

NetScaler SD-WAN 10.0

Apr 04, 2018

The NetScaler SD-WAN product was formerly called "CloudBridge". Refer to the links below to access CloudBridge documentation.

CloudBridge

[CloudBridge 9.0](#) [CloudBridge 8.1](#) [CloudBridge 8.0](#) [CloudBridge 7.4](#) [CloudBridge 7.4](#) [CloudBridge 7.3](#)

NetScaler SD-WAN appliances are available in three different editions, allowing you to deploy the features you need at each location with easy upgrades, configuration, and monitoring.

Note

All references to the term "CloudBridge" are applicable to the new product term "NetScaler SD-WAN".

For more information about the NetScaler SD-WAN platform editions, see the product datasheet and product portfolio at https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-sd-wan-datasheet.pdf and <https://www.citrix.com/products/netscaler-sd-wan/platforms.html>.

Important

For information about NetScaler SD-WAN WANOP 10.0, 9.1, 9.2, and 9.3 installation, deployment, and feature configuration, please refer to the [CloudBridge 7.4](#) documentation. The features and procedures for the NetScaler SD-WAN WANOP 10.0, 9.1, 9.2, and 9.3 are similar to the procedures documented in CloudBridge 7.4 release.

Command Center End of Life Notification:

End of Life process for **Citrix Command Center** tool was initiated on 15-May-2017.

It is recommended that you migrate to the new management tool **NetScaler MAS** for your WAN Optimization deployments at the earliest.

Please refer to the articles below for the Command Center EOL calendar and associated details.

- [CTX223806 - Notice of Status Change Announcement for Citrix Command Center Software Version 5.2](#)
- [CTX223786 - FAQ: Citrix Command Center - End Of Life](#)

Citrix Command Center tool for NetScaler SD-WAN WANOP edition is supported only till the NetScaler SD-WAN 9.2 appliance software release.

Starting with the NetScaler SD-WAN 9.3 software release, NetScaler MAS will be the management tool for SD-WAN WANOP edition appliances.

NetScaler SD-WAN Platform Editions

There are three NetScaler SD-WAN Editions each with a different set or subset of NetScaler SD-WAN features.

- **NetScaler SD-WAN Enterprise Edition (EE)** – This Edition includes both Standard Edition and WAN Optimization features. Enterprise Edition Integrates WAN virtualization with WAN optimization capabilities to optimize branch and mobile user experience and to achieve fully resilient applications regardless of network quality. For release 9.1, Enterprise Edition is available for the 1000 and 2000 Standard Edition branch hardware appliances, only.
- **NetScaler SD-WAN Standard Edition (VW/SE)** – This Edition includes Standard Edition Virtual WAN features, only. It supports software-defined WAN capability to create a highly reliable network from multiple network links and to ensure that each application takes the best path to achieve the highest application performance.
- **NetScaler SD-WAN Optimization Edition (WANOP)** – This Edition includes WAN Optimization features, only. It supports application acceleration, data reduction and protocol control to optimize applications across the WAN. Optionally, it can include virtual Windows Server to simplify branch infrastructure and mobile PC plug-in capability.

Note

The WANOP Edition and Standard/Enterprise Edition are separate hardware platforms running different software.

In a data center, administrators can deploy one Standard Edition and one WANOP Edition to achieve Enterprise Edition capabilities. In the branch office, administrators can choose to deploy either a Standard Edition or WANOP Edition. Alternatively, the benefits of both Standard and WANOP Editions can be accomplished by deploying a single Enterprise Edition at the branch office.

See the [Licensing](#) section, for more information about the license options available for using NetScaler SD-WAN platform editions.

What's New

Mar 02, 2018

The NetScaler SD-WAN release version 10.0 introduces the following new features and enhancements:

Application Support

HTML 5 Receiver and HDX Adaptive Transport Support

Support for classification of HTML5 receiver, and Adaptive Transport HDX traffic is added. When classified, these applications can be used in application rules, and to view application statistics.

Custom Application Reporting

You can create custom applications and enable reporting for them. Reporting statistics for the user created custom applications can be viewed and filtered in NetScaler SD-WAN Center.

Configuration

Partial Software Upgrade Using Local Change Management

NetScaler SD-WAN 10.0 allows the network administrator to upgrade the software on the sites in the network selectively, without needing to upgrade all sites simultaneously. A specific use-case for this feature is an administrator who wants to test the new software on few branch sites before installing it on all sites in the network.

Ability to Create a GEO MCN by Cloning the MCN and Geo RCN by Cloning the RCN

You can configure a site as the secondary / geo MCN to support MCN redundancy. The secondary / geo MCN continuously monitors the health of the primary MCN. When the primary MCN fails, the secondary / geo MCN assumes the role of the MCN. In NetScaler SD-WAN 10.0, you can create a secondary MCN easily by cloning the primary MCN.

Multi-region deployment uses Regional Control Nodes (RCN) to control the client sites in a geographical or administrative region. You can also clone the RCN to create a secondary / geo RCN.

Scalability

Ability to scale NetScaler SD-WAN deployment for 2,500 sites

Scalability is achieved by defining regions and managing regions using the Region Controller Nodes (RCN). The MCN manages the RCNs in the network and the RCN manages the client sites in its region, allowing the user to centrally manage large scale Enterprise / MSP deployments.

Monitoring

Improved Application Bandwidth Usage by using Path Mapping

Path mapping and bandwidth usage enhancements are implemented. Based on the incoming traffic bandwidth demand, the traffic is processed in load balanced transmission mode, duplicate transmit mode, or persistent path transmit mode. You can monitor the path information for traffic flows in **Monitoring > Flows**, under **Paths** column. You can also hover your mouse cursor over any flow to view the DPI application name.

License Management

Centralized Licensing

- In the new centralized license model, an administrator can manage licensing from a central licensing server without having to access the appliance in the network. You can configure the IP address of a remote server as the licensing server and select the configuration to the appliances in the network.
- NetScaler SD-WAN Center can be configured as the [licensing server](#).

Routing

Support for BGP Soft Reconfiguration

Support for BGP route refresh as per RFC 2918 to assist non-disruptive route-policy changes is added.

Support for Enterprise/MSP to Scale 64 K Route table for all appliances

The number of routes supported on all appliances is scaled from 16000 to 64000.

Capability to Create Summary Routes for Sites

Route summarization reduces the number of routes that a router must maintain. A summary route is a single route that is used to represent multiple routes. In NetScaler SD-WAN 10.0, you can configure a summary route by using Local and Discard service types. The summary route is advertised to the peer SD-WAN appliances as the only route that encompasses all subnets falling as part of the summary route instead of sharing all subnet routes.

Capability to provide preference for which Data Center a site uses based on Virtual Path Route Cost

An administrator can decide which data center can be the most preferred by influencing route costs based on the new Virtual Path Route Cost feature.

- Virtual path route cost: You can configure Virtual Path route cost for individual virtual paths that are added to the route cost when a route is learnt from a remote site. With the introduction of VP route cost, the WAN to WAN forwarding cost is deprecated, because VP route cost helps influence the decision henceforth.
- OSPF route cost: You can now import OSPF route cost (type1 metric) by enabling “**Copy OSPF Route Cost**” in import filters. OSPF Route cost is considered in route selection instead of SD-WAN cost. Cost up to 65534 instead of 15 is supported, but it is advisable to accommodate for appropriate virtual path route cost that is added when route is learnt from a remote site.
- BGP - Copy VP Route cost to MED: You can now copy Virtual Path route cost for SD-WAN routes into BGP MED values when exporting (redistributing) SD-WAN routes to BGP peers. This can be set for individual neighbors by creating a BGP policy and applying it in the “OUT” direction for each neighbor.

Capability to create Import/Export Route Policy Templates for Large-scale Deployments

You can now create multiple import or export filter templates by using various filter rules and associate the template at each site. The user created site level import/export filter rules take more precedence. The template rules follow the user created rules when associated to the site in Route learning section of Connections.

Using CLI to Access Routing Functionality

You can view additional information related to dynamic routing and the protocol status. Type the following command and syntax to access routing daemon and view the list of commands.

```
dynamic_routing?
```


This is a restricted CLI access for debugging routes.

Support added for Virtual Router Redundancy Protocol

VRRP provides device redundancy to eliminate the single point of failure inherent in the static default-routed environment. VRRP ensures a high availability default path without configuring dynamic routing or router discovery protocols on every end-host. NetScaler SD-WAN 10.0 supports VRRP version 2 and version 3 to inter-operate by using any third party routers. VRRP cannot be used between two NetScaler SD-WAN appliances. It can be used between NetScaler SD-WAN appliance and the peer routers that are standard VRRP RFC compliant routers.

Application Based Traffic Steering

You can create application routes using application objects. This application routes aids in steering the traffic based on DPI or IP infrastructure using various SD-WAN services, such as Virtual Path, Internet, Intranet, Local, GRE, or IPsec.

Support added for Multicast IGMP/MLD Proxy

By using static multicast group, network administrators can control the source and destination of the multicast traffic. In NetScaler SD-WAN 10.0, users can statically configure multicast groups and enable IGMP Proxy for updating the upstream code networks by using all the sources in the downstream networks of the edge

NetScaler SD-WAN Center

Multi-Region Deployment

A hierarchical tiered network architecture is introduced to enable higher scale, and delegation of regional administration in NetScaler SD-WAN 10.0. NetScaler SD-WAN Center supports multi-region mode deployment, RCN discovery, and SD-WAN collector configuration and software upgrade.

Dashboard

- The NetScaler SD-WAN center 10.0 dashboard includes a multi-region summary dashboard. This dashboard provides a graphical overview of the network health at the various regions.
- You can view the network maps in either the tile view or the schematic view.

NetScaler SD-WAN Center License Server

You can now configure NetScaler SD-WAN Center to act as the remote license server for centralized license management.

Platforms

SD-WAN VPX-SE/VPXL-SE Platforms in VMWare ESXi – 10G NIC Support

Support added for 10G Virtual Ethernet interfaces on the SD-WAN VPX-SE/VPXL-SE appliances in the VMware ESXi deployment. You can enable this feature by changing the driver for the virtual NIC from E1000 when deploying and configuring SD-WAN VPX-SE/VPXL-SE platforms using VMware ESXi.

NetScaler SD-WAN Standard Edition – 1 Gbps support on Hyper-V Platform

Support for 1Gbps throughput for SD-WAN Standard Edition platforms deployed on Hyper-V is added.

Virtual Ethernet Ports per VPX-SE/VPXL-SE Platforms

Support for more ports for VPX-SE HA deployments between servers is added. This support would enable customers to

map high availability interfaces one-to-one to real ports to avoid any hypervisor misconfiguration that would separate the virtual appliances and cause both virtual appliance to become active.

Maximum Network Interfaces Supported by SD-WAN VPX-SE appliances

In release 10.0, the number of maximum network interfaces supported by the SD-WAN VPX-SE platforms is 8 unlike in previous release versions in which the number of network interfaces supported was only 4.

NetScaler SD-WAN 2100 Enterprise Edition Appliance

- NetScaler SD-WAN 2100 EE new platform edition is introduced.

REST API

- Enhancement to current appliance configuration for REST APIs to include Site, WAN Link, Virtual Path, Firewall, Quality of Service, DPI, iPerf, and Management IP.
- Support for local user and group management REST APIs.
- Capability to update the NetScaler SD-WAN Appliance OS and License files using REST APIs.
- Enhance current monitoring REST APIs to include WAN Link, Virtual Path, Firewall, Quality of Service, Applications, and Flows.
- Introduced REST APIs for NetScaler SD-WAN Center.

Release Notes

Mar 01, 2018

This release note describes known issues, and fixed issues applicable to Citrix NetScaler SD-WAN software release 10.0 for the SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances.

For information about the previous release versions, see the [NetScaler SD-WAN](https://docs.citrix.com) documentation on docs.citrix.com.

Fixed Issues

SD-WAN appliance

Issue ID 700046: NetScaler SD-WAN appliance crashes when you try to generate STS while processing high traffic volume.

SD-WAN VPX appliance high availability Deployment

Issue ID 693737: In a high availability deployment with NetScaler SD-WAN VPX appliance on VMware ESXi platform, the virtual path service becomes inactive.

MPLS Quality of Service Queues

Issue ID 697906: NetScaler SD-WAN service is disabled when MPLS Quality of Service queues with all tagged queues are configured through a WAN Link Template, and on receiving a packet without DSCP tag.

ICMP request

Issue ID 695993: Packets sent to the SD-WAN (IP host) Virtual IP address from a trusted WAN interface is dropped when the flow table is exhausted or unable to allocate flows. In this case, proper ICMP reply was expected from the SD-WAN appliance.

IPsec Virtual Path

Issue ID 699665: When you configure Virtual Path IPsec between MCN appliance and two of the branch appliances, and when you attempt to send traffic from Branch1 appliance to Branch2, WAN-to-WAN forwarding packets with large size are dropped by IPsec due to buffer overflow.

GRE Tunnels

Issue ID 700183: When GRE tunnel is transmitted through an untrusted interface, for example, Internet Service, the ping requests are responded, but the IP host will not forward replies/messages back to the GRE tunnel.

Issue ID 699982: When GRE Routes with Gateway eligibility are enabled, ICMP Packets to check gateway eligibility are not guaranteed to be transmitted through the GRE Tunnel.

When the tunnel is down or the gateway address does not route to the tunnel, the packet uses standard IP routing. This leads to a GRE route being eligible inappropriately.

DPI processing

Issue ID 700285: Do not update VLAN ID in the packet descriptor after DPI processing is complete.

DPI multi-thread

Issue ID 700247: When DPI multi-threading is enabled, it can cause conn_mgr/other threads to wait for connection lock on platforms. This occurs when the release conn->lock is removed before returning from firewall.

DPI – Dual-mode IPERF test identifies traffic only from one node

Issue ID 678131: When dual-mode IPERF test is performed between two appliances, the traffic in NetScaler SD-WAN web management interface under **Monitoring > Firewall > Connections** with DPI identifies traffic flow only from one of the connections.

BGP Peering

Issue ID 700585: Disabling service on SD-WAN appliances configured with BGP peering for more BGP hold time duration, results in the BGP session becoming disabled after enabling the service.

Routing

Issue ID 703248: Ensure that you always enable the **Internet for all Routing Domain** option with multiple routing domains for the WAN link which is enabled to carry internet traffic. You should not enable this option for the WAN link which is not enabled to carry internet traffic.

DHCP-410 SE appliance

Issue ID 701855: DHCP is enabled on lights out management by default on some factory shipped 410-SE appliances. Assign an unreachable IP address to the LOM.

Two Box Mode

Issue ID 700181: The ability to reconfigure or disable two box mode is not possible when caches are configured with any other subnets other than /24.

Change Management process

Issue ID 698803: As part of change management procedure during SD-WAN appliance staging phase, configuration fails when you change MTU on the intermediate router to 600.

IPsec Tunnel Configuration

Issue ID 681121: On a NetScaler SD-WAN VPX appliance, a web GUI error is displayed and configuration fails when you try to add and configure IPsec tunnel through the SD-WAN configuration editor.

Workaround: Configure IKE and IPsec parameters except protected networks and save the configuration. Edit the configuration to add protected networks.

Enterprise Edition as MCN – SSL Profile

Issue ID 680199: On a factory shipped Enterprise Edition appliance when you create an SSL profile and associate a Service Class to the profile with unidirectional setting, the SSL profile is not checked/enabled in the SSL Profile page of the SD-WAN EE web GUI. In addition, the service class is not associated to the SSL profile.

Workaround: Create a SSL profile and associate unidirectional service classes.

Known Issues

Platform

SD-WAN VPX Appliances

Issue ID 694837: For High Availability in AWS (AWS) environment, Virtual WAN service is disabled on a NetScaler SD-WAN VPX Primary (active) appliance citing duplicate IP address when the high availability interface on the primary appliance goes down.

Issue ID 702889: RCN branch that is changed from GEO to Client does not get updated to latest build even though it has an active Virtual path available by using the RCN.

Issue ID 701517: Over provisioning of the XenServer can lead to SD-WAN VPX appliance crash.

SD-WAN 4000 WANOP and 4000 SE

Issue ID 681550: On a NetScaler SD-WAN 4000 WANOP appliance, uploading DER encoded certificate for the SSL profile is ignored and no error message is displayed in the web GUI. Only PEM encoded certificates are accepted.

SD-WAN 2100 EE and 5100 EE

Issue ID 704923: The Domain Join/ Delegate user Pre-check Tools Summary Status table is not displayed you try to access them.

Workaround: You can obtain the status summary by selecting the 'More' option in the summary dialog page.

Two Box Mode

Issue ID 681680: After a factory reset on the SD-WAN SE appliance in a two box mode, configuration sync between SD-WAN WANOP and SD-WAN SE appliances fails due to stale SSL certificates.

Workaround: Disable and re-enable two-box mode on the SD-WAN WANOP appliance.

SD-WAN 1000 / 2000

Issue ID 681663: When you upgrade SD-WAN 1000 / 2000 appliance from release build version 9.1.2.26 to 9.2.x, a warning is displayed in the browser.

Workaround: Perform the upgrade in an in-cognito mode window of the Google Chrome browser.

HDX CGP over SSL

Issue ID 690794: HDX ICA/CGP over SSL session's behavior In Virtual WAN Standard Edition:

- HDX sessions are not being negotiated as multi stream sessions even though MSI is enabled on the appliance and MSI+MP policies are set on incoming ICA traffic.
- HDX traffic is classified as belonging to HTTP Secure (https) application and web family.
- HDX traffic falls under **interactive_very_low** class. This can cause issues in QoS, bandwidth allocation and so on as application Quality of Service will not be triggered because the traffic is not classified as HDX sessions.

Configuration

Virtual WAN Configuration

Issue ID 704926: Configuration error occurs when you attempt to override service in a Virtual Path by changing the IP Rule properties.

Issue ID 704156: Activating LCM package for RCN on an appliance with release version 9.x, prepares packages for its branches only when virtual path with MCN is active and running.

Issue ID 704160: The Site Name in Virtual WAN configuration should be configured with alpha numeric characters between 3-15 characters only. This is due to the hostname restrictions in WAN Optimization which is required for domain join operation.

Issue ID 704645: Appliance staging of latest software version might not occur for some Regional Control Node (RCN) and its branch sites.

Workaround: Download the LCM package for RCN, and perform local change management on RCN only to upgrade the RCN network to latest build. This applies latest software version to all RCN branch sites.

Application Steering

Issue ID 699285: The Application family added as one of the match types in the Application Object which is used for Application Routes configuration is not considered for steering.

Custom Application Reporting

Issue ID 703794: If an existing application name is changed and change management is performed, the new application name might not be listed in the SD-WAN Center under the **Top Sites-> Application** drop-down menu. When the page is hard refreshed, then the new application name gets listed and reported, when traffic matches the application.

WAN GRE Tunnel

Issue ID 681171: A NetScaler SD-WAN appliance does not reassemble fragmented GRE tunnel packets properly.

Transparent proxy support for TLS 1.2

Issue ID 691900: In NetScaler SD-WAN WANOP 9.3.0, for SSL compression the SSL profile has to be configured in split mode only as transparent proxy mode is not supported.

Change Management (Single Step Upgrade) SD-WAN GUI

Issue ID 691571: On low-end platform editions, such as the SD-WAN 400, 100, 2000, or VPX appliances by using 4 GB or smaller memory assigned, if concurrent local change management package downloads are initiated the appliance runs out of memory and becomes unresponsive.

Workaround: Download local change management package one at a time, this reduces the load on the appliance.

Issue ID 691953: During software upgrade on an appliance using a Standard Edition license, a WAN optimization related warning message appears. After the scheduled upgrade and after the WAN optimization, SVM and XenServer hotfixes are installed the warning message is cleared.

Workaround: Clear the warning messages manually or open the SD-WAN web UI in an incognito browser window.

Issue ID 705037: In the new **Global Multi-Region Summary** table, the “**Total Sites**” value appeared is less than the sum of the remaining columns. For example; if a branch node is not connected, it is possible that the branch is counted twice; once as “Not Connected” and once as “Preparing/Staging.”

Secure Peering Certificate and Keys

Issue ID 695363: In the SD-WAN GUI, on the Secure Peering Certificate and Keys page, the CA certificate contents are displayed if the private CA radio button is selected after setting the Keystore password on a new appliance.

Workaround: You need to switch between the radio buttons of the 'Private CA' and 'CA Certificate' once to get the correct contents displayed under 'Private CA' and 'CA Certificate' for Secure Peering Certificate and Keys.

Multicast Traffic

Issue ID 694894: When you configure Application Quality of Service rule with match type as "Application" to match 'icmp' and change the class to Real-time, and mode to load balance which overrides the default rule, the multicast traffic is not processed.

Routing

Issue ID 704561: Unable to make the routing domain as default for a site after disabling it.

Workaround:

1. Disable site routing domain (all).
2. Enable routing domain for the site without making it default. Select **Apply**.
3. Make the enabled routing domain for the site as default. Select **Apply**.

Issue ID 705255: Dynamic routes can be installed by using path eligibility, LOCAL service as part of Import filters. In NetScaler SD-WAN 10.0, if the path becomes inactive, then all routes are termed as REACHABLE – YES, and ELIGIBLE - NO instead of REACHABLE - NO and ELIGIBLE – NO. These routes which are ineligible will stay in the remote SD-WAN routing table instead of being purged.

DPI Functionality

DPI- ICMP Functionality

Issue ID 677356: A firewall policy for blocking ICMP as an application blocks only pings (echo requests). All other ICMP types are allowed to pass through.

Workaround: Instead of blocking ICMP as an application, block **IP-protocol > ICMP**.

DPI –Traffic for Top App Family as "Standard" and Top App as "Unknown Virtual protocol" for a Standard Edition appliance

Issue IDs 678373, 678339, 678545, 675063, 676017: On a NetScaler SD-WAN Standard Edition appliance, enable EDT policy for MSI+MP for Win7 and Win2K12 XenDesktop 7.12 VDAs on ports 2598, 2599, 2600, 2601 and subsequently disable Session Reliability policy for Win7 VDA.

Start sending internet traffic and check the monitoring flows in the Standard-Edition web management interface for Classes, Rule groups – ICAUDP and ICACGPUDP, and Firewall. Check the Dashboard and Reporting page in SD-WAN Center web management interface. The results display **Top Application Family** as **Standard** and **Top Applications** as **Unknown**

Virtual Protocol.

SD-WAN Center

Issue ID 693436: The clear connections/flows clear SD WAN connection table entries and all the later ICA sessions. The SD-WAN Center dashboard shows incorrect results for HDX TCP and EDT classification sessions and reports it as "Not Classified."

Issue ID 693026: For HDX configuration, only UDP ICA sessions are classified by ICA classifier. The Framehawk ICA session is ignored. The SD-WAN DPI fails to classify the Framehawk sessions.

Issue ID 704713: The Licensing tab under Configuration view in the SD-WAN Center UI displays the "Under Construction" message after an upgrade from release version 9.3 to release version 10.0.

Workaround: You can clear the browser cache with Ctrl+Shift+R on Chrome, Shift+Ctrl+Delete in a Mozilla browser, after which the UI displays the Licensing tab. You can also log out and log in after you upgrade the SD-WAN Center.

SD-WAN 10.0.1 Release Notes

Apr 09, 2018

This release note describes what's new, known issues, and fixed issues applicable to Citrix NetScaler SD-WAN software release 10.0.1 for the SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances and NetScaler SD-WAN Center.

For information about the previous release versions, see the [SD-WAN](#) documentation.

What's New

The NetScaler SD-WAN release version 10.0.1 introduces the following enhancements:

- Improved stability and minor bug fixes related to the Routing, Configuration and Change Management, Upgrade, and Diagnostics (STS improvements) functionality.
- Support for 2 Gbps license model on the SD-WAN 2100-Standard Edition Platform.
- Single sign-on access from SD-WAN Center to MCN Change Management for admin user privilege.
- DHCP support; next-server and filename parameter configuration.
- Support for configuration of two DHCP Relay addresses to deploy DHCP topology.

Fixed Issues

Change Management process

Issue ID 706577: During the change management staging process on an SD-WAN 1000 appliance, a branch node might remain in the unpacking phase for a long duration.

Issue ID 702890: When you use the Single-Step Upgrade feature on the change management screen, it is possible for a branch node status to show as 'Failed' even though the change management process is successful.

Configuration

Issue ID 705855: After configuration activation, the SD-WAN service might crash when traffic flow is moved from one WAN service to another WAN service where NAT'ing is enabled.

Traffic

Issue ID 707003: In NetScaler SD-WAN release version 9.3.3, generation of STS in peak traffic or load can lead to memory issues causing the STS generation process incomplete.

Known Issues

Platform

SD-WAN VPX Appliances

Issue ID 694837: For High Availability in AWS (AWS) environment, Virtual WAN service is disabled on a NetScaler SD-WAN VPX Primary (active) appliance citing duplicate IP address when the high availability interface on the primary appliance goes down.

Issue ID 702889: RCN branch that is changed from GEO to Client does not get updated to latest build even though it has an active Virtual path available by using the RCN.

Issue ID 701517: Over provisioning of the XenServer can lead to SD-WAN VPX appliance crash.

SD-WAN 4000 WANOP and 4000 SE

Issue ID 681550: On a NetScaler SD-WAN 4000 WANOP appliance, uploading DER encoded certificate for the SSL profile is ignored and no error message is displayed in the web GUI. Only PEM encoded certificates are accepted.

SD-WAN 2100 EE

Issue ID 704923: The Domain Join/ Delegate user Pre-check Tools Summary Status table is not displayed you try to access them.

Workaround: You can obtain the status summary by selecting the 'More' option in the summary dialog page.

Two Box Mode

Issue ID 681680: After a factory reset on the SD-WAN SE appliance in a two box mode, configuration sync between SD-WAN WANOP and SD-WAN SE appliances fails due to stale SSL certificates.

Workaround: Disable and re-enable two-box mode on the SD-WAN WANOP appliance.

SD-WAN 1000 / 2000

Issue ID 681663: When you upgrade SD-WAN 1000 / 2000 appliance from release build version 9.1.2.26 to 9.2.x, a warning is displayed in the browser.

Workaround: Perform the upgrade in an incognito mode window of the Google Chrome browser.

HDX CGP over SSL

Issue ID 690794: HDX ICA/CGP over SSL session's behavior In Virtual WAN Standard Edition:

- HDX sessions are not being negotiated as multi stream sessions even though MSI is enabled on the appliance and MSI+MP policies are set on incoming ICA traffic.
- HDX traffic is classified as belonging to HTTP Secure (https) application and web family.
- HDX traffic falls under **interactive_very_low** class. This can cause issues in QoS, bandwidth allocation, and so on, as application Quality of Service will not be triggered because the traffic is not classified as HDX sessions.

Configuration

Virtual WAN Configuration

Issue ID 704926: Configuration error occurs when you attempt to override service in a Virtual Path by changing the IP Rule properties.

Issue ID 704160: The Site Name in Virtual WAN configuration should be configured with alpha numeric characters

between 3-15 characters only. This is due to the hostname restrictions in WAN Optimization which is required for domain join operation.

Application Steering

Issue ID 699285: The Application family added as one of the match types in the Application Object which is used for Application Routes configuration is not considered for steering.

Custom Application Reporting

Issue ID 703794: If an existing application name is changed and change management is performed, the new application name might not be listed in the SD-WAN Center under the **Top Sites-> Application** drop-down menu. When the page is hard refreshed, then the new application name gets listed and reported, when traffic matches the application.

WAN GRE Tunnel

Issue ID 681171: A NetScaler SD-WAN appliance does not reassemble fragmented GRE tunnel packets properly.

Transparent proxy support for TLS 1.2

Issue ID 691900: In NetScaler SD-WAN WANOP 9.3.0, for SSL compression the SSL profile has to be configured in split mode only as transparent proxy mode is not supported.

Change Management (Single Step Upgrade) SD-WAN GUI

Issue ID 691953: During software upgrade on an appliance using a Standard Edition license, a WAN optimization related warning message appears. After the scheduled upgrade and after the WAN optimization, SVM and XenServer hotfixes are installed the warning message is cleared.

Workaround: Clear the warning messages manually or open the SD-WAN web UI in an incognito browser window.

Issue ID 705037: In the new **Global Multi-Region Summary** table, the “**Total Sites**” value appeared is less than the sum of the remaining columns. For example; if a branch node is not connected, it is possible that the branch is counted twice; once as “Not Connected” and once as “Preparing/Staging.”

Secure Peering Certificate and Keys

Issue ID 695363: In the SD-WAN GUI, on the Secure Peering Certificate and Keys page, the CA certificate contents are displayed if the private CA radio button is selected after setting the Keystore password on a new appliance.

Workaround: You need to switch between the radio buttons of the 'Private CA' and 'CA Certificate' once to get the correct contents displayed under 'Private CA' and 'CA Certificate' for Secure Peering Certificate and Keys.

Multicast Traffic

Issue ID 694894: When you configure Application Quality of Service rule with match type as "Application" to match 'icmp' and change the class to Real-time, and mode to load balance which overrides the default rule, the multicast traffic is not processed.

Routing

Issue ID 704561: Unable to make the routing domain as default for a site after disabling it.

Workaround:

1. Disable site routing domain (all).
2. Enable routing domain for the site without making it default. Select **Apply**.
3. Make the enabled routing domain for the site as default. Select **Apply**.

Issue ID 705255: Dynamic routes can be installed by using path eligibility, LOCAL service as part of Import filters. In NetScaler SD-WAN 10.0, if the path becomes inactive, then all routes are termed as REACHABLE – YES, and ELIGIBLE - NO instead of REACHABLE - NO and ELIGIBLE – NO. These routes which are ineligible will stay in the remote SD-WAN routing table instead of being purged.

DPI Functionality

DPI- ICMP Functionality

Issue ID 677356: A firewall policy for blocking ICMP as an application blocks only pings (echo requests). All other ICMP types are allowed to pass through.

Workaround: Instead of blocking ICMP as an application, block **IP-protocol > ICMP**.

DPI –Traffic for Top App Family as "Standard" and Top App as "Unknown Virtual protocol" for a Standard Edition appliance

Issue IDs 678373, 678339, 678545, 675063, 676017: On a NetScaler SD-WAN Standard Edition appliance, enable EDT policy for MSI+MP for Win7 and Win2K12 XenDesktop 7.12 VDAs on ports 2598, 2599, 2600, 2601 and then disable Session Reliability policy for Win7 VDA.

Workaround: Start sending internet traffic and check the monitoring flows in the Standard-Edition web management interface for Classes, Rule groups – ICAUDP and ICACGPUUDP, and Firewall. Check the Dashboard and Reporting page in SD-WAN Center web management interface. The results display **Top Application Family** as **Standard** and **Top Applications** as **Unknown Virtual Protocol**.

SD-WAN Center

Issue ID 693436: The clear connections/flows clear SD WAN connection table entries and all the later ICA sessions. The SD-WAN Center dashboard shows incorrect results for HDX TCP and EDT classification sessions and reports it as “Not Classified.”

Issue ID 693026: For HDX configuration, only UDP ICA sessions are classified by ICA classifier. The Framhawk ICA session is ignored. The SD-WAN DPI fails to classify the Framhawk sessions.

SD-WAN 10.0.2 Release Notes

Jun 14, 2018

This release notes describes what's new, known issues, and fixed issues applicable to SD-WAN software release version 10.0.2 for the SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances, and SD-WAN Center.

For information about the previous release versions, see the [SD-WAN](#) documentation.

What's New

The SD-WAN release version 10.0.2 introduces the following enhancements:

210-SE LTE Configuration and Change Management Process

If you configured a WAN link on a 210-SE appliance with release 9.3 version 5, it is possible to misconfigure the 210-SE appliance with the incorrect hardware. For instance; a 210-SE appliance with no LTE port can still turn on the LTE port in the configuration and push that change to the non LTE 210-SE appliance during the change management process.

To prevent misconfiguring the 210-SE appliance, update the network to release 10.0 version 2, and ensure the following:

- Any 210-SE LTE appliances in the network have the "LTE" submodel configured or selected for those sites.
- Any 210-SE base (non-LTE) appliances in the network have the "BASE" submodel configured at those sites.

A 210-SE appliance with the "LTE" port enabled in release 9.3 version 5 automatically translates to the 210-SE LTE submodel after migrating to release 10.0 version 2.

210-SE Sub Model Information

In the SD-WAN GUI, when creating a client site for the 210-SE appliance, the GUI displays submodel information; LTE and BASE.

HA Support

The NetScaler SD-WAN release 10.0 version 2 supports configuring High availability on the 210-SE BASE and LTE appliances.

SD-WAN Center

- Support to upload modem firmware on multiple sites is added.
- MOS score for Applications and Application QoS Rules is added.

Multi-regions in SD-WAN Center

Multi-region network support is added. The enhancements related to multi-region support are as follows:

- The Head end SD-WAN Center can only perform upload operation for sites in the "Default Region" and the Collector SD-WAN Center can perform upload operation for the sites in its region.
- The Mobile Broadband tab in the Collector SD-WAN Center GUI shows data and summary from LTE sites in the region. Modem operations are performed from this Collector.

Inventory Manager

The Inventory Manager field in the SD-WAN Center GUI displays the submodel information for the 210-SE platform.

Licensing

When Centralized licensing is configured for a site with a specific license rate (bandwidth), the site appliance can consume the license rate equal to or greater than the license rate configured for that site.

Fixed Issues

Configuration

- **Issue ID 709418:** If a new site that has a WAN link with public IP address learning enabled is added to the network, after configuration change, it is possible that a WAN path on the network will go DEAD.
- **Issue ID 707003:** In NetScaler SD-WAN release 9.3 version 3, generation of STS in peak traffic or load can lead to memory issues causing the STS generation process incomplete.
- **Issue ID 709309:** In NetScaler SD-WAN release 9.3 version 4, packets are dropped when packets are received on an untrusted link with a source MAC address, which is different than the link gateway MAC address.

Application QOS Rule Index

- **Issue ID 707561:** In NetScaler SD-WAN release 9.3 version 3, the SD-WAN service restarts unexpectedly, when switching from static virtual paths to dynamic virtual paths due to memory issues because of incorrect application QOS rule index.

SD-WAN Service

- **Issue ID 703119:** In NetScaler SD-WAN release 9.3 version 2, the SD-WAN service restarts on a 410-SE appliance edition because of high rate of packet bursts. Sometimes, the appliance might go into a hung state.
- **Issue ID 709077:** In NetScaler SD-WAN release 10.0 version 1, the WAN Link usage report shows multiple Internet Services view instead of one when multiple routing domains are configured.
- **Issue ID 709392:** In NetScaler SD-WAN release 9.3 version 4, the SD-WAN service restarts when the Internet Service transfers from Primary/Secondary mode to balanced mode with internet access to all routing domains configured in the WAN link access interface.

DHCP Server

- **Issue ID 709403:** In NetScaler SD-WAN release 10.0 version 1, the DHCP server cannot allocate IP address in the configured subnet, if a new site is created and the DHCP server is configured before the **Audit Now** button is clicked.

WANOP Plug-in

- **Issue ID 709125:** In NetScaler SD-WAN WAN OP release 9.3 version 4, passive FTP connectivity issue is encountered when using the WAN OP plug-in on Windows platform.

STS Packet Capture

- **Issue ID 708889:** In NetScaler SD-WAN release 10.0 version 1, on the 4100 or 5100 platform editions, STS packet capture does not contain any data when it is collected for the first time with only 5 seconds on the data interface.

ESP Protocol

- **Issue ID 705654:** in NetScaler SD-WAN WANOP release 9.3 version 3, on the SD-WAN 4000 or 5000 platform editions, the WANOP module drops the ESP protocol packets when it is configured with return to Ethernet sender.

Ether IP Protocol

- **Issue ID 702652:** in NetScaler SD-WAN WANOP release 9.3 version 3, on the SD-WAN 4000 or 5000 platform editions, the WANOP module drops the Ether IP protocol packets when it is configured with return to Ethernet sender.

Change Management process

- **Issue ID 706577:** During the change management staging process on an SD-WAN 1000 appliance, a branch node might remain in the unpacking phase for a long duration.

SD-WAN Configuration

- **Issue ID 709212:** A "Backup file parsing failed" error is encountered when an SD-WAN WAN OP appliance configuration running with release 10.0.x is restored after a backup.
- **Issue ID 709079:** In NetScaler SD-WAN release 10.0 version 1, the SD-WAN Center application notification configuration settings such as; Virtual Path, Dynamic Virtual Path, Appliance, License, and Events are not applied to the SD-WAN appliances in the network.

WAN-to-WAN Forwarding

- **Issue ID 710635:** In NetScaler SD-WAN release 10.0 version 1, packets matching the same header (source/destination IP/port) processed simultaneously through the firewall can cause the system to restart, if WAN-to-WAN forwarding is disabled and an external router is used to forward branch-to-branch traffic.

Site Cloning

- **Issue ID 709572:** In NetScaler SD-WAN release 10.0 version 1, you do not have to change the access interface IP address when cloning a site, if it is a private Virtual IP address, and public IP address is configured for that WAN link.

Relearn Routes

- **Issue ID 710493:** In NetScaler SD-WAN release 10.0 version 1, when WAN gateway is unavailable and becomes available in a fraction of second, the routes are not relearned. Restart the SD-WAN service at the Branch to relearn routes.

OSPF Configuration

- **Issue ID 710960:** When configuring OSPF, the OSPF areas configuration in the SD-WAN GUI does not show the routing domain drop-down option. Therefore, areas for multiple routing domains cannot be created. The BGP configuration works fine showing the routing domains by listing the VNIs to choose for enabling the dynamic routing participating interface.

TCP connections

- **Issue ID 709163:** In NetScaler SD-WAN, release versions 10.0.0 and 10.0.1, the TCP connections are not established, if WANOP redirection is enabled in the multi routing domain environment on an Enterprise Edition appliance, which has SD-WAN release 9.1 version 2 factory shipped base image.

SD-WAN WANOP 4000/4100/5000/5100 Appliances

- **Issue ID 681372, 0709820:** NetScaler SD-WAN appliance becomes unresponsive when sending traffic that encounters a forwarding session.
- **Issue ID 0710023:** NetScaler SD-WAN appliance becomes unresponsive when processing GRE fragmented packet.

Known Issues

Platform

SD-WAN VPX Appliances

- **Issue ID 694837:** For High Availability in Amazon Web Services (AWS) environment, Virtual WAN service is disabled on a NetScaler SD-WAN VPX Primary (active) appliance citing duplicate IP address when the HA interface on the primary appliance goes down.
- **Issue ID 702889:** RCN branch that is changed from GEO to Client is not updated to latest build even though it has an active Virtual path available with the RCN.
- **Issue ID 701517:** Over provisioning of the XenServer can lead to SD-WAN VPX appliance crash.

SD-WAN 4000 WANOP and 4000 SE

- **Issue ID 681550:** On a NetScaler SD-WAN 4000 WANOP appliance, uploading DER encoded certificate for the SSL profile is ignored and no error message is displayed in the web GUI. Only PEM encoded certificates are accepted.

SD-WAN 2100 EE

- **Issue ID 704923:** The Domain Join/ Delegate user Pre-check Tools Summary Status table is not displayed you try to access them.

- **Workaround:** You can obtain the status summary by selecting the **More** option in the summary dialog page.

Two Box Mode

- **Issue ID 681680:** After a factory reset on the SD-WAN SE appliance in a two-box mode, configuration sync between SD-WAN WANOP and SD-WAN SE appliances fails due to stale SSL certificates.

- **Workaround:** Disable and re-enable two-box mode on the SD-WAN WANOP appliance.

SD-WAN 1000 / 2000

- **Issue ID 681663:** When you upgrade SD-WAN 1000 / 2000 appliance from release build version 9.1.2.26 to 9.2.x, a warning is displayed in the browser.

- **Workaround:** Perform the upgrade in an incognito mode window of the Google Chrome browser.

HDX CGP over SSL

Issue ID 690794: HDX ICA/CGP over SSL session's behavior In Virtual WAN Standard Edition:

- HDX sessions are not being negotiated as multi stream sessions even though MSI is enabled on the appliance and MSI+MP policies are set on incoming ICA traffic.

- HDX traffic is classified as belonging to Hyper Text Transfer Protocol Secure (https) application and web family.
- HDX traffic falls under interactive_very_low class. This may cause issues in QoS, bandwidth allocation, and so on, as application QoS will not be triggered because the traffic is not classified as HDX sessions.

DPI Functionality

DPI- ICMP Functionality

- **Issue ID 677356:** A firewall policy for blocking ICMP as an application blocks only pings (echo requests). All other ICMP types are allowed to pass through.

- **Workaround:** Instead of blocking ICMP as an application, block IP-protocol > ICMP.

DPI –Traffic for Top App Family as "Standard" and Top App as "Unknown Virtual protocol" for a Standard Edition appliance

- **Issue IDs 678373, 678339, 678545, 675063, 676017:** On a NetScaler SD-WAN Standard Edition appliance, enable EDT policy for MSI+MP for Win7 and Win2K12 XD 7.12 VDAs on ports 2598, 2599, 2600, 2601 and then disable Session Reliability policy for Win7 VDA.

Workaround: Start sending internet traffic and check the monitoring flows in the Standard-Edition web management interface for Classes, Rule groups – ICAUDP and ICACGPUUDP, and Firewall. Check the Dashboard and Reporting page in SD-WAN Center web management interface. The results display Top Application Family as Standard and Top Applications as Unknown Virtual Protocol.

SD-WAN Center

- **Issue ID 693436:** The clear connections/flows clear SD WAN connection table entries and later all the ICA sessions. The SD-WAN Center dashboard shows incorrect results for HDX TCP and EDT classification sessions and reports it as “Not Classified.”
- **Issue ID 693026:** For HDX configuration, only UDP ICA sessions are classified by ICA classifier. The FrameHawk ICA sessions are ignored. The SD-WAN DPI fails to classify the FrameHawk sessions.

Configuration

Virtual WAN Configuration

- **Issue ID 704926:** Configuration error occurs when you attempt to override service in a Virtual Path by changing the IP Rule properties.
- **Issue ID 704160:** The Site Name in Virtual WAN configuration should be configured with alpha-numeric characters between 3-15 characters only. This is due to the hostname restrictions in WAN Optimization which is required for domain join operation.

Application Steering

- **Issue ID 699285:** The Application family added as one of the match types in the Application Object, which is used for Application Routes configuration is not considered for steering.

Custom Application Reporting

- **Issue ID 703794:** When an existing application name is modified and change management is performed, the new application name may not be listed in the SD-WAN Center under the **Top Sites**-> **Application** drop-down menu. If the page is hard refreshed, then the new application name gets listed and reported, if traffic matches the application.

WAN GRE Tunnel

- **Issue ID 681171:** NetScaler SD-WAN appliance does not reassemble fragmented GRE tunnel packets properly.

Transparent proxy support for TLS 1.2

- **Issue ID 691900:** In NetScaler SD-WAN WANOP 9.3.0, for SSL compression the SSL profile has to be configured in split mode only as transparent proxy mode is not supported.

Change Management (Single Step Upgrade) SD-WAN GUI

- **Issue ID 691953:** During software upgrade on an appliance using a Standard Edition license, a WAN optimization related warning message appears. After the scheduled upgrade and after the WAN optimization, SVM and XenServer hotfixes are installed the warning message is cleared.

- **Workaround:** Clear the warning messages manually or open the SD-WAN web UI in an incognito browser window.

- **Issue ID 705037:** In the new **Global Multi-Region Summary** table, the “**Total Sites**” value displayed is less than the sum of the remaining columns. For example; when a branch node is not connected, it is possible that the branch is counted twice; once as “Not Connected” and once as “Preparing/Staging.”

Routing

- **Issue ID 704561:** Unable to make the routing domain as default for a site after disabling it.

- **Workaround:**

1. Disable **site routing domain** (all).
2. Enable routing domain for the site without making it default. Click **Apply**.
3. Make the enabled routing domain for the site as default and click **Apply**.

- **Issue ID 705255:** Dynamic routes can be installed with path eligibility, LOCAL service as part of Import filters. In NetScaler SD-WAN 10.0, if the path becomes inactive, then all routes are termed as REACHABLE – YES, and ELIGIBLE – NO instead of REACHABLE – NO and ELIGIBLE – NO. These routes which are ineligible will stay in the remote SD-WAN routing table instead of being purged.

Secure Peering Certificate and Keys

- **Issue ID 695363:** In the SD-WAN GUI, on the Secure Peering Certificate and Keys page, the CA certificate contents are displayed when the private CA radio button is selected after setting the Key Store password on a new appliance.

- **Workaround:** You need to switch between the radio buttons of the 'Private CA' and 'CA Certificate' once to get the correct contents displayed under 'Private CA' and 'CA Certificate' for Secure Peering Certificate and Keys.

Multicast Traffic

- **Issue ID 694894:** When you configure Application QoS rule with match type as "**Application**" to match '**icmp**' and change the class to Real-time, and mode to load balance which overrides the default rule, the multicast traffic is not processed.

Software Installation and Upgrade

Jul 26, 2018

There are two main upgrade scenarios:

1. Upgrade appliances with [working Virtual WAN configuration](#) from a previous release version, 8.1, 9.0, 9.1, 9.2 to 9.3 latest MR first, and then to the current release version of 10.0.
2. Upgrade appliances to release 10.0 without existing Virtual WAN configuration.

Important

Appliances shipped with 8.0.x image are not supported to upgrade to Enterprise Edition.

Note

Upgrading to 10.0 release is a single-step process. If you are currently using an earlier version of the software, such as release version 9.2, you should first upgrade the software to release version 9.3 latest MR, and then upgrade to release 10.0.

Upgrading to 9.3 release is a multi-step process. Virtual WAN software is upgraded centrally from the MCN appliance using *tar.gz* files followed by single step upgrade package.

System Requirements

Mar 01, 2018

Hardware Requirements

Instructions for installing your NetScaler SD-WAN appliances are provided in [Setting up the SD-WAN appliances](#).

Firmware Requirements

All SD-WAN appliance models in a Virtual WAN environment are required to be running the same NetScaler SD-WAN firmware release.

Note

Appliances running earlier software versions will not be able to establish a Virtual Path connection to the appliance running SD-WAN release 9.2. For additional information, please contact NetScaler Customer Support.

Software Requirements

For details regarding license requirements, see [Licensing](#).

Browser Requirements

Browsers must have cookies enabled, and JavaScript installed and enabled.

The NetScaler SD-WAN Management Web Interface is supported on the following browsers:

- Mozilla Firefox 35.0+ (Recommended version 43.x)
- Google Chrome 40.0+ (Recommended version 49.x)

Supported browsers must have cookies enabled, and JavaScript installed and enabled.

