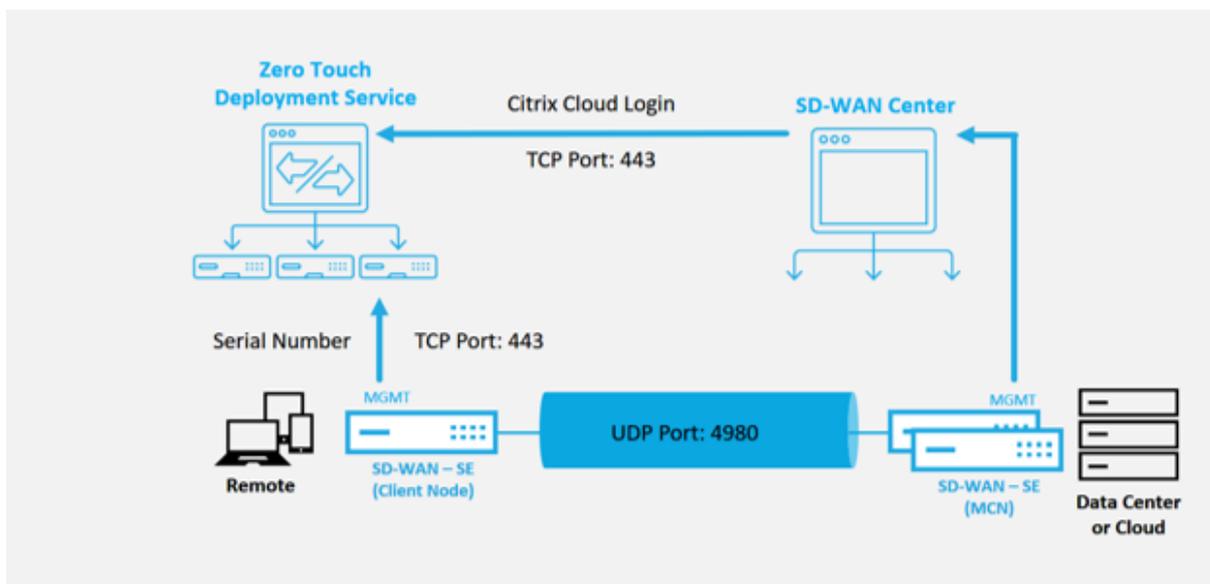


Die folgenden Voraussetzungen sind erforderlich, bevor Sie einen Zero Touch-Bereitstellungsdienst starten:

- Aktive Ausführung von SD-WAN auf Master Control Node (MCN) heraufgestuft.

- Citrix Cloud-Anmeldeinformationen, die auf <https://onboarding.cloud.com> erstellt wurden (verweisen Sie auf die nachstehende Anleitung zur Kontoerstellung).
- Verwaltung der Netzwerkkonnektivität (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 Client-Modus mit gültiger Virtual Path-Konnektivität zum MCN betrieben wird, um die erfolgreiche Pfadinrichtung im vorhandenen Underlay-Netzwerk zu validieren.

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:

Um den Zero Touch Deployment Service (oder den Zero-Touch-Bereitstellungs-Cloud-Service) verwenden zu können, muss ein Administrator zunächst das erste SD-WAN-Gerät in der Umgebung bereitstellen.

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. Durch die Anmeldung beim Zero-Touch-Dienst wird die Kunden-ID authentifiziert, die der jeweiligen SD-WAN-Umgebung zugeordnet ist.

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 ver-

wendende 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. Außerdem 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.

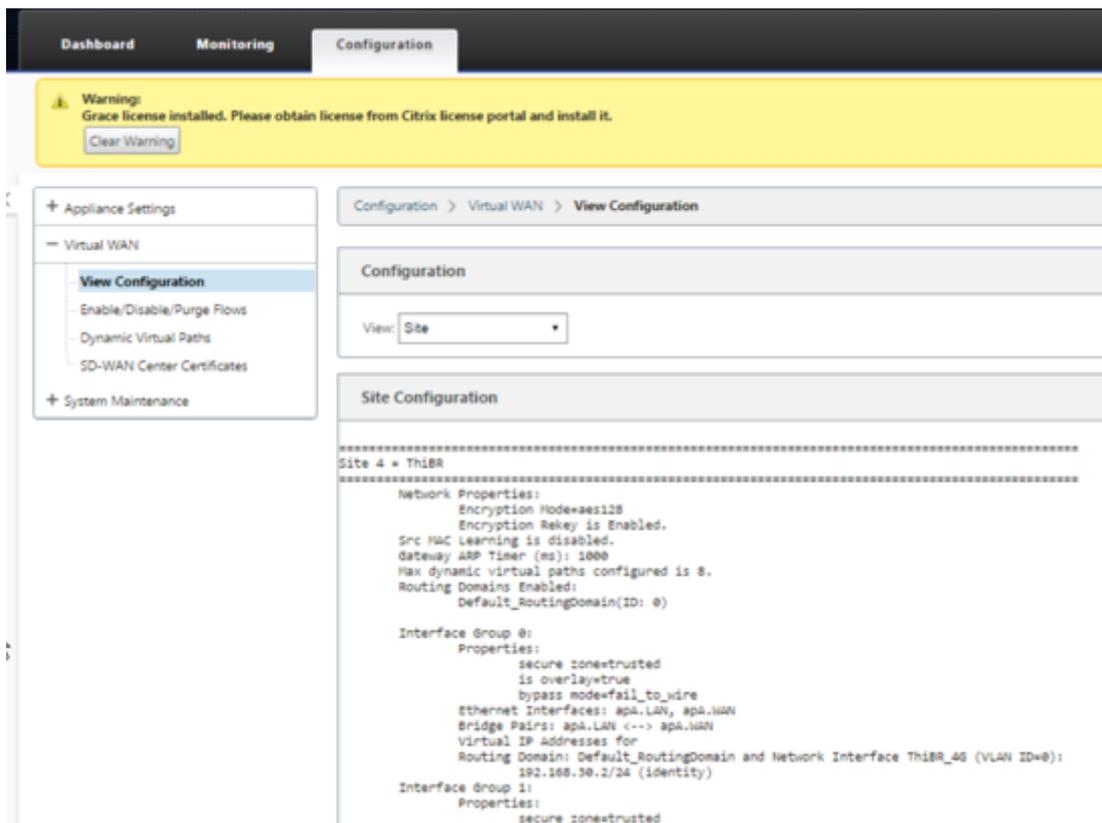
- Authentifizieren Sie die Zweigstellenappliance, indem Sie die Seriennummer überprüfen.
- Schieben Sie die für die Ziel-Appliance spezifische Konfigurationsdatei an die Zweigeinheit.
- Installieren Sie die Konfigurationsdatei auf der Zweigeinheit.
- Schieben Sie alle fehlenden SD-WAN-Softwarekomponenten 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.

Die Appliance-Konfiguration kann über die Seite **Konfiguration > Virtuelles WAN > Konfiguration anzeigen** validiert werden.



Die Appliance-Lizenzdatei kann auf der Seite **Konfiguration > Appliance-Einstellungen > Lizenzierung** auf eine permanente Lizenz aktualisiert werden.

Dashboard Monitoring Configuration

Warning: Grace license installed. Please obtain license from Citrix license portal and install it.
Clear Warning

Configuration > Appliance Settings > Licensing

Appliance Settings

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

License Status

State:	Licensed
License Server Location:	Local
Local License Server HostID:	02c47a512af0
System Platform:	NetScaler SD-WAN 1000 Series
Model:	1000VW-020
Maximum Bandwidth (MAXBW):	10 Mbps
License Type:	N/A
Action Required:	Grace license installed. Please obtain license from Citrix license portal and install it.
Maintenance Expiration Date:	N/A
License Expiration Date:	Sat May 27 02:48:57 2017

License Configuration

Local Remote

Upload License for this Appliance

Filename: No file chosen

Nach dem Hochladen und Installieren der permanenten Lizenzdatei wird das Warnbanner der Grace License ausgeblendet, und während des Lizenzinstallationsprozesses tritt kein Verbindungsverlust zur Remote-Site auf (keine Pings werden verworfen).

AWS

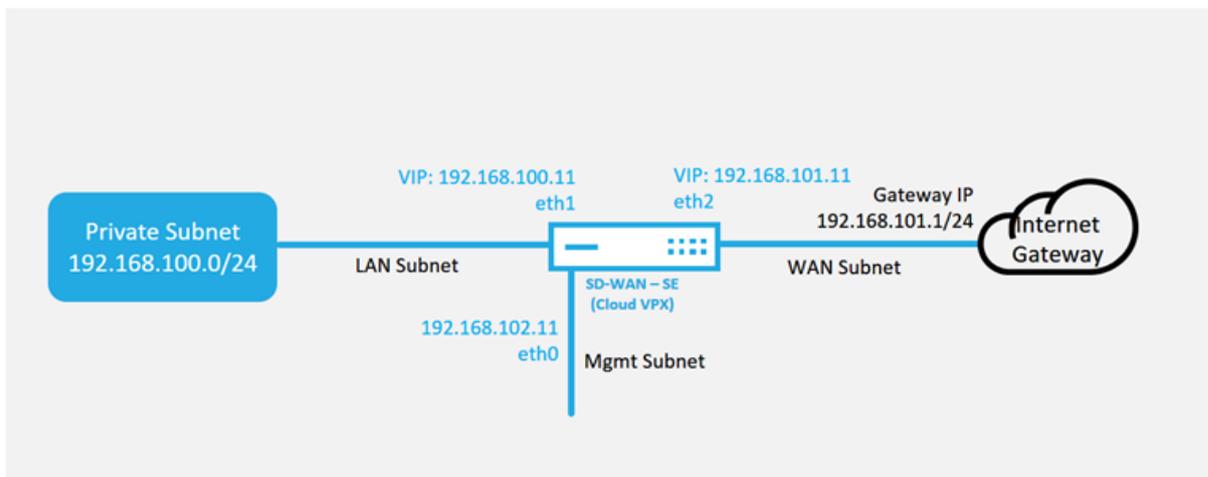
August 29, 2022

Mit SD-WAN Version 11.5 wird die Zero-Touch-Bereitstellung in einer AWS-Umgebung durch den SD-WAN Orchestrator Service unterstützt.

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 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.

Azure

August 29, 2022

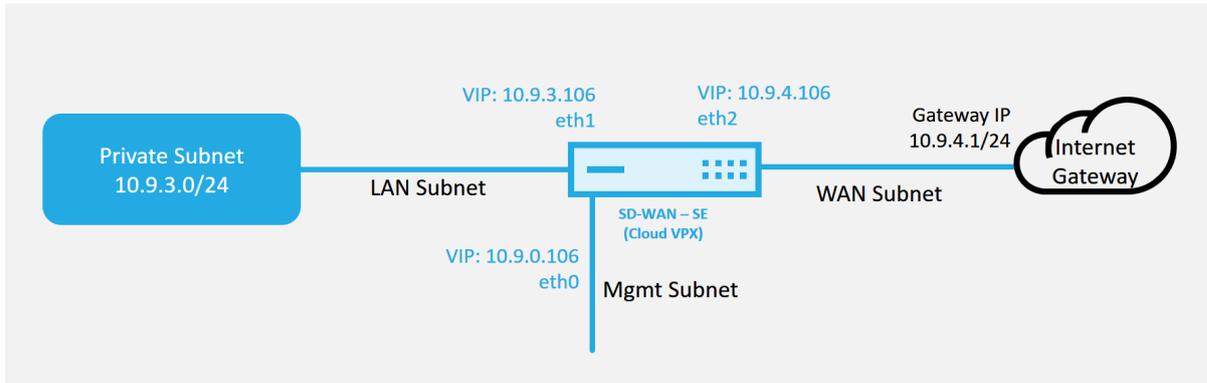
Mit SD-WAN Version 11.5 wird die Zero-Touch-Bereitstellung in einer Azure-Umgebung über den SD-WAN Orchestrator Service unterstützt.

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 eine Beispielbereitstellung einer in der 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.

Bereitstellung in einer Region

August 29, 2022

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.

Weitere Informationen zur Bereitstellung einzelner Regionen über den Citrix SD-WAN Orchestrator Service finden Sie unter [Regionen](#).

Bereitstellung in mehreren Regionen

August 29, 2022

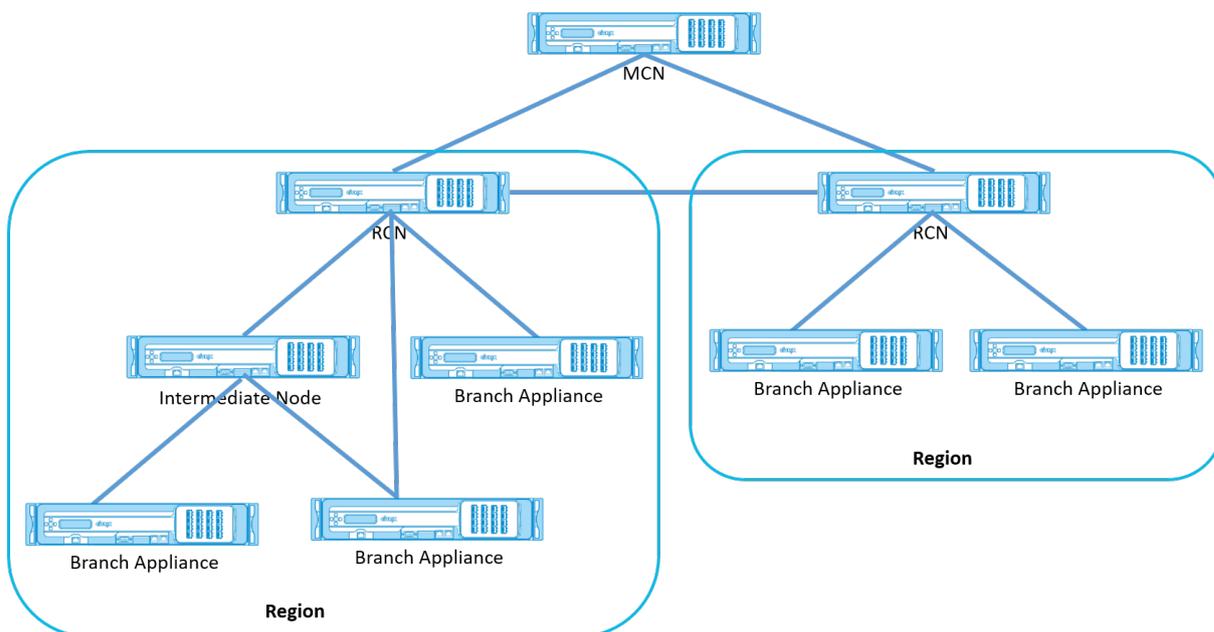
Eine SD-WAN-Appliance, die als Master Control Node (MCN) konfiguriert ist, unterstützt die Bereitstellung mehrerer Regionen. Der MCN verwaltet mehrere regionale Kontrollknoten (RCNs). Jeder RCN wiederum verwaltet mehrere Clientsites. Der MCN kann auch verwendet werden, um einige der Client-Standorte 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 1000 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.

Weitere Informationen zur Bereitstellung mehrerer Regionen über den Citrix SD-WAN Orchestrator Service finden Sie unter [Regionen](#).



Die folgende Tabelle enthält eine Liste der Plattformen, die für die Konfiguration des primären und sekundären MCN/RCN unterstützt werden.

HINWEIS:

Verwenden Sie das Citrix SD-WAN 210 SE-Gerät nur in den verwalteten SD-WAN Orchestrator Net-

zwerken als MCN.

Plattform-Edition	Primär-/Sekundär-MCN	Primär/Sekundär-RCN
110-SE	Nein	Nein
210-SE	Ja	Ja
1100-SE	Ja	Ja
VPX-SE, VPXL-SE	Ja	Ja
2100-SE, 4100-SE, 5100-SE, 6100-SE	Ja	Ja

Konfigurationshandbuch für Citrix Virtual Apps and Desktops Workloads

August 29, 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

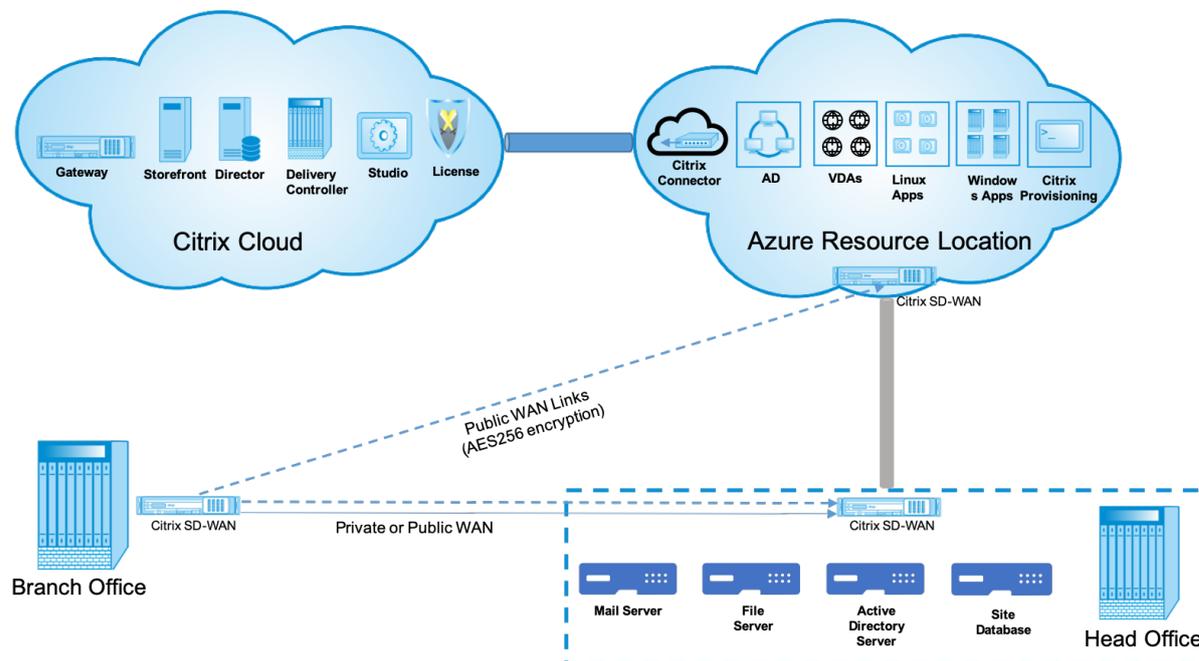
- Verkehrsmanagement zur Sicherstellung der Quality of Service (QoS)
 - QoS über HDX/ICA-Datenverkehrsströme (HDX AutoQoS mit einem Port)
 - QoS zwischen HDX und anderem Datenverkehr
 - HDX QoS Fairness zwischen Benutzern
 - End-to-End-QoS
- Link-Bonding bietet mehr Bandbreite für schnellere Leistung
- 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 Rechenzentrums Umgebung), oder Sie können Azure Active Directory (AAD) verwenden.
- Der DNS-Server muss in der Lage sein, sowohl interne (private) als auch externe (öffentliche) IPs aufzulösen.
- Stellen Sie sicher, dass der FQDN (sdwan-location.citrixnetworkapi.net) der Zulassungsliste in der Firewall hinzugefügt wird. Dies ist der FQDN für den Netzwerkstandortdienst, der für das Senden von Datenverkehr über den virtuellen SD-WAN-Pfad von entscheidender Bedeutung ist. Eine bessere Möglichkeit, wenn Sie mit Positivlisten von Wildcard-FQDNs vertraut sind, wäre es auch möglich *.citrixnetworkapi.net zur zulässigen Liste hinzuzufügen, da dies die Subdomain für andere Citrix Cloud-Dienste wie Zero-Touch-Provisioning ist.
- Melden Sie sich bei sdwan.cloud.com an, um den SD-WAN Orchestrator für die Verwaltung Ihres SD-WAN-Netzwerks zu verwenden. SD-WAN Orchestrator ist eine auf Citrix Cloud basierende Multitenant-Verwaltungsplattform für Citrix SD-WAN.

Bereitstellungsarchitektur



Die folgenden Entitäten sind für die Bereitstellung erforderlich:

- Ein on-premises Standort, der die SD-WAN-Appliance hostet 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.

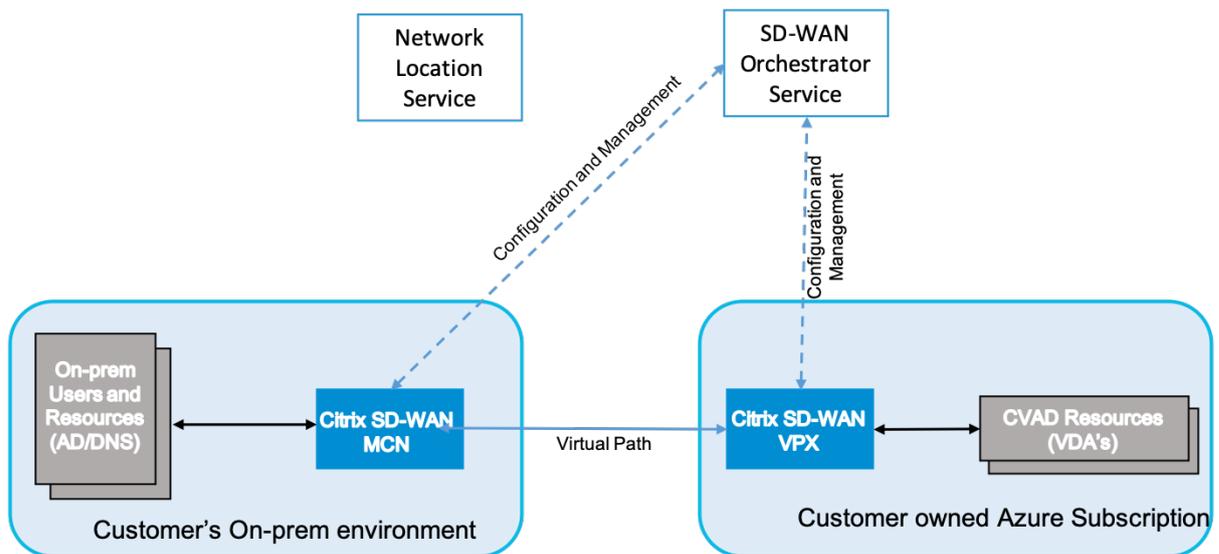
Mit dem Citrix Virtual Apps and Desktops s-Dienst können Sie sichere virtuelle Apps und Desktops auf jedem Gerät bereitstellen und den Großteil der Produktinstallation, Setup, Konfiguration, Upgrades und Überwachung von Citrix überlassen. Sie behalten die vollständige Kontrolle über Anwendungen, Richtlinien 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. Ressourcenstan-

dorte 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 Orches-

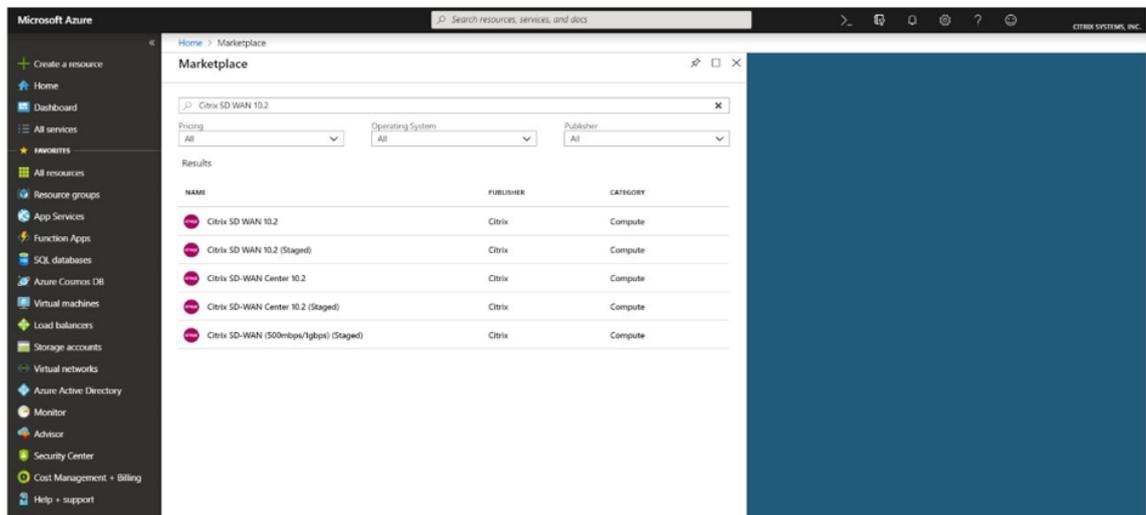
trator verwaltet. Sobald die SD-WAN-Appliance konfiguriert wurde, stellt sie eine Verbindung zum vorhandenen Citrix SD-WAN Netzwerk her. Weitere Aufgaben wie Konfiguration, Transparenz und Verwaltung werden über SD-WAN Orchestrator erledigt.

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.

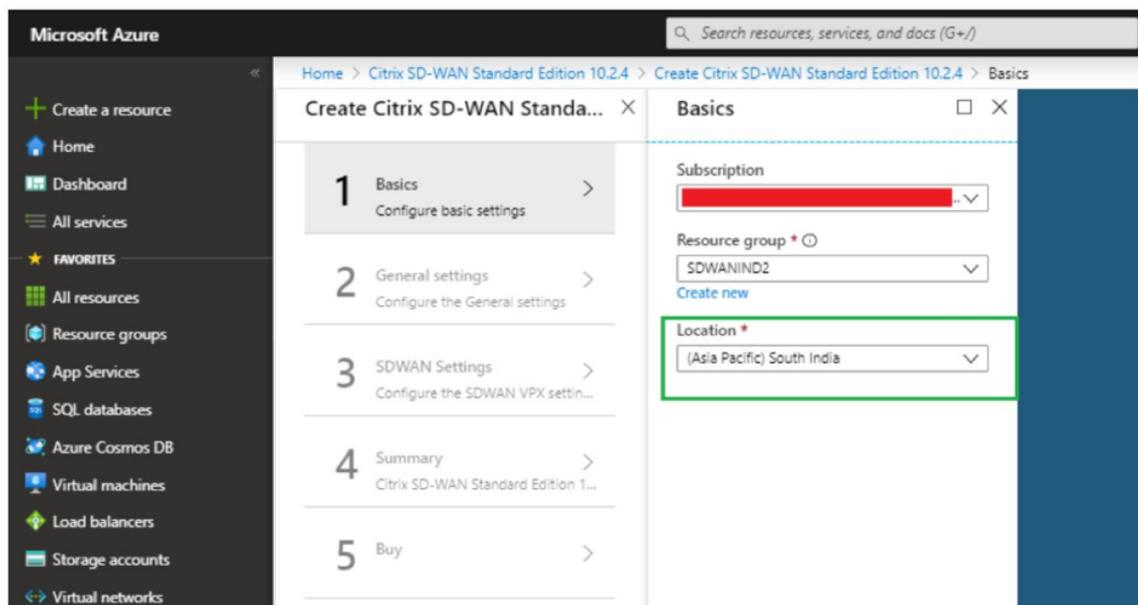


Klicken Sie auf **Erstellen**, einen Assistenten, der mit den erforderlichen Details zum Erstellen der virtuellen Maschine auffordert.

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.

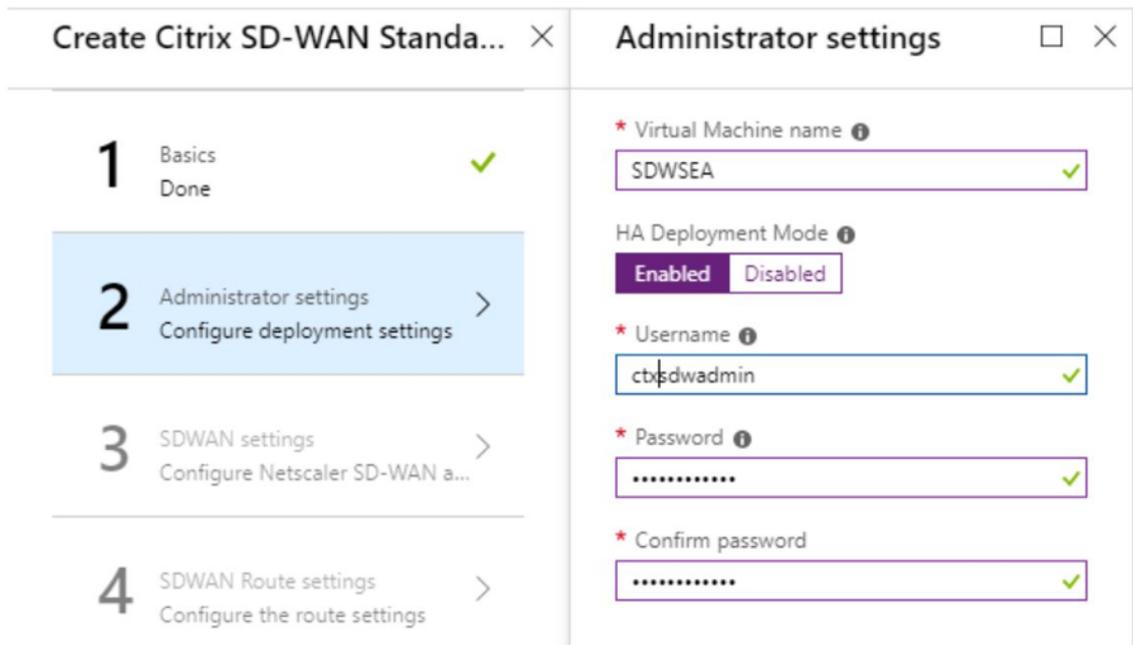
Für Citrix SD-WAN wird empfohlen, dass die ausgewählte Ressourcengruppe leer sein muss. Wählen Sie in ähnlicher Weise die Azure-Region aus, in der Sie die SD-WAN-Instanz bereitstellen möchten. Die Region muss mit der Region identisch sein, in der Ihre Citrix Virtual Apps and Desktops Ressourcen bereitgestellt 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**.

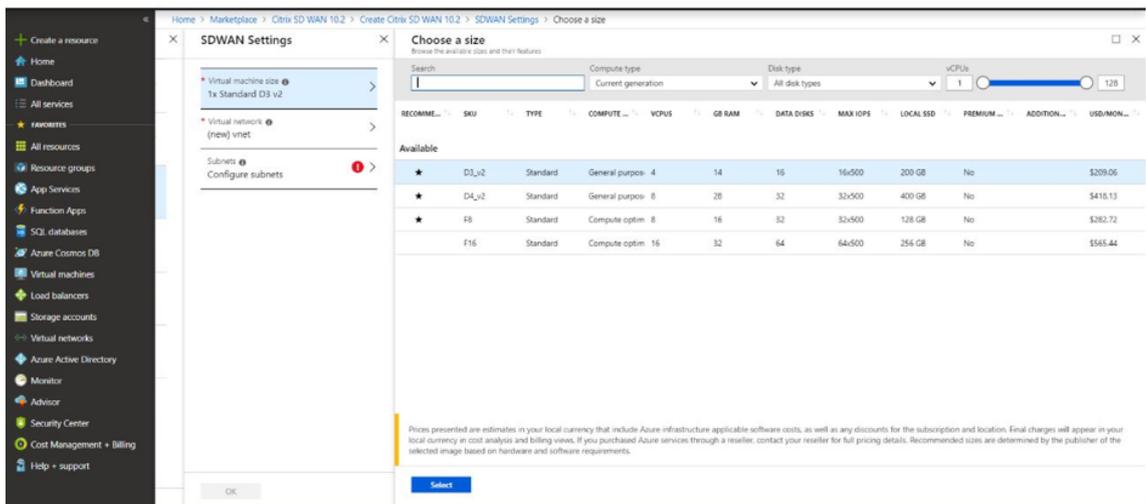
Dieses Kennwort ist erforderlich, um sich als Gastbenutzer an der Verwaltungsoberfläche der Instanz anzumelden. Um Admin-Zugriff auf die Instanz zu erhalten, verwenden Sie admin als Benutzernamen und das Kennwort, das während der Provisioning der Instanz erstellt wurde. Wenn Sie den Benutzernamen verwenden, 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.

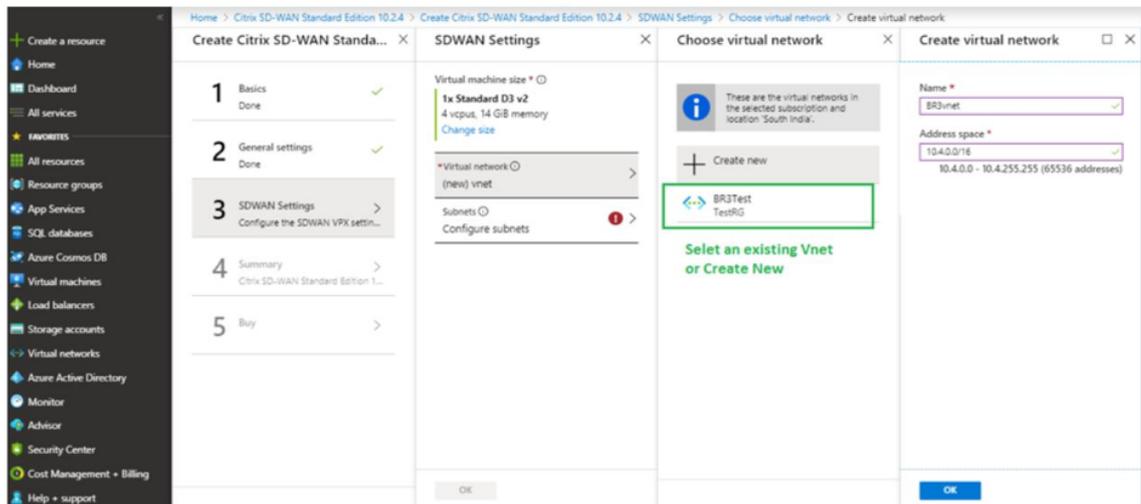


5. Wählen Sie auf der **SD-WAN-Einstellungsseite** die Instanz aus, in der Sie das Image ausführen möchten. Wählen Sie den folgenden Instanz-Typ gemäß Ihrer Anforderung:

- 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.



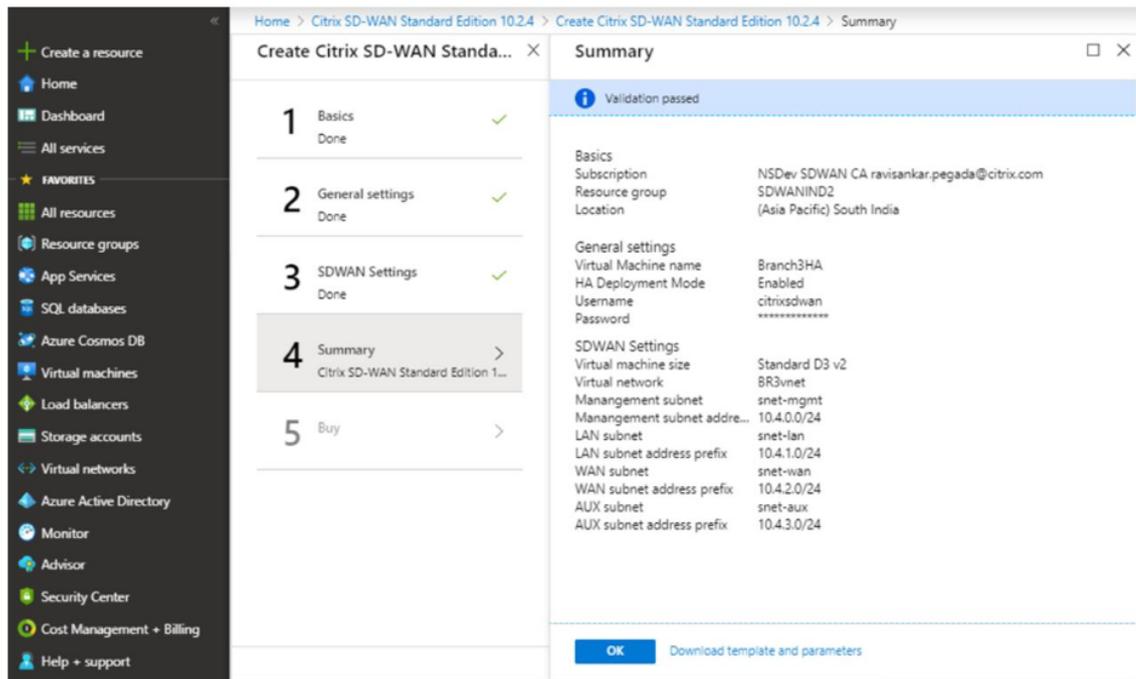
Das Aux-Subnetz wird nur benötigt, wenn Sie die Instanzen im HA-Modus bereitstellen. Stellen Sie sicher, dass die SD-WAN-Instanz im selben VNet wie Ihre Citrix Virtual Apps and Desktops-Ressourcen bereitgestellt wird und sich im selben Subnetz wie die LAN-Schnittstelle der SD-WAN VPX-Appliance befindet.

The image shows two overlapping configuration windows. The left window, titled "SDWAN Settings", has a sidebar with three items: "Virtual machine size * ①" (1x Standard D3 v2, 4 vcpus, 14 GiB memory, Change size), "*Virtual network ①" ((new) BR3vnet), and "Subnets ①" (Configure subnets, with a red exclamation mark icon). The right window, titled "Subnets", contains the following configuration fields, each with a green checkmark:

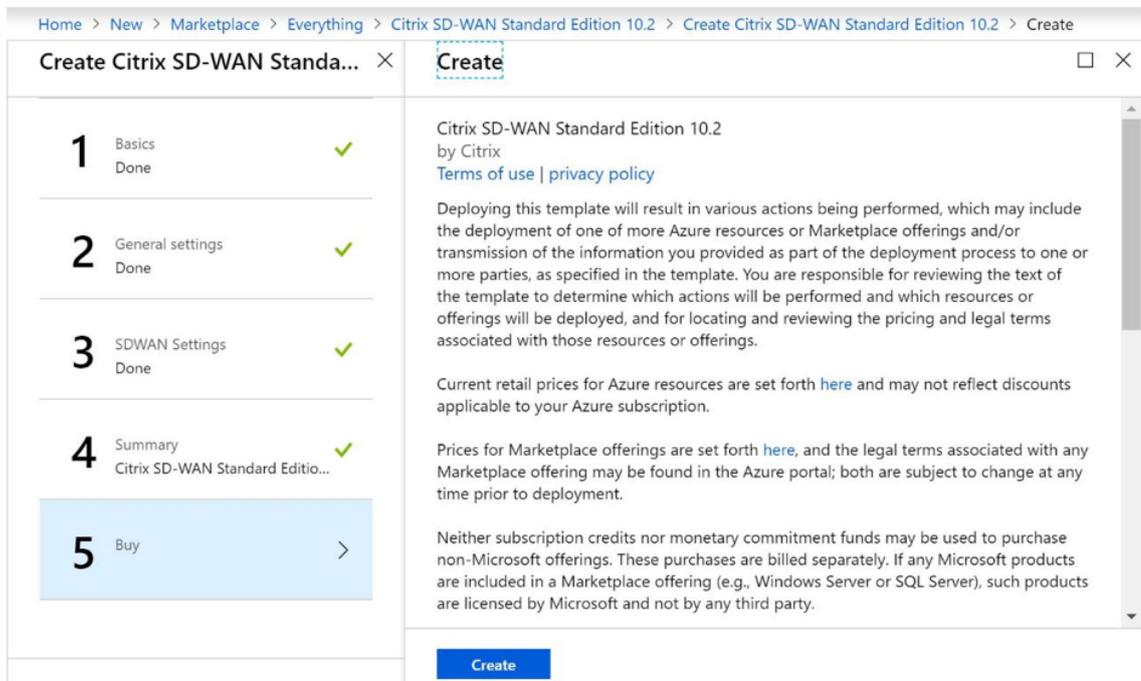
- Management subnet name *: snet-mgmt
- Management subnet address prefix *: 10.4.0.0/24
- LAN subnet name *: snet-lan
- LAN subnet address prefix *: 10.4.1.0/24
- WAN subnet name *: snet-wan
- WAN subnet address prefix *: 10.4.2.0/24
- AUX subnet name *: snet-aux
- AUX subnet address prefix *: 10.4.3.0/24

Both windows have an "OK" button at the bottom.

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).

The screenshot shows a web form titled "New Site". Inside the form, there is a section titled "Site Details". This section contains two primary input fields. The first is labeled "Site Name" with a red asterisk indicating it is required; below it is a text box with the placeholder "Name". The second is labeled "Site Address" with a red asterisk; below it is a text box with the placeholder "Search for Site Address". To the right of the "Site Address" field is a checkbox labeled "Lat/Lng". At the bottom right of the form, there are two buttons: a grey "Cancel" button and a blue "Next" button with a right-pointing arrow.

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.

- 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**.

The screenshot shows the 'Configuration' tab of the Citrix SD-WAN interface. Under 'System Status', the following information is displayed:

- Name: DCAzure
- Model: VPX
- Sub-Model: BASE
- Appliance Mode: MCN
- Serial Number: 0000-0007-5714-8818-8276-7561-41
- Management IP Address: 10.2.0.4
- Appliance Uptime: 6 days, 8 hours, 59 minutes, 5.8 seconds
- Service Uptime: 4 days, 8 hours, 29 minutes, 10.0 seconds
- Routing Domain Enabled: Default_RoutingDomain

- Sobald Sie mit der Konfiguration der Instanz fertig sind. Klicken Sie auf **Config/Software bereitstellen**, indem Sie zu **Konfiguration > Netzwerkkonfiguration Homenavigieren**.

The screenshot shows the 'Configuration' tab with several action buttons: '+ Add Site', 'Batch Add Sites', 'Deploy Config/Software', 'Back Up/Review Checkpoints', and 'More Actions ...'. Below these buttons is a 'Deployment Tracker' section with a search bar and a table of sites.

Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Serial No	Bandwidth Tier	Management IP	Actions
■	● Offline	AzureBranch	MCN	VPX-SE	0000-0009-9954-...	1000		

- 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 pinggen. 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

August 29, 2022

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 über den Citrix SD-WAN Orchestrator Service mithilfe der folgenden Arten von DNS-Diensten konfigurieren:

- **Statischer DNS-Dienst:** Ermöglicht Ihnen die Konfiguration der statischen IPv4-DNS-Server-IP-Adressen. Sie können Internal, ISP, Google oder jeden anderen Open Source DNS-Dienst erstellen. Statischer DNS-Dienst kann auf globaler und Standortebene konfiguriert werden.

- **Dynamischer DNS-Dienst:** Ermöglicht Ihnen die Konfiguration der dynamischen IPv4-DNS-Server-IP-Adressen. Dynamischer DNS-Dienst kann nur auf Standortebene konfiguriert werden. Pro Standort ist nur ein dynamischer DNS-Dienst zulässig.
- **StaticV6 DNS-Dienst:** Ermöglicht Ihnen, die statischen IP-Adressen des IPv6-DNS-Servers zu konfigurieren. Sie können Internal, ISP, Google oder jeden anderen Open Source DNS-Dienst erstellen. Der StaticV6 DNS-Dienst kann auf globaler und Standortebene konfiguriert werden.
- **DynamicV6 DNS-Dienst:** Ermöglicht Ihnen die Konfiguration der dynamischen IPv6-DNS-Server-IP-Adressen. Der DynamicV6 DNS-Dienst kann nur auf Standortebene konfiguriert werden. Pro Standort ist nur ein dynamischer DNS-Dienst zulässig.

DNS-Proxy

Sie können einen Proxy mit mehreren Weiterleitungen konfigurieren, mit denen DNS-Anfragen basierend auf Anwendungsdomännennamen gesteuert werden können. Die DNS-Weiterleitung funktioniert für die Anfragen, die über UDP-Verbindungen empfangen werden. Informationen zum Konfigurieren des DNS-Proxys über den SD-WAN Orchestrator Service finden Sie unter [DNS-Proxy](#).

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. Informationen zum Konfigurieren der transparenten DNS-Weiterleitung über den SD-WAN Orchestrator Service finden Sie unter [Transparente DNS-Weiterleitungen](#).

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

The screenshot shows the 'Monitoring > DNS' page. It features a left-hand navigation menu with options like Statistics, Flows, Routing Protocols, Firewall, IKE/IPsec, ICMP, Performance Reports, QoS Reports, Usage Reports, Availability Reports, Appliance Reports, DHCP Server/Relay, VRRP, PPPoE, and DNS (selected). The main content area is divided into three sections: 'DNS Statistics' with a 'Refresh' button, 'Proxy Statistics' with a search bar and a table, and 'Transparent Forwarder Statistics' with a search bar and a table.

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

Application Name	DNS Service Name	DNS Service Active	Hits
office365_allow	Quad9	YES	0
office365_default	Quad9	YES	0
office365_optimize	Quad9	YES	0

Transparente Weiterleitungsstatistiken

This screenshot shows the 'Transparent Forwarder Statistics' section of the dashboard. It includes a search bar and a table with columns for Application Name, DNS Service Name, DNS Service Active, and Hits. The table lists several entries, including SocialMedia, OnlineShopping, and office365 entries.

Application Name	DNS Service Name	DNS Service Active	Hits
SocialMedia	Google	YES	5
OnlineShopping	Google	YES	2
office365_optimize	Quad9	YES	1
office365_default	Quad9	YES	11
office365_allow	Quad9	YES	8

DHCP

November 16, 2022

Citrix SD-WAN führt die Möglichkeit ein, Standard 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.

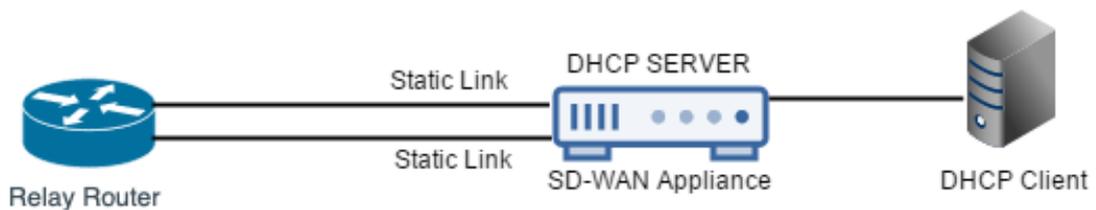
Im Folgenden sind die Vorteile der Verwendung des DHCP-Servers und der DHCP-Relay-Funktionen aufgeführt:

- 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.

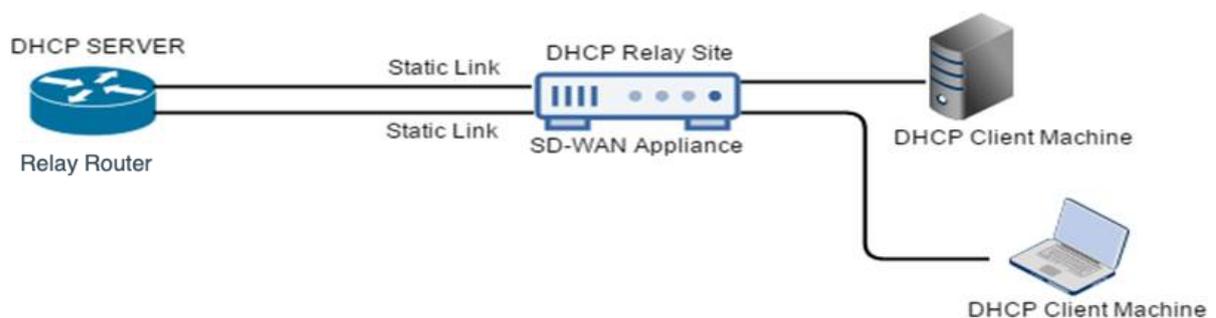
DHCP-Server

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.



WAN-Link-IP-Adressen-Lernen über DHCP-Client

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.

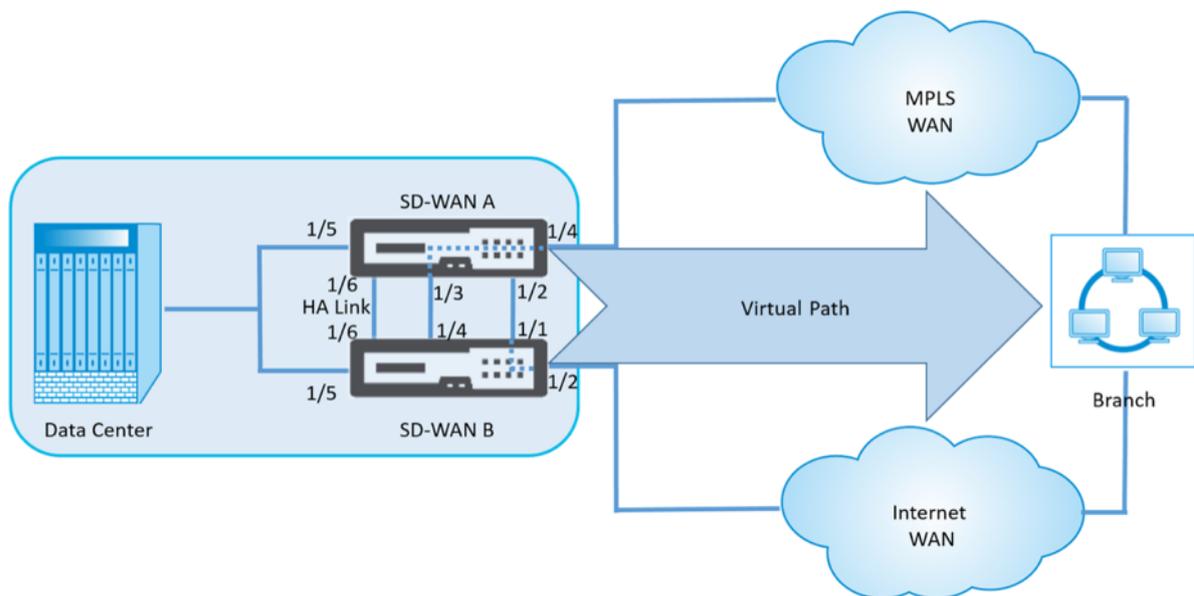
Ab Version Citrix SD-WAN 11.5 können Sie DHCP für eine nicht vertrauenswürdige virtuelle Schnittstelle im Fail-to-Block-Modus über den Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Lernen von WAN-Link-IP-Adressen über den DHCP-Client](#).

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 **WAN-Links im privaten Intranet**.

Der DHCP-Client wird nun auf dem privaten Intranetlink unterstützt.

**Hinweis:**

Eine LAN-Schnittstelle darf nicht an das Fail-to-Wire-Paar angeschlossen werden, da Pakete möglicherweise zwischen den Schnittstellen überbrückt werden.

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.

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 <input type="button" value="↕"/> <input type="button" value="Submit"/>
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew <input type="button" value="↕"/> <input type="button" value="Submit"/>

DHCP-Protokolle

Mit Citrix SD-WAN können Sie DHCP-Serverprotokolle für IP-Adressen generieren. Immer wenn IP-Adressen Endpunkten zugewiesen werden, werden die Protokolle generiert. Die Protokolle enthalten Details wie den Zeitstempel der IP-Adresszuweisung und Lease-Dauer, die MAC-Adresse, die Client-ID usw. Die Client-ID **none** zeigt an, dass sie nicht in der DHCP-Anforderung vorhanden ist.

Um DHCP-Protokolle zu generieren und anzuzeigen, navigieren Sie zu **Konfiguration > Protokollierung/Überwachung**. Wählen Sie in der Dropdownliste die Option **SDWAN_dhcp.log** aus und klicken Sie auf **Protokoll anzeigen**.

```
Feb 4 11:58:30 BR1-Primary dhcpd: Internet Systems Consortium DHCP Server 4.3.2
Feb 4 11:58:30 BR1-Primary dhcpd: Copyright 2004-2015 Internet Systems Consortium.
Feb 4 11:58:30 BR1-Primary dhcpd: All rights reserved.
Feb 4 11:58:30 BR1-Primary dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Feb 4 11:58:30 BR1-Primary dhcpd: Write 0 deleted host decls to leases file.
Feb 4 11:58:30 BR1-Primary dhcpd: Write 0 new dynamic host decls to leases file.
Feb 4 11:58:30 BR1-Primary dhcpd: Write 1 leases to leases file.
Feb 4 11:58:30 BR1-Primary dhcpd: Listening on LPF/vni-1/36:00:d6:52:9f:cc/172.58.3.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Sending on LPF/vni-1/36:00:d6:52:9f:cc/172.58.3.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb 4 11:58:30 BR1-Primary dhcpd: Listening on LPF/vni-0/de:02:2f:9e:4c:3d/172.58.30.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Sending on LPF/vni-0/de:02:2f:9e:4c:3d/172.58.30.0/24
Feb 4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPDISCOVER from 02:03:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPOFFER on 172.58.30.151 to 02:03:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPREQUEST for 172.58.30.151 from 02:03:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: DHCPACK on 172.58.30.151 to 02:03:f0:de:19:3f via vni-0
Feb 4 11:58:31 BR1-Primary dhcpd: Lease time Start : 4 1970/01/01 00:00:00; Lease time end : 4 1970/01/01 00:00:00; for IP : 172.58.30.151; MAC-Address : 02:03:f0:de:19:3f; Client-ID : <none>
```

Hinweis

Diese Protokolle werden nur generiert, wenn Citrix SD-WAN als DHCP-Server fungiert.

Dynamische PAC-Dateianpassung

August 29, 2022

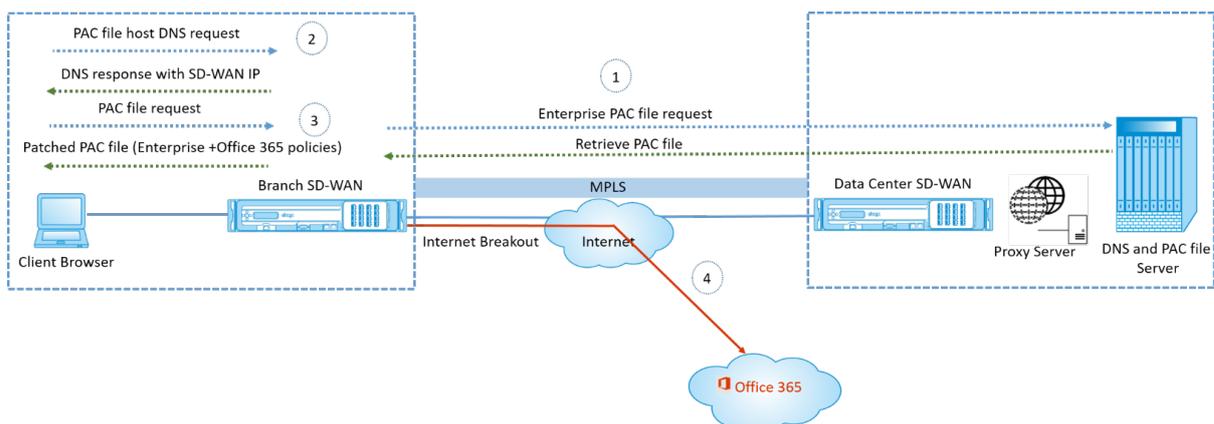
Mit der zunehmenden Akzeptanz geschäftskritischer SaaS-Anwendungen und verteilter Belegschaft in Unternehmen wird es äußerst wichtig, Latenz und Überlastung zu reduzieren. Latenz und Überlastung sind traditionellen Methoden zum Backhauling des Datenverkehrs durch das Rechenzentrum inhärent. Citrix SD-WAN 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

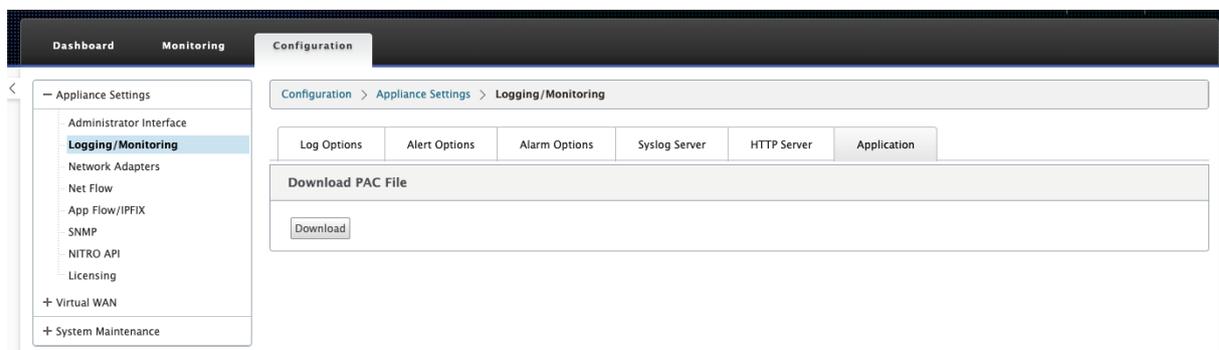
1. Die Unternehmen sollten eine PAC-Datei gehostet haben.
2. Die PAC-Datei sollte einen Platzhalter *SDWAN_TAG* oder ein Vorkommen der *findproxyforurl-Funktion* zum Patchen von Office 365-URLs haben.
3. Die PAC-Datei-URL sollte domänenbasiert und nicht IP-basiert sein.
4. Die PAC-Datei wird nur über 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 mit dem Citrix SD-WAN Orchestrator Service aktivieren. Weitere Informationen finden Sie unter [Automatische Proxy-Konfiguration](#).

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.

The screenshot shows the 'Diagnostics' section of the Citrix SD-WAN 11.5 interface. It includes a navigation menu on the left with options like 'Appliance Settings', 'Virtual WAN', and 'System Maintenance'. The main area is titled 'Configuration > System Maintenance > Diagnostics' and contains several sub-sections: 'Insert Event', 'Download Events', 'Alert Count', and 'View Events'. The 'View Events' section is expanded, showing a table of events with columns for ID, Object ID, Object Name, Object Type, Time, Event Type, Severity, and Description. The events listed are all 'PAC File Patching' operations that were successful.