SD-WAN Platform Models and Software Packages

Mar 01, 2018

This section provides information about downloading the NetScaler Citrix SD-WAN software packages.

Note

Before you download the software, you must obtain and register a Citrix SD-WAN software license. For information, please see [Licensing](#).

A SD-WAN appliance package contains the SD-WAN software package for a particular appliance model bundled with a specific SD-WAN configuration package. The two packages are bundled together and distributed to the clients by using the **Change Management** wizard in the Management Web Interface running on the Master Control Node (MCN).

If this is an initial installation, you must manually upload, stage, and activate the appropriate appliance package on each of the client appliances that will reside in your SD-WAN network. If you are updating the configuration for an existing SD-WAN deployment, the MCN automatically distributes and activates the appropriate appliance package on each of the existing clients, as soon as the virtual paths to the clients become operational.

Downloading the Software Packages

There is a different NetScaler Citrix SD-WAN software package for each appliance model. You will need to download the appropriate software package for each appliance model you want to include in your network.

To download the Citrix SD-WAN software packages, go to the URL; <https://www.citrix.com/downloads/netscaler-sd-wan.html>. Instructions for downloading the software are provided on this site.

Citrix SD-WAN Software Packages

There is different Citrix SD-WAN software package for each supported SD-WAN appliance model. You will need to acquire the appropriate package for each appliance model you plan to incorporate into your network.

Supported SD-WAN Appliance Models

There are three main categories of Citrix SD-WAN Appliances:

- SD-WAN Appliance hardware models
 - WANOP, Standard Edition, and Enterprise Edition
- SD-WAN VPX Virtual Appliances (SD-WAN VPX)
 - Standard Edition and WANOP Edition

Note

All SD-WAN appliance models in a SD-WAN environment are required to be running the same SD-WAN firmware release. For additional information, please contact Citrix SD-WAN Customer Support.

For a complete description of SD-WAN Appliances, please refer to the following SD-WAN datasheet:

https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-sd-wan-datasheet.pdf

SD-WAN Standard Edition Hardware Appliances

Citrix SD-WAN release 10.0 supports the following SD-WAN standard edition hardware appliance models:

SD-WAN SE PLATFORM MODEL	ROLE
210-SE	Small branch appliance
410-SE	Small branch appliance
1000-SE	Large branch appliance
2000-SE	Large branch appliance
2100-SE	Large branch appliance
4100-SE	Data Center - Master Control Node (MCN) appliance
5100-SE	Data Center - Master Control Node (MCN) appliance

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

Citrix SD-WAN 10.0 supports the following SD-WAN WAN Optimization (WANOP) appliance models:

SD-WAN WANOP PLATFORM MODELS	ROLE
WANOP 800	Small branch appliance
WANOP 1000 Windows Server	Large branch appliance
WANOP 1000	Large branch appliance
WANOP 2000	Large branch appliance
WANOP 3000	Large branch appliance
WANOP 4000, WANOP 4100	Data Center appliance
WANOP 5000	Data Center appliance

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

Citrix SD-WAN 10.0 supports the following SD-WAN VPX Virtual Appliance (VPX-SE) models:

SD-WAN VPX-SE PLATFORM MODELS	ROLE
VPX 20-SE	MCN or client appliance, small branch
VPX 50-SE	MCN or client appliance, small branch
VPX 100-SE	MCN or client appliance, small branch
VPX 200-SE	MCN or client appliance, small branch
VPX 500-SE	MCN or client appliance, small branch
VPX 1000-SE	MCN or client appliance, small branch

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

Citrix SD-WAN 10.0 supports the following SD-WAN WANOP Virtual Appliance (VPX-WANOP) models:

SD-WAN VPX WANOP PLATFORM MODELS	ROLE
WANOP VPX-2	Small branch appliance
WANOP VPX-6	Small branch appliance
WANOP VPX-10	Small branch appliance
WANOP VPX-20	Small branch appliance
WANOP VPX-50	Large branch appliance
WANOP VPX-100	Large branch appliance
WANOP VPX-200	Large branch appliance

SD-WAN Enterprise Edition Hardware Appliances (SD-WAN EE)

Citrix SD-WAN 10.0 supports the following SD-WAN Enterprise Edition appliance (SD-WAN EE) models:

SD-WAN EE PLATFORM MODELS	ROLE
1000-EE	Large branch, data center appliance
2000-EE	Large branch, data center appliance
2100-EE	Large branch, data center appliance

Upgrade to 10.0 With Working Virtual WAN Configuration

Mar 11, 2018

Note

The upgrade is a [multi-step process](#), if you are upgrading from previous release versions; 8.1.x, 9.0.x, 9.1.x, 9.2.x to 10.0. The Virtual WAN software is upgraded centrally from the MCN appliance using *tar.gz* files first, and then the *.zip* file is used to upgrade to 10.0.

Prerequisites

1. Have a valid SD-WAN license.
2. Have a working Virtual WAN configuration running release version 8.1.x, 9.0.x, 9.1.x, 9.2.x with virtual paths established from MCN appliance to the branch site appliances.

Upgrade Procedure

If your MCN appliance is running previous releases 8.1.x, 9.0.x, 9.1.x, 9.2.x, follow steps outlined in the [Upgrading with Virtual WAN configuration](#) using the *cb-vw_<APPLIANCE-MODEL>_9.3.x.tar.gz*.

If your MCN appliance is running 9.3.x or newer proceed with the steps below. This procedure is accomplished by using the *ns-sdw-sw-<release-version>.zip* file.

1. Perform Change Management by uploading single step upgrade package, *ns-sdw-sw-10.0.0.x.zip* file after downloading the package from the download server; <https://www.citrix.com/downloads/netscaler-sd-wan/>

The screenshot displays the Citrix SD-WAN management console interface. The main content area is titled "Change Process Overview" and shows a three-step workflow: Step 1: Change Preparation (Upload Files to MCN), Step 2: Appliance Staging (Transfer Files to Clients), and Step 3: Activation (Activate Change). Below the steps, there are buttons for "MCN" and "Clients" for each step, and an "Activate Staged" button. A note indicates that clicking "Activate Staged" will skip to the Appliance Staging step. Below the overview, there is a table of configuration files and a table of site appliances.

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1KSite-Appliance	CB1000		10.0.0.200.660093	035 on 2/23/18			Loc Chg Mgt		active / none
Branch2KSite-Appliance	CB2000	0%	10.0.0.200.660093	035 on 2/23/18			Loc Chg Mgt		active / none
Branch400-Appliance	CB400	Not Connected					Loc Chg Mgt		active / none
Branch410-Appliance	CB410	Not Connected					Loc Chg Mgt		active / none
BranchVFX-Appliance	CBVFX	Not Connected					Loc Chg Mgt		active / none

Note

If your appliance is already running release version 10.0 and you are upgrading the appliance to the next build version, uploading the single step upgrade (.zip) package file will display only the MCN software unless you click on the **Verify** or **Stage** appliance change management options.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

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

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

Upload Item: ns-sdw-sw-10.0.0.198.zip

Valid file types: .tar.gz, .zip

Configuration: Software: current

Selected file(s): ns-sdw-sw-10.0.0.198.zip - Press **Upload**.

Configuration Filenames: Active - Staged - VPX-HA.cfg

Virtual WAN

- View Configuration
- Configuration Editor
- Change Management**
- Change Management Settings
- Restart/Reboot Network
- Enable/Disable/Purge Flows
- Dynamic Virtual Paths
- SD-WAN Center Certificates
- + System Maintenance

Upload and Verify Files

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

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

Upload Item: No file chosen

Valid file types: .tar.gz, .zip

Configuration: Software: current

Verification Success - The configuration is valid

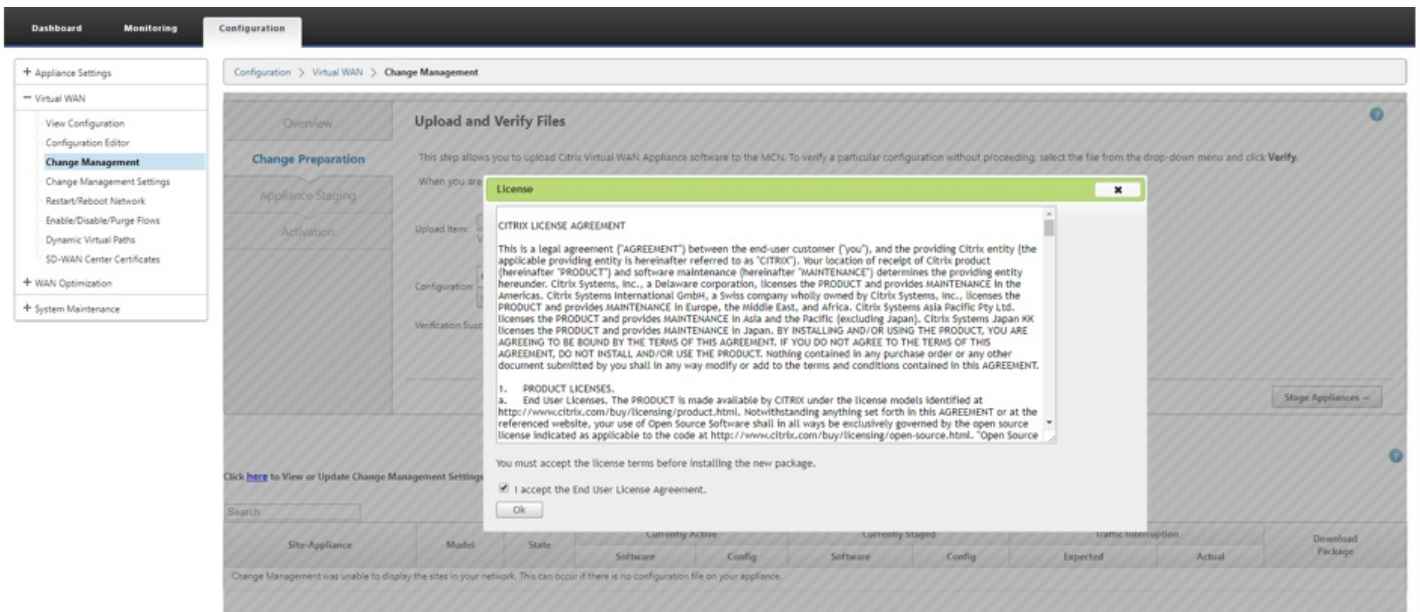
Configuration Filenames: Active - u3-conf1-final121-noipsec-MCN-SITE-HA-10.zip Staged - u3-conf1-final121-noipsec-MCN-SITE-HA-10.zip

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

Show entries

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
u3-mcn-conf-Appliance	CBVPX		10.0.0.199.659787	9:28 on 2/21/18	10.0.0.196.659357	4:24 on 2/20/18	<3 min	205 s	active / staged
u3-mcn-conf-HA-MCN	CBVPX		10.0.0.199.659787	9:28 on 2/21/18	10.0.0.196.659357	4:24 on 2/20/18	<3 min	208 s	active / staged
u3-nod1-conf-Appliance	CBVPX		10.0.0.199.659787	9:28 on 2/21/18	10.0.0.196.659357	4:24 on 2/20/18	<3 min	188 s	active / staged
u3-nod2-conf-Appliance	CBVPX		10.0.0.199.659787	9:28 on 2/21/18	10.0.0.196.659357	4:24 on 2/20/18	<3 min	191 s	active / staged
u3-nod2-conf-u3-noce2-conf-HA	CBVPX		10.0.0.199.659787	9:28 on 2/21/18	10.0.0.196.659357	4:24 on 2/20/18	<3 min	190 s	active / staged

2. Click **Stage Appliances** once upload process is successful and relevant models are displayed that would be upgraded based on the configuration file that has information about each branch platform models. License agreement page is displayed.



3. After accepting license agreement, you are navigated to **Appliance Staging** page which shows the status of package preparation and staging followed by transfer status for each branches.

Overview

Change Preparation

Appliance Staging

Activation

Appliance Staging ?

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

Ignore Incomplete

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

Configuration Filenames: Active - Multir_dvp9_ipsecFIPS.zip Staged - MCN_3WL_ipsecFIPS.zip

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

Global Multi-Region Summary ?

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

Region - Default_Region Details ?

Show 25 entries Search

?

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100		10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 sec	371 ms	active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000		10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 sec	269 ms	active / staged
BR1-BR1-CBVPXL	CBVPXL		10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 sec	304 ms	active / staged
RCN01-2000-RCN01-2000	CB2000		10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 min	183 ms	active / staged

▼

Appliance Staging

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

Transfer Progress:

100%

Appliance Staging complete. You may now proceed to Activation.

Prepare Packages Stage Packages Done

Abort Ignore Incomplete Next --

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

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

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

Global Multi-Region Summary

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

Region - Default_Region Details

Show entries

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 sec	371 ms	active / staged	
APAC_RCN-APAC_RCN-CB1000	CB1000	10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 sec	269 ms	active / staged	
BR1-BR1-CBVPXL	CBVPXL	10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 sec	304 ms	active / staged	
RCN01-2000-RCN01-2000	CB2000	10.0.0.201.660309	12:56 on 2/23/18	10.0.0.201.660309	11:56 on 2/23/18	<1 min	183 ms	active / staged	

Previous 1 Next

The various states of software package configuration displayed in the summary table indicates the following:

- Preparing - local processing to prepare update package for transfer to the appliance.
- Preparing Region Pkgs - local processing to prepare update package for transfer to RCN. (Applicable if RCN is part of network).
- Percentage - percent of package transferred to the appliance.
- Unpacking - remote appliance processing to apply the update package.
- Transferring Region - Package are being transferred to RCN. (Applicable if RCN is part of network).
- Failed - remote detected incomplete transfer.
- Cancelled - cancelled by user when 'Ignore Incomplete' was checked during Stage Appliances
- Not Needed - prepared staged package does not include this site-appliance name..
- Not Connected - local cannot see the remote's active package information.

4. After completion of transfer, you are navigated to Activation page where you can click on **Activate Staged** button to active the staged software.

Virtual WAN

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

System Maintenance

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Activating in:

5s

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

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

Activate Staged Abort Revert on Error Done

5. Click **done** once the countdown is completed and the button is enabled.

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

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In:

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

Revert Abort Done

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

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

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

Global Multi-Region Summary

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

Region - Default_Region Details

Show entries
Search
Customize
Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.0.0.201.660309	13:15 on 2/23/18	10.0.0.201.660309	13:43 on 2/23/18	0 sec		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.0.0.201.660309	13:15 on 2/23/18	10.0.0.201.660309	13:43 on 2/23/18	0 sec		active / staged
BRL-BRL-CBVPXL	CBVPXL	Done	10.0.0.201.660309	13:15 on 2/23/18	10.0.0.201.660309	13:43 on 2/23/18	0 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.0.0.201.660309	13:15 on 2/23/18	10.0.0.201.660309	13:43 on 2/23/18	0 sec		active / staged

Previous 1 Next

6. Navigate to **Change Management** page and you can check the transfer status of WANOP, SVM , XenServer Hotfixes for applicable branches only.

Configuration > Virtual WAN > Change Management

Change Process Overview

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

Step 1
Change Preparation

Upload Files to MCN

MCN

Step 2
Appliance Staging

Transfer Files to Clients

MCN → Clients

Step 3
Activation

Activate Change

MCN → Clients

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

Currently Prepared: Configuration - MCN_1WL_ipsecFIPS.zip Software - Current Running
Configuration Filenames: Active - Multir_dvp9_ipsecFIPS.zip Staged - MCN_1WL_ipsecFIPS.zip

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

Global Multi-Region Summary

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	4	0	0	0	0
AMEA_r1	23	1	0	0	0
APAC_r1	2	0	0	0	0

Region - Default_Region Details

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.0.0.201.660309	13:43 on 2/23/18	10.0.0.201.660309	13:49 on 2/23/18	<1 sec		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.0.0.201.660309	13:43 on 2/23/18	10.0.0.201.660309	13:49 on 2/23/18	<1 sec		active / staged
BR1-BR1-CBVPXL	CBVPXL	Done	10.0.0.201.660309	13:43 on 2/23/18	10.0.0.201.660309	13:49 on 2/23/18	<1 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.0.0.201.660309	13:43 on 2/23/18	10.0.0.201.660309	13:49 on 2/23/18	<1 sec		active / staged

7. Navigate to **Change Management Settings** page to schedule the installation of software other than non-SDWAN like WANOP, SVM, XenServer Hotfixes. By default the MCN assigns schedules installation to be attempted every day at 21:20:00 based on software availability on the branches.

Configuration > Virtual WAN > Change Management Settings

Enable/Disable Partial Software Upgrade

Enable Partial Software Upgrade **Apply**

Scheduling Information

Show 10 entries Search: [] Edit Selected Refresh

Site Name	Scheduling Information	Status	Edit
<input type="checkbox"/> RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟡	✎
<input type="checkbox"/> RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟠	✎
<input type="checkbox"/> RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟡	✎
<input type="checkbox"/> RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🔴	✎
<input type="checkbox"/> MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟢	✎
<input type="checkbox"/> MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟢	✎
<input type="checkbox"/> GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟡	✎
<input type="checkbox"/> RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟡	✎
<input type="checkbox"/> RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟡	✎
<input type="checkbox"/> RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	🟡	✎

Showing 1 to 10 of 17 entries Previous 1 2 Next

8. For detailed information or help on the scheduling information, you can click on the help icon. You can also edit scheduling information.

Help
✕

Scheduling Information

- To schedule installation of non-VW packages like SVM, WO, XenServer hotfixes, please navigate to "Change Management Setting" sub tree under "Virtual WAN" tree after performing activation in Change Management.
- "Change Management Setting" contains Site Name, Scheduling Information and edit option to update the schedule details for respective branches.
- Scheduling Information Edit dialog screen contains information like Date, Time, Maintenance Window and Repeat Window.
- Below is a brief description of each field
 - Site Name : Appliance name as given by user in Config Editor for each site.
 - Date : Date on which scheduled installation/upgrade will start from.
 - Time : local time of the appliance when the installation should be once the files are received. Valid Format is HH:MM:SS
 - Maintenance Window : The amount of time given by the user for installation. If "0" is provided installation will start immediately once the files are present on the appliance irrespective of the date and time values given under date and time fields.
 - Repeat Window: Frequency after which the system will check for a new upgrade version and perform upgrade only when a new version is available.
 - Unit : Unit chosen to check for new versions, could be any one of Hours/Days/Weeks/Months.
- By default for each site scheduled install will be attempted at 21:20 hour every day (local time) once the files are ready with the site.
- Installation will get triggered as long as 30 minutes is left for maintenance window to close. For instance, appliance has been scheduled to upgrade on "2017-06-12" at 23:20 hours with maintenance window of 1 hour. Attempt to install in the current maintenance window will be made until 23:50 hours and after that it will attempt in the next scheduled maintenance window.
- Installation will get trigger as long as 30 mins is left for maintenance window to close. Say appliance has been scheduled to install non-VM softwares on "2017-06-12" at 23:20 hours with maintenance window of 1 hours and repeated every day. Attempt to install in the current maintenance window will be made until 23:50 hours and after that it will attempt in the next scheduled maintenance window.
- Scheduled maintenance window can be overridden to install the component instantly by changing the maintenance window to "0" and this will skip scheduled time and date and start the installation once all the packages are received.
- Scheduling details can be changed based on the need of the user with different maintenance windows, repeat window and unit.

Close

Edit Scheduling Info
✕

Site Name:

Date:

Time:

Maintenance Window(hours):

Repeat Window:

Unit:

Apply
Cancel

Below is a sample scheduling information with the supported status details.

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

Showing 1 to 10 of 17 entries

Scheduling Information Status	Description
Green check mark	Upgrade is Successful.
Orange exclamation	Appliance has received all necessary components, waiting for it's scheduled installation window to start
Yellow circle	Change Management has not been done, No action is required.
Red cross mark	An error has occurred during installation of OS components. Please try Change Management once again, if problem persists, please contact tech support.
Orange dotted circle	Files are being transferred to the appliance.
Yellow dotted circle	Upgrade is in progress.

Upgrade to 10.0 Without Virtual WAN Configuration

Mar 01, 2018

Important

This upgrade procedure to software release 10.0 assumes that virtual paths are not established between the MCN and Branches.

Note

If you are upgrading from a previous release version such as; 8.1.x, 9.0.x, 9.1.x, 9.2.x; see the instructions provided in the following link: [Upgrading to 9.3 without Virtual WAN configuration](#).

Note

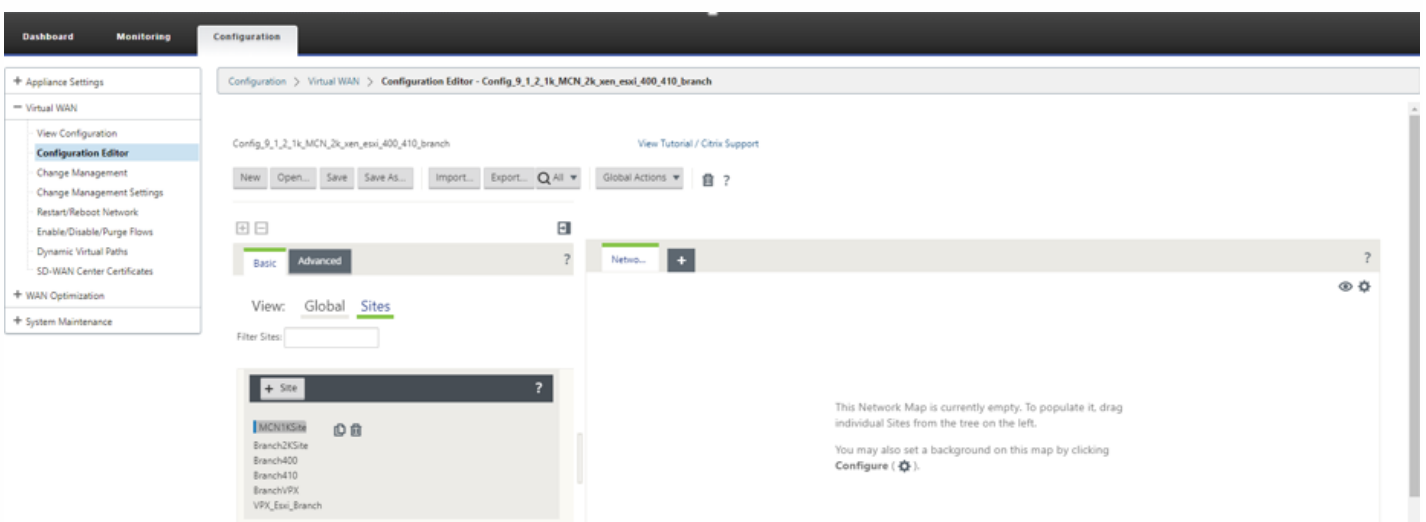
If you are upgrading release version 9.3.x or newer, follow the steps below.

Single Step Upgrade Process

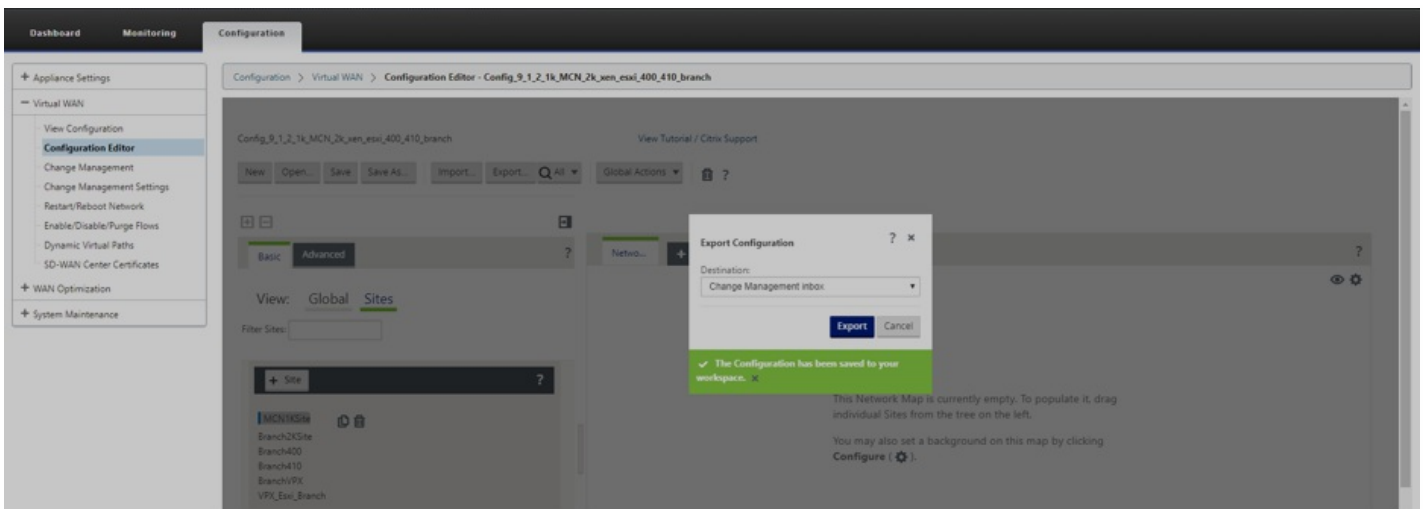
On the SD-WAN MCN appliance:

- You can upload single step upgrade package file; (*ns-sdw-sw-<release.version>.zip*).
- Proceed with **Change Management** workflow in the GUI.
- Schedule install components other than Virtual WAN software.

1. Prepare Configuration from **Configuration Editor** and **Save** configuration with valid name as shown below.

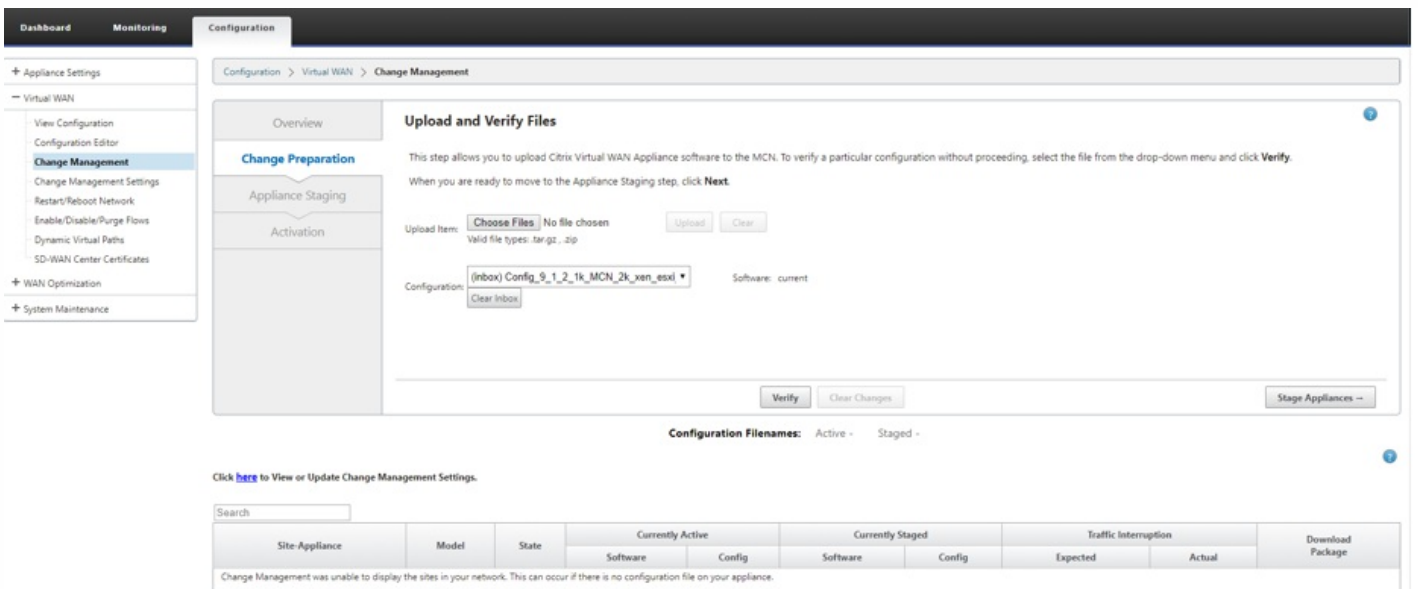


2. Export **Save Config** file to Change Management by selecting **Export** button and choose destination as **Change Management Inbox**.



3. After clicking **Export**, navigate to the **Change Management** page.

4. In the **Change Management** page, upload the `ns-sdw-sw-<release-version>.zip` software package file after downloading from the download server, and provide the location from where to upload by selecting '**Choose Files**'.



5. After selecting the file(s) to upload, click **upload** and a progress bar appears showing the current upload progress.

Upload and Verify Files

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

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

Upload Item: ns-sdw-sw-10.0.0.203.zip

Valid file types: .tar.gz, .zip

Configuration: Software: 10.1.0.8.660125
 Model(s): CB2000
 CB1000
 CB2100
 CBVPX

Selected file(s): ns-sdw-sw-10.0.0.203.zip - Press **Upload**.

Configuration Filenames: Active - Staged -

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Upload and Verify Files

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

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

Upload Item: ns-sdw-sw-10.0.0.200.zip

Valid file types: .tar.gz, .zip

Configuration: Software: current

Uploading file(s): ns-sdw-sw-10.0.0.200.zip...

Configuration Filenames: Active - Staged -

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

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

6. After upload is successful, the uploaded files are processed for any invalid errors.

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Upload and Verify Files

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

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

Upload Item: ns-sdw-sw-10.0.0.200.zip

Valid file types: .tar.gz, .zip

Configuration: Software: current

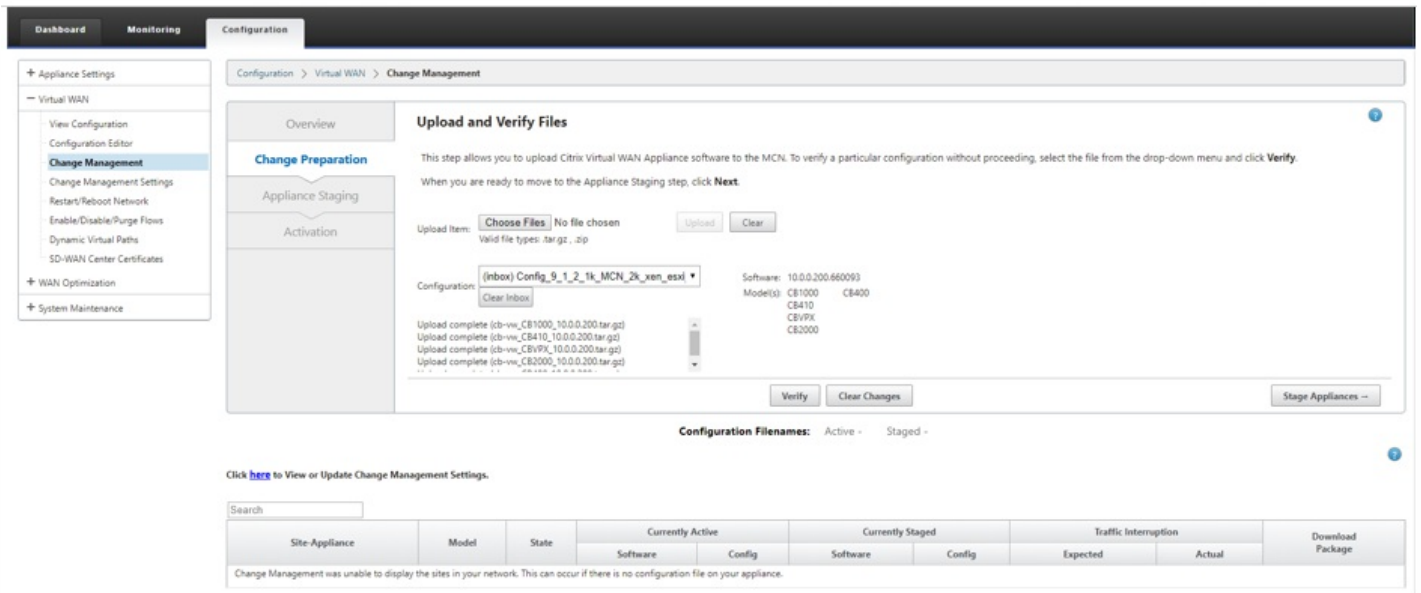
Processing uploaded file(s)...

Configuration Filenames: Active - Staged -

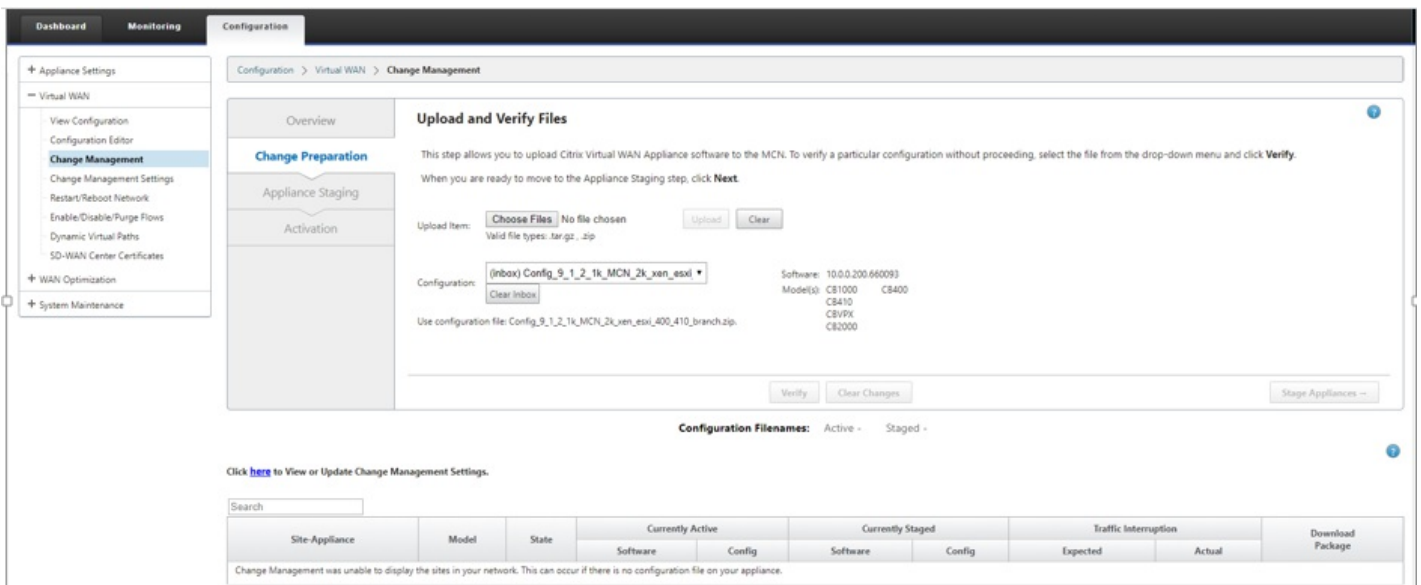
Click [here](#) to View or Update Change Management Settings.

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

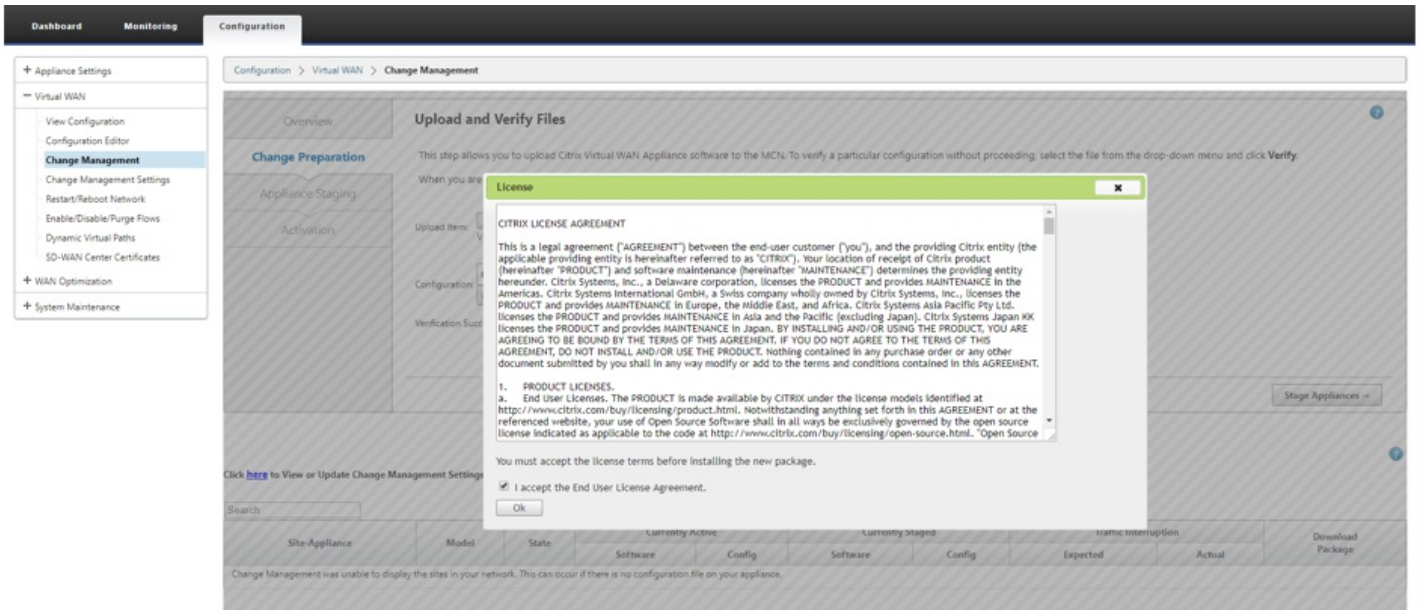
7. After upload processing is successful, information about which platform models the software has been uploaded and processed is displayed.



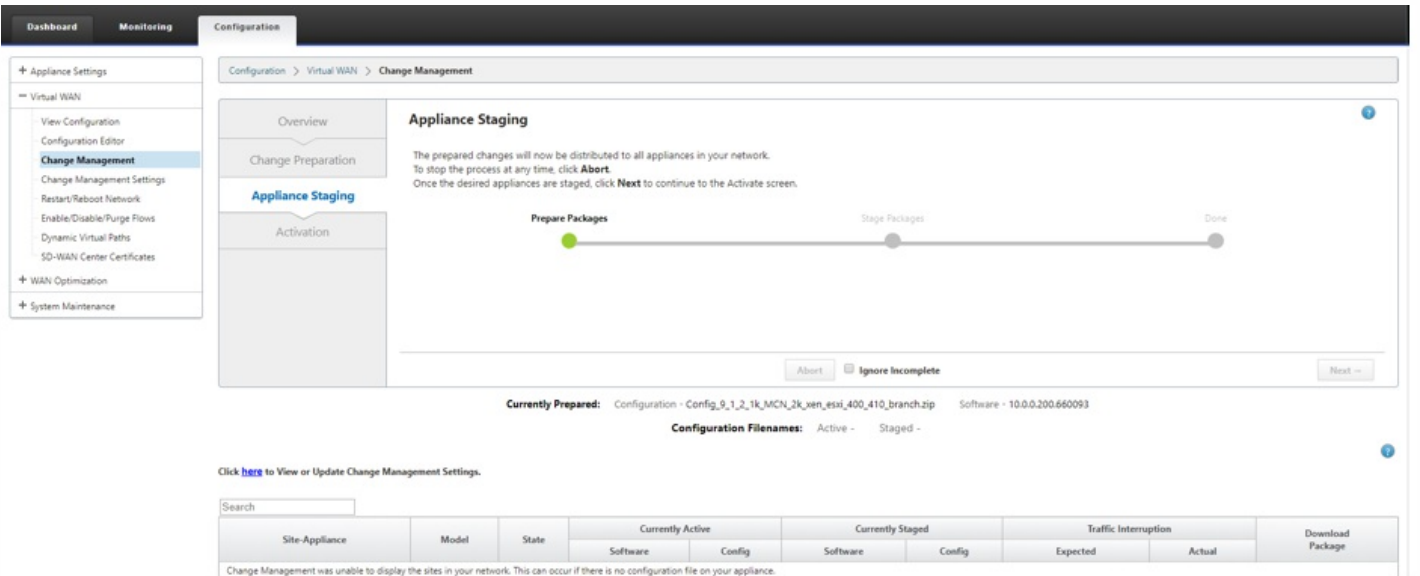
8. Click **Next** to proceed with Validation of Configuration file and appropriate message is shown based on the validation results. Accept and proceed with license agreement.



9. The License agreement page for user acceptance is displayed. Click on accept and proceed.



10. After accepting the license successfully you are navigated to Appliance Staging, click on **Stage Appliances** to proceed.



11. The transfer progress bar appears showing the current preparation and transfer status for each site.

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Overview **Appliance Staging**

Change Preparation

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

Appliance Staging

Activation

Transfer Progress:

0%
0 / 6 appliances finished

Prepare Packages (0 / 6 packages prepared) Stage Packages Done

Abort Ignore Incomplete Next

Currently Prepared: Configuration - Config_9_1_2_1k_MCN_2k_xen_esi_400_410_branch.zip Software - 10.0.0.200.660093

Configuration Filenames: Active - Staged -

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

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Branch2KSite-Appliance	CB2000	Preparing	Not Connected				Loc Chg Mgt		none / staged
Branch400-Appliance	CB400	Preparing	Not Connected				Loc Chg Mgt		none / staged
Branch410-Appliance	CB410	Preparing	Not Connected				Loc Chg Mgt		none / staged
BranchVPX-Appliance	CBVPX	Preparing	Not Connected				Loc Chg Mgt		none / staged
MCN1KSite-Appliance	CB1000	Preparing	Not Connected				Loc Chg Mgt		none / staged
VPX_Esi_Branch-Appliance	CBVPX	Preparing	Not Connected				Loc Chg Mgt		none / staged

12. After preparing of package is completed, the Transfer Progress bar shows as 100% , click **Next** and proceed to the activate page.

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Overview **Appliance Staging**

Change Preparation

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

Appliance Staging

Activation

Transfer Progress:

100%

Appliance Staging complete. You may now proceed to Activation.