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
261	26	PAC File Patching	APPLICATIONS	2019-05-28 08:39:02	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
260	26	PAC File Patching	APPLICATIONS	2019-05-28 08:29:02	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
259	26	PAC File Patching	APPLICATIONS	2019-05-28 08:19:02	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
258	26	PAC File Patching	APPLICATIONS	2019-05-28 08:09:02	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
257	26	PAC File Patching	APPLICATIONS	2019-05-28 07:59:02	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
256	26	PAC File Patching	APPLICATIONS	2019-05-28 07:49:01	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
255	26	PAC File Patching	APPLICATIONS	2019-05-28 07:39:01	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
254	26	PAC File Patching	APPLICATIONS	2019-05-28 07:29:01	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
253	26	PAC File Patching	APPLICATIONS	2019-05-28 07:19:01	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
252	26	PAC File Patching	APPLICATIONS	2019-05-28 07:09:01	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
251	26	PAC File Patching	APPLICATIONS	2019-05-28 06:59:01	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
250	26	PAC File Patching	APPLICATIONS	2019-05-28 06:49:00	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS
249	26	PAC File Patching	APPLICATIONS	2019-05-28 06:39:00	SUCCESS	INFO	Successfully patched the enterprise PAC file with Office 365 LURLS

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

August 29, 2022

Mit der GRE-Tunnel-Funktion können Sie Citrix SD-WAN-Appliances zum Beenden von GRE-Tunneln im LAN oder Intranet konfigurieren. Informationen zum Konfigurieren eines GRE-Tunnels mithilfe des SD-WAN Orchestrator Service finden Sie unter [GRE-Dienst](#).

In-Band- und Backup-Management

November 16, 2022

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.

Ab Version Citrix SD-WAN 11.4.2 ist es zwingend erforderlich, die In-Band-Verwaltung zu konfigurieren, um die Konnektivität zum Citrix SD-WAN Orchestrator Service über einen In-Band-Verwaltungsport herzustellen. Andernfalls verliert die Appliance die Konnektivität zum Citrix SD-WAN Orchestrator Service, wenn der Management-Port nicht verbunden ist und die In-Band-IP-Adresse ebenfalls nicht konfiguriert ist.

Hinweis

- 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.

Ab Citrix SD-WAN 11.5 können Sie die In-Band-Verwaltung auf einer virtuellen IP nur über den Citrix SD-WAN Orchestrator Service aktivieren. Weitere Informationen finden Sie unter [Inband-Verwaltung](#).

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

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.

The screenshot shows the 'Monitoring > Firewall' page in the Citrix SD-WAN web interface. The 'Firewall Statistics' section is visible, with a 'Connections' dropdown menu. Below it, there are various filtering options for Routing Domain, IP Protocol, Source Service Type, Destination Service Type, Application, Source Zone, Destination Zone, Source IP, and Destination IP. The 'Destination IP' field is set to '172.170.10.78'. The 'Connections' table below shows several active connections to this IP address on ports 22 and 443.

Routing Domain	Application	Family	IP Protocol	Source				Destination				State	Is NAT	Sent			Received					
				IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type			Service Name	Zone	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS
Corporate	Secure Shell(ssh)	Encrypted	TCP	172.170.10.135	54257	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	22	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	78	6824	0.364	0.255	53	7429	0.247
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54288	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	139	10130	5.692	3.319	234	238238	9.583
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54299	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	565	28811	23.147	9.443	1087	1594099	44.533
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54300	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	90	9201	3.691	3.019	157	212744	6.439
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54301	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	111	7987	4.554	2.631	202	291743	8.287
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54302	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.419	0.434	4	309	0.280
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54303	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.422	0.437	4	309	0.282
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54289	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	355	20266	13.558	6.619	1666	1980449	25.435

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.

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 Softwarevereinbarung 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.

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
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 Kontrol-

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.

WAN Settings (Ports: 2)					
Port	DHCP Mode	IP Address	Gateway IP Address	VLAN ID	Wan Tracking IP Address
2	<input type="checkbox"/>	11.11.11.10/24	11.11.11.11	50	
4	<input checked="" type="checkbox"/>				9.9.9.9
5	<input checked="" type="checkbox"/>				9.9.9.9

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.

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 Management-Port nur auf den folgenden Plattformen in einen Datenport umwandeln:

- Citrix SD-WAN 110 SE/LTE
- Citrix SD-WAN 210 SE/LTE

Sie können einen Verwaltungsport nur konfigurieren, wenn die In-Band-Verwaltung auf anderen vertrauenswürdigen Schnittstellen der Appliance aktiviert ist.

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 über einen Internetdienst verfügt, der mit einer einzigen Routingdomäne konfiguriert ist, wird standardmäßig eine vertrauenswürdige Schnittstelle mit aktivierter Identität als Backup-Verwaltungsnetzwerk ausgewählt.

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.

The screenshot shows the 'Firewall Statistics' and 'Connections' sections of the Citrix SD-WAN management interface. The 'Connections' table lists various network connections with columns for Routing Domain, Application, Family, IP Protocol, IP Address, Port, Service Type, Service Name, Zone, Destination IP Address, Port, Service Type, Service Name, Zone, State, Is NAT, Packets, Bytes, PPS, kbps, and Received. The IP address 172.170.10.78 is highlighted in red in the 'IP Address' column of the first row.

Routing Domain	Application	Family	IP Protocol	Source			Destination				State	Is NAT	Sent			Received						
				IP Address	Port	Service Type	IP Address	Port	Service Type	Service Name			Zone	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS		
Corporate	Transmission Control Protocol(tcp)	Network Service	TCP	172.170.10.78	49818	IPHost	-	Default_LAN_Zone	182.102.11	443	Internet	Branch1-Internet	Untrusted_Internet_Zone	SYN_SENT	Yes	1	60	-	-	0	0	-
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58939	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	NEW	Yes	2	148	-	-	0	0	-
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43012	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	168	0.070	0.047	2	297	0.070
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36558	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	148	0.011	0.007	2	277	0.011
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.78	60624	IPHost	-	Default_LAN_Zone	18.235.40.8	443	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	9	1271	0.176	0.199	7	4069	0.131
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	60585	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	0.002	1	128	0.002
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58010	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.020	0.013	1	80	0.020
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36684	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	0.004	1	161	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	33173	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	0.002	1	80	0.002
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53914	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	0.004	1	128	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53708	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	128	0.013	0.007	2	144	0.013
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43704	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.020	0.013	1	144	0.013

Internetzugriff

November 16, 2022

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

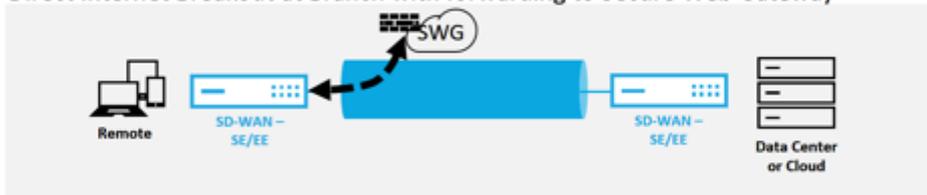
Informationen zum Konfigurieren eines Internetdienstes über den Citrix SD-WAN Orchestrator Service finden Sie unter [Internetdienst](#).

Internet Traffic Control

Direct Internet Breakout at Branch with Integrated Firewall



Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



Backhaul Internet to Data Center MCN



Direktes Internetbreakout in Branch mit integrierter Firewall

Der Internetdienst kann in den verschiedenen Bereitstellungsmodi verwendet werden, die von Citrix SD-WAN unterstützt werden.

- Inline-Bereitstellungsmodus (SD-WAN-Overlay)

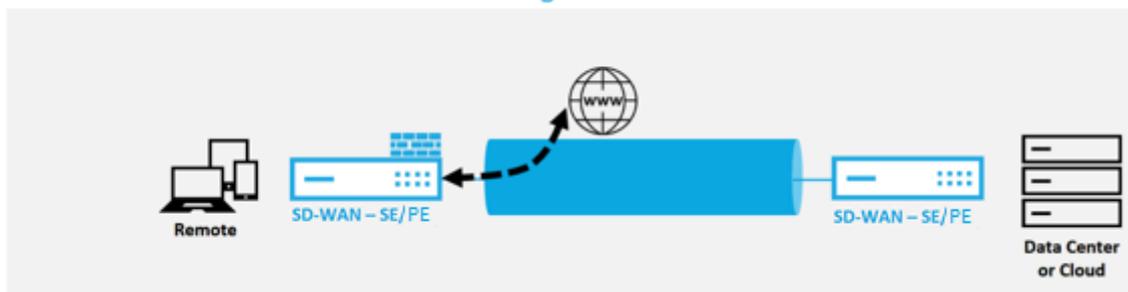
Citrix SD-WAN kann als Overlay-Lösung in jedem Netzwerk bereitgestellt werden. Als Overlay-Lösung wird SD-WAN im Allgemeinen hinter vorhandenen Edge-Routern und/oder Firewalls eingesetzt. Wenn SD-WAN hinter einer Netzwerk-Firewall bereitgestellt wird, kann die Schnittstelle als vertrauenswürdig konfiguriert 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.

Informationen zum Konfigurieren eines Internetdienstes über den Citrix SD-WAN Orchestrator Service finden Sie unter [Internetdienst](#).

Direct Internet Breakout at Branch with Integrated Firewall



Direkter Internetzugang mit Secure Web Gateway

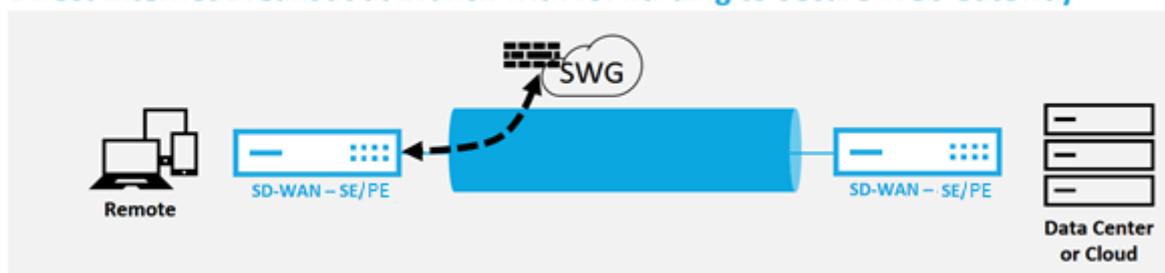
Um Datenverkehr zu sichern und Richtlinien durchzusetzen, verwenden Unternehmen häufig MPLS-Links, um Zweigdatenverkehr in das Unternehmens-Rechenzentrum zurückzuleiten. Das Rechenzentrum wendet Sicherheitsrichtlinien an, filtert den Datenverkehr durch Sicherheitsanwendungen, um Malware zu erkennen, 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.

Informationen zum Konfigurieren eines Internetdienstes über den Citrix SD-WAN Orchestrator Service finden Sie unter [Internetdienst](#).

Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



Citrix SD-WAN unterstützt die folgenden Secure Web Gateway-Lösungen von Drittanbietern:

- [Zscaler](#)
- [Forcepoint](#)
- [Palo Alto](#)
- [Citrix Secure Internet Access](#)

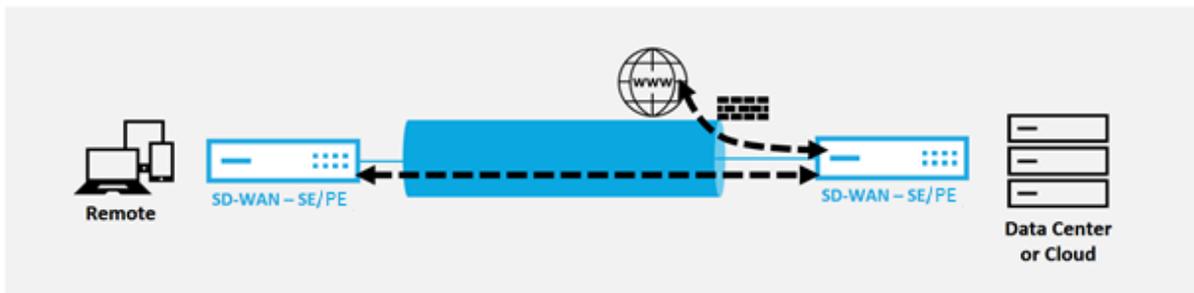
Backhaul Internet

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.

Backhaul Internet to Data Center MCN



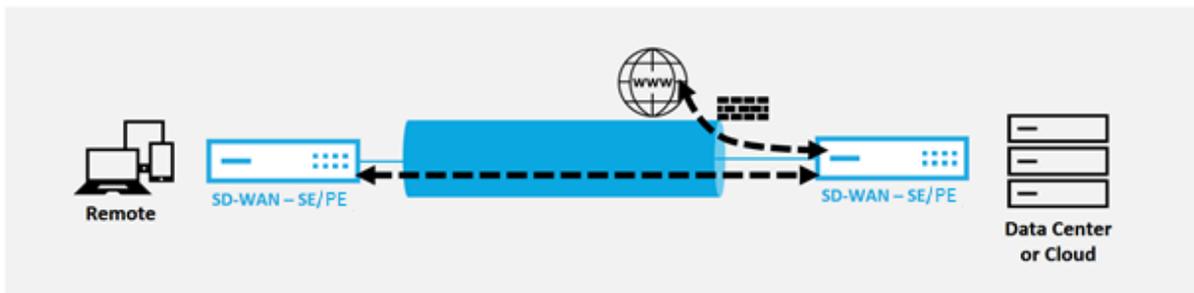
Alle Citrix SD-WAN Geräte können bis zu acht verschiedene Internet-WAN-Verbindungen in einem einzigen Gerät beenden. Lizenzierte Durchsatzfunktionen für die aggregierten WAN-Verbindungen werden pro entsprechender Appliance im Citrix SD-WAN Datenblatt aufgeführt.

Hairpin-Modus

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.

Backhaul Internet to Data Center MCN



Betrachten Sie beispielsweise einen Administrator mit mehreren SD-WAN-Sites, A und B. Standort A verfügt über einen schlechten Internetdienst. 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-Weiterleitung 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-Weiterleitung und Hairpin-Bereitstellung schließen sich gegenseitig aus. Nur einer von ihnen kann zu einem bestimmten Zeitpunkt konfiguriert werden.

Citrix SD-WAN SE- und VPX-Appliances (virtuell) 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.

Gehostete Firewalls

November 16, 2022

Der Citrix SD-WAN Orchestrator Service unterstützt die folgenden gehosteten Firewalls:

- [Palo Alto Netzwerke](#)
- [Check Point](#)

Palo Alto Networks Firewall-Integration auf SD-WAN 1100 Plattform

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 in den **Virtual Wire-Modus** integriert, an den zwei virtuelle Datenschnittstellen angeschlossen sind. Erforderlicher Datenverkehr kann durch Konfigurieren von Richtlinien auf SD-WAN an die virtuelle Firewall-Maschine umgeleitet werden.

Informationen zum Bereitstellen der virtuellen Firewallmaschine über den SD-WAN Orchestrator Service finden Sie unter [Gehostete Firewalls](#).

Vorteile

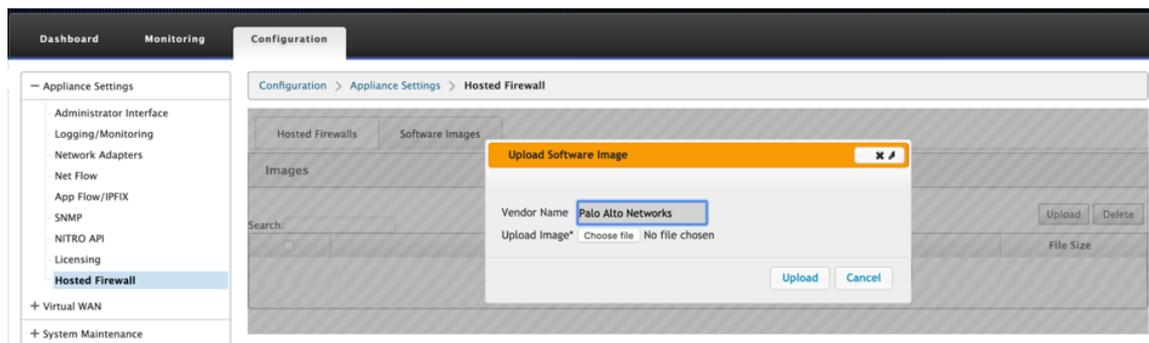
Im Folgenden sind die Hauptziele oder Vorteile der Integration von Palo Alto Networks auf der SD-WAN 1100-Plattform aufgeführt:

- Konsolidierung von Zweigstellengeräten: Eine einzelne Appliance, die sowohl SD-WAN als auch erweiterte Sicherheit bietet.
- Sicherheit in Zweigstellen mit On-Prem NGFW (Next Generation Firewall) zum Schutz des LAN-zu-LAN-, LAN-zu-Internet- und Internet-zu-LAN-Datenverkehrs.

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**.

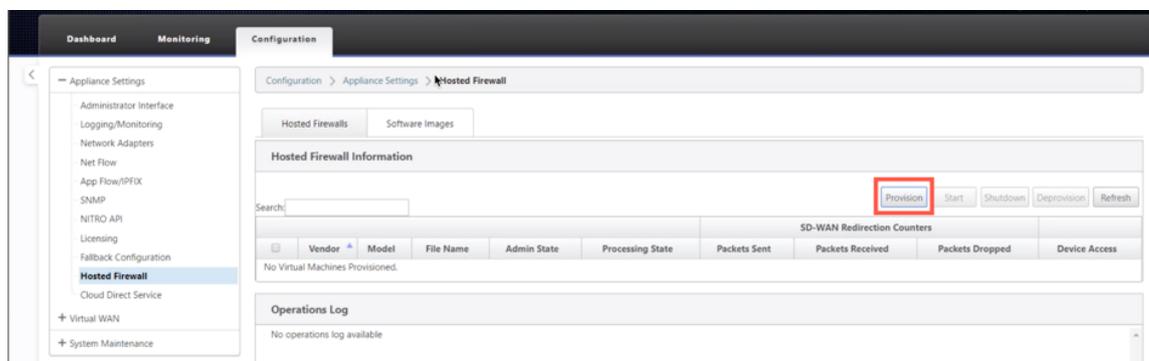


Hinweis:

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**.



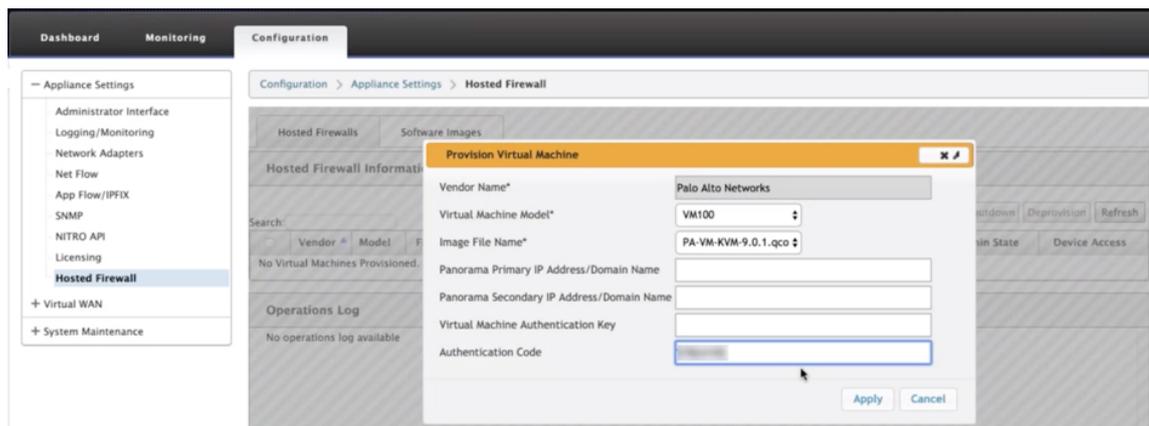
4. Geben Sie die folgenden Details für die Provisioning.

- **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).

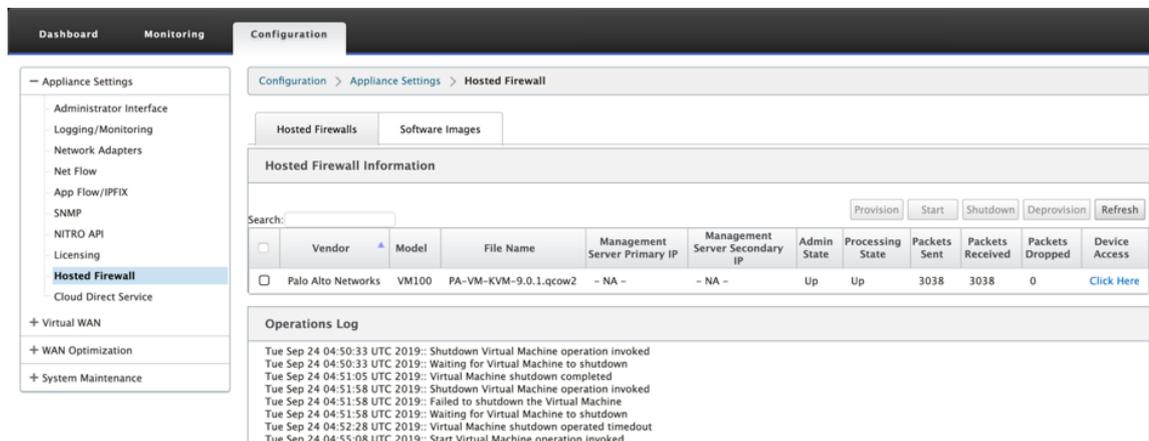
- **Authentifizierungsschlüssel für virtuelle Maschinen:** Geben Sie den Authentifizierungsschlüssel für die virtuelle Maschine an (optional).

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 **Anwenden**.



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.

Check Point Firewall-Integration auf der SD-WAN 1100-Plattform

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 SE-Plattform. Die virtuelle Firewall-Maschine ist im Bridge-Modus mit zwei verbundenen virtuellen Datenschnittstellen integriert. Erforderlicher Datenverkehr kann durch Konfigurieren von Richtlinien auf SD-WAN an die virtuelle Firewall-Maschine umgeleitet werden.

Informationen zum Bereitstellen der virtuellen Firewallmaschine über den SD-WAN Orchestrator Service finden Sie unter [Gehostete Firewalls](#).

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

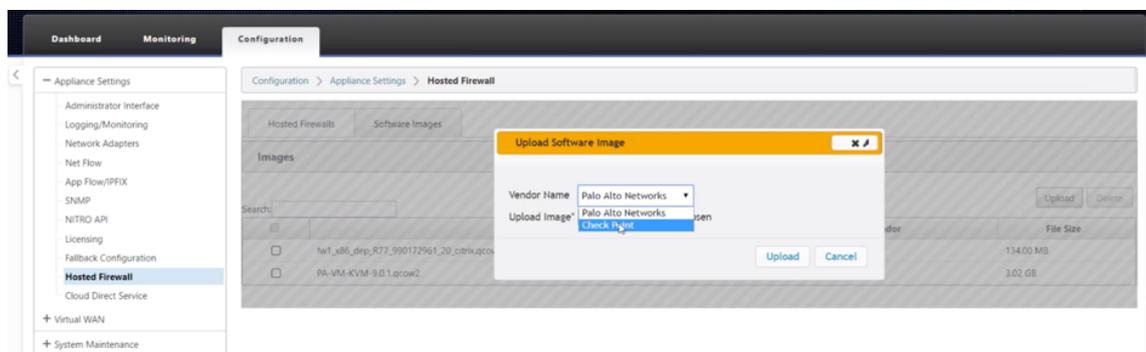
Im Folgenden werden die wichtigsten Ziele oder Vorteile der Check Point-Integration auf der SD-WAN 1100 Plattform aufgeführt:

- 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

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**.

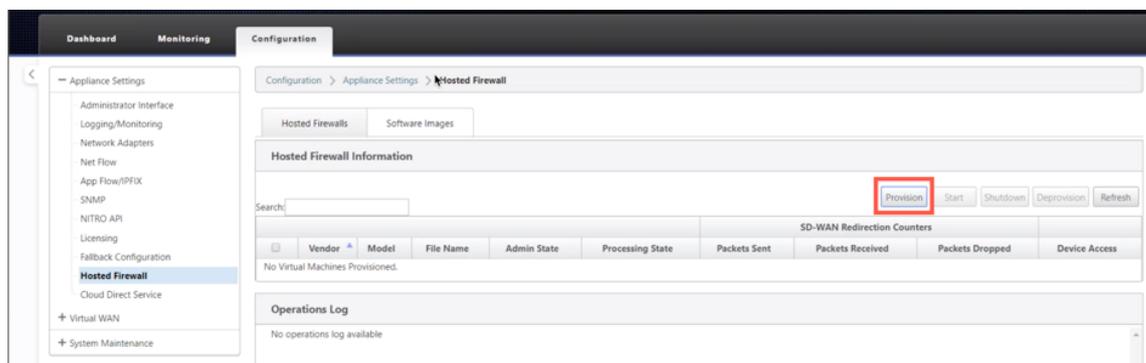


Hinweis:

Es können maximal zwei Images hochgeladen werden. Das Hochladen des Images der Check Point virtuellen Maschine kann je nach Bandbreitenverfügbarkeit länger dauern.

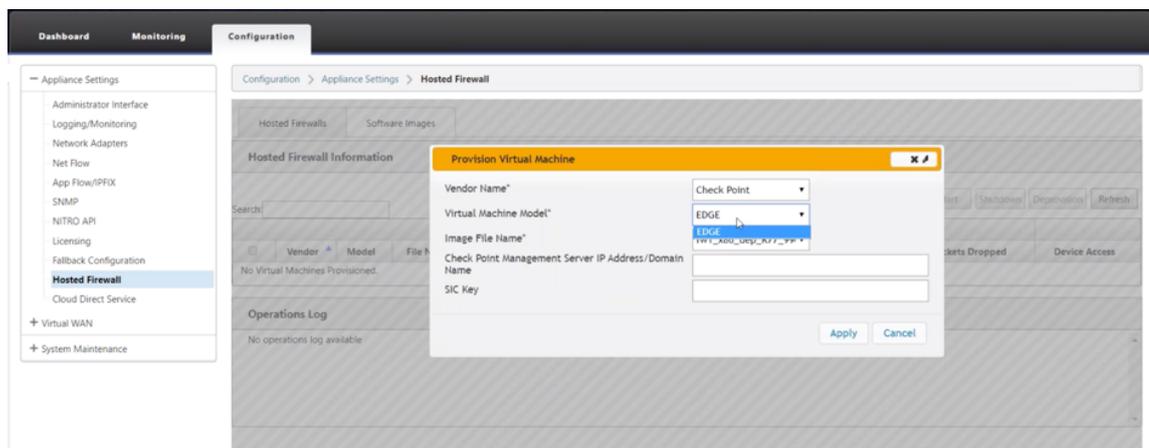
Sie können eine Statusleiste sehen, um den Upload-Prozess zu verfolgen. Das Dateidetail wird aktualisiert, sobald das Image erfolgreich hochgeladen wurde. Das Image, das für die Bereitstellung verwendet wird, kann nicht gelöscht werden. Führen Sie keine Aktion aus oder gehen Sie zurück zu einer anderen Seite, bis die Imagedatei 100% hochgeladen zeigt.

3. Für die Provisioning wählen Sie die Registerkarte **Gehostete Firewall** > klicken Sie auf die Schaltfläche **Bereitstellen**.

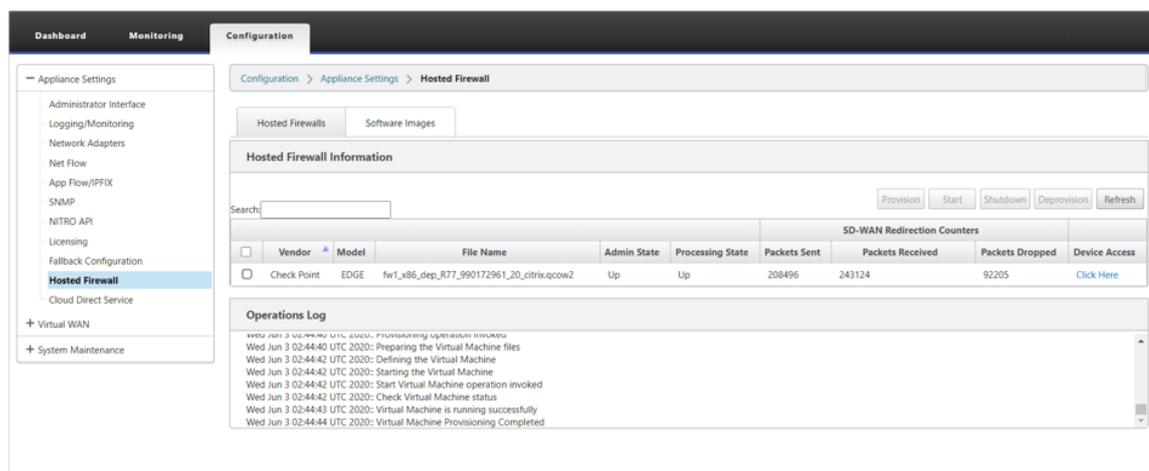


4. Geben Sie die folgenden Details für die Provisioning.

- **Anbietername:** Wählen Sie den **Namen des Anbieters** als Check Point aus.
- **Modell der virtuellen Maschine:** Das Modell der virtuellen Maschine wird automatisch als **Edge** ausgefüllt.
- **Imagedateiname:** Der Name der Imagedatei wird automatisch ausgefüllt.
- **Überprüfen Sie die IP Adresse/Domäne des Point Management Servers:** Geben Sie die IP-Adresse/Domäne des Checkpoint Management Servers an.
- **SIC-Schlüssel:** Geben Sie den SIC-Schlüssel an (optional). SIC schafft vertrauenswürdige Verbindungen zwischen **Check Point-Komponenten**. Klicken Sie auf **Anwenden**.



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.

Während die gesamte Netzwerkkonfiguration aktiv ist und ausgeführt wird, können Sie die Verbindung unter **Überwachung > Firewall > Filterrichtlinien** überwachen.

The screenshot displays the 'Filter Policies' configuration page in the Citrix SD-WAN GUI. The interface includes a sidebar on the left with navigation options such as 'Dashboard', 'Monitoring', and 'Configuration'. The main content area is titled 'Monitoring > Firewall' and contains 'Firewall Statistics' and a table of 'Filter Policies'.

Firewall Statistics

Statistics: Filter Policies ▾
 Maximum entries to display: 50 ▾
 Filtering: Application: Any ▾ Family: Any ▾ IP Protocol: Any ▾
 Filter Policy Action: Any ▾ Source Service Type: Any ▾ Source Service Name: Any ▾ Source IP: *
 Source Port: * Destination Service Type: Any ▾ Destination Service Name: Any ▾ Destination IP: *
 Destination Port: * Source Zone: Any ▾ Destination Zone: Any ▾ DSCP: Any ▾
 Show latest data.
 Refresh Help

Filter Policies

Default Policy= Allow(Not Tracked) Packets= 42 Bytes= 3528
 Match In Progress Packets= 0 Bytes= 0

ID	Application	Family	IP Protocol	DSCP	Source				Destination				Action	Conn Match Type	Track Connection	Allow Fragments		
					Service Type	Service Name	IP Address	Port or ICMP Type	Zone	Service Type	Service Name	IP Address					Port or ICMP Code	Zone
1	*	*	*	*	*	-	*	NA	*	Internet	-	*	NA	*	Redirect	Symmetric	No	Yes
2	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
3	*	*	*	*	*	-	*	NA	*	Virtual Path	-	*	NA	*	Redirect	Symmetric	No	Yes
4	*	*	*	*	Virtual Path	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
5	*	*	*	*	IPHost	-	*	NA	*	*	-	*	NA	*	Allow	Symmetric	No	Yes
6	*	*	TCP	*	Internet	-	*	*	Internet_Zone	*	-	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes
7	*	*	UDP	*	Internet	-	*	*	Internet_Zone	*	-	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes
8	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Drop	Symmetric	No	Yes

Filter Policies Displayed: 8
 Filter Policies In Use: 8/1000

Verknüpfungsaggregationsgruppen

August 29, 2022

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 Citrix SD-WAN 11.3 werden die protokollbasierten Verhandlungen des 802.3AD Link Aggregation Control Protocol (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 **Aktiv-Aktiv-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 1100 SE
- Citrix SD-WAN 2100 SE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE
- Citrix SD-WAN 6100 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.

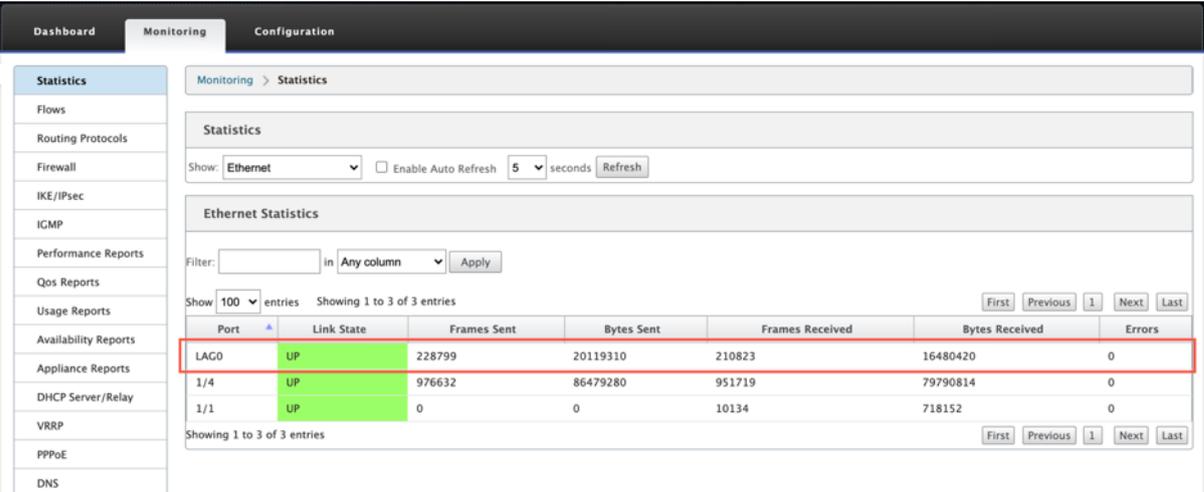
Hinweis

- Für Citrix SD-WAN 210 SE Appliances können Sie nur eine LAG mit maximal drei darin gruppierten Ports erstellen.
- Die [Link State Propagation \(LSP\)](#) -Funktion wird nicht unterstützt, wenn LAGs als Ethernet-Schnittstellen in Schnittstellengruppen verwendet werden.

Ab Citrix SD-WAN 11.5 können Sie Link-Aggregationsgruppen über den SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Link-Aggregationsgruppen](#).

Überwachung und Fehlerbehebung

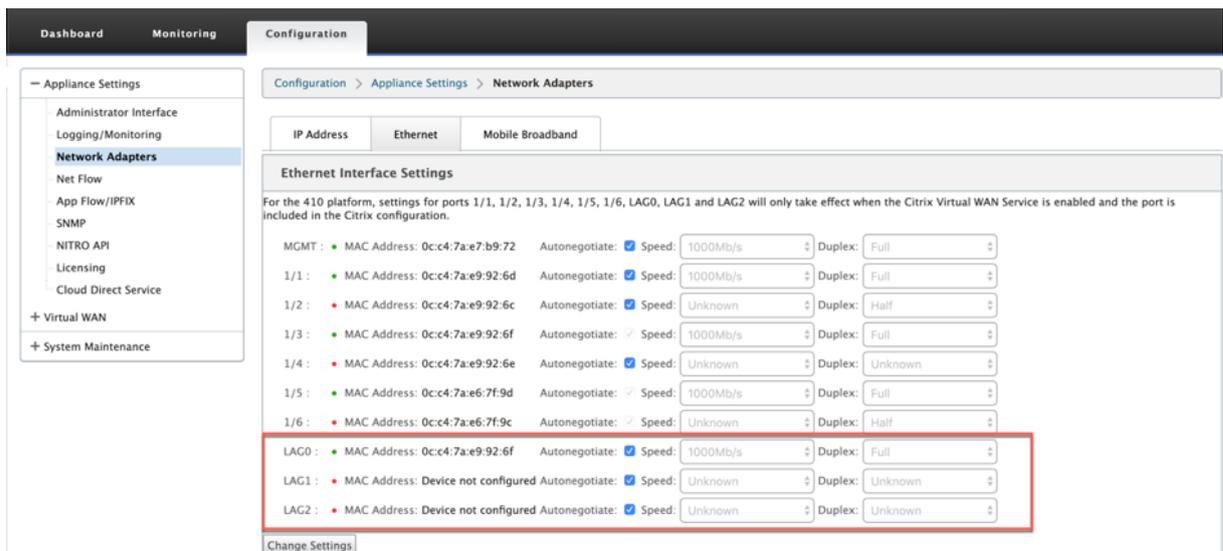
Um die Statistiken oder den Linkstatus anzuzeigen, navigieren Sie zu **Überwachung > Statistiken**. Wählen Sie **Ethernet** aus der Dropdownliste **Anzeigen** aus.



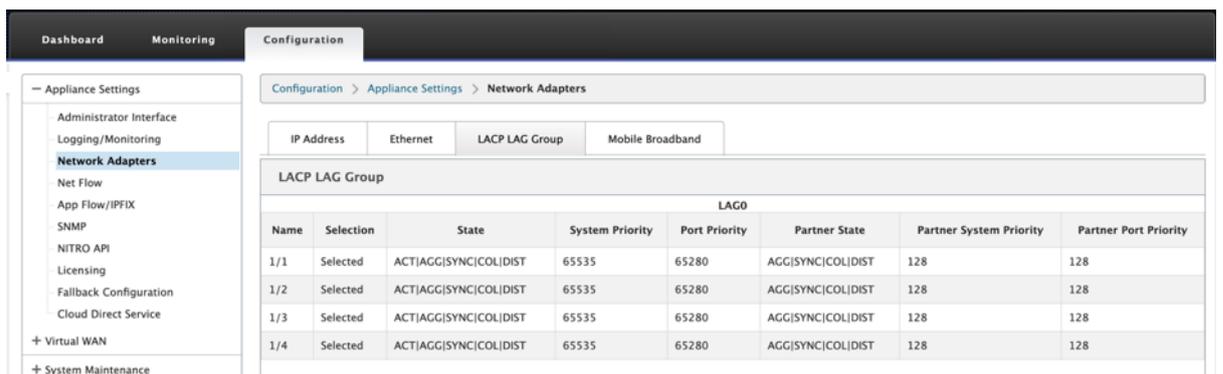
The screenshot displays the 'Monitoring > Statistics' page in the Citrix SD-WAN Orchestrator Service. The 'Statistics' section is active, showing 'Ethernet' selected in the 'Show' dropdown. The 'Ethernet Statistics' table is displayed with the following data:

Port	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
LAG0	UP	228799	20119310	210823	16480420	0
1/4	UP	976632	86479280	951719	79790814	0
1/1	UP	0	0	10134	718152	0

Um die aktiven und Standby-LAG-Ports anzuzeigen, navigieren Sie zu **Konfiguration > Appliance-Einstellungen > Netzwerkadapter > Ethernet**.



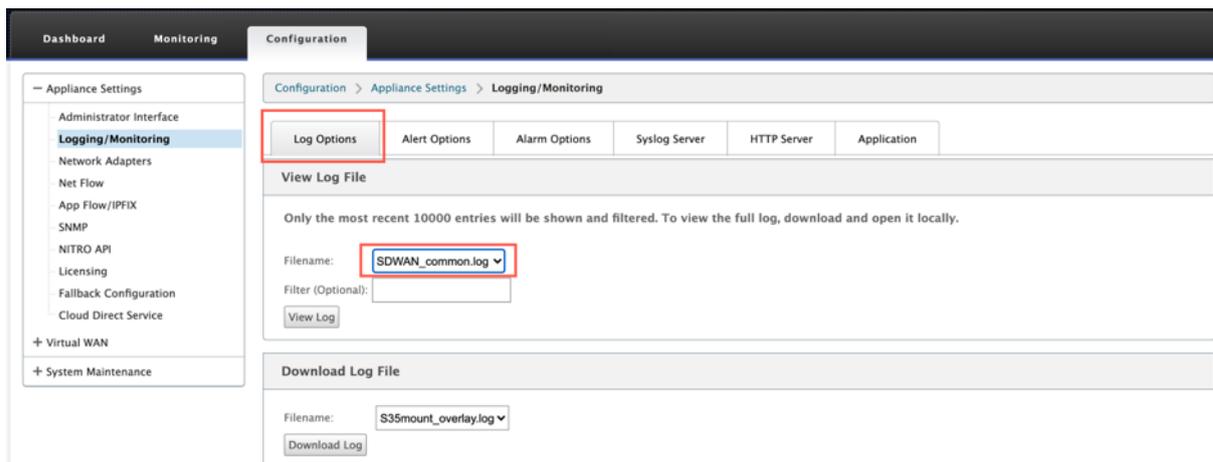
Wählen Sie die Registerkarte **LACP LAG Group**, um die verschiedenen Details zur LACP LAG-Gruppe anzuzeigen.



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

August 29, 2022

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.

Überwachung von Linkstatistiken

1. Wählen Sie auf der Seite **Monitor > Statistiken** im Dropdownmenü **Anzeigen** die Option **Ethernet aus**, um den Status des Bypass-Portpaares 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.

Statistics

Show: **Ethernet** Enable Auto Refresh 5 seconds Refresh

Ethernet Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries

Port	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
1	DOWN	132885	8755483	212584	15332801	0
2	DISABLED	17984552	1531084459	18189043	1584612144	3258

Showing 1 to 2 of 2 entries

2. Navigieren Sie zur Registerkarte **Konfiguration > Einheiteneinstellungen > Netzwerkadapter > Ethernet**. Die administrativ ausgefallenen Ports sind in der Liste **Ethernet-Schnittstelleneinstellungen** durch ein rotes Sternchen (*) gekennzeichnet.

Ethernet Interface Settings

1 :	•	MAC Address: 0c:c4:7a:12:bc:8d	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
2 :	• *	MAC Address: 0c:c4:7a:12:bc:8c	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
3 :	•	MAC Address: 0c:c4:7a:12:bc:8f	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
4 :	•	MAC Address: 0c:c4:7a:12:bc:8e	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
5 :	•	MAC Address: 0c:c4:7a:12:bc:91	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
MGT :	•	MAC Address: 0c:c4:7a:12:bc:90	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 100Mb/s	Duplex: Full
X1 :	•	MAC Address: 00:25:90:ed:22:9f	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
X2 :	•	MAC Address: 00:25:90:ed:22:9e	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
X3 :	•	MAC Address: 00:25:90:ed:22:9d	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
X4 :	•	MAC Address: 00:25:90:ed:22:9c	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown

* interface disabled by Port State Reflection

Change Settings

Mess- und Standby-WAN-Verbindungen

November 16, 2022

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. 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

- **AufAnforderung:** Der Standby-Link, der aktiv wird, wenn eine der Bedingungen erfüllt ist.
Wenn die verfügbare Bandbreite im virtuellen Pfad kleiner ist als das konfigurierte Bandbreitenlimit bei Bedarf UND eine ausreichende Nutzung vorhanden ist. Ausreichende Auslastung ist definiert als mehr als 95% (ON_DEMAND_USAGE_THRESHOLD_PCT) der aktuellen verfügbaren Bandbreite, oder die Differenz zwischen der aktuellen verfügbaren Bandbreite und der aktuellen Nutzung beträgt weniger als 250 kbps (ON_DEMAND_THRESHOLD_GAP_KBPS), beide Parameter können mit t2_variables geändert werden, wenn alle Nicht-Standby Pfade sind tot oder deaktiviert.
- **Last-Resort** - ein Standby-Link, der nur aktiv wird, wenn alle Nicht-Standby-Links und On-Demand-Standby-Links deaktiviert oder deaktiviert sind.
- Standby-Priorität gibt die Reihenfolge an, in der eine Standby-Verbindung aktiv wird, wenn mehrere Standby-Links vorhanden sind:

- 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 Weiterleitungspfades bevorzugt werden.

Der Pfadstatus eines Standby-Pfades 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-Pfades nicht zur Berechnung der MTU des virtuellen Pfades 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.

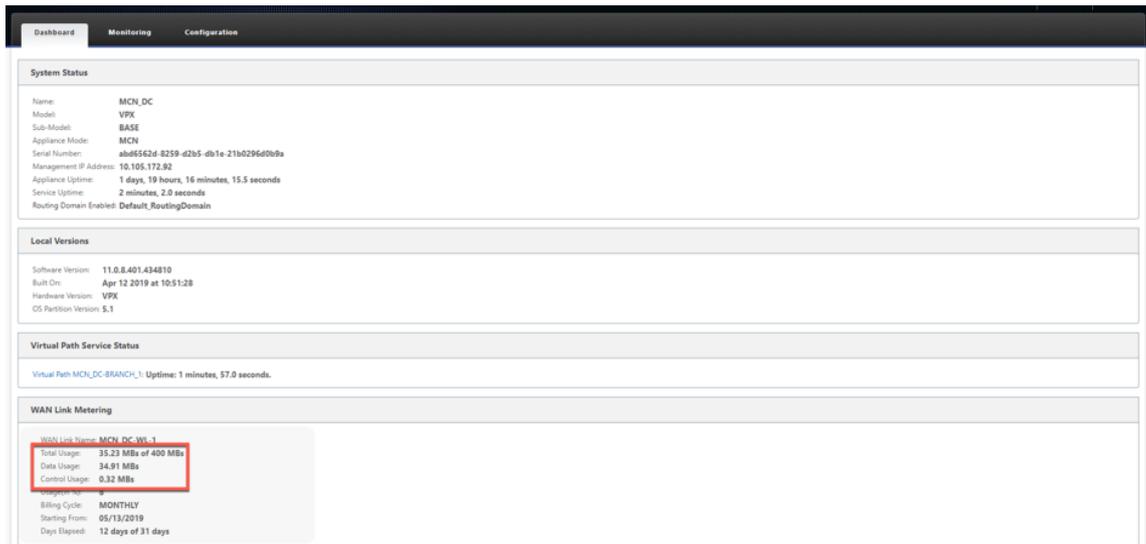
Ab SD-WAN 11.5 können Sie getaktete WAN-Verbindungen und Standby-WAN-Verbindungen mithilfe des Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Messung und Standby-WAN-Verbindungen](#).

Konfigurationsvoraussetzungen:

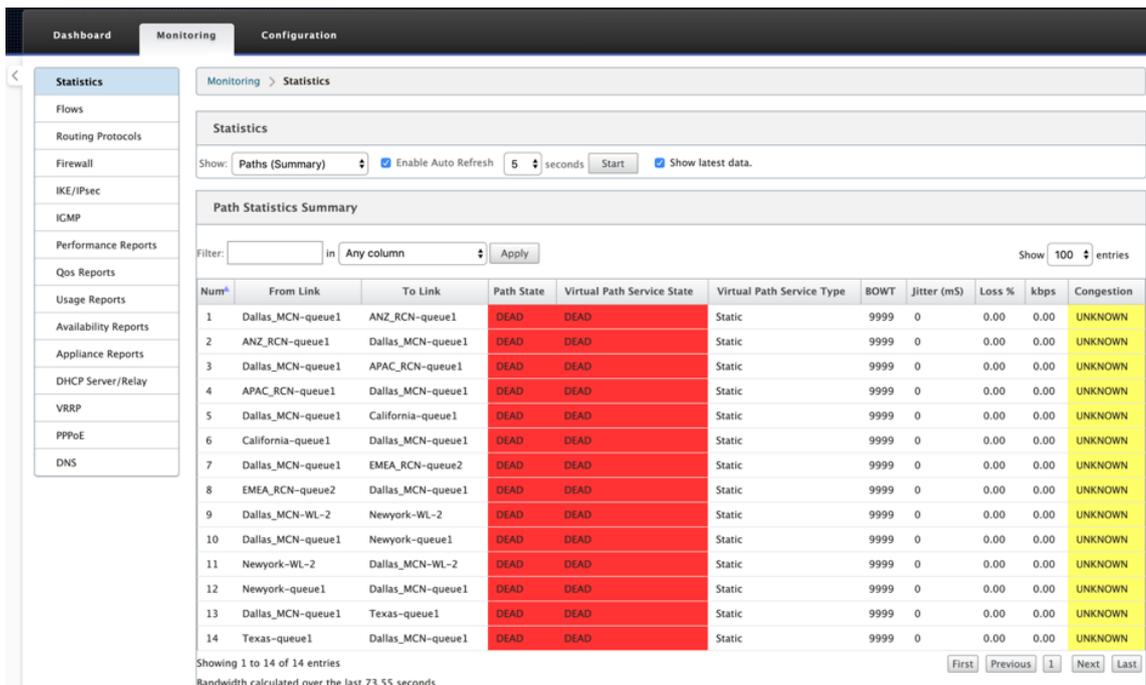
- Eine Zählerverbindung kann von jedem Zugriffstyp sein.
- Alle Links an einem Standort können mit aktivierter Messung konfiguriert werden.
- Ein Standby-Link kann vom Zugriffstyp “Public Internet” oder “Private Intranet” sein. Eine WAN-Verbindung vom Privaten MPLS-Zugriffstyp kann nicht als Standby-Verbindung 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.

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**).

Local WAN-to-LAN On Demand WAN Link Usages

Filter: in

Show entries Showing 0 to 0 of 0 entries

Adaptive Bandwidth Detection										
WAN Link	WAN Link Mode	Standby Priority	Configured	Minimum Acceptable BW Kbps	Maximum Allowed BW Kbps	Current Allowed BW Kbps	Virtual Path Name	Virtual Path On Demand Bandwidth Limit Kbps	Virtual Path Available Bandwidth Kbps	In Use
No data available in table										

Showing 0 to 0 of 0 entries

Bandwidth calculated over the last 5.078 seconds

- Wenn die Verwendung eines getakteten Links 50% des konfigurierten Datendeckels überschreitet, wird oben im Dashboard ein Warnbanner angezeigt. Wenn die Nutzung 75% der konfigurierten Datenbegrenzung übersteigt, werden außerdem die numerischen Messinformationen am unteren Rand des Dashboards hervorgehoben.

The data usage on the following Metered Wanlinks has reached the threshold:

- BR1-WL-1-New : 75%.

System Status

Name: BR1
 Model: VPX
 Sub-Model: BASE
 Appliance Mode: Client
 Serial Number: aa4580cb-7527-8dee-fbee-9824a89142e6
 Management IP Address: 10.105.184.72
 Appliance Uptime: 10 hours, 7 minutes, 34.6 seconds
 Service Uptime: 9 hours, 17 minutes, 53.0 seconds
 Routing Domain Enabled: Default, RoutingDomain

Local Versions

Configuration Created On: Thu Apr 18 20:08:57 2019
 Software Version: 11.0.13.401.434810
 Built On: Apr 18 2019 at 19:35:14
 Hardware Version: VPX
 OS Partition Version: 5.1

Virtual Path Service Status

Virtual Path DC-BR1 Uptime: 9 hours, 17 minutes, 43.0 seconds.

WAN Link Metering

WAN Link Name: BR1-WL-1-New
 Total Usage: **329.58 MBs of 400 MBs**
 Data Usage: 258.09 MBs
 Control Usage: 71.48 MBs
 Usage (%) : 82
 Billing Cycle: MONTHLY
 Starting From: 07/17/2019
 Days Elapsed: 3 days of 31 days

Ein WAN-Link-Verwendungsereignis wird auch an der Appliance generiert, wenn die Verwendung 50%, 75% und 90% der konfigurierten Datenobergrenze überschreitet.

ID	Link ID	Link Name	Type	Timestamp	Usage	Warning	Details
17654	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:22:58	USAGE_3	WARNING	Total usage 1.84 Cbytes used (91% of limit 2.00 Cbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17653	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:17:58	USAGE_2	WARNING	Total usage 1.52 Cbytes used (75% of limit 2.00 Cbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17652	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:09:58	USAGE_1	WARNING	Total usage 1.00 Cbytes used (50% of limit 2.00 Cbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017

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

- Die konfigurierten aktiven und Standby-Taktintervalle für jeden Pfad können unter **Konfiguration > Virtuelles WAN > Konfiguration anzeigen > Pfade** angezeigt werden.

Dashboard Monitoring **Configuration**

+ Appliance Settings

- Virtual WAN

View Configuration

- Configuration Editor
- Change Management
- Change Management Settings
- Compare Configurations
- Restart/Reboot Network
- Enable/Disable/Purge Flows
- Dynamic Virtual Paths
- SD-WAN Center Certificates

+ System Maintenance

Configuration > Virtual WAN > View Configuration

Configuration

View: Paths

Path Configuration

Paths on virtual path 3 'Dallas_MCN-ANZ_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	ANZ_RCN-queue1	192.168.1.10	192.168.90.10	-	-	4980	4980	
0	ANZ_RCN-queue1	Dallas_MCN-queue1	192.168.90.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	ANZ_RCN-queue1	YES	YES	YES	0	n/a	n/a
ANZ_RCN-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 8 'Dallas_MCN-APAC_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	APAC_RCN-queue1	192.168.1.10	192.168.80.10	-	-	4980	4980	
0	APAC_RCN-queue1	Dallas_MCN-queue1	192.168.80.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	APAC_RCN-queue1	YES	YES	YES	0	n/a	n/a
APAC_RCN-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 9 'Dallas_MCN-California':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	California-queue1	192.168.1.10	192.168.50.10	-	-	4980	4980	
0	California-queue1	Dallas_MCN-queue1	192.168.50.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	California-queue1	YES	YES	YES	0	n/a	n/a
California-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 12 'Dallas_MCN-EMEA_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	EMEA_RCN-queue2	192.168.1.10	17.1.1.10	-	-	4980	4980	
0	EMEA_RCN-queue2	Dallas_MCN-queue1	17.1.1.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	EMEA_RCN-queue2	YES	YES	YES	0	n/a	n/a
EMEA_RCN-queue2	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 13 'Dallas_MCN-Newyork':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
1	Dallas_MCN-queue1	Newyork-queue1	192.168.1.10	192.168.70.10	-	-	4980	4980	
0	Dallas_MCN-WL-2	Newyork-WL-2	192.168.10.10	192.168.60.10	-	-	4980	4980	
0	Newyork-WL-2	Dallas_MCN-WL-2	192.168.60.10	192.168.10.10	-	-	4980	4980	
1	Newyork-queue1	Dallas_MCN-queue1	192.168.70.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	Newyork-queue1	YES	YES	YES	0	n/a	n/a
Dallas_MCN-WL-2	Newyork-WL-2	YES	YES	YES	0	n/a	n/a
Newyork-WL-2	Dallas_MCN-WL-2	YES	YES	YES	0	n/a	n/a
Newyork-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Paths on virtual path 14 'Dallas_MCN-Texas':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	dallas_MCN-queue1	Texas-queue1	192.168.1.10	192.168.40.10	-	-	4980	4980	
0	Texas-queue1	Dallas_MCN-queue1	192.168.40.10	192.168.1.10	-	-	4980	4980	

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
Dallas_MCN-queue1	Texas-queue1	YES	YES	YES	0	n/a	n/a
Texas-queue1	Dallas_MCN-queue1	YES	YES	YES	0	n/a	n/a

Office 365-Optimierung

November 16, 2022

Die **Office 365-Optimierungsfunktionen** entsprechen den [Microsoft Office 365-Netzwerkverbindungsprinzipien](#) um Office 365 zu optimieren. Office 365 wird als Service über mehrere Service-Endpunkte (Front-türen) bereitgestellt, die sich global befinden. Um eine optimale Benutzererfahrung für 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 Datenverkehr eine Haustür erreicht, geht er über das Microsoft-Netzwerk 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. Office 365-Endpunkte werden in die Kategorien **Optimieren**, **Zulassen** und **Standard** klassifiziert. Citrix SD-WAN 11.4.0 bietet eine detailliertere Klassifizierung der Kategorien **“Optimieren“** und **“Zulassen“**, sodass selektive Buchungen die Leistung des netzwerksensitiven Office 365-Datenverkehrs verbessern können. Die Weiterleitung von netzwerksensitivem Datenverkehr zu SD-WAN in der Cloud (Cloud Direct oder ein SD-WAN VPX auf Azure) oder von einem SD-WAN-Gerät zu einem SD-WAN an einem nahe gelegenen Ort mit zuverlässigerer Internetkonnektivität ermöglicht QoS und eine überlegene Verbindungsresilienz im Vergleich zur einfachen Steuerung des Datenverkehrs auf den nächsten Office 365 Haustür, auf Kosten einer Erhöhung der Latenz. Eine mit Büchern geschlossene SD-WAN-Lösung mit QoS reduziert VoIP-Ausfälle und -Verbindungsabbruchungen, reduziert Jitter und verbessert die Mittelmeinung in Medienqualität für Microsoft Teams:

- **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 abrechen und dürfen nicht über das Rechenzentrum gehen.

Die Kategorie **Optimieren** ist in die folgenden Unterkategorien unterteilt:

- 1 - Teams Realtime
- 2 - Exchange Online
- 3 - SharePoint Optimize

Informationen zu Upgrade-Überlegungen finden Sie unter [Wichtige Überlegungen zum Upgrade](#).

- **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.

Die Kategorie **“Zulassen”** ist in die folgenden Unterkategorien unterteilt:

- 1 - Teams TCP Fallback
- 2 - Exchange Mail
- 3 - SharePoint Allow
- 4 - Office365 Common

Informationen zu Upgrade-Überlegungen finden Sie unter [Wichtige Überlegungen zum Upgrade](#).

Hinweis

Die Unterkategorie **Teams Realtime** verwendet das UDP-Echtzeit-Transportprotokoll zur Verwaltung des Microsoft Teams-Datenverkehrs, während die **TCP-Fallback-Unterkategorie Teams** das TCP-Transport-Layer-Protokoll verwendet. Da der Medienverkehr sehr latenzempfindlich ist, bevorzugen Sie möglicherweise, dass dieser Datenverkehr den direktesten Weg einschlägt und UDP anstelle von TCP als Transportschichtprotokoll verwendet (am meisten bevorzugter Transport für interaktive Echtzeitmedien in Bezug auf Qualität). Während UDP ein bevorzugtes Protokoll für den Medienverkehr von Teams ist, müssen bestimmte Ports in der Firewall zugelassen werden. Wenn die Ports nicht erlaubt sind, verwendet der Teams-Datenverkehr TCP als Fallback, und die Aktivierung der Optimierung für Teams TCP Fallback gewährleistet eine bessere Bereitstellung der Teams-Anwendung in diesem Szenario. Weitere Informationen finden Sie unter [Microsoft Teams-Callflows](#).

- **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.

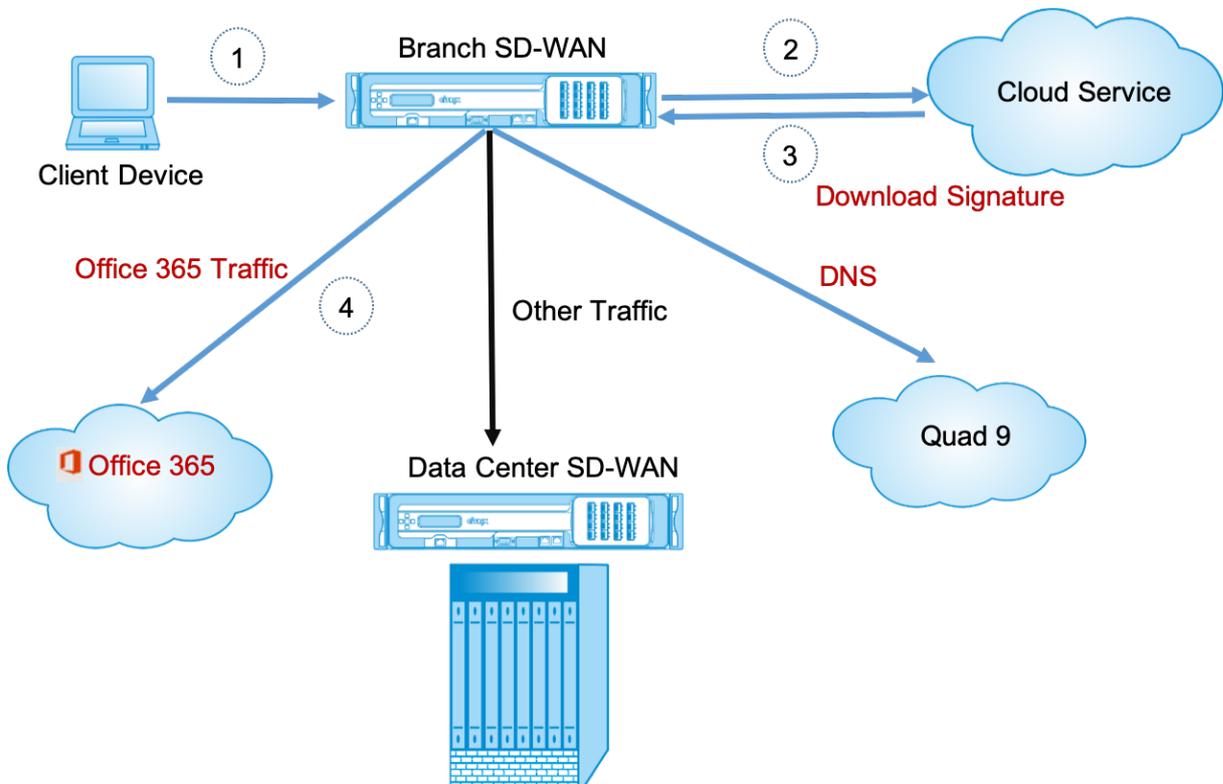
Funktionsweise der Office 365-Optimierung

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

Mit Ausnahme der Kategorie Office 365 Default wird standardmäßig die erste Paketerkennung und -klassifizierung des Office 365-Datenverkehrs durchgeführt, 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.

Ab Citrix SD-WAN 11.5 können Sie Office 365-Breakout über den Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Office 365-Optimierung](#).

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.

Wichtige Überlegungen für das Upgrade

Kategorien optimieren und zulassen

Wenn Sie die Internet-Breakout-Richtlinie für die Kategorien **Optimieren** und **Zulassen** von Office 365 aktiviert haben, aktiviert Citrix SD-WAN automatisch die Internet-Breakout-Richtlinie für die entsprechenden Unterkategorien beim Upgrade auf Citrix SD-WAN 11.4.0.

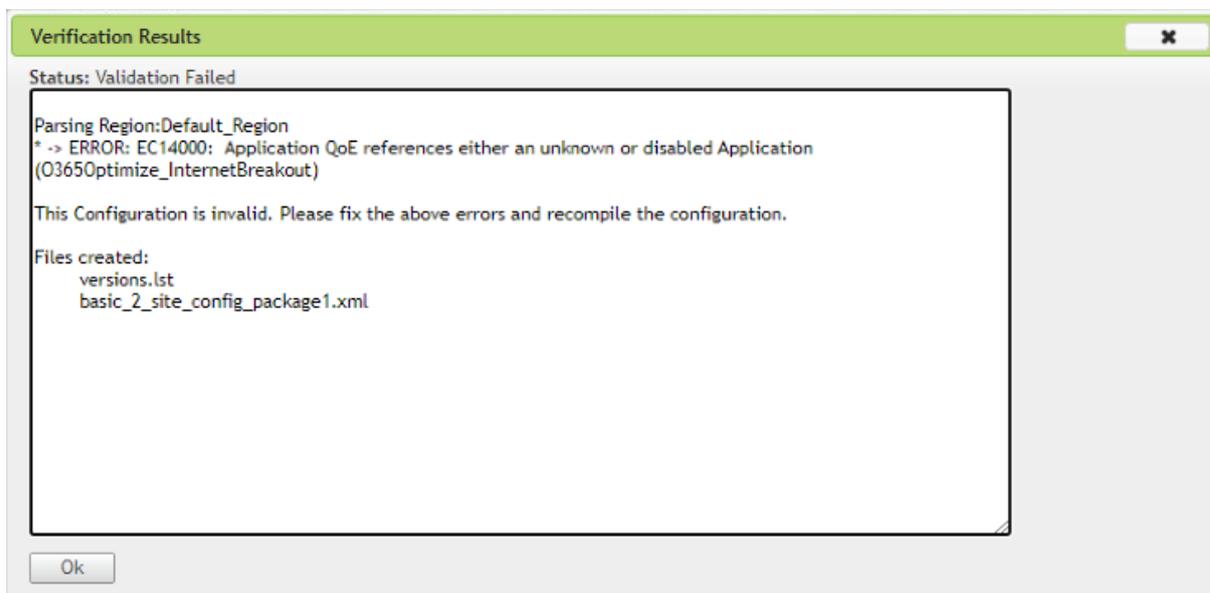
Wenn Sie auf eine Softwareversion herabstufen, die älter als Citrix SD-WAN 11.4.0 ist, müssen Sie den Internet-Breakout für die Kategorie **Optimize** oder **Allow** Office 365 manuell aktivieren, unabhängig davon, ob Sie die entsprechenden Unterkategorien in der Citrix SD-WAN 11.4.0 Version aktiviert haben oder nicht.

Office 365-Anwendungsobjekten

Wenn Sie Regeln/Routen mit den automatisch generierten Anwendungsobjekten **O365Optimize_InternetBreakout** und **o365allow_InternetBreakout** erstellt haben, löschen Sie die Regelungen/Routen, bevor Sie auf Citrix SD-WAN 11.4.0 aktualisieren. Nach dem Upgrade können Sie Regeln/Routen mit den entsprechenden neuen Anwendungsobjekten erstellen.

Wenn Sie mit dem Citrix SD-WAN 11.4.0-Upgrade fortfahren, ohne die Regeln/Routen zu löschen, wird ein Fehler angezeigt, und daher wird das Upgrade nicht erfolgreich. Im folgenden Beispiel hat ein

Benutzer ein Application QoE-Profil konfiguriert und zeigt einen Fehler beim Versuch, auf Citrix SD-WAN 11.4.0 zu aktualisieren, ohne die Regeln/Routen zu löschen:



Hinweis

Dieses Upgrade ist für automatisch erstellte Regeln/Routen nicht erforderlich. Sie gilt nur für Regele/Routen, die Sie erstellt haben.

DNS

Wenn Sie DNS-Proxy-Regeln oder transparente DNS-Forwarder-Regeln mit den Anwendungen **Office 365 Optimize** und **Office 365 Allow** erstellt haben, müssen Sie die Regeln vor dem Upgrade auf Citrix SD-WAN 11.4.0 löschen. Nach dem Upgrade können Sie die Regeln erneut mit den entsprechenden neuen Anwendungen erstellen.

Wenn Sie mit dem Citrix SD-WAN 11.4.0-Upgrade fortfahren, ohne die alten DNS-Proxy- oder transparenten Forwarder-Regeln zu löschen, wird kein Fehler angezeigt und das Upgrade wird ebenfalls erfolgreich. Die DNS-Proxy-Regeln und transparenten Weiterleitungsregeln werden in Citrix SD-WAN 11.4.0 jedoch nicht wirksam.

Hinweis

Diese Aktivität gilt nicht für die automatisch erstellten DNS-Regeln. Sie gilt nur für DNS-Regeln, die Sie erstellt haben.

Überwachen

Sie können die Office 365-Anwendungsstatistiken in den folgenden SD-WAN-Statistikberichten überwachen:

- Firewall-Statistiken

Connections		Source										Destination										Sent										Received									
Routing Domain	Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	IN Packets	Bytes	PPS	Mbps	Packets	Bytes	PPS	Mbps	Age (min)	Last Activity (min)	Related Objects																
Default_RoutingDomain	Windows Live(LiveConnect)	Web	TCP	172.170.10.135	60362	Local	VirtualInterface1	Default_LAN_Zone	104.137.251.20	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	10	1868	0.071	0.071	13	4764	0.062	0.236	211	30509	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	59278	Local	VirtualInterface1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	54	7076	0.737	0.772	56	13280	0.754	1.470	73	293	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	60302	Local	VirtualInterface1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	1089	82353	5.411	22.460	1880	66900	6.418	18.274	293	4662	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	60345	Local	VirtualInterface1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	63	23010	0.231	0.796	72	14114	0.287	0.489	251	32496	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	60682	Local	VirtualInterface1	Default_LAN_Zone	13.107.6.156	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	381	131932	0.903	2.643	472	35682	0.933	6.600	432	14217	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	60301	Local	VirtualInterface1	Default_LAN_Zone	40.126.13.101	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	22	4236	0.073	0.116	17	16036	0.058	0.381	234	8268	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	59275	Local	VirtualInterface1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	28	6469	0.317	0.769	23	10039	0.260	0.910	88	28294	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	59276	Local	VirtualInterface1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	63	7364	0.240	0.717	73	14988	0.281	1.380	88	293	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	62016	Local	VirtualInterface1	Default_LAN_Zone	52.108.256.1	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	21	4379	0.822	1.539	15	10058	0.659	3.745	13	13453	View Refresh Filter															
Default_RoutingDomain	Office 365 Common(Office365_common)	Web	TCP	172.170.10.135	59282	Local	VirtualInterface1	Default_LAN_Zone	40.126.13.232	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	38	15423	0.217	0.745	39	24038	0.175	1.187	166	6262	View Refresh Filter															
Default_RoutingDomain	Microsoft(Microsoft)	Web	TCP	172.170.10.135	60397	Local	VirtualInterface1	Default_LAN_Zone	13.107.6.163	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	37	7321	0.124	0.196	42	10403	0.141	0.279	296	8887	View Refresh Filter															
Default_RoutingDomain	Microsoft(Microsoft)	Web	TCP	172.170.10.135	60347	Local	VirtualInterface1	Default_LAN_Zone	52.253.156.4	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	24	3618	0.098	0.115	19	9821	0.076	0.318	251	9877	View Refresh Filter															
Default_RoutingDomain	Microsoft(Microsoft)	Web	TCP	172.170.10.135	60361	Local	VirtualInterface1	Default_LAN_Zone	23.58.14.31	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	14	1766	0.083	0.064	13	8889	0.059	0.230	221	40163	View Refresh Filter															
Default_RoutingDomain	Microsoft(Sign for Business (Formerly Microsoft Lync Online) (Office 365)(sync_online)	Web	TCP	172.170.10.135	59277	Local	VirtualInterface1	Default_LAN_Zone	13.107.3.128	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	21	2330	0.288	0.254	22	13247	0.299	1.641	74	18086	View Refresh Filter															
Default_RoutingDomain	Microsoft(Sign for Business (Formerly Microsoft Lync Online) (Office 365)(sync_online)	Web	TCP	172.170.10.135	62015	Local	VirtualInterface1	Default_LAN_Zone	52.114.74.44	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	18	5435	0.397	0.835	11	9605	0.211	1.475	32	7332	View Refresh Filter															
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	Web	TCP	172.170.10.135	60309	Local	VirtualInterface1	Default_LAN_Zone	13.107.6.168	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	56	8714	0.198	0.246	68	10772	0.240	0.432	283	31023	View Refresh Filter															
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	Web	TCP	172.170.10.135	60308	Local	VirtualInterface1	Default_LAN_Zone	13.107.138.9	443	Internet	Branch-Internet	Internet_Zone	ESTABLISHED	Yes	620	230709	2.116	6.735	700	386371	2.251	10.377	256	20467	View Refresh Filter															

- Strömungen

Flows Data														
LAN to WAN Flows														
Details	Routing Domain	Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Hit Count	Service Type	Service Name	Age (ms)	Packets	Bytes	PPS	Application
+	Optimize	172.147.100.146	52.98.65.178	57930	443	TCP	4	INTERNET	-	120979	3	156	0.000	outlook
+	Optimize	172.147.100.146	13.107.18.11	57931	443	TCP	15	INTERNET	-	26513	14	1683	0.018	outlook
+	Optimize	172.147.100.146	13.107.42.11	57891	443	TCP	20	INTERNET	-	8418	19	1903	0.036	outlook
+	Optimize	172.147.100.146	40.100.136.146	57926	443	TCP	14	INTERNET	-	730	13	2118	0.036	outlook
+	Optimize	172.147.100.146	40.97.229.82	57918	443	TCP	15	INTERNET	-	1229	14	2178	0.036	outlook
+	Optimize	172.147.100.146	52.98.65.178	57929	443	TCP	4	INTERNET	-	121224	3	156	0.000	outlook
+	Optimize	172.147.100.146	34.203.255.247	51236	443	TCP	5	INTERNET	-	599759	4	164	0.000	okta
+	Optimize	172.147.100.146	34.203.255.247	51237	443	TCP	4	INTERNET	-	592420	3	123	0.000	okta
+	Optimize	172.147.100.146	13.107.6.156	51298	443	TCP	29	INTERNET	-	42061	28	11416	0.018	office365_common
+	Optimize	172.147.100.146	20.190.140.51	57935	443	TCP	16	INTERNET	-	24735	15	4184	0.018	office365_common
+	Optimize	172.147.100.146	13.67.50.225	57897	443	TCP	3	INTERNET	-	2250	2	81	0.047	office365_common
+	Optimize	172.147.100.146	13.67.50.225	51228	443	TCP	4	INTERNET	-	603355	3	123	0.000	office365_common
+	Optimize	172.147.100.146	13.107.6.156	51255	443	TCP	249	INTERNET	-	377061	248	85307	0.000	office365_common
+	Optimize	172.147.100.146	52.109.124.84	57939	443	TCP	20	INTERNET	-	22933	19	4679	0.018	office365_common
+	Optimize	172.147.100.146	13.67.50.225	51346	443	TCP	3	INTERNET	-	5900	2	81	0.044	office365_common

- DNS-Statistiken

Dashboard	Monitoring	Configuration
Statistics	Monitoring > DNS	
Flows	DNS Statistics	
Routing Protocols	<input type="button" value="Refresh"/>	
Firewall	Proxy Statistics	
IKE/IPsec	Search:	
ICMP	Proxy Name	Application Name
Performance Reports	DNS_Proxy1	office365_optimize
QoS Reports	DNS_Proxy1	office365_allow
Usage Reports	DNS_Proxy1	office365_default
Availability Reports	DNS_Proxy1	Any
Appliance Reports	Showing 1 to 4 of 4 entries	
DHCP Server/Relay	Transparent Forwarder Statistics	
VRRP	Search:	
PPPoE	Application Name	DNS Service Name
DNS	office365_allow	Quad9
	office365_default	Quad9
	office365_optimize	Quad9
	Showing 1 to 3 of 3 entries	

- Anwendungs-Routenstatistiken

Monitoring > Statistics

Statistics

Show: Application Routes Enable Auto Refresh 5 seconds Clear Counters on Refresh Processing...

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 3 of 3 entries

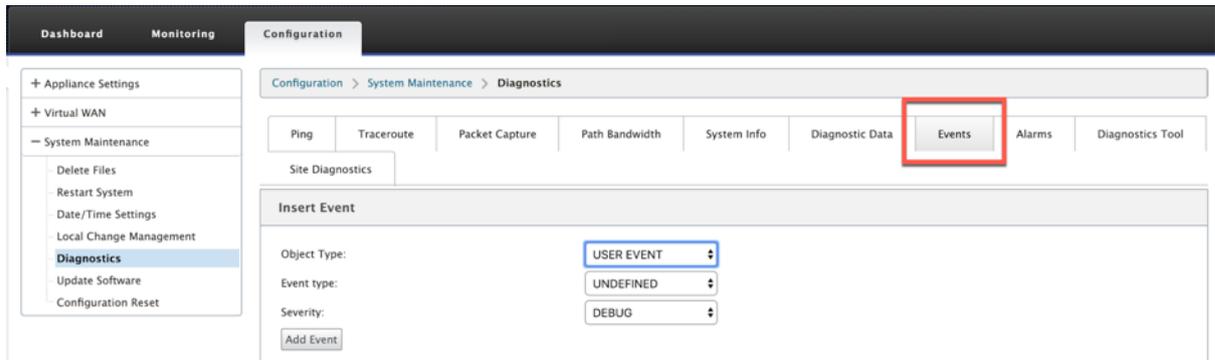
Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1792	YES	N/A	N/A
2	O365Allow_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1395	YES	N/A	N/A
1	O365Default_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A

Showing 1 to 3 of 3 entries

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

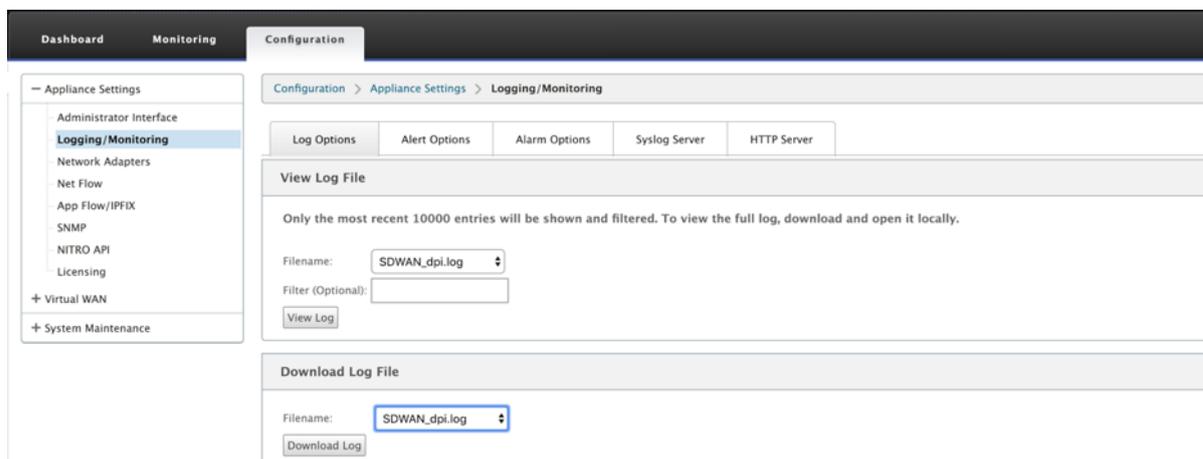
ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API

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 Anwendungsrouten 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

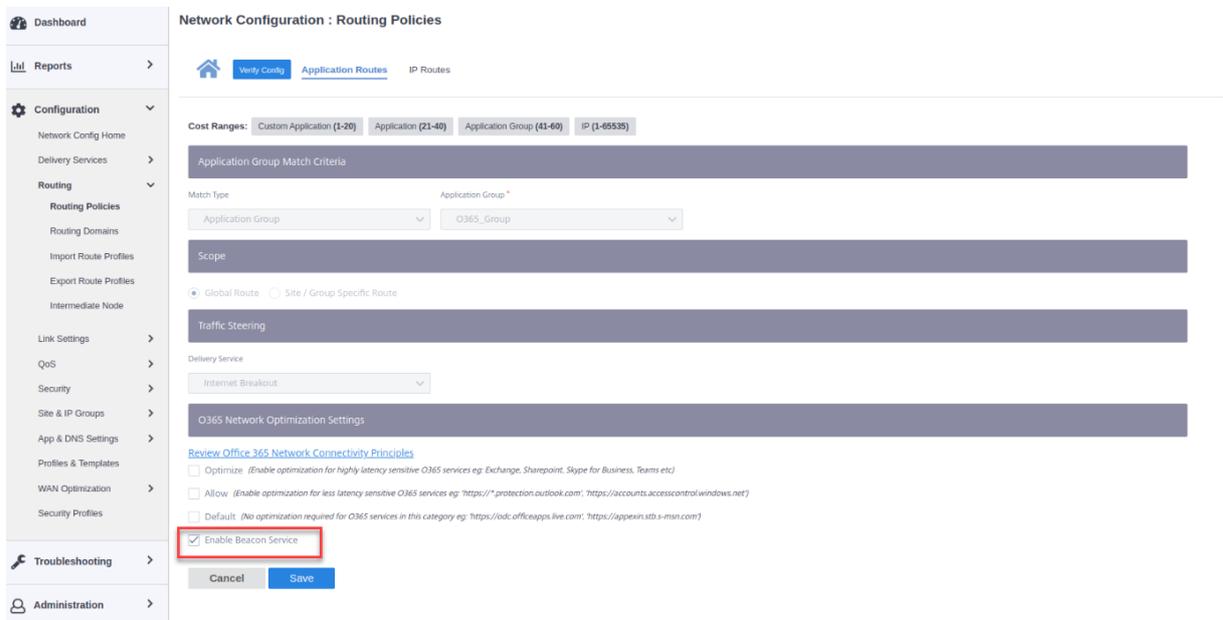
den Bericht zur Beacon-Service-Latenz anzeigen und den besten Internetlink für den direkten Office 365-Breakout manuell auswählen. Das Beacon-Sondieren ist nur über Citrix SD-WAN Orchestrator aktiviert. Standardmäßig ist das Beacon-Sondieren für alle internetfähigen WAN-Verbindungen aktiviert, wenn der Office 365-Ausbruch über Citrix SD-WAN Orchestrator aktiviert ist.

Hinweis

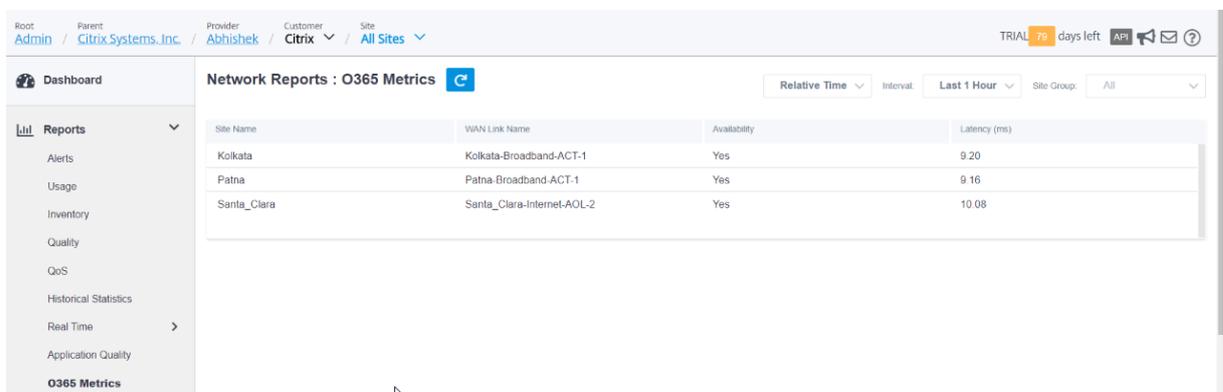
Office 365-Beacon-Probing ist für getaktete Links nicht aktiviert.

Sie können Office 365-Beacon-Probing deaktivieren und Latenzberichte im SD-WAN Orchestrator anzeigen. Weitere Informationen finden Sie unter [Office 365-Optimierung](#).

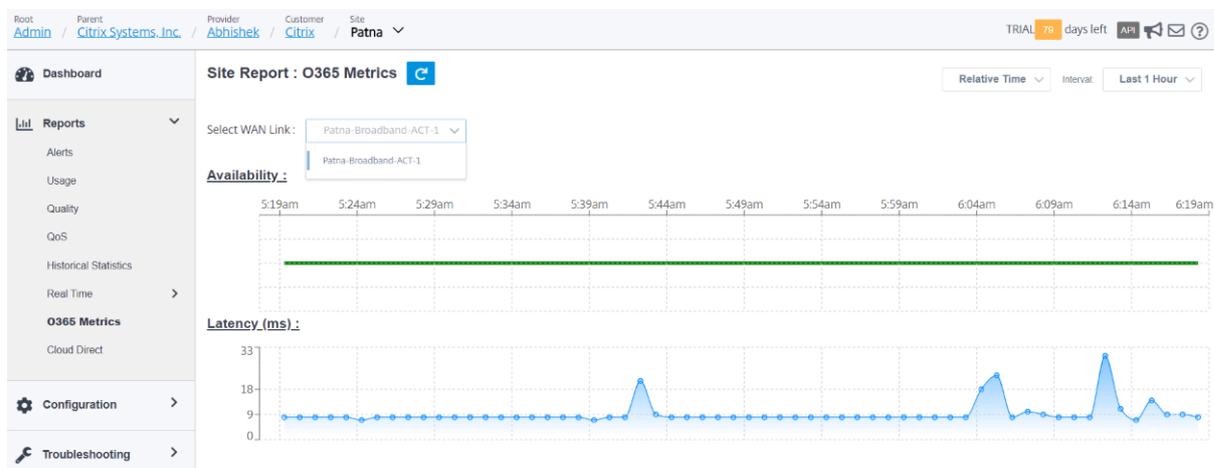
Um den Office 365 Beacon-Dienst zu deaktivieren, navigieren Sie in SD-WAN Orchestrator auf Netzwerkebene zu **Konfiguration > Routing > Routing-Richtlinien > O365 Network Optimization Settings** und deaktivieren **Sie Enable Beacon Service**.



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-Dienstverkehrs 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 Webproxymdatenverkehrs. 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

The first screenshot shows a table of connections with columns for Application, Family, IP Protocol, IP Address, Port, Service Type, Service Name, Zone, IP Address, Port, Service Type, Service Name, Zone, State, In NAT, Packets, Bytes, PPS, kbps, Packets, Bytes, PPS, kbps, Age (s), Last Activity (min), Related Objects, and Clear Connection. A red box highlights the entry for Citrix Gateway service Client Dataings, client_data.

The second screenshot shows a similar table with connections for Citrix Cloud Download Services and Domain Name Services. A red box highlights the entry for Citrix Gateway service Client Dataings, client_data.

- Strömungen

The screenshot shows the 'Flows Data' section with a table of flows. The table has columns for IP, Src, Dest, Service Name, Path, Rule ID, App Rule ID, Class, Class Type, Path, Hdr Compression Saved Bytes, Transmission Type, and Application. A red box highlights a flow for Citrix Gateway service Client Dataings, client_data.

- 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

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	7	YES	N/A	N/A
1	NGS_WebProxy_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A
2	NGS_ServerData_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	44	YES	N/A	N/A
3	NGS_ControlTraffic_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	72	YES	N/A	N/A
4	NGS_ClientData_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A
5	CitrixCloud_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A

Showing 1 to 6 of 6 entries

Application Route Statistics
Maximum allowed routes: 64000

Application Routes for routing domain: Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 2 of 2 entries

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	CitrixSdwanOrchestrator_Breakout	*	Internet	Internet_Zone	YES	BRANCH_KVMVPK	Static	50	35	YES	N/A	N/A
1	CitrixCloudDownloadSvc_Breakout	*	Internet	Internet_Zone	YES	BRANCH_KVMVPK	Static	50	8	YES	N/A	N/A

Showing 1 to 2 of 2 entries

Problembehandlung

Sie können den Dienstfehler im Abschnitt **Ereignisse** der SD-WAN-Appliance anzeigen.

Um die Fehler zu überprüfen, navigieren Sie zu **Konfiguration > Systemwartung > Diagnose**, und klicken Sie auf die Registerkarte **Ereignisse**.

The screenshot shows the 'Configuration' menu with 'System Maintenance > Diagnostics' selected. The 'Events' tab is highlighted with a red box. Below it, the 'Insert Event' form is visible, with 'Object Type' set to 'USER EVENT', 'Event type' set to 'UNDEFINED', and 'Severity' set to 'DEBUG'.

Wenn bei der Verbindung mit dem Citrix Dienst ein Problem auftritt (sdwan-app-routing.citrixnetworkapi.net), wird die Fehlermeldung in der Tabelle **Ereignisse anzeigen** angezeigt.

View Events

Quantity:

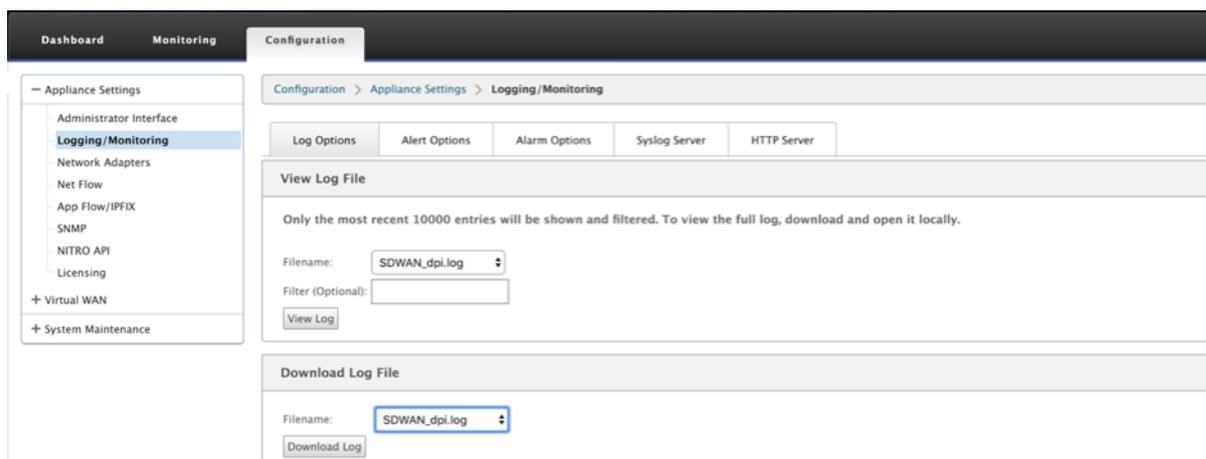
Filter: Object Type = APPLICATIONS Event type = FAILURE Severity = ERROR

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 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**.



PPPoE-Sitzungen

August 29, 2022

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 Internetdiensteanbietern (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 eine dynamische IP-Adresse oder verwendet eine statische IP-Adresse, um PPPoE-Verbindungen herzustellen.

Folgendes ist erforderlich, um erfolgreiche PPPoE-Sitzungen aufzubauen:

- 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:

Es dürfen mehrere VNIs mit demselben 802.1Q >VLAN-Tag erstellt werden.

Einschränkungen für die PPPoE-Konfiguration:

- 802.1q VLAN-Tagging wird nicht unterstützt.
- Die EAP-TLS-Authentifizierung wird nicht unterstützt.
- Adress-/Steuerungskomprimierung.
- Entleeren Sie die Kompression.
- Verhandlung über Protokoll-Feld-Komprimierung
- Protokoll zur Kompressionssteuerung.
- BSD Kompression komprimieren.
- IPX-Protokolle.
- PPP Multilink.
- TCP/IP-Header-Kompression im Van Jacobson-Stil.
- Verbindungs-ID-Komprimierungsoption bei der TCP/IP-Header-Komprimierung im Van Jacobson-Stil.
- 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.

Informationen zum Konfigurieren von PPPoE über den Citrix SD-WAN Orchestrator Service finden Sie unter [Schnittstellen](#).

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 über den Citrix SD-WAN Orchestrator Service zu starten und 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.

Virtual Interface	IP Address	Gateway IP	Session ID	State	Action
PORT2-VLAN0	192.168.1.22	192.168.1.254	18	Ready	Stop
abcd	0.0.0.0	0.0.0.0	0	Failed	Start
newVIF	0.0.0.0	0.0.0.0	0	Stopped	Start

In der Spalte **Status** wird der Status der PPPoE-Sitzung mit drei Farbcodes angezeigt: Grün, Rot, Gelb und Werte. In der folgenden Tabelle werden 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.

PPPoE-Sitzungstyp	Farbe	Beschreibung
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.
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).

PPPoE-Sitzungstyp	Farbe	Beschreibung
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.

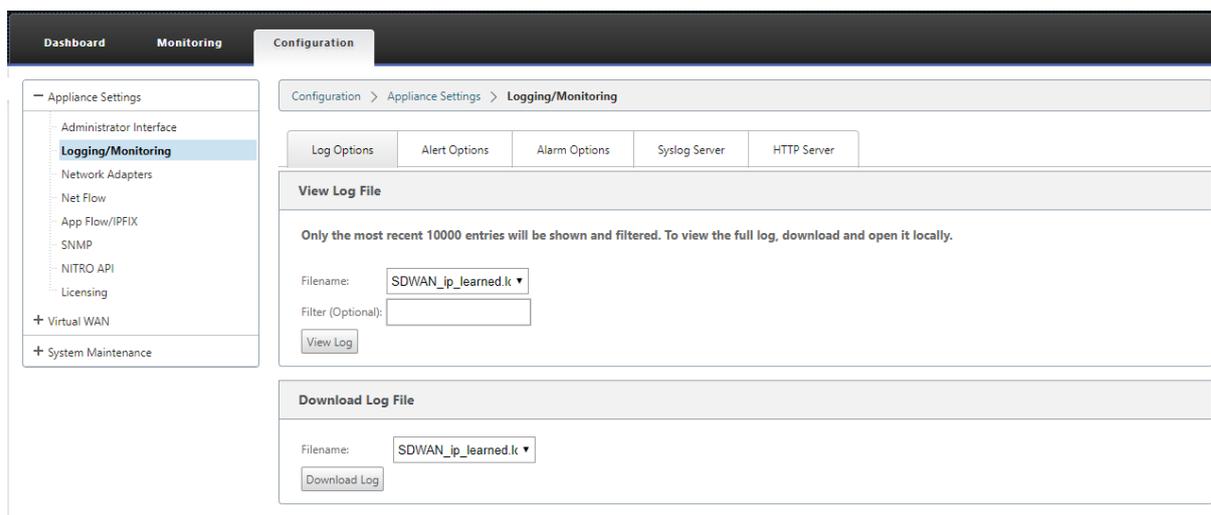
- Wenn der Fehler normal ist, wird er sofort neu gestartet.
- Wenn der Fehler ein Fehler ist, wird der Neustart für 10 Sekunden zurückgesetzt.
- Wenn der Fehler schwerwiegend ist, wird der Neustart vor dem Neustart für 30 Sekunden zurückgesetzt.

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

November 16, 2022

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.

Ab SD-WAN 11.5-Version können QoS-Funktionen über den Citrix SD-WAN Orchestrator Service konfiguriert werden. Weitere Informationen finden Sie unter [Servicequalität](#).

Klassen

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.

Der Citrix SD-WAN Orchestrator Service unterstützt 13 Klassen. Weitere Informationen finden Sie unter [Klassen](#).

Im Folgenden sind die verschiedenen Arten von Klassen:

- **Echtzeit:** Wird für geringe Latenz, geringe 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 interaktiven Datenverkehr mit niedrigen bis mittleren Latenzanforderungen und niedrigen bis mittleren Bandbreitenanforderungen verwendet. Die Interaktion erfolgt in der Regel zwischen einem Client und einem Server. Die Kommunikation benötigt möglicherweise keine hohe Bandbreite, ist aber empfindlich gegenüber Verlust und Latenz.
- **Bulk:** Wird für Traffic mit hoher Bandbreite und Anwendungen verwendet, die hohe Latenz tolerieren können. Anwendungen, die Dateiübertragung verarbeiten und eine hohe Bandbreite benötigen, werden als Massenkategorie kategorisiert. Diese Anwendungen beinhalten wenig menschliche Eingriffe und werden meist von den Systemen selbst behandelt.

Bandbreitenfreigabe zwischen Klassen

Bandbreite wird wie folgt von Klassen gemeinsam genutzt:

- **Echtzeit:** Traffic, der Echtzeitklassen trifft, hat garantiert eine geringe Latenz und die Bandbreite ist bei konkurrierenden Datenverkehr auf den Klassenanteil begrenzt.
- **Interaktiv:** Traffic, der die interaktiven Klassen trifft, erhält nach der Bereitstellung von Echtzeit-Datenverkehr die verbleibende Bandbreite, und die verfügbare Bandbreite wird fair unter den interaktiven Klassen geteilt.

- **Bulk:** Masse ist beste Anstrengung. Die Bandbreite, die nach der Bereitstellung von Echtzeit- und interaktivem Datenverkehr übrig bleibt, wird Massenklassen auf fairer Basis gegeben. Massenverkehr kann verhungern, wenn Echtzeit- und interaktiver Datenverkehr die gesamte verfügbare Bandbreite nutzt.

Hinweis

Jede Klasse kann die gesamte verfügbare Bandbreite verwenden, wenn kein Konflikt besteht.

Im folgenden Beispiel wird die Bandbreitenverteilung basierend auf der Klassenkonfiguration erläutert:

Betrachten Sie, dass eine aggregierte Bandbreite von 10 Mbit/s über virtuellen Pfad vorhanden ist. Wenn die Klassenkonfiguration

- Echtzeit: 30%
- Interaktives Hoch: 40%
- Interaktives Medium: 20%
- Interaktiv niedrig: 10%
- Bulk: 100%

Das Ergebnis der Bandbreitenverteilung ist:

- Der Echtzeitverkehr erhält je nach Bedarf 30% von 10 Mbit/s (3 Mbit/s). Wenn weniger als 10% benötigt werden, wird der Rest der Bandbreite den anderen Klassen zur Verfügung gestellt.
- Interaktive Klassen teilen sich die verbleibende Bandbreite auf Fair Share-Basis (4 Mbit/s: 2 Mbit/s: 1 Mbit/s).
- Alles, was übrig ist, wenn interaktiver Echtzeit-Verkehr seinen Anteil nicht vollständig nutzt, wird der Bulk-Klasse übergeben.

Regeln nach IP-Adresse und Portnummer

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.

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.

Ab Version Citrix SD-WAN 11.5 können Sie IP-Regeln mit dem Citrix SD-WAN Orchestrator Service erstellen. Weitere Informationen finden Sie unter [IP-Regeln](#).

Regeln überprüfen

Navigieren Sie 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**.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Flows Data

Both LAN to WAN and WAN to LAN Flows

Details	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
<input checked="" type="checkbox"/>	172.186.30.74	172.186.10.89	LAN to WAN	55502	5003	TCP	default	88311	Virtual Path	DC-Client-1	LOCAL	0	88251	126636068	7558.028	86763.328	3446.461	0.000	1	N/A	9	BULK	DC-WL-1->Client-1-WL-1	N/A	Persistent	iperf
<input checked="" type="checkbox"/>	172.186.10.89	172.186.30.74	WAN to LAN	5003	55502	TCP	default	45207	Virtual Path	DC-Client-1	LOCAL	1	45207	2385488	3871.667	1634.405	1765.480	0.000	69	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Total LAN to WAN flows displayed: 1 out of 1
Total WAN to LAN flows displayed: 1 out of 1

Navigieren Sie zu **Überwachung > Statistik**, und überprüfen Sie die konfigurierten Regeln.

Monitoring > Statistics

Statistics

Show: **Rules** Enable Auto Refresh **5** seconds

Rule Statistics

Filter: in **Any column**

Show **100** entries Showing 1 to 100 of 275 entries

Num#	Site	Service	IP Address		IP Proto	Port			LAN to WAN		WAN to LAN														
			Src	Dst		Src	Dst	VLAN ID	IP DSCP	Bytes	Packets	Bytes	Packets	Jitter (ms)	Packets Lost	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)							
0	DC	DC-Client-1	*	*	TCP	5003	*	*	*	0	0	0	0												
1	DC	DC-Client-1	*	*	TCP	*	5003	*	*	426121168	285604	0	0												
2	DC	DC-Client-1	*	*	TCP	5060-5061	*	*	ef	0	0	0	0												
3	DC	DC-Client-1	*	*	TCP	*	5060-5061	*	ef	0	0	0	0												
4	DC	DC-Client-1	*	*	UDP	5060-5061	*	*	ef	0	0	0	0												
5	DC	DC-Client-1	*	*	UDP	*	5060-5061	*	ef	0	0	0	0												

Regeln nach Anwendungsname

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 Datenverkehrsflüsse basierend auf Übereinstimmungstypen von Anwendungen, Anwendungsfamilien oder Anwendungsobjekten filtern und Anwendungsregeln auf sie anwenden. Die Anwendungsregeln ähneln 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	Aktivieren Sie Pakettaggen	Neusequenzieren	Haltezeit (ms)	Wiederholung von Paketen	Drop-Limit (ms)	Drop-Tiefe (Byte)	RED aktivieren	Deaktivieren Sie Limit (ms)	Deaktivieren Sie Tiefe (Byte)
HDX_Priority_0	Priority_0	Lastausgleich	True	True	True	250	True	350	30000	True	0	128000
	(HDX_priority_tag_0)											
HDX_Priority_1	Priority_1	Lastausgleich	True	True	True	250	True	350	30000	True	0	128000
	(HDX_priority_tag_1)											

Regel	Klasse	Übertragungsmodus	Übertragen Sie verlorene Pakete	Übertragungsmodus	Übertragen Sie verlorene Pakete	Aktivieren Sie	Neu von	Sequenznummer	Drop-Limit (ms)	Drop-Tiefe (Byte)	RED aktivieren	Deaktivieren Sie Limit (ms)	Deaktivieren Sie Tiefe (Byte)
HDX_Priority_2	11	Lastausgleich	True	False	True	250	True	350	30000	True	0	128000	
(HDX_priority_tag_2)													
HDX_Priority_3	11	Lastausgleich	True	False	True	250	True	350	30000	True	0	128000	
(HDX_priority_tag_3)													
HDX	11	Lastausgleich	True	False	True	250	True	350	30000	True	0	128000	
(inter-active_high_class)													

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.

Informationen zum Erstellen von Anwendungsregeln mit Citrix SD-WAN Orchestrator finden Sie unter [Anwendungsregeln](#).

Um zu bestätigen, ob Anwendungsregeln auf den Verkehrsfluss angewendet werden, navigieren Sie zu **Überwachung > Flows**.

Notieren Sie sich die App-Regelkennung und überprüfen Sie, ob der Klassentyp und der Übertragungsmodus gemäß Ihrer Regelkonfiguration sind.

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPF	IP DSCP	HR Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
172.168.30.74	172.168.10.89	LAN to WAN	35118	5001	UDP	default	4961	Virtual Path	DC-Clients-1	LOCAL	0	4959	7428562	292.687	3507.565	126.441	0.000	45	0	11	INTERACTIVE	DC-WL-1->Client-1-WL-1	N/A	Duplicate

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.

Num	Site	Service	IP Address			Application Object	Application	Family	LAN to WAN		WAN to LAN		Dropped		Last Hit (DHHMM ago)
			Src	Dst	Port				Bytes	Packets	Bytes	Packets	Bytes	Packets	
0	DC	DC-Clients-1	*	*	*	*	iperf	*	26325792	32262	0	0	287616	192	00:00
1	DC	DC-Clients-1	*	*	*	*	ica_priority_0	*	0	0	0	0	0	0	
2	DC	DC-Clients-1	*	*	*	*	ica_priority_1	*	0	0	0	0	0	0	
3	DC	DC-Clients-1	*	*	*	*	ica_priority_2	*	0	0	0	0	0	0	
4	DC	DC-Clients-1	*	*	*	*	ica_priority_3	*	0	0	0	0	0	0	
5	DC	DC-Clients-1	*	*	*	*	ica	*	0	0	0	0	0	0	
6	Clients-1	DC-Clients-1	*	*	*	*	iperf	*	0	0	4710	5	1484	1	00:38

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.

Anwendungsklassifizierung

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)
- Domännennamenbasierte 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.

Informationen zum Aktivieren der DPI-Bibliotheksklassifizierung im Citrix SD-WAN Orchestrator Service finden Sie unter [Klassifizierung der DPI-Bibliothek](#).

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 von ICA-Datenverkehr, der über SSL/TLS oder DTLS bereitgestellt wird, wird in SD-WAN Standard Edition nicht 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 Multistream-ICA-Funktionalität ordnungsgemäß funktioniert, müssen Sie über SD-WAN Standard Edition 10.1 oder höher verfügen.
- Damit benutzerbasierte HDX-Berichte im SDWAN-Center angezeigt werden, müssen Sie über SD-WAN Standard Edition 11.0 oder höher verfügen.

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 Insights](#) an.
- Ab Version 11.2 ist die Paketduplizierung jetzt standardmäßig für HDX-Echtzeitverkehr aktiviert, wenn Multistream-ICA verwendet wird.

Nach der Klassifizierung kann die ICA-Anwendung in Anwendungsregeln und zum Anzeigen von Anwendungsstatistiken ähnlich wie bei anderen klassifizierten Anwendungen verwendet werden.

Es gibt fünf Standardanwendungsregeln für ICA-Anwendungen jeweils eine für die folgenden Prioritäts-Tags:

- Unabhängige Datenverarbeitungsarchitektur (Citrix) (ICA)
- ICA Echtzeit (ica_priority_0)
- ICA Interaktiv (ica_priority_1)
- ICA Bulk-Transfer (ica_priority_2)
- ICA-Hintergrund (ica_priority_3)

Weitere Informationen finden Sie unter [Regeln nach Anwendungsname](#)

Wenn Sie eine Kombination von Software ausführen, die Multi-Stream-ICA nicht über einen einzigen

Port unterstützt, müssen Sie zum Ausführen von QoS mehrere Ports konfigurieren, einen für jeden ICA-Stream.

Um HDX auf nicht standardmäßigen Ports wie in der XA/XD-Serverrichtlinie konfiguriert zu klassifizieren, müssen Sie diese Ports in ICA-Portkonfigurationen hinzufügen. Um den Datenverkehr an diesen Ports mit gültigen IP-Regeln abzugleichen, müssen Sie außerdem die ICA-IP-Regeln aktualisieren.

In der ICA-IP- und Portliste können Sie nicht standardmäßige Ports angeben, die in der XA/XD-Richtlinie für die HDX-Klassifizierung verwendet werden. IP-Adresse wird verwendet, um die Ports weiter auf ein bestimmtes Ziel zu beschränken. Verwenden Sie '*' für den Port, der für eine beliebige IP-Adresse bestimmt ist. IP-Adresse mit Kombination aus SSL-Port wird auch verwendet, um anzuzeigen, dass der Datenverkehr wahrscheinlich ICA ist, obwohl der Datenverkehr nicht endgültig 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.

Informationen zum Aktivieren der ICA-basierten Klassifizierung für den Citrix SD-WAN Orchestrator Service finden Sie unter [ICA-Klassifizierung](#).

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](#).

Domännennamenbasierte Anwendungsklassifizierung

Die DPI-Klassifikations-Engine wurde erweitert, um Anwendungen basierend auf dem Domännennamen und -mustern zu klassifizieren. Nachdem der DNS-Weiterleitung 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 Domännennamen basierende Anwendungs-ID wird angehängt.

Mit der auf Domännennamen 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 Domännennamen basierende Anwendungen können konfiguriert werden.

Informationen zum Definieren von auf Domännennamen basierenden Anwendungen im Citrix SD-WAN Orchestrator Service finden Sie unter [Domännennamen basierte Anwendungsklassifizierung](#).

Hinweis

- Ab Version 11.4.2 unterstützen die auf Domännennamen basierenden Anwendungen konfigurierbare Ports und Protokolle im Citrix SD-WAN Orchestrator Service. Weitere Informationen finden Sie unter [Domänen und Anwendungen](#).
- Ab der Version Citrix SD-WAN 11.5.0 werden AAAA-Datensätze im Citrix SD-WAN Orchestrator Service unterstützt.

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 Domännennamenmuster 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.
- 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 Dienstypen 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 in den Datenflüssen nach binären Mustern, z. B. sucht die DPI-Engine bei Skype nach einem binären Muster innerhalb des Zertifikats und bestimmt die Anwendung.

Anwendungsobjekte

Anwendungsobjekte ermöglichen es Ihnen, verschiedene Arten von Übereinstimmungskriterien in einem einzigen Objekt zu gruppieren, das für Firewall-Richtlinien und Anwendungssteuerung verwendet werden kann. IP-Protokoll, Anwendung und Anwendungsfamilie sind die verfügbaren Übereinstimmungstypen.

Die folgenden Funktionen verwenden das Anwendungsobjekt als Übereinstimmungstyp:

- [Anwendungsrouten](#)
- [Firewall-Richtlinie](#)
- [QoS-Regeln für Anwendungen](#)
- [Anwendung QoE](#)

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](#).

Edit Firewall Policy ? x

Priority:

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action: Log Interval (s): Log Start Log End Connection State Tracking:

Match Type: Application Objects: Application: Application Family:

Allow Fragments Reverse Also Match Established

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

→

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 zu **Überwachung > Firewall**. Im Abschnitt **Verbindungen** werden in den Spalten **Anwendung** und **Familie** die Anwendungen und die zugehörige Familie aufgeführt.

Firewall Statistics

Statistics: **Connections**
 Maximum entries to display: 50

Filtering: Application: Any, Family: Any, IP Protocol: Any, Source Zone: Any, Destination Zone: Any, Source Service Type: Any, Source Service Instance: Any, Destination Service Type: Any, Destination Service Instance: Any, Source IP: , Source Port: , Destination IP: , Destination Port:

Connections

Application	Family	IP Protocol	Source					Destination					Sent					
			IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps
CoToMeeting Online Meeting(gotomeeting)	Audio/Video	TCP	172.16.30.30	54612	Local	Site1_VL1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	4	259	0.716	0.371
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	47397	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	1	60	0.262	0.126
Network Time Protocol(ntp)	Network Service	UDP	172.16.30.30	48743	Local	Site1_VL1	Default_LAN_Zone	91.189.94.4	123	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	NEW	No	1	76	0.264	0.160
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	41348	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	118	0.476	0.225
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44961	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	114	0.513	0.234
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44119	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	1	60	0.263	0.126
Google Generic(google_gen)	Web	TCP	172.16.30.30	45706	Local	Site1_VL1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	394	1.017	0.534
BING	Custom Application	TCP	172.16.30.30	45464	Local	Site1_VL1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	31	1348	6.428	2.236
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	59856	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	116	0.410	0.190
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	49607	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	122	0.354	0.173
Mozilla.com - Mozilla.org(mozilla)	Web	TCP	172.16.30.30	46324	Local	Site1_VL1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	395	1.551	0.817
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	52889	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	112	0.332	0.149
Microsoft(microsoft)	Web	TCP	172.16.30.30	51194	Local	Site1_VL1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	397	1.433	0.758

Connections Displayed: 13
 Connections in Use: 13/128000

Wenn Sie die Anwendungsklassifizierung nicht aktivieren, zeigen die Spalten **Anwendung** und **Familie** keine Daten an.

Firewall Statistics

Statistics: **Connections**
 Maximum entries to display: 50

Filtering: Application: Any, Family: Any, IP Protocol: Any, Source Zone: Any, Destination Zone: Any, Source Service Type: Any, Source Service Instance: Any, Destination Service Type: Any, Destination Service Instance: Any, Source IP: , Source Port: , Destination IP: , Destination Port:

Connections

Application	Family	IP Protocol	Source					Destination					Sent				Received					
			IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps
*	*	TCP	172.16.30.30	54632	Local	Site1_VL1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	4	259	0.909	0.471	3	217	0.682	0.395
*	*	UDP	172.16.30.30	41664	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	112	0.383	0.171	2	156	0.383	0.239
*	*	UDP	172.16.30.30	36817	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	122	0.408	0.199	2	196	0.408	0.320
*	*	TCP	172.16.30.30	45726	Local	Site1_VL1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	394	1.207	0.634	4	744	0.804	1.197
*	*	TCP	172.16.30.30	45484	Local	Site1_VL1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	26	1136	6.780	2.370	53	63972	13.820	133.449
*	*	UDP	172.16.30.30	53904	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	118	0.589	0.278	2	272	0.589	0.641
*	*	UDP	172.16.30.30	49809	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	116	0.513	0.238	2	354	0.513	0.727
*	*	TCP	172.16.30.30	51214	Local	Site1_VL1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	397	1.796	0.951	4	361	1.197	0.864
*	*	TCP	172.16.30.30	46344	Local	Site1_VL1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	395	1.904	1.003	4	387	1.269	0.982
*	*	UDP	172.16.30.30	52627	Local	Site1_VL1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	114	0.622	0.283	2	210	0.622	0.522

Connections Displayed: 10
 Connections in Use: 10/128000

Informationen zu Flows Navigieren Sie zu **Monitoring > Flows**. Im Abschnitt **“Flows Data“** werden in der Spalte **“Anwendung“** die Anwendungsdetails aufgeführt.

Monitoring > Flows

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): Help

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6979	2	112	0.287	0.128	0.131	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4967	2	118	0.403	0.190	0.184	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	28	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4963	27	1176	4.950	1.725	2.257	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	bing
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4811	2	114	0.416	0.190	0.190	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	5	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5715	4	259	0.644	0.334	0.294	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	gotomeeting
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6717	2	122	0.298	0.145	0.136	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6692	6	394	0.876	0.460	0.399	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	google_gen
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4016	6	395	1.254	0.660	0.572	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	mozilla
P default	3	INTERNET	-	LOCAL	5711	2	116	0.350	0.162	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4775	6	397	1.222	0.647	0.557	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	microsoft
P default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6883	2	156	0.288	0.180	0.131	0.000	117	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4936	2	272	0.403	0.439	0.184	0.000	117	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P default	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4969	53	64273	9.730	94.396	4.437	0.000	94	N/A	N/A	N/A	N/A	N/A	N/A	bing
P cs4	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4804	2	210	0.416	0.350	0.190	0.000	117	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Total LAN to WAN flows displayed: 10 out of 10
Total WAN to LAN flows displayed: 10 out of 10

Anwendungsstatistiken Navigieren Sie zu **Überwachung > Statistik**. 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 (RED)

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 der 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 Hierarchical Fair Service Curve (HFSC) -Algorithmus, 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.

Informationen zur Verwendung und Aktivierung von RED finden Sie unter [How to use RED](#).

MPLS-Warteschlangen

Diese Funktion vereinfacht das Erstellen von SD-WAN-Konfigurationen beim Hinzufügen einer Multi-protocol 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. Informationen zum Konfigurieren von MPLS mit dem Citrix SD-WAN Orchestrator Service finden Sie unter [MPLS-Warteschlangen](#).

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.

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, Benutzeranfrage 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.

The screenshot shows the 'Monitoring > Statistics' page. Under the 'Statistics' section, 'WAN Link' is selected in the 'Show' dropdown. The 'Enable Auto Refresh' checkbox is checked, set to 5 seconds. Below this, the 'WAN Link Statistics' section is visible, showing a table with 6 entries. The table has columns: WAN Link, Access Interface, IP Address, Proxy Address, Proxy ARP State, MAC, and Last ARP Reply Age (ms). The 'Proxy ARP State' column shows 'DISABLED' for two entries. Below this, the 'Virtual Path Service Data Rates' section is visible, showing a table with 4 entries. The table has columns: Name, Direction, Virtual Path Service Packets, Virtual Path Service kB, Delta Virtual Path Service Packets, Delta Virtual Path Service kB, Virtual Path Service kbps, and IP,TCP,UDP Header Compression Bytes Saved.

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
Client-1-WL-1	N/A	172.186.10.75	N/A	N/A	N/A	N/A
Client-1-WL-2	N/A	172.186.20.75	N/A	N/A	N/A	N/A
Client-2-WL-1	N/A	172.186.70.50	N/A	N/A	N/A	N/A
Client-2-WL-2	N/A	172.186.80.50	N/A	N/A	N/A	N/A
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	DISABLED	N/A	N/A
DC-WL-2	DC-WL-2-AI-1	172.186.40.85	N/A	DISABLED	N/A	N/A

Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved
DC-WL-1	Recv	2618687	195069.42	289	26.16	37.81	0

Gehen Sie zu **Monitor > Statistiken** und wählen Sie in der Dropdownliste **Anzeigen** die Option **WAN-Link-Nutzung** aus.

Statistics

Show: WAN Link Usage Enable Auto Refresh 5 seconds Show latest data Processing...