Prepare Packages Stage Packages Done

Abort Ignore Incomplete Next

Currently Prepared: Configuration - Config_9_1_2_1k_MCN_2k_xen_esi_400_410_branch.zip Software - 10.0.0.200.660093

Configuration Filenames: Active - Staged -

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

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Branch2KSite-Appliance	CB2000	Not Needed	Not Connected				Loc Chg Mgt		none / staged
Branch400-Appliance	CB400	Not Needed	Not Connected				Loc Chg Mgt		none / staged
Branch410-Appliance	CB410	Not Needed	Not Connected				Loc Chg Mgt		none / staged
BranchVPX-Appliance	CBVPX	Not Needed	Not Connected				Loc Chg Mgt		none / staged
MCN1KSite-Appliance	CB1000	Not Needed	Not Connected				Loc Chg Mgt		none / staged
VPX_Esi_Branch-Appliance	CBVPX	Not Needed	Not Connected				Loc Chg Mgt		none / staged

13. In the **Activation** page, staged software package can be activated.

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

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

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

Activate Staged Abort Revert on Error Done

Currently Prepared: Configuration - Config_9_1_2_1k_MCN_2k_xen_esxi_400_410_branch.zip Software - 10.0.0.200.660093

Configuration Filenames: Active - Staged -

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

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Branch2KSite-Appliance	CB2000	Not Needed	Not Connected					Loc Chg Mgt	none / staged
Branch400-Appliance	CB400	Not Needed	Not Connected					Loc Chg Mgt	none / staged
Branch410-Appliance	CB410	Not Needed	Not Connected					Loc Chg Mgt	none / staged
BranchVPX-Appliance	CBVPX	Not Needed	Not Connected					Loc Chg Mgt	none / staged
MCN1KSite-Appliance	CB1000	Not Needed	Not Connected					Loc Chg Mgt	none / staged

14. On clicking **Activate Staged**, user acceptance pop-up message is displayed. Accept and proceed as shown below.

15. After accepting the message, click **OK**. The package gets copied to **Appliance Staging** state.

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

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

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

Activate Staged Abort Revert on Error Done

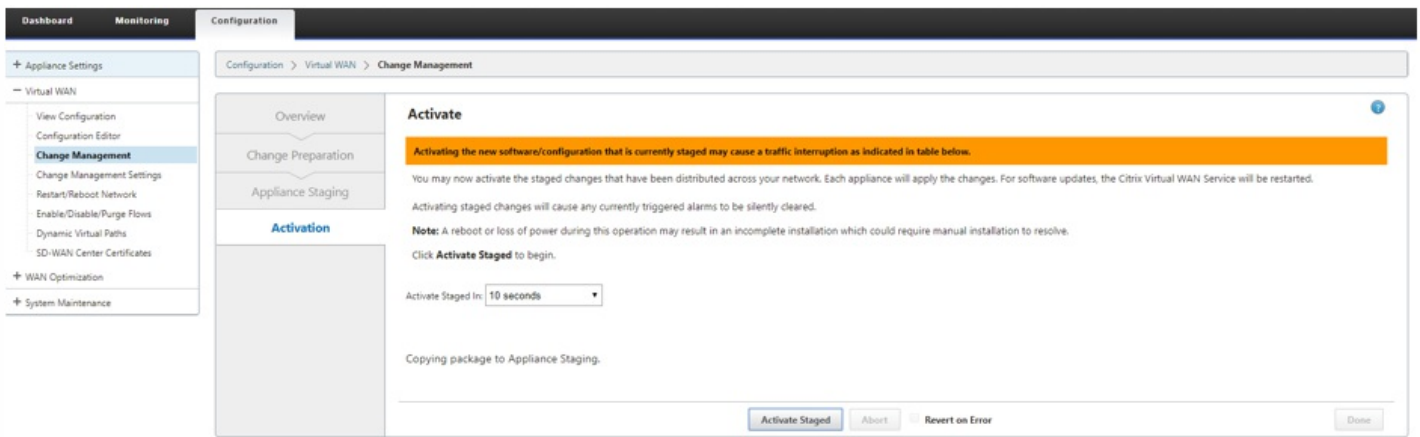
Currently Prepared: Configuration - Config_9_1_2_1k_MCN_2k_xen_esxi_400_410_branch.zip Software - 10.0.0.200.660093

Configuration Filenames: Active - Staged -

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

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Branch2KSite-Appliance	CB2000	Not Needed	Not Connected					Loc Chg Mgt	none / staged
Branch400-Appliance	CB400	Not Needed	Not Connected					Loc Chg Mgt	none / staged
Branch410-Appliance	CB410	Not Needed	Not Connected					Loc Chg Mgt	none / staged
BranchVPX-Appliance	CBVPX	Not Needed	Not Connected					Loc Chg Mgt	none / staged
MCN1KSite-Appliance	CB1000	Not Needed	Not Connected					Loc Chg Mgt	none / staged
VPX Esxi Branch-Appliance	CBVPX	Not Needed	Not Connected					Loc Chg Mgt	none / staged

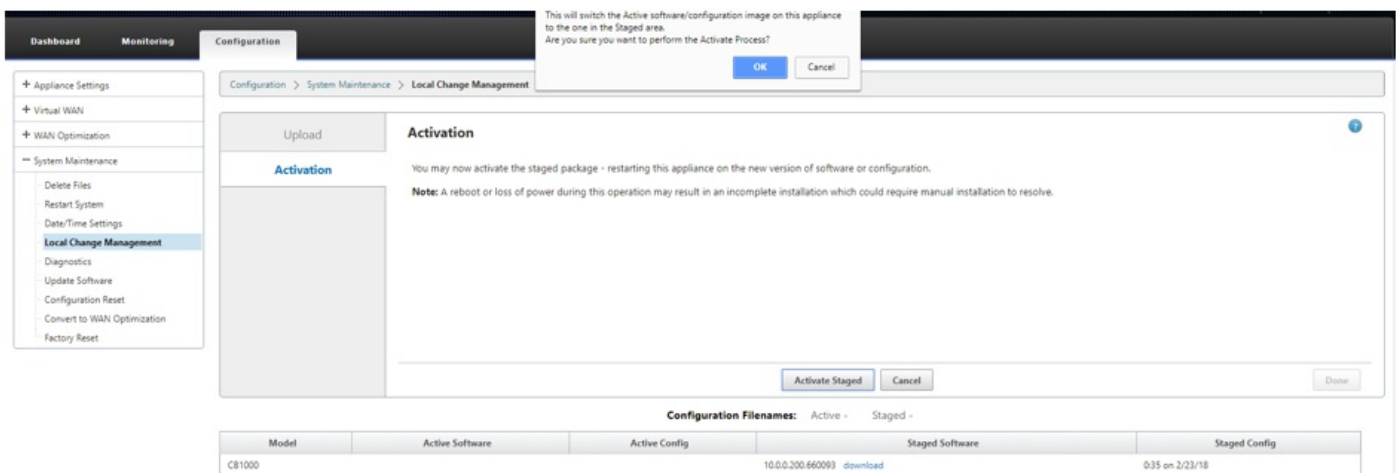


Currently Prepared: Configuration - Config_9_1_2_1k_MCN_2k_xen_esxi_400_410_branch.zip Software - 10.0.0.200.660093
 Configuration Filenames: Active - Staged -

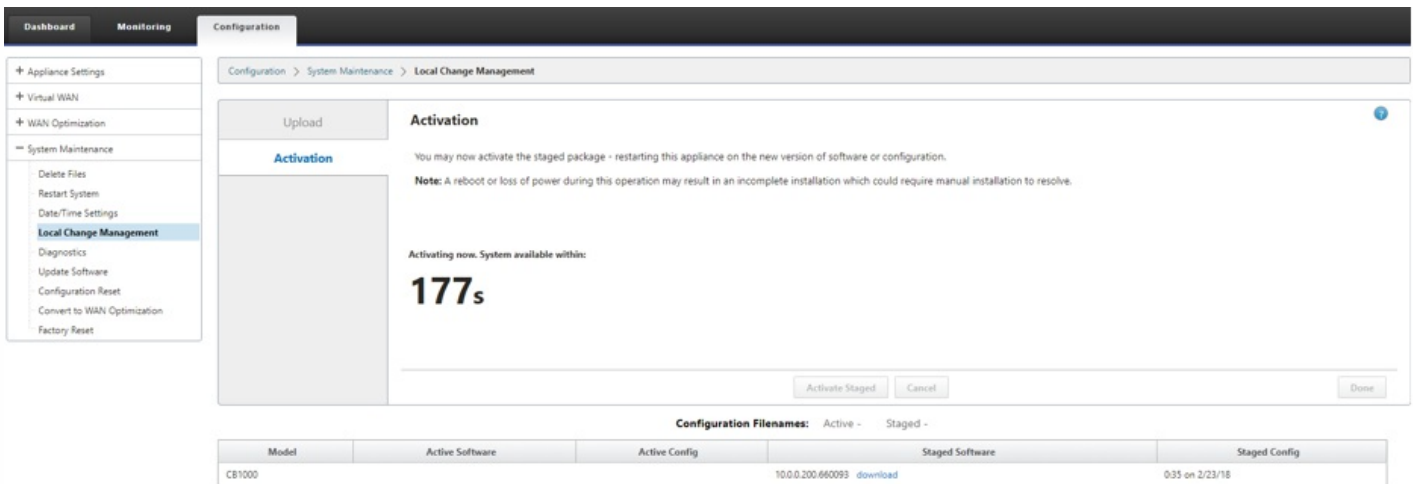
Click [here](#) to View or Update Change Management Settings.

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Branch2KSite-Appliance	CB2000	Not Needed	Not Connected				Loc Chg Mgt		none / staged
Branch400-Appliance	CB400	Not Needed	Not Connected				Loc Chg Mgt		none / staged
Branch410-Appliance	CB410	Not Needed	Not Connected				Loc Chg Mgt		none / staged
BranchVPX-Appliance	CBVPX	Not Needed	Not Connected				Loc Chg Mgt		none / staged
MCN1KSite-Appliance	CB1000	Not Needed	Not Connected				Loc Chg Mgt		none / staged
VPX_Esxi_Branch-Appliance	CBVPX	Not Needed	Not Connected				Loc Chg Mgt		none / staged

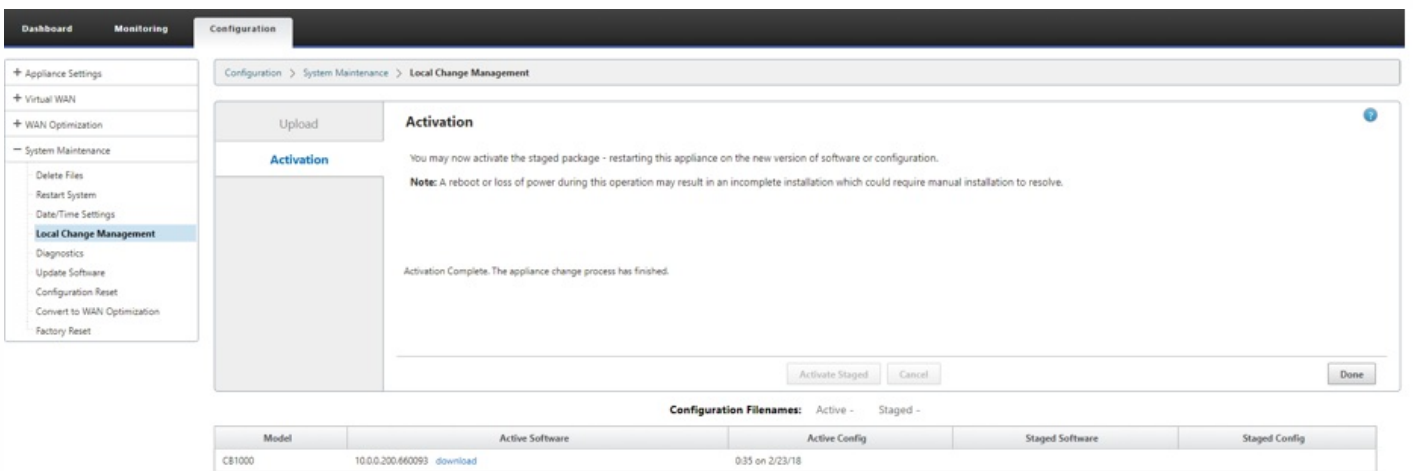
16. As this is the first time Appliance is being staged, you will be redirected to the **Local Change Management** page for activating the local appliance. After clicking on Activate Staged in Local Change Management once again, user confirmation is requested to proceed further.



17. After accepting, activation starts with a countdown timer of 180s.



18. After the countdown timer expiration, a message indicating activation has completed is displayed. Click **Done**.



19. Navigate to **Change Management** page to download the local change management for respective branches that you need to bootstrap to the network with Virtual WAN software upgrade only, or else move to the next step as shown below.

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Change Process Overview

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

Step 1
Change Preparation

Upload Files to MCN

MCN

Step 2
Appliance Staging

Transfer Files to Clients

MCN Clients

Step 3
Activation

Activate Change

MCN Clients

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

[Activate Staged](#) [Begin](#)

Configuration Filenames: Active - Config_9_1_2_1k_MCN_2k_xen_esxi_400_410_branch.cfg Staged -

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

Show 25 entries

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1KSite-Appliance	CB1000	10.0.0.200.660093	0:35 on 2/23/18				Loc Chg Mgt		active / none
Branch2KSite-Appliance	CB2000	Not Connected					Loc Chg Mgt		active / none
Branch400-Appliance	CB400	Not Connected					Loc Chg Mgt		active / none
Branch410-Appliance	CB410	Not Connected					Loc Chg Mgt		active / none
BranchVPX-Appliance	CBVPX	Not Connected					Loc Chg Mgt		active / none
VPX_Ext_Branch-Appliance	CBVPX	Not Connected					Loc Chg Mgt		active / none

[Previous](#) [1](#) [Next](#)

20. You can enable SD-WAN service and see that virtual paths are up between the branch and MCN.

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Enable/Disable/Purge Flows

System Status

Name: 1000
 Model: 1000
 Management IP Address: 10.105.199.28
 Software Version: 10.0.0.200.660093
 OS Partition Version: 4.6
 Serial Number: DVS4KCP5MW

! The Citrix Virtual WAN Service is currently disabled.
 The Citrix Virtual WAN Service was disabled because the configuration was missing. That problem has been fixed and the service can now be enabled.
 The Citrix Virtual WAN Service was disabled at: Fri Feb 23 00:41:07 2018
 The configuration has been updated - you may now re-enable the service on the Configuration -> Virtual WAN -> Enable/Disable/Purge Flows screen.

Enable Citrix Virtual WAN Service

! The Citrix Virtual WAN Service is currently disabled.
 The Citrix Virtual WAN Service was disabled because the configuration was missing. That problem has been fixed and the service can now be enabled.
 The Citrix Virtual WAN Service was disabled at: Fri Feb 23 00:41:07 2018
 The configuration has been updated - you may now re-enable the service.

[Enable](#)

Single-Step Upgrade for SD-WAN Appliances

Mar 01, 2018

Note

To use single step upgrade feature, the MCN must run a version which supports single step upgrade. For example; SD-WAN release version 9.3.x or newer.

A single step upgrade package using the SD-WAN GUI change management option to upgrade non-SD-WAN components in the network for all applicable platform editions is introduced. The MCN distributes all necessary software components to the sites (Branch) in the network.

After the branch receives the upgrade component files, these can be installed at scheduled time intervals as specified by the user. If the scheduled time is not specified, it uses the default time which is set by MCN for all branches.

The MCN also generates packages for sites on demand. Download the active package from the active hyperlink. You can bring or boot strap a new site into the network using the downloaded active package.

Note

Change management upload error occurs, if you attempt to perform single step upgrade (ns-sdw-sw-<version-number>.zip file) from previous release versions (8.1.x, 9.0.x, 9.1.x, 9.2.x).

Follow these procedures to upgrade:

[Upgrade to 10.0 with working Virtual WAN configuration](#)

[Upgrade to 10.0 without working Virtual WAN configuration](#)

Supported Upgrade and Downgrade Scenarios

Following are the supported upgrade and downgrade scenarios for SD-WAN SE and EE appliances. It is assumed that we are upgrading Virtual WAN software first and then upgrading the other components after the required software is staged at the branch sites or on the MCN.

Factory shipped appliances

You can download local change management package from MCN and apply it on the factory shipped appliance. After the local change management package is applied to the branch site boxes, all relevant components are upgraded immediately without waiting for maintenance window, if applicable.

Appliances with legacy Virtual WAN software

1. The appliances currently in an active network with virtual paths up and running.
 - The appliances receive packages from MCN. The components are installed and all files from MCN are received, and are

available in the scheduled time window.

2. The appliances are currently out of the network with virtual paths down.

- This process is similar to upgrading appliances which are factory shipped. You need to download local change management from MCN and upload the software package to the branch site appliances.

Appliances with single-step upgrade support

The appliance stages multiple files applicable at the branch site based on the appliance model and platform edition. The version information is reported by the branch site and/or configuration options, if applicable. The branch site appliances perform the upgrade utilizing the staged files. The non-Virtual WAN software components can be installed based on the preferences, manual and/or schedule.

Version switch or revert

Downgrading to a previous version of Virtual WAN software is supported. With single step upgrade process, you can install WANOP software packaged with a given Virtual WAN software version. You can only upgrade hotfix and/or SVM versions, if the software versions in the packages are higher.

Single step upgrade to legacy Virtual WAN software support

You can re-install the legacy software with the required configurations (using *tar.gz* files).

Downgrading to previous software version

If you upgraded an existing software version to release version 10.0 using the *tar.gz* upgrade process, you can downgrade the software version to a previous software version.

If you used the .zip (single step upgrade) procedure to upgrade to version 10.0, you cannot downgrade the software version to a previous software version.

Single step upgrade in high availability deployment mode

During single step upgrade if high-availability flip occurs, then you need to switch back to the old primary appliance manually, or upload the single bundle package to the new primary appliance.

Partial Software Upgrade Using Local Change Management

Mar 11, 2018

Important

By default, the **Partial Software Upgrade** option is disabled.

In NetScaler SD-WAN 10.0 release, a user can install a newer SD-WAN software release version on a subset of client sites using the **Local Change Management** option. This is achieved through the partial software upgrade feature which allows the network administrator to selectively upgrade the software on sites in the network without needing to upgrade all sites simultaneously. A specific use-case for this feature is an Administrator testing the new software on few branch sites before installing it on all sites in the network.

Prerequisites and Requirements

Before proceeding with performing partial software upgrade; review the following requirements:

1. Have an active SD-WAN version 10.0 or newer software. Click **Enable Partial Software Upgrade** checkbox. If you uncheck the box, the software that is currently running on the MCN appliance is applied to the branches which have active virtual paths running.

The screenshot displays the 'Change Management Settings' page in the NetScaler SD-WAN configuration interface. At the top, the breadcrumb navigation shows 'Configuration > Virtual WAN > Change Management Settings'. Below this, there is a section titled 'Enable/Disable Partial Software Upgrade' with a checkbox labeled 'Enable Partial Software Upgrade' and an 'Apply' button. A help icon (?) is visible in the top right corner of this section.

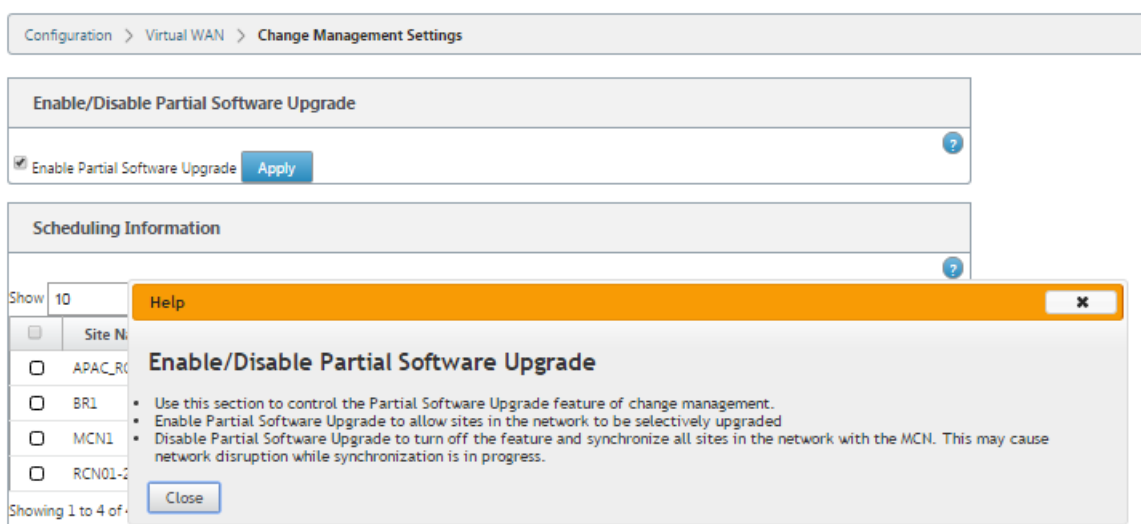
Below the checkbox is a section titled 'Scheduling Information'. It includes a 'Show' dropdown menu set to '10' entries, a search input field, and buttons for 'Edit Selected' and 'Refresh'. A help icon (?) is also present in the top right corner of this section.

The main content is a table with the following columns: 'Site Name', 'Scheduling Information', 'Status', and 'Edit'. The table lists 17 entries, showing the first 10. Each entry includes a checkbox, the site name, the scheduling details (e.g., '2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)'), a status indicator (e.g., a green dot, a red exclamation mark, or a red 'X'), and an edit icon.

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

Showing 1 to 10 of 17 entries

Navigation: Previous | 1 | 2 | Next



2. Stage new version of software using the MCN **Change Management** process with the same Major version number as the active software and the same configuration as the active configuration.

3. The new software should be the same major version of software as the active software. The minor version can be different software version.

4. The new software must first be staged to on all sites from the MCN. Stop at **Activate Staged** step of Change Management.

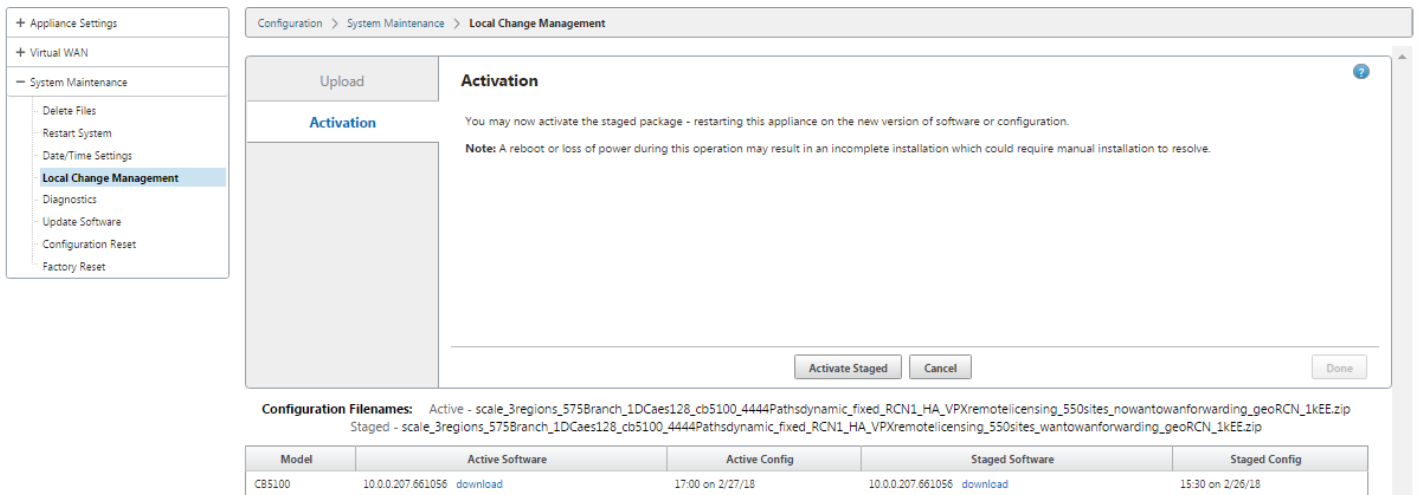
For the configuration of the Active and Partial site, software must be identical on the MCN and Branch sites. It is not possible to have a different feature set enabled on partially upgraded sites. Proceed to individual sites to perform **Local Change Management**. See the instructions below for High Availability deployment.

To perform partial SD-WAN software upgrade:

There are two scenarios in which you can perform partial SD-WAN software upgrade on a branch node; High Availability mode and non-High Availability mode.

Upgrading Branch Node Without High Availability Mode

1. In the NetScaler SD-WAN web management interface, navigate to the branch site, which needs to be upgraded through the Partial Site Upgrade process.
2. Open **Local Change Management**. Click **Next**.
3. Click **Activate Staged**. Each branch site will now be installed with new software version.



Upgrading Branch Node in High Availability Mode

1. In the SD-WAN web management interface, navigate to the branch site, which needs to be upgraded through the Partial Site Upgrade.
2. Disable service on the standby appliance.
3. On the primary appliance, open **Local Change Management**.
4. Click **Activate Staged**. This appliance will now be installed with new software version.
5. On the standby appliance, open **Local Change Management**.
6. Click **Activate Staged**. The standby appliance will now be installed with new software version.
7. After the primary and standby appliances have completed the activation process, enable service on the standby appliance.

Upgrading Network

When you are ready to bring the network in sync, navigate to the MCN network change management screen, and click **Activate Staged**.

WANOP to Enterprise Edition Conversion With USB

Mar 01, 2018

Note

Only the SD-WAN 1000 and 2000 WANOP appliances can be converted to SD-WAN Enterprise Edition appliances.

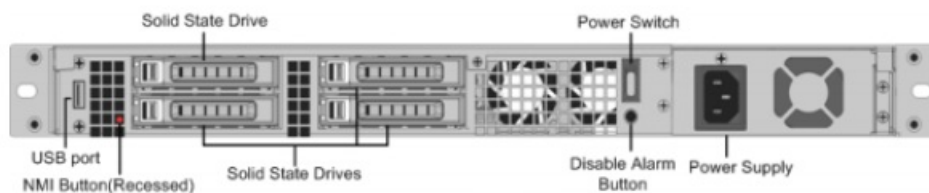
Before You Begin

- Ensure that you are converting the 1000 appliance only, and not the 1000 WS. The 1000 WS appliance does not support conversion to the SD-WAN Enterprise Edition appliance.
- Ensure that you have the default credentials to log into the existing *Dom-0 - root/nsroot*.

Upgrade Procedure

The conversion procedure is a two-step process involving the following steps:

- Insert enclosed USB stick into the Citrix SD-WAN appliance.
- Verify that the serial console is connected and proceed with the conversion process.



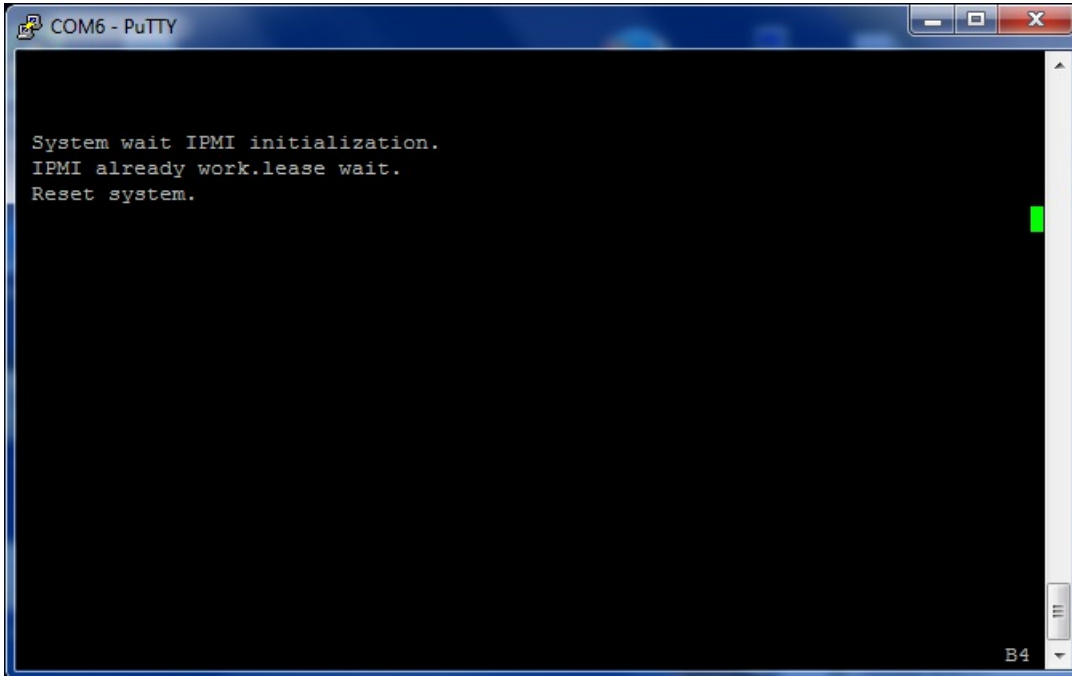
How To Convert With USB Stick

To upgrade the appliance with USB stick:

1. Insert the enclosed USB stick into the Citrix SD-WAN appliance.
2. Connect to the serial console of the appliance.
3. Reboot the appliance.
4. During the boot process, when you see the cursor moving across the screen, do the following:
 - a. Press and hold the **ESC** key.
 - b. Press and hold the **SHIFT** key.
 - c. Press the number **1** key (SHIFT +1 = !) and release all keys.
 - d. Repeat steps a, b, and c until the cursor stops moving.

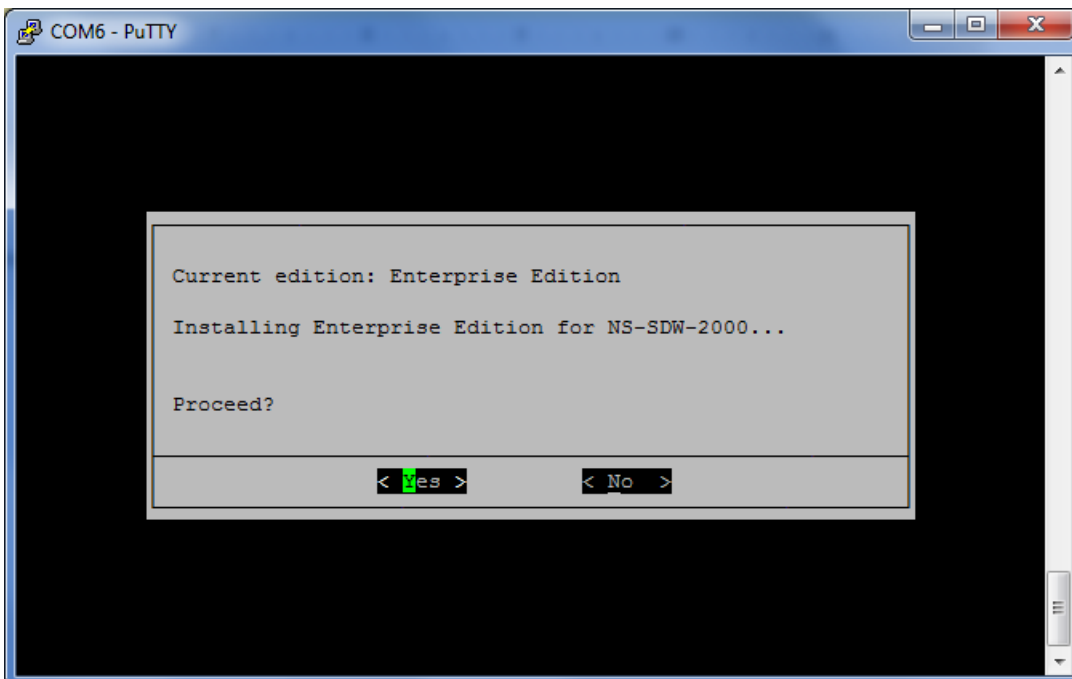
Note

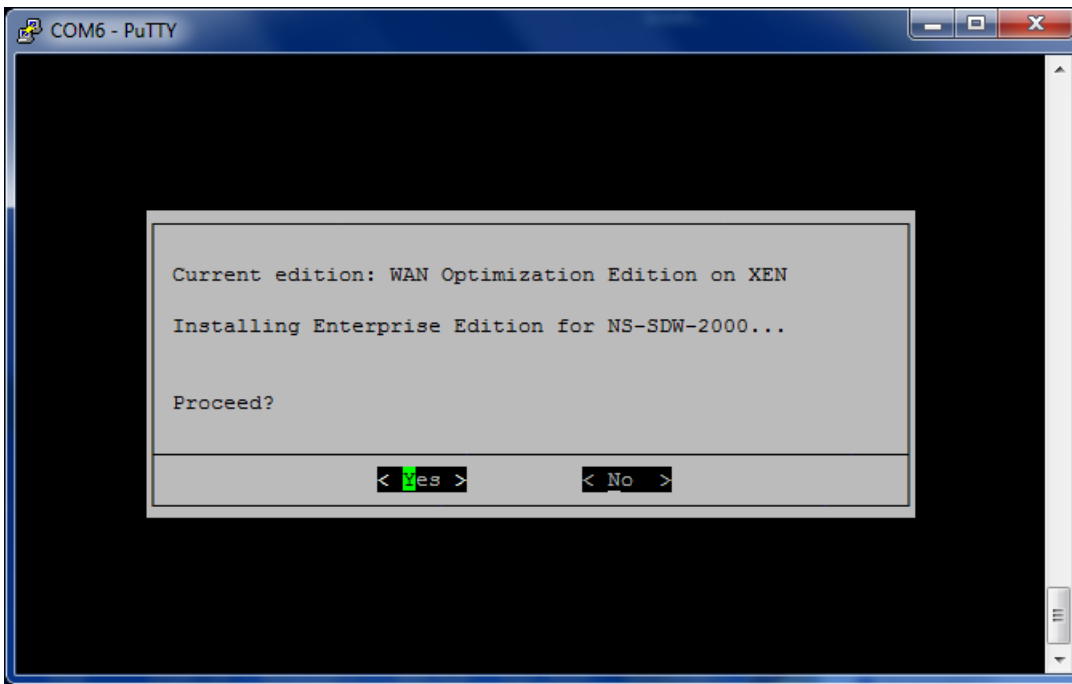
The above steps should be executed during the appliance reboot process. The key strokes should happen during BIOS post stage as described in step 4.



5. When BIOS loads, choose the external USB drive, for example; PNY USB 2.0 FD 1100 to boot the appliance. The external USB drive is shipped by Citrix if you have ordered for it.

You need to choose the platform edition which you want to use, if the platform supports more than one edition, such as 1000 and 2000. Therefore, choose Enterprise Edition first before confirming.





6. Choose the **Enterprise Edition** software upgrade option when prompted.

7. Upgrade process is completed in 20-30 minutes. The system reboots after 1-2 minutes and the login prompt is displayed. For the 1000 platform edition, upgrade process is approximately an hour as updating the internal USB drive itself takes around half an hour.

8. Unplug the USB stick after the procedure is complete.



References

- For licensing about the NetScaler and NetScaler SD-WAN products, see the support link at: <http://support.citrix.com/article/ctx131110>
- For Documentation and Release Notes information about NetScaler SD-WAN, see; <https://docs.citrix.com/en-us/netscaler-sd-wan.html>.

Convert Standard Edition to Enterprise Edition

Mar 01, 2018

To perform platform conversion from Standard Edition to Enterprise Edition:

1. Export the Configuration locally.
2. Download the **Active Package** from the **Change Management** page.
3. Upgrade the appliance using the downloaded package from **System Maintenance** -> **Update Software** -> **Re-image Virtual WAN Appliance software**.
4. Click **Choose File** to provide the *cb-vw_CB1000_x.x.x.tar.gz* file. Where x.x.x is the SD-WAN software release version.
5. Click **Upload**. Select **Accept** and click on **Install** to proceed.
6. Install the Enterprise Edition License.
7. Perform **Local Change Management** on the appliance using the downloaded active package in step 2 above.

Licensing

Mar 01, 2018

NetScaler SD-WAN License Options

There are three NetScaler SD-WAN Editions each with a different set or subset of NetScaler SD-WAN features. The type of license you install determines the NetScaler SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances.

Note

When installing and applying a license, make sure that your specific appliance supports the SD-WAN appliance edition you want to enable, and that you have the correct software version available.

NetScaler SD-WAN Platform Software Support

The following table illustrates which NetScaler SD-WAN platforms are supported for each of the available NetScaler SD-WAN software versions.

Version	WAN Optimization Edition	Standard Edition	Enterprise Edition
Release 7.X	Yes	—	—
Release 8.X	—	Yes	—
Release 9.0	—	Yes	Yes
Release 9.1	Yes	Yes	Yes
Release 9.2	Yes	Yes	Yes
Release 9.3	Yes	Yes	Yes
Release 10.0	Yes	Yes	Yes

Earlier version of licenses, including those compatible with release 7.x, are not supported with the newer NetScaler SD-WAN release. The existing process to obtain NetScaler SD-WAN licenses remains consistent with the CloudBridge 8.0.x, and 9.0.x releases. Once obtained, the licenses can be activated through the appliance's management web interface.

The following table lists all the appliance models supported in Citrix SD-WAN release 10.0:

Platform Edition	License Model
Standard Edition VPX	VPX-020, 050, 100, 200, 500, 1000
Standard Edition 210, 410	210-20, 210-50, 410-050, 410-100, 410-200
Standard Edition 1000	1000-020, 1000-050, 1000-100
Standard Edition 2000	2000-100, 2000-200, 2000-300
Standard Edition 2100	2100-200, 2100-300, 2100-500, 2100-1000, 2100-1500, 2100-2000
Standard Edition 4100	4100-1000, 4100-2000, 4100-3000
Standard Edition 5100	5100-3000, 5100-4000, 5100-5000
WANOP Edition VPX	VPX-2, 6, 10, 20, 50, 100, 200
WANOP Edition 800	800-002, 800-006, 800-010
WANOP Edition 1000 Windows Server	1000WS-006, 1000WS-010, 1000WS-020
WANOP Edition 1000	1000-006, 1000-010, 1000-020
WANOP Edition 2000	2000-010, 2000-020, 2000-050
WANOP Edition 3000	3000-050, 3000-100, 3000-155
WANOP Edition 4000	4000-310, 4000-500, 4000-1000
WANOP Edition 4100	4100-310, 4100-500, 4100-1000
WANOP Edition 5000	5000-1500, 5000-2000
WANOP Edition 5100	5100-1500, 5100-2000
Enterprise Edition 1000	1000-010, 1000-020, 1000-050, 1000-100
Enterprise Edition 2000	2000-100, 2000-200, 2000-250
Enterprise Edition 2100	2100-200, 2100-300, 2100-500, 2100-1000

VPX-WANOP models allow 2, 6, 10, 20, 50, 100, and 200 Mbps bandwidth licenses. At least two 2.1 GHZ CPUs are required in order to support the VPX instances.

Before you can download the software, you must obtain and register a NetScaler SD-WAN software license. For instructions on obtaining a NetScaler SD-WAN software license, contact Citrix NetScaler SD-WAN Customer Support. Instructions for uploading and installing the license file on your appliances are provided in the section, [Uploading and](#)

[Installing the SD-WAN Software License File](#). Before installing the license, you must first setup the appliance hardware, and set the date and time for the appliance.

The license procedure for provisioning licensing for SD-WAN platform editions covers the following topics:

- Supported SD-WAN license model: Local, Remote, and Centralized.
- Remote License Server support for SD-WAN appliances.
- Pre-requisites for using Remote License Server.

Returning and Reallocating Licenses

To return or reallocate a license, you must use the Citrix NetScaler SD-WAN Licensing Portal. You also have the option to use the Licensing Portal for license allocation. For instructions, see the Knowledge Base article entitled, “[My Account All Licensing Tools User Guide](#),” at this location: <http://support.citrix.com/article/ctx131110>

Local Licensing

Mar 01, 2018

With local license, you are required to login to each appliance in the network and upload the license file. Even with the ZTD service, the appliance becomes available with only a grace license. You will have to upload a license file for network continuity. The license files are generated based on the host ids of the individual appliances.

You can install and configure license for SD-WAN appliances using the SD-WAN web management interface.

Importing licenses for SD-WAN appliances deployed on XenServer/ESXi/Hyper-V platforms:

1. In the SD-WAN web management interface, navigate to **Configuration > Appliance Settings > Licensing**.
2. Select **Local** and upload the License. Click **Upload and Install**.
3. Save your changes by clicking **Apply Settings**.

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

Remote Licensing

Mar 01, 2018

Pre-requisites for using Remote License Server for SD-WAN appliances.

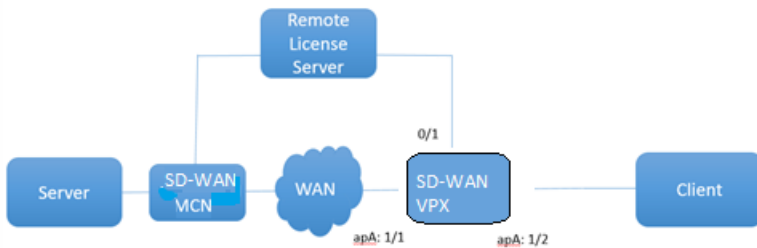
- NTP should be configured for both License server and SD-WAN (date and time should be in-sync)
- Remote License Server version should be 11.13.1 or earlier.

It is recommended that you use the latest License Server version:

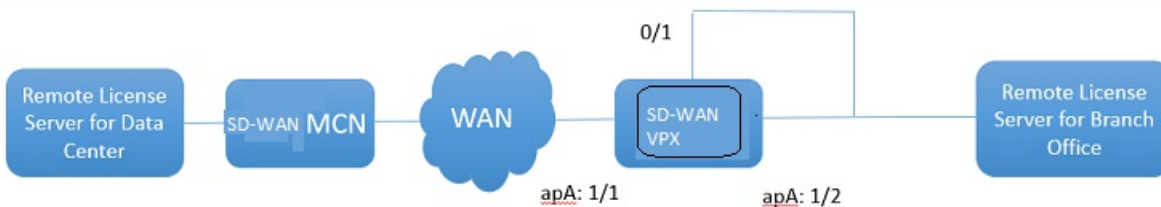
- Release 9.2: 11.13.1 L.S
- Release 9.1: 11.13.1 L.S
- Release 9.0: 11.13.1 L.S
- Release 8.1: 11.12.1 L.S

Use Cases

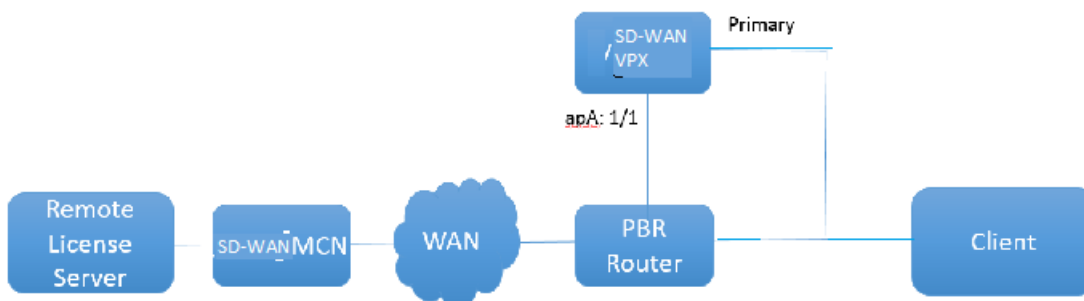
1. Remote license server reachable through the management network without using data/apA Ports.



2. Remote license server in the Branch network.



3. SD-WAN VPX-SE - PBR deployment in the Branch office.



Remote License

1. In the SD-WAN web management interface, navigate to **Configuration > Appliance Settings > Licensing**.
2. Select **Remote** and enter the Remote Server-IP address details.

License Configuration

Local Remote

Configure Licensing Server

IP Address:

Port:

Model:

3. Select the desired appliance **Model** from the drop-down menu. The default port for remote license server is 27000.

Model:

- Not Configured
- 4100vW-500
- 4100vW-1000
- 4100vW-2000
- 4100vW-3000

Important

If you want to install remote licenses for SD-WAN appliance using SD-WAN Center, ensure that you enable Centralized licensing on the SD-WAN MCN appliance in the Global settings of the SD-WAN web management interface Configuration Editor.

Centralized Licensing

Jun 12, 2018

As the network deployments grow with large number of network nodes, managing and licensing appliances becomes cumbersome. To simplify this process for efficient onboarding of the SD-WAN appliances and easy network operations, centralized licensing model for the SD-WAN network has been introduced.

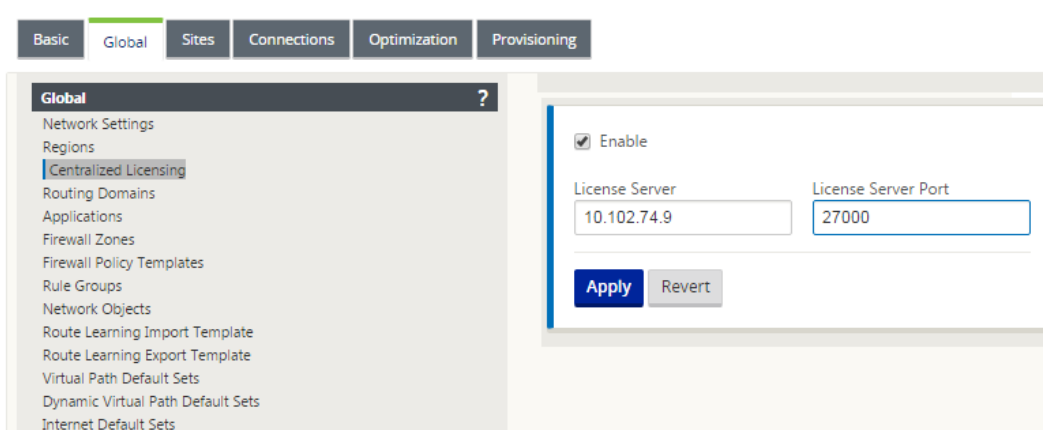
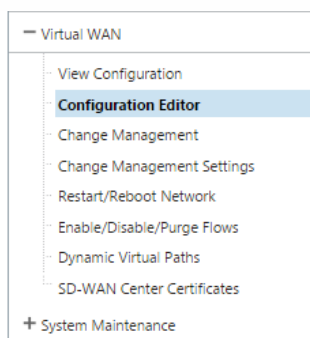
In the new centralized license model, the SD-WAN center web management interface (SD-WAN appliance management and reporting portal), provides licensing services to individual SD-WAN appliances in the network without you having to login to the appliance.

The SD-WAN center IP address is provided in the SD-WAN appliance GUI under **Global > Centralized licensing**. This IP address is propagated to individual appliances through the configuration packages or updates. When the IP address is changed, you have to go through the Change Management process to push it appliances. The global setting can be overridden by the local site settings.

The license bandwidth can be selected with the appliance model for Site settings. The WAN links bandwidth are audited against the license selected.

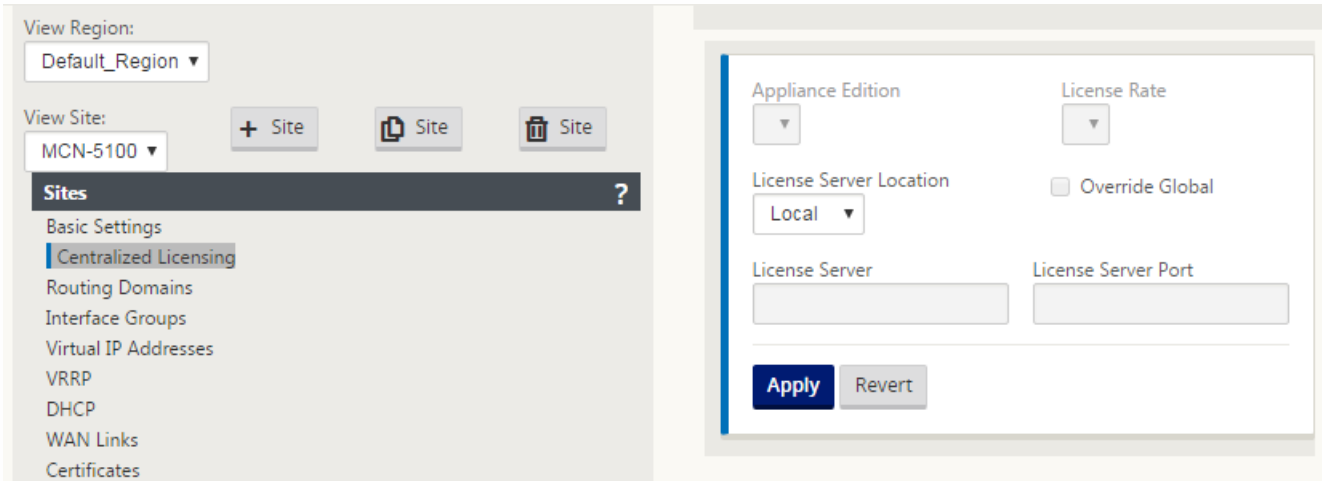
To enable centralized licensing in the SD-WAN appliance GUI:

1. Navigate to **Configuration > Virtual WAN > Configuration Editor**. Open an existing virtual WAN configuration package or create new configuration package. The configuration package opens.
2. Navigate to the **Global** tab. Select **Centralized Licensing**. Click **Enable**.
3. Enter the IP address for the License Server from which you need to download and manage SD-WAN licenses. You can provide the SD-WAN Center management IP address, so that the configuration package for the SD-WAN MCN or branch appliances can download license from SD-WAN Center.
4. Enter **27000** for the **License Server Port** which is a default port number.

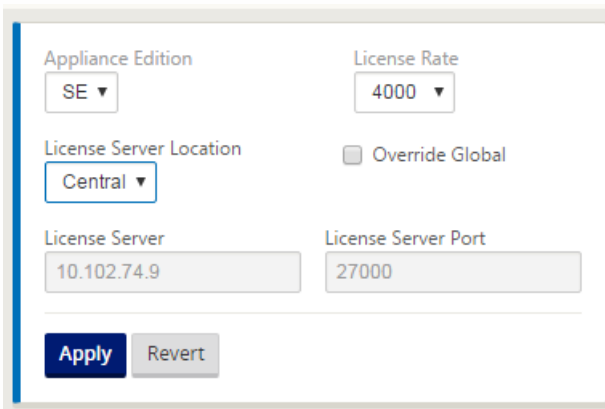


5. Click **Apply**.
6. Navigate to the **Sites** tab. Select MCN or Branch site under **View Site**, depending on the region and site for which you want to manage central licensing.
7. Select **Centralized Licensing**. The central licensing options view is displayed. By default, the **Local** option is selected for

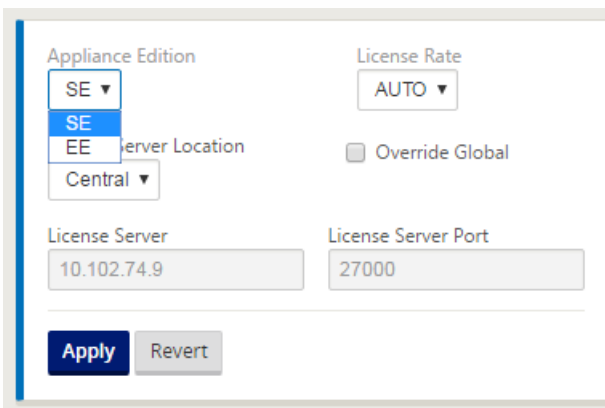
the **License Server Location**.