WAN Link Usage Statistics

Local WAN Links

Filter: in Any column

Show: 100 entries Showing 1 to 6 of 6 entries

WAN Link	Direction	Packets	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
DC-WG-1	Send	2507622	238	17.69	28.24	100000	N/A
DC-WG-1	Recv	2630429	240	21.87	35.38	80000	NO
q1	Send	2358231	372	20.84	33.77	50000	N/A
q1	Recv	2366461	308	18.26	29.74	49000	NO
q2	Send	118164	308	18.32	28.77	50000	N/A
q2	Recv	128766	321	19.88	32.21	49000	NO

Showing 1 to 6 of 6 entries

Usage and Permitted Rates

Filter: in Any column

Show: 100 entries Showing 1 to 14 of 14 entries

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
DC-WG-1	DC-Client-1	Recv	1473996	134885.42	118	10.8	16.99	24491.95	NO
DC-WG-1	DC-Client-2	Recv	958409	71407.76	138	12.12	19.07	24490	NO
DC-WG-1	DC-Client-1	Send	1623618	1080116.24	134	10.34	16.27	24990	N/A
DC-WG-1	DC-Client-2	Send	892096	647710.56	132	9.47	14.9	24990	N/A
DC-WG-1	Internet-Intranet	Send	0	0	0	0	0	50020	N/A
DC-WG-1	Internet-Intranet	Recv	208	35.25	0	0	0	49020	N/A
q1	DC-Client-1	Recv	1337987	96716.01	208	11.12	17.31	24510	NO
q1	DC-Client-2	Recv	821873	52380.57	126	7.4	11.64	24990	NO
q1	DC-Client-1	Send	1314280	973091.68	210	10.51	21.26	25010	N/A
q1	DC-Client-2	Send	847803	572910.06	129	7.53	11.88	24990	N/A
q2	DC-Client-1	Recv	91058	6290.83	237	15.83	24.94	24510	NO
q2	DC-Client-2	Recv	40378	2232.83	124	5.58	8.75	24990	NO
q2	DC-Client-1	Send	81298	47107.84	208	11.12	17.31	25010	N/A
q2	DC-Client-2	Send	40353	22717.00	125	5.81	8.83	24990	N/A

Showing 1 to 14 of 14 entries

Remote WAN Links

Filter: in Any column

Show: 100 entries Showing 1 to 6 of 6 entries

WAN Link	Service	Direction	Congestion
Client-1-WG-1	DC-Client-1	Recv	NO
Client-2-WG-1	DC-Client-2	Recv	NO
q3	DC-Client-1	Recv	NO
q4	DC-Client-1	Recv	NO
q5	DC-Client-2	Recv	NO
q6	DC-Client-2	Recv	NO

Showing 1 to 6 of 6 entries

MPLS-Warteschlangen überwachen

Gehen Sie zu **Überwachen Statistiken** und wählen Sie in der Dropdownliste **Anzeigen** die Option **MPLS-Warteschlangen** aus.

Show: **MPLS Queues** Enable Auto Refresh **5** seconds Show latest data.

MPLS Queue Statistics

Filter: in **Any column**

Show **100** entries Showing 1 to 4 of 4 entries Processing...

Private MPLS	MPLS Queue	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
EE-Branch1-WL-2	SAMPLE-Queue1	EE-Branch1-WL-2-AI-1	172.184.19.19	N/A	DISABLED	N/A	N/A
EE-Branch1-WL-2	SAMPLE-Queue2	EE-Branch1-WL-2-AI-1	172.184.19.19	N/A	DISABLED	N/A	N/A
VPX-DC-WL-2	DC-Queue01	N/A	172.184.3.19	172.184.3.19	N/A	N/A	N/A
VPX-DC-WL-2	DC-Queue2	N/A	172.184.3.19	172.184.3.19	N/A	N/A	N/A

Showing 1 to 4 of 4 entries

Virtual Path Service Data Rates

Filter: in **Any column**

Show **100** entries Showing 1 to 4 of 4 entries

Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	Mismatched DSCP Packets	Mismatched DSCP kB	IP/TCP/UDP Header Compression Bytes Saved
SAMPLE-Queue1	Recv	14279	1177.77	251	20.72	33.15	5932	407.36	0
SAMPLE-Queue1	Send	13400	919.09	217	14.47	23.15	N/A	N/A	0
SAMPLE-Queue2	Recv	12806	705.61	216	11.84	18.95	5803	250.8	0
SAMPLE-Queue2	Send	13953	915.39	241	16.73	26.77	N/A	N/A	0

Showing 1 to 4 of 4 entries

Problembehandlung bei MPLS-Warteschlangen

Um den Status von MPLS-Warteschlangen zu überprüfen, navigieren Sie zu **Überwachen > Statistiken** und wählen Sie in der 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.

Statistics										
Show: Paths (Summary) <input checked="" type="checkbox"/> Enable Auto Refresh 5 seconds <input type="button" value="Stop"/> <input checked="" type="checkbox"/> Show latest data. Processing...										
Path Statistics Summary										
Filter: <input type="text"/> in Any column <input type="button" value="Apply"/> Show 100 entries										
Num [▲]	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
5	q2	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
6	Client-1-WL-1	DC-WL-1	GOOD	GOOD	Static	4	2	0.00	19.96	NO
7	q3	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
8	q3	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
9	q4	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
10	q4	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
11	DC-WL-1	Client-2-WL-1	GOOD	GOOD	Static	2	2	0.00	15.12	NO
12	q1	q5	GOOD	GOOD	Static	2	2	0.00	11.53	NO
13	q2	q6	GOOD	GOOD	Static	2	2	0.00	8.51	NO
14	Client-2-WL-1	DC-WL-1	GOOD	GOOD	Static	2	2	0.00	20.09	NO
15	q5	q1	GOOD	GOOD	Static	2	2	0.00	11.69	NO
16	q6	q2	GOOD	GOOD	Static	2	2	0.00	8.82	NO

Um detaillierte Informationen zu Pfaden zu erhalten, wählen Sie **Pfade (Detailliert)** aus der 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 Show latest data. Processing...

Path Statistics Advanced

Filter: in Any column

Show 100 entries Showing 1 to 16 of 16 entries 1

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 Show latest data. Processing...

Access Interface Statistics

Filter: in Any column

Show 100 entries Showing 1 to 3 of 3 entries 1

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 1

Virtual Path Service Data Rates

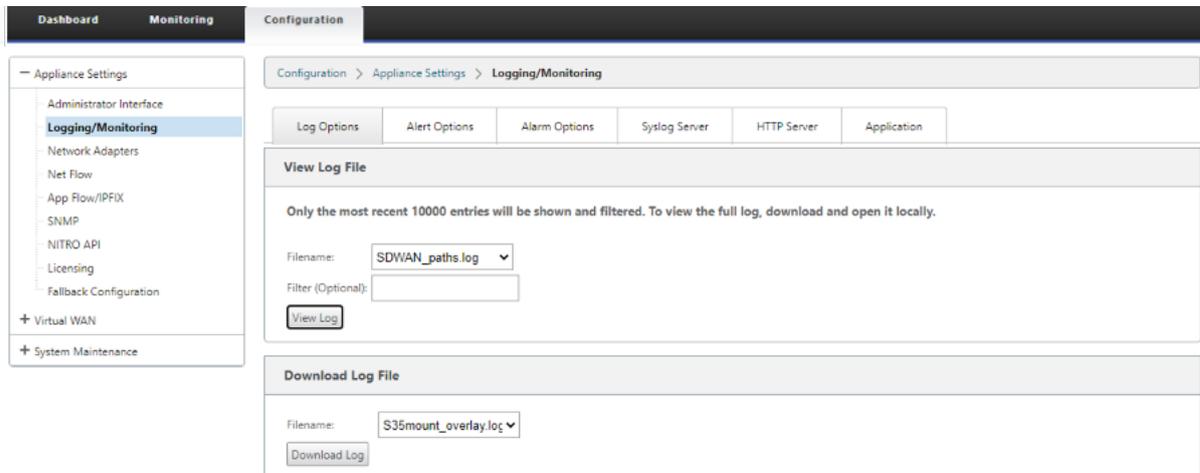
Filter: in Any column

Show 100 entries Showing 1 to 12 of 12 entries 1

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

November 16, 2022

Anwendung QoE

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

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 und bis zu 10 Anwendungen oder Anwendungsobjekte QoE-Profilen zuordnen.

Informationen zum Erstellen benutzerdefinierter QoE-Profile über den Citrix SD-WAN Orchestrator Service finden Sie unter [Anwendungs-QoE-Profile](#).

HDX QoE

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 zum Konfigurieren von HDX QoE mit dem Citrix SD-WAN Orchestrator Service 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.*

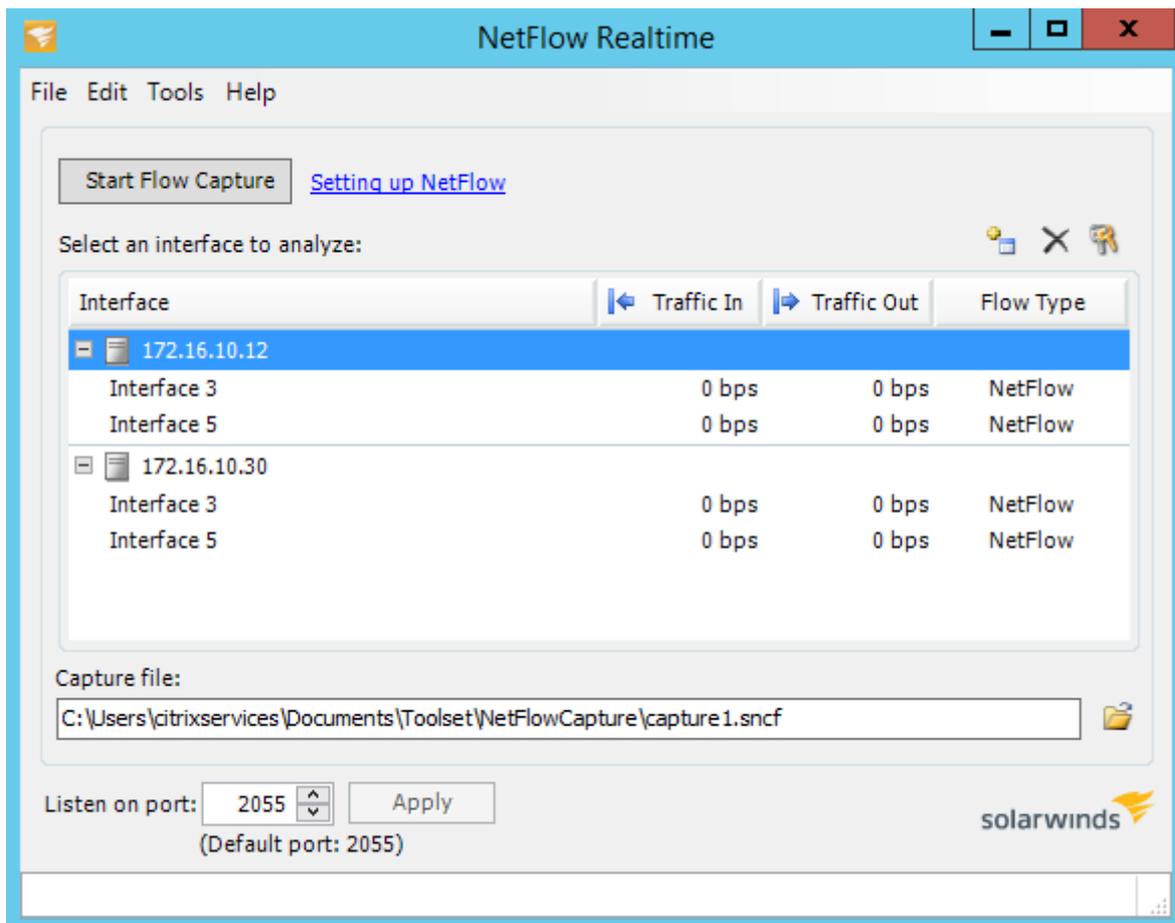
Mehrere Net Flow Kollektoren

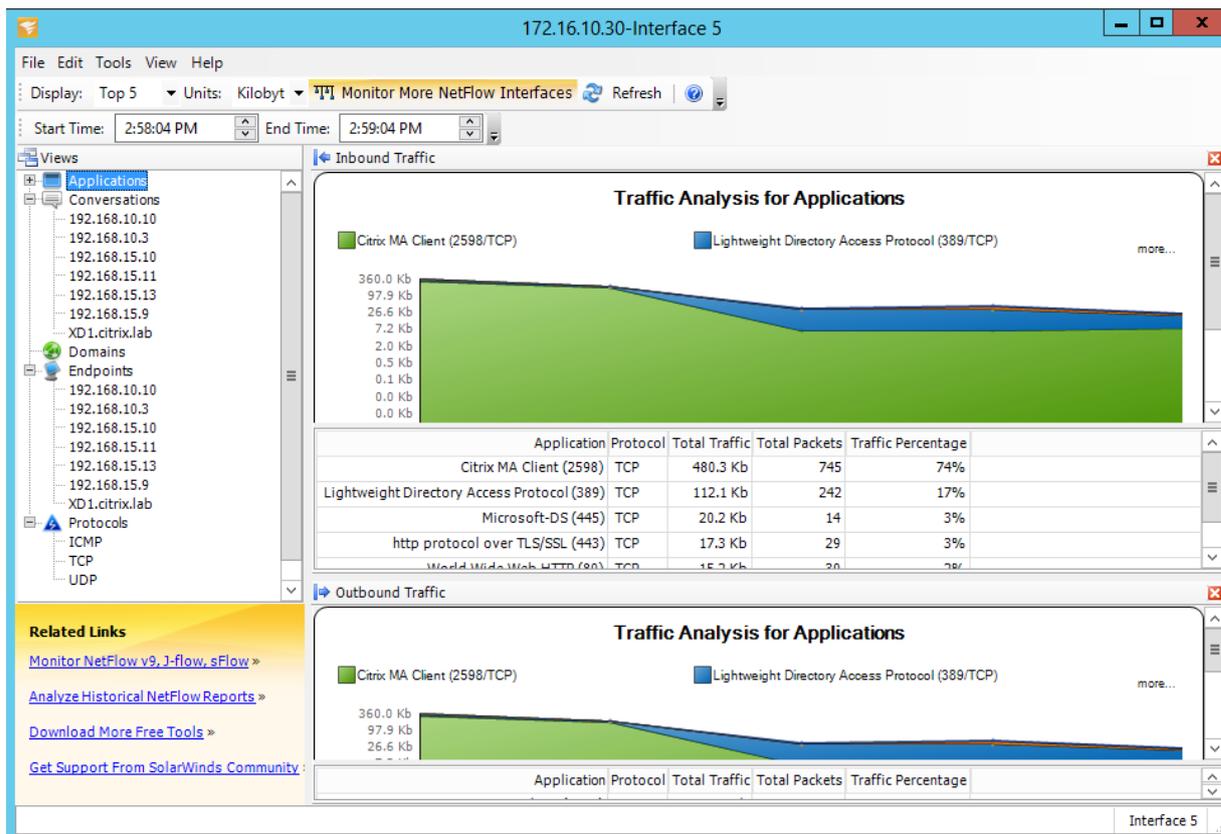
Net Flow Collectors erfassen IP-Netzwerkverkehr, wenn er in eine SD-WAN-Schnittstelle eintritt oder diese verlässt. Durch die Analyse der von Net Flow bereitgestellten Daten können Sie die Quelle und das Ziel des Datenverkehrs, die Serviceklasse und die Ursachen für Verkehrsstaus ermitteln. Citrix SD-WAN-Geräte 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 Edition-Appliances unterstützt.

Informationen zum Konfigurieren von Net Flow Hosts mit dem Citrix SD-WAN Orchestrator Service finden Sie unter [Netflow-Hosteinstellungen](#).

NetFlow-Export

Net Flow-Daten werden vom SD-WAN-Geräteverwaltungspoint 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. Weitere Informationen finden Sie unter [SNMP](#).





NetFlow-Einschränkungen

- Wenn Netflow auf SD-WAN Standard Edition-Appliances aktiviert ist, werden Virtual Path-Daten an die angegebenen Netflow-Sammler gestreamt. Eine Einschränkung besteht darin, dass man nicht unterscheiden kann, welche physische WAN-Verbindung von SD-WAN verwendet wird, da die Lösung aggregierte Virtual Path Informationen meldet (Ein virtueller Pfad kann aus mehreren unterschiedlichen WAN-Pfaden bestehen), gibt es keine Möglichkeit, die Netflow-Datensätze nach den unterschiedlichen WAN-Pfaden zu filtern.
- TCP-Steuerungsbits melden sich als N/A, was darauf hinweist, dass SD-WAN nicht dem Internetstandard für Netflow-Exporte folgt, der auf [RFC 7011](#) basiert und die Element-ID 6 für TcpControl-Bits (IANA) hat. Ohne TCP-Flags ist die Berechnung der Roundtrip-Zeit (RTT), Latenz, Jitter und anderer Leistungsmetriken in den Flussdaten nicht möglich. Auf der Sicherheitsseite kann der Net Flow-Collector ohne TCP-Flags nicht feststellen, ob FIN, ACK/RST oder SYN-Scans auftreten.

Routenstatistik

Um Routenstatistiken Ihrer SD-WAN-Appliances anzuzeigen, navigieren Sie in der SD-WAN-GUI zu **Überwachung > Statistiken > Routen**.

Details#	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
	0	172.186.30.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	55365	YES	N/A	N/A
	1	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
	2	172.186.50.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11	YES	N/A	N/A
	3	172.186.10.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	27912	YES	N/A	N/A
Site Path:		Client-1														
Optimal Route:		NO														
Summarized / Summary Route:		NO/NO														
	4	172.186.20.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
	5	172.186.10.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
	6	172.186.20.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
	7	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	DC	Static	-	-	5	20	YES	N/A	N/A
	8	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	238	YES	N/A	N/A
	9	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

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/Zusammenfassungsrouten:** Eine Übersichtsrouten 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 Übersichtsrouten 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

November 16, 2022

Hinweis

Ab Version SD-WAN 11.5 werden alle Routingkonfigurationen nur über den Citrix SD-WAN Orchestrator Service unterstützt. Informationen zu den Routingkonfigurationen des Citrix SD-WAN Orchestrator Service finden Sie unter [Routing](#).

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

August 29, 2022

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

Das SD-WAN ermöglicht statische Routeneinträge für bestimmte Standorte und Routeneinträge, die über unterstützte Routing-Protokolle wie OSPF, eBGP und iBGP aus dem Underlay-Netzwerk 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. Über-

prüfen 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 Pfadrouten 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).

Die Routing-Tabelle für den lokalen Client-Knoten kann auf der Seite **Überwachung > Statistiken** überwacht werden, wobei Routen für die Dropdownliste **Anzeigen** ausgewählt sind.

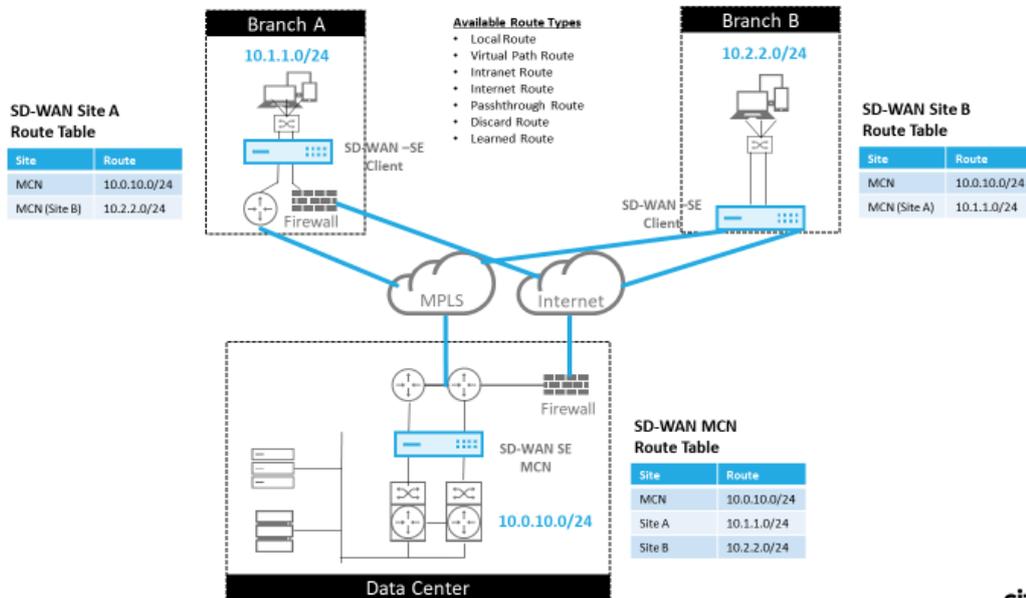
Route Statistics															
Maximum allowed routes: 64000															
Routes for routing domain : Default_RoutingDomain															
Filter: <input type="text"/> in Any column <input type="button" value="Apply"/>															
Num#	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	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	224.255.1.1/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
4	224.255.1.2/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
5	224.255.1.3/32	*	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_Lvpx01	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_Lvpx02	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_Lvpx03	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_Lvpx04	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_Lvpx05	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_Lvpx06	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_Lvpx07	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_Lvpx08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
22	192.172.8.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_Lvpx13	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_Lvpx14	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_Lvpx15	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_Lvpx16	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_Lvpx17	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_Lvpx18	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_Lvpx19	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_Lvpx20	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_Lvpx01	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_Lvpx02	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_Lvpx03	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_Lvpx04	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_Lvpx05	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_Lvpx06	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_Lvpx07	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_Lvpx08	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_Lvpx13	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_Lvpx14	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_Lvpx15	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_Lvpx16	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_Lvpx17	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_Lvpx18	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_Lvpx19	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_Lvpx20	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.

SD-WAN Overlay Route Tables



35 © 2017 Citrix

CITRIX

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 Dienstyp (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 im SD-WAN Orchestrator Service aktiviert waren, wurde die Konfiguration von Subnetzen, die für die Verwendung des SD-WAN-Overlays angegeben sind, vereinfacht. 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.

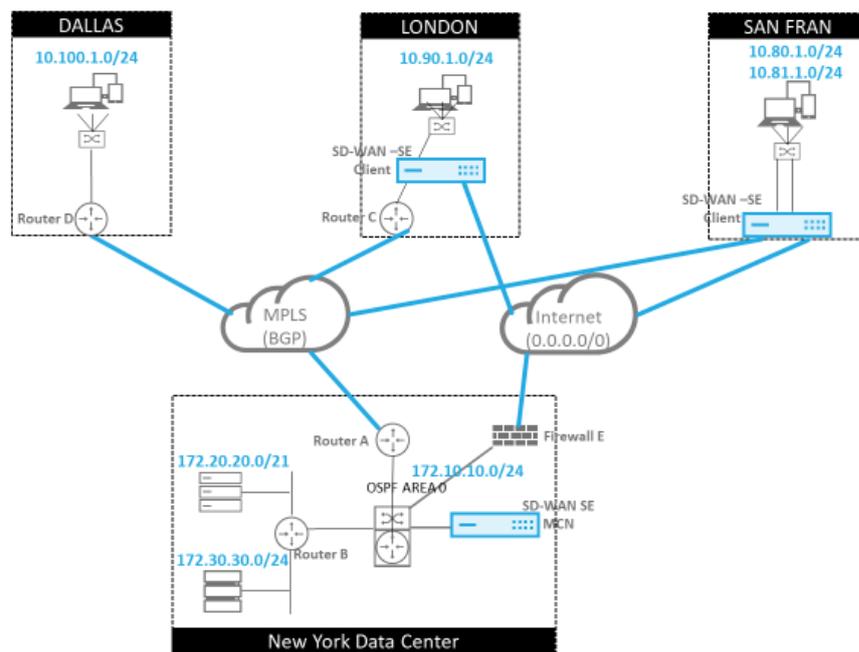
Die SD-WAN Virtual Path Routen-Tabelle funktioniert wie ein External Gateway Protocol (EGP), ähnlich wie BGP (Think Site-to-Site). Wenn SD-WAN beispielsweise Routen von der SD-WAN-Appliance zu OSPF anmeldet, werden sie normalerweise als extern für Standort und Protokoll betrachtet.

Hinweis

Beachten Sie Umgebungen mit IGP über die gesamte Infrastruktur (über das WAN), da dies die Verwendung von SD-WAN-angekündigten Routen erschwert. EIGRP wird in großem Umfang auf dem Markt verwendet, und SD-WAN arbeitet nicht mit diesem Protokoll zusammen.

Eine Herausforderung bei der Einführung von Routingprotokollen in eine SD-WAN-Bereitstellung besteht darin, dass die Routingtabelle erst verfügbar ist, wenn der SD-WAN-Dienst aktiviert und im Netzwerk ausgeführt wird. Daher wird es nicht empfohlen, zuerst 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:



37 © 2017 Citrix

CITRIX

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 hat, 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

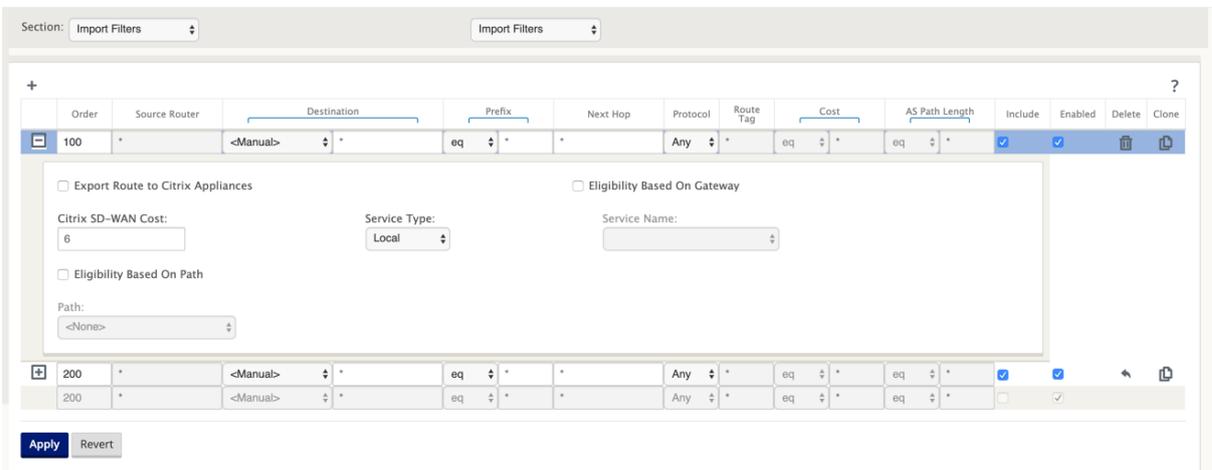
In diesem Beispiel können Sie das Subnetz 192.168.65.0/24 ignorieren. Dies ist ein Management-Netzwerk und nicht relevant für das Beispiel. Alle Router sind mit dem Management-Subnetz verbunden, werden jedoch in keinem Routingprotokoll angekündigt.

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 neu zu anzukündigen. Jede Route, die mit einem Präfix SD-WAN übereinstimmt, hat über die virtuellen Pfade gelernt.

Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
100	<Manual> *	eq 24	eq *	Local	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
200	<Manual> 0.0.0.0/0	eq *	eq *	Any	<Any>	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(auto)	<Manual> *	eq *	eq *	Any	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Nachdem die Citrix SD-WAN Appliances bereitgestellt wurden, können wir einen aktualisierten Blick auf die Routentabellen für den BGP-Router am Standort Dallas werfen. Wir sehen, dass 10.80.1.0/24 und 10.81.1.0/24 Subnetze korrekt 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

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

Num ^a	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 funktionierenden/aufbereitenden Zustand befindet.

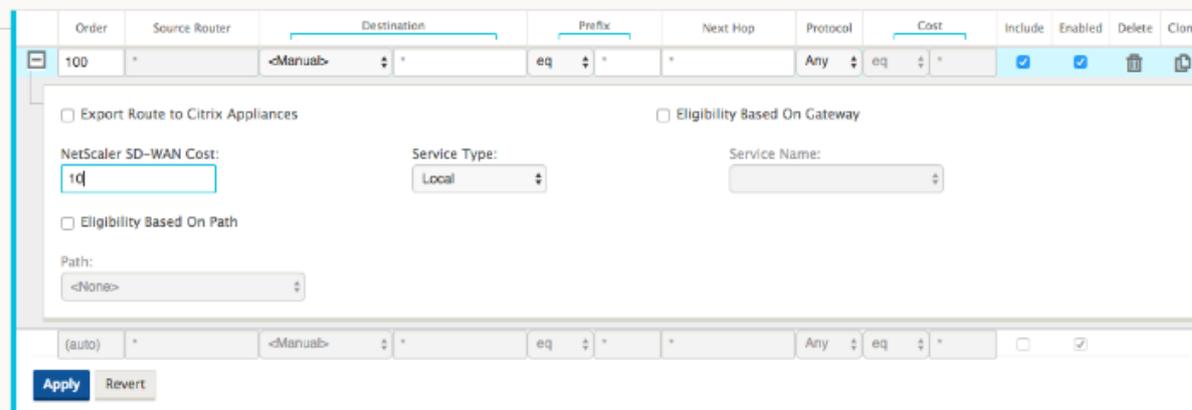
- Als beworbene Route durch BGP (Nummer 6), mit einem Preis von 6. Dies gilt jetzt als Fallback-Route.

Da das Präfix gleich ist und die Kosten unterschiedlich sind, verwendet SD-WAN die virtuelle Pfadrouten, es sei denn, sie wird nicht verfügbar. In diesem Fall wird die Fallback-Route über BGP erlernt.

Betrachten wir nun die Route 172.20.20.0/24.

- Dies wird als Virtual Path Route (Nummer 9) erlernt, hat aber eine Art von Dynamik und einen Preis von 6. Dies bedeutet, dass die Remote-SD-WAN-Appliance diese Route über ein Routingprotokoll, in diesem Fall OSPF, gelernt hat. Standardmäßig sind die Routenkosten höher.
- SD-WAN lernt diese Route auch über BGP mit den gleichen Kosten, so dass in diesem Fall diese Route möglicherweise gegenüber der Virtual Path Route bevorzugt wird.

Um ein korrektes Routing zu gewährleisten, müssen wir die BGP-Routenkosten erhöhen, um sicherzustellen, ob wir eine Virtual Path Route haben und es ist die bevorzugte Route. Dies kann getan werden, indem Sie das Gewicht der Import-Filter-Route so anpassen, dass es höher ist als der Standardwert 6 ist.



Nach der Anpassung können wir die SD-WAN-Routentabelle auf der San Francisco-Appliance aktualisieren, um die angepassten Routenkosten anzuzeigen. Verwenden Sie die Filteroption, um die angezeigte Liste zu fokussieren.

Routes for routing domain : Default_RoutingDomain

Filter: 172.20.20.0/24 in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries (filtered from 16 total entries)

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
5	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
8	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A

Showing 1 to 2 of 2 entries (filtered from 16 total entries)

Lassen Sie uns schließlich die erlernte Standardroute auf dem San Francisco SD-WAN betrachten. Wir wollen den gesamten Internetverkehr nach New York zurückholen. Wir können sehen, dass wir es mit dem virtuellen Pfad senden, wenn es oben ist, oder durch das MPLS-Netzwerk als Fallback.

Routes for routing domain : Default_RoutingDomain

Filter: 0.0.0.0/0 in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 16 total entries)

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
12	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
13	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 16 total entries)

Wir sehen auch eine Passthrough und verwerfen Route mit Kosten 16. Dies sind automatische Routen, die nicht entfernt werden können. Wenn das Gerät inline ist, wird die Passthrough-Route als 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.

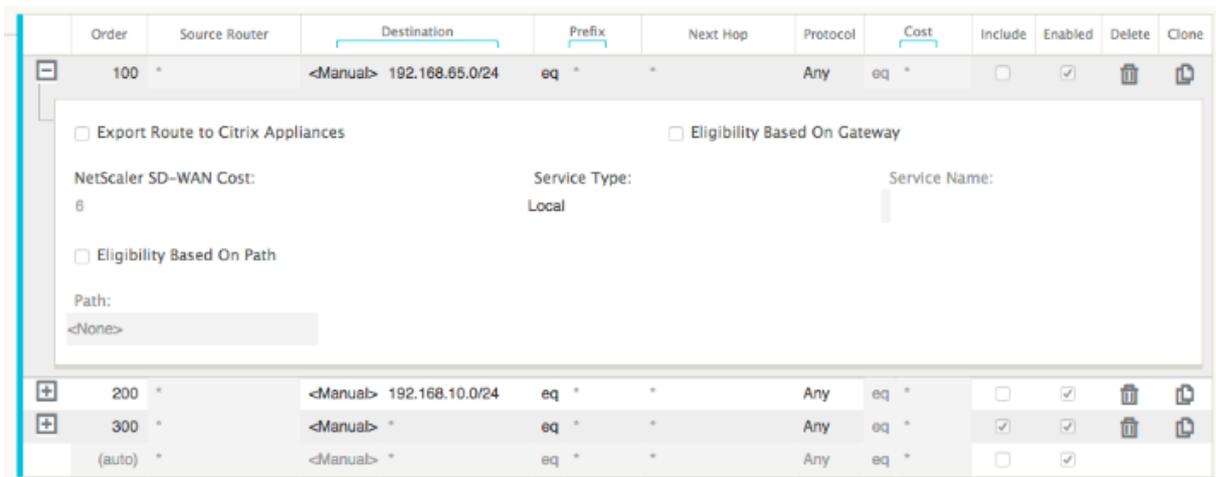
Wenn wir uns jetzt auf die New Yorker Site konzentrieren, möchten wir den Datenverkehr für entfernte Standorte (London und San Francisco) an die SD-WAN-Appliance weiterleiten, wenn der virtuelle Pfad aktiv ist.

Auf der New Yorker Site sind mehrere Subnetze verfügbar:

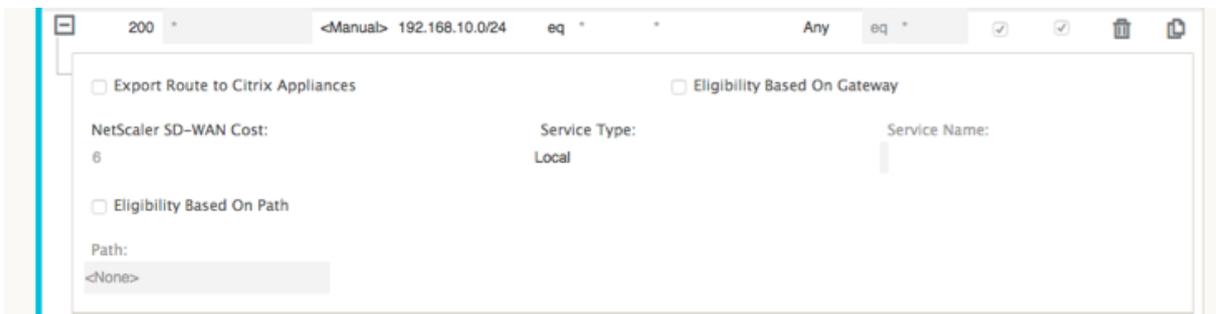
- 172.10.10.0/24 (direkt angeschlossen)
- 172.20.20.0/24 (über OSPF vom Core-Router B aus beworben)
- 172.30.30.0/24 (über OSPF vom Core-Router B aus beworben)

Wir müssen auch den Verkehrsfluss nach Dallas (10.100.1.0/24) über MPLS bereitstellen.

Schließlich wollen wir die gesamte internetgebundene Verkehrsrouten 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:

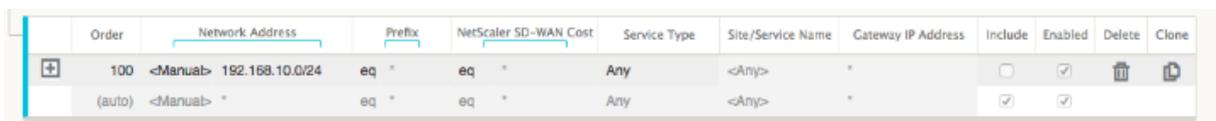


Der New York SD-WAN-Standort importiert alle Routen für das Management-Netzwerk. Dies kann ignoriert werden. Wir können uns auf Filter 200 konzentrieren.



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

Show entries Showing 1 to 11 of 11 entries

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24	*	Local	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0.0/0	172.10.10.3	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
10	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Wir können die richtigen Routen für die lokalen Subnetze sehen, die über OSPF gelernt wurden, eine Route zum Standort Dallas, die vom MPLS Router A gelernt wurde, und die Remote-Subnetze für die Standorte San Francisco und London. Schauen wir uns den MPLS Router A an. Dieser Router beteiligt sich an OSPF und BGP.

```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:04:12
O 10.80.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O 10.81.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O 10.90.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 00:05:11
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 00:04:28
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 00:05:24
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 00:05:09
C>* 192.168.10.0/24 is directly connected, eth2
O 192.168.65.0/24 [110/20] via 172.10.10.2, 00:04:12
C>* 192.168.65.0/24 is directly connected, eth0
```

Aus der Routentabelle lernt dieser Router A die entfernten Subnetze über BGP und OSPF mit der administrativen Entfernung und Kosten der BGP-Route (20/5) niedriger als OSPF (110/10) und daher bevorzugt. In diesem Beispiel kann das Netzwerk, in dem nur eine Kernroute vorhanden ist, keine Bedenken verursachen. Der hier ankommende Datenverkehr würde jedoch über das MPLS-Netzwerk zugestellt und nicht an die SD-WAN-Appliance gesendet werden (172.10.10.10). Wenn wir eine vollständige Routing-Symmetrie beibehalten möchten, benötigen wir eine Routenkarte, um die AD/Metrik-Kosten so anzupassen, dass es Routenpräferenz von der Route kommt aus 172.10.10.10 statt der Route, die über eBGP gelernt wurde.

Alternativ kann eine “Backdoor”-Route 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.

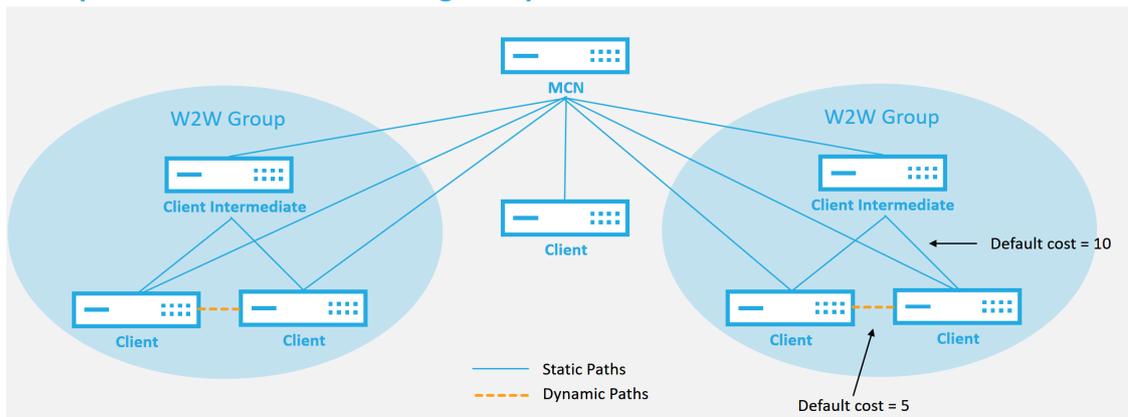
Sobald die Schwellenwerte für dynamische virtuelle Pfade erreicht sind, erstellen die Clientknoten dynamisch ihren virtualisierten Pfad zueinander unter Verwendung aller verfügbaren WAN-Pfade zwischen den Standorten und nutzen ihn auf folgende Weise voll aus:

- 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.

In SD-WAN sind mehrere WAN-zu-WAN-Weiterleitungsgruppen zulässig, wodurch die vollständige Kontrolle über die Pfadeinrichtung zwischen bestimmten Clientknoten und nicht anderen ermöglicht wird.

Multiple WAN to WAN Forwarding Groups



WAN to WAN Forwarding Group:

- A network can have multiple WAN to WAN Forwarding Groups
- Direct dynamic path will have a lower cost than through the intermediate node

51 © 2017 Citrix

CITRIX

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**

Show **100** entries Showing 1 to 13 of 13 entries

Num [#]	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	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	-	-	3	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 13 of 13 entries

Beachten Sie aus der vorangegangenen SD-WAN-Routentabelle, dass in herkömmlichen Routern normalerweise mehr Elemente nicht verfügbar sind. Am bemerkenswertesten ist die Spalte Erreichbar, die die Route je nach WAN-Pfadstatus entweder aktiv oder inaktiv (ja/nein) macht. Die hier aufgelisteten Routen werden basierend auf verschiedenen Zuständen des Dienstes unterdrückt (der virtuelle Pfad ist als Beispiel heruntergefahren). Andere Ereignisse, die erzwingen können, dass eine Route nicht berechtigt ist, sind Pfad-Down-Status, nächster Hop nicht erreichbar oder WAN-Link down.

Aus der obigen Tabelle können wir 14 definierte Routen sehen. Eine Beschreibung der Routen oder Streckengruppen wird wie folgt beschrieben:

- Route 0 —Auf dem MCN handelt es sich um eine Host-Subnetzroute, die sich am DC-Standort befindet. 172.16.10.0/24 befindet sich im DC-LAN und 192.168.15.1 ist das Gateway im LAN, das der nächste Hop ist, der zu diesem Subnetz gelangen wird.
- Route 1 —Dies ist eine lokale Route zu diesem SD-WAN-Gerät, 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

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

August 29, 2022

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

August 29, 2022

Citrix SD-WAN-Appliances ermöglichen die Konfiguration von Routingprotokollen und bieten einen einzigen Verwaltungspunkt für die Verwaltung eines Unternehmensnetzwerks, eines Zweigstellennetzwerks oder eines Rechenzentrumsnetzwerks. Sie können bis zu 254 Routingdomänen konfigurieren.

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.

Verwenden von CLI für den Zugriff auf Routing

August 29, 2022

In Citrix SD-WAN Version 10.0 können Sie zusätzliche Informationen zum dynamischen Routing und zum Protokollstatus anzeigen. Geben Sie den folgenden Befehl und die folgende Syntax ein, um auf den Routing-Daemon zuzugreifen und die Liste der Befehle anzuzeigen.

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

Dynamisches Routing

August 29, 2022

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.

Hinweis

- Citrix SD-WAN-Appliances nehmen nicht als Designated Router (DR) und BDR (Backup Designated 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).

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.

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.

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.

Monitoring > Statistics

Statistics

Show: **Routes** Enable Auto Refresh **5** seconds **Refresh** Clear Counters on Refresh **Purge dynamic routes**

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in **Any column** **Apply**

Show **100** entries Showing 1 to 28 of 28 entries

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	115.1.1.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
1	115.168.0.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
2	115.168.0.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
3	115.168.0.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
4	115.168.0.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
5	115.168.0.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	115.14.14.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	115.13.13.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	115.12.12.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	115.10.10.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
10	115.9.9.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
11	115.8.8.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
12	115.7.7.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
13	115.6.6.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
14	115.5.5.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
15	115.4.4.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
16	115.3.3.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
17	115.2.2.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
18	182.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
19	172.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
20	182.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
21	172.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
22	182.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
23	172.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
24	192.120.1.0/24	172.120.1.2	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	75612	YES	N/A	N/A
25	192.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Dynamic	Virtual WAN	YES	6	75612	YES	N/A	N/A
26	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
27	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 28 of 28 entries

OSPF

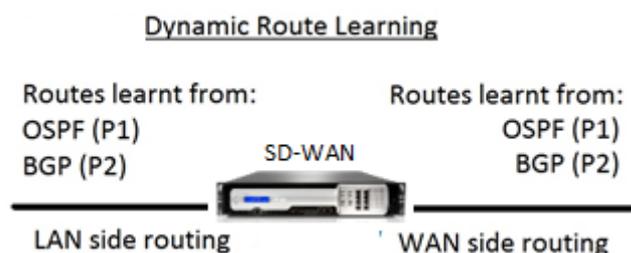
August 29, 2022

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.

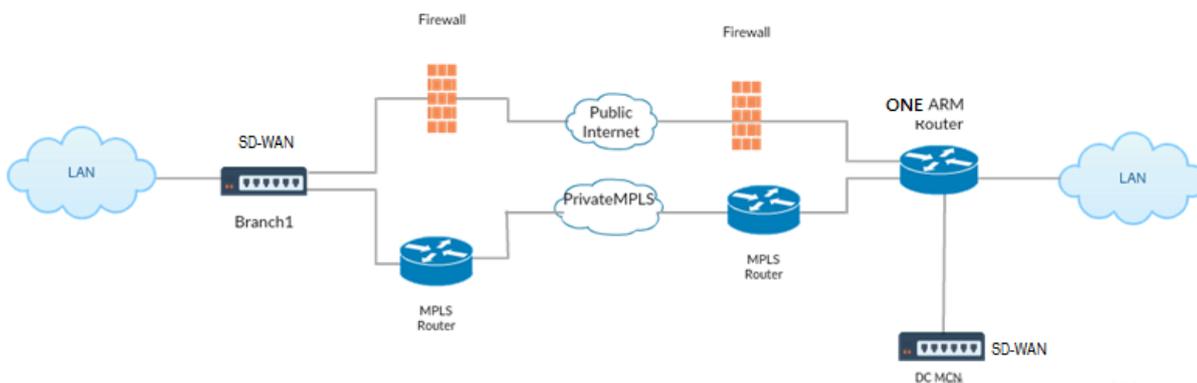
Mit der neuesten Version kann SD-WAN jetzt Routen als flächeninterne Routen (LSA Typ 1) ankündigen, um mithilfe des OSPF-Pfadauswahlalgorithmus die Präferenz gemäß den Routenkosten zu erhalten. Die Routenkosten können konfiguriert und dem Nachbarrouter angekündigt werden. Dies ermöglicht die Bereitstellung 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.

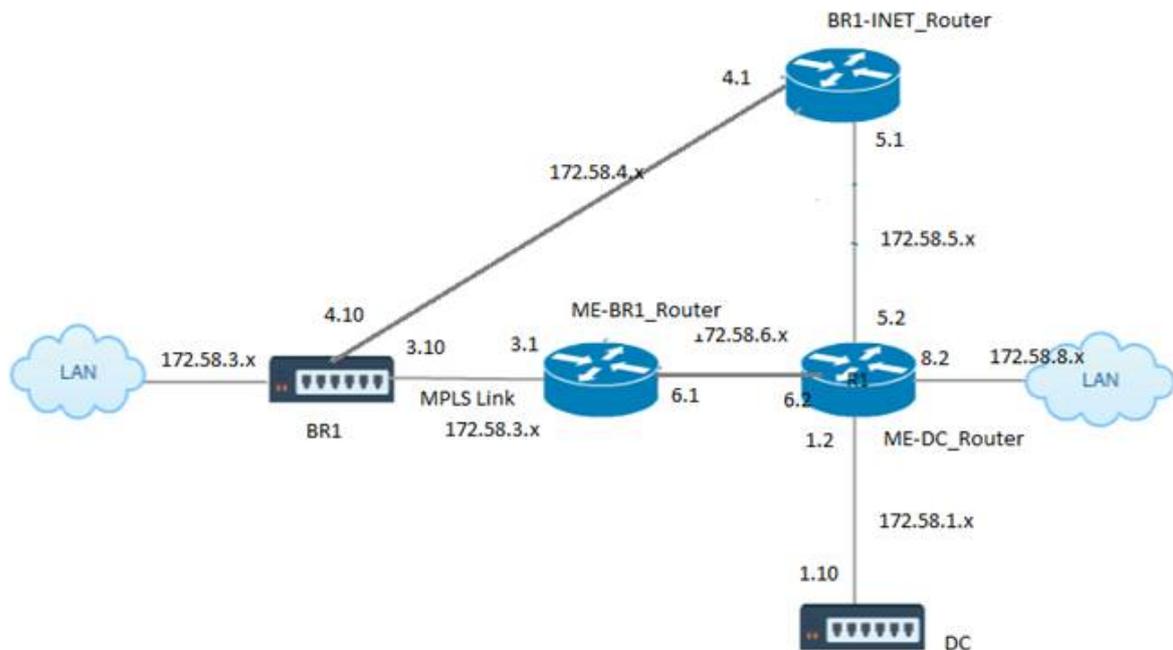


Wie in der Abbildung oben gezeigt, wird DC MCN in der Einarm-Topologie eingesetzt. Wenn der DC-Standort hochgefahren ist, leitet der einarmige Router den gesamten Datenverkehr vom lokalen LAN an andere Standorte weiter, z. B. das lokale LAN der Zweigstelle, dessen Ziel-IP-Adresse sich innerhalb desselben 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.

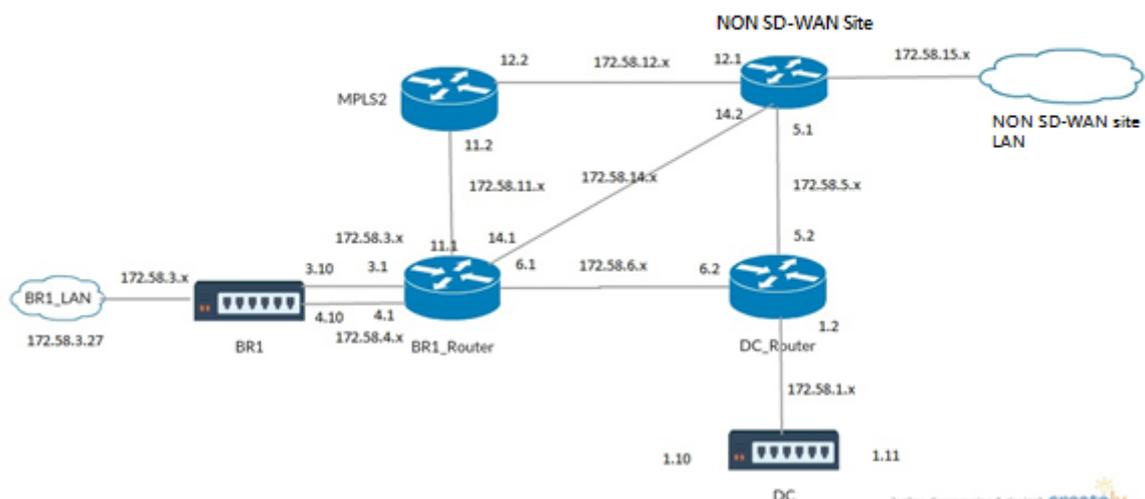
Dadurch wird auch sichergestellt, dass bei einem Ausfall der DC SD-WAN-Appliance die alternative Route zur Verwendung des ME-BR1_Routers als nächstes bevorzugtes Gateway einen unterbrechungsfreien Datenfluss gewährleistet.

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.

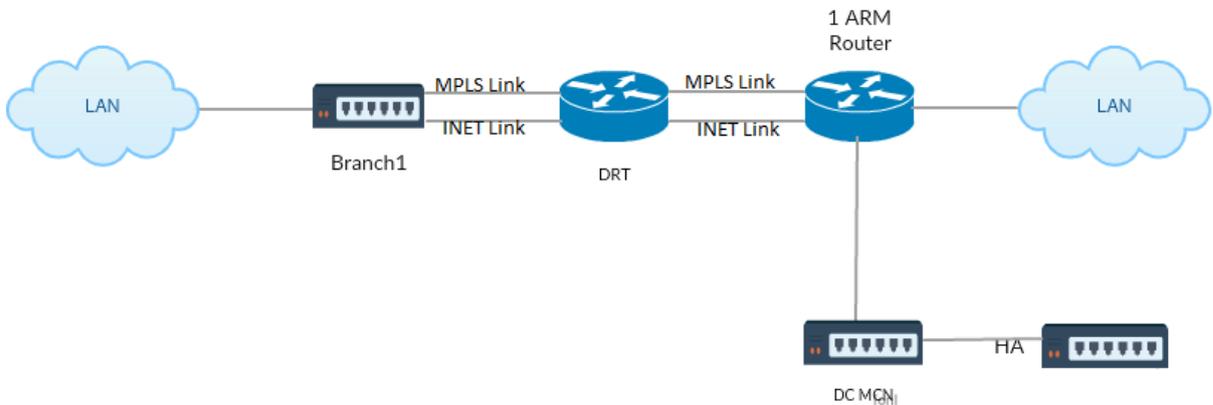
Bereitstellung von SD-WAN- und Drittanbieter-Appliances (Nicht-SD-WAN)

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.



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:

Problembehandlung

Sie können die OSPF-Parameter unter **Monitoring > Routing Protocols** anzeigen.

The screenshot shows the Citrix SD-WAN management interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Monitoring' tab is active, and the 'Routing Protocols' sub-tab is selected. On the left, a sidebar menu lists various monitoring options, with 'Routing Protocols' highlighted. The main content area displays the 'Dynamic Routing Protocol' configuration. It includes a 'View' dropdown set to 'OSPF Interface' and a 'Routing Domain' dropdown set to 'Default_RoutingDomain', with a 'Refresh' button. Below this, the 'OSPF Interface' configuration is shown for 'ospf_rdomain_0' on 'Interface vni-0 (172.58.1.0/24)'. The configuration details are as follows:

```

ospf_rdomain_0:
Interface vni-0 (172.58.1.0/24)
  Type: broadcast
  Area: 0.0.0.0 (0)
  State: DROther
  Priority: 0
  Cost: 10
  Hello timer: 10
  Wait timer: 40
  Dead timer: 40
  Retransmit timer: 5
  Designated router (ID): 105.105.105.105
  Designated router (IP): 172.58.1.28
  Backup designated router (ID): 0.0.0.0
  Backup designated router (IP): 0.0.0.0
    
```

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: OSPF Neighbors Routing Domain: Default_RoutingDomain Refresh

OSPF Neighbors

```
ospf_rdomain_0:
Router ID      Pri      State      DTime      Interface  Router IP
105.105.105.105  1      Full/DR    00:39      vni-0      172.58.1.28
```

Sie können auch die dynamischen Routingprotokolle beobachten, um festzustellen, ob ein Problem mit der OSPF-Konvergenz vorliegt.

Diagnose

Debug Logging: On Off

Filename: dynamic_routing_diagnostics.log

View Log

BGP

August 29, 2022

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.

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.

1. 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.

The screenshot shows the 'Monitoring > Routing Protocols' page. On the left is a navigation menu with 'Routing Protocols' selected. The main content area shows 'Dynamic Routing Protocol' settings and a 'BGP State' section. The 'BGP State' section contains a table with columns: name, proto, table, state, since, and info. Below the table is a detailed text output of BGP statistics and session information.

name	proto	table	state	since	info
bgp1_rdomain_0	BGP	T0	up	2020-08-27 10:46:44	Established

```

Preference: 100
Input filter: neighbour_0_in
Output filter: neighbour_0_out
Routes: 8 imported, 4 exported, 1 preferred
Route change stats: received rejected filtered ignored accepted
Import updates: 16 0 0 8 8
Import withdraws: 0 0 --- 0 0
Export updates: 43 19 18 --- 6
Export withdraws: 2 --- --- --- 2
BGP state: Established
Neighbor address: 172.58.1.28
Neighbor AS: 10
Citrix SD-WAN Interface: vni-0
Neighbor ID: 105.105.105.105
Neighbor caps: refresh AS4
Session: internal multihop AS4
Source address: 172.58.1.10
Hold timer: 130/180
Keepalive timer: 46/60
    
```

Sie können die Dynamische Routingprotokolle beobachten, um festzustellen, ob ein Problem mit der BGP-Konvergenz vorliegt.

Diagnose

Debug Logging: On Off

Filename: ▼

iBGP

August 29, 2022

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

August 29, 2022

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.

Anwendungsrouten

August 29, 2022

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 Dienstypen in Zeiten der Überlastung begrenzt. Unter bestimmten Bedingungen und wenn Intranet-

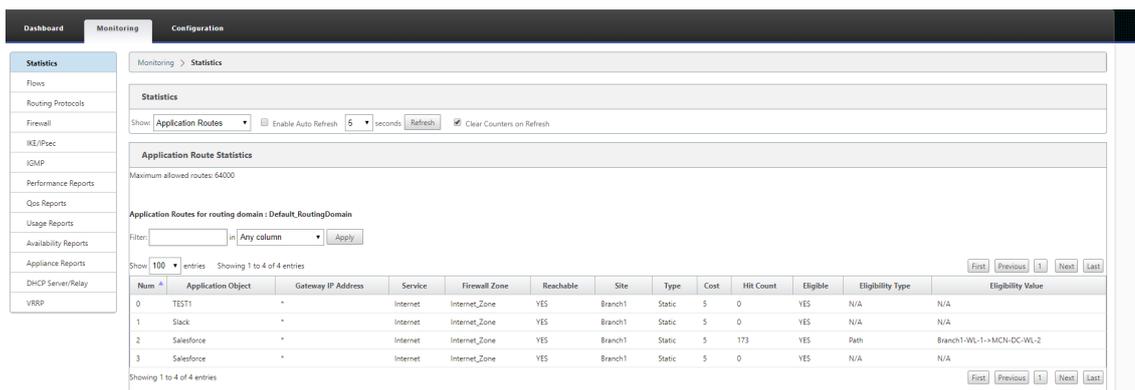
Fallback auf dem virtuellen Pfad konfiguriert ist, kann Datenverkehr, der normalerweise durch den virtuellen Pfad fließt, stattdessen als Intranet-Verkehr behandelt werden.

- **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 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 Dienstyp, 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.
- **Berechtigenswert:** 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

August 29, 2022

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.

Routenzusammenfassung

August 29, 2022

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 Übersichtsrouten mit den Dienstypen Lokal und Discard konfigurieren. Diese zusammenfassende Route wird für die Next-Hop-Geräte beworben.

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.

The screenshot displays the Citrix SD-WAN 11.5 interface with three main navigation tabs: **Dashboard**, **Monitoring**, and **Configuration**. The **Configuration** tab is active.

System Status

Name:	BR1_VPX
Model:	VPX
Sub-Model:	BASE
Appliance Mode:	Client
Serial Number:	5f4519dd-e39a-d3f6-24a6-6ba0e6578d2c
Management IP Address:	10.105.172.7
Appliance Uptime:	6 days, 56 minutes, 1.4 seconds
Service Uptime:	6 days, 50 minutes, 39.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Local Versions

Configuration Created On:	Wed Sep 2 11:15:54 2020
Software Version:	11.2.1.53.864510
Built On:	Aug 25 2020 at 19:02:21
Hardware Version:	VPX
OS Partition Version:	5.1

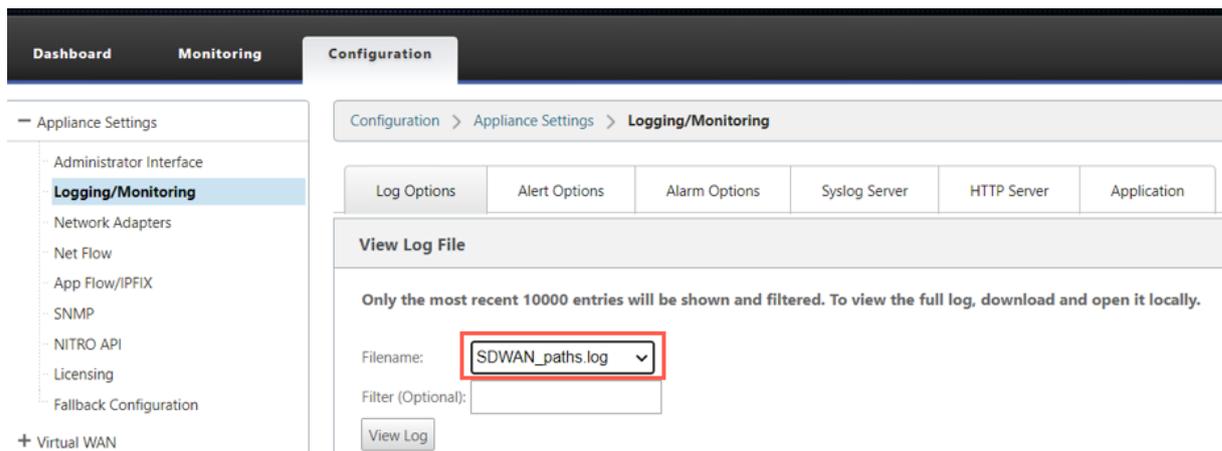
Virtual Path Service Status

Virtual Path MCN_VPX-BR1_VPX	Uptime: 6 days, 50 minutes, 19.0 seconds.
-------------------------------------	--

Wenn der virtuelle Pfad ausgefallen ist, überprüfen Sie den Grund dafür unter **Konfiguration > Logging/Monitoring**.

Wählen Sie eine der folgenden Dateien aus der Dropdownliste **Dateiname** aus, um dies zu überprüfen:

- SDWAN_paths.log
- SDWAN_common.log



Protokollpräferenz

August 29, 2022

Die Protokolleinstellung ist eine Citrix SD-WAN-spezifische Funktion, die der administrativen Entfernung des Routers ähnelt. Das Protokoll mit der höchsten Präferenzreihenfolge ist am meisten bevorzugt. Die Route, die das Protokoll mit dem höchsten Protokollpräferenzwert verwendet. Die Protokollprioritätsinformationen befinden sich lokal auf der Citrix SD-WAN-Appliance und werden nicht für Peer-Netzwerkelemente angekündigt.

Multicast-Routing

August 29, 2022

Multicast-Routing ermöglicht eine effiziente Verteilung des 1:n-Datenverkehrs. Eine Multicastquelle sendet Multicast-Datenverkehr in einem einzelnen Stream an eine Multicast-Gruppe. Die Multicast-Gruppe enthält Empfänger wie Hosts und angrenzende Router, die das IGMP-Protokoll für die Multicastkommunikation verwenden. Voice over IP, Video on Demand, IP-TV und Videokonferenzen sind einige der gängigen Technologien, die Multicast-Routing verwenden. Wenn Sie Multicastroouting auf der Citrix SD-WAN Appliance aktivieren, fungiert die Appliance als Multicastrouter.

Quellspezifischer Multicast

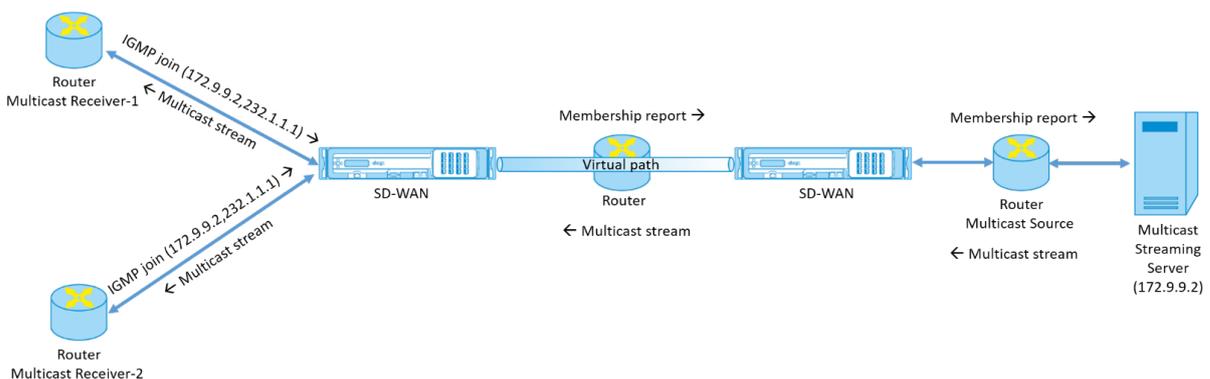
Multicast-Protokolle ermöglichen Multicastempfänger in der Regel den Empfang von Multicast-Datenverkehr von jeder Quelle. Mit quellspezifischem Multicast (SSM) können Sie die Quelle

angeben, von der die Empfänger den Multicastverkehr empfangen. Es stellt sicher, dass die Empfänger nicht offene Listener für jede Quelle sind, die Multicast-Streams sendet, sondern vielmehr eine bestimmte Multicastquelle hören. SSM reduziert die Kosten für Ressourcen, die für den Verbrauch von Datenverkehr aus jeder möglichen Quelle verwendet werden, und bietet außerdem eine Sicherheitsstufe, indem sichergestellt wird, dass die Empfänger Datenverkehr von einem bekannten Absender empfangen.

Die folgende Topologie zeigt zwei Multicastempfänger an einem Zweigstandort und einen Multicastserver (172.9.9.2) im Rechenzentrum. Der Multicast-Server streamt Datenverkehr über eine bestimmte Gruppe (232.1.1.1), wobei die Empfänger der Gruppe beitreten. Jeder Datenverkehr, der in der Multicastgruppe gestreamt wird, wird an alle Empfänger weitergeleitet, die der Gruppe beigetreten sind.

Hinweis

Damit SSM funktioniert, muss die IP der Multicastgruppe im Bereich 232.0.0.0/8 liegen.



1. Die Multicastempfänger senden eine IP-IGMP-Join-Anforderung, die angibt, dass die Empfänger der Multicastgruppe beitreten und den Multicast-Stream von der Quelle empfangen möchten. Der IGMP-Join enthält 2 Attribute die Multicastquelle und -gruppe (S, G). IGMP Version 3 wird für SSM auf der Multicastquelle und der Empfänger verwendet, um einige INCLUDE-spezifische Quelladressen weiterzuleiten. SSM ermöglicht es den Empfängern, Streams von bestimmten Multicast-Servern explizit zu empfangen, deren Quelladresse explizit von den Empfängern als Teil der JOIN-Anfrage bereitgestellt wird. In diesem Beispiel wird eine IGMP v3-Join-Anforderung mit einer expliziten Include-Quellliste ausgelöst, die die Quelle 172.9.9.2 enthält, um die Adresse zu sein, die den Multicast-Stream über die Gruppe 232.1.1.1 sendet.
2. Das Citrix SD-WAN in der Zweigstelle hört alle IGMP-Anforderungen von diesen Empfängern ab und konvertiert sie in einen Mitgliedschaftsbericht und sendet ihn über den virtuellen Pfad an die SD-WAN-Appliance im Rechenzentrum.
3. Die Citrix SD-WAN Appliance im Rechenzentrum empfängt den Mitgliedschaftsbericht über den virtuellen Pfad und leitet ihn an die Multicastquelle weiter, um einen Kontrollkanal zu erstellen.

4. Die Multicastquelle überträgt den Multicast-Stream über den virtuellen Pfad an die Multicastempfänger.

Der Datenverkehr des Kontrollkanals und der Multicast-Stream fließen durch den etablierten virtuellen Pfad zwischen der Zweigstelle und dem Rechenzentrum. Der Citrix SD-WAN Overlay-Pfad sichert und isoliert Multicast-Datenverkehr vor WAN-Verschlechterung oder Link-Brownouts.

Konfigurieren von Multicast

Um Multicast zu konfigurieren, führen Sie die folgenden Schritte auf der SD-WAN-Appliance sowohl an der Quelle als auch am Ziel aus.

1. Multicastgruppe erstellen - Geben Sie einen Namen und eine IP-Adresse für die Multicastgruppe an. Die IP der Multicastgruppe muss im Bereich 232.0.0.0/8 für quellspezifisches Multicast liegen.
2. IGMP-Proxy aktivieren — Sie können die Citrix SD-WAN Appliance als IGMP-Proxy konfigurieren, um die IGMP-Kontrollkanalinformationen für Multicast-Routing zu übertragen. IGMP V3 ist für Single-Source-Multicast erforderlich.
3. Definieren der Upstream- und Downstream-Dienste - Eine Upstream-Schnittstelle ermöglicht es dem IGMP PROXY, eine Verbindung mit der SD-WAN-Appliance herzustellen, die näher an der eigentlichen Multicastquelle liegt, die den Datenverkehr streamt. Eine Downstream-Schnittstelle ermöglicht es dem IGMP-Proxy, eine Verbindung zu den Hosts herzustellen, die weiter von der eigentlichen Multicastquelle entfernt sind, die den Datenverkehr streamt. Die Upstream- und Downstream-Dienste unterscheiden sich für die Appliance an der Quelle und die Appliance am Ziel.

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 einen MLD-Join, der initiiert wurde und der Nachrichtentyp RECV zum Empfangen von Multicastgruppenadressen verwendet wird. Sie können auch die IGMP/MLD-Nachrichtenstatistik unten sehen.

Dashboard
Monitoring
Configuration

Monitoring > IGMP

Filter/Purge

IGMP PROXY Groups

Max Groups to Display:
Service Type to Display:

Type	Name	Group	Filter	Version	Packets Sent	Bytes Sent
HOST	VIF-1-Bridge-1	232.1.1.1	INCLUDE	IGMPv3	4285	6418930

Total Groups Displayed: 1 out of 1

IGMP Stats

Max IGMP Stats to Display:
Stats Type to Display:

Type	Description	Value
MEMBER	Add Member	1
MEMBER	Remove Member	0
MEMBER	Current Member	1

Total IGMP Stats Displayed: 3 out of 70

Die folgende Abbildung zeigt Informationen zu IGMP/MLD-Proxygruppen. Sie können auch die IGMP/MLD-Proxygruppenstatistiken und die verwendete Version sehen.

IGMP/MLD Proxy Groups

Select the maximum Proxy Groups to display

Type	Name	Group	Filter	Version	Packets Sent	Bytes Sent	
HOST	VIF-1-LAN-1		EXCLUDE	MLDv2	12380158	1832263384	
HOST	VIF-1-LAN-1		EXCLUDE	MLDv2	12380158	1832263384	
HOST	VIF-1-LAN-1		EXCLUDE	MLDv2	12380158	1832263384	
HOST	VIF-1-LAN-1		EXCLUDE	MLDv2	11905188	1761967824	

Routenkosten für virtuelle Pfade konfigurieren

August 29, 2022

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.

Überwachung und Fehlerbehebung

In der Routingtabelle wird angezeigt, wie dieselben Subnetze, die von zwei Standorten angekündigt werden, die über den virtuellen Pfad mit einem Zweigstandort verbunden sind, mit dem Kostenanteil virtueller Pfadrouten installiert werden.

Um die Routenkosten und die in der Routing-Tabelle verwendeten Routen zu überprüfen, navigieren Sie zu **Überwachung > Statistiken**. Wählen Sie unter dem Feld **Anzeigen** die Option **Routen** aus. Routenkosten und Trefferzählungen können auf derselben Seite überprüft werden.

Die folgende Abbildung zeigt die Routing-Tabelle mit zwei unterschiedlichen Kosten für dieselbe Route, die 172.16.6.0/24 mit Kosten 10 und 11 für die Dienste **DC-Branch01** bzw. **GEOMCN-Branch01** beträgt.

Monitoring > Statistics

Statistics

Show: Enable Auto Refresh seconds Clear Counters on Refresh

Routing Domain:

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in

Show entries Showing 1 to 18 of 18 entries

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
<input type="checkbox"/>	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
<input type="checkbox"/>	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
<input type="checkbox"/>	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input checked="" type="checkbox"/>	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
<input type="checkbox"/>	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
<input type="checkbox"/>	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
<input checked="" type="checkbox"/>	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
<input type="checkbox"/>	11	172.16.4.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A

Konfigurieren des Virtual Router-Redundanzprotokolls

August 29, 2022

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.

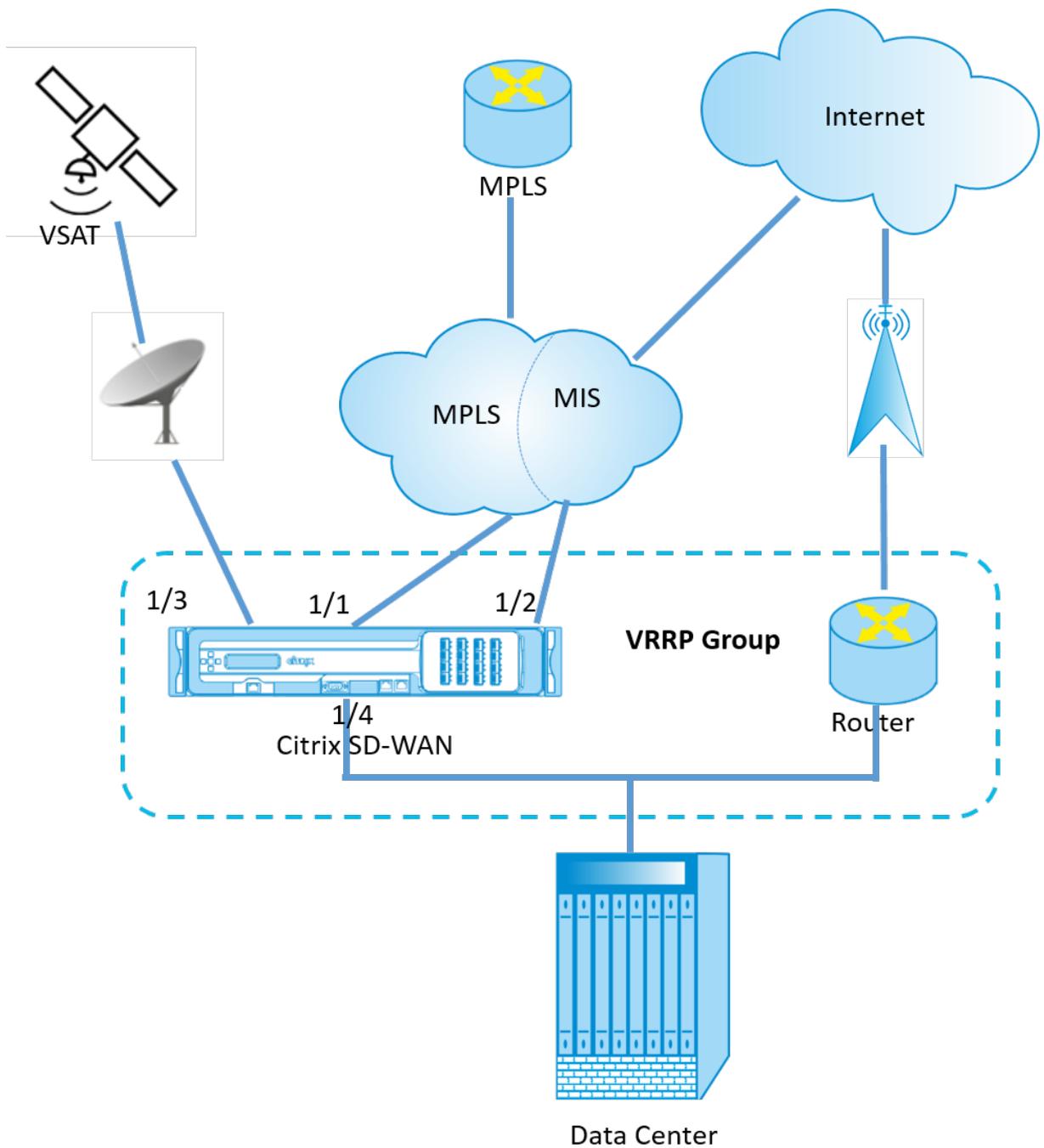
VRRP gibt einen Wahlprozess an, bei dem der Router mit der höchsten Priorität zum Master wird. Wenn die Priorität unter den Routern gleich ist, wird der Router mit der höchsten IP-Adresse zum Master. Die anderen Router befinden sich im Backup-Zustand. Der Wahlprozess wird erneut eingeleitet, wenn

der Master ausfällt, ein neuer Router der Gruppe beitrifft oder ein vorhandener Router die Gruppe verlässt.

VRRP stellt einen Standardpfad für hohe Verfügbarkeit sicher, ohne dynamische Routing- oder Routererkennungspkotoolle auf jedem Endhost zu konfigurieren.

Citrix SD-WAN Version 10.1 untersttzt 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 knnen die SD-WAN-Appliance als VRRP-Master konfigurieren, indem Sie die Virtual Interface IP als VRRP-IP konfigurieren und die Priorittt manuell auf einen hheren Wert als die Peer-Router festlegen. Sie knnen das Ankndigungsintervall und die Prempt-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 ausfllt, bernimmt der Backup-Router innerhalb von Millisekunden und stellt sicher, dass keine Ausfallzeiten vorliegen.



VRRP-Statistik

Sie können die VRRP-Statistiken unter **Monitoring > VRRP** einsehen.

The screenshot shows the 'Monitoring > VRRP Protocol' page. On the left is a navigation menu with options: Statistics, Flows, Routing Protocols, Firewall, IKE/IPsec, Performance Reports, Qos Reports, Usage Reports, Availability Reports, Appliance Reports, DHCP Server/Relay, and VRRP Protocol (selected). The main content area displays a table of VRRP instances.

VRRP ID	Version	Interface(s)	State	Priority	Virtual Router IP	Advertisement Interval	Enable	Disable
20	2	LAN-7	Master	250	172.58.7.100	2000	Enable	Disable
245	3	LAN	Master	200	172.58.5.20	1000	Enable	Disable

Sie können die folgenden Statistikdaten anzeigen:

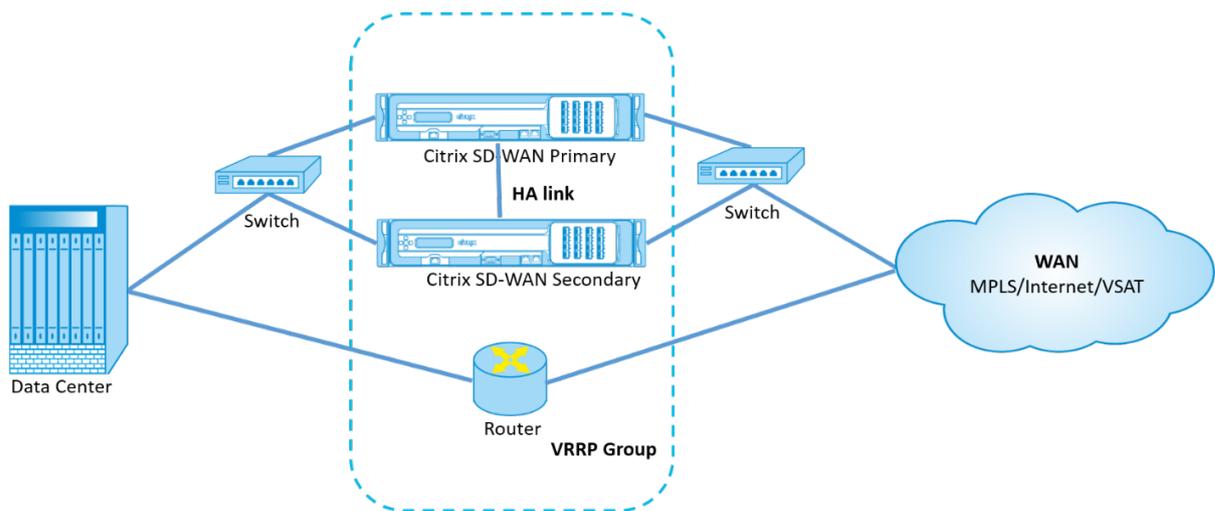
- **VRRP-ID:** Die VRRP-Gruppen-ID
- **Version:** Die VRRP-Protokollversion.
- **Schnittstelle:** Die für VRRP verwendete virtuelle Schnittstelle.
- **Zustand:** Der VRRP-Status der SD-WAN-Appliance. Es zeigt an, ob die Appliance ein Master oder ein Backup ist.
- **Priorität:** Die Priorität der SD-WAN-Appliance 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](#).

Routing-Unterstützung für die LAN-Segmentierung

August 29, 2022

Die SD-WAN Standard Edition-Appliances implementieren eine LAN-Segmentierung über verschiedene Standorte hinweg, an denen beide Appliances bereitgestellt werden. Die Appliances erkennen und speichern die verfügbaren LAN-seitigen VLANs und konfigurieren Regeln dafür, zu welchen anderen LAN-Segmenten (VLANs) an einem Remote-Standort mit einer anderen SD-WAN Standard Edition-Appliance eine Verbindung herstellen können.

Die oben genannte Funktion wird mithilfe einer VRF-Tabelle (Virtual Routing and Forwarding) implementiert, die in der SD-WAN Standard Edition-Appliance verwaltet wird und die Remote-IP-Adressbereiche verfolgt, 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 Netzwerkkumgebung 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.

Domänendienst für den übergreifenden Routing

August 29, 2022

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. 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.

Überwachen

Unter Überwachung > Firewall-Statistiken > Verbindungen können Sie Überwachungsstatistiken für Verbindungen anzeigen, die Interrouting-Domain-Dienste verwenden.

Source		Destination										Sent						
Routing Domain	Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	In Mfr	Packets	Bytes	PPS
Default-Routing-Domain	Internet Control Message Protocol(ICMP)	Network Service	ICMP	172.16.25.10	19973	Local	VIF-2-LAN-1	Default_LAN_Zone	172.16.1.10	19973	Inter-Routing-Domain	Default_L3_MPLS	Inter-Routing-Domain_Zone	ESTABLISHED	Yes	10124	850416	0.999
RD_MPLS	Internet Control Message Protocol(ICMP)	Network Service	ICMP	172.16.15.100	19973	Inter-Routing-Domain	Default_L3_MPLS	Inter-Routing-Domain_Zone	172.16.1.10	19973	Virtual Path	DC_MCN-BR3	Default_LAN_Zone	ESTABLISHED	No	10124	850416	0.999

ECMP Load Balancing

August 29, 2022

Equal Cost Multi-Path (ECMP) -Gruppen ermöglichen es Ihnen, mehrere Pfade mit denselben Kosten, Zielen und demselben Service zu gruppieren. Die Verbindungen oder Sitzungsdaten haben je nach Typ der ECMP-Gruppe einen Lastenausgleich über alle Pfade in der ECMP-Gruppe. Stellen Sie sich beispielsweise ein Netzwerk mit zwei WAN-Verbindungen zwischen einer Zweigstelle und einem Rechenzentrum mit den gleichen Routenkosten vor. Traditionell wäre einer der WAN-Verbindungen aktiv und der andere bleibt inaktiv und fungiert als Fallback-Link. Mit ECMP-Gruppen können Sie diese WAN-Verbindungen zusammenfassen und den Lastenausgleich des Datenverkehrs über beide WAN-Verbindungen zulassen. Der ECMP-Lastenausgleich gewährleistet:

- Verteilung des Datenverkehrs auf mehrere kostengleiche Wege.
- Optimale Nutzung der verfügbaren Bandbreite.
- Dynamische Übertragung des Datenverkehrs auf einen anderen ECMP-Mitglieds Pfad, wenn eine Verbindung fehlschlägt. ECMP unterstützt statische Routen auf IPsec/GRE-Tunneln.

Der ECMP-Lastenausgleich wird für virtuelle Pfade und Intranetdienste unterstützt. ECMP-Gruppen werden auf globaler Ebene definiert. Sie können maximal 254 ECMP-Gruppen in Ihrem Netzwerk definieren. Die maximale Anzahl von ECMP-berechtigten Routen in einer ECMP-Gruppe hängt von Ihrer Appliance und Ihrem Lizenztyp ab. Die folgenden zwei Arten von ECMP-Gruppen werden auf Citrix SD-WAN unterstützt:

- Quell-/Ziel-IP-Adresse: Netzwerke, in denen mehrere Clients versuchen, sich mit demselben Ziel zu verbinden, sind die Verbindungen über kostengünstige WAN-Verbindungen Lastausgleichlich.

- Sitzung: Netzwerke, in denen ein einzelner Client mit einem Ziel verbunden ist und mehrere Sitzungen erzeugt werden. Die Sitzungsdaten haben einen Lastausgleich bei WAN-Verbindungen mit gleichen Kosten.

Um den ECMP-Lastausgleich zu überwachen, navigieren Sie in der SD-WAN-Benutzeroberfläche zu **Überwachung > Statistiken > Routen** und filtern Sie die Suchergebnisse mithilfe des ECMP-Gruppennamens.

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Clear Counters on Refresh

Routing Domain: <ALL>

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain: Default_RoutingDomain

Filter: Tonowhere in ECMP Group Network Address Type: ALL

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 35 total entries)

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	ECMP Group	Eligible	Eligibility Type	Eligibility Value
<input type="checkbox"/>	6	6.6.6.0/24	*	New_Intranet_Service-3	Intranet_Zone	YES	BR1	Static	-	-	5	0	Tonowhere	YES	N/A	N/A
<input type="checkbox"/>	7	5.5.5.0/24	*	New_Intranet_Service-3	Intranet_Zone	YES	BR1	Static	-	-	5	630	Tonowhere	YES	Path	BR1_Inet1->DC_Inet1
<input type="checkbox"/>	8	5.5.5.0/24	*	New_Intranet_Service-4	Intranet_Zone	YES	BR1	Static	-	-	5	315	Tonowhere	YES	N/A	N/A
<input type="checkbox"/>	9	4.4.4.0/24	*	New_Intranet_Service-4	Intranet_Zone	YES	BR1	Static	-	-	5	0	Tonowhere	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 35 total entries)

In den Beispieldaten sehen wir, dass alle Routen innerhalb eines Dienstes mit einer gemeinsamen ECMP-Gruppe Teil dieser ECMP-Gruppe sind. Beispielsweise gehören 6.6.6.0/24 und 5.5.5.0/24 zur ECMP-Gruppe **Tonowhere**. Die Verkehrslast wird jedoch zwischen den Diensten **New_Intranet_Service-3** und **New_Intranet_Service-4** ausgeglichen, die sich eine Ziel-IP 5.5.5.0/24 teilen und derselben ECMP-Gruppe zugeordnet sind.

Hinweis

Für den SIA- und Zscaler-Dienst können Sie mit ECMP (Active/Active) den Lastenausgleich über zwei IPSec-Tunnelpfade durchführen.

Sicherheit

August 29, 2022

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:

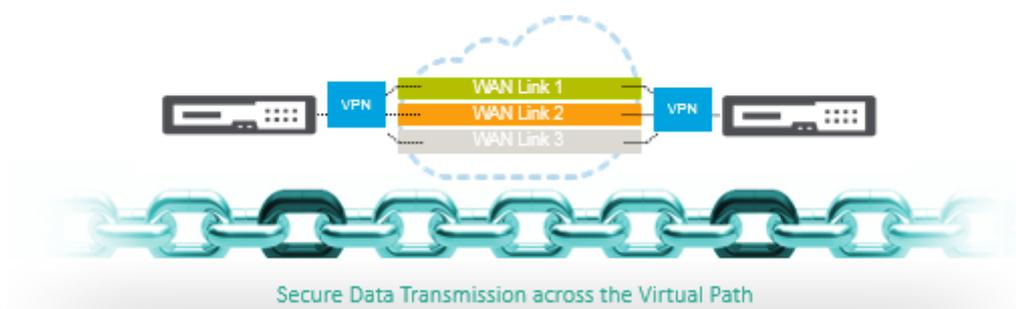
- [IPsec-Tunnel](#)
- [Firewall](#)

IPsec-Tunnelterminierung

August 29, 2022

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.



Wichtiger Hinweis:

- Ab Version SD-WAN 11.5 werden alle IPsec-Tunnelkonfigurationen und IKE-Einstellungen nur über den Citrix SD-WAN Orchestrator Service unterstützt. Informationen zu IPsec/IKE-Konfigurationen des Citrix SD-WAN Orchestrator Service finden Sie unter [IPsec-Dienst](#).

- Citrix SD-WAN unterstützt die Konnektivität zu Oracle Cloud Infrastructure (OCI) über IPsec.

Citrix SD-WAN Integration mit AWS Transit Gateway

November 16, 2022

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 nahebasieren Cloud-Ressourcen zu verbinden. Der **AWS Transit Gateway Network Manager** ändert dieses Paradigma. Citrix SD-WAN-Kunden, die AWS verwenden, können jetzt Citrix SD-WAN mit AWS Transit Gateway verwenden, indem sie die Citrix SD-WAN-Zweigstellen-Appliance AWS Transit Gateway integrieren, um Benutzern mit der Möglichkeit, alle mit dem Transit Gateway verbundenen VPCs zu erreichen.

Im Folgenden werden die Schritte beschrieben, um Citrix SD-WAN mit AWS Transit Gateway zu integrieren:

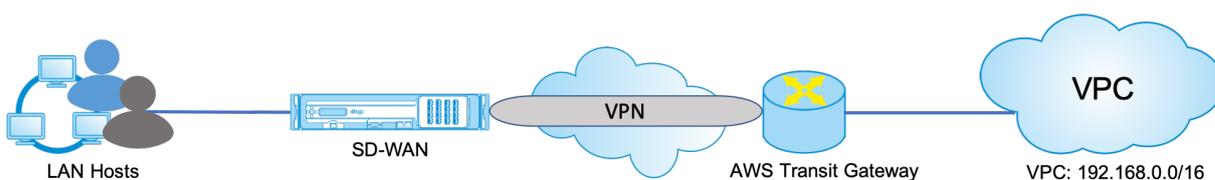
1. Erstellen Sie das AWS Transit Gateway.
2. Verbinden Sie ein VPN mit dem Transit Gateway (entweder vorhandenes oder ein neues VPN).
3. Verbinden Sie VPN mit dem konfigurierten Transit Gateway, an dem sich das VPN mit dem SD-WAN-Site befindet, der sich On-Prem oder in einer beliebigen Cloud befindet (AWS, Azure oder GCP).
4. Stellen Sie das Border Gateway Protocol (BGP) Peering über den IPsec-Tunnel mit dem AWS Transit Gateway von Citrix SD-WAN ein, um die mit Transit Gateway verbundenen Netzwerke (VPCs) zu lernen.

Anwendungsfall

Der Anwendungsfall besteht darin, Ressourcen, die in AWS (in jeder VPC) bereitgestellt werden, aus der Zweigstellenumgebung zu erreichen. Mit AWS Transit Gateway kann der Datenverkehr zu allen VPCs gelangen, die mit dem Transit Gateway verbunden sind, ohne BGP-Routen zu behandeln. Um dies zu erreichen, führen Sie die folgenden Methoden aus:

- Richten Sie die IPsec to AWS Transit Gateway über die Zweigstelle Citrix SD-WAN Appliance ein. Bei dieser Bereitstellungsmethode erhalten Sie keine vollständigen SD-WAN-Vorteile, da der Datenverkehr über IPsec geht.
- Stellen Sie eine Citrix SD-WAN Appliance in AWS bereit, und verbinden Sie sie über einen virtuellen Pfad mit Ihrer lokalen Citrix SD-WAN Appliance.

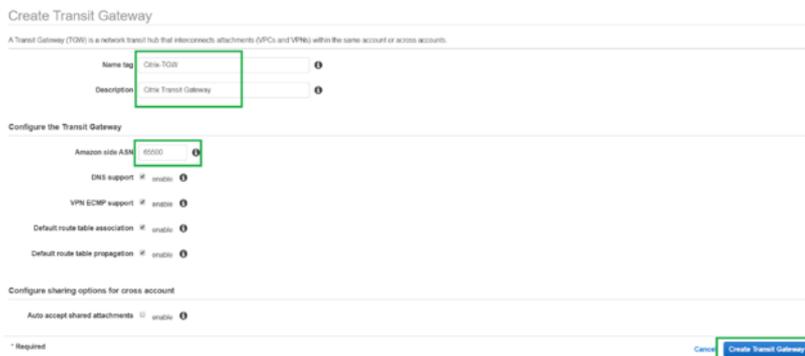
Unabhängig davon, welche Methode gewählt wird, erreicht der Datenverkehr zu den VPCs, die mit dem Transit Gateway verbunden sind, ohne das Routing innerhalb von AWS infra manuell zu verwalten.



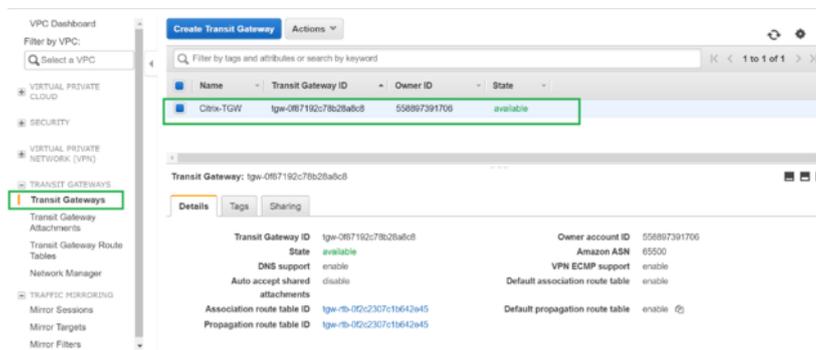
Konfiguration von AWS Transit Gateway

Um das **AWS Transit Gateway** zu erstellen, navigieren Sie zum VPC-Dashboard und wechseln Sie zum Abschnitt **Transit Gateway**.

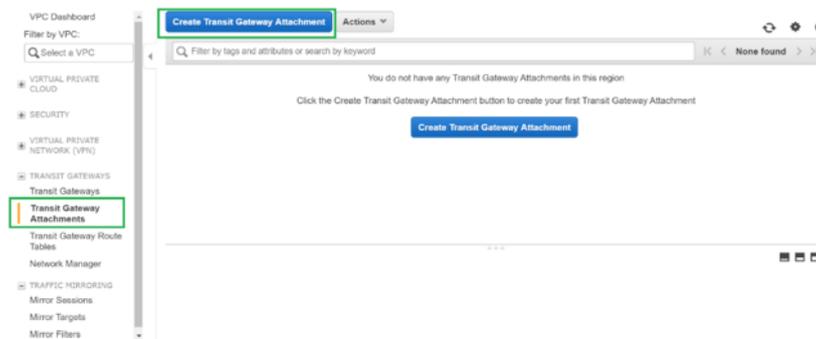
1. Geben Sie den Transit Gateway-Namen, die Beschreibung und die Amazon-ASN-Nummer wie im folgenden Screenshot hervorgehoben an, und klicken Sie auf **Transit Gateway erstellen**.



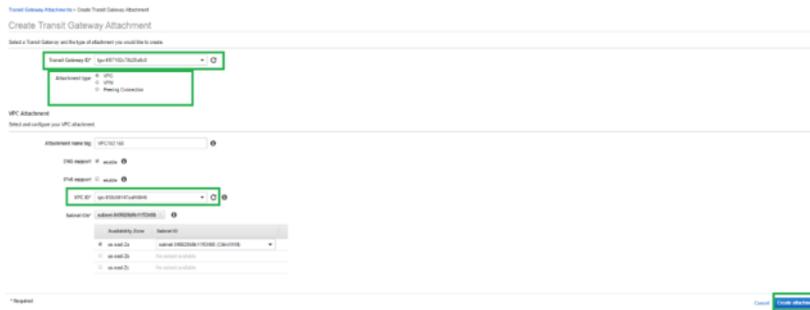
Sobald die Transit Gateway-Erstellung abgeschlossen ist, können Sie den Status als **Verfügbar** sehen.



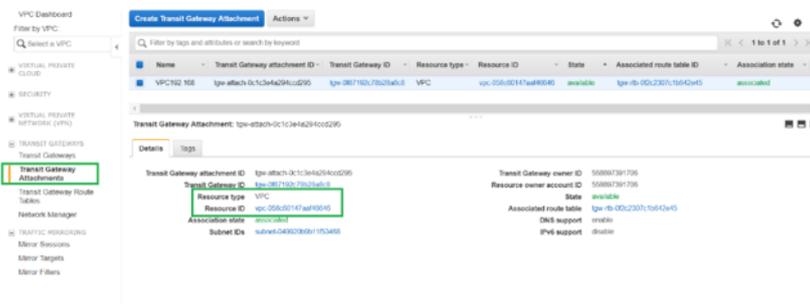
- Um die **Transit Gateway-Anhänge** zu erstellen, navigieren Sie zu **Transit Gateways > Transit Gateway Attachments** und klicken Sie auf **Transit-Gateway-Anlage erstellen**



- Wählen Sie das Transit Gateway aus der 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.

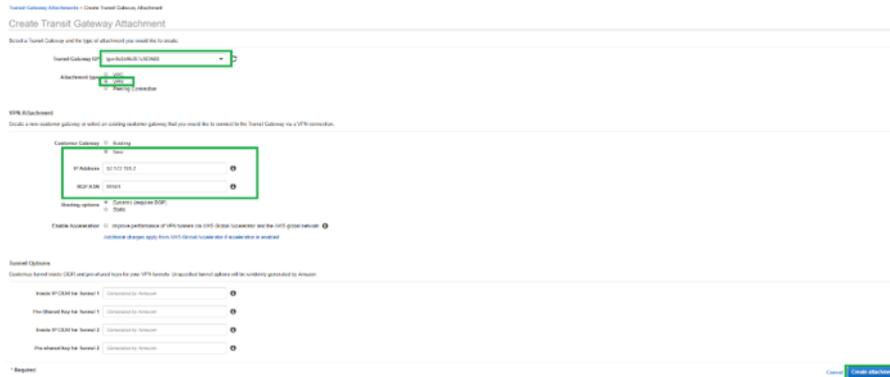


- Nachdem Sie die VPC an das Transit-Gateway angeschlossen haben, können Sie sehen, dass die **VPC des Ressourcentyps** mit dem Transit-Gateway verknüpft wurde.

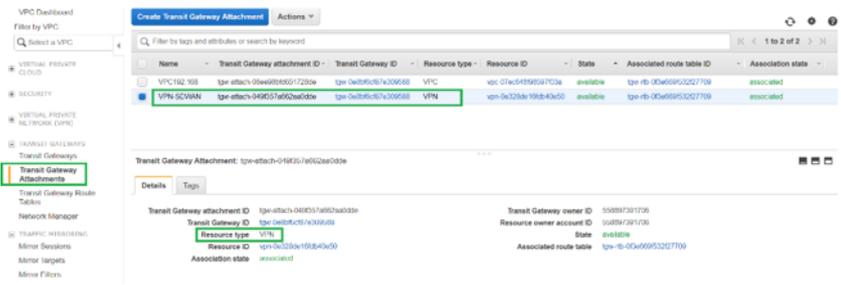


- Um SD-WAN über VPN an das Transit Gateway anzuschließen, wählen Sie die **Transit Gateway-ID** aus der Dropdownliste aus und wählen Sie **Anhangstyp** als **VPN** aus. Stellen Sie sicher, dass Sie die richtige Transit Gateway ID auswählen.

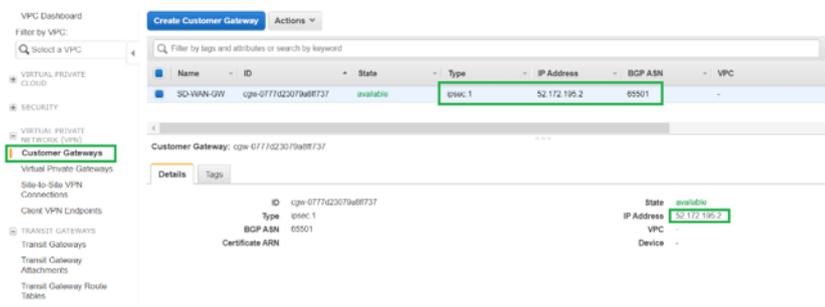
Fügen Sie ein neues VPN Customer Gateway hinzu, indem Sie die öffentliche IP-Adresse des SD-WAN-Links und die BGP-ASN-Nummer angeben. Klicken Sie auf **Anlage erstellen**, um VPN mit Transit Gateway zu verbinden.



- Sobald das VPN an das Transit Gateway angeschlossen ist, können Sie die Details sehen, wie im folgenden Screenshot gezeigt:

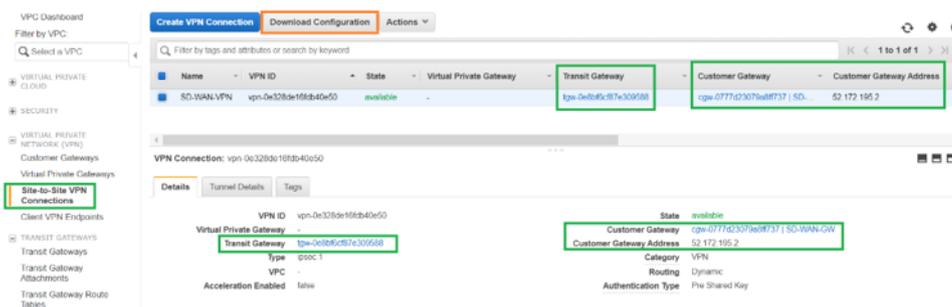


7. Unter **Customer Gateways** werden SD-WAN Customer Gateway und Site-to-Site VPN Connection als Teil von VPN Attachment to Transit Gateway erstellt. Sie sehen, dass das SD-WAN Customer Gateway zusammen mit der IP-Adresse dieses Customer Gateways erstellt wird, das die öffentliche WAN-Link-IP-Adresse von SD-WAN darstellt.

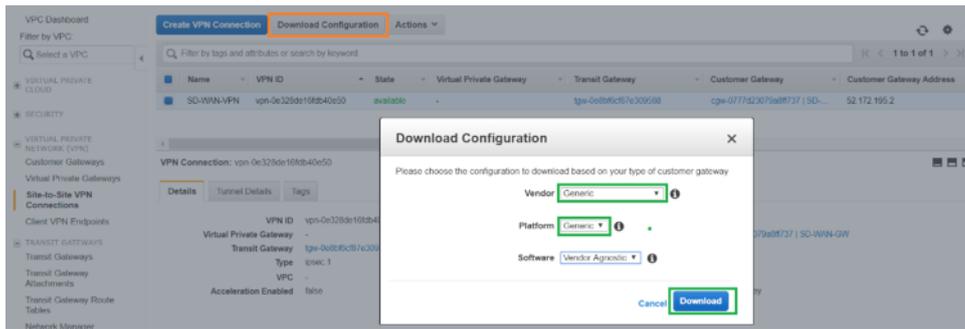


8. Navigieren Sie zu **Site-to-Site VPN Connections**, um die **VPN-Konfiguration des SD-WAN-Kunden-Gateways** Diese Konfigurationsdatei enthält zwei IPsec-Tunneldetails zusammen mit den BGP-Peer-Informationen. Zwei Tunnel werden aus SD-WAN zu Transit Gateway für Redundanz erstellt.

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 Agnostica**.



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:

[!Zwei IPsec-Tunnel](#)

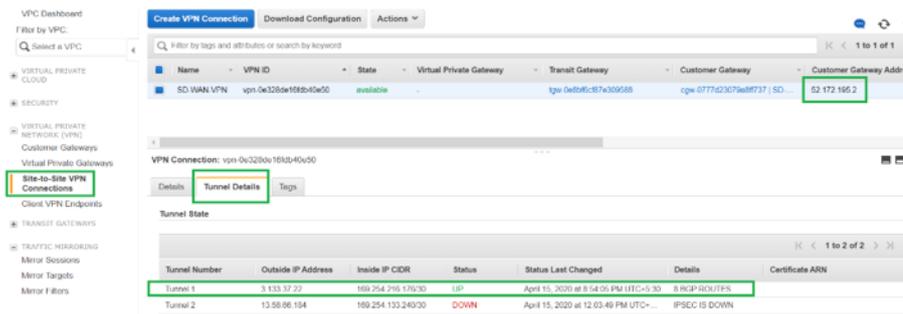
Konfigurieren des Intranetdienstes auf SD-WAN

Um einen Intranetdienst über den Citrix SD-WAN Orchestrator Service zu konfigurieren, gehen Sie zu [Bereitstellungsdienste](#).

Überwachung und Fehlerbehebung in AWS

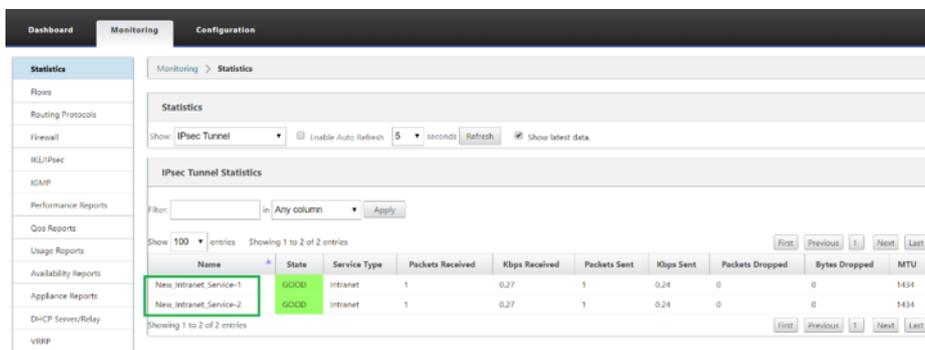
1. Um den Status der IPsec-Tunneleinrichtung auf AWS zu überprüfen, navigieren Sie zu **VIRTUAL PRIVATE NETWORK (VPN) > Site-to-Site VPN-Verbindungen**. Im folgenden Screenshot können Sie beobachten, dass die Customer Gateway-Adresse SD-WAN Link öffentliche IP-Adresse darstellt, mit der Sie Tunnel eingerichtet 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.

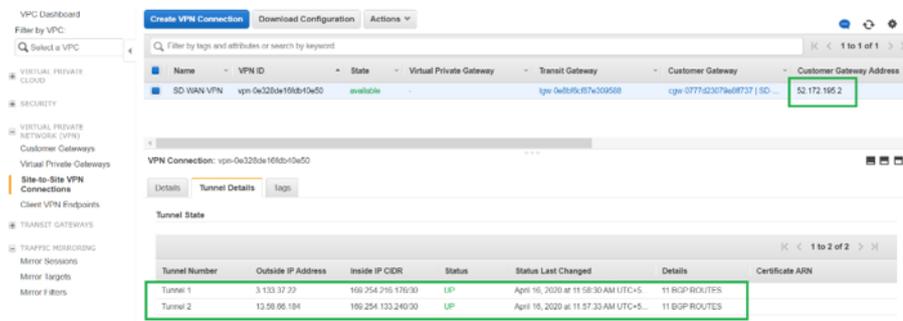


2. Konfigurieren Sie IPsec- und BGP-Details im Zusammenhang mit dem zweiten Tunnel basierend auf der heruntergeladenen Konfigurationsdatei auf SD-WAN.

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:



So zeigen Sie die IPsec-Tunnelkonfiguration an

August 29, 2022

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 aktiviert ist.

The screenshot shows the 'Configuration' page for 'Virtual WAN' with the 'View Configuration' tab selected. The 'View' dropdown is set to 'Virtual Path Service'. The main content area displays the 'Virtual Path Service Configuration' for 'Virtual Path 515' on 'HCN-5100-88372'. It lists various settings like 'Local site=HCN-5100', 'Remote site=88372', and 'IPsec settings=on'. Below this, there are two tables: one for 'PATHS' showing link details and another for 'Classes' showing traffic classification rules.

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alternate Src Port	Alternate Dst Port	IP DSCP	Encrypt	Loss	Percent	Sensitive To
0	HCN-5100-UL-1	88372-UL-1	172.111.64.5	172.111.39.5	-	-	4888	4888	-	-	-	+	ses128	YES	-
3	HCN-5100-UL-2	88372-UL-2	172.111.65.5	192.113.39.6	-	-	4888	4888	-	-	-	+	ses128	YES	-
1	HCN-5100-UL-1	88372-UL-2	172.111.64.5	192.113.39.6	-	-	4888	4888	-	-	-	+	ses128	YES	-
2	HCN-5100-UL-2	88372-UL-1	172.111.65.5	172.111.39.5	-	-	4888	4888	-	-	-	+	ses128	YES	-
0	88372-UL-1	HCN-5100-UL-1	172.111.39.5	172.111.64.5	-	-	4888	4888	-	-	-	+	ses128	YES	-
3	88372-UL-2	HCN-5100-UL-2	192.113.39.6	172.111.65.5	-	-	4888	4888	-	-	-	+	ses128	YES	-
1	88372-UL-1	HCN-5100-UL-2	172.111.39.5	172.111.65.5	-	-	4888	4888	-	-	-	+	ses128	YES	-
2	88372-UL-2	HCN-5100-UL-1	192.113.39.6	172.111.64.5	-	-	4888	4888	-	-	-	+	ses128	YES	-

3. Wählen Sie **IPsec-Tunnel** aus dem Dropdownmenü, um die IPsec-Tunnelkonfiguration anzuzeigen.

The screenshot shows the 'Configuration' page with the 'View' dropdown set to 'IPsec Tunnels'. The main content area displays the 'IPsec Tunnel Configuration' for 'VPN-ASA-1'. It lists various settings like 'ipsec_service_type=intranet', 'ike_local_ip_addr=10.0.0.6', and 'ipsec_tunnel_type=esp_auth'. At the bottom, it lists 'Protected Networks' with their respective IP ranges.

```

Name: VPN-ASA-1

ipsec_service_type=intranet
ike_local_ip_addr=10.0.0.6
ike_remote_ip_addr=10.101.0.100
network_mtu=1500
ike_version=2
ike_auth=psk
ike_identity=auto
ike_peer_auth=cert
ike_validate_peer_identity=1
ike_hash_algorithm=sha256
ike_integ_algorithm=sha256
ike_encryption_mode=aes256
ike_dhgroup=group2
ike_lifetime_s=300
ike_lifetime_s_max=86400
ike_dpd_s=300
ipsec_tunnel_mode=tunnel
ipsec_tunnel_type=esp_auth
ipsec_encryption_mode=aes128
ipsec_hash_algorithm=sha
ipsec_pfsgroup=none
ipsec_lifetime_s=28800
ipsec_lifetime_s_max=86400
ipsec_lifetime_kb=0
ipsec_lifetime_kb_max=0
ipsec_mismatch_behavior=drop
Protected Networks:
[1] 10.0.0.0/16 -> 10.101.0.0/16
[2] 10.4.0.0/16 -> 10.101.0.0/16
[3] 10.3.0.0/16 -> 10.101.0.0/16
[4] 10.2.0.0/16 -> 10.101.0.0/16
[5] 10.1.0.0/16 -> 10.101.0.0/16
    
```

4. Jeder virtuelle Pfad zeigt seinen eigenen IPsec-Tunnelstatus, wie unten gezeigt.

The screenshot shows the 'Monitoring' tab of the Citrix SD-WAN interface. It is divided into three sections:

- System Status:**
 - Name: MCN-5100
 - Model: 5100
 - Appliance Mode: MCN
 - Serial Number: 4H30GCNPD0
 - Management IP Address: 10.199.107.201
 - Appliance Uptime: 1 weeks, 3 days, 2 hours, 7 minutes, 28.6 seconds
 - Service Uptime: 6 hours, 21 minutes, 54.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions:**
 - Software Version: 10.0.0.193.659091
 - Built On: Feb 17 2018 at 17:32:45
 - Hardware Version: 5100
 - OS Partition Version: 4.6
- Virtual Path Service Status:**
 - Virtual Path MCN-5100-BR572: Uptime: 5 hours, 59 minutes, 34.0 seconds. IPsec state: GOOD.
 - Virtual Path MCN-5100-BR573: Uptime: 5 hours, 45 minutes, 0.0 seconds. IPsec state: GOOD.
 - Virtual Path MCN-5100-BR574: Uptime: 4 hours, 56 minutes, 48.0 seconds.
 - Virtual Path 'MCN-5100-BR575' is currently dead.
 - Virtual Path MCN-5100-RCN1-5100: Uptime: 2 hours, 7 minutes, 3.0 seconds.
 - Virtual Path 'MCN-5100-RCN3-2100' is currently dead (Configuration version mismatch)
 - Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.
 - Virtual Path 'MCN-5100-RCN4-ESxil' is currently dead.

IPsec-Überwachung und -Protokollierung

August 29, 2022

So überwachen Sie IPsec/IKE SA-Statistiken:

1. Navigieren Sie zu **Monitor > IPsec**. Wählen Sie **IPsec-SAs**:

The screenshot shows the 'IPsec Tunnel Statistics' table in the Citrix SD-WAN interface. The table has the following columns: Name, State, Service Type, Packets Received, Kbps Received, Packets Sent, Kbps Sent, Packets Dropped, Bytes Dropped, and MTU. The data is as follows:

Name	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropped	MTU
AS-TB-NCN-AS-TB-CL-1	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-2	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-3	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-4	GOOD	Conduit	0	0	0	0	0	0	1359
VPN-ASA-1	GOOD	Intranet	0	0	0	0	0	0	1427
VPN-ASA-2	GOOD	LAN	0	0	0	0	0	0	1377
VPN-PaloAlto	GOOD	Intranet	0	0	0	0	0	0	1439
VPN-SonicWall	GOOD	Intranet	0	0	0	0	0	0	1456

2. Navigieren Sie zu **Monitor > IKE SAs**. Beachten Sie die konfigurierten IPsec-Tunnel, die

IKE- und IPsec-Dienstzuordnungen zwischen zwei oder Modus-VPN-Endpunkten, die im SD-WAN-Netzwerk konfiguriert sind.

Name	Service Type	Intranet Service Type	Initiator Cookie	Responder Cookie	Host
IPv61-Tunnel_IPv61-Tunnel	Intranet	Default	5476506b6a5df0cf	0876d5a5e792790d	fdff8.cc:10:4500
IPv62-Tunnel_IPv62-Tunnel	Intranet	Default	b609da9c78244d04	95eb4dd7a3480166	edf8:cb:10:4500

So überwachen Sie IPsec-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

```

00028:948:324:607 INFO Current time is:Tue Mar 22 19:02:46 2016
00029:000:334:900 INFO Current time is:Tue Mar 22 19:03:46 2016
00029:000:345:638 INFO Current time is:Tue Mar 22 19:04:46 2016
00029:004:056:825 INFO Citrix_ikeStatMgr@forward/hosted/ipsec_host.c:3327 IKE SA CREATED (Virtual Path HON1-BR2CBZK): v=2, R_id=0xaf3151ca,rc=OK,next state=0000
00029:004:492:766 INFO Citrix_ikeStatMgr@forward/hosted/ipsec_host.c:3327 IKE SA CREATED (Virtual Path HON1-BR1): v=2, R_id=0xaf3151c9,rc=OK,next state=0000
00029:119:436:901 INFO Citrix_ikeStatMgr@forward/hosted/ipsec_host.c:3361 IKE SA DELETED (Virtual Path HON1-BR2CBZK): v=2, R_id=0xaf3151ca,rc=STATUS_IKE_DELETE_PAYLOAD,next state=0000
00029:119:041:550 INFO Citrix_ikeStatMgr@forward/hosted/ipsec_host.c:3361 IKE SA DELETED (Virtual Path HON1-BR1): v=2, R_id=0xaf3151c9,rc=STATUS_IKE_DELETE_PAYLOAD,next state=0000
00029:120:356:054 INFO Current time is:Tue Mar 22 19:05:46 2016
00029:180:366:422 INFO Current time is:Tue Mar 22 19:06:46 2016
00029:240:376:931 INFO Current time is:Tue Mar 22 19:07:46 2016
    
```

So werden IPsec-Tunnelwarnungen angezeigt

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.

The screenshot displays the configuration interface for Citrix SD-WAN 11.5, specifically the 'Logging/Monitoring' section under 'Appliance Settings'. The interface is divided into two main sections: 'Email Alerts' and 'General Event Configuration'.

Email Alerts Configuration:

- Enable Email Alerts (with a 'Send Test Email' button)
- Destination Email Address(es): [Text input field]
- SMTP Server Hostname or IP Address: [Text input field]
- SMTP Server Port: [Text input field, value: 25]
- Source Email Address: [Text input field]
- Enable SMTP Authentication
- SMTP User Name: [Text input field]
- SMTP Password: [Text input field]
- Verify SMTP Password: [Text input field]

General Event Configuration Table:

Event Type	Alert if State Persists	Email	Email Severity Filter	Syslog	Syslog Severity Filter	SNMP	SNMP Severity Filter
SERVICE	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
VIRTUAL_PATH	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
WAN_LINK	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
PATH	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
DYNAMIC_VIRTUAL_PATH	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
WAN_LINK_CONGESTION	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
USAGE_CONGESTION	0	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
HARD_DISK		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
APPLIANCE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
USER_EVENT		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
CONFIG_UPDATE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
SOFTWARE_UPDATE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
PROXY_ARP		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
ETHERNET		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
WATCHDOG		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
APPLIANCE_SETTINGS_UPDATE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
DISCOVERED_MTU		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
GRE_TUNNEL		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
IPSEC_TUNNEL		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
VIRTUAL_INTERFACE		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼
LICENSE_EVENT		<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼	<input type="checkbox"/>	Warning ▼

An 'Apply Settings' button is located at the bottom of the configuration area.

So überwachen Sie 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.

Dashboard | **Monitoring** | **Configuration**

- + Appliance Settings
- + Virtual WAN
- System Maintenance
 - Delete Files
 - Restart System
 - Date/Time Settings
 - Local Change Management
 - Diagnostics**
 - Update Software
 - Configuration Reset
 - Factory Reset

Configuration > System Maintenance > **Diagnostics**

Ping | Traceroute | Packet Capture | Path Bandwidth | System Info | Diagnostic Data | **Events** | Alarms | Diagnostics Tool

Insert Event

Object Type:

Event type:

Severity:

Download Events

There are currently 487678 in the Events database, spanning from event 183612 at 2018-01-18 18:24:55 to event 671289 at 2018-02-17 18:14:15. You can download some or all of them in CSV format. You may wish to limit the amount to download because some common spreadsheet programs limit you to 65,536 rows.