8. Click the drop-down menu and select **Central** to change the default license server location. This displays the IP address and port information you provided for the license server when you enable central licensing in the Global settings. For example; the license server could be the IP address of the SD-WAN Center managing the appliances in the network.



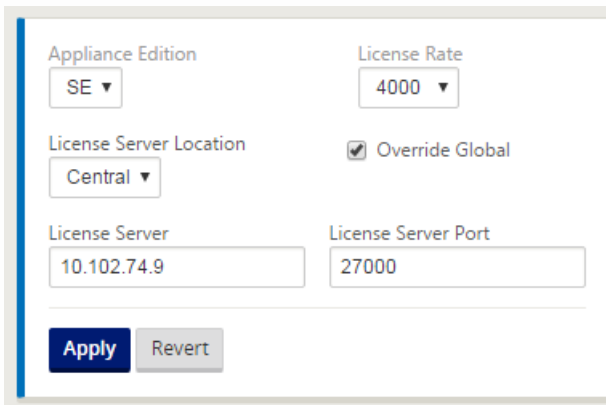
9. Choose the **Appliance Edition** and **License Rate** depending on the appliances to be installed; such as the Standard Edition or Enterprise Edition. Click **Apply**.



Note

You can choose to override the license server information provided in the Global settings of the configuration.

10. Select **Override Global** to override global settings. Configure new license server IP address. Retain the default license server port number; 27000. Click **Apply**.



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

- Appliance Edition:** A dropdown menu with 'SE' selected.
- License Rate:** A dropdown menu with '4000' selected.
- License Server Location:** A dropdown menu with 'Central' selected.
- Override Global:** A checked checkbox.
- License Server:** A text input field containing '10.102.74.9'.
- License Server Port:** A text input field containing '27000'.
- Buttons:** 'Apply' (highlighted in blue) and 'Revert' (disabled).

You can now manage licenses for all the nodes in branch and MCN sites configured for a specific SD-WAN appliance configuration package from the licensing server you configured.

This license server can be an SD-WAN Center management portal which acquires licenses obtained from the network configuration to the sites through the change management process.

Note

When Centralized licensing is configured for a site with a specific license rate (bandwidth), the site appliance can consume the license rate equal to or greater than the license rate configured for that site.

Managing Licenses

Mar 01, 2018

SD-WAN appliances licenses are managed by communicating with the remote license service to check for licenses. If the appliance is licensed, the network operations continue without interruption. If the appliance is not licensed, the grace license mode is initiated.

SD-WAN appliance license management process:

1. Each site communicates with Remote Server or SD-WAN Center using the Web Management Interface. This communication occurs through a heartbeat mechanism to monitor connectivity and a checkout mechanism that verifies the license status.
2. Heartbeats are sent over a TCP connection to the license server every 10-20 mins to check connectivity.
3. After a loss of 2 consecutive Heartbeats, the appliance goes into a grace mode. The checkout method determines the license status. This status could be "Real", "Grace", or "Denied" that is sent to the appliance from the SD-WAN Center. Every time an appliance reaches out to the SD-WAN Center for license status, it checks-in and checks-out the new license. If SD-WAN center does not receive 2 heart beats, the SD-WAN center will release the license allocated to the site into the pool. The grace period is 30 days, so after loss of 2 heartbeats, the appliance will go into the grace period. During these 30 days, the communication has to be restored. Once restored, the appliance reverts back to normal operational mode. If the communication is NOT restored, the appliance will be put into unlicensed state and follows the unlicensed/license expiry procedure.

Out-of-Box licensing (OOB) for MCN appliance:

- MCN appliance will not have an initial grace period. It needs to be licensed to come up.

Out-of-Box licensing (OOB) for client appliance:

- Client node will come up with a 30-day grace period with or without ZTD functionality.
- The appliance will be enabled and installed with a OOB license file valid for 30 days.
- You have 30 days to upload a license file or get licensed through the Centralized Licensing server.
- If the appliance is licensed, it will function normally and be part of the network.
- If the appliance is not licensed within 30 days, the license expiry procedure is followed.
- The only way to reset the appliance to again come up with OOB license is to perform a "Factory Reset".

License Expiry

Mar 01, 2018

The SD-WAN appliance goes into a 30-day grace period and you have to upload the license after the license expires.

During the grace period, all operations function normally. If the license is not uploaded in time (30 days after expiry), Virtual WAN Service is disabled.

Centralized licensing has a log file to track the functioning of grace period, unlicensed, licensed, communication status and failures.

In the SD-WAN appliance GUI, under diagnostics, the MCN connectivity test functionality in SD-WAN Center to other sites is available. This can be used to test if each appliance can reach the licensing server. Sites, license state, and status table are available for managing and tracking licenses.

Grace Period

1. 30 day grace period is provided for Out-of-Box client nodes. Notification indicates that the appliance is in Out-of-Box mode and needs a valid license. This option uses a grace license file.
2. License expiry: Once the license expires, a 30 day grace period is provided. Notification indicates that the reason for grace period is the license expiry and needs a renewal.
3. Loss of communication with SD-WAN center: After 2 heart beats loss, the appliance goes into the grace mode for 30 days. Notification indicates that the reason for the grace period is a communication failure.

Configuration

Mar 01, 2018

After you have installed the SD-WAN software and licenses, you can configure SD-WAN appliance settings to start managing your network and deployment.

NetScaler SD-WAN appliance configuration includes the following:

Configure MCN: The MCN serves as the distribution point for the initial system configuration and any subsequent configuration changes. You perform most upgrade procedures through the Management Web Interface on the MCN. There can be only one active MCN in a Virtual WAN.

By default, appliances have the pre-assigned role of client. To establish an appliance as the MCN, you must first add and configure the MCN site, and then stage and activate the configuration and appropriate software package on the designated MCN appliance.

Configure Branch: The procedure for adding a branch site is very similar to creating and configuring the MCN site. However, some of the configuration steps and settings do vary slightly for a branch site. In addition, once you have added an initial branch site, for sites that have the same appliance model you can use the **Clone** (duplicate) feature to streamline the process of adding and configuring those sites. As with creating the MCN site, to set up a branch site you must use the **Configuration Editor** in the Management Web Interface on the MCN appliance. The **Configuration Editor** is available only when the interface is set to **MCN Console** mode.

Configure virtual path between MCN and branch sites: Configure the Virtual Path Service between the MCN and each of the client (branch) sites. To do this, you will use the configuration forms and settings available in the **Connections** section configuration tree of the **Configuration Editor**.

Enable and configure WAN optimization: The section provides step-by-step instructions for enabling and configuring SD-WAN Enterprise Edition WAN Optimization features for your Virtual WAN. To do this, you will use the **Optimization** section forms in the **Configuration Editor** in the Web Management Interface on the MCN.

Initial Setup

Mar 01, 2018

These procedures must be completed for each appliance you want to add to your SD-WAN. Consequently, this process will require some coordination with your Site Administrators across your network, to ensure the appliances are prepared and ready to deploy at the proper time. However, once the Master Control Node (MCN) is configured and deployed, you can add client appliances (client nodes) to your SD-WAN at any time.

For each appliance you want to add to your Virtual WAN, you will need to do the following.

1. Set up the SD-WAN Appliance hardware and any SD-WAN VPX Virtual Appliances (SD-WAN VPX-VW) you will be deploying.
2. Set the Management IP Address for the appliance and verify the connection.
3. Set the date and time on the appliance.
4. Set the console session **Timeout** threshold to a high or the maximum value.

Warning

If your console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is strongly recommended that you set the console session **Timeout** interval to a high value when creating or modifying a configuration package, or performing other complex tasks.

5. Upload and install the software license file on the appliance.

For instructions on installing a SD-WAN Virtual Appliance (SD-WAN VPX), see the following sections:

- [About SD-WAN VPX.](#)
- [Installing and Deploying a SD-WAN VPX-SE on ESXi.](#)
- [Differences Between a SD-WAN VPX-SE and SD-WAN WANOP VPX Installation.](#)

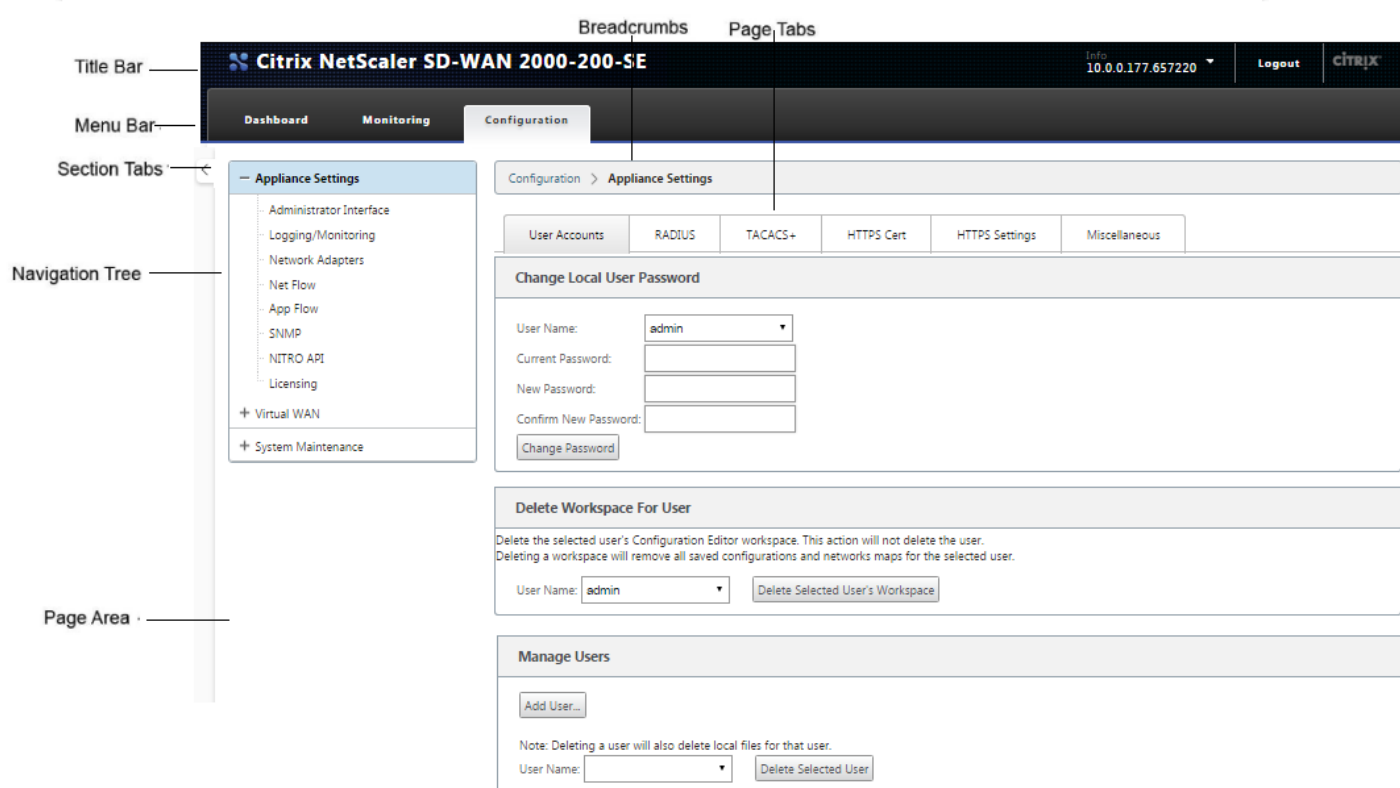
Overview of Web Interface (UI) Layout

Mar 01, 2018

This section provides basic navigation instructions, and a navigation roadmap of the SD-WAN web management interface page hierarchy. Also provided are specific navigation instructions for the **Configuration Editor** and **Change Management wizard**.

Basic Navigation

The below figure outlines the basic navigation elements of the Web Management Interface, and the terminology used to identify them.



The basic navigation elements are as follows:

- **Title bar** – This displays the appliance model number, Host IP Address for the appliance, the version of the software package currently running on the appliance, and the user name for the current login session. The title bar also contains the **Logout** button for terminating the session.
- **Main menu bar** – This is the bar displayed below the title bar on every Management Web Interface screen. This contains the section tabs for displaying the navigation tree and pages for a selected section.
- **Section tabs** – The section tabs are located in the main menu bar at the top of the page. These are the top-level categories for the Web Management Interface pages and forms. Each section has its own navigation tree for navigating the page hierarchy in that section. Click a **section** tab to display the navigation tree for that section.

- **Navigation tree** – The navigation tree is located in the left pane, below the main menu bar. This displays the navigation tree for a section. Click a section tab to display the navigation tree for that section. The navigation tree offers the following display and navigation options:
 - Click a section tab to display the navigation tree and page hierarchy for that section.
 - Click + (plus sign) next to a branch in the tree to reveal the available pages for that branch topic.
 - Click a page name to display that page in the page area.
 - Click – (minus sign) next to a branch item to close the branch.
- **Breadcrumbs** – This displays the navigation path to the current page. The breadcrumbs are located at the top of the page area, just below the main menu bar. Active navigation links display in blue font. The name of the current page is displayed in black bold font.
- **Page area** – This is the page display and work area for the selected page. Select an item in the navigation tree to display the default page for that item.
- **Page tabs** – Some pages contain tabs for displaying additional child pages for that topic or configuration form. These are usually located at the top of the page area, just below the breadcrumbs display. In some cases (as for the **Change Management** wizard), tabs are located in the left pane of the page area, between the navigation tree and the work area of the page.
- **Page area resizing** – For some pages, you can grow or shrink the width of the page area (or sections of it) to reveal additional fields in a table or form. Where this is the case, there will be a grey, vertical resize bar on the right border of a page area pane, form, or table. Roll your cursor over the resize bar until the cursor changes to a bi-directional arrow. Then click and drag the bar to the right or left to grow or shrink the area width.

If the resize bar is not available for a page, you can click and drag the right edge of your browser to display the full page.

Web Management Interface Navigation Tree Hierarchy

TOP LEVEL SECTION TAB	TREE LEVEL 1	TREE LEVEL 2
Dashboard		
	System Status	
	Local Versions	
	Virtual Path Service Status	
Monitoring		
	Statistics	
	Flows	
	Routing Protocols	
	Firewall	
	IKE/IPsec	
	IGMP	
	Performance Reports	
	QoS Reports	
	Usage Reports	

	Appliance Reports	
	DHCP Server/Relay	
	VRRP	
	WAN Optimization	
		Connections
		Compression
		Usage Graph
		App Flow
		Filesystem (CIFS/SMB)
		Citrix (ICA/CGP)
		ICA Advanced
		Outlook (MAPI)
		Partners
Configuration		
	Appliance Settings	
		Administrator Interface
		Logging/Monitoring
		Network Adapters
		Net Flow
		App Flow
		SNMP
		NITRO API
		Licensing
	Virtual WAN	
		View Configuration
		Configuration Editor
		Change Management Settings
		Change Management
		Restart/Reboot Network
		Enable/Disable/Purge Flows
		Dynamic Virtual Paths
		SD-WAN Center Certificates
	System Maintenance	
		Delete Files
		Restart System
		Date/Time Settings
		Local Change Management
		Diagnostics
		Update

		Update Software
		Configuration Reset
		Factory Reset

Web Management Interface Dashboard

Click the **Dashboard** section tab to display basic information for the local appliance.

The **Dashboard** page displays the following basic information for the appliance:

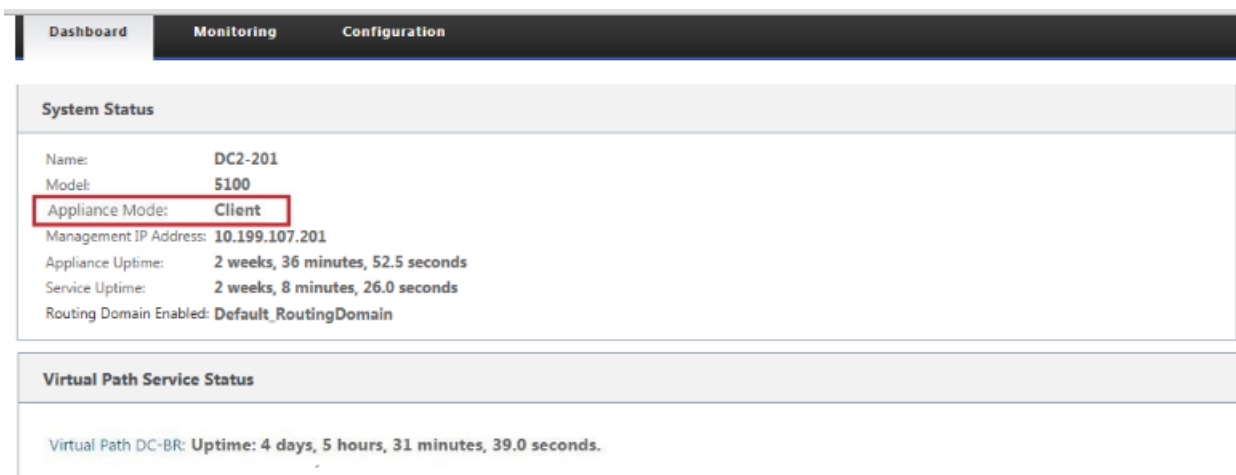
- System status
- Virtual Path service status
- Local appliance software package version information

The below figure shows a sample Master Control Node (MCN) appliance **Dashboard** display.

The screenshot displays the Citrix Dashboard for a Master Control Node (MCN) appliance. The interface includes a navigation bar with 'Dashboard', 'Monitoring', and 'Configuration' tabs. The main content area is organized into three sections:

- System Status:**
 - Name: DC2k
 - Model: 2000
 - Appliance Mode: MCN
 - Serial Number: 75XHP2F8U9
 - Management IP Address: 10.199.106.186
 - Appliance Uptime: 1 weeks, 4 days, 2 hours, 27 minutes, 47.4 seconds
 - Service Uptime: 4 hours, 35 minutes, 26.0 seconds
 - Routing Domain Enabled: Default_RoutingDomain
- Local Versions:**
 - Software Version: 10.0.0.177.657220
 - Built On: Feb 9 2018 at 17:04:16
 - Hardware Version: 2000
 - OS Partition Version: 4.6
- Virtual Path Service Status:**
 - Virtual Path DC2k-BR01: Uptime: 4 hours, 34 minutes, 49.0 seconds.
 - Virtual Path DC2k-BR02: Uptime: 4 hours, 34 minutes, 49.0 seconds.
 - Virtual Path DC2k-BR03: Uptime: 4 hours, 34 minutes, 47.0 seconds.
 - Virtual Path DC2k-BR04: Uptime: 4 hours, 3 minutes, 57.0 seconds.
 - Virtual Path DC2k-BR05: Uptime: 4 hours, 4 minutes, 2.0 seconds.
 - Virtual Path DC2k-BR06: Uptime: 4 hours, 3 minutes, 58.0 seconds.

The below figure shows a sample client appliance Dashboard display.



Configuration Editor

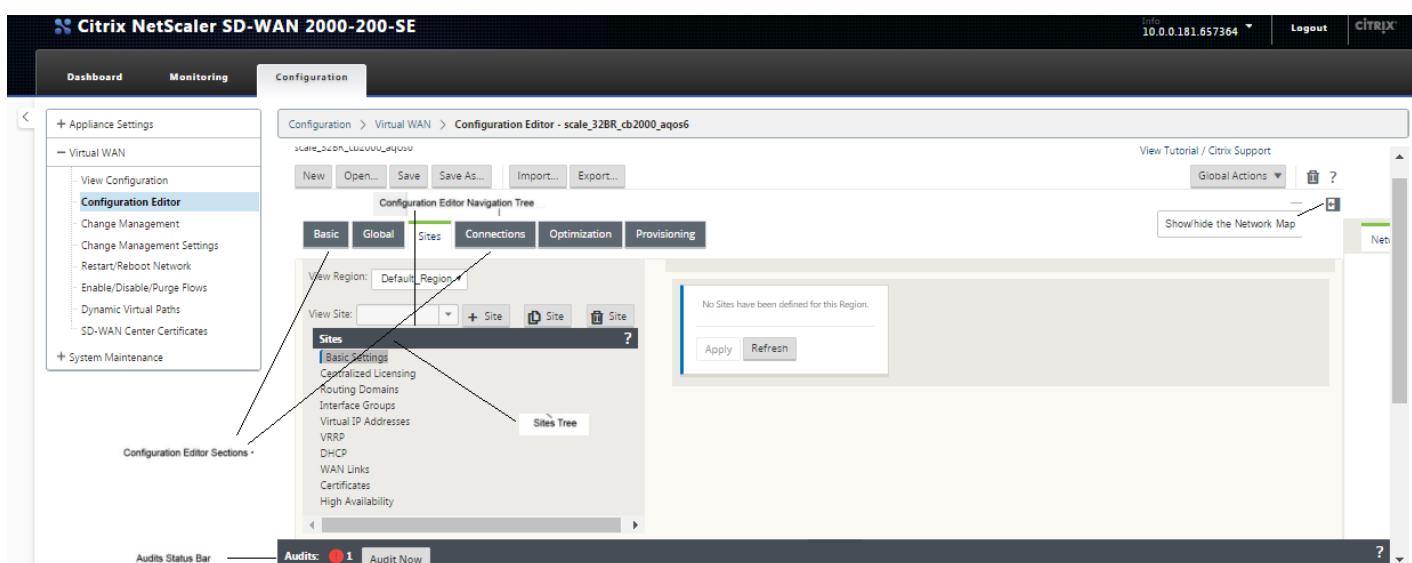
The Configuration Editor enables you to add and configure Virtual WAN Appliance sites, connections, optimization, and provisioning, and to create and define the Virtual WAN Configuration.

The Configuration Editor is available when the Web Management Interface is in the MCN Console mode, only. By default, the web Interface on a new appliance is set to Client mode. You must change the mode setting to MCN Console before you can access the Configuration Editor. For instructions, see the section [Switching the Management Web Interface to MCN Console Mode](#).

To navigate to the **Configuration Editor**, do the following:

1. Log into the Web Management Interface on the MCN appliance.
2. Select the **Configuration** tab.
3. In the navigation tree, click **+** next to the **Virtual WAN** branch in the tree. This displays the available pages for the **Virtual WAN** category.
4. In the Virtual WAN branch of the tree, select **Configuration Editor**.

The below figure outlines the basic navigation and page elements of the **Configuration Editor**, and the terminology used to identify them.



The following describes the primary **Configuration Editor** navigation elements referenced in this guide:

- **Configuration Editor menu bar** – This is located at the top of the page area, just below the breadcrumbs links. The menu bar contains the primary activity buttons for **Configuration Editor** operations. In addition, at the far right edge of the menu bar is the **View Tutorial** link button for initiating the **Configuration Editor** tutorial. The tutorial steps you through a series of bubble descriptions for each element of the **Configuration Editor** display.
- **Configuration Editor sections tree** – This is the stack of dark grey bars located in the left pane of the **Configuration Editor** page area. Each grey bar represents a top-level section. Click a section name to reveal the sub-branches for that section.
- **Sections tree branches** – Click a section name in the sections tree to open a section branch. Each section branch contains one or more sub-branches of configuration categories and forms, which in turn may contain additional child branches and forms.
- **Sites tree** – This lists the site nodes that have been added to the configuration currently opened in the **Configuration Editor**. In the section tree. Click a site name to open the branch for that site. Click the site to close a branch. For detailed instructions on navigating and using the **Sites** tree and configuration forms, see the following sections:
 - [Setting up the Master Control Node \(MCN\) Site.](#)
 - [Adding and Configuring the Branch Sites.](#)
- **Audits status bar** – This is the dark grey bar at the bottom of the **Configuration Editor** page, and spanning the entire width of the Management Web Interface screen. The **Audits** status bar is available only when the **Configuration Editor** is open. An Audit Alert icon (red dot or goldenrod delta) at the far left of the status bar indicates one or more errors present in the currently-opened configuration. Click the status bar to display a complete list of all unresolved Audit Alerts for that configuration.

Change Management Wizards

The **Change Management** wizards guide you through the process of uploading, downloading, staging, and activating the Virtual WAN software and configuration on the Master Control Node (MCN) appliance and client appliances. There are two versions of the **Change Management** wizard, one for Virtual WAN system-wide (“global”) change management, and one for local change management, as follows:

- **MCN (Global) Change Management wizard – The MCN Global Change Management** wizard is the primary (main) version, and is available in the MCN appliance Web Management Interface, only. Use this to generate the Virtual WAN appliance packages to be deployed for each type of Virtual WAN Appliance in your network. You can also use the wizard to automatically propagate configuration changes to appliances already deployed in your Virtual WAN. Basic navigation instructions are provided in the section, “Using the MCN Global Change Management Wizard” below. Instructions for using the MCN global **Change Management** wizard to create the Appliance Packages are provided in the section [Preparing the Virtual WAN Appliance Packages on the MCN.](#)
- **Local Change Management wizard – The Local Change Management** wizard is available in the Web Management Interface running on both the MCN and on all client node appliances. Use this to upload, stage, and activate the appropriate Virtual WAN appliance package on a local appliance to be added to your Virtual WAN. You can also use this wizard to upload an updated Appliance Package specifically to the local MCN, or to an individual, local Virtual WAN Appliance already deployed in your network.

Using the MCN Global Change Management Wizard

To open the MCN Global **Change Management** Wizard, do the following:

1. Log into the Web Management Interface on the MCN appliance.
2. Select the **Configuration** tab. In the navigation tree, click **+** next to the **Virtual WAN** branch in the tree.
3. In the **Virtual WAN** branch, select **Change Management**.

This displays the first page of the **Change Management** wizard, the **Change Process Overview** page, as shown in the below figure.

The screenshot shows the 'Change Management Wizard Page Tabs' interface. The main content area is titled 'Change Process Overview' and contains a three-step process:

- Step 1: Change Preparation** (Upload Files to MCN)
- Step 2: Appliance Staging** (Transfer Files to Clients)
- Step 3: Activation** (Activate Change)

Below the steps, there is a note: 'Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a previously-staged appliance package (if present).' A 'Back' button is located at the bottom right of the main content area.

The bottom section of the page displays 'Global Multi-Region Summary' and 'Region - Default_Region Details'. The 'Region - Default_Region Details' section includes a 'Site-Appliance Table' with the following data:

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-5100-Appliance	CB5100	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
BR572-Appliance	CBVPX	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
BR573-Appliance	CBVPX	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
BR574-Appliance	CBVPX	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
BR575-Appliance	CBVPX	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
RCN1-5100-Appliance	CB5100	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
RCN1-5100-RCN1_HA-Appliance	CB5100	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
RCN3-2100-Appliance	CB2100	Done	10.0.0.178.657275	17:31 on 2/10/18	10.0.0.182.657619	20:10 on 2/12/18	<3 min		active / staged
RCN3Geo-2100-Appliance	CB2100	0%	Not Connected					Loc Chg Mgt	active / staged
RCN4-ESxIL-Appliance	CBVPXL	0%	Not Connected					Loc Chg Mgt	active / staged

5. To start the wizard, click **Begin**.

For complete instructions on using the wizard to upload, stage, and activate the SD-WAN software and configuration on the appliances, see the following sections:

- [Preparing the Virtual WAN Appliance Packages on the MCN](#)
- [Installing the Virtual WAN Appliance Packages on the Clients](#)

The **Change Management** wizard contains the following navigation elements:

- **Page area** – This displays the forms, tables, and activity buttons for each page of the **Change Management** wizard.
- **Change Management wizard page tabs** – The page tabs are located in the left pane of the page area on each page of the wizard. Tabs are listed in the order that the corresponding steps occur in the wizard process. When a tab is active, you can click it to return to a previous page in the wizard. If a tab is active, the name displays in blue font. Grey font indicates an inactive tab. Tabs are inactive until all dependencies (previous steps) have been fulfilled without error.
- **Appliance-Site table** – This is located at the bottom of the wizard page area, on most wizard pages. The table contains information about each configured appliance site, and links for downloading the active or staged Appliance Packages for that appliance model and site. A package in this context is a Zip file bundle containing the appropriate NetScaler SD-WAN software package for that appliance model, and the specified configuration package. The **Configuration Filenames** section above the table shows the package name for the current active and staged packages on the local appliance.
- **Active/Staged download links** – These are located in the **Download Package** field (far right column) of each entry in the **Appliance-Site** table. Click a link in an entry to download the active or staged package for that appliance site.
- **Begin** – Click **Begin** to initiate the **Change Management** wizard process and proceed to the **Change Preparation** tab page.
- **Activate Staged** – If this is not an initial deployment, and you want to activate the currently staged configuration, you have the option of proceeding directly to the **Activation** step. Click **Activate Staged** to proceed directly to the Activation page and initiate activation of the currently staged configuration.

Setting up the Appliance Hardware

Mar 01, 2018

To set up your NetScaler SD-WAN Appliance hardware, do the following:

1. Set up the chassis.

NetScaler SD-WAN Appliances can be installed in a standard rack. For desktop installation, place the chassis on a flat surface. Make sure that there is a minimum of two inches of clearance at the sides and back of the appliance, for proper ventilation.

2. Connect the Power.

- a. Make sure the power switch is set to Off.
- b. Plug the power cord into the appliance and an AC outlet.
- c. Press the power button located on the front of the appliance.

3. Connect the appliance Management Port to a personal computer.

You will need to connect the appliance to a PC in preparation for completing the next procedure, setting the Management IP Address for the appliance.

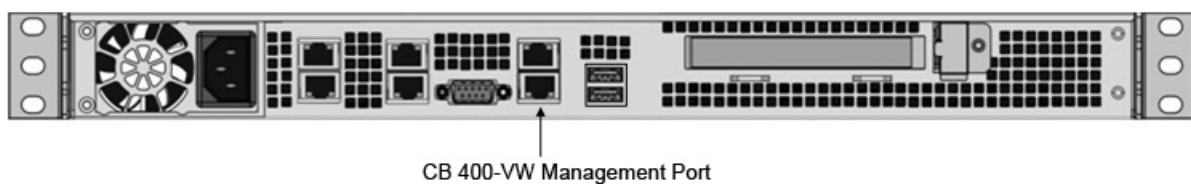
Note

Before you connect the appliance, make sure the Ethernet port is enabled on the PC. Use an Ethernet cable to connect the SD-WAN Appliance Management Port to the default Ethernet port on a personal computer.

NetScaler SD-WAN 400-SE Management Port

The NetScaler SD-WAN 400-SE Management Port is the bottom far right port labeled **MGMT**, on the back of the chassis. The default IP Address for the Management Port is 192.168.100.1.

The below figure shows the location of the NetScaler SD-WAN 400-SE Management Port.



NetScaler SD-WAN 1000-SE Management Port

The NetScaler SD-WAN 1000-SE Management Port is the bottom far right port labeled **MGMT**, on the back of the chassis. The default IP Address for the Management Port is 192.168.100.1.

The below figure shows the location of the NetScaler SD-WAN 1000-SE Management Port.



CB 1000-VW Management Port

NetScaler SD-WAN 2000-SE Management Port

The NetScaler SD-WAN 2000-SE Management Port is the bottom-left port labeled 0/1, on the front of the chassis. The default IP Address for the Management Port is 192.168.100.1.

The following figure shows the location of the NetScaler SD-WAN 2000-SE Management Port.



CB 2000-VW Management Port

NetScaler SD-WAN 4000-SE Management Port

The NetScaler SD-WAN 4000-SE Management Port is the bottom-left port labeled 0/1, on the front of the chassis. The default IP Address for the Management Port is 192.168.100.1.

The below figure shows the location of the NetScaler SD-WAN 4000-SE Management Port.



CB 4000-VW Management Port

NetScaler SD-WAN 5100-SE Management Port

The NetScaler SD-WAN 5100-SE Management Port is the bottom-left port labeled 0/1, on the front of the chassis. The default IP Address for the Management Port is 192.168.100.1.

The below figure shows the location of the NetScaler SD-WAN 5100-SE Management Port.



NetScaler SD-WAN VPX-SE Management Port

The NetScaler SD-WAN VPX-SE Virtual Appliance is a Virtual Machine, so there is no physical Management Port. However, if you did not configure the Management IP Address for the SD-WAN VPX-SE when you created the VPX Virtual Machine, you will need to do so now, as outlined in the section, [Configuring the Management IP Address for the SD-WAN VPX-SE](#).

Configure Management IP Address

Mar 01, 2018

To enable remote access to a NetScaler SD-WAN appliance, you must specify a unique Management IP Address for the appliance. To do so, you must first connect the appliance to a personal computer. You can then open a browser on the PC and connect directly to the Management Web Interface on the appliance, where you can set the Management IP Address for that appliance. The Management IP Address must be unique for each appliance.

The procedures are different for setting the Management IP Address for a hardware SD-WAN Appliance and a VPX Virtual Appliance (NetScaler SD-WAN VPX-SE). For instructions for configuring the address for each type of appliance, see the following:

- **SD-WAN VPX Virtual Appliance** – See the sections, [Configuring the Management IP Address for the SD-WAN VPX-SE](#) and [Differences Between a SD-WAN VPX-SE and SD-WAN WANOP VPX Installation](#).

To configure the Management IP Address for a hardware SD-WAN Appliance, do the following:

Note

You must repeat the following process for each hardware appliance you want to add to your network.

1. If you are configuring a hardware SD-WAN appliance, physically connect the appliance to a PC.

If you have not already done so, connect one end of an Ethernet cable to the Management Port on the appliance, and the other end to the default Ethernet port on the PC.

Note

Ensure that the Ethernet port is enabled on the PC you are using to connect to the appliance.

2. Record the current Ethernet port settings for the PC you will be using to set the appliance Management IP Address.

You will need to change the Ethernet port settings on the PC before you can set the appliance Management IP Address. Be sure to record the original settings so you can restore them after configuring the Management IP Address.

3. Change the IP Address for the PC.

On the PC, open your network interface settings and change the IP Address for your PC to the following:

192.168.100.50

4. Change the Subnet Mask setting on your PC to the following:

255.255.0.0

5. On the PC, open a browser and enter the default IP Address for the appliance. Enter the following IP Address in the address line of the browser:

192.168.100.1

Note

It is recommended that you use Google Chrome browser when connecting to a SD-WAN appliance.

Ignore any browser certificate warnings for the Management Web Interface.

This opens the SD-WAN management web interface login screen on the connected appliance, as shown in the below figure.

6. Enter the administrator user name and password, and click **Login**.

- Default administrator user name: *admin*
- Default administrator password: *password*

Note

It is strongly recommended that you change the default password. Be sure to record the password in a secure location, as password recovery might require a configuration reset.

After you have logged into the management web interface, the **Dashboard** page displays, as shown below.

The first time you log into the management web interface on an appliance, the **Dashboard** displays an Alert icon (goldenrod delta) and alert message indicating that the SD-WAN Service is disabled, and the license has not been installed. For now, you can ignore this alert. The alert will be resolved after you have installed the license, and completed the configuration and deployment process for the appliance.

Below figure shows a sample **Dashboard** after the SD-WAN has been fully configured and deployed.

7. In the main menu bar, select the **Configuration** section tab.

This displays the **Configuration** navigation tree in the left pane of the screen. The **Configuration** navigation tree contains the following three primary branches:

- **Appliance Settings**
- **Virtual WAN**
- **System Maintenance**

When you select the **Configuration** tab, the **Appliance Settings** branch automatically opens, with the **Administrator Interface** page preselected by default, as shown in the below figure.

8. In the **Appliance Settings** branch of the navigation tree, select **Network Adaptors**.

This displays the **Network Adaptors** settings page with the **IP Address** tab preselected by default, as shown in the below figure.

9. In the **IP Address** tab page, enter the following information for the SD-WAN appliance you want to configure.

- IP Address

- Subnet Mask
- Gateway IP Address

Note

The management IP address must be unique for each appliance.

10. Click **Change Settings**.

A confirmation dialog box displays, prompting you to verify that you want to change these settings.

11. Click **OK**.

12. Change the network interface settings on your PC back to the original settings.

Note

Changing the IP address for your PC automatically closes the connection to the appliance, and terminates your login session on the management web interface.

13. Disconnect the appliance from the PC and connect the appliance to your network router or switch. Disconnect the Ethernet cable from the PC, but do not disconnect it from your appliance. Connect the free end of the cable to your network router or switch.

The SD-WAN appliance is now connected to and available on your network.

14. Test the connection. On a PC connected to your network, open a browser and enter the Management IP Address you just configured for the appliance.

If the connection is successful, this displays the **Login** screen for the SD-WAN management web interface on the appliance you just configured.

Tip

After verifying the connection, do not log out of the management web interface. You will be using it to complete the remaining tasks outlined in the subsequent sections.

You have now set the management IP address of your SD-WAN appliance, and can connect to the appliance from any location in your network.

Set Date and Time

Mar 01, 2018

Before installing the SD-WAN software license on an appliance, you must set the date and time on the appliance.

Note

You must repeat this process for each appliance you want to add to your network.

To set the date and time, do the following:

1. Log into the Management Web Interface on the appliance you are configuring.
2. In the main menu bar, select the **Configuration tab**.
This displays the **Configuration** navigation tree in the left pane of the screen.
3. Open the **System Maintenance branch in the navigation tree**.
4. Under the **System Maintenance branch, select Date/Time Settings**.

This displays the Date/Time Settings page, as shown below.

The screenshot displays the Management Web Interface with the Configuration tab selected. The left navigation pane shows the System Maintenance branch expanded, with Date/Time Settings highlighted. The main content area shows the Date/Time Settings page with the following sections:

- NTP Settings:** Use NTP Server (checked), Server Address: time.nist.gov, Change Settings button.
- Date/Time Settings:** Date: April 11, 2016; Time: 09:30:57, Change Date button.
- Timezone Settings:** Note: After changing the timezone setting, a reboot will also be necessary... Time Zone: UTC, Change Timezone button.

5. Select the time zone from the **Time Zone** field drop-down menu at the bottom of the page.

Note

If you need to change the time zone setting, you must do this before setting the date and time, or your settings will not persist as entered.

6. Click **Change Timezone**.

This updates the time zone and recalculates the current date and time setting, accordingly. If you set the correct date and time before this step, then your settings will no longer be correct.

When the time zone update completes, a success Alert icon (green check mark) and status message displays in the top section of the page.

7. (Optional) Enable NTP Server service.

- a) Select **Use NTP Server**.
- b) Enter the server address in the **Server Address** field.
- c) Click **Change Settings**.

A success Alert icon (green checkmark) and status message displays when the update completes.

8. Select the month, day, and year from the **Date** field drop-down menus.

9. Select the hour, minutes, and seconds from the **Time** field drop-down menus.

10. Click **Change Date**.

Note

This updates the date and time setting, but does not display a success Alert icon or status message.

The next step is to set the console session **Timeout** threshold to the maximum value. This step is optional, but strongly recommended. This prevents the session from terminating prematurely while you are working on the configuration, which could result in a loss of work. Instructions for setting the console session **Timeout** value are provided in the following section. If you do not want to reset the timeout threshold, you can proceed directly to the section, [Uploading and Installing the SD-WAN Software License File](#).

Warning

If your console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning.

Session Timeout

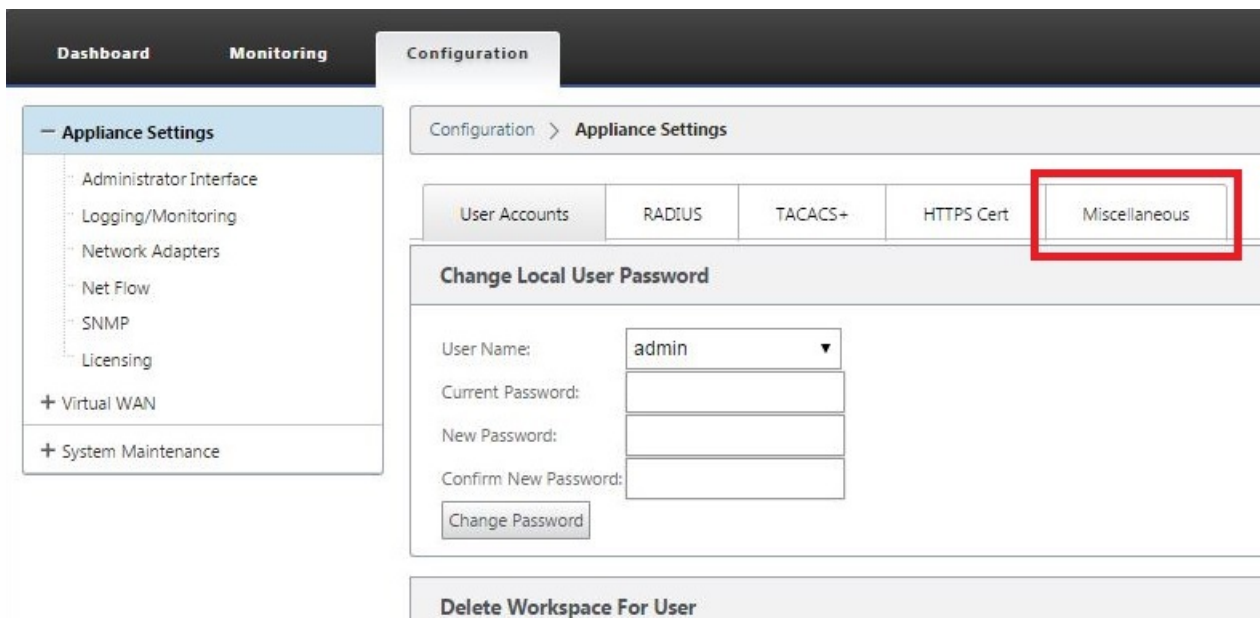
Mar 01, 2018

If your console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is strongly recommended that you set the console session **Timeout** interval to a high value when creating or modifying a configuration package, or performing other complex tasks. The default is 60 minutes; the maximum is 9999 minutes. For security reasons, you should then reset it to a lower threshold after completing those tasks.

To reset the console session **Timeout** interval, do the following:

1. Select the **Configuration** tab, and then select the **Appliance Settings** branch in the navigation tree.

This displays the **Appliance Settings** page, with the **User Accounts** tab preselected by default.



2. Select the **Miscellaneous** tab (far right corner).

This displays the **Miscellaneous** tab page.

Configuration > **Appliance Settings**

User Accounts RADIUS TACACS+ HTTPS Cert Miscellaneous

Change Web Console Timeout

Timeout: Enter the new timeout value in minutes (1-9999).

Switch to Client Console

Switch the mode of the Web Console to enable configuration of Client functionality.

3. Enter the console **Timeout** value.

In the **Timeout** field of the **Change Web Console Timeout** section, enter a higher value (in minutes) up to the maximum value of 9999. The default is 60, which is usually much too brief for an initial configuration session.

Note


For security reasons, be sure to reset this value to a lower interval after completing the configuration and deployment.

4. Click **Change Timeout**.

This resets the session **Timeout** interval, and displays a success message when the operation completes.

Configuration > **Appliance Settings**

Timeout Change Success

 Your timeout has been changed.

You will be automatically logged out in seconds.

After a brief interval (a few seconds), the session is terminated and you are automatically logged out of the Management Web Interface. The Login page page appears.



5. Enter the Administrator user name (*admin*) and password (*password*), and click **Login**.

The next step is to upload and install the SD-WAN software license file on the appliance.

Configure Alarms

Mar 01, 2018

You can now configure your SD-WAN appliance to identify alarm conditions based on your network and priorities, generate alerts, and receive notifications via email, syslog or SNMP trap.

An alarm is a configured alert consisting of an event type, a trigger state, a clear state, and a severity.

To configure alarm settings

1. In the SD-WAN web management interface, navigate to **Configuration > Appliance Settings > Logging/Monitoring** and click **Alarm Options**.
2. Click **Add Alarm** to add a new alarm.

The screenshot shows the SD-WAN web management interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar shows 'Appliance Settings' with sub-items: 'Administrator Interface', 'Logging/Monitoring' (selected), 'Network Adapters', 'Net Flow', 'SNMP', 'Licensing', '+ Virtual WAN', and '+ System Maintenance'. The main content area shows the breadcrumb trail 'Configuration > Appliance Settings > Logging/Monitoring' and tabs for 'Log Options', 'Alert Options', 'Alarm Options', and 'Syslog Server'. The 'Alarm Configuration' section has an 'Add Alarm' button and a table of configured alarms.

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"/>

An 'Apply Settings' button is located below the table.

3. Select or enter values for the following fields:

- **Event Type:** The SD-WAN appliance can trigger alarms for particular subsystems or objects in the network, these are called event types. The available event types are SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL, and IPSEC_TUNNEL.
- **Trigger State:** The event state that triggers an alarm for an Event Type. The available Trigger State options depend on the chosen event type.
- **Trigger Duration:** The duration in seconds, this determines how quickly the appliance triggers an alarm. Enter '0' to receive immediate alerts or enter a value between 15-7200 seconds. Alarms are not triggered, if additional events occur on the same object within the Trigger Duration period. Additional alarms are triggered only if an event persists longer than the Trigger Duration period.
- **Clear State:** The event state that clears an alarm for an Event Type after the alarm is triggered. The available Clear State options depend on the chosen Trigger State.
- **Clear Duration:** The duration in seconds, this determines how long to wait before clearing an alarm. Enter '0' to immediately clear the alarm or enter a value between 15-7200 seconds. The alarm is not cleared, if another clear state event occurs on the same object within the specified time.
- **Severity:** A user-defined field that determines how urgent an alarm is. The severity is displayed in the alerts sent when the alarm is triggered or cleared and in the triggered alarm summary.
- **Email:** Alarm trigger and clear alerts for the Event Type is sent via email.

- **Syslog:** Alarm trigger and clear alerts for the Event Type is sent via Syslog.
- **SNMP:** Alarm trigger and clear alerts for the Event Type is sent via SNMP trap.

4. Continue adding alarms as required.

5. Click **Apply Settings**.

Viewing Triggered Alarms

To view a summary of all the triggered alarms:

In the SD-WAN web management interface, navigate to **Configuration > System Maintenance > Diagnostics > Alarms**.

A list of all the triggered alarms is displayed.