Download events starting from (487678 events)

Alert Count

Alert Type	Alerts Sent
Emails:	0
System Messages:	0
SNMP Traps:	0

View Events

Quantity:

Filter:

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
671289	0	MCN-5100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671288	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671287	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671286	2	MCN-5100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:14	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671285	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671284	0	MCN-5100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671283	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671282	2	MCN-5100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671281	3	MCN-5100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671280	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671279	1	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671278	2	MCN-5100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671277	2	MCN-5100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671276	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671275	3	MCN-5100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.
671274	1	MCN-5100-WL-1->BR574-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671273	3	MCN-5100-WL-2->BR574-WL-2	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from BAD to GOOD because notified by peer.
671272	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671271	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:06:08	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671270	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671269	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671268	3	MCN-5100-WL-2->BR574-WL-2	PATH	2018-02-17 18:05:57	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671267	1	MCN-5100-WL-1->BR573-WL-2	PATH	2018-02-17 18:05:58	GOOD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671266	3	MCN-5100-WL-2->BR572-WL-2	PATH	2018-02-17 18:05:09	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671265	1	MCN-5100-WL-1->BR573-WL-2	PATH	2018-02-17 18:04:58	BAD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.

Berechtigung für nicht-virtuelle IPsec-Pfadrouten

August 29, 2022

In früheren Versionen blieben ipsec-Tunnelrouten in der Routentabelle, selbst wenn der Tunnel nicht verfügbar wäre.

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

317

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain: Default_RoutingDomain

Filter: in Any column Apply

Show: 100 entries Showing 1 to 13 of 13 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11389	YES	N/A	N/A
3	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES	*	BRANCH2	Static	-	-	5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.186.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
11	0.0.0.0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

FIPS-Konformität

August 29, 2022

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

Informationen zum Aktivieren der FIPS-Konformität mithilfe des Citrix SD-WAN Orchestrator Service finden Sie unter [FIPS-Modus](#).

Secure Web Gateway für Citrix SD-WAN

August 29, 2022

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

November 16, 2022

Die Zscaler Cloud Security Platform fungiert als eine Reihe von Sicherheitskontrollen in mehr als 100 Rechenzentren auf der ganzen Welt. Indem Sie Ihren Internetverkehr einfach an Zscaler umleiten, können Sie Ihre Geschäfte, Filialen und Remotestandorte sofort sichern. Zscaler verbindet Benutzer und das Internet und überprüft jedes Byte des Datenverkehrs, auch wenn er verschlüsselt oder komprimiert ist.

Citrix SD-WAN-Appliances können über GRE-Tunnel am Standort des Kunden eine Verbindung zu einem Zscaler-Cloud-Netzwerk herstellen. Eine Zscaler-Bereitstellung mit SD-WAN-Appliances unterstützt die folgenden Funktionen:

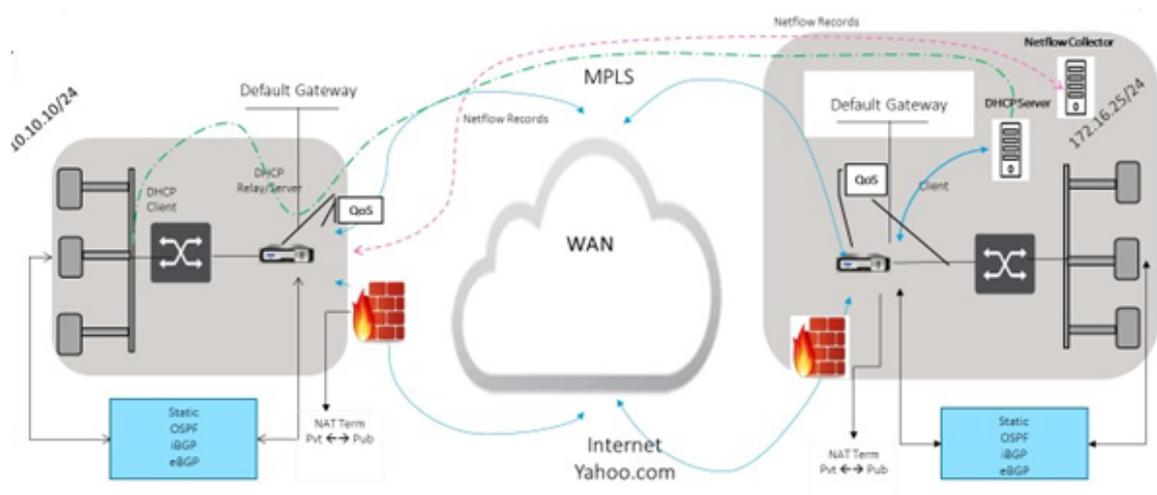
- Weiterleiten des gesamten GRE-Datenverkehrs an Zscaler, wodurch ein direktes Internetbreak-out möglich ist.
- Direkter Internetzugang (DIA) mit Zscaler pro Kundenstandort.
 - Auf einigen Websites möchten Sie DIA möglicherweise on-premises Sicherheitsausrüstung zur Verfügung stellen und Zscaler nicht verwenden.
 - Auf einigen Websites können Sie den Traffic auf einer anderen Kundenseite für den Internetzugang zurückholen.
- Virtuelle Routing- und Weiterleitungsbereitstellungen.
- Ein WAN-Link als Teil von Internetdiensten.

Zscaler ist ein Cloud-Dienst. Sie müssen es als Service einrichten und die zugrunde liegenden WAN-Links definieren:

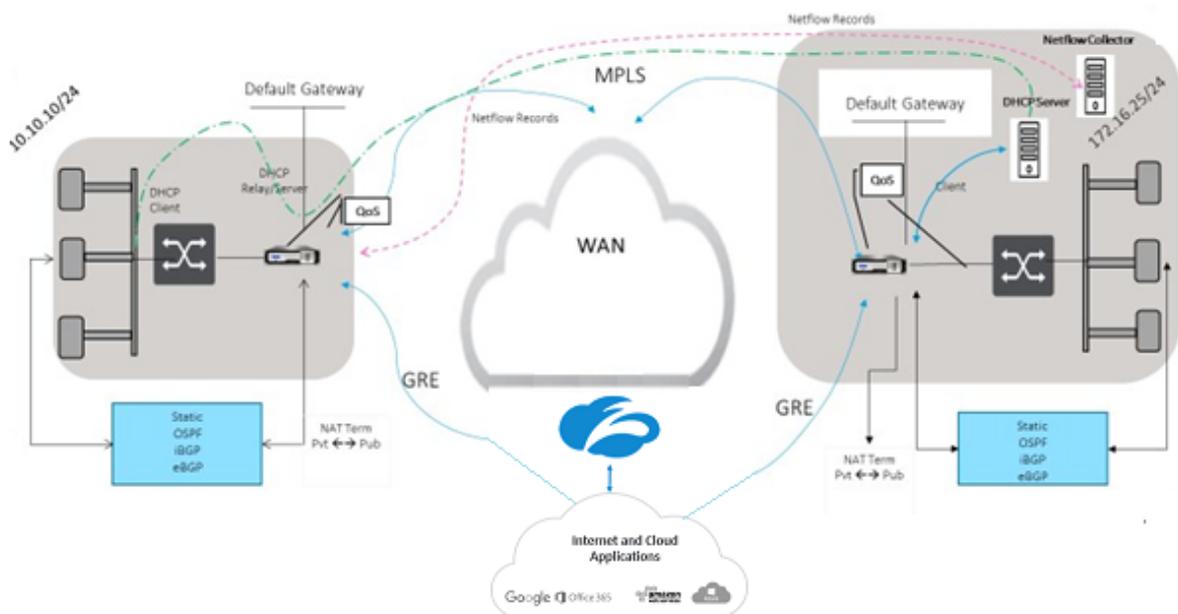
- Konfigurieren Sie einen Internetdienst im Rechenzentrum und verzweigen Sie über GRE.
- Konfigurieren Sie eine vertrauenswürdige öffentliche Internetverbindung im Rechenzentrum und an den Zweigstellen.

Topologie

CURRENT DEPLOYMENT MODEL WITH ON-PREMISE FIREWALL



ZSCALER SECURITY AS SERVICE DEPLOYMENT MODEL



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], auf 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

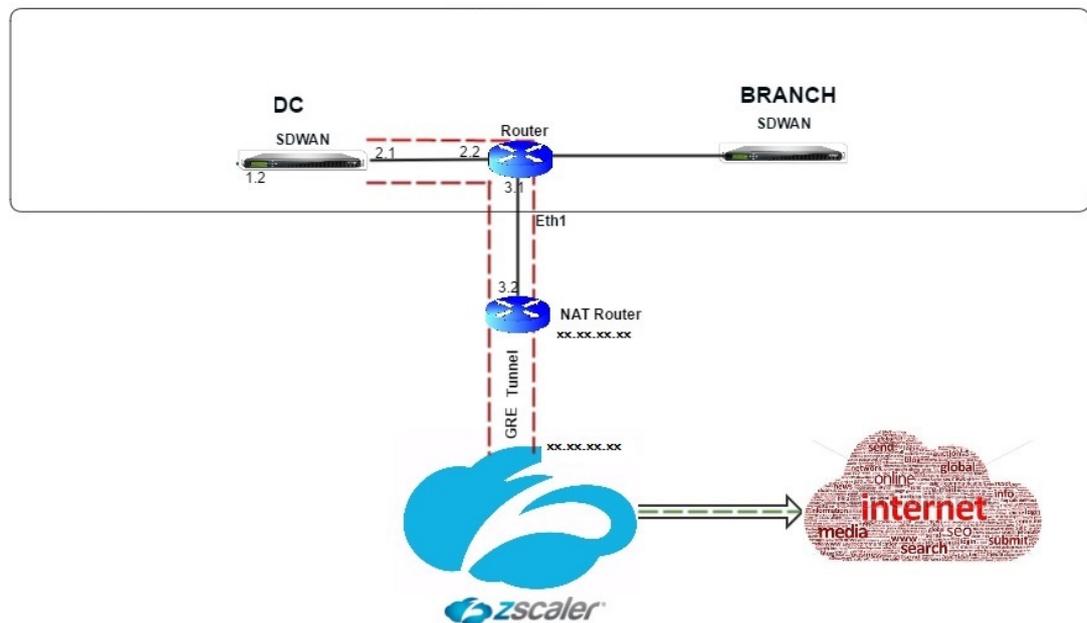
Interne ZEN-IP-Adresse: 172.17.6.246/30

Konfigurieren eines Internetdienstes

Informationen zum Konfigurieren eines Internetdienstes über den Citrix SD-WAN Orchestrator Service finden Sie unter [Bereitstellungsdienste](#). Weitere Informationen zum Aktivieren des Internetdienstes für eine Site finden Sie unter [Direct Internet Breakout](#).

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.



Informationen zum Konfigurieren des GRE-Tunnels über den Citrix SD-WAN Orchestrator Service finden Sie unter [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 für 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 hat 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.

Hinweis

Wenn Sie keine spezifischen Routen für die Zscaler-IP-Adresse haben, konfigurieren Sie das Routenpräfix 0.0.0.0/0 so, dass es mit der ZEN-IP-Adresse übereinstimmt, und leiten Sie es durch eine GRE-Tunnelkapselungsschleife. Diese Konfiguration verwendet die Tunnel in

einem Aktiv-Backupmodus. Mit den in der obigen Abbildung dargestellten Werten wechselt der Datenverkehr automatisch in den Tunnel mit Gateway-IP-Adresse 172.17.6.242. Konfigurieren Sie bei Bedarf eine virtuelle Backhaul-Pfadroute. Andernfalls setzen Sie das Keep-Alive-Intervall des Backup-Tunnels auf Null. Dies ermöglicht einen sicheren 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.

So überwachen Sie GRE- und IPSec-Tunnelstatistiken:

Navigieren Sie im SD-WAN-Webinterface zu **IPsec-Tunnel**.
Überwachung > Statistiken > [GRE-Tunnel]

Weitere Informationen finden Sie unter [Überwachung von IPSec-Tunneln](#) und [GRE-Tunneln](#).

Unterstützung der Firewall-Verkehrsumleitung mithilfe von Forcepoint in Citrix SD-WAN

August 29, 2022

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)

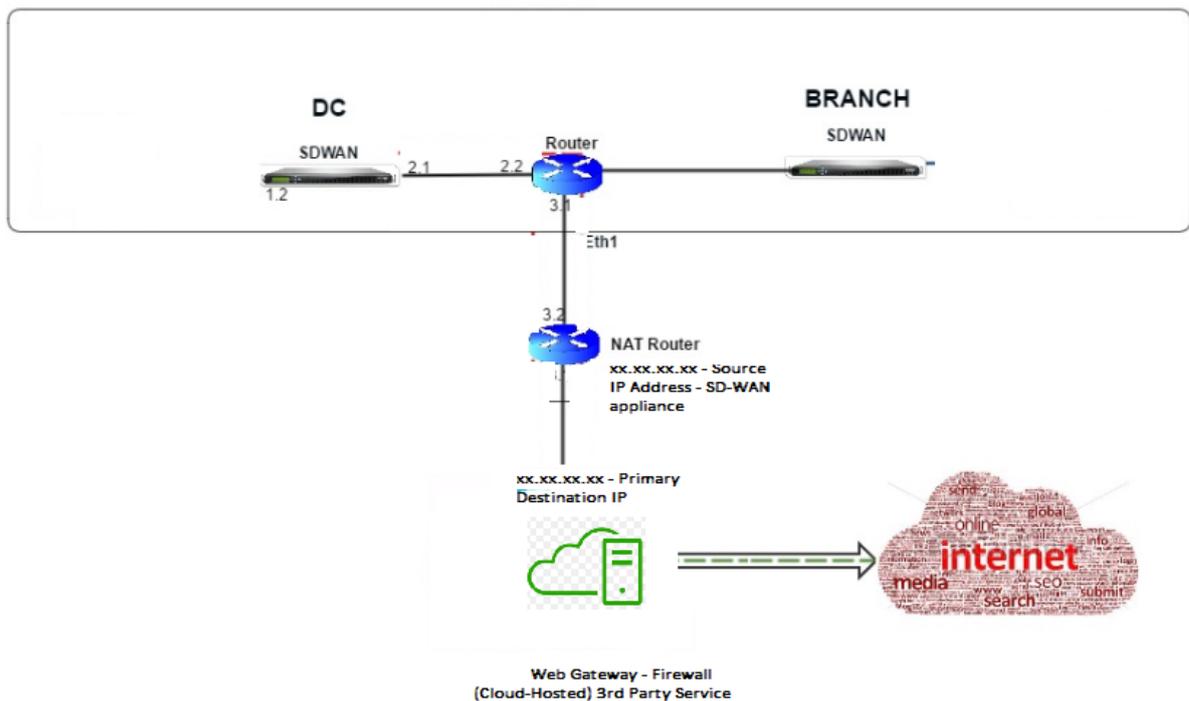
Die Ziel-NAT-Richtlinie ermöglicht es Unternehmen, den Internetverkehr mithilfe von ForcePoint über einen in der Cloud gehosteten Sicherheitsdienst weiterzuleiten.

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-Portalseite](#) an. 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.

Sie können NAT mit dem Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Netzwerkadressübersetzung](#).



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.

The screenshot shows the Citrix SD-WAN GUI. The top navigation bar includes Dashboard, Monitoring, and Configuration. The left sidebar shows various reports and configurations. The main content area is titled 'Monitoring > Firewall' and displays 'Firewall Statistics' and 'NAT Policies'.

Firewall Statistics

Statistics: NAT Policies
 Maximum entries to display: 50
 NAT: IP Protocol: Any, NAT Type: Any, Dynamic NAT Type: Any
 Service Type: Any, Service Name: Any
 Inside IP: *, Inside Port: *, Outside IP: *, Outside Port: *

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside		Outside		Allow Related	Allow IPsec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
							IP Address	Port	IP Address	Port									
1	Dynamic PR	-	Outbound	*	Internet	*	*	172.16.2.101/32	0-65535	No	No	No	253825	26477410	452674	614179776	3	[Connections]	

NAT Policies Displayed: 1
 NAT Policies In Use: 1/1000
 Port Restricted Dynamic NAT Policies In Use: 1/100
 Destination NAT Policies In Use: 0/100

Application	Family	IP Protocol	Source				Destination				State		
			IP Address	Port	Service Type	Service Name	IP Address	Port	Service Type	Service Name		Zone	
Domain Name Service(dns)	Network Service	UDP	172.16.6.10	38080	Virtual Path	DC-MCN-BR1-CB2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED
Domain Name Service(dns)	Network Service	UDP	172.16.16.1	58451	Virtual Path	DC-MCN-BR1-CB2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED

Palo Alto Integration mit IPsec-Tunneln

August 29, 2022

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 einschließen 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.

Stateful Firewall und NAT-Unterstützung

August 29, 2022

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 Flusstatus 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

Hinweis

Es wird aus Sicherheitsgründen nicht empfohlen, die Firewall im Fail-to-Wire-Inline-Modus zu

verwenden.

Globale Firewall-Einstellungen

August 29, 2022

Nachdem Sie die Firewall-Richtlinienvorlagen erstellt haben, können Sie diese Richtlinie verwenden, um Firewall-Einstellungen für das Citrix SD-WAN-Netzwerk zu konfigurieren. Mit den globalen Firewall-Einstellungen können Sie die globalen Firewallparameter konfigurieren. Diese Einstellungen werden auf alle Sites im virtuellen WAN-Netzwerk angewendet.

Erweiterte Firewall-Einstellungen

November 16, 2022

Sie können die erweiterten Firewall-Einstellungen für jede Site einzeln konfigurieren. Dadurch werden die globalen Einstellungen außer Kraft gesetzt.

Informationen zum Konfigurieren der erweiterten Firewall-Einstellungen auf Site-Ebene finden Sie unter [Firewall-Einstellungen](#).

Zonen

August 29, 2022

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:

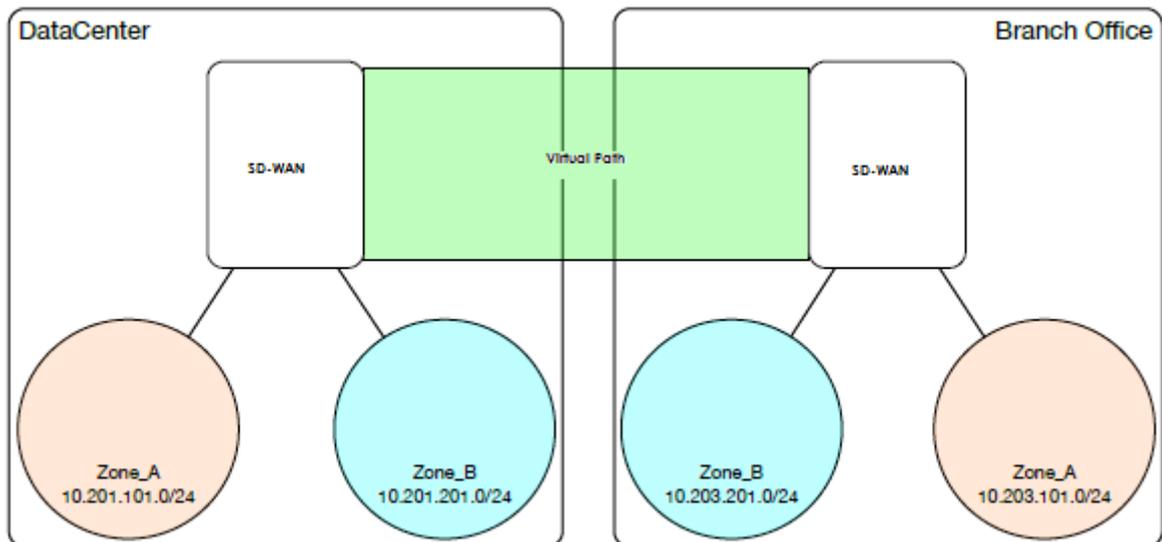
- Virtuelle Netzwerkschnittstellen (VNI)
- Intranetdienste
- GRE Tunnel
- LAN IPsec-Tunnel

Die 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 bietet 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.



Richtlinien

August 29, 2022

Richtlinien bieten die Möglichkeit, bestimmte Verkehrsströme zuzulassen, abzulehnen oder zu zählen und fortzusetzen. Sie können Firewall-Richtlinien über den Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Firewall-Richtlinien](#).

Netzwerkadressübersetzung (NAT)

August 29, 2022

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 über den Citrix SD-WAN Orchestrator Service 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. Weitere Informationen finden Sie unter [Netzwerkadressübersetzung](#).

Statische NAT

August 29, 2022

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.

Statische NAT-Richtlinien für den IPv6-Internetdienst

Citrix SD-WAN unterstützt ab Version 11.4.0 statische NAT-Richtlinien für den IPv6-Internetdienst. Eine statische NAT-Richtlinie für den IPv6-Internetdienst legt die Zuordnung eines internen Netzwerkpräfixes zu einem externen Netzwerkpräfix fest. Die Anzahl der erforderlichen statischen NAT-Richtlinien hängt von der Anzahl der internen Netzwerke und der Anzahl der externen Netzwerke (WAN-Verbindungen) ab. Wenn es eine **M-Anzahl** von internen Netzwerken und eine Anzahl von **N** WAN-Verbindungen gibt, beträgt die Anzahl der erforderlichen statischen NAT-Richtlinien **M x N**.

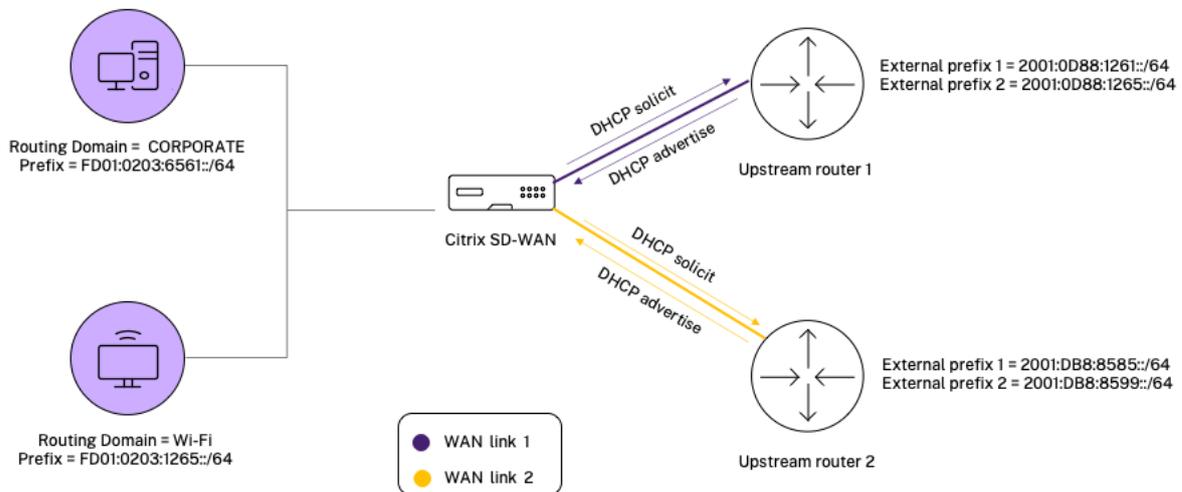
Ab Citrix SD-WAN Version 11.4.0 können Sie beim Erstellen einer statischen NAT-Richtlinie entweder die externe IP-Adresse manuell eingeben oder **Autolearn über PD** aktivieren. Wenn **Autolearn via PD** aktiviert ist, erhält die Citrix SD-WAN Appliance delegierte Präfixe vom Upstream-Delegierungsrouter über die DHCPv6-Präfix-Delegierung. Vor Citrix SD-WAN Version 11.4.0 wurde die externe IP-Adresse automatisch vom Dienst abgeleitet und es gab keine Möglichkeit, die externe IP-Adresse manuell einzugeben. Wenn Sie eine Appliance auf 11.4.0 oder eine höhere Version aktualisieren und statische NAT-Richtlinien für den IPv6-Internetdienst konfiguriert haben, müssen Sie die Richtlinien manuell aktualisieren.

Beispiel für eine Konfiguration

In der folgenden Topologie ist die Citrix SD-WAN-Appliance mit 2 internen Netzwerken und 2 WAN-Verbindungen konfiguriert:

- Innerhalb von Netzwerk 1 befindet sich in der Routing-Domäne CORPORATE mit dem Netzwerkpräfix FD01:0203:6561::/64

- Innerhalb von Netzwerk 2 befindet sich in der Wi-Fi-Routing-Domäne mit dem Netzwerkpräfix FD01:0203:1265::/64
- Über WAN Link 1 empfängt die SD-WAN-Appliance vom Upstream-Delegierungsrouter über DHCPv6-Präfix-Delegation 2 delegierte Präfixe 2001:0D88:1261::/64 und 2001:0D88:1265::/64. Diese 2 delegierten Präfixe werden als externe Netzwerkpräfixe verwendet, wenn der Verkehr von den inneren Netzwerken die WAN-Verbindung 1 überträgt.
- Über WAN Link 2 empfängt die SD-WAN-Appliance vom Upstream-Delegierungsrouter über die DHCPv6-Präfix-Delegation 2 delegierte Präfixe 2001:DB8:8585::/64 und 2001:DB8:8599::/64. Diese 2 delegierten Präfixe werden als externe Netzwerkpräfixe verwendet, wenn der Verkehr von den inneren Netzwerken die WAN-Verbindung 2 überträgt.

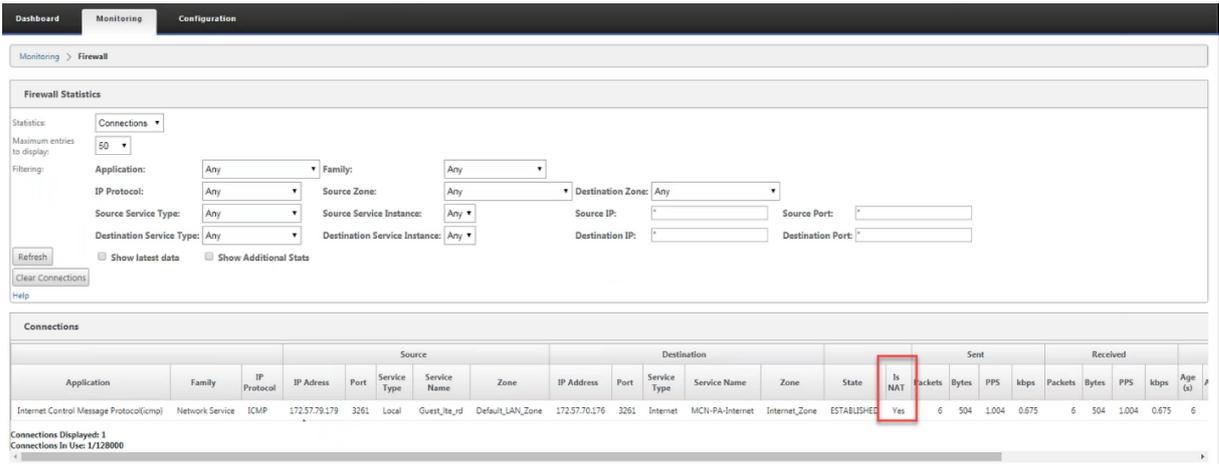


In diesem Szenario gibt es $M=2$ innerhalb von Netzwerken und $N=2$ WAN-Verbindungen. Daher beträgt die Anzahl der statischen NAT-Richtlinien, die für die ordnungsgemäße Bereitstellung des IPv6-Internetdienstes erforderlich sind, $2 \times 2 = 4$. Diese 4 statischen NAT-Richtlinien spezifizieren die Adressübersetzung für:

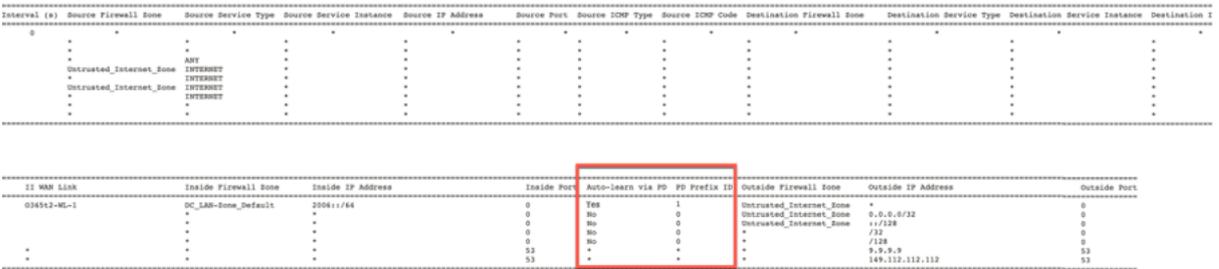
- Innerhalb von Netzwerk 1 über WAN-Verbindung 1
- Innerhalb von Netzwerk 1 über WAN-Verbindung 2
- Innerhalb von Netzwerk 2 über WAN-Verbindung 1
- Innerhalb von Netzwerk 2 über WAN-Link 2

Überwachen

Um NAT zu überwachen, navigieren Sie zu **Monitoring > Firewall-Statistiken > Verbindungen**. Für eine Verbindung können Sie sehen, ob NAT fertig ist oder nicht.

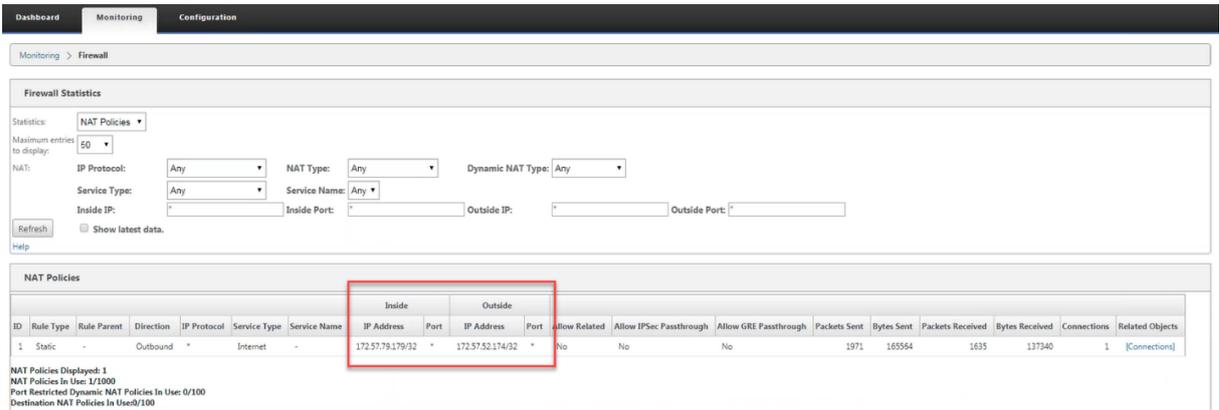


Um zu überprüfen, ob Auto-Learn via PD für eine NAT-Regel konfiguriert ist, navigieren Sie zu **Konfiguration > Virtuelles WAN > Konfiguration anzeigen** und wählen Sie **Firewall** aus der Dropdownliste **Ansicht. Automatisches Lernen über PD - und PD-Präfix-ID-Spalten** zeigen die Details an.



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**.

Der folgende Screenshot zeigt die Zuordnung von Innenadresse zu einer externen Adresse in einer statischen IPv4-NAT-Richtlinie.



Der folgende Screenshot zeigt die Zuordnung von Innenadresse zu einer externen Adresse in einer statischen IPv6-NAT-Richtlinie.

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any

Service Type: Any Service Name: Any

Inside IP: * Inside Port: * Outside IP: * Outside Port: *

Refresh Show latest data.

[Help](#)

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside		Outside		Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received
							IP Address	Port	IP Address	Port						
1	Static	-	Outbound	*	Internet	-	2006::/64	*	2004::/64	*	Yes	No	No	26	2144	0
2	Dynamic PR	-	Outbound	*	Internet	-	*	*	172.170.11.85/32	*	No	No	No	390832	71419346	409
3	Dynamic Sym	-	Outbound	*	Internet	-	*	*	2004::85/128	*	No	No	No	51	4112	0

NAT Policies Displayed: 3
 NAT Policies In Use: 3/1000
 Port Restricted Dynamic NAT Policies In Use: 2/100
 Destination NAT Policies In Use: 0/100

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. NAT-Protokolle enthalten die folgenden Informationen:

- Datum und Uhrzeit
- Routing-Domäne
- IP-Protokoll
- Quell-Port
- Quell-IP-Adresse
- Übersetzte IP-Adresse
- Übersetzter Port
- Ziel-IP-Adresse
- Destination port

Edit ? x

Priority: Policy Type:

Match Criteria

From Zones	To Zones		
Zone	Enable	Zone	Enable
Any	<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>	Default_LAN_Zone	<input type="checkbox"/>
gre_zone	<input type="checkbox"/>	gre_zone	<input type="checkbox"/>
Inter Routing Domain Zone	<input type="checkbox"/>	Inter Routing Domain Zone	<input type="checkbox"/>

Routing Domain:

Traffic Match Type: IP Protocol: DSCP: Match Established

Application: Application Family: Application Objects:

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

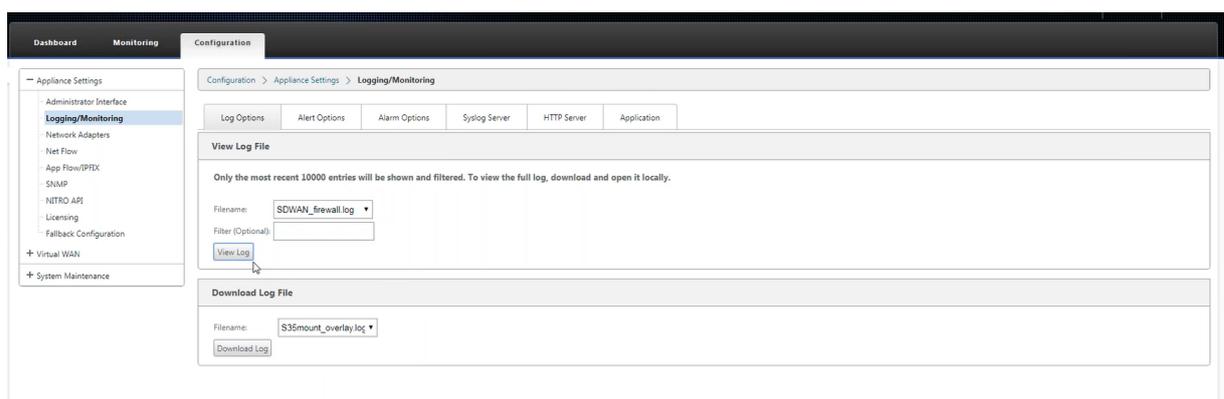
Actions

Action: Allow Fragments Connection State Tracking:

Logging & Other Options

Log Interval (s): Log Start Log End Add Reverse Policy

Um NAT-Protokolle zu generieren, navigieren Sie zu **Logging/Monitoring > Log Options**, wählen Sie **SDWAN_firewall.log** aus und klicken Sie auf **View Log**.



Die NAT-Verbindungsdetails werden in der Protokolldatei angezeigt.

```

2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/ FirewallConnection:18704 Removed 1 Connections
2020-05-11T10:15:44.750189+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)
2020-05-11T10:16:16.581504+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)
2020-05-11T10:16:21.299956+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 REQUEST 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:22.353441+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)
2020-05-11T10:20:22.374890+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)

2022-02-14T11:43:53.184990+0000 WARN find_and_update_connection@forward/firewall/connection.c:4828 Conn 0x7ffffdbf5f168 Aborted, NAT
2022-02-14T11:43:53.185044+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:43:53.565134+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:43:59.572977+0000 INFO t2_firewall_monitor.pl Connection DELETED for (Routing Domain Default_RoutingDomain) IPv6_ICMP
2022-02-14T11:45:12.399564+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) UDP 1
2022-02-14T11:45:48.516174+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:45:48.717951+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 488 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:18.786955+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:21.768939+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:21.761368+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 3 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:27.766610+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:32.774464+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:32.775063+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)

```

Dynamische NAT

November 16, 2022

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.

Port-Weiterleitung

Dynamische NAT mit Portweiterleitung ermöglicht es Ihnen, bestimmten Datenverkehr an eine definierte IP-Adresse weiterzuleiten. Dies wird normalerweise für Hosts wie Webserver verwendet. Sobald der dynamische NAT konfiguriert ist, können Sie die Portweiterleitungsrichtlinien definieren. Konfigurieren Sie dynamische NAT für die IP-Adressenübersetzung und definieren Sie die Portweiterleitungsrichtlinie, um einen externen Port einem internen Port zuzuordnen. Dynamische NAT-Portweiterleitung wird normalerweise verwendet, um Remotehosts die Verbindung zu einem Host oder Server in Ihrem privaten Netzwerk zu ermöglichen. Für einen detaillierteren Anwendungsfall siehe [Citrix SD-WAN Dynamic NAT erklärt](#).

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 mithilfe des Citrix SD-WAN Orchestrator Service. Weitere Einzelheiten finden Sie unter [Konfigurieren der Firewall-Segmentierung](#).
- Konfigurieren von DNS-Weiterleitungen oder DNS-Proxy im SD-WAN Orchestrator Service. 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.

The screenshot shows the 'Monitoring > Firewall' section with 'Firewall Statistics' selected. The 'Connections' table lists traffic details. The 'Is NAT' column is highlighted with a red box, showing 'Yes' for several entries.

Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	By
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	34202	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	140	0.008	0.004	2	4
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	42261	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	140	0.008	0.004	2	4
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	34058	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	114	0.008	0.004	2	2
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	50486	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	114	0.008	0.004	2	2
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	33928	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	124	0.008	0.004	2	2
Domain Name Service(dns)	Network Service	UDP	172.57.48.50	50354	Local	VF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	124	0.008	0.004	2	2

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.

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any, NAT Type: Any, Dynamic NAT Type: Any

Service Type: Any, Service Name: Any

Inside IP: *, Inside Port: *, Outside IP: *, Outside Port: *

Refresh Show latest data.

Help

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside IP Address	Port	Outside IP Address	Port	Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
1	Dynamic Sym	-	Outbound	*	Internet	-	*	*	172.147.12.83/32	*	No	No	No	0	0	0	0	0	0
2	Port Forward	1	Outbound	*	Internet	-	172.147.90.12/32	5001-5010	172.147.12.83/32	5001-5010	No	No	No	82	47232	8928	13374144	0	

NAT Policies Displayed: 2
 NAT Policies In Use: 2/1000
 Port Restricted Dynamic NAT Policies In Use: 0/100
 Destination NAT Policies In Use: 0/100

Wenn eine Portweiterleitungsregel erstellt wird, wird auch eine entsprechende Firewallregel erstellt.

Site: Branch1

Connections

WAN-to-WAN Forwarding

Virtual Paths

Dynamic Virtual Paths

Internet Service

Intranet Services

WAN Links

GRE Tunnels

IPsec Tunnels

Firewall

Application Routes

Routes

OSPF

BGP

Route Learning Properties

Inter Routing Domain Services

Multicast Groups

Applications

Pre-Appliance Template Policies

Local Policies

Priority	Routing Domain	Action	From	To	Application	Application Family	Application Objects	IP Protocol	DSCP	Service	IP Address	Port	Match	Add	Info	Edit	Delete	Clone
(auto)	*	Allow	*	*	*	*	*	Any	*	IP Host	*	*	*					
(auto)	*	Allow	Internet_Zone	*	*	*	*	Any	*	Internet	*	*	*	Yes				
(auto)	*	Allow	Internet_Zone	*	*	*	*	TCP (6)	*	Internet	0-65535	*	15.15.15.1	443				
(auto)	*	Allow	Internet_Zone	*	*	*	*	UDP (17)	*	Internet	0-65535	*	15.15.15.1	443				
(auto)	*	Drop	*	*	*	*	*	Any	*	Internet	*	*	*					

Post-Appliance Template Policies

Apply Refresh

Sie können die Statistiken der Filterrichtlinie anzeigen, indem Sie zu **Überwachung > Firewall-Statistiken > Filterrichtliniennavigieren**.

Monitoring > Firewall

Firewall Statistics

Statistics: Filter Policies

Maximum entries to display: 50

Filtering: Routing Domain: Any, Application: Any, Family: Any, IP Protocol: Any

Filter Policy Action: Any, Source Service Type: Any, Source Service Name: Any, Source IP: *

Source Port: *, Destination Service Type: Any, Destination Service Name: Any, Destination IP: *

Destination Port: *, Source Zone: Any, Destination Zone: Any, DSCP: Any

Refresh Show latest data.

Help

Filter Policies

Default Policy=Allow(Not Tracked) Packets=3414 Bytes=213489
 Match in Progress Packets=0 Bytes=0

ID	Routing Domain	Application	Family	IP Protocol	DSCP	Service Type	Service Name	IP Address	Port or ICMP Type	Zone	Service Type	Service Name	IP Address	Port or ICMP Code	Zone	Action	Conn Match Type	Track Connection	Allow Fragments	Log Connection Start	Log Connection End	Packets	Bytes	Related Objects
1	*	*	*	*	*	IPHost	-	*	NA	*	*	*	*	NA	*	Allow	Default	No	Yes	No	No	0	0	
2	*	*	*	*	*	Internet	-	*	NA	Internet_Zone	*	*	*	NA	*	Allow	Established	No	Yes	No	No	0	0	
3	*	*	*	TCP	*	Internet	-	*	*	Internet_Zone	*	*	15.15.15.1/32	443	*	Allow	Default	No	Yes	No	No	0	0	
4	*	*	*	UDP	*	Internet	-	*	*	Internet_Zone	*	*	15.15.15.1/32	443	*	Allow	Default	No	Yes	No	No	0	0	
5	*	*	*	*	*	Internet	-	*	NA	*	*	*	*	NA	*	Drop	Default	No	Yes	No	No	0	0	

Protokolle

Sie können Protokolle im Zusammenhang mit NAT in Firewall-Protokollen anzeigen. Um Protokolle für NAT anzuzeigen, erstellen Sie eine Firewallrichtlinie, die Ihrer NAT-Richtlinie entspricht, und stellen Sie sicher, dass die Protokollierung auf dem Firewallfilter aktiviert ist. NAT-Protokolle enthalten die folgenden Informationen:

- Datum und Uhrzeit
- Routing-Domäne
- IP-Protokoll
- Quell-Port
- Quell-IP-Adresse
- Übersetzte IP-Adresse
- Übersetzter Port
- Ziel-IP-Adresse
- Destination port

? x

Edit

Priority: Policy Type:

Match Criteria

From Zones	To Zones
Zone	Zone
Any <input checked="" type="checkbox"/>	Any <input checked="" type="checkbox"/>
Default_LAN_Zone <input type="checkbox"/>	Default_LAN_Zone <input type="checkbox"/>
gre_zone <input type="checkbox"/>	gre_zone <input type="checkbox"/>
Inter Routing Domain Zone <input type="checkbox"/>	Inter Routing Domain Zone <input type="checkbox"/>

Routing Domain:

Traffic Match Type: IP Protocol: DSCP: Match Established

Application: Application Family: Application Objects:

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

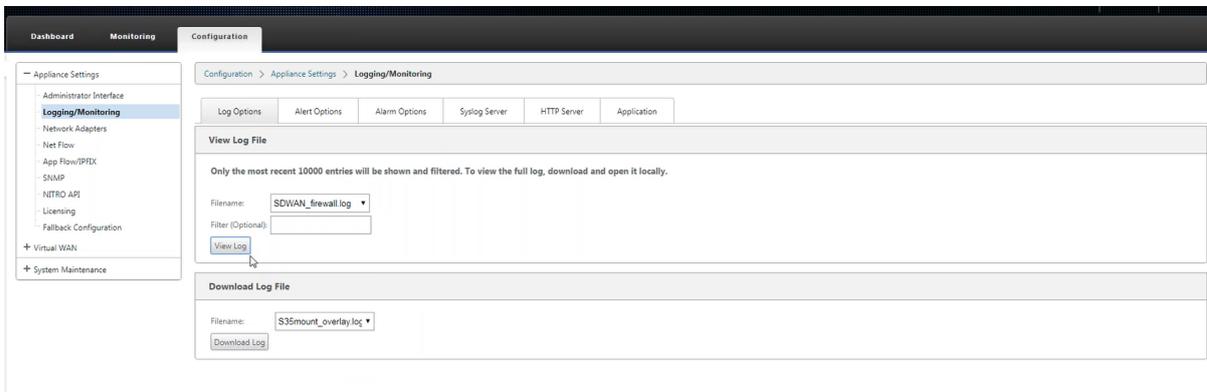
Actions

Action: Allow Fragments Connection State Tracking:

Logging & Other Options

Log Interval (s): Log Start Log End Add Reverse Policy

Um NAT-Protokolle zu generieren, navigieren Sie zu **Logging/Monitoring > Log Options**, wählen Sie **SDWAN_firewall.log** aus und klicken Sie auf **View Log**.