The screenshot displays the 'Alarms' configuration page in the SD-WAN web management interface. On the left is a 'System Maintenance' menu with options like 'Delete Files', 'Restart System', 'Date/Time Settings', 'Local Change Management', 'Diagnostics', 'Update Software', and 'Configuration Reset'. The top navigation bar includes tabs for 'Ping', 'Traceroute', 'Packet Capture', 'Path Bandwidth', 'System Info', 'Diagnostic Data', 'Events', 'Alarms', and 'Diagnostics Tool'. The 'Alarms' section features a 'Triggered Alarms Summary' table. Above the table, there are controls for 'Enable Auto Refresh' (checkbox), 'Time Interval' (set to 5 seconds), and 'Refresh' button. There are also buttons for 'Clear Checked Alarms' and 'Clear All Alarms'. The table has a filter and 'Apply' button, and a 'Show 100 entries' dropdown. The table columns are: Severity, Event Type, Object Name, Trigger State, Trigger Duration (sec), Clear State, Clear Duration (sec), and Clear Action. The table contains 11 rows of data, with the first 10 rows showing various path and virtual path alarms, and the 11th row showing a 'WAN_LINK' alarm. All alarms have a 'DEAD' trigger state and a 'GOOD' clear state.

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 Triggered Alarms

To manually clear triggered alarms:

1. In the SD-WAN web management interface, navigate to **Configuration > System Maintenance > Diagnostics > Alarms**.
2. In the **Clear Action** column, select the alarms that you want to clear.
3. Click **Clear Checked Alarms**. Alternately, Click **Clear All Alarms** to clear all the alarms.

Configure Rollback

Mar 01, 2018

The Configuration Rollback feature allows the Change Management system to detect and recover from certain software / configuration errors by reverting to the previously active software/configuration. Not all failure modes will result in a rollback. This feature can detect network outage and appliance crash.

The configuration rollback feature is enabled by default, to disable this feature uncheck **Revert on Error** option in the **Activation** tab of the Change Management wizard.

Configuration > Virtual WAN > Change Management

Overview
Change Preparation
Appliance Staging
Activation

Activate

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

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

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

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

Activate Staged In: 10 seconds

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

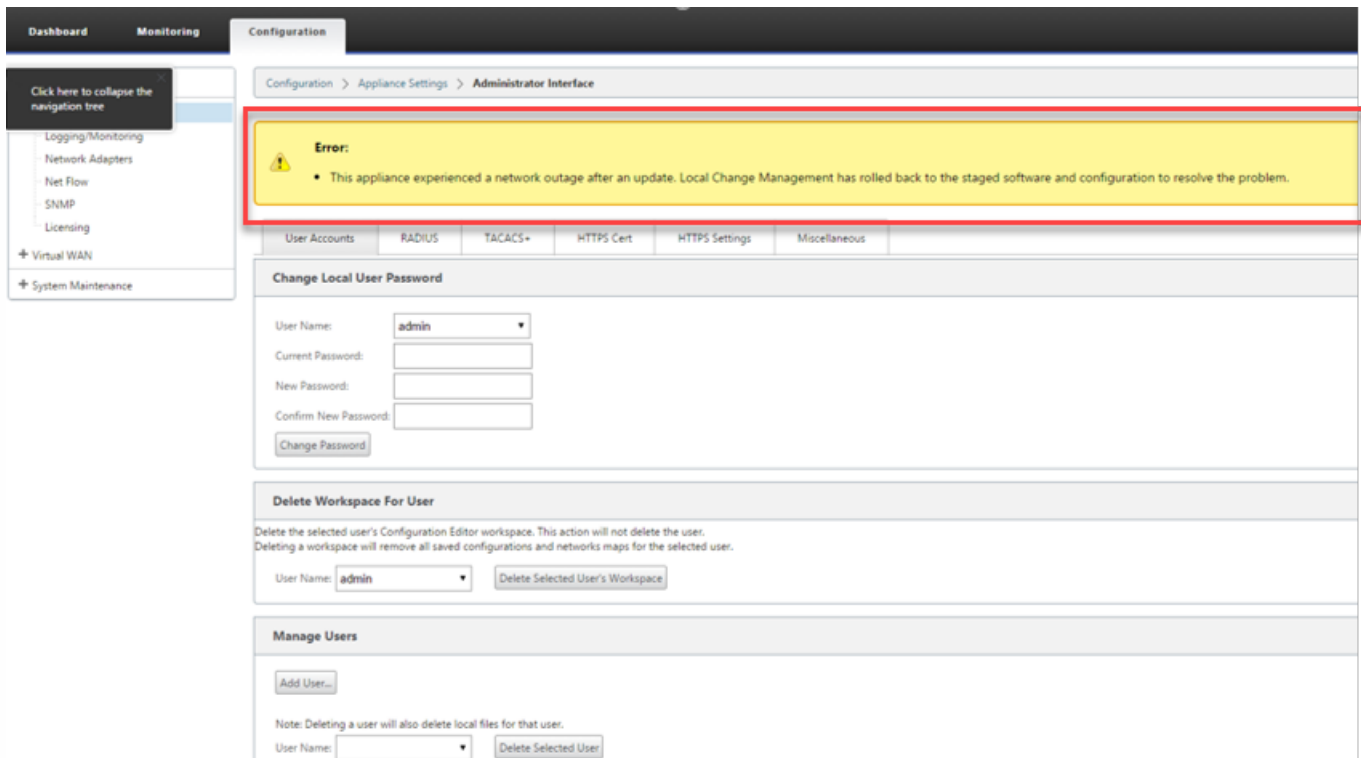
Note: For software upgrade, please follow the instructions in release documentation.

Activate Staged Abort **Revert on Error** Done

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

If a system / configuration error occurs on a client while activating staged package from an MCN the client will revert to the previous software / configuration and an error message appears as shown in the screenshot below.

The client generates a critical severity event for the SOFTWARE_UPDATE object if an appliance crash is detected, or generates a critical severity event for the CONFIG_UPDATE object if a network outage is detected.



If **Revert on Error** is enabled, the client appliances will monitor itself for about 10 minutes. If the software crashes within 10 minutes, or if the network is down (unable to establish a Virtual Path to the MCN) for 10 minutes, then a rollback is triggered.

On the MCN, an error message appears as shown in the screen shot below. As the clients rejoin the network, it reports the type of error encountered. A summary count of the number of errors is displayed in the error message.

Configuration > Virtual WAN > Change Management

Error:

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

- **Software Errors : 1**
- **Configuration Errors : 1**

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

Overview

Change Process Overview

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

Step 1

Change Preparation

Upload Files to MCN

MCN

Step 2

Appliance Staging

Transfer Files to Clients

MCN → Clients

Step 3

Activation

Activate Change

MCN → Clients

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

Activate Staged **Begin --**

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

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Dallas_MCN-Appliance	CBVPX	Software Error	9.3.0.952.99598118	4:37 on 6/12/17	9.3.0.952.99598118	10:56 on 6/12/17	0 sec		active / staged
Dallas_MCN-Dallas_HA_secondary	CBVPX		9.3.0.952.99598118	4:37 on 6/12/17	9.3.0.952.99598118	10:56 on 6/12/17	0 sec	0 ms	active / staged
Bangalore-Bangalore-CBVPX	CBVPX		9.3.0.952.99598118	4:37 on 6/12/17	9.3.0.952.99598118	10:56 on 6/12/17	0 sec	0 ms	active / staged
Bangalore-BLR_HA_secondary	CBVPX		9.3.0.952.99598118	4:37 on 6/12/17	9.3.0.952.99598118	10:56 on 6/12/17	0 sec	0 ms	active / staged
Beijing-Appliance	CBVPX		9.3.0.952.99598118	4:37 on 6/12/17	9.3.0.952.99598118	10:56 on 6/12/17	0 sec	0 ms	active / staged
SanJose-Appliance	CB2000	Configuration Error	9.3.0.952.99598118	4:37 on 6/12/17	9.3.0.952.99598118	10:56 on 6/12/17	0 sec	63 ms	active / staged

In the **Change Management** window of the MCN, you can see the state of the site appliances indicating if that site had encountered a Software Error, or a Configuration Error.

Setup Master Control Node (MCN)

Mar 01, 2018

The SD-WAN Master Control Node is the head end appliance in the Virtual WAN. Typically, this is a 4000-VW or 5100-VW Virtual WAN appliance deployed at the Enterprise data center. The MCN serves as the distribution point for the initial system configuration and any subsequent configuration changes. In addition, you conduct most upgrade procedures through the Management Web Interface on the MCN. There can be only one active MCN in a Virtual WAN.

By default, appliances have the pre-assigned role of client. To establish an appliance as the MCN, you must first add and configure the MCN site, and then stage and activate the configuration and appropriate software package on the designated MCN appliance.

Supplemental MCN Site Deployment Information

The following Knowledge Base support articles are recommended:

- Virtual WAN PBR Mode Deployment Steps ([CTX201577](http://support.citrix.com/article/CTX201577))
<http://support.citrix.com/article/CTX201577>
- Virtual WAN Gateway Mode Deployment Steps ([CTX201576](http://support.citrix.com/article/CTX201576))
<http://support.citrix.com/article/CTX201576>

Overview of MCN Site Configuration Procedures

The steps for adding and configuring the MCN site are as follows:

1. Switch the Management Web Interface to **MCN Console** mode.
2. Add the MCN site.
3. Configure the Virtual Interface Groups for the MCN site.
4. Configure the Virtual IP Addresses for the MCN site.
5. (Optional) Configure the LAN GRE Tunnels for the site.
6. Configure the WAN links for the MCN site.
7. Configure the Access Interfaces for the MCN site.
8. Configure the routes for the MCN site.
9. (Optional) Configure High Availability for the MCN site.
10. (Optional) Configure Virtual WAN security and encryption.
11. Name and save the MCN site configuration.

Instructions for each of these tasks are provided in the following sections.

MCN Overview

Mar 01, 2018

The Master Control Node (MCN) is the central Virtual WAN Appliance that acts as the master controller of the Virtual WAN, and the central administration point for the client nodes. All configuration activities, as well as preparation of the Appliance Packages and their distribution to the clients, are performed on the MCN. In addition, certain Virtual WAN monitoring information is available only on the MCN. The MCN can monitor the entire Virtual WAN, whereas client nodes can monitor only their local Intranets, along with some information for those clients with which they are connected.

The primary purpose of the MCN is to establish and utilize Virtual Paths with one or more client nodes located across the Virtual WAN, for Enterprise Site-to-Site communications. An MCN can administer and have Virtual Paths to multiple client nodes. There can be more than one MCN, but only one can be active at any given time.

The below figure illustrates the basic roles and context of the MCN (data center) and client (branch node) appliances for a Virtual WAN Edition deployment.



Switch to MCN Console

Mar 01, 2018

To add and configure the MCN site, you must first log into the Management Web Interface on the appliance you are promoting to the MCN role, and switch the Management Web Interface to **MCN Console** mode. **MCN Console** mode enables access to the Configuration Editor in the Management Web Interface to which you are currently connected. You can then use the **Configuration Editor** to add and configure the MCN site.

Note

Switching to **MCN Console** mode changes the operating mode of the Management Web Interface mode only, and not the active role of the appliance itself. To promote an appliance to the role of MCN, you must first add and configure the MCN site and activate the configuration and software package on the designated MCN appliance.

To switch the Management Web Interface to **MCN Console** mode, do the following:

1. Log into the Management Web Interface on the appliance you want to configure as the MCN.
2. Click **Configuration** in the main menu bar of the Management Web Interface main screen (blue bar at the top of the page).
3. In the navigation tree (left pane), open the **Appliance Settings** branch and click **Administrator Interface**.

This displays the Administrator Interface page in the middle pane.

4. Select the **Miscellaneous** tab.

This displays the Miscellaneous administrative settings page.

The screenshot shows the Management Web Interface Configuration page. The top navigation bar includes Dashboard, Monitoring, and Configuration. The left navigation pane shows Appliance Settings expanded, with Administrator Interface selected. The main content area shows the Configuration > Appliance Settings page. The Miscellaneous tab is selected, and the 'Switch to MCN Console' section is highlighted with a red box. This section contains the text 'Switch the mode of the Web Console to enable configuration of MCN functionality.' and a 'Switch Console' button.

At the bottom of the **Miscellaneous** tab page is the **Switch to [Client | MCN] Console** section. This section contains the **Switch Console** button for toggling between appliance console modes.

The section heading indicates the current console mode, as follows:

- When in **Client Console** mode (default), the section heading is **Switch to MCN Console**.
- When in **MCN Console** mode, the section heading is **Switch to Client Console**.

By default, a new appliance is set to **Client Console** mode.

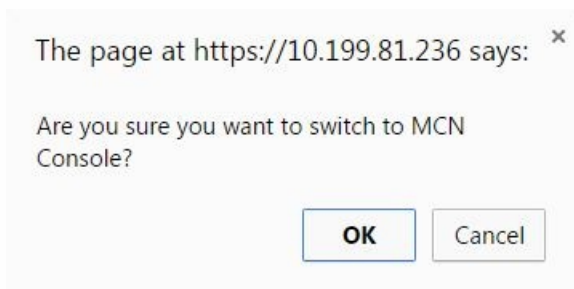
MCN Console mode enables the **Configuration Editor** branch in the navigation tree. The **Configuration Editor** is available on the MCN appliance, only.

Note

Before proceeding to the next step, make sure that the appliance is still set to the default (**Client Console** mode). The section heading should be: **Switch to MCN Console**.

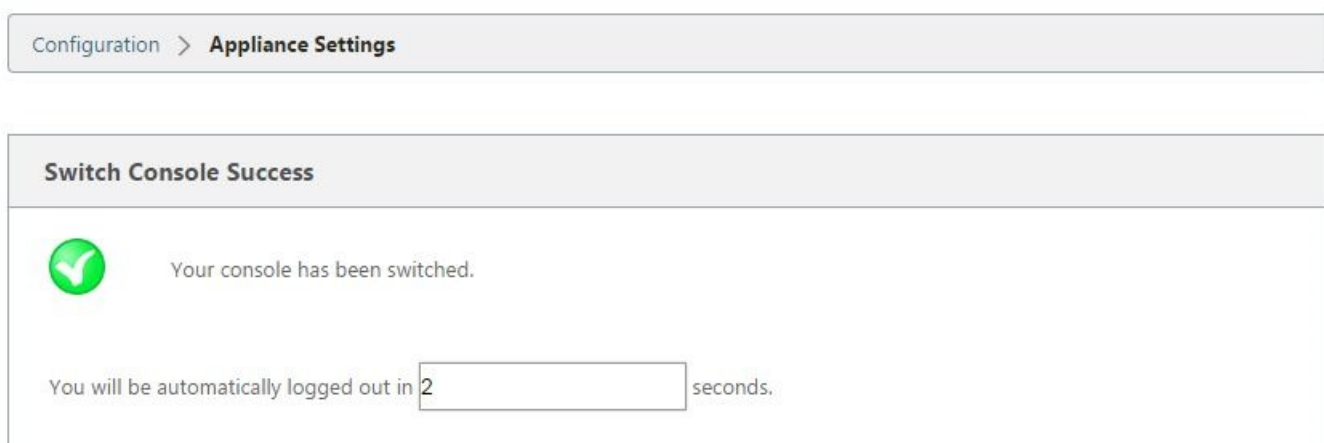
5. Click **Switch Mode** to set the appliance mode to **MCN Console** mode.

This displays a dialog box prompting you to confirm that you want to switch to MCN mode.

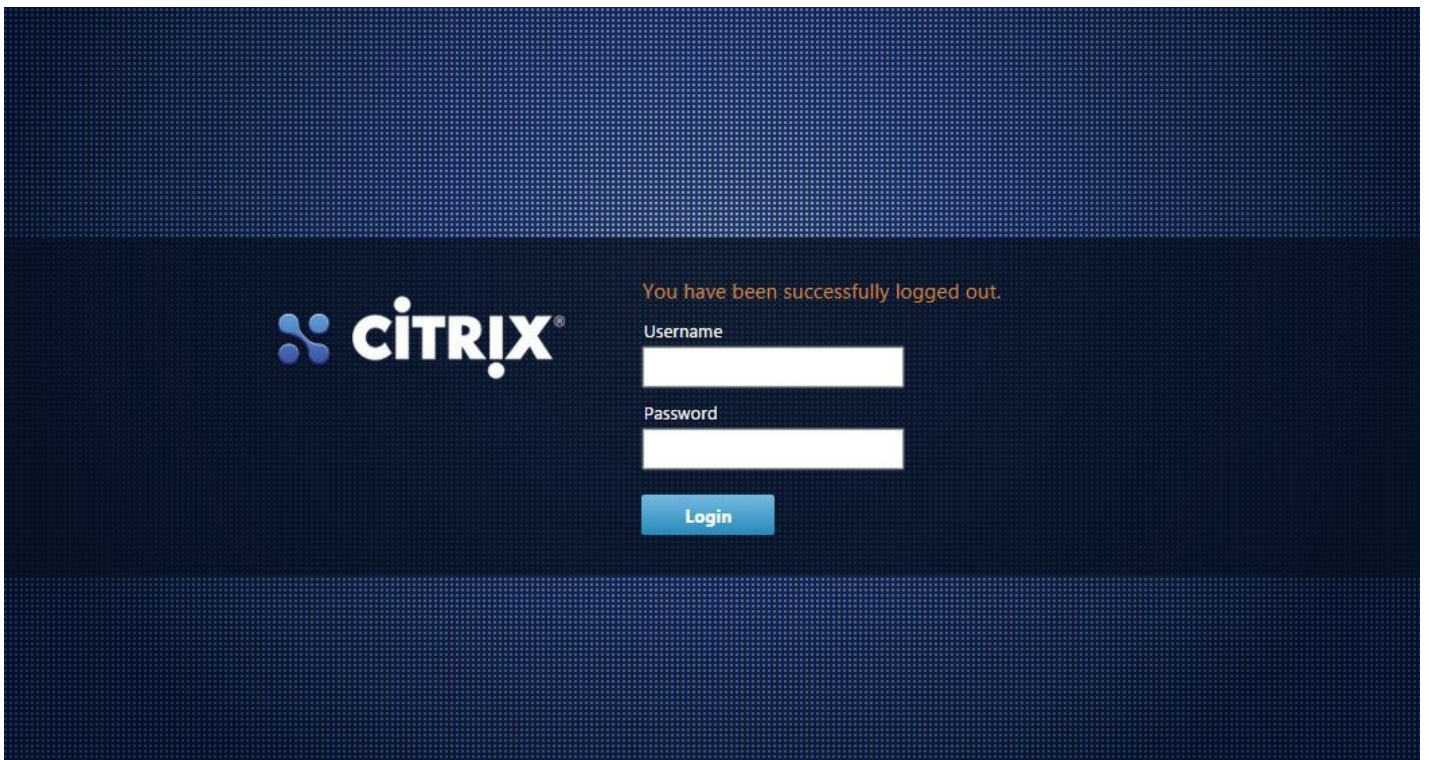


6. Click **OK**.

This switches the console mode to **MCN Console** mode, and terminates the current session. A success message displays, along with a countdown status indicating the number of seconds remaining before the session terminates.



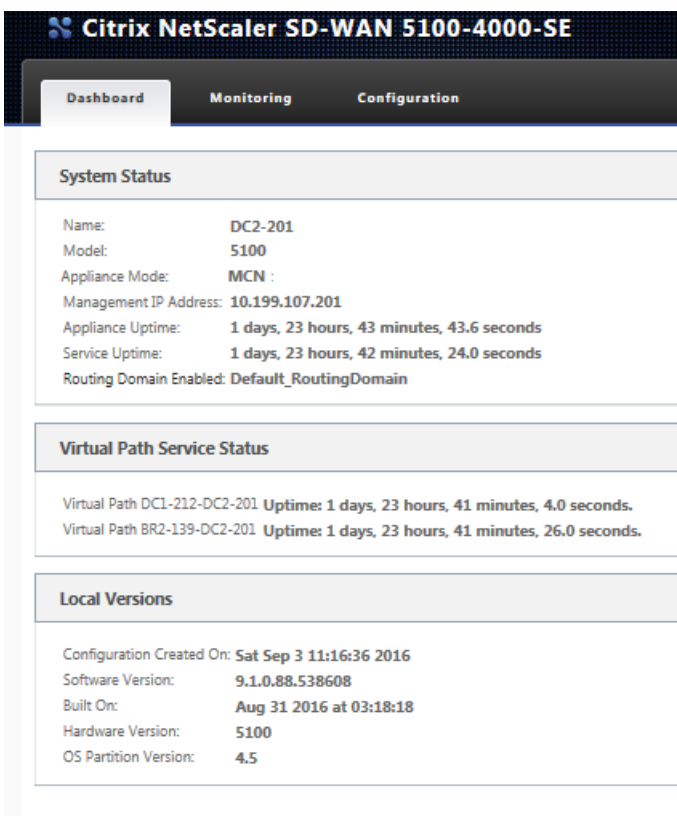
After the countdown completes, the session is terminated and the login page appears.



7. Enter the Administrator user name and password, and click **Login**.

- Default Administrator user name: *admin*
- Default Administrator password: *password*

After logging in, the **Dashboard** displays, now indicating that the appliance is in MCN mode.



The next step is to open a new configuration and add the MCN site to the Sites table, and begin configuring the new MCN site.

Configure MCN

Jun 07, 2018

The first step is to open a new configuration package, and add the MCN site to the new configuration.

Note

It is strongly recommended that you save the configuration package often, or at key points in the configuration. Instructions are provided in the section [Naming, Saving, and Backing Up the MCN Site Configuration](#).

Warning

If the console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is strongly recommended that you set the console session Timeout interval to a high value when creating or modifying a configuration package, or performing other complex tasks. The default is 60 minutes; the maximum is 9999 minutes. For security reasons, you should then reset it to a lower threshold after completing those tasks. For instructions, see the section [Setting the Console Session Timeout Interval \(Optional\)](#).

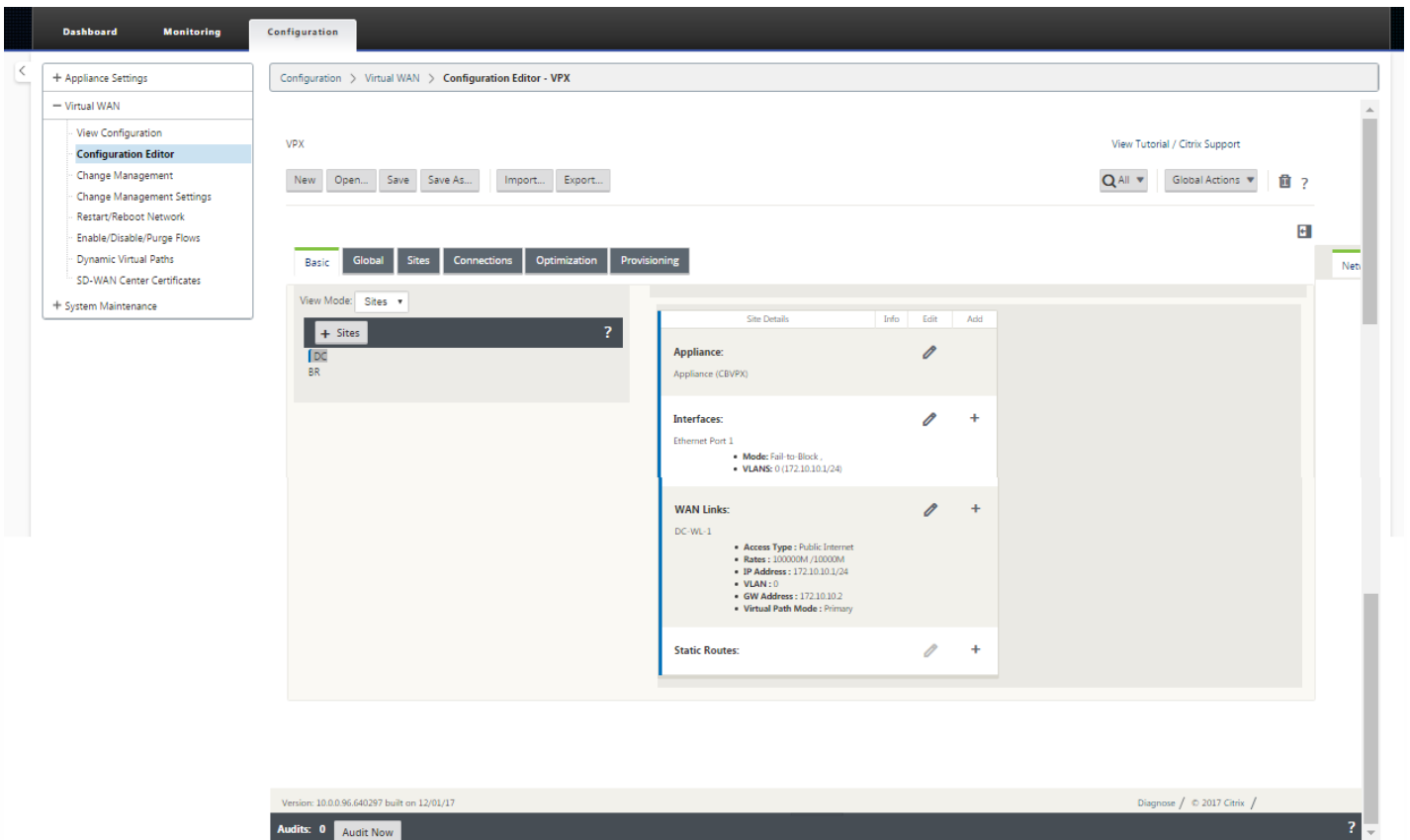
To add and begin configuring the MCN appliance site, do the following:

1. In the navigation tree, navigate to **Virtual WAN > Configuration Editor**.

Note

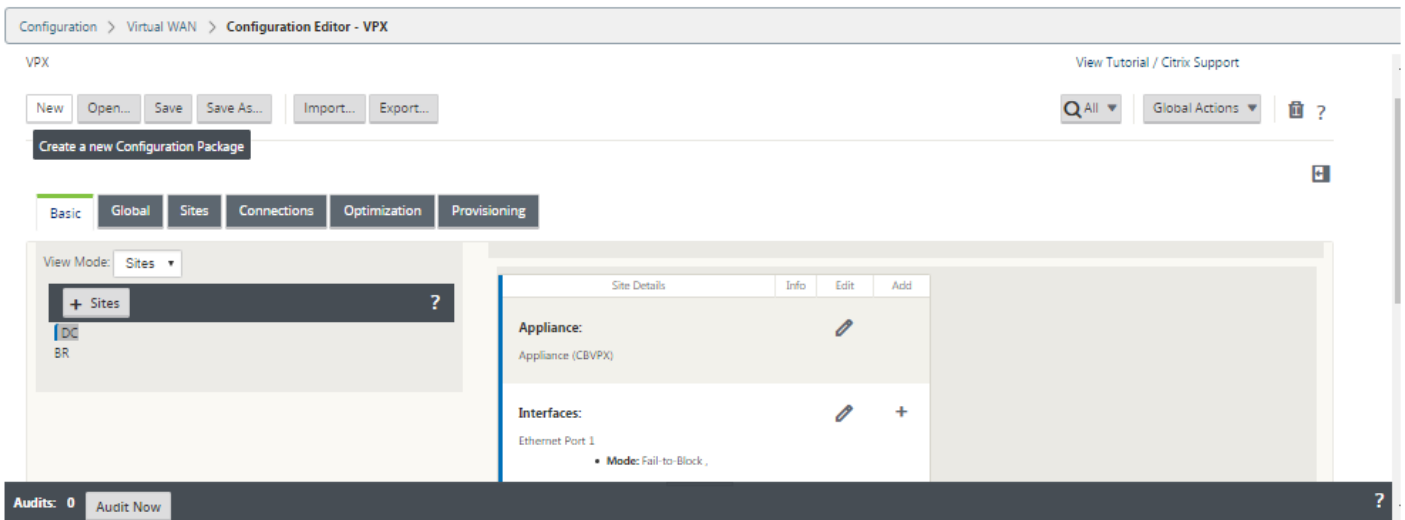
The **Configuration Editor** is available in **MCN Console** mode, only. If the **Configuration Editor** option is not available in the Virtual WAN branch of the navigation tree, please see section, [Switching the Management Web Interface to MCN Console Mode](#), for instructions on changing the console mode.

This displays the **Configuration Editor** main page (middle pane).



2. Click **New** to start defining a new configuration.

This displays the **New** configuration settings page.



3. Click **+ Sites** in the **Sites** bar to begin adding and configuring the MCN site.

This displays the **Add Site** dialog box.

Add [X]

Site Name: *

Site Location:

Secure Key:

Model:

Mode:

- client
- primary MCN
- secondary MCN
- primary RCN
- secondary RCN

Add Cancel

4. Enter the site information.

Do the following:

- Enter the **Site Name** and **Secure Key**.
- Select the appliance **Model**.
- Select the **Mode**. Select **primary MCN** as the mode.

Note

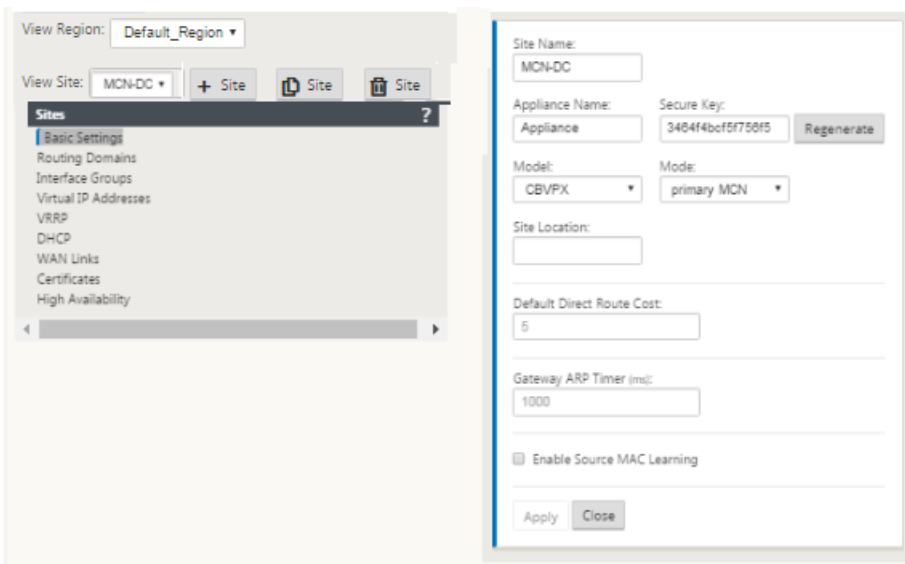
The Model options menu lists the generic model names for the supported appliance models. The generic names do not include the -Standard Edition model suffix, but do correspond to the equivalent SD-WAN Appliance models. Select the corresponding model number for this SD-WAN Appliance model. (For example, select 4000 if this is a SD-WAN4000-SE appliance.)

Note

Entries cannot contain spaces and must be in Linux format

5. Click **Add** to add the site.

This adds the new site to the **Sites** tree, and displays the **Basic Settings** configuration form for the new site.



Note

After you click **Apply**, audit warnings appear indicating that further action is required. A red dot or goldenrod delta icon indicates an error in the section where it appears. You can use these warnings to identify errors or missing configuration information. Roll your cursor over an audit warning icon to display a short description of the error(s) in that section. You can also click the dark grey **Audits** status bar (bottom of page) to display a complete list of all unresolved audit warnings.

6. Enter the basic settings for the new site, or accept the defaults.
7. (Optional, strongly recommended) Save the configuration-in-progress.

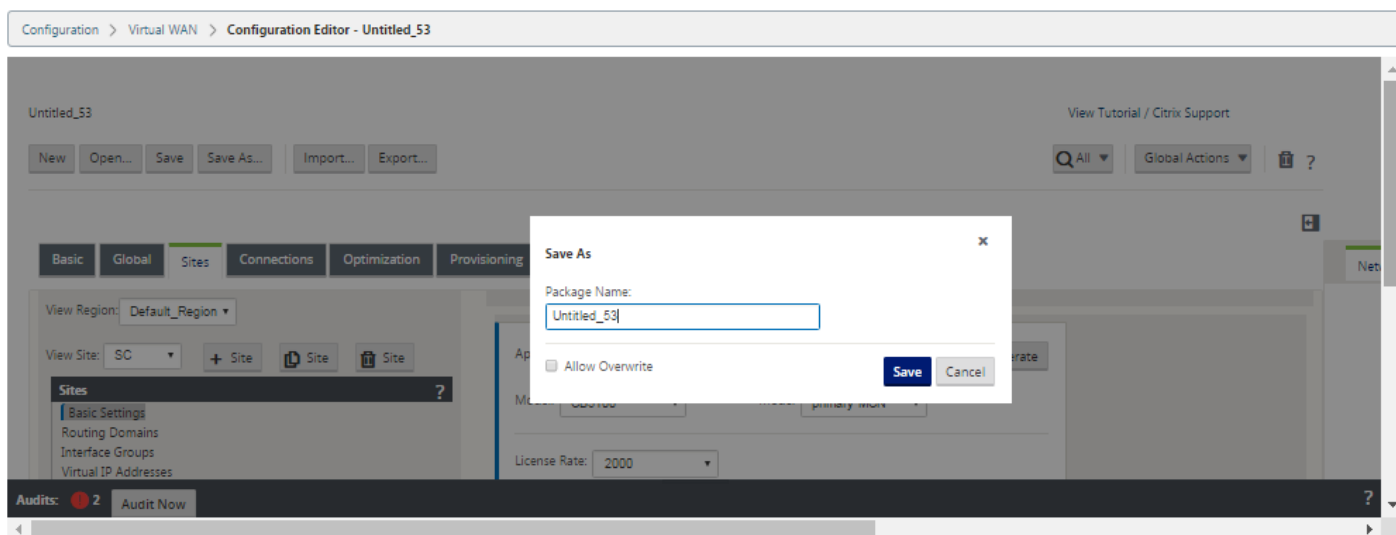
If you cannot complete the configuration in one session, you can save it at any time, so you can return to complete it later. The configuration is saved to your workspace on the local appliance. To resume working in a saved configuration, click **Open** in the **Configuration Editor** menu bar (top of page area). This displays a dialog box for selecting the configuration you want to modify.

Note

As an extra precaution, it is recommended that you use **Save As**, rather than **Save**, to avoid overwriting the wrong configuration package.

To save the current configuration package, do the following:

1. Click **Save As** (at the top of the **Configuration Editor** middle pane). This opens the **Save As** dialog box.



2. Enter the configuration package name.

Note

If you are saving the configuration to an existing package, be sure to select **Allow Overwrite** before saving.

3. Click **Save**.

How to Configure Interface Groups for the MCN

After adding the new MCN site, the next step is to create and configure the Virtual Interface Groups for the site.

The following are some guidelines for configuring Virtual Interface groups:

- Use logical names that will best describe the group.
- Trusted networks are networks that are protected behind a Firewall.
- Virtual Interfaces associate interfaces to Fail to Wire (FTW) pairs.
- Single WAN interfaces cannot be in an FTW pair.

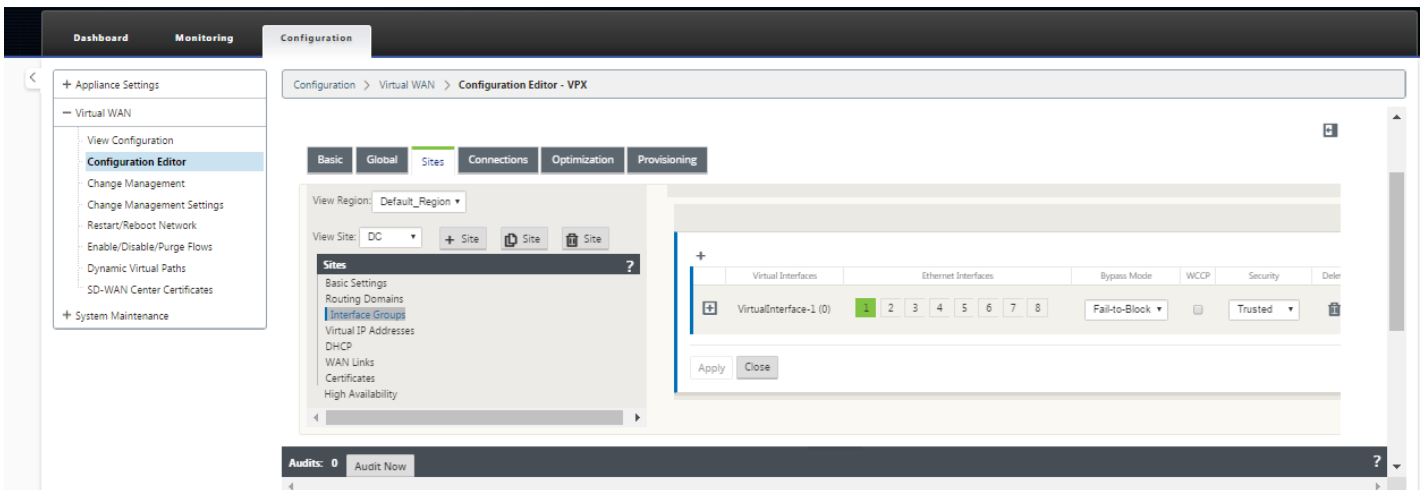
Note

For additional guidelines and information on configuring Virtual Interface Groups, see the Virtual Routing and Forwarding section.

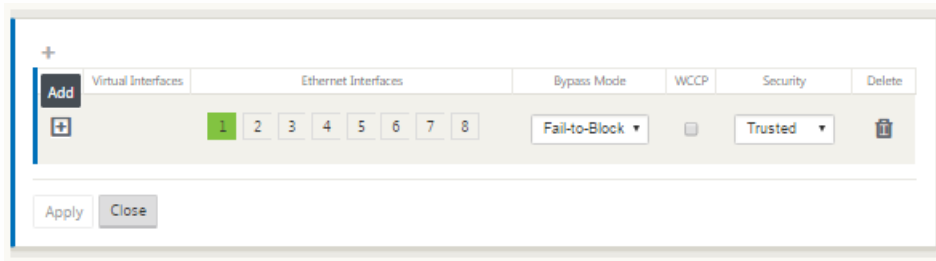
To add a Virtual Interface Group to the new MCN site, do the following:

1. Continuing in the **Sites** view of the **Configuration Editor**, select the site from the **View Site** drop-down menu.

This opens the configuration view for the site you selected.

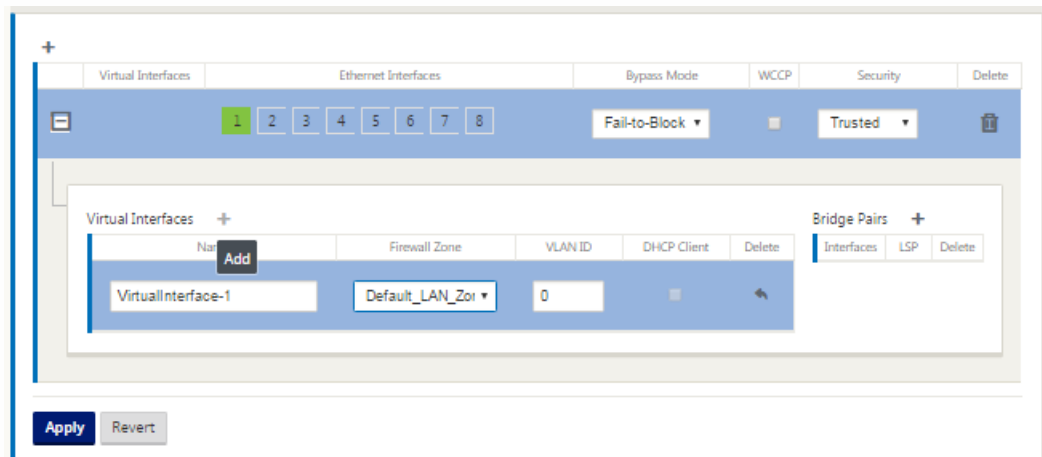


2. Click **+** to add the **Virtual Interface Group**. This adds a new blank Virtual interface group entry to the table and opens it for editing.



3. Click **+** to the right of **Virtual Interfaces**.

This adds a new blank group entry to the table and opens it for editing.



4. Select the Ethernet Interfaces to include in the group.

Under **Ethernet Interfaces**, click an interface to include/exclude that interface. You can select any number of interfaces to include in the group.



5. Select the **Bypass Mode** from the drop-down menu (no default).

The **Bypass Mode** specifies the behavior of bridge-paired interfaces in the Virtual Interface Group, in the event of an appliance or service failure or restart. The options are: **Fail-to-Wire** or **Fail-to-Block**.

6. Select the Security Level from the drop-down menu.

This specifies the security level for the network segment of the Virtual Interface Group. The options are: **Trusted** or **Untrusted**. Trusted segments are generally protected by a firewall (default is Trusted).

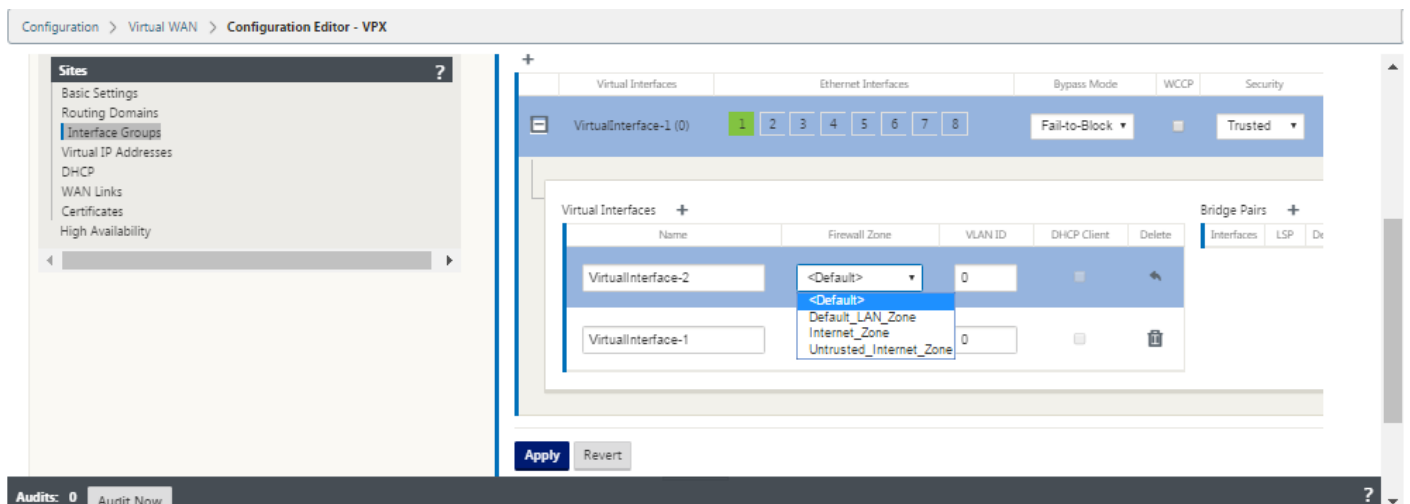
7. Click **+** at the left edge of the Virtual Interface you added.

This displays the **Virtual Interfaces** table.



8. Click **+** to the right of **Virtual Interfaces**.

This reveals the **Name**, **Firewall Zone**, and **VLAN ID** Ids.



9. Enter the **Name** and **VLAN ID** for this Virtual Interface Group.

Name – This is the name by which this Virtual Interface will be referenced.

Firewall Zone - Select a firewall zone from the drop-down menu.

VLAN ID – This is the ID for identifying and marking traffic to and from the Virtual Interface. Use an ID of 0 (zero) for native/untagged traffic.

10. Click **+** to the right of **Bridge Pairs**. This adds a new **Bridge Pairs** entry and opens it for editing.

11. Select the Ethernet interfaces to be paired from the drop-down menus. To add more pairs, click **+** next to **Bridge Pairs** again.

12. Click **Apply**. This applies your settings and adds the new Virtual Interface Group to the table.

Note

At this stage, you will see a yellow delta AuditAlert icon, to the right of the new Virtual Interface Group entry. This is because you have not yet configured any Virtual IP Addresses (VIPs) for the site. For now, you can ignore this alert, as it will be resolved automatically when you have properly configured the Virtual IPs for the site.

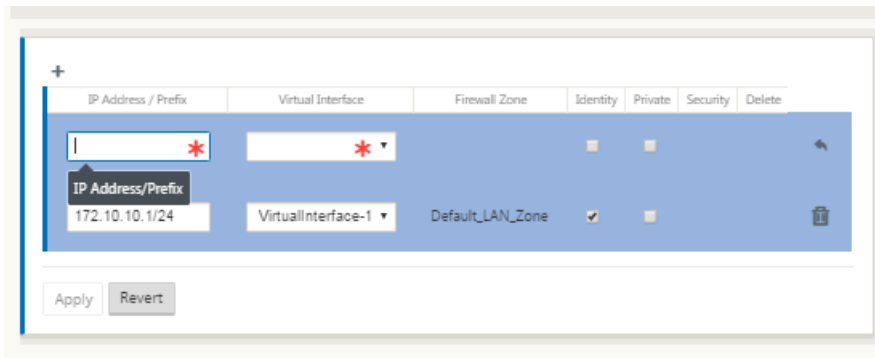
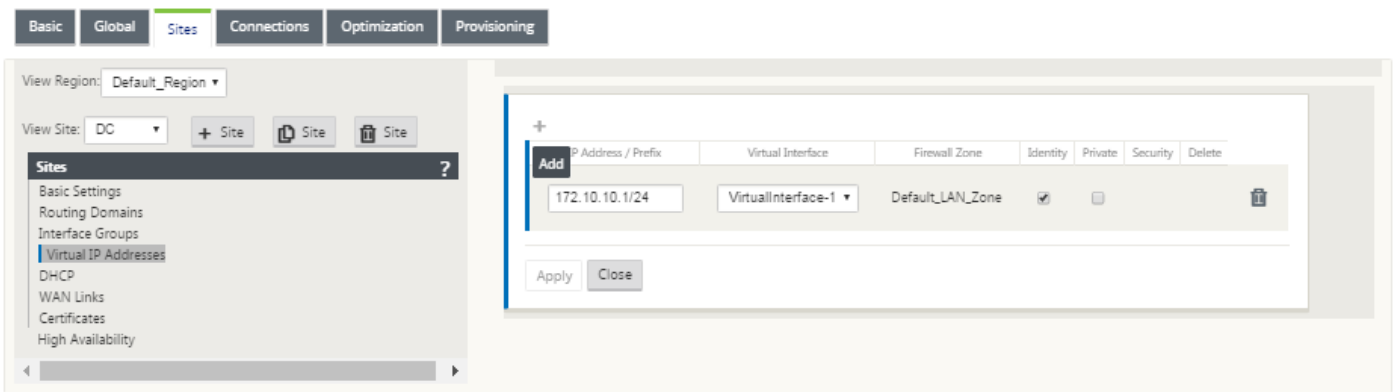
13. To add more Virtual Interface Groups, click **+** to the right of the **Interface Groups** branch, and proceed as above.

How to Configure Virtual IP Address for the MCN

The next step is to configure the Virtual IP Addresses for the site, and assign them to the appropriate group.

1. Continuing in the **Sites** view for the new MCN site, click **+** to the left of the **Virtual IP Addresses**. This displays the **Virtual IP Addresses** table for the new site.

2. Click **+** to the right of **Virtual IP Addresses** to add an address. This opens the form for adding and configuring a new Virtual IP Address.

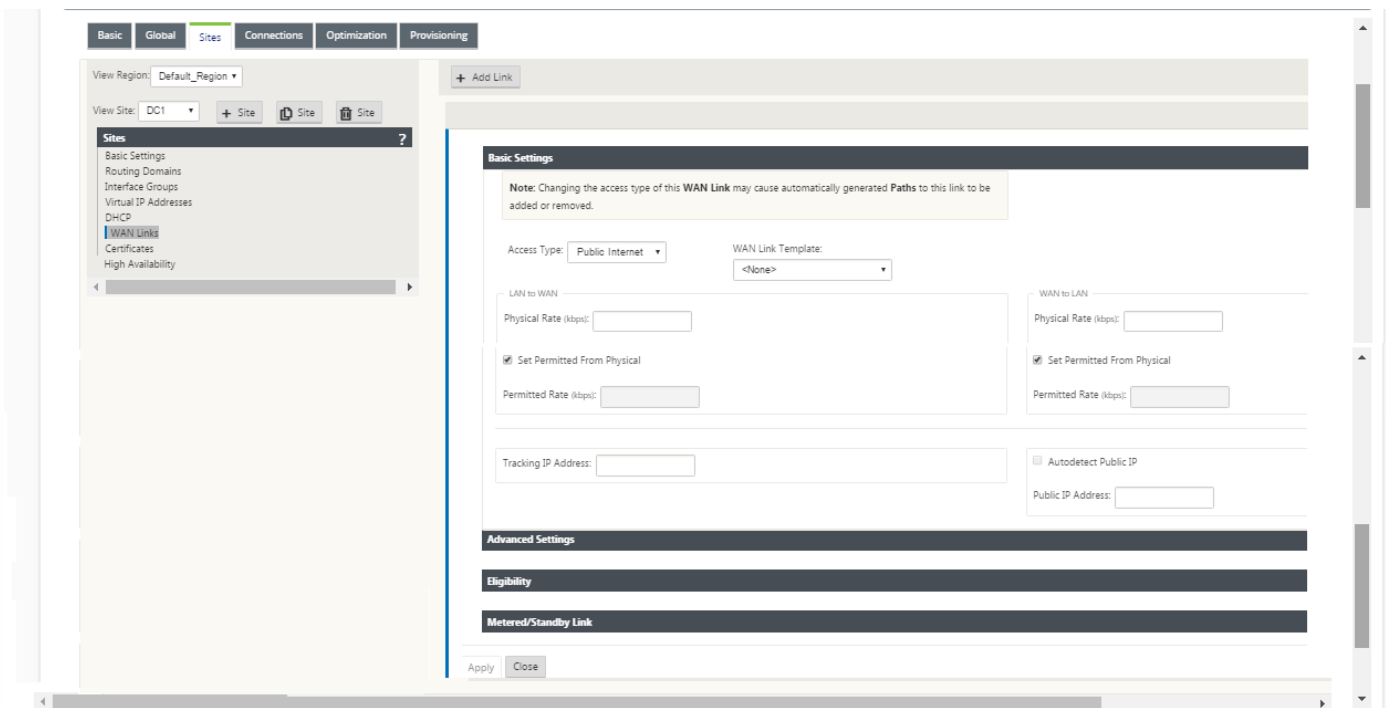


3. Enter the **IP Address / Prefix** information, and select the **Virtual Interface** with which the address is associated. The Virtual IP Address must include the full host address and netmask.
4. Select the desired settings for the Virtual IP address; such as the Firewall Zone, Identity, Private, and Security.
5. Click **Apply**. This adds the address information to the site and includes it in the site **Virtual IP Addresses** table.
6. To add more Virtual IP Addresses, click **+** to the right of the **Virtual IP Addresses**, and proceed as above.

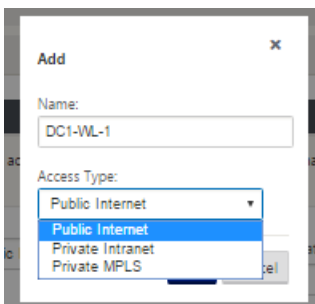
How to Configure WAN Links for the MCN

The next step is to configure the WAN links for the site.

1. Continuing in the **Sites** view for the new MCN site, click the **WAN Links** label.



2. Click **Add Link** to the right of the **WAN Links** to add a new WAN link. This opens the **Add** dialog box.



3. (Optional) Enter a name for the WAN Link if you do not want to use the default.

The default is the site name, appended with the following suffix:

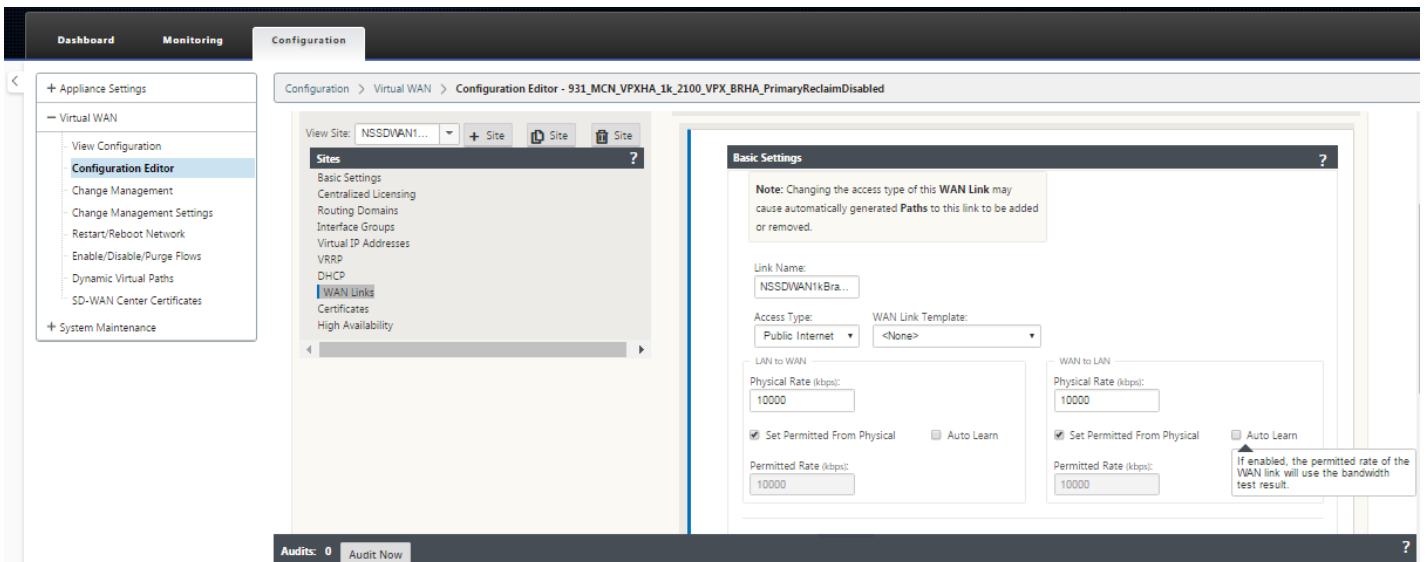
-WL-<number>

Where <number> is the number of WAN Links for this site, incremented by one.

4. Select the **Access Type** from the drop-down menu.

The options are **Public Internet**, **Private Intranet**, or **Private MPLS**.

5. Click **Add**. This displays the **WAN Links** Basic Settings configuration page, and adds the new unconfigured WAN link to the page.

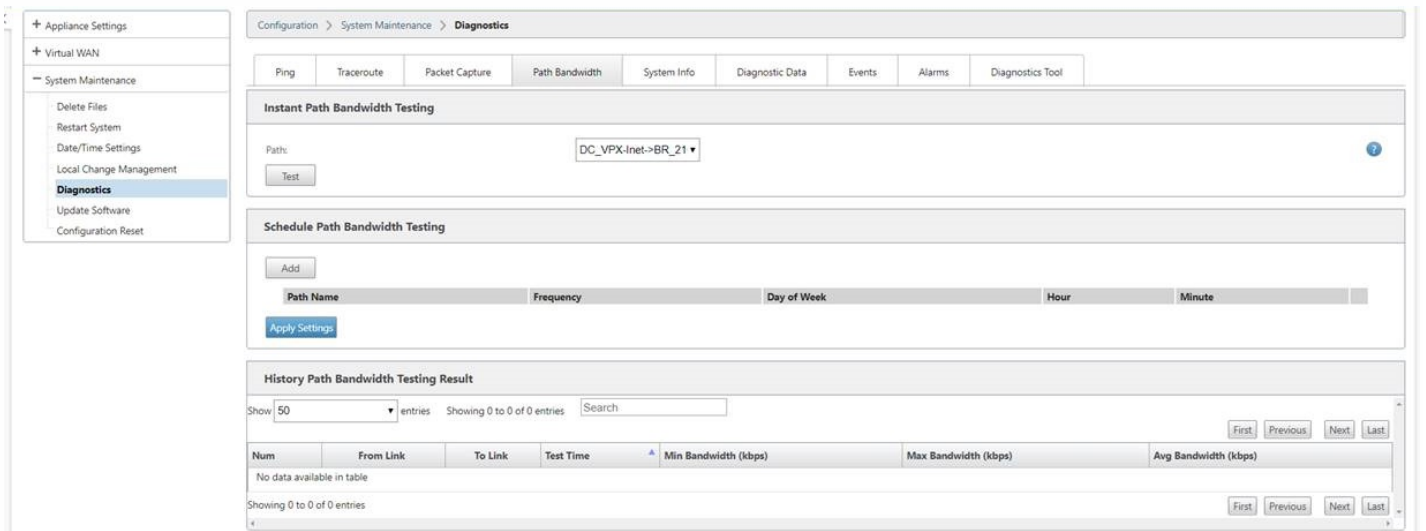


Auto Learn of bandwidth consumption

Auto learn runs on system startup and repeats every 5 minutes until a successful result is observed. Auto learn also runs after any WAN link configuration changes are made from the config editor.

You can execute tests manually or schedule tests in the SD-WAN GUI. Results from these tests should also apply to the permitted rate when the test is successful and auto learn is enabled.

When using auto learn on large networks, if config change restarts then all sites run tests simultaneously on the MCN, causing high bandwidth usage leading to inaccurate results. It is recommended that you schedule bandwidth tests once or twice a day, typically when traffic volume is low.



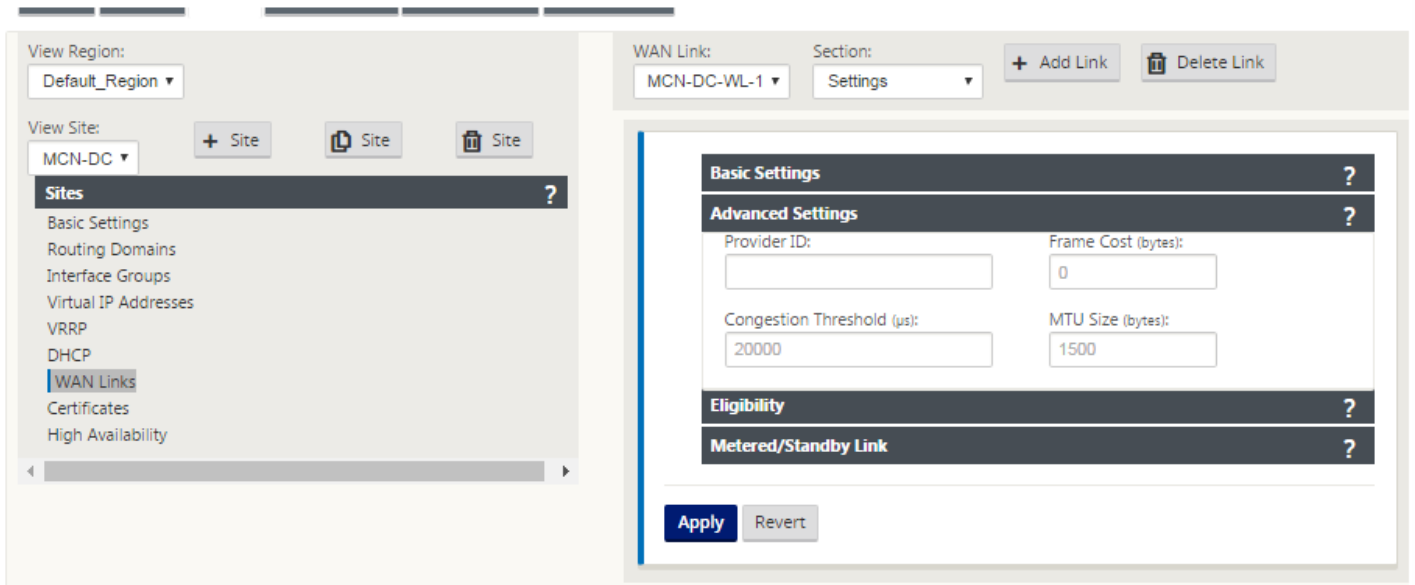
6. Enter the link details for the new WAN link. Configure the LAN to WAN, WAN to LAN settings.

Some guidelines are as follows:

- Some Internet links might be asymmetrical.
- Misconfiguring the permitted speed can adversely affect performance for that link.
- Avoid using burst speeds that surpass the Committed Rate.

- For Internet WAN links, be sure to add the Public IP Address.

7. Click the grey **Advanced Settings** section bar. This opens the **Advanced Settings** form for the link.

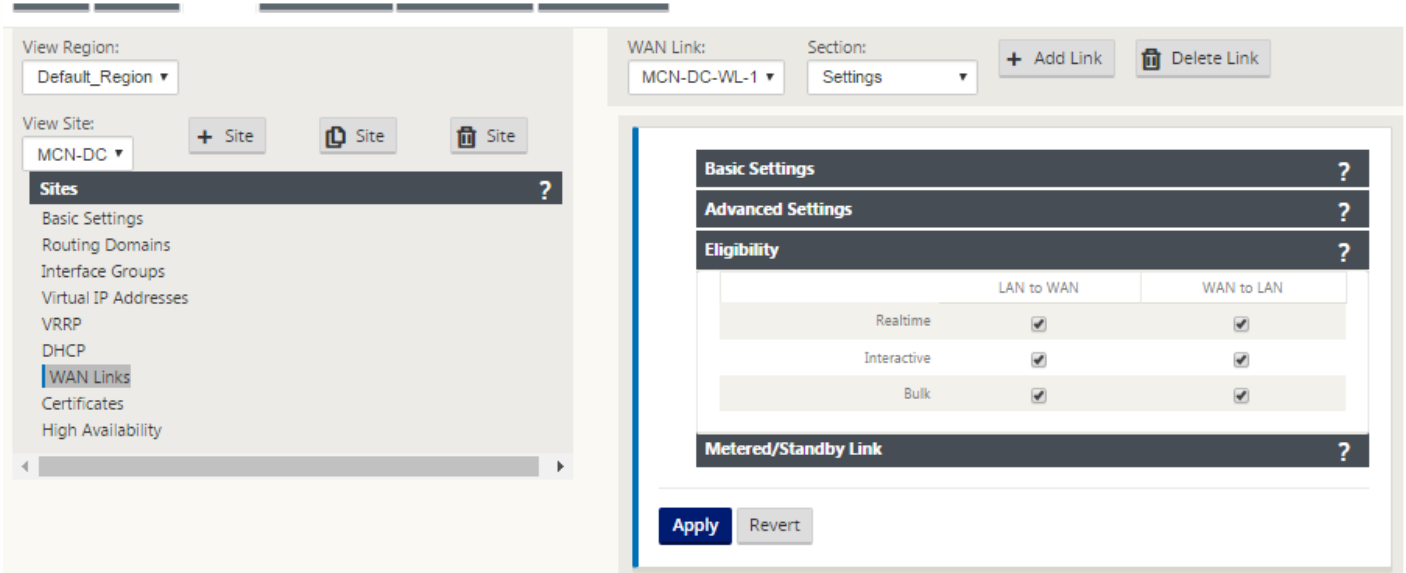


8. Enter the **Advanced Settings** for the link.

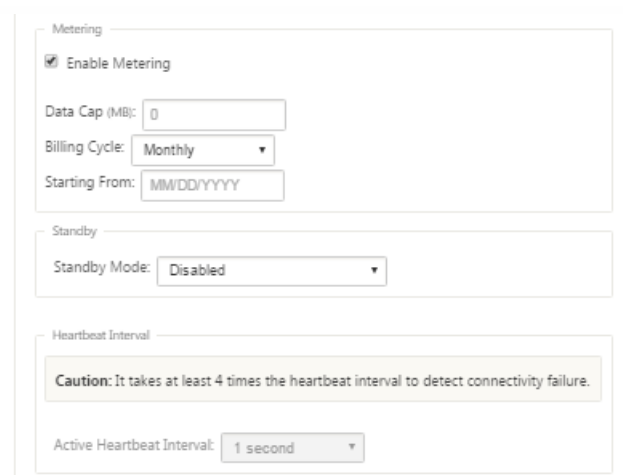
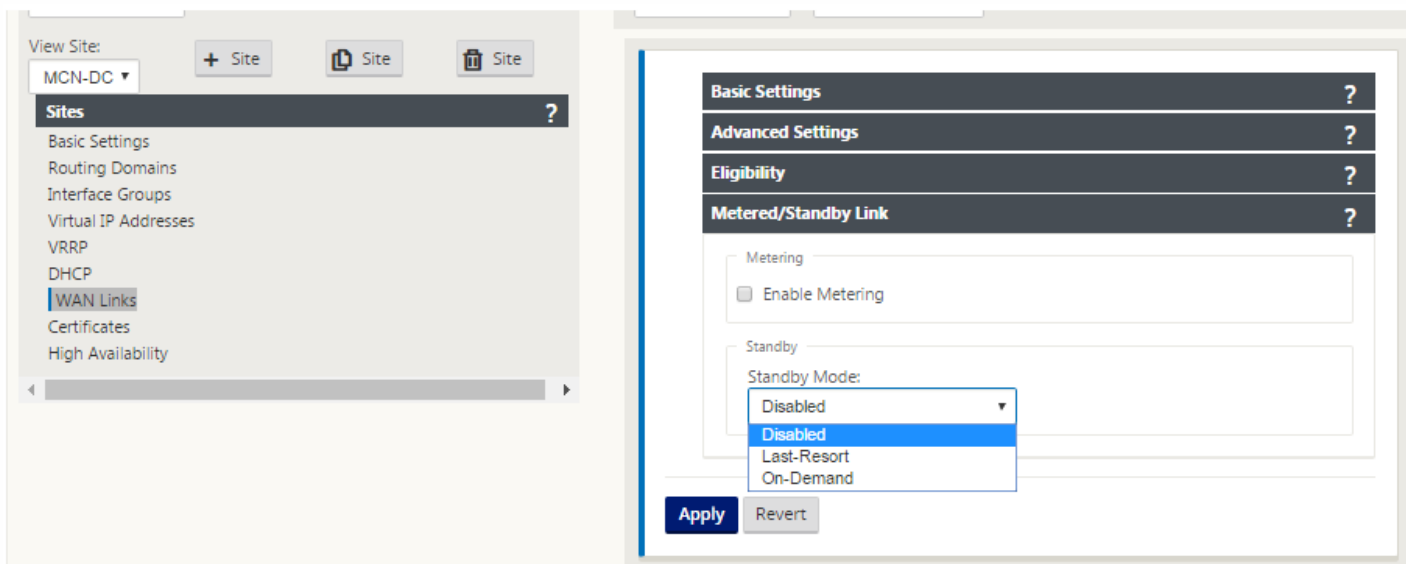
- **Provider ID** – (Optional) Enter a unique ID number from 1-100 to designate WAN Links connected to the same service provider. Virtual WAN uses the Provider ID to differentiate paths when sending duplicate packets.
- **Frame Cost (bytes)** – Enter the size (in bytes) of the header/trailer added to each packet; for example, the size in bytes of added Ethernet IPG or AAL5 trailers.
- **Congestion Threshold** – Enter the congestion threshold (in microseconds) after which the WAN link will throttle packet transmission to avoid further congestion.
- **MTU Size (bytes)** – Enter the largest raw packet size (in bytes), not including the Frame Cost.

9. Click the grey **Eligibility** section bar. This opens the **Eligibility** settings form for the link.

10. Select the **Eligibility** settings for the link.



11. Click the grey **Metered Link** section bar. This opens the **Metered Link** settings form for the link.
12. (Optional) Select **Enable Metering** to enable metering for this link. This displays the **Enable Metering** settings fields.



13. Configure the metering settings for the link.

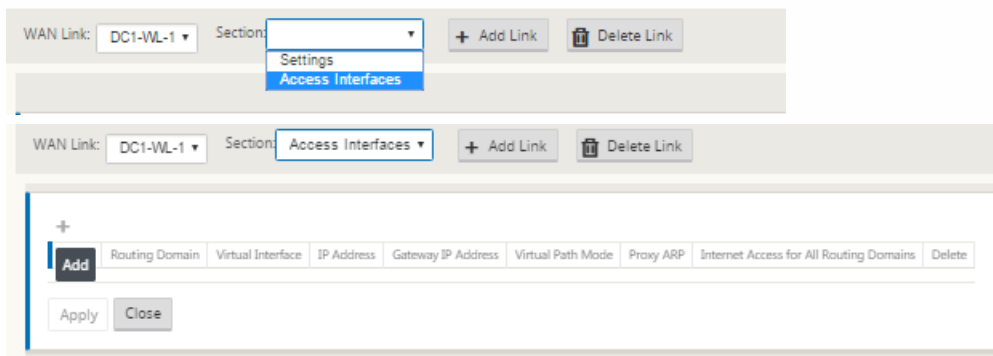
Enter the following:

- **Data Cap (MB)** – Enter the data cap allocation for the link, in megabytes.
- **Billing Cycle** – Select either Monthly or Weekly from the drop-down menu.
- **Starting From** – Enter the start date of the billing cycle.
- **Set Last Resort** – Select this to enable this link as a link of last resort in the event of a failure of all other available links. Under normal WAN conditions, Virtual WAN sends only minimal traffic over metered links, for the purpose of checking link status. However, in the event of a failure, SD-WAN can use active metered links as a last resort for forwarding production traffic.

14. Click **Apply**. This applies your specified settings to the new WAN link.

The next step is to configure the Access Interfaces for the new WAN link. An Access Interface consists of a Virtual Interface, WAN endpoint IP Address, Gateway IP Address, and Virtual Path Mode defined collectively as an interface for a specific WAN link. Each WAN link must have at least one Access Interface.

15. Select **Access Interfaces** in the WAN Link configuration page for the link. This opens the **Access Interfaces** view for the site.



16. Click **+** to add an interface. This adds a blank entry to the table and opens it for editing. Enter the **Access Interfaces** settings for the link.

Note

- Each WAN link must have at least one Access Interface.
- You can ignore the MAC address binding for configuring Access Interface for 210-SELTE appliance networks.

WAN Link: DC-WL-1 Section: Access Interfaces + Add Link Delete Link

Name	Routing Domain	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Internet Access for All Routing Domains	Delete
DC-WL-1-AI-1	Default_RoutingDomain	VirtualInterface-1	172.10.10.1	172.10.10.2	Primary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Close

17. Enter the following:

- **Name** – This is the name by which this Access Interface will be referenced. Enter a name for the new Access Interface, or accept the default. The default uses the following naming convention:

WAN_link_name-AI-number

Where *WAN_link_name* is the name of the WAN link you are associating with this interface, and number is the number of Access Interfaces currently configured for this link, incremented by 1.

Note

If the name appears truncated, you can place your cursor in the field, then click and hold and roll your mouse right or left to see the truncated portion.

- **Virtual Interface** – This is the Virtual Interface this Access Interface will use. Select an entry from the drop-down menu of Virtual Interfaces configured for this branch site.

- **Routing Domain** - The routing domain which you want to choose for the Access Interface.

- **IP Address** – This is the IP Address for the Access Interface endpoint from the appliance to the WAN.

- **Gateway IP Address** – This is the IP Address for the gateway router.

- **Virtual Path Mode** – This specifies the priority for Virtual Path traffic on this WAN link. The options are: **Primary**, **Secondary**, or **Exclude**. If set to **Exclude**, this Access Interface will be used for Internet and Intranet traffic, only.

- **Proxy ARP** – Select the checkbox to enable. If enabled, the Virtual WAN Appliance replies to ARP requests for the Gateway IP Address, when the gateway is unreachable.

18. Click **Apply**.

You have now finished configuring the new WAN link. Repeat these steps to add and configure additional WAN links for the site.

The next step is to add and configure the routes for the site.

How to Configure Routes for the MCN

To add and configure the routes for the site, do the following:

1. Click the **Connections** view for the new MCN site and select **Routes**. This displays the **Routes** view for the site.
2. Click **+** to the right of **Routes** to add a route. This opens the **Routes** dialog box for editing.

3. Enter the route configuration information for the new route.

Enter the following:

- **Network IP Address** – Enter the Network IP Address.
- **Cost** – Enter a weight from 1 to 15 for determining the route priority for this route. Lower-cost routes take precedence over higher-cost routes. The default value is 5.
- **Service Type** – Select the service type for the route from the drop-down menu for this field. The options are as follows:
 - * **Virtual Path** – This service manages traffic across the Virtual Paths. A Virtual Path is a logical link between two WAN links. It comprises a collection of WAN Paths combined to provide high service-level communication between two SD-WAN nodes. This is accomplished by constantly measuring and adapting to changing application demand and WAN conditions. SD-WAN Appliances measure the network on a per-path basis. A Virtual Path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN Appliances reaches a configured threshold).
 - * **Internet** – This service manages traffic between an Enterprise site and sites on the public Internet. Traffic of this type is not encapsulated. During times of congestion, the SD-WAN actively manages bandwidth by rate-limiting Internet traffic relative to the Virtual Path, and Intranet traffic according to the SD-WAN configuration established by the Administrator.
 - * **Intranet** – This service manages Enterprise Intranet traffic that has not been defined for transmission across a Virtual Path. As with Internet traffic, it remains unencapsulated, and the SD-WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Note that under certain conditions, and if configured for Intranet Fallback on the Virtual Path, traffic that ordinarily travels by means of a Virtual Path may instead be treated as Intranet traffic, in order to maintain network reliability.
 - * **Passthrough** – This service manages traffic that is to be passed through the Virtual WAN. Traffic directed to the Passthrough Service includes broadcasts, ARPs and other non-IPv4 traffic, as well as traffic on the Virtual WAN Appliance local subnet, specifically-configured subnets, or Rules applied by the Network Administrator. This traffic is not delayed,

shaped or modified by the SD-WAN. Consequently, you must ensure that Passthrough traffic does not consume substantial resources on the WAN links that the SD-WAN Appliance is configured to use for other services.

* **Local** – This service manages IP traffic local to the site that matches no other service. SD-WAN ignores traffic sourced and destined to a local route.

* **GRE Tunnel** – This service manages IP traffic destined for a GRE tunnel, and matches the LAN GRE tunnel configured at the site. The GRE Tunnel feature enables you to configure SD-WAN Appliances to terminate GRE tunnels on the LAN. For a route with service type GRE Tunnel, the gateway must reside in one of the tunnel subnets of the local GRE tunnel.

* **LAN IPsec Tunnel** – This service manages IP traffic destined for IPsec tunnel.

- **Gateway IP Address** – Enter the Gateway IP Address for this route.

- **Eligibility Based on Path** (checkbox) – (Optional) If enabled, the route will not receive traffic when the selected path is down.

- **Path** – This specifies the path to be used for determining route eligibility.

Depending on the "Service Type", the following settings are displayed:

Service Type	Service Type Settings
Virtual Path	Next Hop Site – This indicates the remote site to which Virtual Path packets will be directed.
Internet	<ul style="list-style-type: none"> • Export Route: Enable/Disable to export routes to other connected sites. • Eligibility based on path
Intranet	<ul style="list-style-type: none"> • Export route • Intranet service • Eligibility based on path • Eligibility based on tunnel
Passthrough	<ul style="list-style-type: none"> • Eligibility based on path
Local	<ul style="list-style-type: none"> • Export route • Summary route • Eligibility based on path
GRE Tunnel	<ul style="list-style-type: none"> • Export route • Eligibility based on path • Eligibility based on Gateway
IPsec Tunnel	<ul style="list-style-type: none"> • Export route • Eligibility based on path • IPsec Tunnel • Eligibility based on tunnel
Discard	<ul style="list-style-type: none"> • Export route • Summary route

4. Click **Apply**.

Note

After you click **Apply**, audit warnings might appear indicating that further action is required. A red dot or goldenrod delta icon indicates an error in the section where it appears. You can use these warnings to identify errors or missing configuration information. Roll your cursor over an audit warning icon to display a short description of the error(s) in that section. You can also click the dark grey **Audits** status bar (bottom of page) to display a complete list of all audit warnings.

+

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	0.0.0.0/0	5	Virtual Path	Branch1				
2	172.147.21.52/24	5	Local					
3	172.147.22.52/24	5	Local					
4	0.0.0.0/0	65535	Passthrough					

« < 1 > »

Apply Close

You can also edit configured routes as shown below.

?

Edit

Network IP Address:

Cost:

Service Type:

Gateway IP Address:

Next Hop Site:

Eligibility Based On Path

Path:

Apply Cancel

To add more routes for the site, click **+** to the right of the **Routes** branch, and proceed as above.

You have now finished entering the primary configuration information for the new MCN site. The following two sections provide instructions for additional optional steps:

- [Configuring High Availability \(HA\) for the MCN Site \(Optional\).](#)
- [Enabling and Configuring Virtual WAN Security and Encryption \(Optional\).](#)

If you do not want to configure these features at this time, you can proceed directly to the section [Naming, Saving, and Backing Up the MCN Site Configuration.](#)

Enable and Configure Virtual WAN Security and Encryption (Optional)

Mar 01, 2018

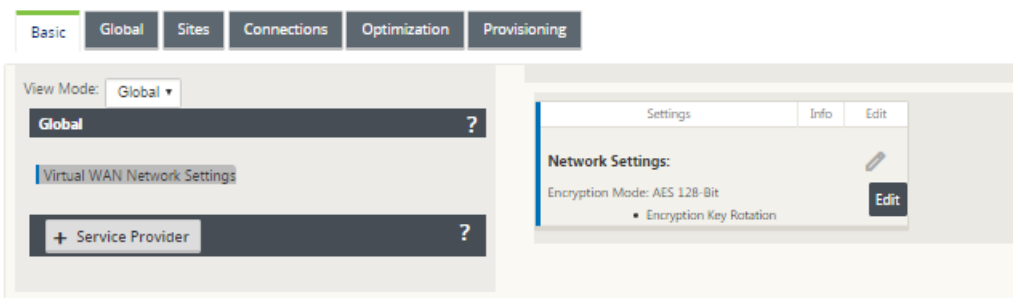
To enable and configure Virtual WAN security and encryption, do the following:

Note

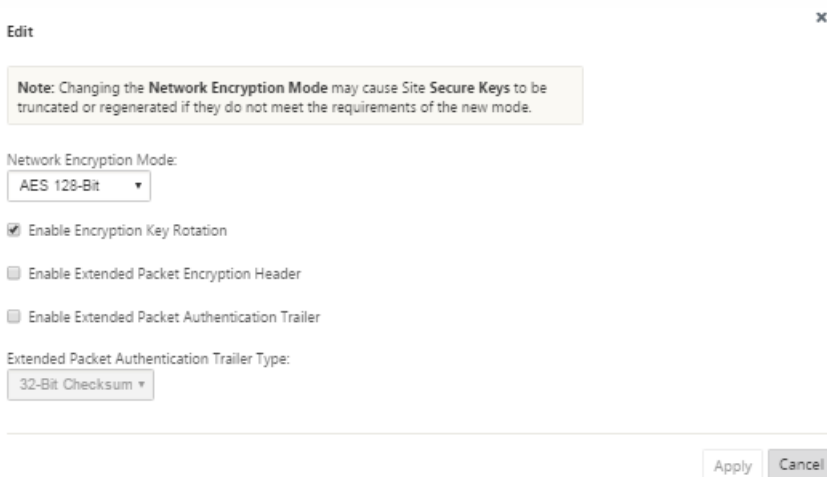
Enabling Virtual WAN security and encryption is optional.

1. Navigate to the **Basic** tab in the **Configuration Editor**, Select **Global** from **View Mode**.

This displays the **Virtual Network Settings** configuration form to the right-hand side of the screen.



2. Click Edit (pencil icon) to enable editing for the form.



3. Enter your global security settings.

The options are as follows:

- **Network Encryption Mode** – This is the encryption algorithm used for encrypted paths. Select one of the following from the drop-down menu: **AES 128-Bit** or **AES 256-Bit**.
- **Enable Encryption Key Rotation** – When enabled, encryption keys are rotated at intervals of 10 to 15 minutes.

- **Enable Extended Packet Encryption Header** – When enabled, a 16 byte encrypted counter is prepended to encrypted traffic to serve as an initialization vector, and randomize packet encryption.
 - **Enable Extended Packet Authentication Trailer** – When enabled, an authentication code is appended to the contents of the encrypted traffic to verify that the message is delivered unaltered.
 - **Extended Packet Authentication Trailer Type** – This is the type of trailer used to validate packet contents. Select one of the following from the drop-down menu: **32-Bit Checksum** or **SHA-256**.
4. Click **Apply** to apply your settings to the configuration.

This completes the configuration of the MCN site. The next step is to name and save the new MCN site configuration (optional, but strongly recommended), as described in the following section.

Warning

If your console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is strongly recommended that you save the configuration package often, or at key points in the configuration.

Configure Secondary MCN

Apr 04, 2018

You can configure a site as the secondary MCN to support MCN redundancy. The secondary MCN continuously monitors the health of the primary MCN. If the primary MCN fails, the secondary MCN assumes the role of the MCN. To create a secondary MCN, while adding a new site in the **Mode** option select secondary MCN. You have to configure the virtual interface, virtual IP, WAN link, and other settings manually. Similarly, you can also configure a secondary RCN.

Note

Do not confuse the secondary MCN configuration with High Availability configuration. In secondary MCN configuration, a branch / client site in a different geographical location is configured as a secondary MCN to enable disaster recovery. In HA configuration, two appliances are configured with the same subnet or geographical location to ensure fault tolerance. For information on configuring High Availability configuration, see [High Availability Deployment](#).

The secondary MCN appliance may or may not be the same platform model as the primary MCN. You can choose an appliance model based on the usage, bandwidth requirement and the number of sites to be supported.

The primary MCN to secondary MCN switch over happens after 15 seconds of the primary MCN being inactive. You cannot configure primary reclaim for secondary MCN, the primary reclaim happens automatically after the primary appliance is back ON and the hold timer expires.

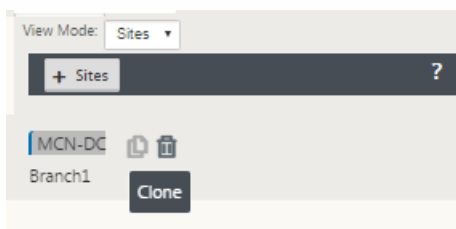
The best way to configure a secondary MCN would be to clone the existing MCN as it retains most of the MCN configuration. When a site is cloned, the entire set of configuration settings for the site are copied and displayed in a single form screen. You can then modify the settings according to the requirements quickly and easily.

Note

You can clone an MCN to create a secondary MCN or branch sites. You can configure only one secondary MCN.

To clone an MCN site and create a secondary MCN:

1. In the Configuration Editor, navigate to **Basic > Sites**, and click the clone icon for the MCN site.



2. Enter the configuration parameter settings for the new site.

Clone x

Please review the following fields and make the appropriate changes for the new Site.

Site Name: **MCN-DC** ! Appliance Name: Mode: **secondary MCN** Secure Key:

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
VirtualInterface-1	<input type="text" value="0"/>	<input type="checkbox"/>
VirtualInterface-2	<input type="text" value="0"/>	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	VirtualInterface-1	172.147.21.52/24 !
<input checked="" type="checkbox"/>	VirtualInterface-2	172.147.22.52/24 !

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type										
<input checked="" type="checkbox"/>	MCN-DC-WL-1 !											
<p>Access Interfaces</p> <table border="1"> <thead> <tr> <th>Include Interface</th> <th>Access Interface</th> <th>Virtual Interface</th> <th>Virtual IP Address</th> <th>Gateway</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>MCN-DC-WL-1-...</td> <td>VirtualInterface-1</td> <td>172.147.21.52 !</td> <td>172.147.21.1 !</td> </tr> </tbody> </table>			Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway	<input checked="" type="checkbox"/>	MCN-DC-WL-1-...	VirtualInterface-1	172.147.21.52 !	172.147.21.1 !
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway								
<input checked="" type="checkbox"/>	MCN-DC-WL-1-...	VirtualInterface-1	172.147.21.52 !	172.147.21.1 !								
<input checked="" type="checkbox"/>	MCN-DC-WL-2 !											

GRE Tunnels

Include	Name	Source IP	Destination IP	Tunnel IP / Prefix
---------	------	-----------	----------------	--------------------

Note

A highlighted field with an Audit Alert icon (red dot) indicates a required parameter setting that must have a value different from the current setting.

- In the **Mode** field, select **secondary MCN**. Resolve all Audit Alerts.
- Click **Clone** to create the secondary MCN site.

Manage MCN Configuration

Apr 24, 2018

The next step is to name and save the new configuration, seen also as a configuration package. This step is optional at this point in the configuration, but recommended. The configuration package is saved to your workspace on the local appliance. You then have the option to log out of the Management Web Interface and continue the configuration process later. However, if you log out, you need to reopen the saved configuration when you resume. Instructions for opening a saved configuration are provided below.

Warning

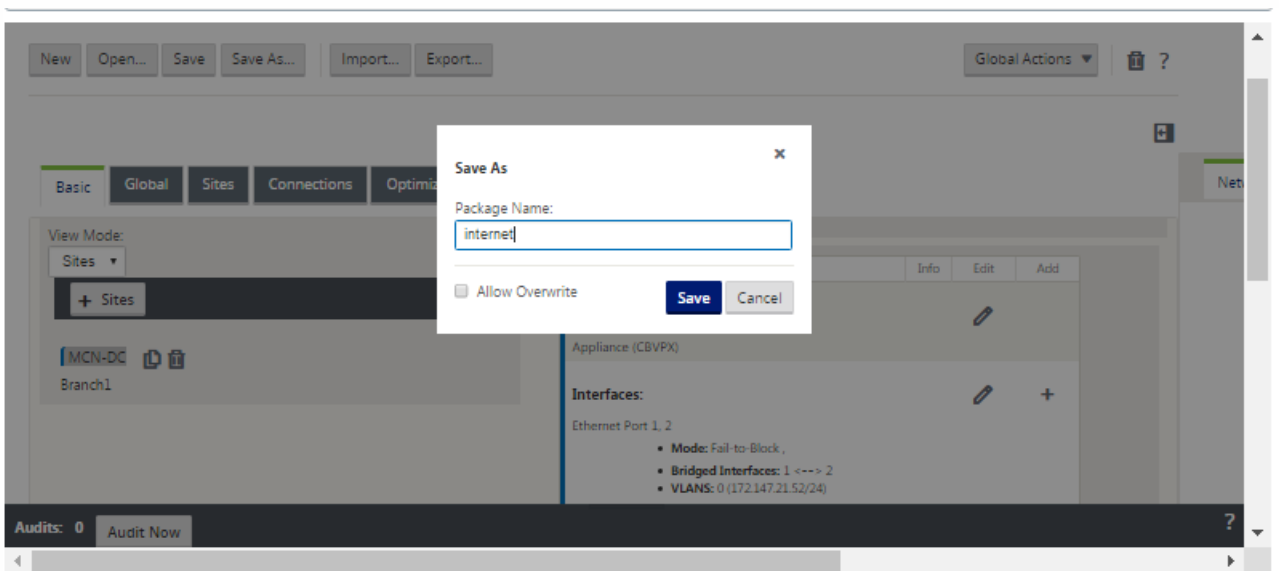
If the Console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes are lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is recommended that you save the configuration package often, or at key points in the configuration.

Tip

As an extra precaution, it is recommended that you use **Save As**, rather than **Save**, to avoid overwriting the wrong configuration package.

1. Click **Save As** (at the top of the **Configuration Editor** middle pane).

This opens the **Save As** dialog box.



2. Type the configuration package name.

Note

If you are saving the configuration to an existing configuration package, be sure to select **Allow Overwrite** before saving.

3. Click **Save**.

Note

After saving the configuration file, you have the option to log out of the Management Web Interface and continue the configuration process later. However, if you log out, you need to reopen the saved configuration when you resume. Instructions are provided in the section, [Loading a Saved Configuration Package into the Configuration Editor](#).

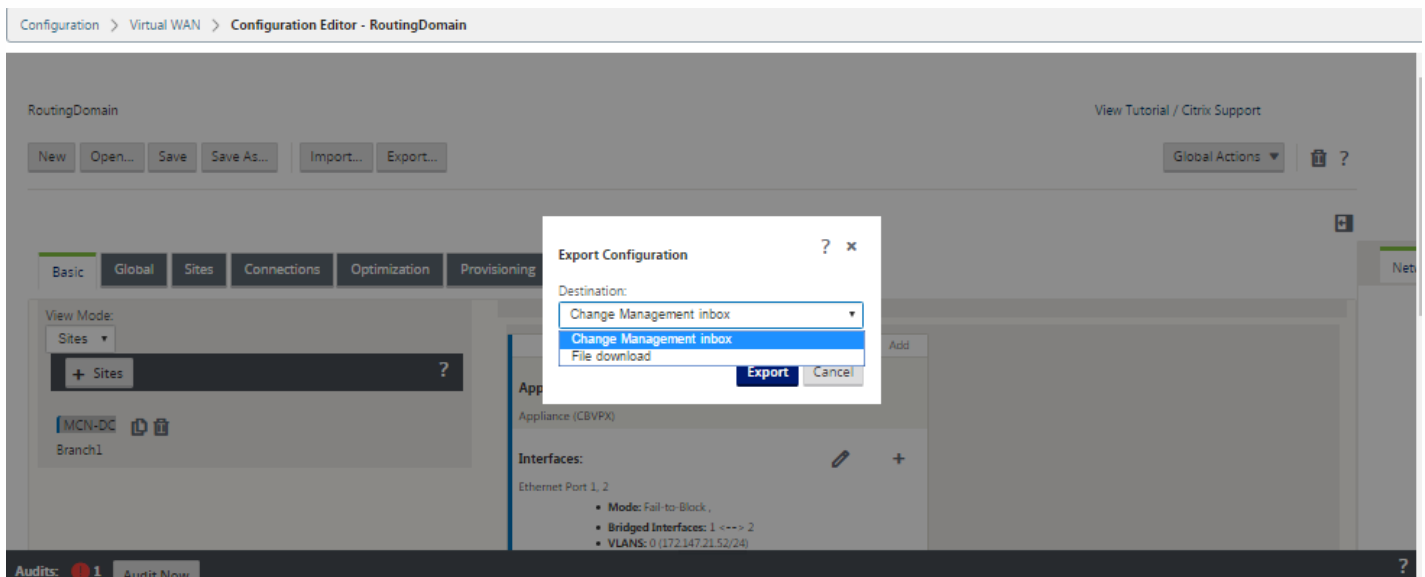
You have now completed the MCN site configuration, and created a new SD-WAN configuration package. You are now ready to add and configure the branch sites. Instructions are provided in [setup Branch Sites](#).

Export Backup Copy of the Configuration Package

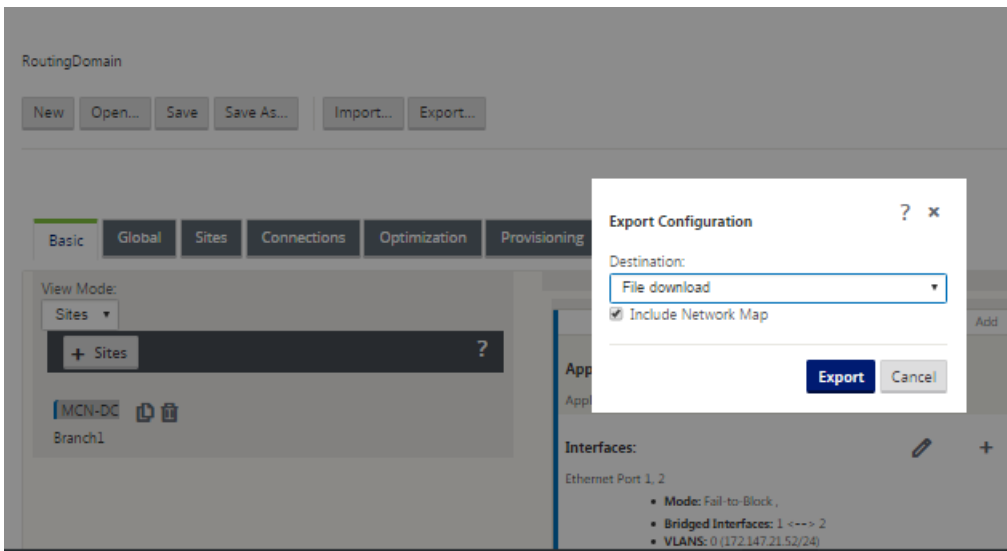
In addition to saving the configuration-in-progress to your appliance workspace, is recommended that you also periodically back up the configuration to your local PC.

To export the current configuration package to your PC, do the following:

1. Click **Export**. This displays the **Export Configuration** dialog box.



2. Select **File Download** from the **Destination**: drop down menu. This reveals the **Include Network Map** option, which is selected by default.



3. Accept the default, and click **Export**. This includes the **Network Map** information in the configuration package, and opens a file browser for specifying the name and location for saving the configuration.

4. Navigate to the save location on your PC and click **Save**. This saves the configuration package to your PC.

Note

To recover a backed-up configuration package, you can use an **Import** operation to import the package from your PC and load it into the **Configuration Editor**. You can then save the imported package to your Management Web Interface workspace for future use.