Die NAT-Verbindungsdetails werden in der Protokolldatei angezeigt.

```
2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/firewall/connection-18204 Removed 3 Connections
2020-05-11T10:15:44.759109+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)
2020-05-11T10:16:21.299056+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112659+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 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)
2020-05-11T10:20:22.374899+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)
2020-05-11T10:20:22.598378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.70.176 (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 REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 59 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.046123+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

August 29, 2022

Die Citrix SD-WAN-Konfiguration beschreibt und definiert die Topologie Ihres Citrix SD-WAN-Netzwerks. Informationen zum Konfigurieren des virtuellen WAN-Dienstes mit dem Citrix SD-WAN Orchestrator Service finden Sie unter [Flows](#).

Sicherheit und Verschlüsselung

Die Aktivierung der Verschlüsselung für SD-WAN (für die virtuellen Pfade) ist 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-Chiffren (Schlüsselgrößen) werden von den SD-WAN Appliances unterstützt und sind konfigurierbare Optionen.

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.

Konfigurieren der Firewall-Segmentierung

November 16, 2022

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. Ab SD-WAN 11.5-Version können Sie die Firewallsegmentierung mithilfe des Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Firewall-Segmentierung](#).

- 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.

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: 1/23

Both WAN Ingress and WAN Egress Flows Toggle Columns

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

Sie können auch die Routing-Tabelle für jede Routingdomäne unter **Monitor > Statistiken > Routen**überprüfen.

Routes for routing domain - Guest

Filter: in Any column

Show 100 entries Showing 1 to 5 of 5 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 5 of 5 entries

Anwendungsfälle

In früheren Citrix SD-WAN-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:

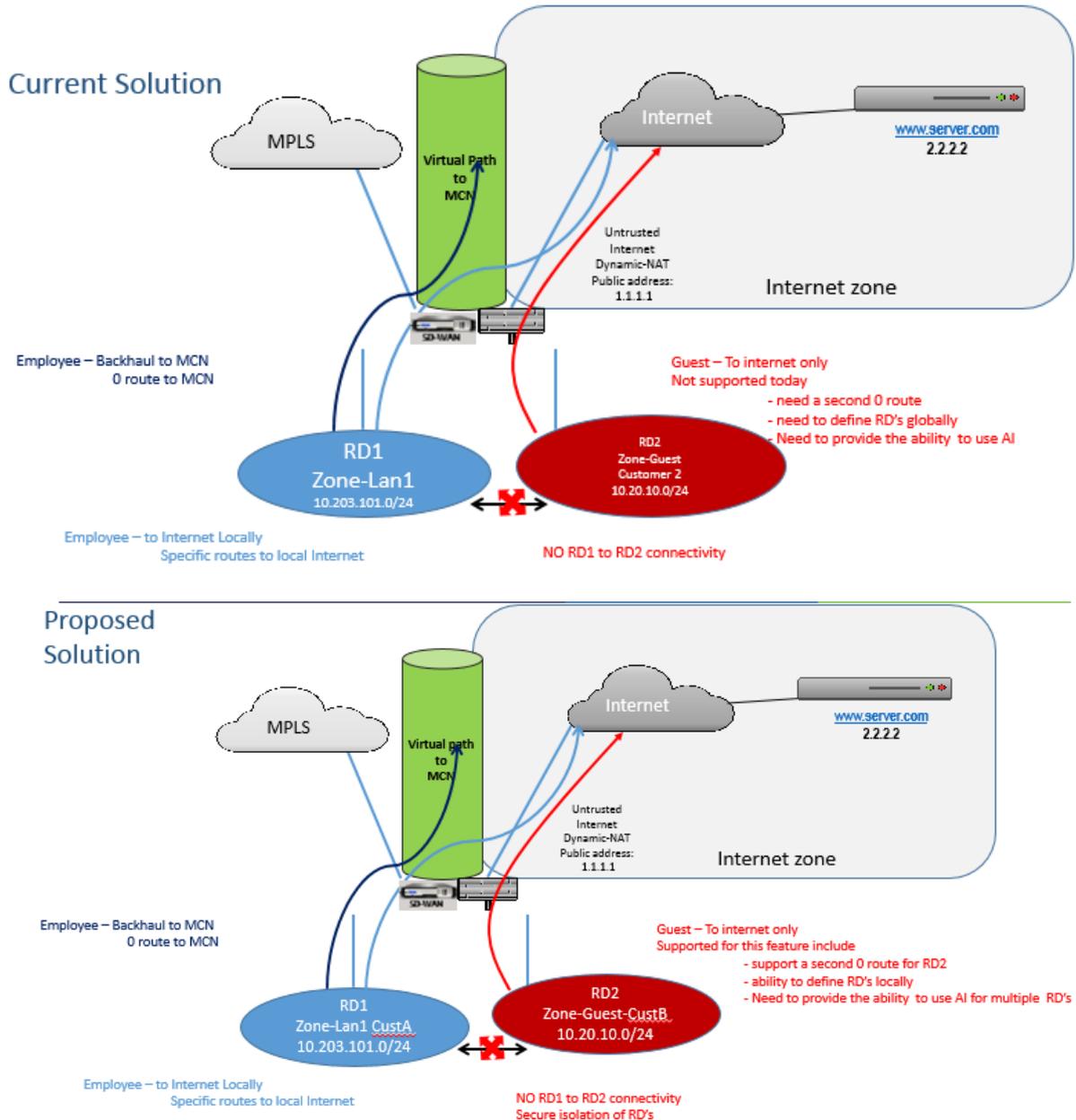
- Stellen Sie am Zweigstandort eine Infrastruktur bereit, die sichere Konnektivität für mindestens zwei Benutzergruppen wie Mitarbeiter und Gäste unterstützt. Die Infrastruktur kann bis zu 16 Routingdomänen unterstützen.
- Isolieren Sie den Traffic jeder Routingdomäne vom Traffic einer anderen Routingdomäne.
- 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 sicher, dass der Internetdienst richtig definiert wurde.

Bereitstellungsszenarios



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

August 29, 2022

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.

Die Zertifikatauthentifizierung ermöglicht es Unternehmen, von ihrer privaten Zertifizierungsstelle (CA) ausgestellte Zertifikate zur Authentifizierung von Appliances zu verwenden. 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.

Sie können die Zertifikatauthentifizierung Ihrer SD-WAN-Appliance mithilfe des Citrix SD-WAN Orchestrator Service aktivieren. Weitere Informationen zur Zertifikatauthentifizierung finden Sie unter [Zertifikatauthentifizierung](#).

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, sogenannte Flow Records, werden an einen oder mehrere IPv4- oder IPv6-Collector 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](#).

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, Dienstyp, 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 und 613 zum Exportieren von IPv4-IPFIX-Flussdaten, 615 und 616, um IPv6-IPFIX-Flussdaten zusammen mit der Optionsvorlage 612 zu exportieren.

Application Flow Info (IPFIX) exportiert Datensätze gemäß Vorlagen 611 für IPv4-Flüsse, 615 für IPv6-Flüsse und 612-Optionsvorlage mit Anwendungsinformationen.

Basic Properties (IPFIX) exportiert Datensätze gemäß Vorlagen 613 für IPv4-Flüsse und 616 für IPv6-Flüsse.

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	
Ipv4 DST IP	destinationIpv4Address, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	Stellen Sie auf 4 ein.
IP-Protokollnummer	protocolIdentifier, 4	Unsigned8, 1	
Padding	Nicht zutreffend	Unsigned16, 2	
SRC-Port	sourceTransportPort, 7	Unsigned16, 2	
DST-Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte-Anzahl	octetDeltaCount, 1	Unsigned64, 8	
Zeit für den ersten Pkt in Mikrosekunden	flowStartMicroseconds, 154	dateTimeMicroseconds, 8	
Zeit für lastpkt in Mikrosekunden	flowEndMicroseconds, 155	dateTimeMicroseconds, 8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow-Flags	tcpControlBits, 6	Unsigned8, 2	Derzeit auf 0 eingestellt.
Fließrichtung	flowDirection, 61	Unsigned8, 1	0x00: ingress flow 0x01: egress flow WAN-WAN und LAN-LAN flows sind in SDWAN möglich

Infoelement (IE)	IE Name & ID	Typ und len	Beschreibung
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	
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indikator	flowKeyIndicator, 173	Unsigned64, 8	Stellen Sie auf 0x1E037F.

Infoelement (IE)	IE Name & ID	Typ und len	Beschreibung
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.

Template-ID — 615 (IPv6-Flüsse) |Infoelement (IE)|Name und ID des IE|Typ und len|Kommentar|

|---|

|Beobachtungspunkt-ID|observationPointId, 138|Unsigned32, 4|

|Prozess-ID exportieren|exportingProcessId, 144|Unsigned32, 4|

|Flow-ID|flowId, 148|Unsigned64, 8|

|IPv6-SRC IP|sourceIPv6Address, 27|Ipv6address, 16|

|Ipv6 DST IP|destinationIpv6Address, 28|Ipv6address, 16|

|Ipversion|ipVersion, 60|Unsigned8, 1|Set to 6|

|IP protocol number|protocolIdentifier, 4|Unsigned8, 1|

|Padding|N/A|Unsigned16, 2|

|SRC Port|sourceTransportPort, 7|Unsigned16, 2|

|DST Port|destinationTransportPort, 11|Unsigned16, 2|

|Pkt Count|packetDeltaCount, 2|Unsigned64, 8|

|Byte Count|octetDeltaCount, 1|Unsigned64, 8|

|Time for first pkt in microseconds|flowStartMicroseconds, 154|dateTimeMicroseconds, 8|

|Time for lastpkt in microseconds|flowEndMicroseconds, 155|dateTimeMicroseconds, 8|

|IP ToS|ipClassOfService, 5|Unsigned8, 1|

|Flow Flags|tcpControlBits, 6|Unsigned8, 2|Currently set to 0.|

|Flow Direction|flowDirection, 61|Unsigned8, 1|0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN|

|Input Interface|ingressInterface, 10|Unsigned32, 4| Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combina-

tions. |

|Output Interface|egressInterface, 14|Unsigned32, 4|Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations. |

|Input Vlan ID|vlanId, 58|Unsigned16, 2| |

|Output Vlan ID|postVlanId, 59|Unsigned16, 2| |

|VRF ID|ingressVRFID, 234|Unsigned32, 4| |

|Flow Key Indicator|flowKeyIndicator, 173|Unsigned64, 8|Set to 0x1E037F. |

|Application ID|applicationId, 95|octetArray, variable|The Application ID is same as the ID of the applications classified by the DPI engine. Die Anwendungs-IDs bleiben konstant. Die Anwendungs-IDs für auf benutzerdefinierten Domänennamen basierenden Anwendungen ändern sich bei jedem Konfigurationsupdate. |

Vorlage 612 (Vorlage für Optionen)

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.

Basic Properties (IPFIX) —V9-konforme Vorlage - Vorlage 613 (IPv4-Flüsse)

Infoelement (IE)	IE Name & ID	Typ und len	Kommentar
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Address, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP-Protokollnummer	protocolIdentifier, 4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Fließrichtung	flowDirection, 61	Unsigned8, 1	0x00: ingress flow 0x01: egress flow WAN-WAN und LAN-LAN flows sind in SDWAN möglich
SRC-Port	sourceTransportPort, 7	Unsigned16, 2	
DST-Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte-Anzahl	octetDeltaCount, 1	Unsigned64, 8	
Eingangsschnittstelle	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN -Lastenausgleich Datenflüsse über mehrere Elementpfade, daher kann ein einzelner Datenfluss mehrere Eingabe-/Ausgabe-Schnittstellenkombinationen aufweisen.

Infoelement (IE)	IE Name & ID	Typ und len	Kommentar
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	

Template-ID — 616 (IPv6-Flüsse) |Infoelement (IE)|Name und ID des IE|Typ und len|Kommentar|
|-|-|-|
|IPv6-SRC IP|sourceIPv6Address, 27|Ipv6address, 16|
|Ipv6 DST IP|destinationIpv6Address, 28|Ipv6address, 16|
|Ipversion|ipVersion, 60|Unsigned8, 1|Set to 6| |
|IP protocol number|protocolIdentifier,4|Unsigned8, 1| |
|IP ToS|ipClassOfService, 5|Unsigned8, 1| |
|Flow Direction|flowDirection, 61|Unsigned8, 1|0x00: ingress flow0x01: egress flowWAN-WAN and
LAN-LAN flows are a possibility in SDWAN|
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through
multiple member paths, hence a single data flow can have multiple input/output interface combina-			
tions.			
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through
multiple member paths, hence a single data flow can have multiple input/output interface combina-			
tions.			
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

Einschränkungen

- AppFlow unterstützt keine IPv6-Collector- und Flow-Datensätze.
- 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 nur über den Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [AppFlow und IPFIX](#).

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.

The screenshot displays the Citrix SD-WAN 11.5 Configuration interface. The left-hand navigation pane shows the 'Logging/Monitoring' section expanded. The main content area is titled 'Configuration > Appliance Settings > Logging/Monitoring'. It features five tabs: 'Log Options', 'Alert Options', 'Alarm Options', 'Syslog Server', and 'HTTP Server'. The 'View Log File' section includes a warning: 'Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally'. It has a 'Filename:' dropdown menu set to 'SDWAN_export.log', a 'Filter (Optional):' text input field, and a 'View Log' button. The 'Download Log File' section also has a 'Filename:' dropdown menu set to 'SDWAN_export.log' and a 'Download Log' button.

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.

The screenshot shows the Citrix SD-WAN Configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar shows 'Appliance Settings' with sub-items: Administrator Interface, Logging/Monitoring, Network Adapters, Net Flow, App Flow, **SNMP**, NITRO API, Licensing, Virtual WAN, and System Maintenance. The main content area is titled 'Configuration > Appliance Settings > SNMP'. It features a 'Managers' tab and a 'Download MIB File' button. The 'SNMP' section contains the following fields: UDP Port (161), System Description (Citrix Virtual WAN Appliance), System Contact (support@citrix.com), and System Location (Citrix). Below this are two sections: 'SNMP v1/v2' and 'SNMP v3'. The 'SNMP v1/v2' section has an unchecked 'Enable v1/v2 Agent' checkbox, a 'Community String' field (public), an unchecked 'Enable v1/v2 Traps' checkbox, a 'Send v1/v2 Test Trap' button, a 'Destination IP Address(es)' field, and a 'Port' field (162). The 'SNMP v3' section has an unchecked 'Enable v3 Agent' checkbox, 'User Name', 'Password', and 'Verify Password' fields, 'Authentication' (MD5) and 'Encryption' (None) dropdowns, an unchecked 'Enable v3 Traps' checkbox, a 'Send v3 Test Trap' button, 'Destination IP Address(es)', 'Port' (162), and another set of 'User Name', 'Password', 'Verify Password', 'Authentication' (MD5), and 'Encryption' (None) fields. An 'Apply Settings' button is located at the bottom.

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

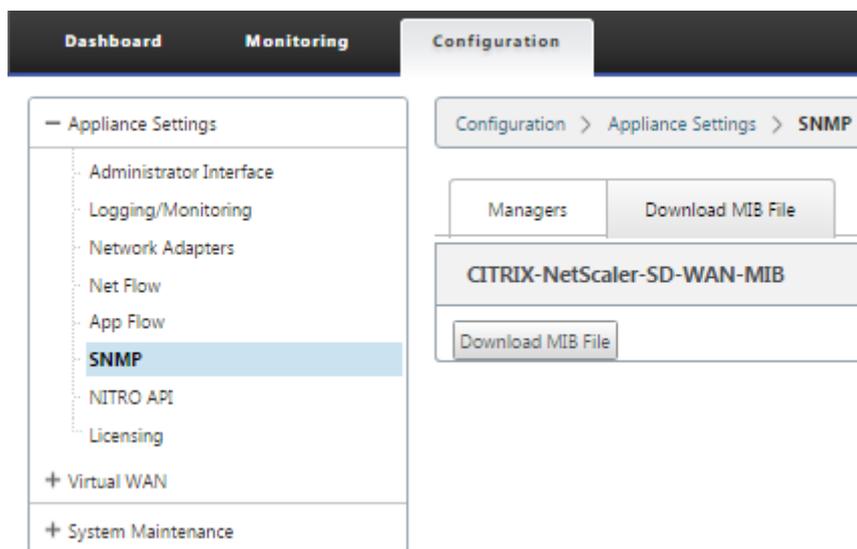
Sie müssen die folgenden SNMP-Dateien herunterladen, bevor Sie mit der Überwachung einer Citrix SD-WAN-Appliance beginnen können:

- 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.

Administrative Schnittstelle

August 29, 2022

Sie können Ihre Citrix SD-WAN-Appliances mit den folgenden Verwaltungsoptionen über Citrix SD-WAN Orchestrator Service verwalten und warten. Weitere Informationen finden Sie unter [Appliance-](#)

Einstellungen.

- 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 Lese-/Schreibzugriff nur für die Firewall und sicherheitsbezogene Einstellungen, während er schreibgeschützten Zugriff auf die verbleibenden 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 verfügt über Lese- und Schreibberechtigungen für alle Abschnitte und kann eine Zweigstelle mit Ausnahme der Firewall- und sicherheitsbezogenen Einstellungen 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.

The screenshot displays the Citrix SD-WAN VPX-50-SE administrator interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' section is active, showing a breadcrumb trail: 'Configuration > Appliance Settings > Administrator Interface'. Below this, there are tabs for 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', 'HTTPS Settings', and 'Miscellaneous'. The 'User Accounts' tab is selected, and the 'Change Local User Password' section is visible. This section contains a dropdown menu for 'User Name' (set to 'admin'), and three input fields for 'Current Password', 'New Password', and 'Confirm New Password'. A 'Change Password' button is located below these fields. Below the password change section is the 'Delete Workspace For User' section, which includes a dropdown for 'User Name' (set to 'admin') and a 'Delete Selected User's Workspace' button. The 'Manage Users' section features an 'Add User...' button, a note stating 'Deleting a user will also delete local files for that user.', a dropdown for 'User Name', and a 'Delete Selected User' button. Finally, the 'Firewall Access' section has a dropdown for 'User Name' (set to 'admin') and a 'Disable Firewall Access' button.

Benutzer hinzufügen

Um einen Benutzer hinzuzufügen, klicken Sie im Abschnitt **Benutzerverwalten** auf **Benutzerhinzufügen**. 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**.



Configuration > Appliance Settings

Add a New User Account

User Name: newuser

Password:

Confirm Password:

User Level: **Admin** (selected), Viewer, Security Admin, Network Admin

Apply Cancel

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**.

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**.

Configuration > Appliance Settings > Administrator Interface

User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous
---------------	--------	---------	------------	----------------	---------------

RADIUS

Enable RADIUS:

Server 1 IP Address: Authentication Port:

Server 2 IP Address (Optional): Authentication Port:

Server 3 IP Address (Optional): Authentication Port:

Server Key:

Confirm Server Key:

Timeout (seconds): (Optional)

Test RADIUS Server Connection

User Name:

Password:

TACACS+ Server

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

So konfigurieren Sie den TACACS+-Server:

1. 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**.

Configuration > Appliance Settings > Administrator Interface

User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous
---------------	--------	---------	------------	----------------	---------------

TACACS+

Enable TACACS+

Server 1 IP Address: Authentication Port:

Server 2 IP Address (Optional): Authentication Port:

Server 3 IP Address (Optional): Authentication Port:

Authentication Type: PAP ASCII

Server Key:

Confirm Server Key:

Timeout (seconds): (Optional)

Test TACACS+ Server Connection

User Name:

Password:

NDP-Router-Werbung und Präfix-Delegationsgruppe

November 16, 2022

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.

Sie können die NDP-Routerankündigung mit dem Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Ankündigung des NDP-Routers](#).

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.

Sie können die Präfixdelegierung über den Citrix SD-WAN Orchestrator Service konfigurieren. Weitere Informationen finden Sie unter [Präfix-Delegierungsgruppen](#).

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](#)

- [Configuration](#)
- [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](#)
- [Zero-Touch-Bereitstellung](#)

Konfiguration der Zugriffsschnittstelle

August 29, 2022

Informationen zum Konfigurieren der Zugriffsschnittstelle über den Citrix SD-WAN Orchestrator Service finden Sie unter [WAN-Links](#).

Virtuelle IP-Adressen konfigurieren

August 29, 2022

Informationen zum Konfigurieren virtueller IP-Adressen über den Citrix SD-WAN Orchestrator Service finden Sie unter [WAN-Links](#).

GRE Tunnel konfigurieren

August 29, 2022

Informationen zum Konfigurieren von GRE-Tunneln mit dem Citrix SD-WAN Orchestrator Service finden Sie unter [GRE-Dienst](#).

Dynamische Pfade für Zweigkommunikation einrichten

November 16, 2022

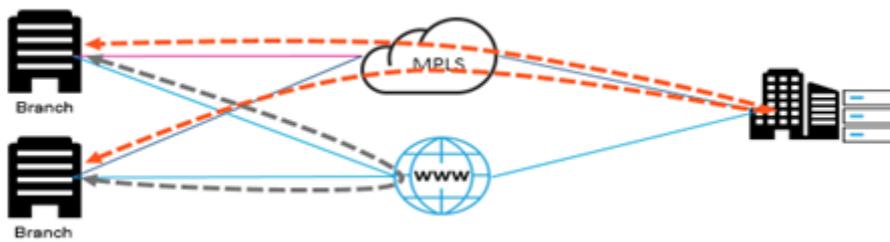
Angesichts der Nachfrage nach VoIP und Videokonferenzen bewegt sich der Verkehr zunehmend zwischen Büros. Es ist ineffizient, Vollmaschenverbindungen über Rechenzentren einzurichten, was zeitaufwändig sein kann.

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.

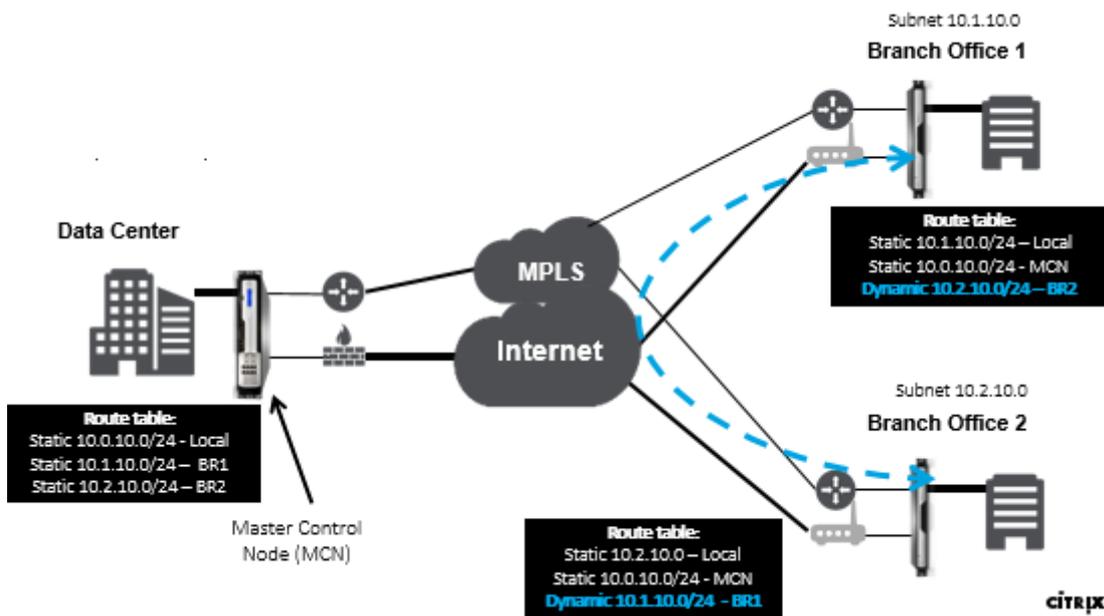
Zusätzliche Vorteile des SD-WAN-Netzwerks sind:

- 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 ist
- 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

Informationen zum Aktivieren dynamischer virtueller Pfade mit dem Citrix SD-WAN Orchestrator Service finden Sie unter [Virtuelle Pfade](#).

WAN-zu-WAN-Weiterleitung

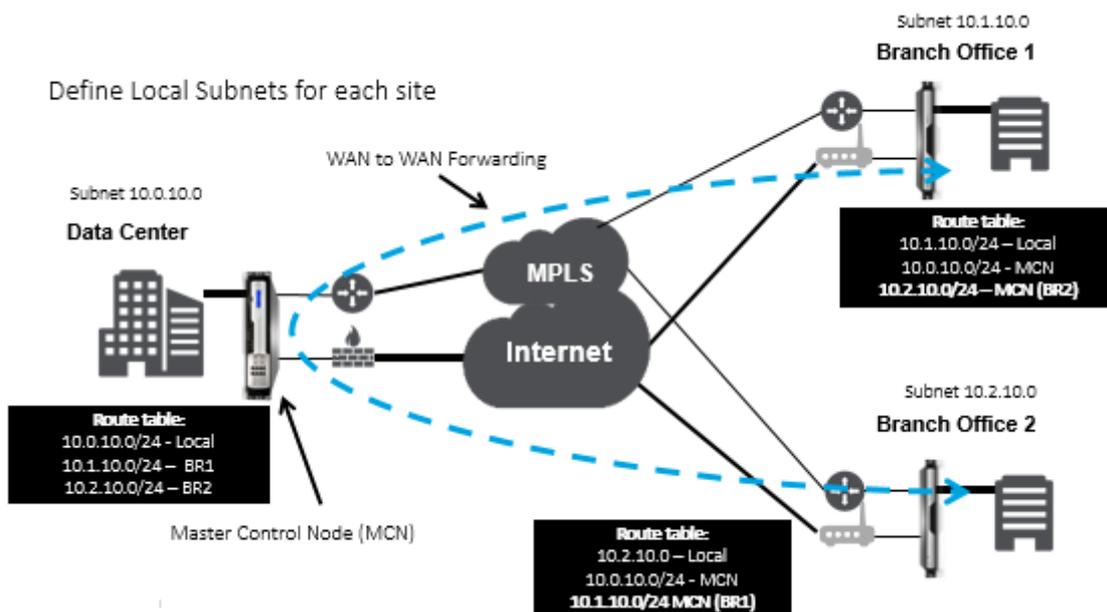
August 29, 2022

Das Aktivieren der WAN-zu-WAN-Weiterleitung auf dem MCN ermöglicht es dem MCN, Routen für Remote-Standorte anzukündigen.

- Kunden kennen die lokalen Routen von MCN und anderen Routen des Clientstandorts
- Aus Kundensicht werden alle Routen als MCN-Routen betrachtet

Wenn die WAN-zu-WAN-Weiterleitung auf dem MCN nicht aktiviert ist, treten im Kundennetzwerk Probleme mit der Kommunikation von Zweig zu Zweig auf.

Appliances, die im Clientmodus ausgeführt werden, kennen andere Zweigsubnetze nicht, bis die WAN-zu-WAN-Weiterleitung im MCN aktiviert ist. Wenn Sie diese Option aktivieren, werden die SD-WAN-Knoten der Zweigstelle auf andere Zweigsubnetze aufmerksam. Der Verkehr, der zu anderen Zweigstellen bestimmt ist, wird an MCN weitergeleitet. MCN leitet es zum richtigen Ziel.



Überwachung und Fehlerbehebung

August 29, 2022

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](#)

[Statistische Informationen anzeigen](#)

[Anzeigen von Flussinformationen](#)

[Anzeigen von Berichten](#)

[Firewall-Statistiken anzeigen](#)

[Diagnosetool](#)

[Verbesserte Pfadzuordnung und Bandbreite](#)

[Fehlerbehebung bei Management-IP](#)

[Aktive Bandbreitentests](#)

[Adaptive Bandbreitenerkennung](#)

Virtuelles WAN überwachen

August 29, 2022

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:

Virtueller Pfad [Site-Name] —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.

The screenshot shows a dashboard with three tabs: Dashboard, Monitoring, and Configuration. The 'Dashboard' tab is active. The main content area is divided into three sections:

- System Status:**
 - Name: MCN_23
 - Model: VPX
 - Sub-Model: BASE
 - Appliance Mode: MCN
 - Serial Number: 67e0772c-5190-a2ee-d183-9244189b30a0
 - Management IP Address: 10.102.78.154
 - Appliance Uptime: 6 days, 13 hours, 22 minutes, 23.0 seconds
 - Service Uptime: 6 days, 13 hours, 14 minutes, 46.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions:**
 - Software Version: 10.1.0.111.690027
 - Built On: Jun 21 2018 at 23:42:30
 - Hardware Version: VPX
 - OS Partition Version: 4.6
- Virtual Path Service Status:**
 - Virtual Path MCN_23-Site1: Uptime: 6 days, 13 hours, 11 minutes, 45.0 seconds.

Statistische Informationen anzeigen

August 29, 2022

Dieser Abschnitt enthält grundlegende Anweisungen zum Anzeigen von Virtual WAN-Statistikinformationen.

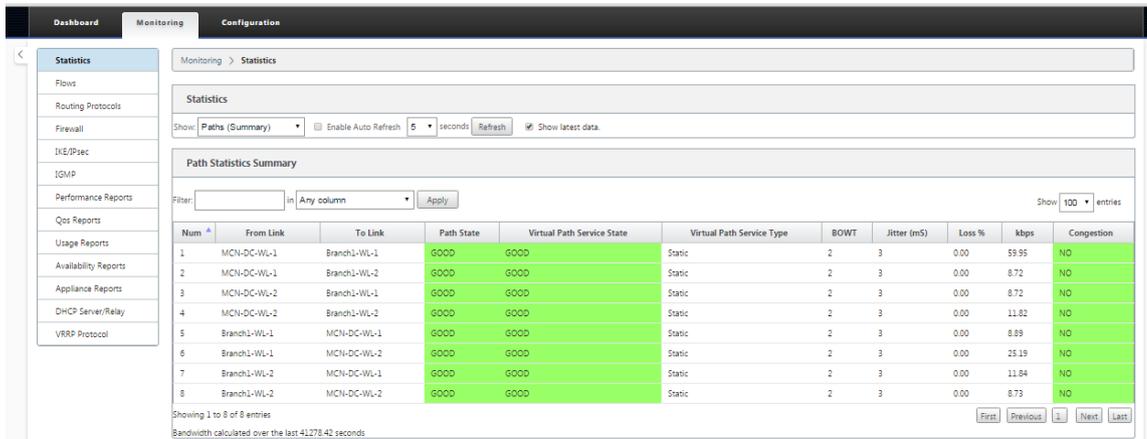
1. Melden Sie sich beim Management Web Interface für den MCN an.

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.

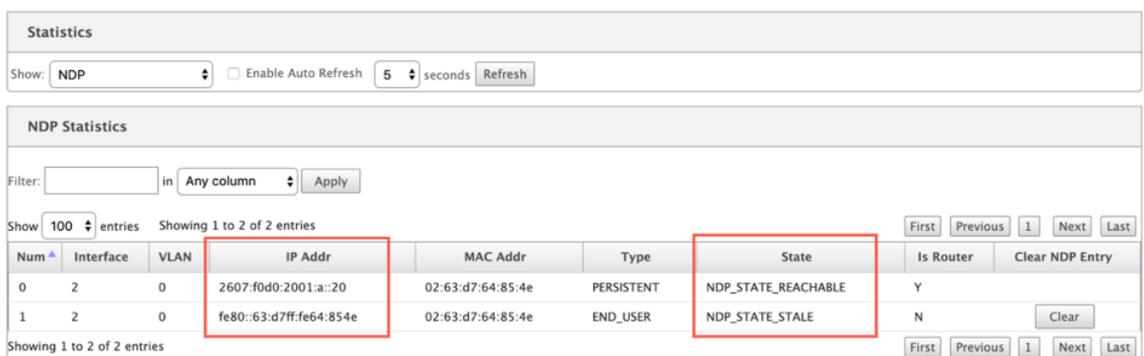
Hinweis

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.

Statistics

Show: **WAN Link** Enable Auto Refresh **5** seconds Refresh Show latest data.

WAN Link Statistics

Filter: in **Any column** Apply

Show **100** entries Showing 1 to 6 of 6 entries First Previous **1** Next Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
demo_cl1_inet	N/A	2607:f0d0:2001:b::10	N/A	N/A	N/A	N/A
demo_cl1_inet2	N/A	172.16.100.1	N/A	N/A	N/A	N/A
demo_cl2_inet	N/A	2607:f0d0:2001:c::10	N/A	N/A	N/A	N/A
demo_cl2_inet2	N/A	172.16.150.1	N/A	N/A	N/A	N/A
demo_mcn_inet	demo_mcn_inet-AI-1	2607:f0d0:2001:a::10	N/A	N/A	N/A	N/A
demo_mcn_inet2	demo_mcn_inet2-AI-1	172.16.200.1	N/A	DISABLED	N/A	N/A

Showing 1 to 6 of 6 entries First Previous **1** Next Last

Virtual Path Service Data Rates

Filter: in **Any column** Apply

3. Sie können auch die Access Interface-Statistiken anzeigen.

Dashboard **Monitoring** Configuration

Monitoring > Statistics

Statistics

Show: **Access Interfaces** Enable Auto Refresh **5** seconds Refresh Show latest data.

Access Interface Statistics

Filter: in **Any column** Apply

Show **100** entries Showing 1 to 2 of 2 entries First Previous **1** Next Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
demo_mcn_inet	demo_mcn_inet-AI-1	2607:f0d0:2001:a::10	N/A	N/A	N/A	N/A
demo_mcn_inet2	demo_mcn_inet2-AI-1	172.16.200.1	N/A	N/A	N/A	N/A

Showing 1 to 2 of 2 entries First Previous **1** Next Last

Virtual Path Service Data Rates:

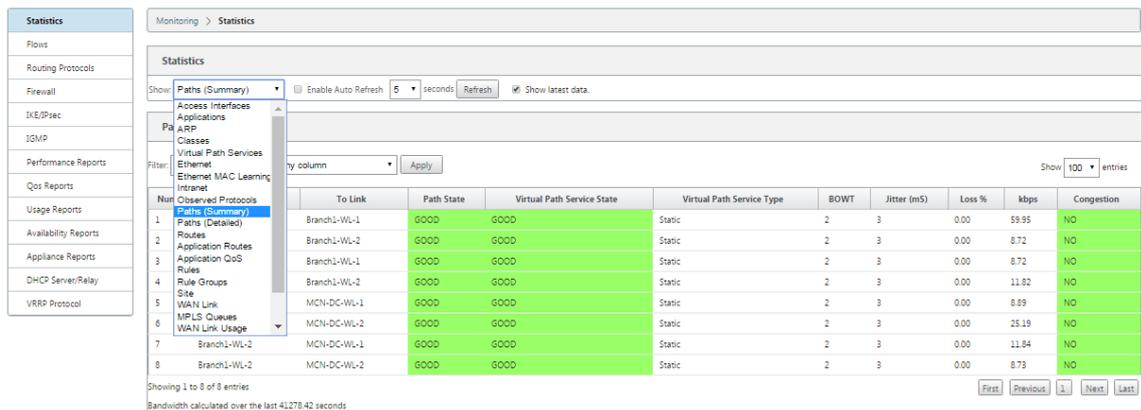
Filter: in **Any column** Apply

Show **100** entries Showing 1 to 8 of 8 entries First Previous **1** Next Last

WAN Link	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved
demo_mcn_inet	demo_mcn_inet-AI-1	demo_mcn-demo_cl2	Recv	20220845	3240115.88	413	74.23	46.47	0
demo_mcn_inet	demo_mcn_inet-AI-1	demo_mcn-demo_cl1	Recv	20196856	3252489.44	289	30.05	18.82	0

4. Öffnen Sie das Drop-down-Menü **Anzeigen**.

Neben den **Statistiken**Pfade, NDP, Access 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.

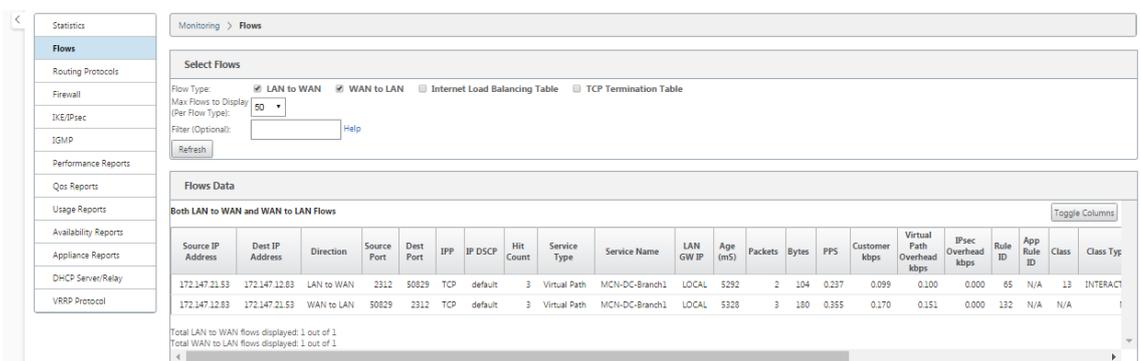
Anzeigen von Flussinformationen

August 29, 2022

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 Managementweboberfläche 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 Kontrollkästchen 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 Hilfanzeige 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.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display: (Per Flow Type:)

Filter (Optional): [Help](#)

Flows Data

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	TCP	default	9577	Virtual Path	DC-BR	LOCAL	5332	12038	1020734	0.079	0.033	0.031
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	TCP	default	9631	Virtual Path	DC-BR	LOCAL	5346	12199	1075706	0.079	0.033	0.031
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	TCP	default	18025	Virtual Path	DC-BR	LOCAL	5346	18025	1294598	0.157	0.052	0.062
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	TCP	default	18244	Virtual Path	DC-BR	LOCAL	5360	18244	1389118	0.157	0.052	0.062

Total LAN to WAN flows displayed: 2 out of 305
Total WAN to LAN flows displayed: 2 out of 305

Internet Load Balancing Flows

LAN IP	WAN IP	Age (mS)	WAN Link	Flow Count
Note: Only the active flows will be displayed and the total number of flows include active and inactive flows.				

TCP Terminated Flows

Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Age (mS)	From Wan kbps	To Wan kbps	Bytes Pending To LAN	Bytes Pending To WAN	State
Total TCP Terminated flows displayed: 0 out of 305										

8. (Optional) Wählen Sie die Spalten aus, die in die Tabelle aufgenommen werden sollen. Führen Sie folgende Schritte aus:
9. Klicken Sie oben rechts in der Tabelle „**Flussdaten**“ auf **Spaltenumschalten**. Es zeigt alle nicht ausgewählten Spalten an und öffnet ein Kontrollkästchen über jeder Spalte, um diese Spalte

auszuwählen oder zu deaktivieren. Deaktivierte Spalten werden ausgegraut angezeigt, wie in der Abbildung gezeigt.

Hinweis

Standardmäßig sind alle Spalten ausgewählt, was dazu führen kann, dass die Tabelle in der Anzeige abgeschnitten wird, wodurch die Schaltfläche **Spalten umschalten** wird. Ist dies der Fall, wird unter der Tabelle eine horizontale Bildlaufleiste angezeigt. Schieben Sie die Bildlaufleiste nach rechts, um den abgeschnittenen Abschnitt der Tabelle anzuzeigen und die Schaltfläche **Spalten umschalten** anzuzeigen. Wenn die Bildlaufleiste nicht verfügbar ist, versuchen Sie, die Breite Ihres Browserfensters zu ändern, bis die Bildlaufleiste angezeigt wird.

Monitoring > Flows

Balancing Table TCP Termination Table

Apply

Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
9598	Virtual Path	DC-BR	LOCAL	2435	12065	1023038	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
9652	Virtual Path	DC-BR	LOCAL	2434	12226	1078010	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
18064	Virtual Path	DC-BR	LOCAL	2448	18064	1297454	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable
18283	Virtual Path	DC-BR	LOCAL	2447	18283	1391974	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable

10. Aktivieren Sie ein Kontrollkästchen, um eine Spalte auszuwählen oder die Auswahl aufzuheben.

- **Quell-IP-Adresse** —Die Quell-IP-Adresse für Pakete in diesem Fluss.
- **Ziel-IP-Adresse** —Die Ziel-IP-Adresse für Pakete in diesem Fluss.
- **Richtung** —Die Richtung für Pakete in diesem Fluss —LAN zu WAN oder WAN zu LAN.
- **Quellport** —Der Quellport für Pakete in diesem Fluss.
- **Zielport** - Der Zielport für Pakete in diesem Fluss.
- **IPP** - Die IP-Protokollnummer für Pakete in diesem Fluss.
- **IP DSCP** —Die IP-DSCP-Tag-Einstellung für Pakete in diesem Fluss.
- **Trefferanzahl** —Die Anzahl, wie oft dieser Flow gesucht und gefunden wurde.
- **Diensttyp** —Gibt an, ob es sich bei diesem Flow-Typ um virtuellen Pfad-, Internet- oder Intranetverkehr handelt.

- **Dienstname** —Der Name des virtuellen Pfads, den der virtuelle Pfadverkehr verwendet.
- **LAN GW IP** —IP-Adresse für das LAN-Gateway, falls eine angegeben ist.
- **Alter (mS)** - Die Zeit (in Millisekunden), seit ein Paket in diesem Fluss klassifiziert wurde.
- **Pakete** —Anzahl der Pakete, die über die Lebensdauer des Flusses gesendet wurden.
- **Byte** —Anzahl der Byte, die während der Lebensdauer des Flows gesendet wurden.
- **PPS** - Pakete pro Sekunde über den Zeitraum seit der letzten Aktualisierung.
- **Kunden-KBit/s/ Virtueller Pfad-Overhead KBit/s/IPSec-Overhead-KBit/s** —Kilobit pro Sekunde über den Zeitraum seit der letzten Aktualisierung.
- **Regel-ID** —Die ID der Regel, mit der der Datenverkehr in diesem Fluss übereinstimmt.
- **App-Regel-ID** —Die ID der App —die Regel, mit der der Datenverkehr in diesem Flow übereinstimmt.
- **Klasse** —Die ID der virtuellen Pfadklasse, die der Datenverkehr verwendet.
- **Klassentyp** - Der Typ der virtuellen Pfadklasse (Realtime, Interactive, Bulk), die der Datenverkehr verwendet.
- **Pfad** —Der Pfad, den der Verkehr benutzt.
- **Hdr Compression Saved Bytes** - Die Anzahl der gespeicherten Byte aufgrund der Header-Komprimierung.
- **Übertragungsart** —Die Übertragungsart, die der Verkehr verwendet.
- **Anwendung** —Der Name der verwendeten Anwendung.

11. Klicken Sie auf **Übernehmen** (oberhalb der rechten oberen Ecke der Tabelle). Es werden die Auswahloptionen geschlossen und die Tabelle aktualisiert, um nur die ausgewählten Spalten einzubeziehen.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type):

Filter (Optional): [Help](#)

Flows Data

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	9613	Virtual Path	DC-BR	LOCAL	12022	12084	1024626
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	9667	Virtual Path	DC-BR	LOCAL	12040	12246	1080066
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	18092	Virtual Path	DC-BR	LOCAL	12040	18092	1299440
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	18312	Virtual Path	DC-BR	LOCAL	12056	18312	1394758

Total LAN to WAN flows displayed: 2 out of 306
Total WAN to LAN flows displayed: 2 out of 306

DPI-Anwendungen im SD-WAN Center

In früheren Versionen können rund 4.000 Anwendungen identifiziert 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

August 29, 2022

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:

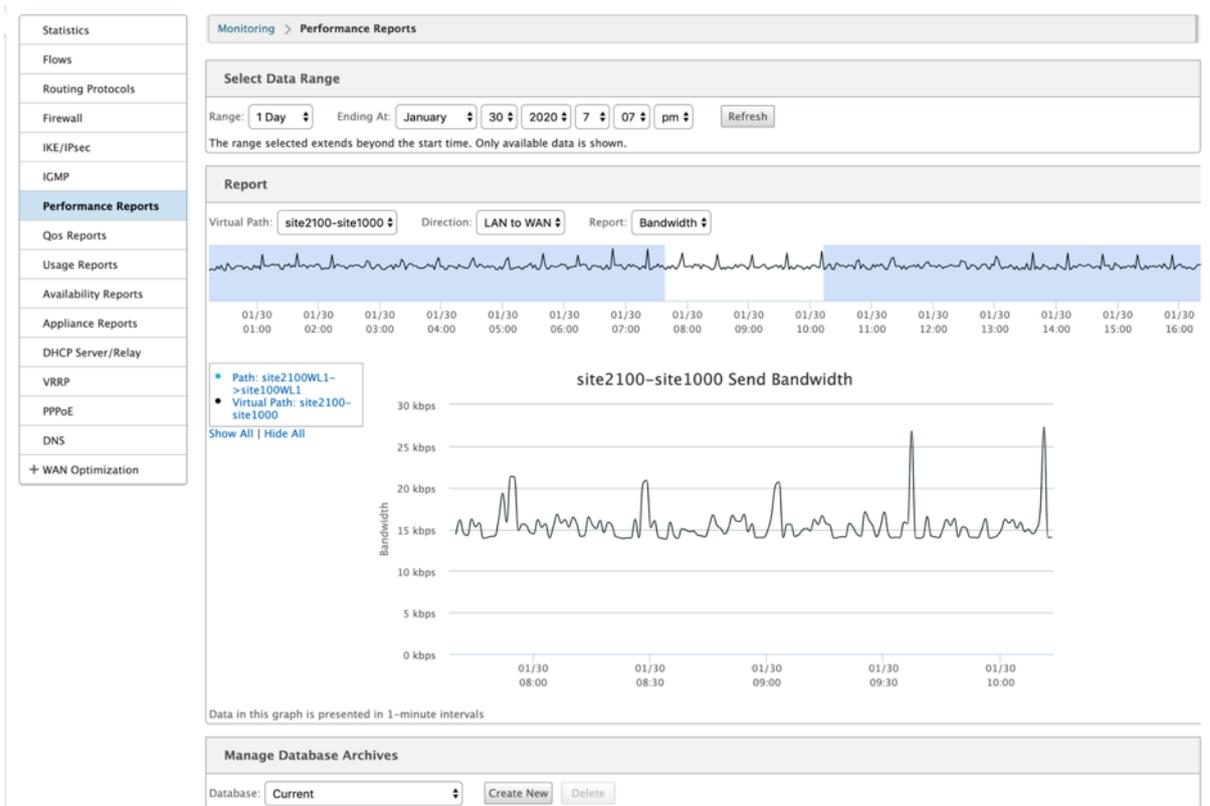
- **Performance-Berichte**
- **QoS-Berichte**
- **Nutzungs-Berichte**
- **Verfügbarkeitsberichte**
- **Appliance-Berichte**

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.

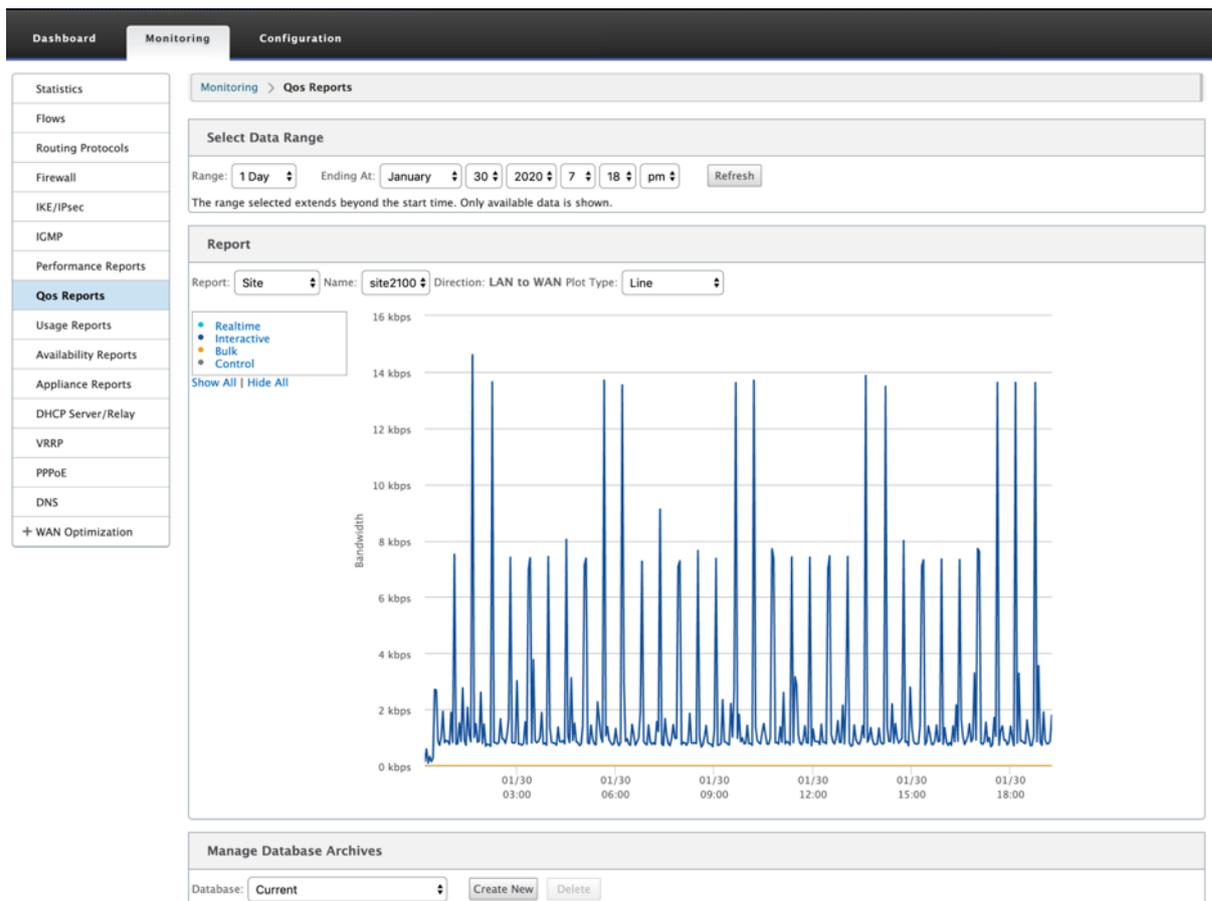


Sie können den Datenbereich nach Bedarf mit den folgenden Feldern auswählen, um den Leistungsbericht anzuzeigen:

- **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.

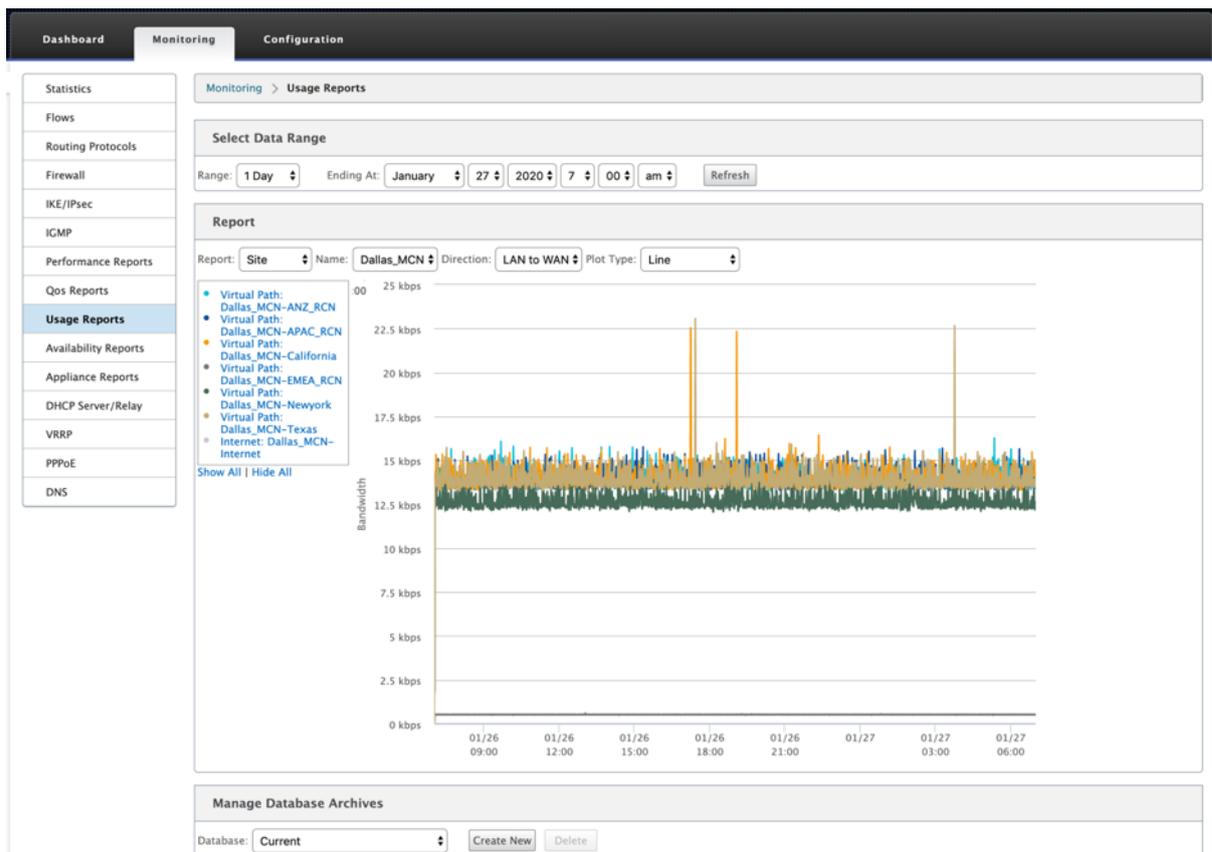


Sie können die folgenden Metriken anzeigen:

- **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 Steuerungskpaketen, 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

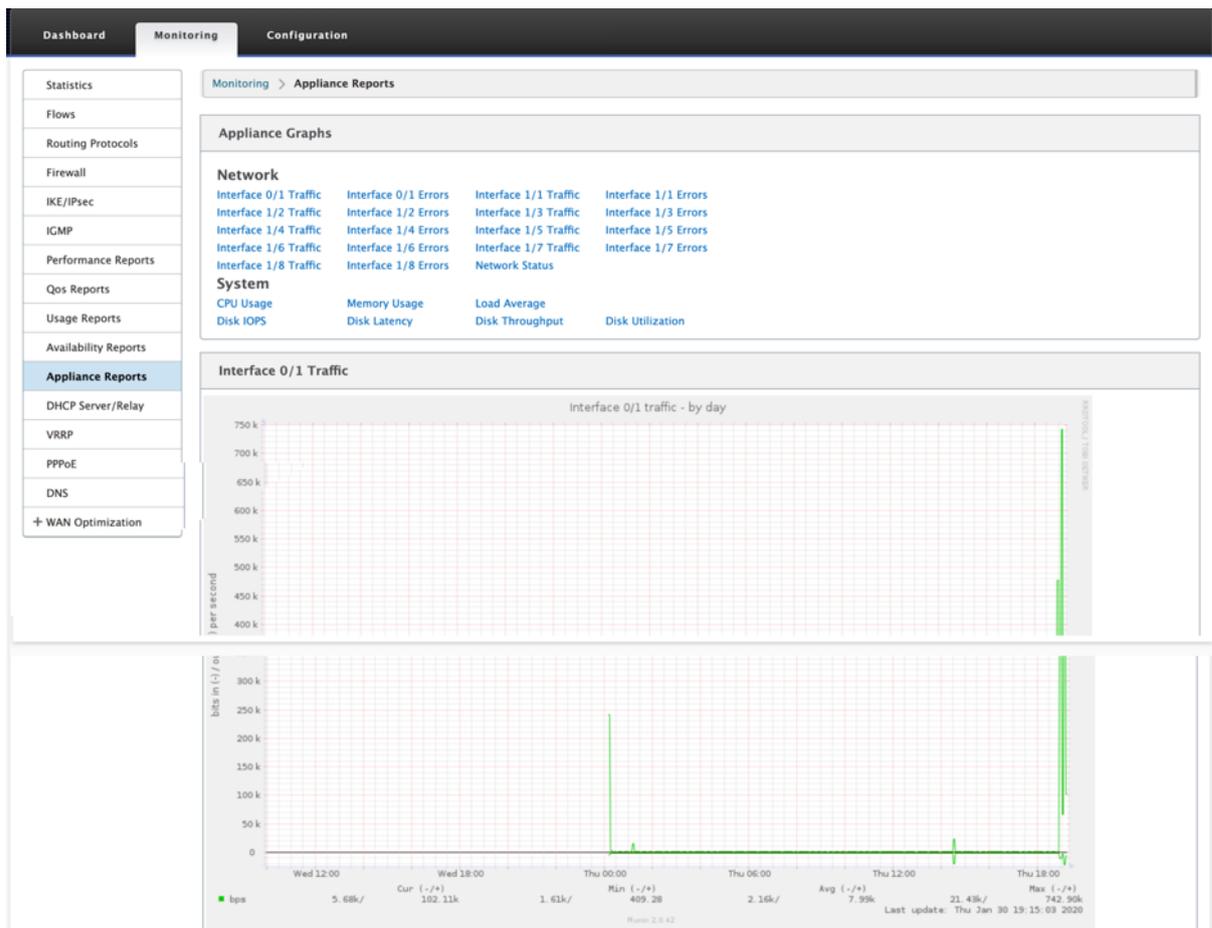
In diesem Bericht können Sie die Verfügbarkeitsdaten von WAN-Links, Pfaden und virtuellen Pfaden anzeigen. Sie können auch zu einem bestimmten Zeitrahmen wechseln, z. B. 1 Stunde, 24 Stunden und 7 Tage, um die verfügbaren Daten anzuzeigen. Die Daten Paths und Virtual Paths werden in einem Format **DD:HH:MM:SS** dargestellt.

Paths and Virtual Paths														
	Uptime	Goodtime	Badtime				Downtime			Incidents				
			Total	Loss	Silence	Peer	Total	Silence	Peer	Total	Loss	Silence	Peer	
Virtual Path Dallas_MCN-ANZ_RCN	1:00:00:00	1:00:00:00	0:00	0:00	5									
Dallas_MCN-queue1->ANZ_RCN-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0:00	0	---	0	0
ANZ_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:10	0:50	0:00	0:50	---	0:00	0:00	---	5	0	5	---	
Virtual Path Dallas_MCN-APAC_RCN	1:00:00:00	1:00:00:00	0:00	0:00	14									
Dallas_MCN-queue1->APAC_RCN-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0:00	0	---	0	0
APAC_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:57:40	2:20	0:00	2:20	---	0:00	0:00	---	14	0	14	---	
Virtual Path Dallas_MCN-California	1:00:00:00	23:59:42	0:18	0:00	2									
Dallas_MCN-queue1->California-queue1	23:58:36	23:58:36	0:00	---	0:00	0:00	0:00	0:00	0:00	0:00	2	---	0	2
California-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:40	0:20	0:00	0:20	---	0:00	0:00	---	2	0	2	---	
Virtual Path Dallas_MCN-EMEA_RCN	0:00	0:00	0:00	1:00:00:00	0									
Dallas_MCN-queue1->EMEA_RCN-queue2	0:00	0:00	0:00	---	0:00	0:00	1:00:03:45	1:00:03:45	0:00	0	---	0	0	0
EMEA_RCN-queue2->Dallas_MCN-queue1	0:00	0:00	0:00	0:00	0:00	---	1:00:03:45	1:00:03:45	---	0	0	0	---	
Virtual Path Dallas_MCN-Newyork	1:00:00:00	1:00:00:00	0:00	0:00	8									
Dallas_MCN-WL-2->Newyork-WL-2	0:00	0:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0:00	0	---	0	0
Dallas_MCN-queue1->Newyork-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0:00	0	---	0	0
Newyork-WL-2->Dallas_MCN-WL-2	0:00	0:00	0:00	0:00	0:00	---	1:00:03:45	1:00:03:45	---	0	0	0	---	
Newyork-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:40	1:20	0:00	1:20	---	0:00	0:00	---	8	0	8	---	
Virtual Path Dallas_MCN-Texas	1:00:00:00	23:59:42	0:18	0:00	12									
Dallas_MCN-queue1->Texas-queue1	23:58:35	23:58:35	0:00	---	0:00	0:00	0:00	0:00	0:00	0:00	2	---	0	2
Texas-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:00	2:00	0:00	2:00	---	0:00	0:00	---	12	0	12	---	

WAN Links			
	Uptime	Downtime	Incidents
Dallas_MCN-WL-2	0:00	1:00:00:00	1
Dallas_MCN-queue1	1:00:00:00	0:00	No downtime

Appliance-Berichte

Appliance-Bericht liefert Berichte zum Netzwerkverkehr und zur Systemverwendung. Klicken Sie auf die einzelnen Links, um das Appliance-Diagramm nach Tag, wöchentlich, monatlich und jährlich anzuzeigen oder zu überwachen.



Firewall-Statistiken anzeigen

August 29, 2022

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](#).

So zeigen Sie Firewall-Statistiken an:

1. Navigieren Sie zu **Monitoring > Firewall**.
2. Wählen Sie nach Bedarf **Verbindungen, Filterrichtlinien oder NAT-Richtlinien** aus.
3. Legen Sie die Filterkriterien nach Bedarf fest.
4. Klicken Sie auf **Aktualisieren**.

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.

Diagnose

August 29, 2022

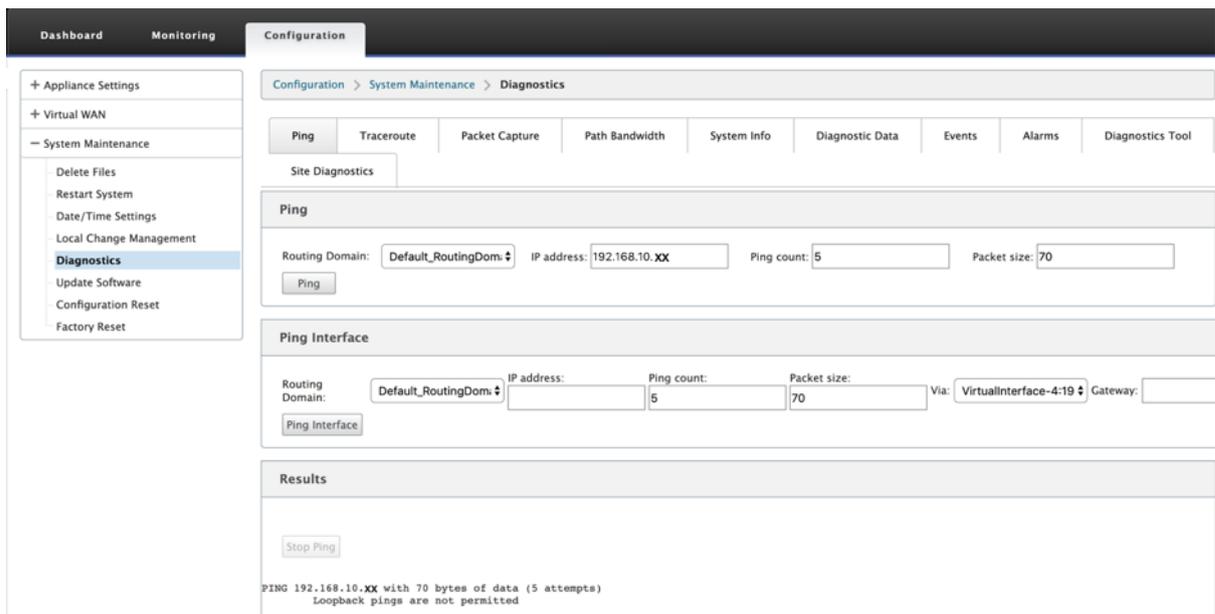
Citrix SD-WAN Diagnostics-Dienstprogramme bieten die folgenden Optionen zum Testen und Untersuchen von Konnektivitätsproblemen:

- 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.

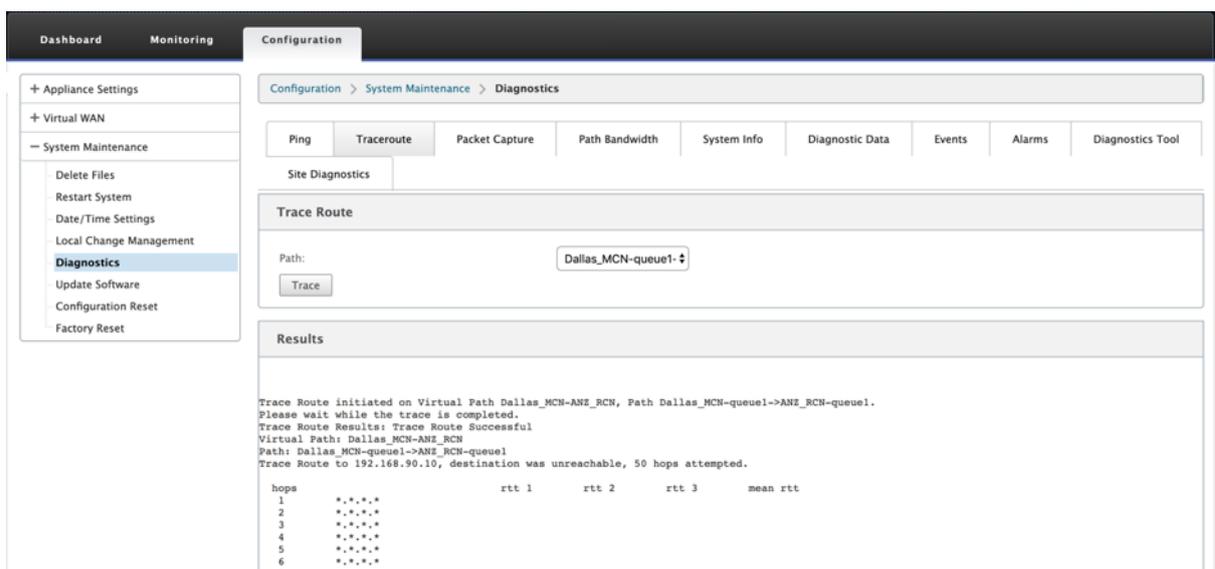


Wählen Sie die Routing-Domäne aus. Geben Sie eine gültige IP-Adresse, die Anzahl der Ping-Zähler (Anzahl der Ping-Anfragen zu senden) und die Paketgröße (Anzahl der Datenbytes) an. Klicken Sie auf **Ping stoppen**, um eine laufende Ping-Suche

Sie können über eine bestimmte Oberfläche pingen. Wählen Sie die Routingdomäne aus und geben Sie die IP-Adresse mit Ping-Anzahl und Paketgröße an und wählen Sie die virtuelle Schnittstelle aus der Dropdown-Liste aus.

Traceroute

Um die Option **Traceroute** zu verwenden, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Traceroute** aus.



Traceroute hilft dabei, den Pfad oder die Route zu einem Remoteserver zu erkennen und anzuzeigen. Verwenden Sie die Option **Traceroute** als Debugging-Tool, um die Fehlerpunkte in einem Netzwerk zu erkennen.

Wählen Sie einen Pfad aus der Dropdownliste aus und klicken Sie auf **Trace**. Sie können die Details im Abschnitt **Ergebnisse** einsehen.

Paketerfassung

Sie können die Option **Paketerfassung** verwenden, um das Echtzeit-Datenpaket abzufangen, das über die ausgewählte aktive Schnittstelle an der ausgewählten Site läuft. Die Paketerfassung hilft Ihnen bei der Analyse und Behebung von Netzwerkproblemen.

Dashboard
Monitoring
Configuration

- + Appliance Settings
- + Virtual WAN
- System Maintenance
 - Delete Files
 - Restart System
 - Date/Time Settings
 - Local Change Management
 - Diagnostics
 - Update Software
 - Configuration Reset
 - Factory Reset

Configuration > System Maintenance > Diagnostics

Ping
Traceroute
Packet Capture
Path Bandwidth
System Info
Diagnostic Data
Events
Alarms

Diagnostics Tool

Site Diagnostics

Packet Capture

Interfaces: X 1/1 X 1/2 X 1/4 X 1/6

Duration (seconds): 30

Max # of packets to view: 5000

Capture Filter (Optional): Help

Capture

Note: Capture file size will not exceed 575 MB. Once the packet capture file reaches this size, packet capturing will be stopped. Atleast 1 interface needs to be selected to trigger a packet capture.

Gathering Requested Data

Generating packet capture information...

Packet Capture Successful

Packet Capture File

A binary file containing the packet data captured during the last successful packet capture. This file can be opened in Wireshark for analysis. Help

The downloaded Packet capture file displays internal labels for interface names. Here are the mappings for this platform:
 MGMT -> tn-mgt0
 1/1 -> dpdk-1_1
 1/4 -> dpdk-1_4
 1/2 -> dpdk-1_2
 1/6 -> dpdk-1_6

Download

Packet View

#	Interface Name	Protocol	Time	Length	Source	Destination	Src
1.	1/2	UDP	May 8, 2019 06:06:30.415518572 UTC	1442	172.168.1.10	152.168.1.10	4980
2.	1/2	UDP	May 8, 2019 06:06:30.415524972 UTC	1442	152.168.1.10	172.168.1.10	4980
3.	1/2	UDP	May 8, 2019 06:06:30.415628324 UTC	1442	152.168.1.10	172.168.1.10	4980
4.	1/2	UDP	May 8, 2019 06:06:30.415648675 UTC	1442	172.168.1.10	152.168.1.10	4980
5.	1/2	UDP	May 8, 2019 06:06:30.415858329 UTC	1442	152.168.1.10	172.168.1.10	4980
6.	1/2	UDP	May 8, 2019 06:06:30.415873459 UTC	1442	172.168.1.10	152.168.2.10	4980
7.	1/2	UDP	May 8, 2019 06:06:30.416073413 UTC	1442	172.168.1.10	152.168.2.10	4980
8.	1/2	UDP	May 8, 2019 06:06:30.416232216 UTC	1442	152.168.1.10	172.168.1.10	4980
9.	1/1	TCP	May 8, 2019 06:06:30.321504133 UTC	1384	152.168.1.51	172.168.1.52	80
10.	1/2	UDP	May 8, 2019 06:06:30.416266227 UTC	1442	152.168.1.10	172.168.1.10	4980
11.	1/2	UDP	May 8, 2019 06:06:30.416435190 UTC	1442	172.168.1.10	152.168.1.10	4980
12.	1/2	UDP	May 8, 2019 06:06:30.416525402 UTC	114	172.168.1.10	152.168.2.10	4980
13.	1/1	TCP	May 8, 2019 06:06:30.321511153 UTC	54	152.168.1.52	172.168.1.51	2307
14.	1/2	UDP	May 8, 2019 06:06:30.416529932 UTC	114	172.168.1.10	152.168.2.10	4980
15.	1/1	TCP	May 8, 2019 06:06:30.321514773 UTC	54	152.168.1.52	172.168.1.51	2163
16.	1/2	UDP	May 8, 2019 06:06:30.416651685 UTC	1442	152.168.1.10	172.168.1.10	4980
17.	1/2	UDP	May 8, 2019 06:06:30.416693075 UTC	1442	152.168.1.10	172.168.1.10	4980
18.	1/2	UDP	May 8, 2019 06:06:30.416783167 UTC	1442	172.168.1.10	152.168.2.10	4980
19.	1/2	UDP	May 8, 2019 06:06:30.416881149 UTC	1442	172.168.1.10	152.168.2.10	4980
20.	1/2	UDP	May 8, 2019 06:06:30.417039802 UTC	1442	152.168.1.10	172.168.1.10	4980
21.	1/2	UDP	May 8, 2019 06:06:30.417127644 UTC	114	172.168.1.10	152.168.2.10	4980
22.	1/2	UDP	May 8, 2019 06:06:30.417132114 UTC	114	172.168.1.10	152.168.1.10	4980
23.	1/2	UDP	May 8, 2019 06:06:30.417135804 UTC	1442	172.168.1.10	152.168.2.10	4980
24.	1/1	TCP	May 8, 2019 06:06:30.321517954 UTC	54	152.168.1.52	172.168.1.51	6265
25.	1/2	UDP	May 8, 2019 06:06:30.417178605 UTC	114	172.168.1.10	152.168.1.10	4980
26.	1/1	TCP	May 8, 2019 06:06:30.321648046 UTC	1384	172.168.1.51	152.168.1.52	80

Geben Sie die folgenden Eingaben für den Paketerfassungsvorgang an:

- **Schnittstellen** - Aktive Schnittstellen sind für die Paketerfassung für die SD-WAN-Appliance verfügbar. Wählen Sie eine Schnittstelle aus oder fügen Sie Schnittstellen aus der Dropdownliste hinzu. Es muss mindestens eine Schnittstelle ausgewählt werden, um eine Paketerfassung auszulösen.

Hinweis:

Die Möglichkeit, die Paketerfassung über alle Schnittstellen gleichzeitig auszuführen, hilft,

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

392

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.
- **Erfassungsfiler (optional)** —Das optionale Feld Erfassungsfiler 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 Aufnahme-Datei 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.

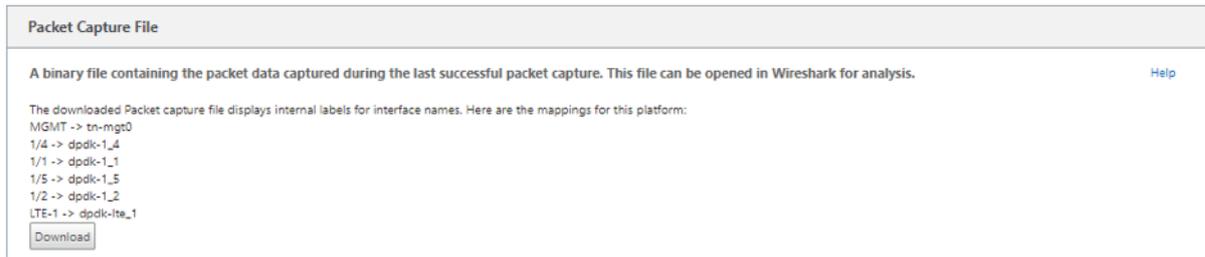
Sammeln angeforderter Daten

In dieser Tabelle sehen Sie den Status der Generierung von Paketerfassungsinformationen (ob die Paketerfassung erfolgreich ist oder keine Paketerfassung ist).

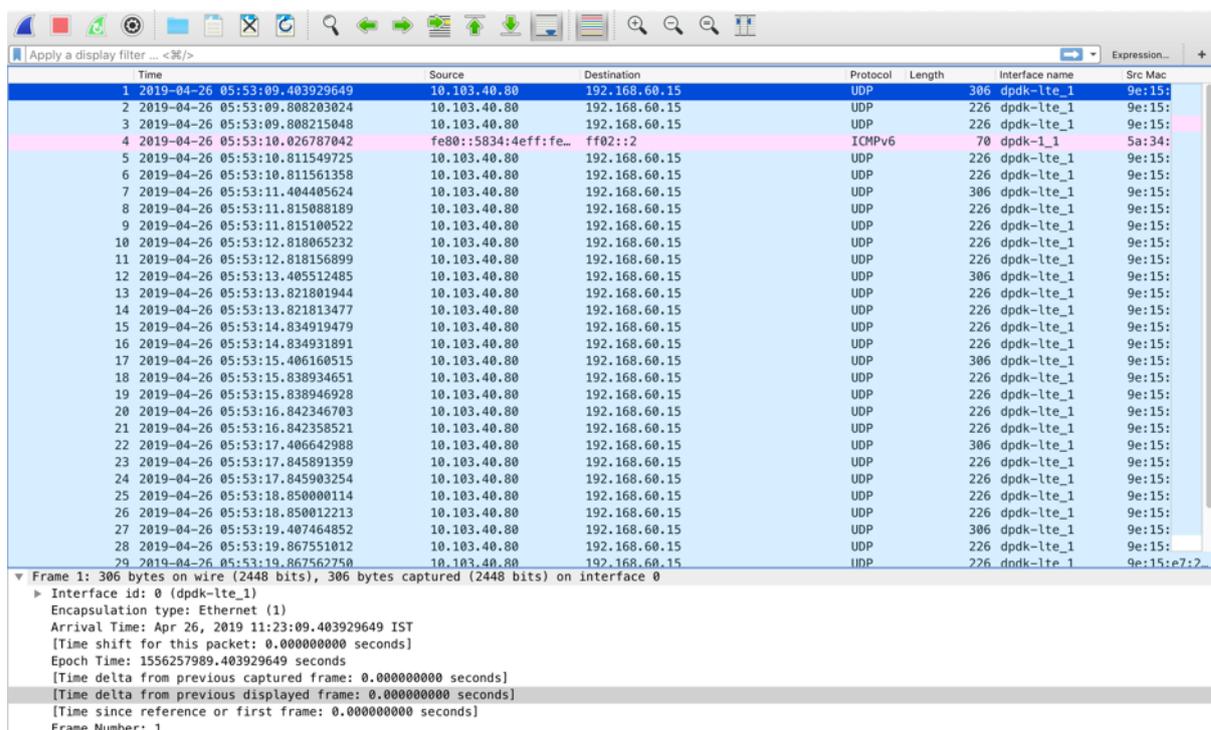
Paket-Capture-Datei

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.

The screenshot displays the 'Diagnostics' section of the Citrix SD-WAN 11.5 interface. It features a navigation menu on the left with options like 'Appliance Settings', 'Virtual WAN', and 'System Maintenance'. The main content area is titled 'Configuration > System Maintenance > Diagnostics' and includes tabs for 'Ping', 'Traceroute', 'Packet Capture', 'Path Bandwidth', 'System Info', 'Diagnostic Data', 'Events', 'Alarms', and 'Diagnostics Tool'. The 'Path Bandwidth' tab is active, showing 'Instant Path Bandwidth Testing' with a path selector set to 'MCN-5100-WL-2->BR572'. Below this, the 'Results' section displays bandwidth statistics: Minimum Bandwidth: 936564 kbps, Maximum Bandwidth: 1213863 kbps, and Average Bandwidth: 1189846 kbps. The 'Schedule Path Bandwidth Testing' section includes an 'Add' button and a table with columns for Path Name, Frequency, Day of Week, Hour, and Minute. The 'History Path Bandwidth Testing Result' section shows a table of 27 test entries with columns for Num, From Link, To Link, Test Time, Min Bandwidth (kbps), Max Bandwidth (kbps), and Avg Bandwidth (kbps). The table shows a progression of tests from 2/17/2018 to 2/19/2018, with the final entry (27) showing a path from MCN-5100-WL-2 to BR572-WL-1.

Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018 2:01:03 PM	2883972	5099707	4357330
2	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018 4:01:03 PM	3109115	3872000	3616157
3	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018 6:01:04 PM	3041280	4119960	3518949
4	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018 8:01:04 PM	2769377	3700672	3276124
5	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018 10:01:04 PM	409245	3574153	2489269
6	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 12:01:04 AM	2481756	4001684	3188214
7	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 2:01:04 AM	2548853	3872000	3236546
8	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 4:01:03 AM	3204413	3882628	3642648
9	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 6:01:03 AM	2997677	4672357	3664018
10	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 8:01:04 AM	2248258	6288360	3612666
11	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 10:01:04 AM	2410236	3372387	2816032
12	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 12:01:03 PM	2613600	4401852	3563752
13	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 2:01:04 PM	2324266	4059961	3101910
14	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 4:01:03 PM	2179340	3684870	2929146
15	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 6:01:03 PM	2613600	3588493	3021890
16	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 8:01:03 PM	1676056	3499380	2655200
17	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 10:01:03 PM	1854093	3558944	2975804
18	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 12:01:03 AM	2161116	3784398	2902068
19	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 2:01:04 AM	2986971	4079766	3821158
20	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 4:01:04 AM	3514064	4181760	3893381
21	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 6:01:03 AM	3338843	4059961	3756691
22	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 8:01:03 AM	3216738	4245441	3716351
23	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 10:01:04 AM	3558944	4202773	3932908
24	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 12:01:03 PM	3427672	4267102	3838552
25	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 2:01:04 PM	2674061	4224000	3608676
26	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 4:01:03 PM	2816000	6288360	4165337
27	MCN-5100-WL-2	BR572-WL-1	2/19/2018 5:23:04 PM	986564	1213863	1109046

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 maximal mögliche 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**.

The screenshot displays the 'System Information' page in the Citrix SD-WAN management console. The page is organized into several sections:

- System Information:** A table listing system details:

Name:	Dallas_MCN
Appliance Mode:	MCN
Hardware Model:	4000
Software Version:	11.0.0.72.760315
Built On:	Apr 10 2019 at 19:08:49
OS Partition Version:	5.1
Serial Number:	HNXCJRGJX
BIOS version:	4.2a
- Hard Disk Usage:** A small table showing disk usage for different partitions:

Partition	Usage
Active OS	51%
/home	18%
- Ethernet Ports:** A table listing 10 ports with their names and MAC addresses:

0/1:	mgt0	0ac4:7a:85:ce:62
1/1:	la0	be:0af7:be:76:3d
1/2:	wa0	e6:18:31:22:b9:84
1/3:	la1	86:c0:b7:3c:03:5d
1/4:	wa1	8e:4bf2:fd:86:75
1/5:	la2	da:6c:7c:73:d4:84
1/6:	wa2	be:e3:26:7e:2b:99
1/7:	la3	82:af:6a:d8:74:72
1/8:	wa3	a2:af:76:6f:90:a2
10/1:	la4	96:9adf:97:77:eb
10/2:	wa4	76:5d:15:d9:f0:26
- License Status:** A table showing license details:

State:	Licensed
License Server HostID:	02c47a85ce62
Model:	4000VW-2000
Maximum Bandwidth (MAXBW):	2000 Mbps
License Type:	Retail
Maintenance Expiration Date:	Sun Dec 1 00:00:00 2019
License Expiration Date:	Mon Dec 2 00:00:00 2019

In den **Systeminformationen** werden alle Parameter aufgeführt, die nicht auf ihre Standardwerte eingestellt sind. Diese Informationen sind schreibgeschützt. Es wird vom Support verwendet, wenn eine Art von Fehlkonfiguration vermutet wird. Wenn Sie ein Problem melden, werden Sie möglicherweise aufgefordert, einen oder mehrere Werte auf dieser Seite zu überprüfen.

Diagnosedaten

Mit **Diagnosedaten** können Sie ein Diagnosedatenpaket zur Analyse durch das Citrix Support-Team erstellen. Sie können das **Diagnostics-Protokolldateienpaket** herunterladen und es mit dem Citrix Support-Team teilen.

Um die **Diagnosedaten** anzuzeigen, navigieren Sie zu **Konfiguration > erweitern Sie Systemwartung > Diagnose** und wählen Sie **Diagnosedaten**.

The screenshot displays the Citrix SD-WAN 11.5 Configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar menu lists various settings, with 'Diagnostics' highlighted. The main content area is titled 'Configuration > System Maintenance > Diagnostics'. A secondary navigation bar at the top of the content area includes 'Ping', 'Traceroute', 'Packet Capture', 'Path Bandwidth', 'System Info', 'Diagnostic Data', 'Events', 'Alarms', and 'Diagnostics Tool'. The 'Diagnostic Data' tab is active, showing the 'Site Diagnostics' section. This section contains three main panels: 'FTP Information', 'Diagnostic Information', and 'Memory Dumps'. The 'FTP Information' panel includes a note about passive mode connections and fields for 'Customer', 'Username', 'Password', and 'FTP Server', with an 'FTP Apply' button. The 'Diagnostic Information' panel includes a note about DNS settings and a 'Create New...' button, followed by a 'Filename' dropdown and 'Download Selected', 'Upload Selected', and 'Delete Selected' buttons. The 'Memory Dumps' panel includes a note about DNS settings and a 'Download' button. The 'Configuration Diagnostic Information' panel includes a note about DNS settings and a 'Create New...' button, followed by a 'Filename' dropdown and 'Download Selected', 'Upload', and 'Delete Selected' buttons.

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 die Verzweigung gesammelten Diagnoseinformationen verfügbar. Geben Sie für jeden Supportfall die Diagnoseinformationen der Zweig- und Konfigurationsdiagnoseinformationen vom Steuerknoten an, an den der Zweig angeschlossen ist.

Um Konfigurationsdiagnoseinformationen von der Control-Knoten-GUI zu sammeln, navigieren Sie zu **Konfiguration > Systemwartung > Diagnose > Diagnosedaten** > unter **Konfigurationsdiagnoseinformationen** und klicken Sie auf **Neu erstellen**.

Configuration Diagnostic Information

NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.

Configuration Diagnostic Files

- This package contains Configuration Diagnostics information you can forward to Citrix Support Representatives. This is an additional package to the STS captured on Branches. This package contains configuration archive and log files which help debug issues on the Branch. They may be downloaded directly through the browser or uploaded via FTP to the FTP server defined in the FTP Information area above.
- Only 5 Configuration diagnostics packages can exist on the system at a time.

Create New...

Filename:

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-Appl-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.

The screenshot shows the 'Events' configuration page in the Citrix SD-WAN interface. The breadcrumb navigation is 'Configuration > System Maintenance > Diagnostics'. The 'Events' tab is selected, showing an 'Insert Event' form with dropdowns for Object Type (USER EVENT), Event type (UNDEFINED), and Severity (DEBUG). Below this is the 'Download Events' section, which provides a summary of the event database and allows filtering by year (2019), month (March), day (24), and count (5). An 'Alert Count' table shows 0 alerts sent for Emails and Syslog Messages, and 5 for SNMP Traps. The 'View Events' section includes a filter for Object Type (Any) and a table of events.

Alert Type	Alerts Sent
Emails:	0
Syslog Messages:	0
SNMP Traps:	5

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
245555	25	License_Alert	LICENSE_EVENT	2019-04-21 06:23:16	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245554	25	License_Alert	LICENSE_EVENT	2019-04-20 06:23:01	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245553	25	License_Alert	LICENSE_EVENT	2019-04-19 06:22:46	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245552	25	License_Alert	LICENSE_EVENT	2019-04-18 06:22:31	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245551	25	License_Alert	LICENSE_EVENT	2019-04-17 06:22:15	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245550	25	License_Alert	LICENSE_EVENT	2019-04-16 06:22:00	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245549	25	License_Alert	LICENSE_EVENT	2019-04-15 06:21:44	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245548	25	License_Alert	LICENSE_EVENT	2019-04-14 06:21:29	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).

Sie können Citrix SD-WAN so konfigurieren, dass Ereignisbenachrichtigungen für verschiedene Ereignistypen wie **E-Mails**, **SNMP-Traps** oder **Syslog-Nachrichten** gesendet werden.

Sobald die Benachrichtigungseinstellungen für E-Mail, SNMP und Syslog-Benachrichtigungen konfiguriert sind, können Sie den Schweregrad für verschiedene Ereignistypen auswählen und den Modus (E-Mail, SNMP, Syslog) zum Senden von Ereignisbenachrichtigungen auswählen.

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 Alarmlöschen** 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**.

The screenshot shows the 'Diagnostics Tool' configuration page. It includes the following fields and controls:

- Tool Mode:** A dropdown menu set to 'Server'.
- Traffic Type:** A dropdown menu set to 'Data'.
- Port:** A text input field containing '10'.
- Iperf:** An empty text input field.
- WAN to LAN Paths:** A dropdown menu set to 'DC-INET-1->BR1-INET-1'.
- Start:** A button to initiate the test.
- Results:** A section containing a 'stop' button and a log output area showing:


```
Server listening on TCP port 10
TCP window size: 85.3 KByte (default)
```

2. Wählen Sie im Feld **Toolmodus** die Option **Server** auf einer Appliance aus und wählen Sie **Client** auf der Appliance aus, die sich am Remote-Ende des ausgewählten Pfades befindet.
3. Wählen Sie im Feld **Traffic Type** die Art des Diagnoseverkehrs aus, entweder **Steuerung** oder **Daten**. Wählen Sie auf beiden Geräten denselben Traffic-Typ aus.
4. Geben Sie im Feld **Port** die **TCP/UDP-Portnummer** an, über die der Diagnoseverkehr gesendet wird. Geben Sie dieselbe Portnummer auf beiden Appliances an.
5. Geben Sie im Feld **Iperf**, falls vorhanden, IPERF-Befehlszeilenoptionen an.

Hinweis

Sie müssen die folgenden IPERF-Befehlszeilenoptionen nicht angeben:

- -c: Clientmodus Option wird durch das Diagnose-Tool hinzugefügt.
- -s: Die Option für den Servermodus wird vom Diagnosetool hinzugefügt.
- -B: Die Bindung von IPERF an eine bestimmte IP/Schnittstelle erfolgt vom Diagnose-tool abhängig vom ausgewählten Pfad.
 - -p: Die Portnummer wird im Diagnose-Tool angegeben.
- -i: Ausgabeintervall in Sekunden.
- -t: Gesamtdauer des Tests in Sekunden.

6. Wählen Sie die WAN-zu-LAN-Pfade aus, auf denen Sie den Diagnoseverkehr senden möchten. Wählen Sie auf beiden Appliances denselben Pfad aus.
7. Klicken Sie auf beiden Geräten auf **Start**.

Das Ergebnis zeigt den Modus (Client oder Server) der ausgewählten Appliance und den TCP- oder UDP-Port an, auf dem der Test ausgeführt wird. Es zeigt regelmäßig die übertragenen Daten und die Bandbreite an, die für das angegebene Intervall genutzt wurde, bis die Gesamtdauer des Tests erreicht ist.

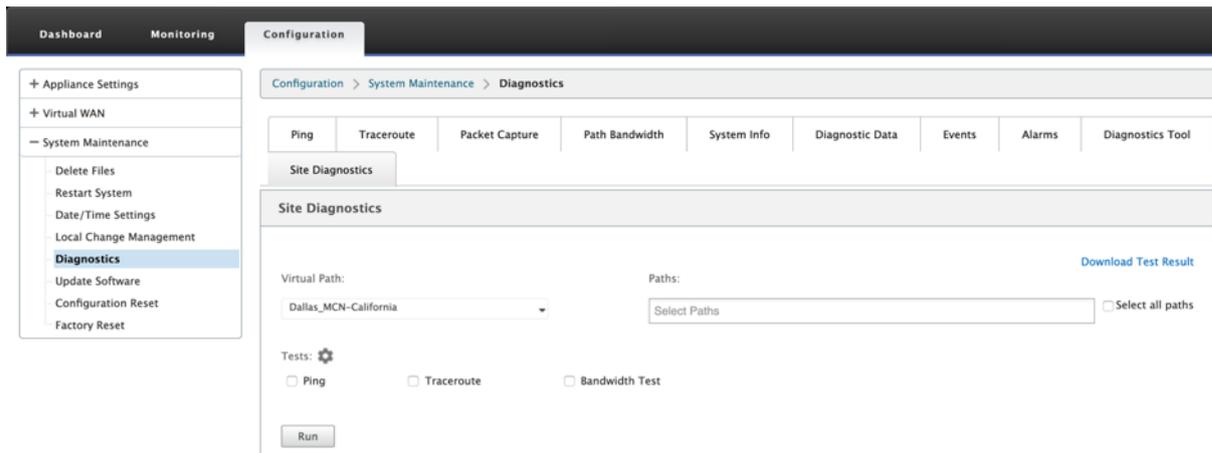
The screenshot shows the 'Diagnostics Tool' configuration page. The 'Tool Mode' is set to 'Client', 'Traffic Type' is 'Data', and 'Port' is '10'. The 'LAN to WAN Paths' dropdown is set to 'MCN_184_78-Broadband'. A 'Start' button is visible. Below the configuration is a 'Results' section with a 'stop' button and a terminal window showing the test output.

```
Client connecting to 172.16.31.10, TCP port 10
Binding to local address 172.16.21.10
TCP window size: 112 KByte (default)
-----
[ 3] local 172.16.21.10 port 39993 connected with 172.16.31.10 port 10
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0- 1.0 sec  10.1 MBytes 84.9 Mbits/sec
[ 3] 1.0- 2.0 sec  11.9 MBytes 99.6 Mbits/sec
[ 3] 2.0- 3.0 sec  13.4 MBytes 112 Mbits/sec
[ 3] 3.0- 4.0 sec  15.1 MBytes 127 Mbits/sec
[ 3] 4.0- 5.0 sec  14.5 MBytes 122 Mbits/sec
[ 3] 5.0- 6.0 sec  14.5 MBytes 122 Mbits/sec
[ 3] 6.0- 7.0 sec  15.1 MBytes 127 Mbits/sec
[ 3] 7.0- 8.0 sec  15.1 MBytes 127 Mbits/sec
[ 3] 8.0- 9.0 sec  15.6 MBytes 131 Mbits/sec
[ 3] 9.0-10.0 sec  16.0 MBytes 134 Mbits/sec
[ 3] 0.0-10.0 sec  141 MBytes 118 Mbits/sec
```

Site-Diagnose

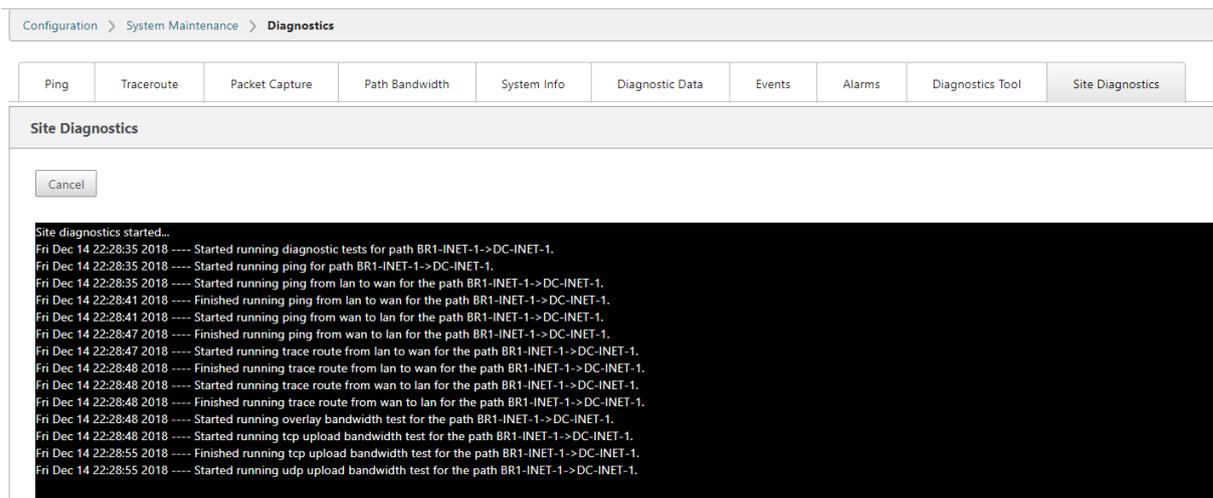
Sie können die Bandbreitennutzung testen, pingen und Traceroute für die WAN-Verbindungen durchführen, die an verschiedenen Standorten im Citrix SD-WAN-Netzwerk konfiguriert wurden. Es enthält Informationen, die bei der Behebung von Problemen in der vorhandenen Konfiguration helfen.

Um **Standortdiagnose** zu verwenden, navigieren Sie zu **Konfiguration** erweitern Sie **Systemwartung > Diagnose** und wählen Sie **Diagnose-Tool**.



Im Ergebnisbereich wird Folgendes angezeigt:

- **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

August 29, 2022

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 Pfad-tabelle 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.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): Help

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

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	Virtu Path Overhe kbps
172.16.14.99	172.16.19.167	LAN to WAN	80	2189	TCP	default	41572	Virtual Path	DC-BR	LOCAL	758	41571	14527110	2.072	6.337	0.8
172.16.14.99	172.16.19.162	LAN to WAN	80	3161	TCP	Override = NO Demote on Large Packets = NO	60	Virtual Path	DC-BR	LOCAL	758	41525	14427708	2.099	6.488	0.8
172.16.14.99	172.16.19.161	LAN to WAN	80	6310	TCP	Separate TCP ACK Class = NO Packet Sequence Inorder = YES	60	Virtual Path	DC-BR	LOCAL	758	41827	14468200	2.115	6.341	0.8
172.16.14.99	172.16.19.170	LAN to WAN	80	10844	TCP	Inorder Holdtime: 900 Late Packet Action = DISCARD	360	Virtual Path	DC-BR	LOCAL	758	41863	14393387	2.110	6.285	0.8
172.16.14.99	172.16.19.164	LAN to WAN	80	3387	TCP	Packet Duplication = NO Persistent Paths = NO	158	Virtual Path	DC-BR	LOCAL	758	41798	14472656	2.070	6.284	0.8
172.16.14.215	172.16.19.99	LAN to WAN	9321	80	TCP	Reliable = YES	14	Virtual Path	DC-BR	LOCAL	758	43483	2592802	2.145	1.022	0.8
172.16.14.99	172.16.19.167	LAN to WAN	80	4200	TCP	TCP Standalone ACKs = NO Check Flow TOS = NO	112	Virtual Path	DC-BR	LOCAL	758	41705	14426227	2.114	6.348	0.8
172.16.14.99	172.16.19.169	LAN to WAN	80	3161	TCP	Deep Packet Inspection = NO IP/TCP/UDP Header Compression = NO	356	Virtual Path	DC-BR	LOCAL	758	40970	14508376	2.054	6.299	0.8
172.16.14.218	172.16.19.99	LAN to WAN	3371	80	TCP	GRE Header Compression = NO Packet Aggregation = NO	407	Virtual Path	DC-BR	LOCAL	758	42980	2552820	2.043	0.967	0.8
172.16.14.99	172.16.19.166	LAN to WAN	80	1116	TCP	TCP Termination = NO Rule ID = 1	113	Virtual Path	DC-BR	LOCAL	758	41286	14568312	2.047	6.220	0.8
172.16.14.213	172.16.19.99	LAN to WAN	17082	80	TCP	VLAN ID = 0 App Rule ID = N/A	161	Virtual Path	DC-BR	LOCAL	758	42915	2556999	2.114	1.006	0.8
172.16.14.217	172.16.19.99	LAN to WAN	4090	80	TCP	DPI Application = http	364	Virtual Path	DC-BR	LOCAL	758	42530	2540882	2.059	0.983	0.8

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.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Flows Data

Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
DC-MCN-BR1-VPX	LOCAL	3	291	435918	85.373	1023.106	36.881	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

Die folgende Abbildung zeigt, 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.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Flows Data

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 LAN 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.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Flows Data

ets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
155	1280790	318.598	3818.082	137.634	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

Die folgende Abbildung zeigt, dass, wenn der 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.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Flows Data

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**.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Flows Data

Flow ID	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
3	551	32640	88.836	42.100	38.377	0.000	0	N/A	9	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Duplicate, Reliable	iperf
4	1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable	iperf

Die folgende Abbildung zeigt, dass 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.

Select Flows

Flow Type: LAN to WAN WAN to LAN Internet Load Balancing Table TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Flows Data

IN IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
CAL	10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Duplicate, Reliable
CAL	0	34213	49055970	267.264	3066.058	115.458	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable

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**.

Flows Data

Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
Local Path	DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

Die folgende Abbildung zeigt, dass wenn der Pfad **DC-MCN-Internet-> BR1-VPX-Internet** latenzanfällig wird oder deaktiviert ist, Sie feststellen, dass 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**.

Flows Data

Toggle Columns

IN / IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
ICAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

Im persistenten Modus 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

August 29, 2022

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 der SD-WAN Standard Edition - physische 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

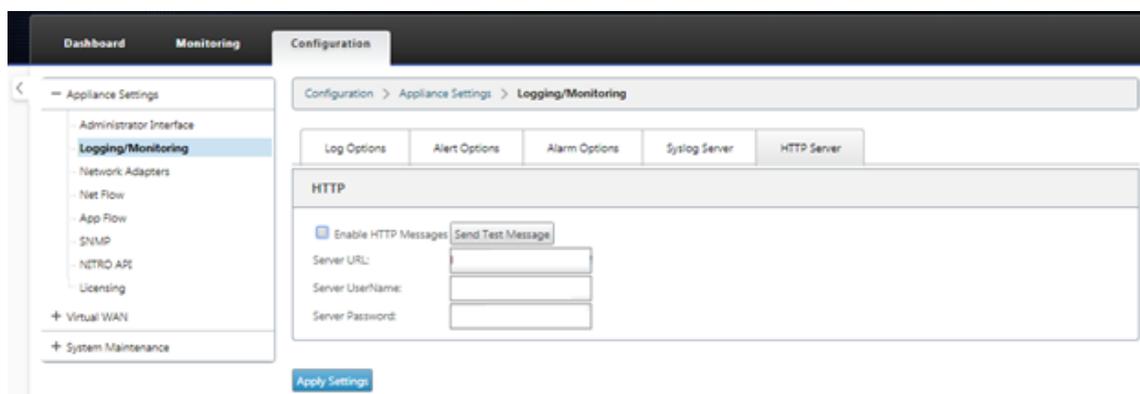
August 29, 2022

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**.

The screenshot shows the 'Logging/Monitoring' configuration page. The 'HTTP Server' tab is selected. The 'Enable HTTP Messages' checkbox is checked. The 'Server URL' field contains 'https://sdwan/nitro/v1/conf'. The 'Server UserName' field contains 'admin'. The 'Server Password' field is masked with dots. A 'Send Test Message' button is visible next to the 'Enable HTTP Messages' checkbox. Below the form is an 'Apply Settings' button.

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.

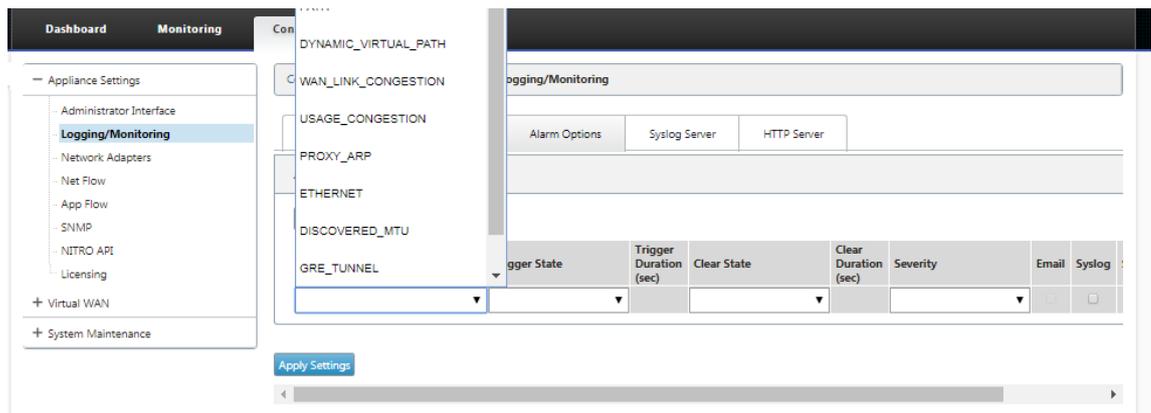
So fügen Sie eine Alarmbenachrichtigung für die HTTP-Server

1. Wechseln Sie auf der Seite **Protokollierung/Überwachung** zur Registerkarte **Alarmoptionen**.
2. Klicken Sie auf **Alarm hinzufügen**.

The screenshot shows the 'Alarm Configuration' page. The 'Alarm Options' tab is selected. An 'Add Alarm' button is visible. Below it is a table with the following columns: Event Type, Trigger State, Trigger Duration (sec), Clear State, Clear Duration (sec), Severity, Email, and Syslog. The table is currently empty. Below the table is an 'Apply Settings' button.

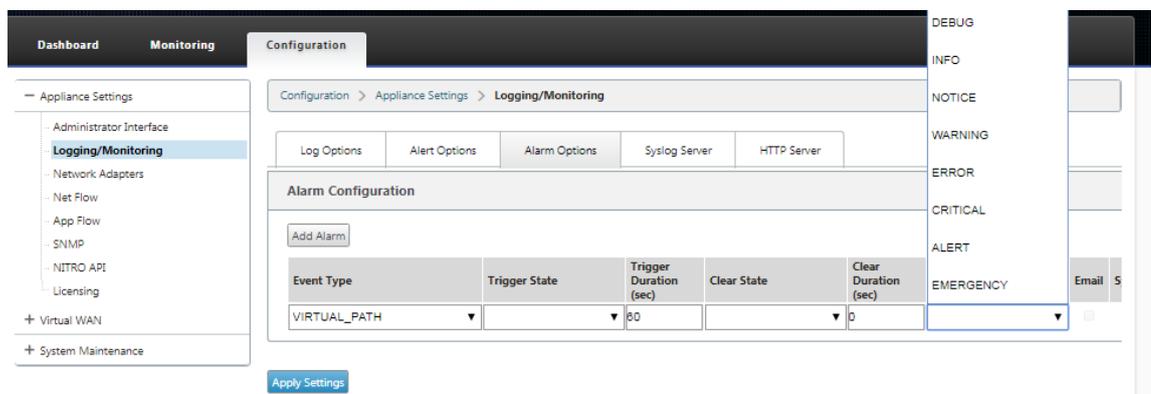
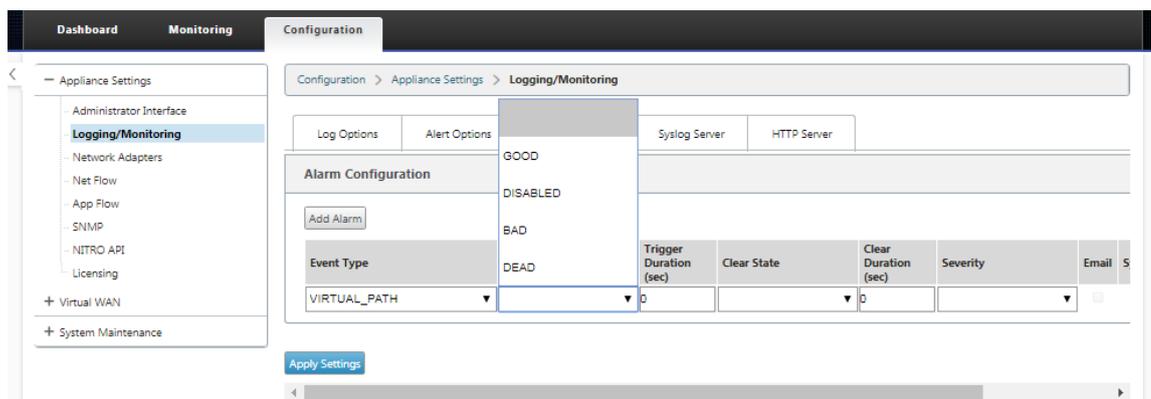
Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog
						<input type="checkbox"/>	<input type="checkbox"/>

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**.

Configuration > Appliance Settings > Logging/Monitoring

Log Options | Alert Options | Alarm Options | Syslog Server | HTTP Server

Alarm Configuration

Add Alarm

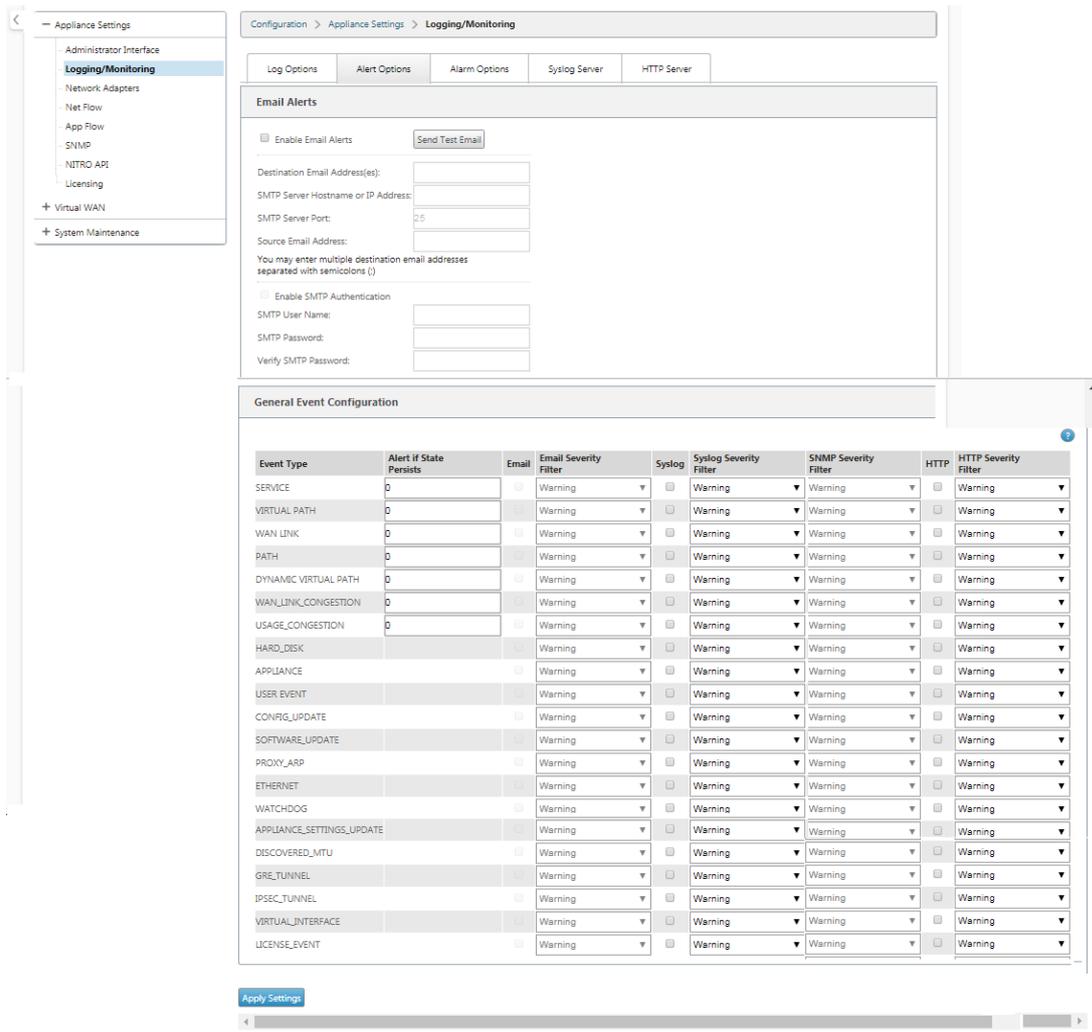
Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog	SNMP	HTTP
VIRTUAL_PATH	DEAD	60	BAD	60	NOTICE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> X

Apply Settings

So konfigurieren Sie Ereignisoptionen:

Wechseln Sie zur Registerkarte **“Warnungsoptionen”**. Wählen Sie auf der Seite **Allgemeine Ereigniskonfiguration** den HTTP-Server-Benachrichtigungsfilter für einen **Ereignistyp** aus und klicken Sie auf **Einstellungen anwenden**.

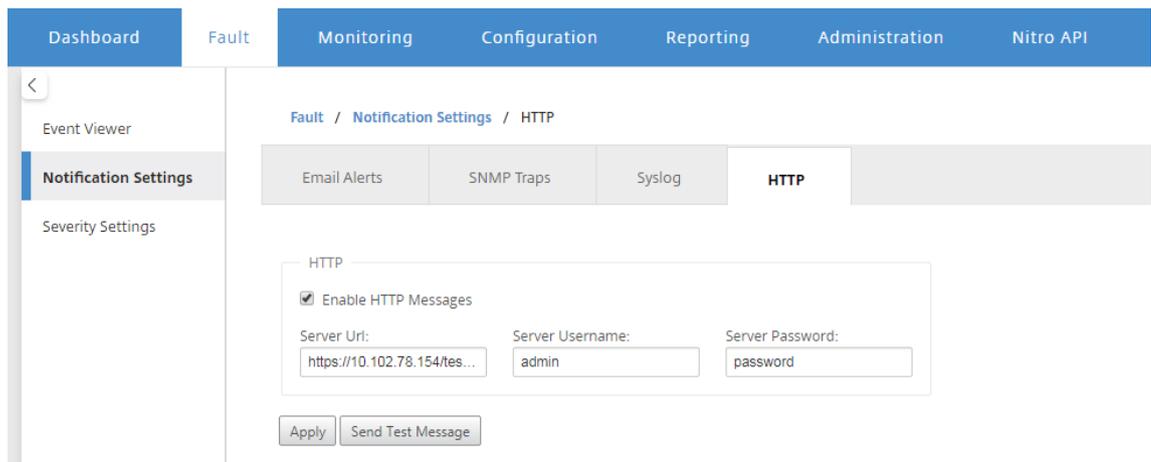
- HTTP
- HTTP-Schweregradfilter



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.

Event Type	Alert if State Persists	Email		Syslog		SNMP		HTTP	
		Enable	Severity Filter						
SERVICE	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WANLINK	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DYNAMIC VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WAN LINK CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USAGE CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼

2. Sie können E-Mail-, Syslog-, SNMP- und HTTP-Ereignisbenachrichtigungen für die folgenden Ereignistypen überwachen. Klicken Sie auf **Anwenden**.

Dashboard | **Fault** | Monitoring | Configuration | Reporting | Administration | Nitro API

Fault / Severity Settings

Event Type	Alert If State Persists	Email		Syslog		SNMP		HTTP	
		Enable	Severity Filter						
SERVICE	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WANLINK	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DYNAMIC VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WAN LINK CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USAGE CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
HARD DISK		<input type="checkbox"/>	WARNING ▼						
APPLIANCE		<input type="checkbox"/>	WARNING ▼						
USER EVENT		<input type="checkbox"/>	WARNING ▼						
CONFIG UPDATE		<input type="checkbox"/>	WARNING ▼						
SOFTWARE UPDATE		<input type="checkbox"/>	WARNING ▼						
PROXY ARP		<input type="checkbox"/>	WARNING ▼						
ETHERNET		<input type="checkbox"/>	WARNING ▼						
WATCHDOG		<input type="checkbox"/>	WARNING ▼						
SD WAN CENTER SYSTEM		<input type="checkbox"/>	WARNING ▼						
APPLIANCE SETTINGS UPDATE		<input type="checkbox"/>	WARNING ▼						
SD WAN CENTER USER		<input type="checkbox"/>	WARNING ▼						
SD WAN CENTER STORAGE		<input type="checkbox"/>	WARNING ▼						
SD WAN CENTER DATABASE		<input type="checkbox"/>	WARNING ▼						
CONNECTION TO VIRTUAL WAN		<input type="checkbox"/>	WARNING ▼						
DISCOVERED MTU		<input type="checkbox"/>	WARNING ▼						
GRE TUNNEL		<input type="checkbox"/>	WARNING ▼						
IPSEC TUNNEL		<input type="checkbox"/>	WARNING ▼						
VIRTUAL INTERFACE		<input type="checkbox"/>	WARNING ▼						
LICENSE EVENT		<input type="checkbox"/>	WARNING ▼						

Apply

Aktive Bandbreitentests

August 29, 2022

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**.

Instant Path Bandwidth Testing

Path: MCN-5100-WL-2->BR572

Test

Results

Minimum Bandwidth: 288584 kbps
 Maximum Bandwidth: 1213883 kbps
 Average Bandwidth: 1109046 kbps

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute
Apply Settings				

History Path Bandwidth Testing Result

Show 50 entries Showing 1 to 27 of 27 entries Search

Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	RCNL-5100-WL-1	MCN-5100-WL-1	2/17/2018, 2:01:03 PM	2883972	5099707	4357230
2	RCNL-5100-WL-1	MCN-5100-WL-1	2/17/2018, 4:01:03 PM	3109115	3872000	3616157
3	RCNL-5100-WL-1	MCN-5100-WL-1	2/17/2018, 6:01:04 PM	3041280	4119960	3518949
4	RCNL-5100-WL-1	MCN-5100-WL-1	2/17/2018, 8:01:04 PM	2769377	3700672	3276124
5	RCNL-5100-WL-1	MCN-5100-WL-1	2/17/2018, 10:01:04 PM	409245	3574153	2489209
6	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:04 AM	2481756	4001684	3198214
7	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 AM	2549853	3872000	3236546
8	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 AM	3204413	3982628	3642643
9	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 AM	2997677	4672357	3664018
10	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:04 AM	2248258	6288360	3612666
11	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:04 AM	2410236	3372387	2816032
12	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:03 PM	2613600	4401852	3563752
13	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 PM	2324266	4059961	3101910
14	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 PM	2173340	3684370	2929146
15	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 PM	2613600	3589499	3021890
16	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:03 PM	1676056	3499380	2655200
17	RCNL-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:03 PM	1954093	3558944	2975804
18	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 AM	2161116	3784398	2902068
19	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 AM	2986971	4079765	3821158
20	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:04 AM	3514084	4181760	3893881
21	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 6:01:03 AM	3358843	4059961	3756691
22	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 8:01:03 AM	3216738	4245441	3716351
23	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 10:01:04 AM	3558944	4202773	3992908
24	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 PM	3427672	4267102	3838552
25	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 PM	2874061	4224000	3605676
26	RCNL-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:03 PM	2816000	6288360	4165337
27	MCN-5100-WL-2	BR572-WL-1	2/19/2018, 5:23:04 PM	936584	1213883	1109046

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 **Site > [Site-Name] > WAN-Links > [WAN-Link-Name] > Einstellungen** erreicht.

Wenn diese Option aktiviert ist, verwendet das System die erlernte Bandbreite.

Sie können auch wiederkehrende Tests der Pfadbandbreite in wöchentlichen, täglichen oder stündlichen Intervallen planen.

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute
DC_MPLS2->Branch_	every day	Sunday	0	0
	every day	Sunday	0	0

Apply Settings

Hinweis

Eine Historie der Ergebnisse der Pfadbandbreitentests wird unten auf dieser Seite angezeigt und die Ergebnisse werden alle sieben Tage archiviert.

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute
-----------	-----------	-------------	------	--------

Apply Settings

History Path Bandwidth Testing Result

show 50 entries Showing 1 to 14 of 14 entries Search

Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	480818
4	BR_1-MPLS-1	DC_MCN-MPLS-1	3/29/2017, 1:34:00 AM	440056	1083357	725514
5	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:10 AM	506768	786784	638673
6	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:18 AM	462584	1388712	669232
7	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:34:27 AM	380679	727895	533286
8	DC_MCN-MPLS-1	BR_1-MPLS-1	3/29/2017, 1:35:12 AM	26823	35495	30578
9	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:09 AM	350097	733929	591542
10	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:47 AM	476024	789756	639048
11	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:36:56 AM	446292	777674	608533

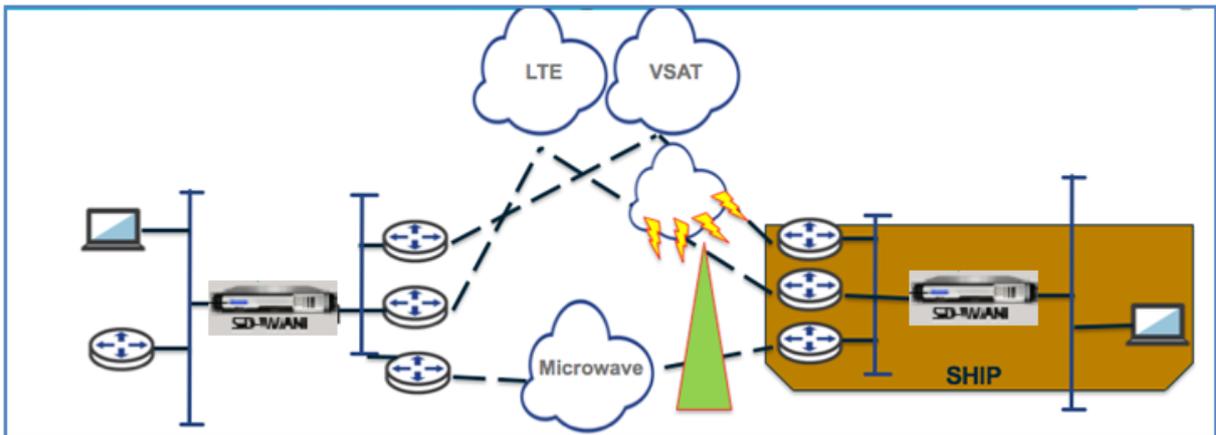
Adaptive Bandbreitenerkennung

November 16, 2022

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. Ab SD-WAN 11.5-Version können Sie es im Citrix SD-WAN Orchestrator Service aktivieren. Weitere Informationen finden Sie unter [Adaptive Bandbreitenerkennung](#).

Zeigen Sie die Tabelle **Nutzungs- und Zulässige Raten** an, indem Sie zu **Überwachen > Statistik > WAN-Link-Nutzung > Nutzung und zulässige Raten** navigieren.

Usages and Permitted Rates

Filter: in Any column

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

August 29, 2022

Die folgenden Themen enthalten die Best Practices, die bei der Planung, Planung und Ausführung der Citrix SD-WAN in Ihrem Netzwerk zu befolgen sind.

[Security](#)

[Routing](#)

[QoS](#)

[WAN-Links](#)

Sicherheit

August 29, 2022

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. Im Falle eines Einbruchs sollte das elektronische Überwachungssystem einen Alarm an das Sicherheitspersonal senden, um sofort reagieren zu können.

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.

Schützen der Stromversorgung - Stellen Sie sicher, dass das Gerät mit einer unterbrechungsfreien Stromversorgung geschützt ist.

Gerätesicherheit

Um die Appliance-Sicherheit zu gewährleisten, sichern Sie das Betriebssystem eines beliebigen Servers, der eine virtuelle Citrix SD-WAN-Appliance (VPX) hostet, führen Sie Remote-Softwareupdates und die folgenden sicheren Lebenszyklusverwaltungsmethoden durch:

- Sichern Sie das Betriebssystem des Servers, der eine Citrix SD-WAN VPX-Appliance hostet - Eine Citrix SD-WAN VPX-Appliance wird als virtuelles Gerät 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 der Security Bulletins können Sie sich registrieren und aktuelle Sicherheitswarnungen 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.
- Stellen Sie die Verwaltungsschnittstelle der Appliance hinter der DMZ bereit, um sicherzustellen, dass kein direkter Internetzugang auf die Verwaltungsschnittstelle besteht. Stellen Sie für zusätzlichen Schutz sicher, dass das Verwaltungsnetzwerk vom Internet isoliert ist und nur autorisierte Benutzer mit zugelassenen Verwaltungsanwendungen im Netzwerk ausgeführt werden.

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 die für die Bereitstellung geeigneten Verwaltungs- und Verwaltungsschutzmaßnahmen.

- 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 Kennwörter für Admin- und Anzeigekonten 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
- Schlüssel

Sonstiges:

- Timeout der Webkonsole

The screenshot shows the 'Administrator Interface' configuration page for the 'HTTPS Cert' section. The left sidebar lists various configuration areas, with 'Administrator Interface' selected. The main content area is titled 'Configuration > Appliance Settings > Administrator Interface' and contains several tabs: 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', 'HTTPS Settings', and 'Miscellaneous'. The 'HTTPS Cert' tab is active, displaying the 'Installed Certificate' details. Below this, there are sections for 'Upload HTTPS Certificate Files' and 'Regenerate HTTPS Certificate'.

Installed Certificate

Issued to:	Issuer:
Country: US	Country: US
State/Province: California	State/Province: California
Locality: San Jose	Locality: San Jose
Organization: Citrix Systems, Inc.	Organization: Citrix Systems, Inc.
Organizational Unit: Engineering	Organizational Unit: Engineering
Common Name: Citrix	Common Name: Citrix
Email: support@citrix.com	Email: support@citrix.com

Certificate Details:

Certificate Fingerprint: 24:BF:11:86:0F:32:AE:6A:DA:86:32:E3:F7:C3:D3:9B:30:51:A2:D5
 Start Date: Mar 20 03:35:15 2017 GMT
 End Date: Mar 18 03:35:15 2027 GMT
 Serial Number: C5586E258899CF6

Upload HTTPS Certificate Files

Upload the certificate that secures the Management HTTPS connection to this Virtual WAN appliance. Uploading and installing the HTTPS Certificate will cause the HTTP server to restart, invalidating all connected sessions.
NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance.

Certificate Filename: No file chosen
 Key Filename: No file chosen

Regenerate HTTPS Certificate

Regenerate the certificate that secures the Management HTTPS connection to this Virtual WAN appliance. Regenerating the HTTPS Certificate will cause the HTTP server to restart, invalidating all connected sessions.
NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance.

Erwägen Sie die Verwendung der Citrix Web App Firewall

Citrix ADC lizenzierte Appliance bietet eine integrierte Citrix Web App Firewall, die ein positives Sicherheitsmodell verwendet und automatisch das richtige Anwendungsverhalten zum Schutz vor Bedrohungen wie Befehlseinschleusung, SQL-Einschleusung und Cross Site Scripting lernt.

Wenn Sie die Citrix Web App Firewall verwenden, können Benutzer der Webanwendung zusätzliche Sicherheit hinzufügen, ohne Codeänderungen und mit geringen Konfigurationsänderungen. Weitere Informationen finden Sie unter Einführung in die [Citrix Web Application Firewall](#).

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 Nachrichtenaufentifizierung 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. Dadurch wird die Ausgabe der Verschlüsselung randomisiert und eine starke Botschaft geliefert, 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.

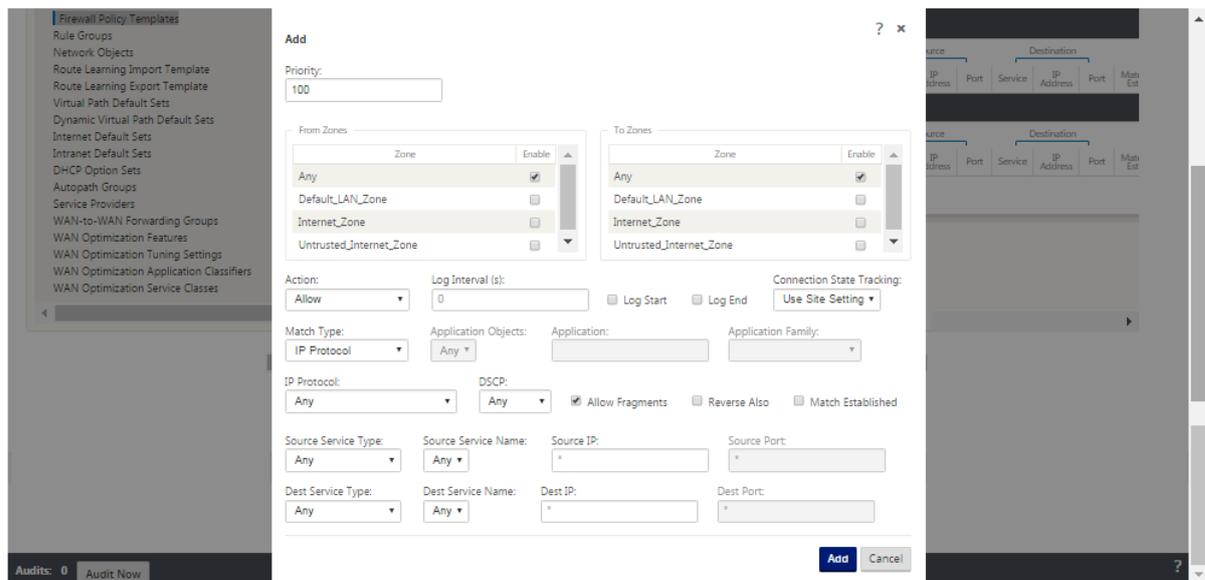
Globale Firewall-Vorlagen - Firewall-Vorlagen ermöglichen die Konfiguration globaler Parameter, die sich auf den Betrieb der Firewall auf einzelnen Appliances auswirken, die in der SD-WAN-Overlay-Umgebung arbeiten.

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 Vererberben werden automatisch mit der standardmäßigen Routingdomäne verknüpft.

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 zur Identifizierung des Peers erfolgen, 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.
- Die Überprüfung der Peer-Identität ermöglicht die Validierung der Peer-Identität des IKE, wenn der ID-Typ des Peers unterstützt wird. Andernfalls aktivieren Sie diese Funktion nicht.
- Diffie-Hellman-Gruppen sind für die IKE-Schlüsselgenerierung mit Gruppe 1 bei 768 Bit, Gruppe 2 bei 1024-Bit und Gruppe 5 bei 1536-Bit-Gruppe verfügbar.
- 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 identifiziert werden, indem Sie die Upstream-Router- und Firewall-Konfiguration überprüfen:

- 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 Dienstyp (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

August 29, 2022

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 Zweigstelle-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

August 29, 2022

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 einer Regel hinzugefügt, um die Konfiguration zu vereinfachen, 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

August 29, 2022

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

August 29, 2022

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 Zweigseinheit 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 Rückgewinnung 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				
Site Name	Scheduling Information	Status	Edit	
<input type="checkbox"/> GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> MCNVXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> MCNVXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			
<input type="checkbox"/> RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)			

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** beschrieben. 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**

Managementgeklickt wird. Sie können das Netzwerk aktivieren, indem Sie auf die Schaltfläche **“Staged aktivieren“** klicken oder auf **“Vorbereitung ändern“** klicken, um den Status abubrechen, 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.

Referenzmaterial

August 29, 2022

[Anwendungssignaturbibliothek](#)

Eine Liste der Anwendungen, die die Citrix SD-WAN Appliances mithilfe der Deep Packet Inspection identifizieren können.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).