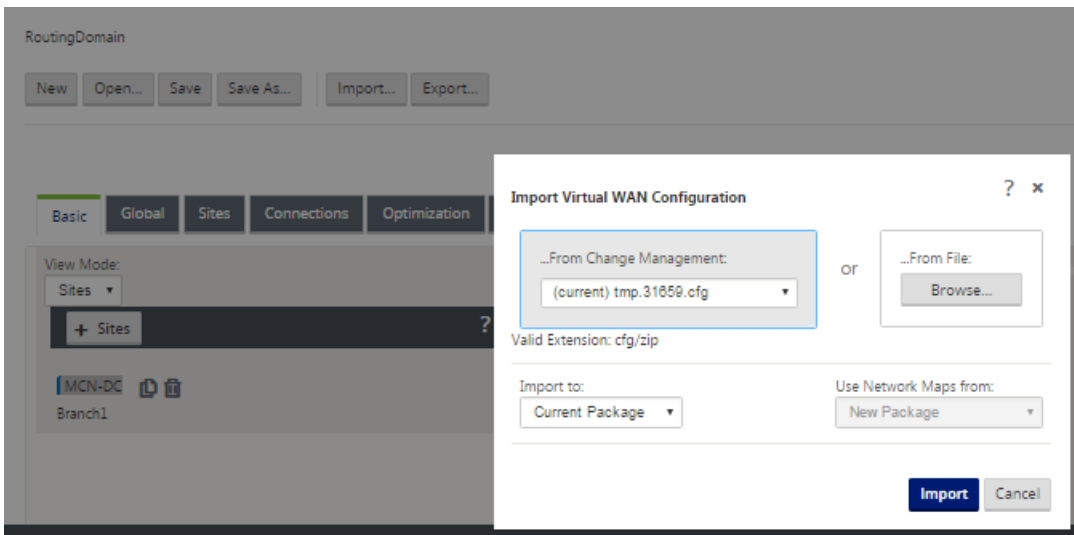
Import Backed up Configuration Package

Sometimes, you might want to revert to an earlier version of a Configuration Package. If you have saved a copy of the earlier version to your local PC, you can import it back into the Configuration Editor, and then open it for editing. If this is not an initial deployment, you can also import an existing Configuration Package from the global Change Management inbox on the current MCN. Instructions for both of these procedures are provided below.

To import a Configuration Package, do the following:

1. Open the **Configuration Editor**.
2. In the **Configuration Editor** menu bar, click **Import**.

The **Import Virtual WAN Configuration** dialog box appears.

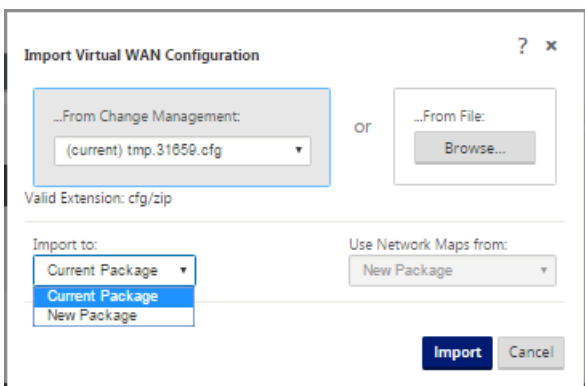


3. Select the location from which to import the package.

- To import a Configuration Package from Change Management: Select the package from the **From Change Management** drop-down menu (top left corner).

- To import a Configuration Package from your local PC: Click **Browse** to open a file browser on your local PC. Select the file and click **OK**.

4. Select the import destination (if applicable). If a Configuration Package is already open in the **Configuration Editor**, then the **Import to:** drop down menu will be available.

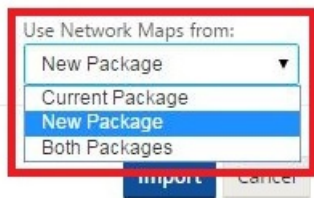


Select one of the following options:

- **Current Package** – Select this to replace the contents of the currently opened Configuration Package with the contents of the imported package, and retain the name of the opened package. However, the contents of the saved version of the current package will not be overwritten until you explicitly save the changed package. If you use **Save As** to save the package, select **Allow Overwrite** to enable overwriting of the previous version.

- **New Package** – Select this to open a new, blank Configuration Package, and populate it with the contents of the imported package. The new package automatically takes the same name as the imported package.

5. Specify which network maps to include (if applicable). If a Configuration Package is already open in the **Configuration Editor**, then the **Use Network Maps From:** drop down menu is available.



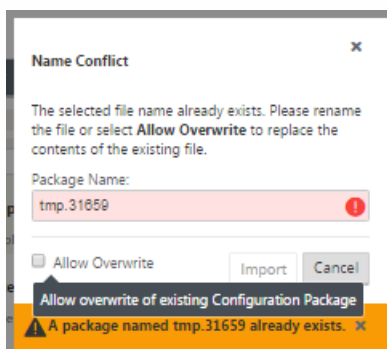
Select one of the following options:

- Current **Package** – This retains the network maps currently configured in the package now available in the Configuration Editor, and discards any network maps from the imported package.
- New **Package** – This replaces the network maps currently configured in the currently open package with the network maps (if any) from the imported package.
- Both **Packages** – This includes all network maps from both the current and the imported package.

6. Click **Import**. The imported file is loaded into the **Configuration Editor**, according to your specifications.

Note

If a package of the same name exists in your workspace, then the **Name Conflict** dialog box displays.



To specify the name to use for the imported package, do one of the following:

- type a different name in the **Package Name** field to rename the new package and enable the **Import** button. The imported package is loaded into the **Configuration Editor** with the specified name. The package name is saved to your workspace now, but the package contents will not be saved to your workspace until you explicitly save the package.
- Select **Allow Overwrite** to confirm that you want to retain the existing name and enable overwriting of the contents of the saved package. However, the contents of the saved version of the current package will not be overwritten until you explicitly save the changed package.

This also enables the **Import** button in the **Name Conflict** dialog box. Click **Import** to complete the import operation.

Load Saved Configuration Package

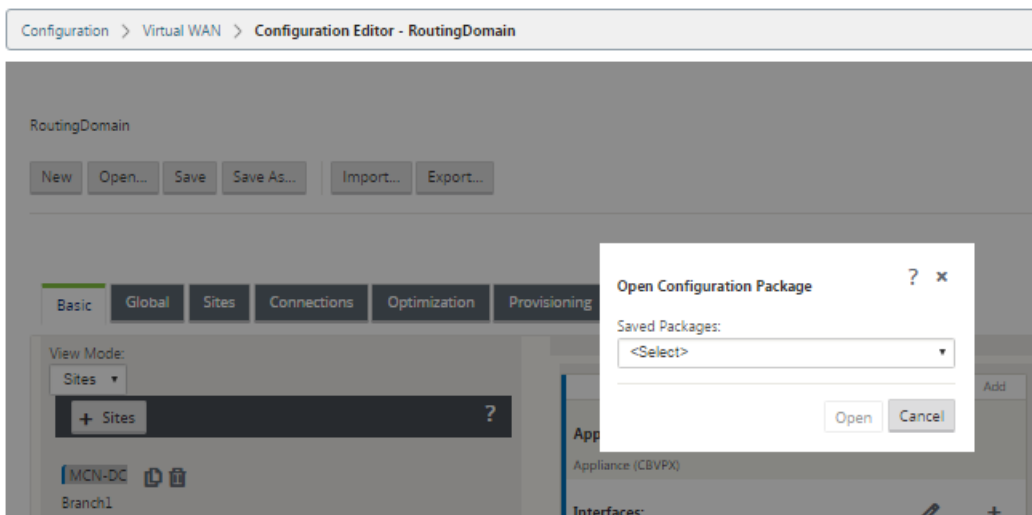
To resume work on a saved configuration package, you must first open the package and load it into the **Configuration Editor**.

To load a saved configuration package, do the following:

1. Log back into the Management Web Interface, and navigate to the **Configuration Editor**. This opens the **Configuration Editor** main page for a new session.

If you have just logged back into the Management Web Interface, the **Configuration Editor** initially opens for a new session, with no configuration package loaded. You have the option of starting a new configuration (**New**), opening an existing saved configuration (**Open**), or importing (**Import**) and then opening (**Open**) a configuration previously backed up to your local PC.

2. Click **Open**. The **Open Configuration Package** dialog box appears.



3. Select the package to open from the **Saved Packages** drop down menu.

Note

If you have just opened the **Configuration Editor**, it might take a few seconds or a minute or two for the **Saved Packages** menu to be populated, depending on the number of configurations you have saved to your workspace. If so, in the interim, the **Saved Packages** menu field might display the message **No saved packages**. If this occurs, click **Cancel** to close the dialog box, wait a few moments, and click **Open** again to reopen the dialog box.

4. Click **Open**.

Note

This opens the specified Configuration Package and loads it into the **Configuration Editor** for editing, only. This does not stage or activates the selected configuration to the local appliance.

Rename Sites

If you change the name of the MCN site in the configuration editor, you have to apply the configuration with the renamed site to the MCN and SD-WAN network. Depending on the MCN role and whether high availability is enabled or disabled, the

following scenarios are applicable for SD-WAN network configuration when renaming sites.

- MCN
- MCN with high availability
- GEO
- GEO with high availability
- RCN
- RCN with high availability

Renaming MCN site

After you rename the MCN, you have to load the new configuration with the renamed site.

To upload new configuration for renamed site:

1. From the MCN, stage network with the new configuration.
2. Download the staging configuration package for the renamed MCN.
3. Navigate to the **Local Change Management** page of the MCN.
 - a. Upload the package downloaded earlier.
 - b. Click **Next** after processing is completed.
 - c. Click **Activate**.

Note

After step 3c is complete, the change management process automatically activates the staged software for appliances (nodes) in the network.

Renaming MCN site with High Availability

After renaming the MCN for which high availability is enabled, you have to load the new configuration.

1. From the MCN, stage network with new configuration.
2. Download the staging configuration package for both the active and high availability MCN appliances with new name.
3. Disable service on the standby MCN appliance.
4. Navigate to the **Local Change Management** page of the active MCN.
 - a. Upload the package downloaded earlier.
 - i. Click **Next** when processing is complete.
 - ii. Click **Activate**.
 - b. Repeat steps 4 a,b, and c for the high availability disabled standby MCN appliance.
 - c. Enable service on the standby MCN appliance.

Note

After step 4c is complete, the change management process automatically activates the staged software for appliances in the network.

Renaming GEO site

To upload new configuration for a renamed GEO site:

1. From the MCN, stage network with new configuration containing the renamed GEO site.
2. From the MCN, download the staging configuration package for the renamed GEO site.
3. On the MCN, select **Activate Staged** for network. This deactivates the renamed site and the site becomes unavailable.
4. Navigate to the **Local Change Management** page on the GEO site.
 - a. Upload the package downloaded earlier.
 - b. Click **Next** when processing the package is complete.
 - c. Click **Activate**.

Renaming GEO site with High Availability

To upload new configuration with a renamed GEO site enabled with high availability:

1. From the MCN, stage network with new configuration containing the renamed the GEO site.
2. From the MCN, download the staging configuration package for both the active and high availability appliances with the renamed GEO site.
3. On the MCN, select **Activate Staged** for the network. This disables the renamed site and the site becomes unavailable.
4. Navigate to the active GEO appliance.
 - a. Go to the Local Change Management page.
 - b. Upload the package downloaded earlier.
 - c. Click Next when processing the package is complete.
 - d. Click Activate.
 - e. Repeat steps 4 a,b,c, and d for the standby appliance.

Renaming RCN site

To upload new configuration with renamed RCN site:

1. From the MCN, stage network with new configuration containing the renamed RCN site.
2. From the MCN, download the staging package for the renamed RCN site.

3. On the MCN, select **Activate Staged** for network. This disables the renamed RCN site and the region site becomes unavailable at the MCN. The RCN site and branches in the region communicate with each other, however until step 4 is complete the region cannot communicate with the MCN (unless there is a GEO RCN that is not renamed).
4. Navigate to the RCN's Local Change Management page:
 - a. Upload the package downloaded earlier.
 - b. Click **Next** when the package processing complete.
 - c. Click **Activate**.

Note

The branches in the region take sometime to become available since the region staging does not occur until after step 4 c is completed. This is driven automatically by the RCN's change management process.

Renaming RCN site with High Availability

To upload new configuration with renamed RCN site enabled with high availability.

1. From the MCN, stage network with new configuration containing the renamed RCN site.
2. From the MCN, download the staging package for both the active and high availability appliances with renamed RCN site. This disables the renamed RCN site and the region site becomes unavailable at the MCN. The RCN site and branches in the region communicate with each other, however until step 4 is complete the region cannot communicate with the MCN (unless there is a GEO RCN that is not renamed).
3. On the MCN, select **Activate Staged for network**.
4. Disable service on the standby RCN appliance.
5. Navigate to the active RCN's **Local Change Management** page:
 - a. Upload the package downloaded earlier.
 - b. Click **Next** when processing the package is complete.
 - c. Click **Activate**.
 - d. Repeat steps 5 a,b, and c for the disabled standby RCN appliance.
6. Enable service on the standby RCN appliance.

Renaming GEO RCN site

To upload new configuration with renamed GEO RCN site:

1. From the MCN, stage network with new configuration with renamed GEO RCN site.
2. From the MCN, download the staging package for the renamed GEO RCN site.

3. On the MCN, select **Activate Staged** for network. This disables the renamed site and the site becomes unavailable. If the primary RCN is online, the region remains connected to the network when renaming GEO RCN site.
4. Navigate to the GEO RCN's **Local Change Management** page:
 - a. Upload the package downloaded earlier.
 - b. Click **Next** when processing the package is complete.
 - c. Click **Activate**.

Renaming GEO RCN site with High Availability

1. From the MCN, stage network with new configuration with renamed GEO RCN site.
2. From the MCN, download the staging package for both the active and high availability appliance for the renamed GEO RCN site.
3. On the MCN, select **Activate Staged** for network. This disables the renamed site and the site becomes unavailable. If the primary RCN is online, the region remains connected to the network when renaming GEO RCN site.
4. Navigate to the active GEO RCN's **Local Change Management** page:
 - a. Upload the package downloaded earlier.
 - b. Click **Next** when processing the package is complete.
 - c. Click **Activate**.
 - d. Repeat steps 4 a,b, and c for the standby appliance.

Setup Branch Nodes

Mar 01, 2018

This chapter provides instructions for adding and configuring the branch sites. The procedure for adding a branch site is very similar to creating and configuring the MCN site. However, some of the configuration steps and settings do vary slightly for a branch site. In addition, once you have added an initial branch site, for sites that have the same appliance model you can use the **Clone** (duplicate) feature to streamline the process of adding and configuring those sites.

As with creating the MCN site, to set up a branch site you must use the **Configuration Editor** in the Management Web Interface on the MCN appliance. The **Configuration Editor** is available only when the interface is set to **MCN Console** mode.

Supplemental Branch Site Deployment Information

In addition to this guide, the following Knowledge Base support articles are also recommended:

- Virtual WAN PBR Mode Deployment Steps ([CTX201577](http://support.citrix.com/article/CTX201577))
<http://support.citrix.com/article/CTX201577>
- Virtual WAN Gateway Mode Deployment Steps ([CTX201576](http://support.citrix.com/article/CTX201576))
<http://support.citrix.com/article/CTX201576>

Overview of Branch Site Configuration Procedures

The steps to complete this process are as follows:

1. Add the branch site.
2. Configure the Virtual Interface Groups for the branch site.
3. Configure the Virtual IP Addresses for the branch site.
4. (Optional) Configure the LAN GRE Tunnels for the branch site.
5. Configure the WAN Links for the branch site.
6. Configure the Routes for the branch site.
7. (Optional) Configure High Availability for the branch site.
8. (Optional) Clone the new branch site to create and configure additional sites.

Note

Cloning the site is optional. The Virtual WAN appliance models must be the same for both the original and the cloned sites. You cannot change the specified appliance model for a clone. If the appliance model is different for a site, you must manually add the site.

9. Resolve any configuration Audit Alerts.

10. Save the completed configuration.

Configure Branch Node

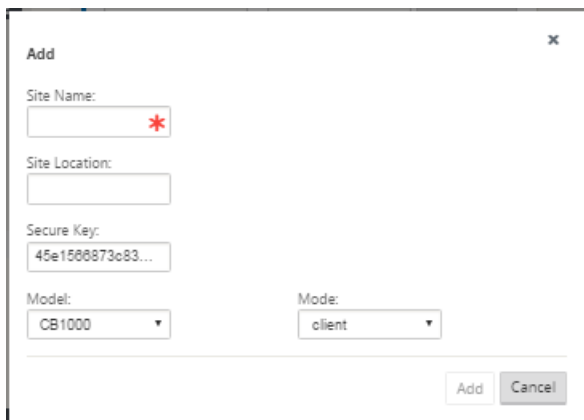
Apr 24, 2018

To add a new branch site to the **Sites** table and begin configuring the site, do the following:

Note

If you logged out of the MCN after creating and saving the new configuration package, you will need to log back in and reopen the configuration before you can continue. To do so, click **Open** in the **Configuration Editor** menu bar (top of page area). This displays a dialog box for selecting the configuration you want to change.

1. Continuing in the **Configuration Editor**, click **Add** in the **Sites** bar to begin adding and configuring the new branch site. The **Add Site** dialog box appears.

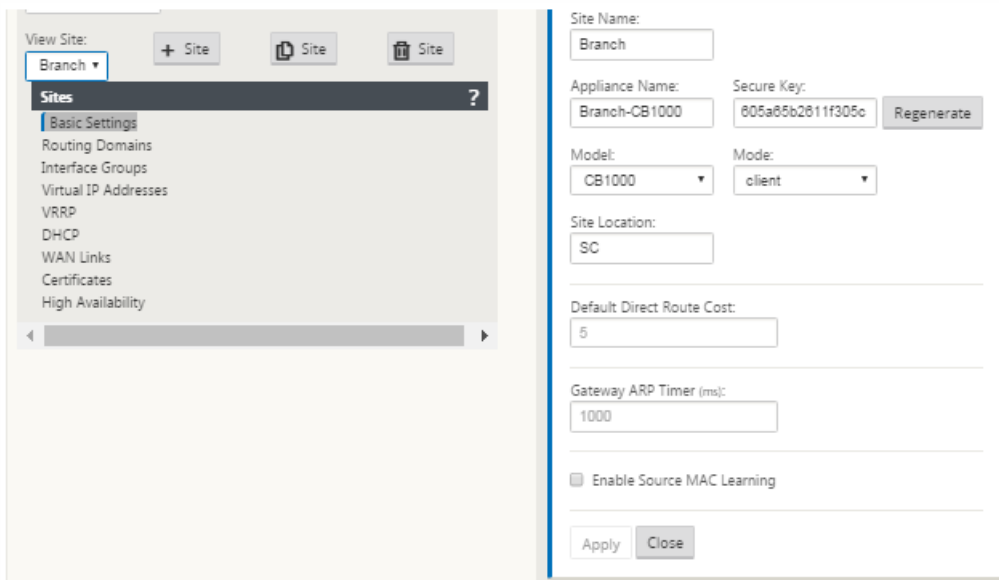


2. Type the following site information.

Note

Entries cannot contain spaces and must be in Linux format.

- Site **Name** – type a name for the site.
 - Appliance **Name** – type the name you want to assign to the appliance.
 - Secure **Key** – This is a hexadecimal key of 8–32 digits used for encryption and membership verification in the SD-WAN Appliance. By default, this field is pre-filled with an automatically generated security key. Accept the default or type a custom key-in hexadecimal format.
 - Model – Select the appliance model from the drop-down menu.
 - Mode – Select client as the mode.
3. Click **Add** to add the site. The new site is added to the **Sites** tree, and opens the **Basic Settings** configuration form for the site.



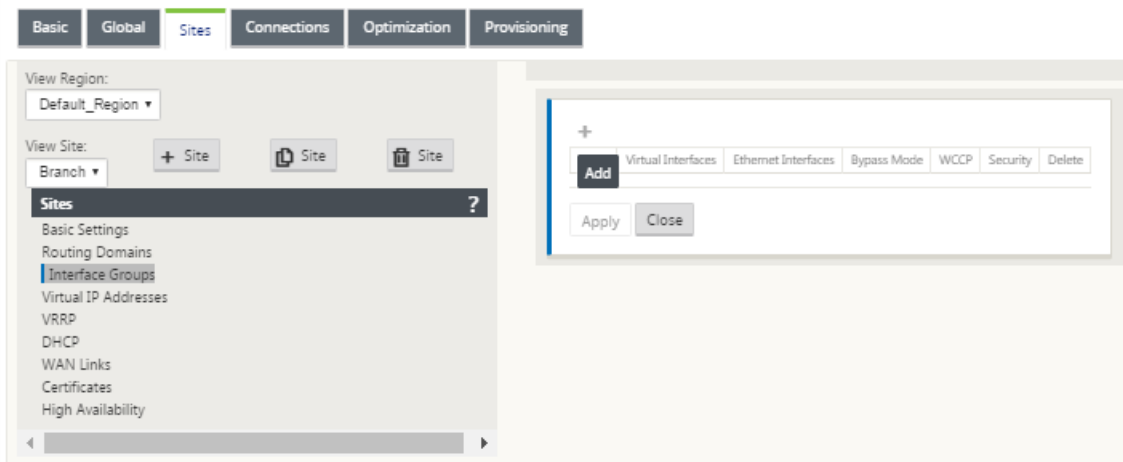
4. Type the basic settings for the site, and click **Apply**.

The next step is to add and configure the Interface Groups for the new branch site.

How to Configure Interface Groups for the Branch

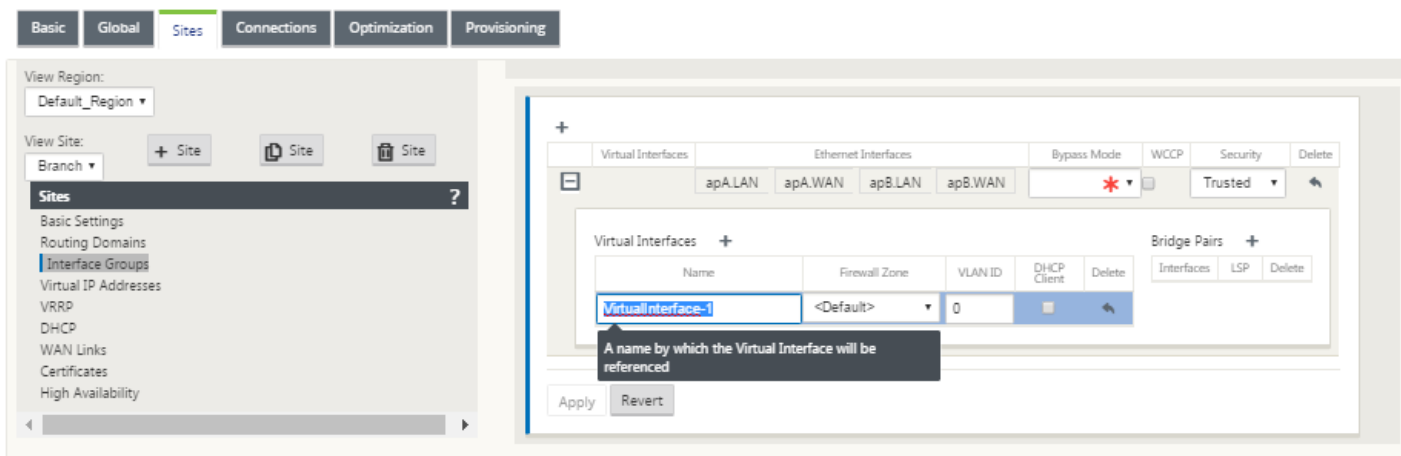
To add Interface Group to the new branch site, do the following:

1. Continuing in the **Sites** view of the **Configuration Editor**, select the branch site from the **View Site** drop down menu. This opens configuration view for the site you selected.



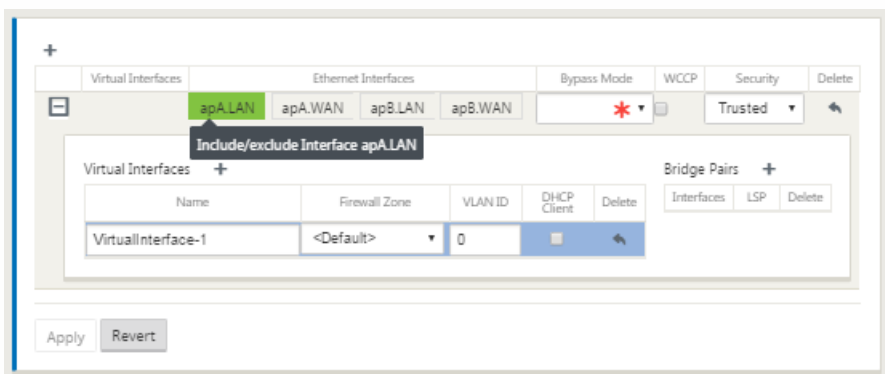
2. Click **+** to add the **Virtual Interface Group**. A new blank Virtual interface group entry is added to the table and opens for editing.

3. Click **+** to the right of **Virtual Interfaces**. A new blank group entry is added to the table and opens for editing.



4. Select the Ethernet Interfaces to include in the group.

Under **Ethernet Interfaces**, click an interface to include/exclude that interface. You can select any number of interfaces to include in the group.



5. Select the **Bypass Mode** from the drop-down menu (no default).

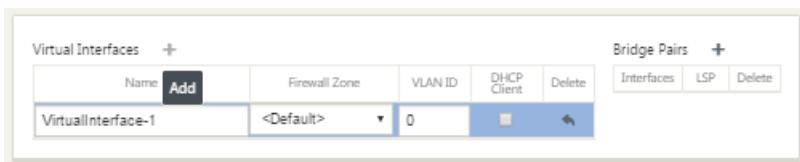
The **Bypass Mode** specifies the behavior of bridge-paired interfaces in the Virtual Interface Group, in the event of an appliance or service failure or restart. The options are: **Fail-to-Wire** or **Fail-to-Block**.

6. Select the Security Level from the drop-down menu.

This specifies the security level for the network segment of the Virtual Interface Group. The options are: **Trusted** or **Untrusted**. Trusted segments are protected by a firewall (default is Trusted).

7. Click **+** at the left edge of the Virtual Interface you added.

This displays the **Virtual Interfaces** table.



8. Click **+** to the right of **Virtual Interfaces**. The **Name**, **Firewall Zone**, and **VLAN ID** ids appear.

9. Type the **Name** and **VLAN ID** for this Virtual Interface Group.

Name – The name by which this Virtual Interface will be referenced.

Firewall Zone - Select a firewall zone from the drop-down menu.

VLAN ID – The ID for identifying and marking traffic to and from the Virtual Interface. Use an ID of 0 (zero) for native/untagged traffic.

10. Click **+** to the right of **Bridge Pairs**. A new **Bridge Pairs** entry is added and opens for editing.

11. Select the Ethernet interfaces to be paired from the drop-down menus. To add more pairs, click **+** next to **Bridge Pairs** again.

12. Click **Apply**. Your settings are applied and added to the new Virtual Interface Group of the table.

Note

At this stage, you see a yellow delta Audit Alert icon, to the right of the new Virtual Interface Group entry. This is because you have not yet configured any Virtual IP Addresses (VIPs) for the site. For now, you can ignore this alert, as it will be resolved automatically when you have properly configured the Virtual IPs for the site.

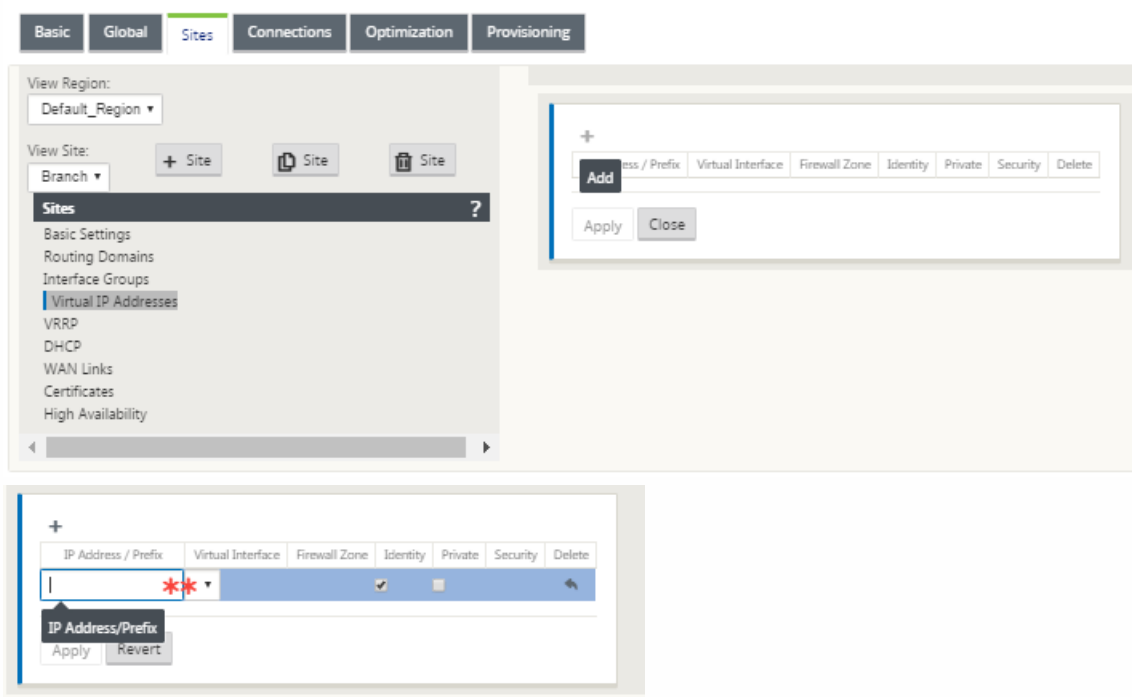
13. To add more Virtual Interface Groups, click **+** to the right of the **Interface Groups** branch, and proceed as above.

How to Configure Virtual IP Address for the Branch Site

The next step is to configure the Virtual IP Addresses for the site, and assign them to the appropriate group.

1. Continuing in the **Sites** view for the new Branch site, click **+** to the left of the **Virtual IP Addresses**. This displays the **Virtual IP Addresses** table for the new site.

2. Click **+** to the right of **Virtual IP Addresses** to add an address. The form for adding and configuring a new Virtual IP Address appears.



3. Type the **IP Address / Prefix** information, and select the **Virtual Interface** with which the address is associated. The Virtual IP Address must include the full host address and netmask.

4. Select the desired settings for the Virtual IP address; such as the Firewall Zone, Identity, Private, and Security.

5. Click **Apply**. The address information to the site is added and includes it in the site **Virtual IP Addresses** table.

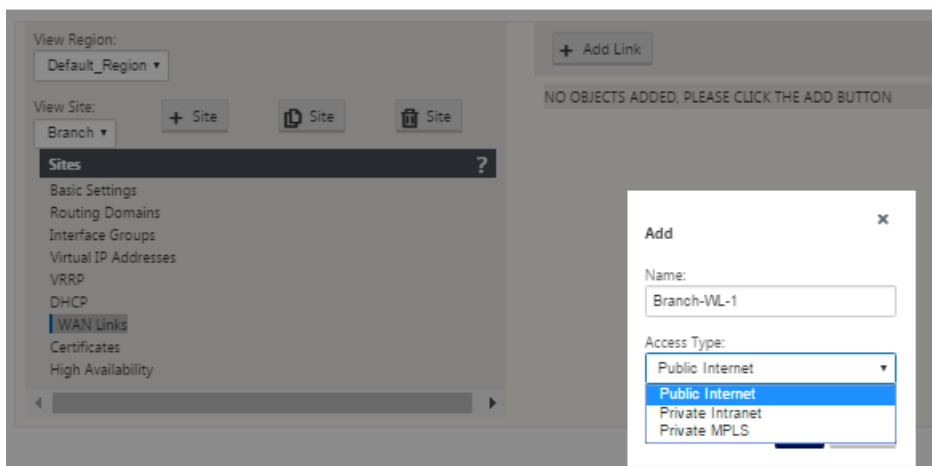
6. To add more Virtual IP Addresses, click **+** to the right of the **Virtual IP Addresses**, and proceed as above.

How to Configure WAN Links for the Branch

The next step is to configure the WAN links for the site.

1. Continuing in the **Sites** view for the new Branch site, click the **WAN Links** label.

2. Click **Add Link** to the right of the **WAN Links** to add a new WAN link. The **Add** dialog box appears.



3. (Optional) type a name for the WAN Link if you do not want to use the default.

The default is the site name, appended with the following suffix:

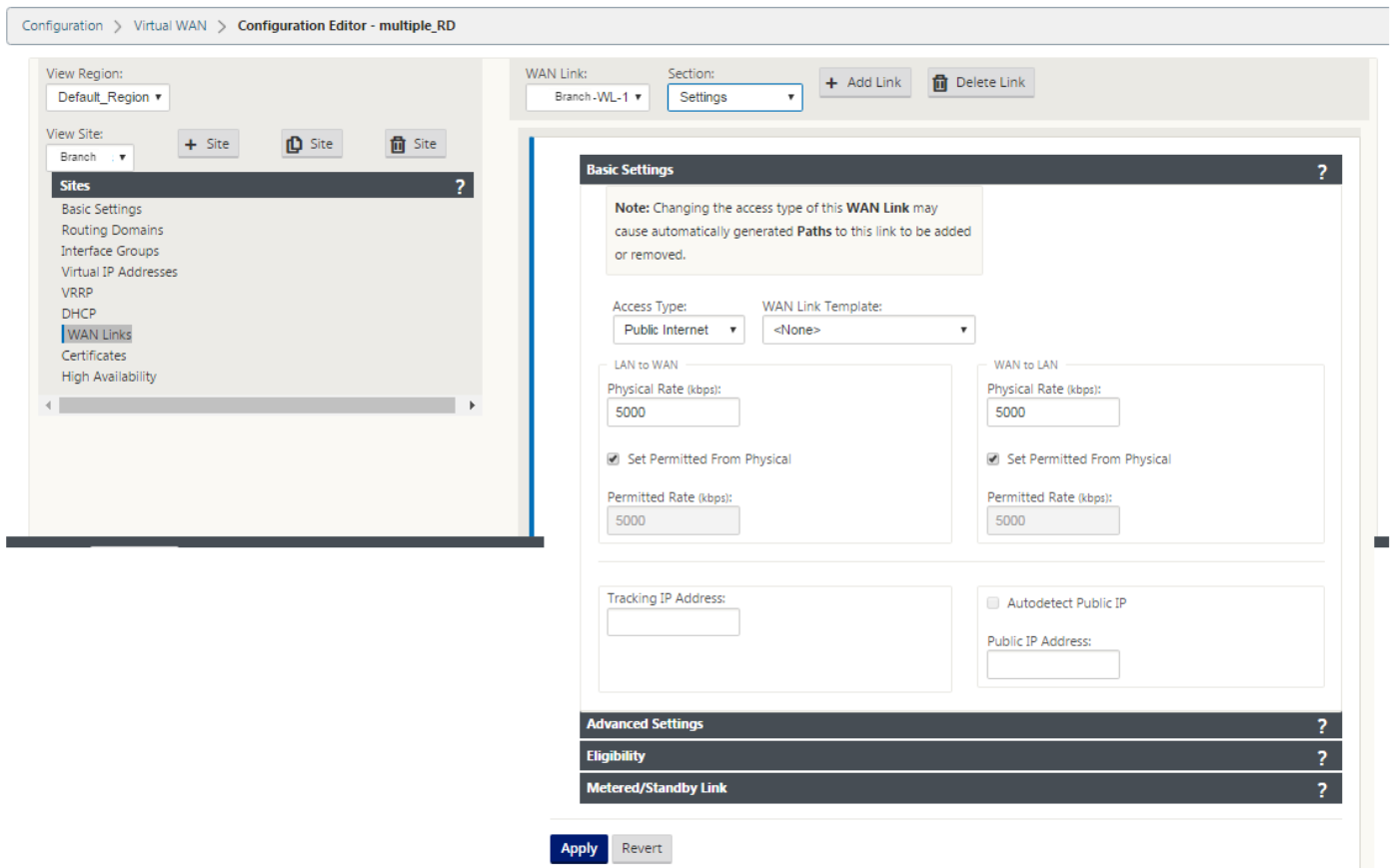
-WL-<number>

Where <number> is the number of WAN Links for this site, incremented by one.

4. Select the **Access Type** from the drop-down menu.

The options are **Public Internet**, **Private Intranet**, or **Private Multiprotocol Label Switching**.

5. Click **Add**. The **WAN Links** Basic Settings configuration page appears and adds the new unconfigured WAN link to the page.

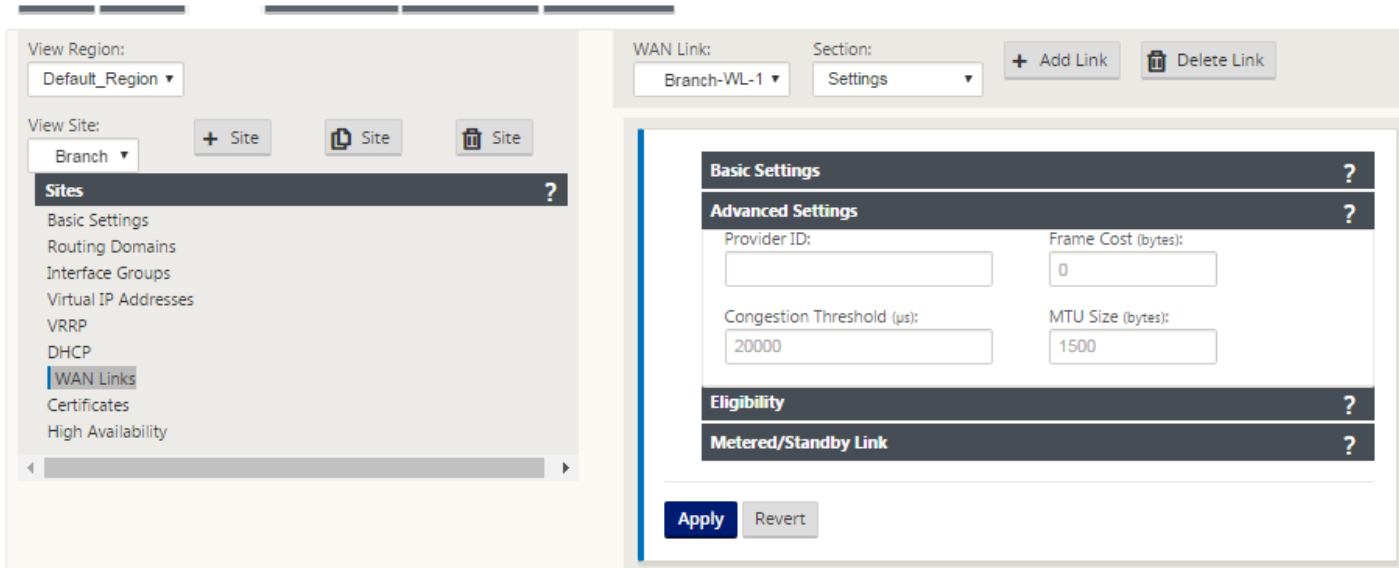


6. Type the link details for the new WAN link. Configure the LAN to WAN, WAN to LAN settings.

Some guidelines are as follows:

- Some Internet links might be asymmetrical.
- Misconfiguring the permitted speed can adversely affect performance for that link.
- Avoid using burst speeds that surpass the Committed Rate.
- For Internet WAN links, be sure to add the Public IP Address.

7. Click the gray **Advanced Settings** section bar. This opens the **Advanced Settings** form for the link.



8. Type the **Advanced Settings** for the link.

- Provider **ID** – (Optional) type a unique ID number 1–100 to designate WAN Links connected to the same service provider. Virtual WAN uses the Provider ID to differentiate paths when sending duplicate packets.

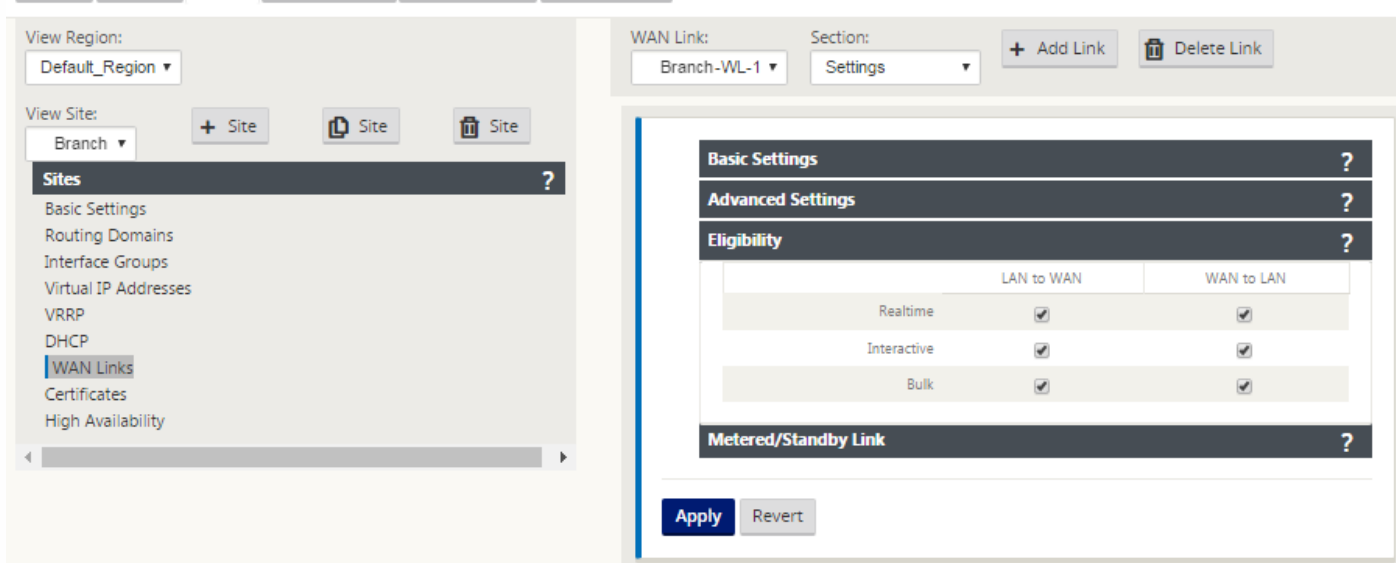
- Frame **Cost (bytes)** – type the size (in bytes) of the header/trailer added to each packet. For example, the size in bytes of added Ethernet IPG or AAL5 trailers.

- Congestion **Threshold** – type the congestion threshold (in microseconds) after which the WAN link throttles packet transmission to avoid further congestion.

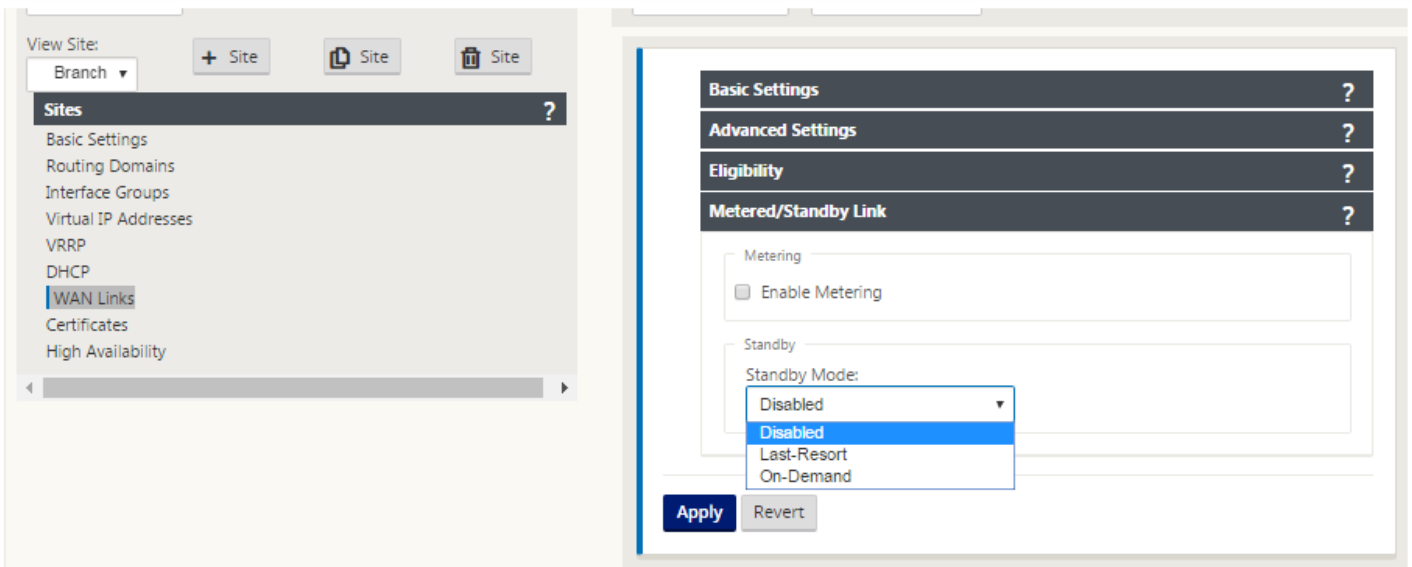
- MTU **Size (bytes)** – type the largest raw packet size (in bytes), not including the Frame Cost.

9. Click the gray **Eligibility** section bar. This opens the **Eligibility** settings form for the link.

10. Select the **Eligibility** settings for the link.



11. Click the gray **Metered Link** section bar. This opens the **Metered Link** settings form for the link.
12. (Optional) Select **Enable Metering** to enable metering for this link. This displays the **Enable Metering** settings fields.



Metering

Enable Metering

Data Cap (MB):

Billing Cycle:

Starting From:

Standby

Standby Mode:

Heartbeat Interval

Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.

Active Heartbeat Interval:

13. Configure the metering settings for the link.

Type the following:

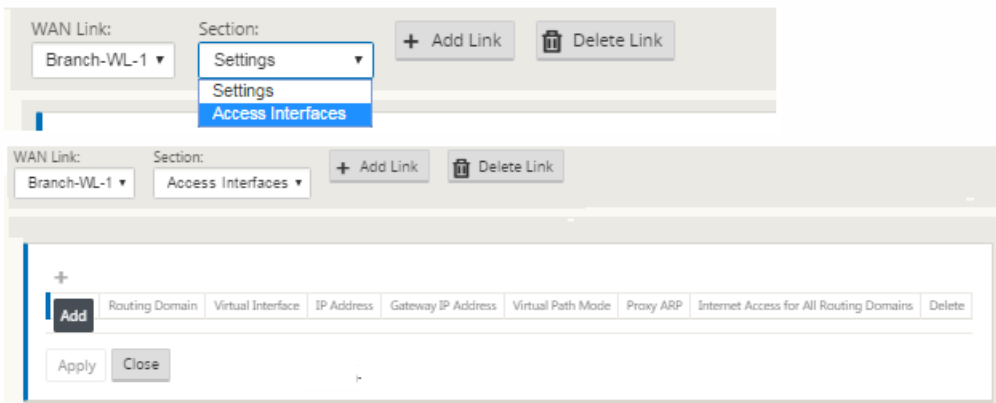
- **Data Cap (MB)** – type the data cap allocation for the link, in MB.
- **Billing Cycle** – Select either Monthly or Weekly from the drop-down menu.
- **Starting From** – type the start date of the billing cycle.
- **Set Last Resort** – Select this to enable this link as a link of last resort in the event of a failure of all other available links. Under normal WAN conditions, Virtual WAN sends only minimal traffic over metered links, for checking link status. However, in the event of a failure, SD-WAN can use active metered links as a last resort for forwarding production traffic.

14. Click **Apply**. This applies your specified settings to the new WAN link.

The next step is to configure the Access Interfaces for the new WAN link. An Access Interface consists of a Virtual Interface, WAN endpoint IP Address, Gateway IP Address, and Virtual Path Mode defined collectively as an interface for a

specific WAN link. Each WAN link must have at least one Access Interface.

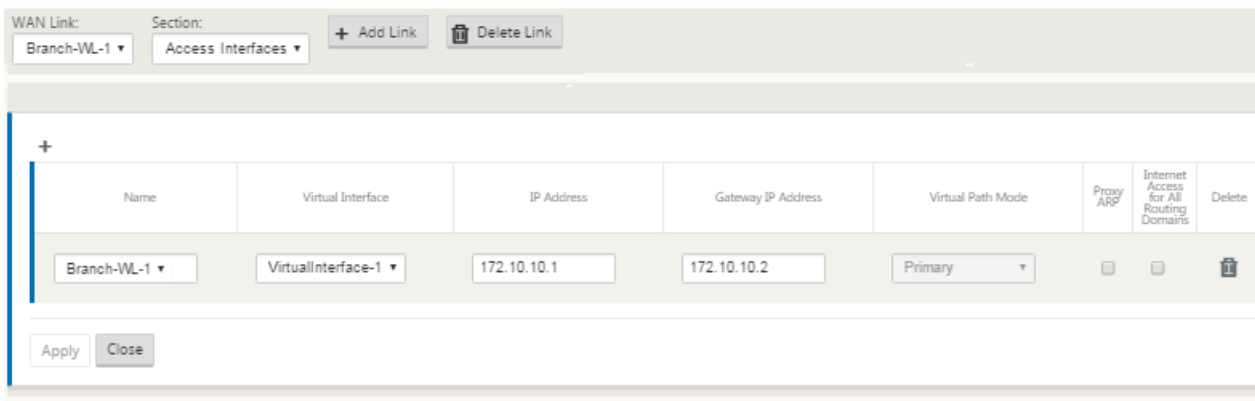
15. Select **Access Interfaces** in the WAN Link configuration page for the link. This opens the **Access Interfaces** view for the site.



16. Click + to add an interface. A blank entry to the table is added and opens for editing. Type the **Access Interfaces** settings for the link.

Note

Each WAN link must have at least one Access Interface.



17. Type the following:

- Name – This is the name by which this Access Interface will be referenced. Type a name for the new Access Interface, or accept the default. The default uses the following naming convention:

WAN_link_name-AI-number

Where *WAN_link_name* is the name of the WAN link you are associating with this interface, and number is the number of Access Interfaces currently configured for this link, incremented by 1.

Note

If the name appears truncated, you can place your cursor in the field, then click and hold and roll your mouse right or left to see the truncated portion.

- **Virtual Interface** – The Virtual Interface this Access Interface uses. Select an entry from the drop-down menu of Virtual Interfaces configured for this branch site.

- **IP Address** – The IP Address for the Access Interface endpoint from the appliance to the WAN.

- **Gateway IP Address** – This is the IP Address for the gateway router.

- **Virtual Path Mode** – The priority for Virtual Path traffic on this WAN link. The options are: **Primary**, **Secondary**, or **Exclude**. If set to **Exclude**, this Access Interface is used for Internet and Intranet traffic, only.

- **Proxy ARP** – Select the checkbox to enable. If enabled, the Virtual WAN Appliance replies to ARP requests for the Gateway IP Address, when the gateway is unreachable.

18. Click **Apply**.

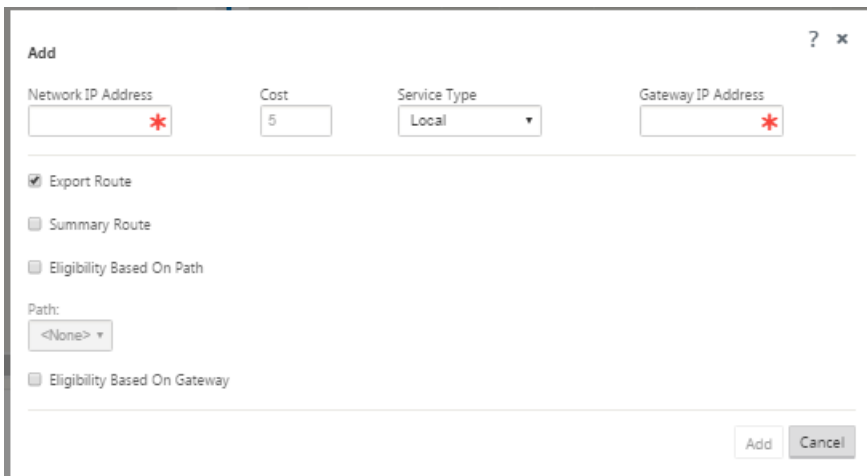
You have now finished configuring the new WAN link. Repeat these steps to add and configure extra WAN links for the site.

The next step is to add and configure the routes for the site.

How to Configure Routes for the Branch

To add and configure the routes for the site, do the following:

1. Click the **Connections** view for the new Branch site and select **Routes**. This displays the **Routes** view for the site.
2. Click **+** to the right of **Routes** to add a route. This opens the **Routes** dialog box for editing.



The screenshot shows a dialog box titled "Add" with the following fields and options:

- Network IP Address: [Empty field with a red asterisk]
- Cost: [5]
- Service Type: [Local]
- Gateway IP Address: [Empty field with a red asterisk]
- Export Route:
- Summary Route:
- Eligibility Based On Path:
- Path: [<None>]
- Eligibility Based On Gateway:
- Buttons: Add, Cancel

3. Type the route configuration information for the new route.

Type the following:

- **Network IP Address** – type the Network IP Address.

- **Cost** – type a weight from 1 to 15 for determining the route priority for this route. Lower-cost routes take precedence over higher-cost routes. The default value is 5.

- **Service Type** – Select the service type for the route from the drop-down menu for this field. The options are as follows:

* **Virtual Path** – This service manages traffic across the Virtual Paths. A Virtual Path is a logical link between two WAN links. It comprises a collection of WAN Paths combined to provide high service-level communication between two SD-WAN nodes. This is done by constantly measuring and adapting to changing application demand and WAN conditions. SD-WAN Appliances measure the network on a per-path basis. A Virtual Path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN Appliances reaches a configured threshold).

* **Internet** – This service manages traffic between an Enterprise site and sites on the public Internet. Traffic of this type is not encapsulated. During times of congestion, the SD-WAN actively manages bandwidth by rate-limiting Internet traffic relative to the Virtual Path, and Intranet traffic according to the SD-WAN configuration established by the Administrator.

* **Intranet** – This service manages Enterprise Intranet traffic that has not been defined for transmission across a Virtual Path. As with Internet traffic, it remains unencapsulated, and the SD-WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Under certain conditions, and if configured for Intranet Fallback on the Virtual Path, traffic that ordinarily travels with a Virtual Path can instead be treated as Intranet traffic, to maintain network reliability.

* **Passthrough** – This service manages traffic that is to be passed through the Virtual WAN. Traffic directed to the Passthrough Service includes broadcasts, ARPs, and other non-IPv4 traffic, and traffic on the Virtual WAN Appliance local subnet, configured subnets, or Rules applied by the Network Administrator. This traffic is not delayed, shaped, or changed by the SD-WAN. Therefore, you must ensure that Passthrough traffic does not consume substantial resources on the WAN links that the SD-WAN Appliance is configured to use for other services.

* **Local** – This service manages IP traffic local to the site that matches no other service. SD-WAN ignores traffic sourced and destined to a local route.

* **GRE Tunnel** – This service manages IP traffic destined for a GRE tunnel, and matches the LAN GRE tunnel configured at the site. The GRE Tunnel feature enables you to configure SD-WAN Appliances to end GRE tunnels on the LAN. For a route with service type GRE Tunnel, the gateway must reside in one of the tunnel subnets of the local GRE tunnel.

* **LAN IPsec Tunnel** – This service manages IP traffic destined for IPsec tunnel.

- **Gateway IP Address** – type the Gateway IP Address for this route.

- **Eligibility Based on Path** (checkbox) – (Optional) If enabled, the route will not receive traffic when the selected path is down.

- **Path** – This specifies the path to be used for determining route eligibility.

4. Click **Apply**.

Note

After you click **Apply**, audit warnings might appear indicating that further action is required. A red dot or goldenrod delta icon indicates an error in the section where it appears. You can use these warnings to identify errors or missing configuration information. Roll your cursor over an audit warning icon to display a short description of the errors in that section. You can also click the dark gray **Audits** status bar (bottom of page) to display a complete list of all audit warnings.

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	0.0.0.0/0	5	Virtual Path	Branch1		ⓘ	✎	🗑️
2	172.147.21.52/24	5	Local			ⓘ	✎	🗑️
3	172.147.22.52/24	5	Local			ⓘ	✎	🗑️
4	0.0.0.0/0	65535	Passthrough			ⓘ	✎	🗑️

You can also edit configured routes as shown below.

Edit ? x

Network IP Address: 172.147.61.0/24

Cost: 5

Service Type: Intranet

Gateway IP Address: [Empty]

Export Route

Intranet Service: Intranet

Eligibility Based On Path

Path: Branch1-WL-2->MCN-DC-WL-1

Eligibility Based On Tunnel

Apply Cancel

You have now completed the required steps for configuring a client site. There are also some additional, optional steps you can choose to complete, before proceeding with the next phase of the deployment. A list of these steps and links to instructions are provided below. If you do not want to configure these features now, you can proceed directly to [Preparing the SD-WAN Appliance Packages on the MCN](#).

The optional steps are as follows:

- **Configure High Availability** – High Availability is a configuration in which two Virtual WAN Appliances at a site serve in an Active/Standby partnership capacity for redundancy purposes. If you are not implementing High Availability for this site, you can skip this step. For instructions, see [Configuring High Availability \(high availability\) for the Branch Site \(Optional\)](#).
- **Clone the new branch site** – You have the option of cloning the branch site you just configured, and using that as a template for adding another site. The appliance models for the original site and the clone must be the same. For instructions, see [Cloning the Branch Site \(Optional\)](#).
- **Configure WAN Optimization** – If your NetScaler SD-WAN Virtual WAN license includes WAN Optimization features, you have the option of enabling and adding these features to your configuration. To do so, you must complete the **Optimization** section in the **Configuration Editor**, and save the changed configuration.

Save Configuration

The next step is to save the completed Sites configuration. The configuration is saved to your workspace on the local

appliance.

Warning

If the console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes are lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is recommended that you save the configuration package often, or at key points in the configuration.

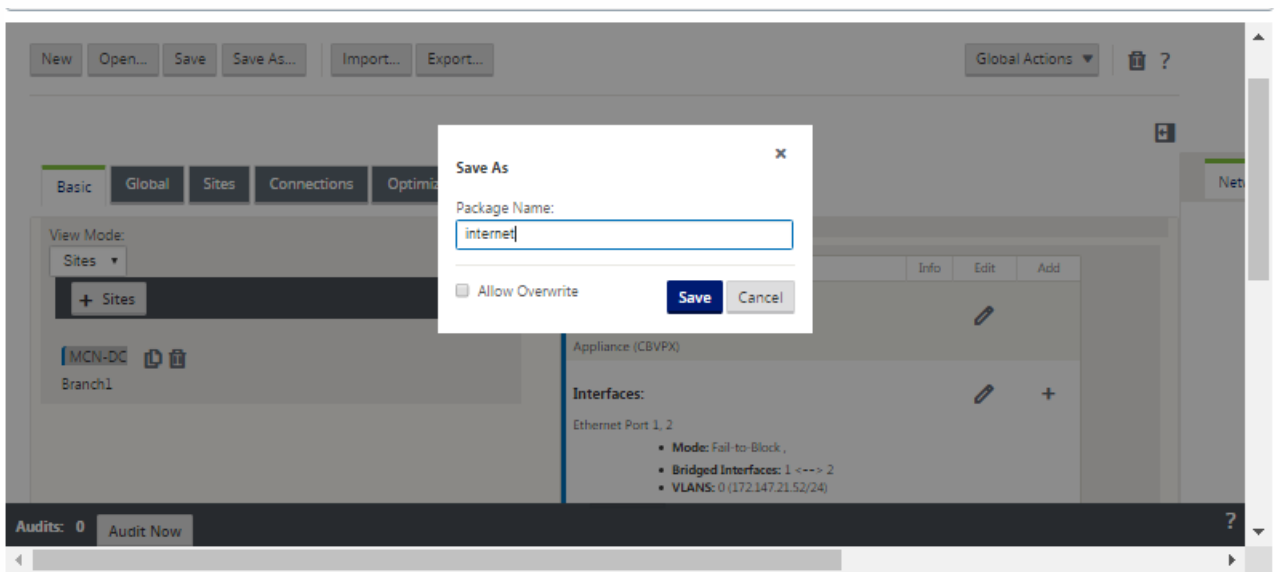
Note

As an extra precaution, it is recommended that you use **Save As**, rather than **Save**, to avoid overwriting the wrong configuration package.

After saving the configuration file, you have the option to log out of the Management Web Interface and continue the configuration process later. However, if you log out, you need to reopen the saved configuration when you resume. Instructions are provided in the section under Configure MCN; [Loading a Saved Configuration Package into the Configuration Editor](#).

To save the current configuration package, do the following:

1. Click **Save As** (at the top of the **Configuration Editor** middle pane). This opens the **Save As** dialog box.



2. Type the configuration package name. Click **Save**.

Note

If you are saving the configuration to an existing configuration package, be sure to select **Allow Overwrite** before saving.

The next step is to configure the Virtual Paths and Virtual Path Service between the MCN and the client sites. Instructions are provided in the [Configuring the Virtual Path Service between the MCN and Client Sites](#).

Renaming Branch Site

After renaming the branch site, you need to upload new configuration package to the network.

1. From the MCN, stage network with new configuration containing the renamed branch site.
2. Download the staging package for the renamed branch site.
3. On the MCN, select **Activate Staged** network. This disables the renamed site and the site becomes unavailable.
4. Navigate to the branch **Local Change Management** page.
5. Upload the package downloaded earlier. Click **Next** and then click **Activate**.

Renaming Branch Site with High Availability

To upload new configuration after renaming a branch site enabled with high availability:

1. From the MCN, stage network with new configuration that contains the renamed branch site.
2. Download the staging package for both the active and high availability appliance with renamed branch site.
3. On the MCN, select **Activate Staged** for network. This disables the renamed site and the site becomes unavailable.
4. Navigate to the active appliance at the branch. Go to the **Local Change Management** page.
 - a. Upload the package downloaded earlier. Click **Next** and then click **Activate**.
 - b. Repeat steps 4a and 4b for the standby appliance.

Clone a Branch Site (Optional)

Mar 01, 2018

This section provides instructions for cloning the new branch site for use as a partial template for adding more branch sites.

Note

Cloning the site is optional. The Virtual WAN appliance models must be the same for both the original and the cloned sites. You cannot change the specified appliance model for a clone. If the appliance model is different for a site, you must manually add the site, as instructed in the previous sections.

Cloning a site streamlines the process of adding and configuring additional branch nodes. When a site is cloned, the entire set of configuration settings for the site are copied and displayed in a single form page. You can then modify the settings according to the requirements of the new site. Some of the original settings can be retained, where applicable. However, most of the settings must be unique for each site.

To clone a site, do the following:

1. In the **Sites** tree (middle pane) of the **Configuration Editor**, click the branch site you want to duplicate.

This opens that site branch in the **Sites** tree, and reveals the Clone button (double page icon) and Delete button (trashcan icon).

2. Click the **Clone** icon to the right of the branch site name in the tree.

This opens the **Clone Site** configuration page.

Clone x

Please review the following fields and make the appropriate changes for the new Site.

Site Name: ! Appliance Name: Mode: Secure Key: Region:

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
VirtualInterface-1	0	<input type="checkbox"/>
VirtualInterface-2	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	VirtualInterface-1	172.110.0.5/24 !
<input checked="" type="checkbox"/>	VirtualInterface-2	192.110.0.5/24 !

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type		
<input checked="" type="checkbox"/>	BR1-WL-1 !			
Access Interfaces				
<input checked="" type="checkbox"/>	BR1-WL-1-AI-1	VirtualInterface-1	172.110.0.5 !	172.110.0.1 !
<input checked="" type="checkbox"/>	BR1-WL-2 !			
Access Interfaces				
<input checked="" type="checkbox"/>	BR1-WL-2-AI-1	VirtualInterface-2	192.110.0.6 !	192.110.0.1 !

GRE Tunnels

Include	Name	Source IP	Destination IP	Tunnel IP / Prefix
---------	------	-----------	----------------	--------------------

3. Enter the configuration parameter settings for the new site.

A pink field with an Audit Alert icon (red dot) indicates a required parameter setting that must have a value different than the setting for the original cloned site. In most cases, this value must be unique.

Tip

To further streamline the cloning process, use a consistent, pre-defined naming convention when naming the clones.

4. Resolve any Audit Alerts.

To diagnose an error, roll your cursor over the Audit Alert icon (red dot or goldenrod delta) to reveal bubble help for that specific alert.

5. Click **Clone** (far right corner) to create the new site and add it to the **Sites** table.

Note

The **Clone** button remains unavailable until you have entered all of the required values, and the new site configuration is error-free.

6. (Optional.) Save your changes to the configuration.

Note

As an extra precaution, it is recommended that you use **Save As**, rather than **Save**, to avoid overwriting the wrong configuration package. Be sure to select **Allow Overwrite** before saving to an existing configuration, or your changes will not be saved.

Repeat the steps up to this point for each branch site you want to add.

After you have finished adding all of the sites, the next step is to check the configuration for Audit Alerts, and make corrections or additions as needed.

Auditing Branch Configuration

Mar 01, 2018

An Audit Alert icon (a red dot or goldenrod delta) next to an item indicates a configuration error or missing parameter information for that item. A number next to the icon indicates the number of associated errors for that alert. To see bubble help for a particular alert, roll your cursor over the alert icon. This displays a brief description of the specific errors flagged by that alert. You must resolve all Audit Alerts in the configuration, or you will not be able to verify, stage, and activate the configuration package, later in the deployment process.

Resolving all of the Audit Alerts (if any), completes the **Sites** phase of the configuration. The next step is to save the completed **Sites** configuration.

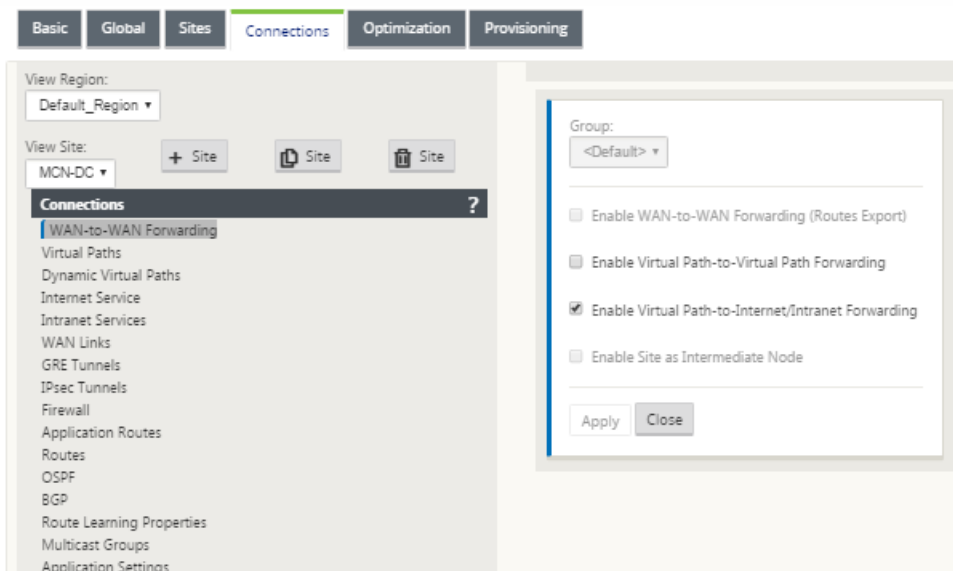
Configuring the Virtual Path Service Between the MCN and Client Sites

Mar 01, 2018

The next step is to configure the Virtual Path Service between the MCN and each of the client (branch) sites. To do this, you will use the configuration forms and settings available in the **Connections** section configuration tree of the **Configuration Editor**.

To configure the Virtual Path Service between the MCN and a client site, do the following:

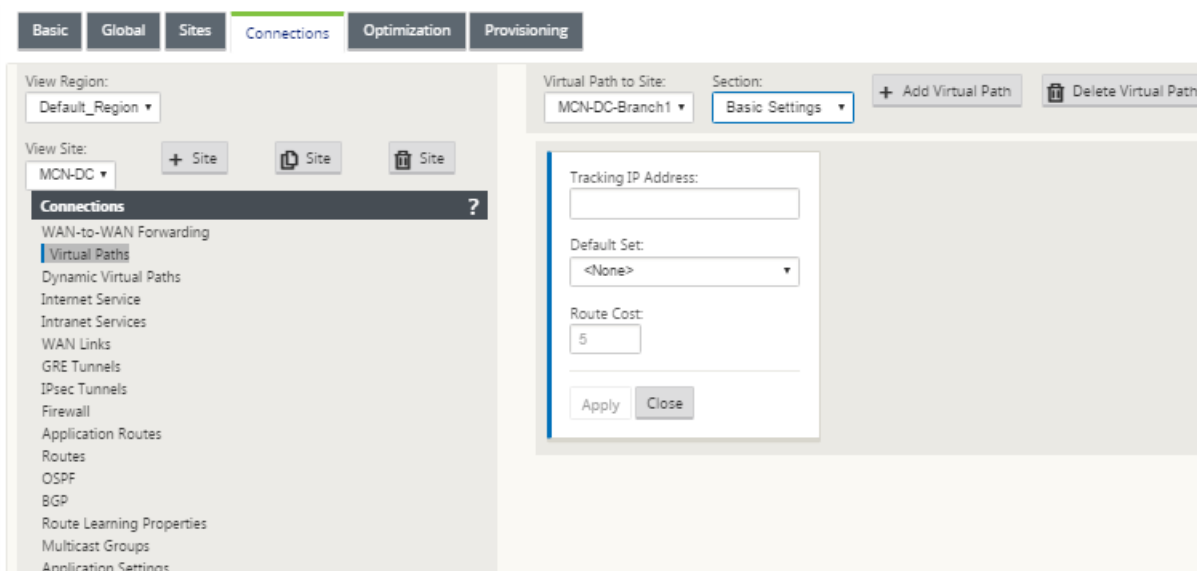
1. Continuing in the **Configuration Editor**, click the **Connections** tab. This displays the **Connections** section configuration tree.
2. Select the MCN from **View Site** drop-down menu in the **Connections** section page. This opens the MCN site in the **Connections** configuration.



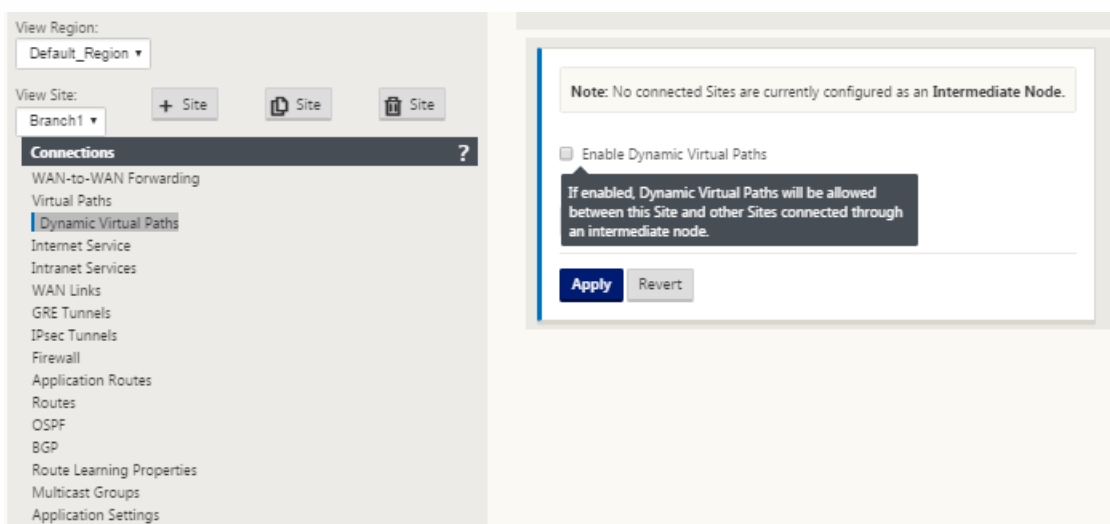
Note

WAN to WAN Forwarding Groups are supported only within a Region and not across Regions. You can use Regions to segregate networks instead of relying on WAN to WAN forwarding groups.

3. Click **Virtual Paths**. This opens the Virtual Paths configuration section (child branch) for the MCN site. This section provides settings and forms for configuring the Virtual Path Service between the MCN and each of the Virtual WAN client sites. The below figure shows an example Virtual Paths section for an MCN site.



The below figure shows an example **Dynamic Virtual Paths** section for a Branch site.



The Dynamic Virtual Paths section allows configuring the following:

- **Dynamic Virtual Paths** – (Optional) The settings in this section allow you to enable and disable Dynamic Virtual Paths, and set the maximum allowable Dynamic Virtual Paths for the site. Dynamic Virtual Paths are Virtual Paths that are established directly between sites, based on a configured threshold. The threshold is typically based on the amount of traffic occurring between those sites. Dynamic Virtual Paths are operational only after the specified threshold is reached. Dynamic Virtual Paths are not required for normal operation, so configuring this section is optional.

- **<MCN_Site_Name>_<Branch_Site_Name>** – The system initially automatically adds a static Virtual Path between the MCN and a client site, as this Virtual Path is required. The name for the path uses the following form:

<MCN_Site_Name>_<Branch_Site_Name>

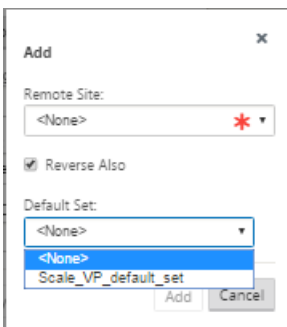
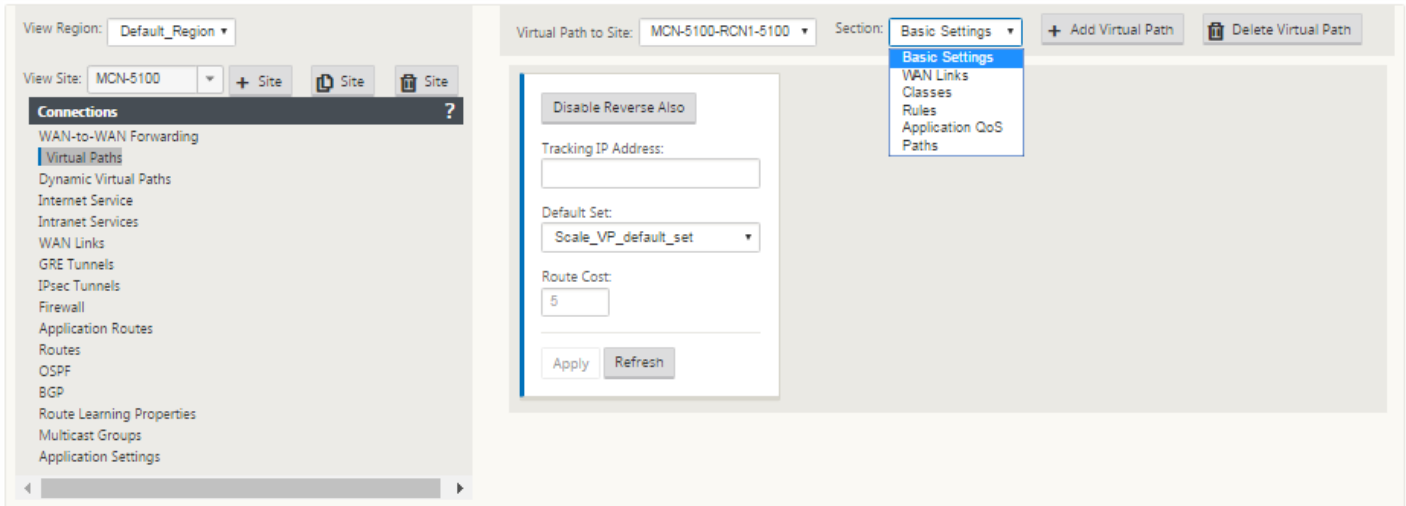
Where:

- * *MCN_Site_Name* is the name of the MCN for this Virtual WAN.
- * *Branch_Site_Name* is the name of a client site identified in the current configuration package.

User configurable default settings are initially applied to the static Virtual Path, as defined in the **Virtual Path** -> **Default Sets** section of the **Connections** configuration tree. However, you can customize or add to the defined **Default Sets**, and also customize the configuration for a specific site and Virtual Path.

Note

To add more static Virtual Paths for a site, you must do so manually. Instructions for manually adding a static Virtual Path are included in the steps below.



4. Click **+ Add Virtual Path** next to the name of the static Virtual Path in the **Virtual Paths** section.

This reveals additional configuration for the static Virtual Path:

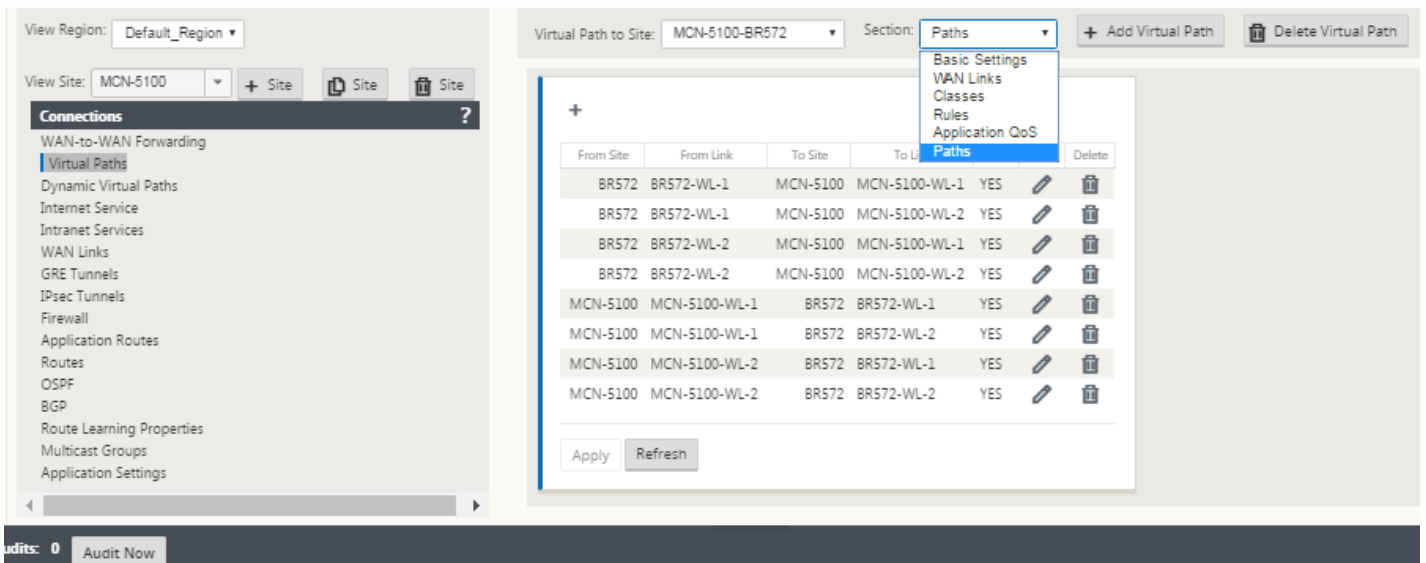
- **Remote Site** – This section enables you to view and configure the Virtual Path settings from the perspective of a remote site. You can view, customize, and add **Class** or **Rules** as required for this specific Virtual Path. You can also add Virtual Paths to the remote site, as needed.

- **Reverse Also** - When enabled, classes and rules will be mirrored on both sites the virtual path.

- **Default Set** - Name of the Virtual Path default set that will be used to populate rules and classes for the virtual path on the site.

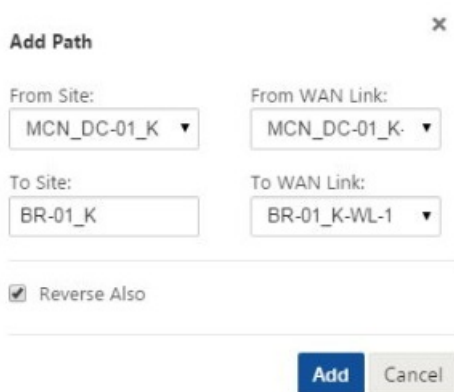
The below figure shows an example MCN static Virtual Path branch and child branches.

5. Select **Paths** from the Section drop-down menu.



6. Click + (Add) above the Paths table.

This displays the Add Path dialog box (configuration form).



7. Specify the source and destination site information for the new Virtual Path.

Specify the following from the available drop-down menus:

Note

Depending on how the WAN links are configured for the sites, some fields will be read-only. Fields that are configurable provide a drop-down menu of the available selections.

- **From Site** – This is the source site for the Virtual Path. For the required static Virtual Path, this is configured as the MCN site by default.
- **From WAN Link** – This is the originating WAN Link for the Virtual Path.
- **To Site** – This is the destination site for the Virtual Path.
- **To WAN Link** – This is the destination WAN link for the Virtual Path.

8. Click **Add**.

This adds the configured Virtual Path to both the MCN and the associated client site in the **Connections > Virtual Paths** tree. This also automatically opens the **Paths** settings configuration form for the **From Site** for the Virtual Path (in this case, the MCN).

From Site	From Link	To Site	To Link	Auto	Edit	Delete
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-2	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-2	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-2	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-2	YES		

Apply Refresh

9. Click Edit (pencil icon), to the right of the MCN-to-client Virtual Path label.

This opens the Virtual Path Service configuration form for editing.

10. Configure the settings for the Virtual Path, or accept the defaults.

The **Paths** configuration form contains the following settings:

- **From Site** section:

* **Site** – This is the source site for the Virtual Path. For the required static Virtual Path, this is configured as the MCN site by default.

* **WAN Link** – This is the originating WAN Link for the Virtual Path.

- **To Site** section:

* **Site** – This is the destination site for the Virtual Path.

* **WAN Link** – This is the destination WAN link for the Virtual Path.

- **Reverse Also** – Select this checkbox to enable Reverse Also for this Virtual Path. If enabled, the system automatically builds a Virtual Path in the opposite direction of the configured path, using the same WAN links as configured for the original path.

- **IP DSCP Tagging** – Select a tag from the drop-down menu. This specifies the DSCP tag to set in the IP header for traffic traveling over this Virtual Path.

- **Enable Encryption** – Select this checkbox to enable encryption of packets sent along this Virtual Path.

- **Bad Loss Sensitive** – Select a setting from the drop-down menu. The options are:

* **Enable**– (Default) If enabled, paths will be marked **BAD** due to loss, and will incur a path scoring penalty.

* **Disable** – Disabling **Bad Loss Sensitive** can be useful when the loss of bandwidth is intolerable.

* **Custom** – Select Custom to specify the percentage of loss over time required to mark a path as BAD. Selecting this option reveals the following additional settings:

- . **Percent Loss (%)** – This specifies the percentage of loss threshold before a path is marked BAD, as measured over the specified time. By default, the percentage is based on the last 200 packets received.

- . **Over Time (ms)** – Specify the time period (in milliseconds) over which to measure packet loss. Select an option between 100 and 2000 from the drop-down menu for this field.

- **Silence Period (ms)** – This specifies the duration (in milliseconds) before the path state transitions from **GOOD** to **BAD**. The default is 150 milliseconds. Select an option between 150 and 1000 from the drop-down menu for this field.

- **Path Probation Period (ms)** – This specifies the wait time (in milliseconds) before a path transitions from **BAD** to **GOOD**. Select an option between 500 and 60000 from the drop-down menu for this field. The default is 10000 milliseconds.

- **Instability Sensitive** – Select this checkbox to enable. If enabled, latency penalties due to a path state of **BAD** and other latency spikes are considered in the path scoring algorithm.

- **Tracking IP Address** – Enter a Virtual IP Address on the Virtual Path that can be pinged to determine the state of the path.

- **Reverse Tracking IP Address** – If **Reverse Also** is enabled for the Virtual Path, enter a Virtual IP Address on the path that can be pinged to determine the state of the reverse path.

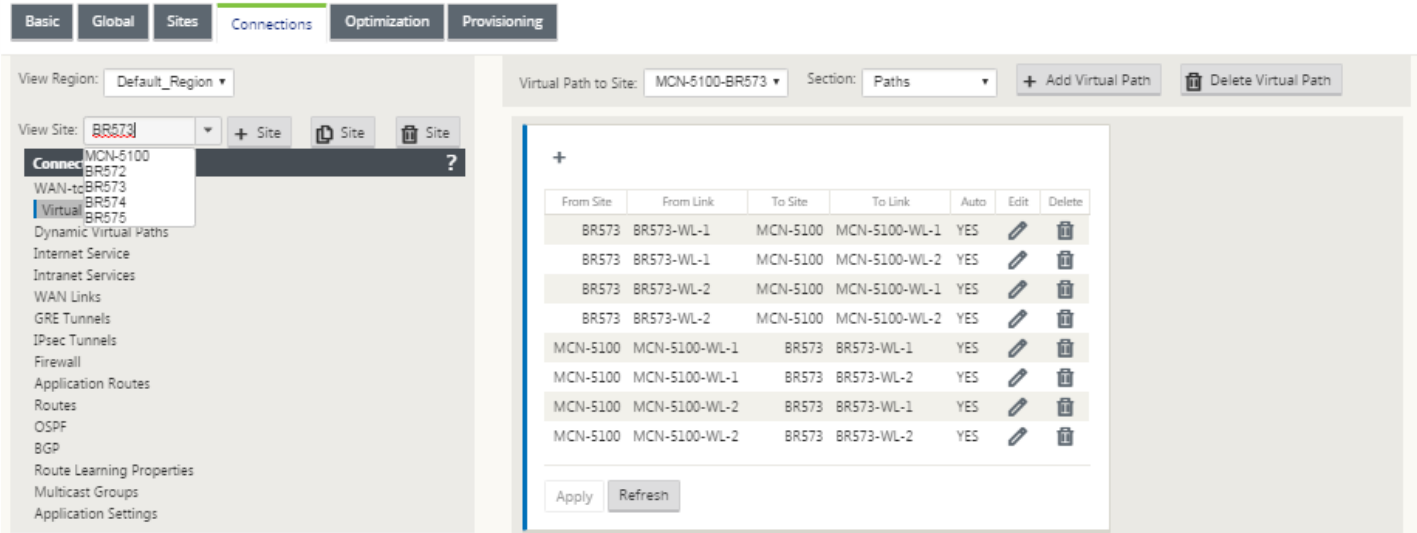
11. Click **Apply**. This reveals that the two new **From Site** and **To Site** Virtual Paths between the MCN and the client site have been added to the Paths table.

The screenshot shows an 'Edit' dialog box for configuring a Virtual Path. At the top, there is a 'Convert to Static Path' button and a warning message: 'Convert Path, AND all other Paths associated by WAN Link, Generated by an Autopath Group, to a Static Path. This action cannot be undone'. Below this, there are two columns of fields: 'MCN-5100' and 'BR572' in the top row, and 'BR572-WL-1' and 'MCN-5100-WL-1' in the bottom row, with 'WAN Link:' labels. Below these are two checked checkboxes: 'Reverse Also' and 'Enable Encryption'. The 'IP DSCP Tagging' section has a dropdown menu set to 'Any'. The 'Bad Loss Sensitive' section has a dropdown menu set to 'Enable (Default)'. The 'Silence Period (ms):' section has a dropdown menu set to 'DEFAULT'. The 'Path Probation Period (ms):' section has a dropdown menu set to '10000 (Default)'. There is a checked checkbox for 'Instability Sensitive'. At the bottom, there are two empty text input fields for 'Tracking IP Address:' and 'Reverse Tracking IP Address:'. At the very bottom are 'Apply' and 'Cancel' buttons.

12. Repeat the steps above for each branch you want to connect to the MCN.

Next, you have the option of customizing the Virtual Paths configurations for the client sites, as well as adding and configuring additional paths between clients. Instructions are provided in the remaining steps, below.

14. Select a client site branch from the **View Site** drop-down menu. This opens the configuration for client site branch in the **Connections** tree.

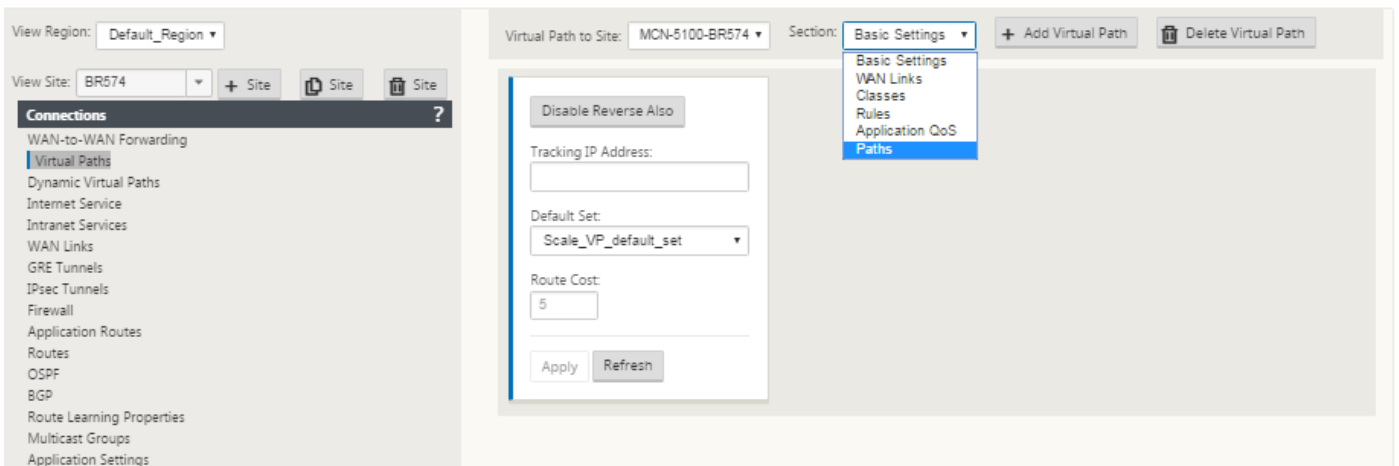


15. Navigate to the **Paths** settings configuration form for any client site Virtual Path you want to configure.

To navigate to the Paths settings form for the client site, do the following:

Select **Paths** from the **Section** tab of branch page for the client site.

The below figures shows an example **Paths** settings form for the new **From Site** path added in the previous steps.



16. Configure the settings for each path you want to customize. Follow the same steps as you did to configure the Virtual Paths for the MCN site.

View Region: Default_Region

View Site: BR574

Virtual Path to Site: MCN-5100-BR574

Section: Paths

+ Add Virtual Path

- Delete Virtual Path

+	site	From Link	To Site	To Link	Auto	Edit	Delete
+	BR574	BR574-WL-1	MCN-5100	MCN-5100-WL-1	YES		
	BR574	BR574-WL-1	MCN-5100	MCN-5100-WL-2	YES		
	BR574	BR574-WL-2	MCN-5100	MCN-5100-WL-1	YES		
	BR574	BR574-WL-2	MCN-5100	MCN-5100-WL-2	YES		
	MCN-5100	MCN-5100-WL-1	BR574	BR574-WL-1	YES		
	MCN-5100	MCN-5100-WL-1	BR574	BR574-WL-2	YES		
	MCN-5100	MCN-5100-WL-2	BR574	BR574-WL-1	YES		
	MCN-5100	MCN-5100-WL-2	BR574	BR574-WL-2	YES		

Apply Refresh

This completes the basic configuration of the Virtual Paths between the client sites and the MCN.

Note

For information on configuring additional settings in the **Connections** or **Provisioning** sections of the **Configuration Editor**, please refer to the Management Web Interface online help for those sections. If you do not want to configure these settings at this time, you can proceed to the appropriate step indicated below.

The next step depends on the SD-WAN Edition license you have activated for your deployment, as follows:

- **SD-WAN Enterprise Edition** – The Enterprise Edition includes the full set of WAN Optimization features. If you want to configure WAN Optimization for your sites, please proceed to the [Enabling and Configuring WAN Optimization](#) topic. Otherwise, you can proceed directly to [Preparing the SD-WAN Appliance Packages on the MCN](#).
- **SD-WAN Edition** – This Edition does not include the WAN Optimization features. You can now proceed directly to [Preparing the SD-WAN Appliance Packages on the MCN](#).

Deploy MCN Configuration

Mar 01, 2018

The next step is to prepare the SD-WAN Appliance Packages for distribution to the client nodes. This involves the following two procedures:

1. Export the Configuration Package to Change Management.

Before you can generate the Appliance Packages, you must first export the completed configuration package from the **Configuration Editor** to the global **Change Management** staging inbox on the MCN. Instructions are provided in the section [Perform Change Management](#).

2. Generate and stage the Appliance Packages.

After you have added the new configuration package to the **Change Management** inbox, you can generate and stage the Appliance Packages. To do this, you will use the **Change Management** wizard in the Management Web Interface on the MCN. Instructions are provided in the section [Deploy Configuration to Branches](#).

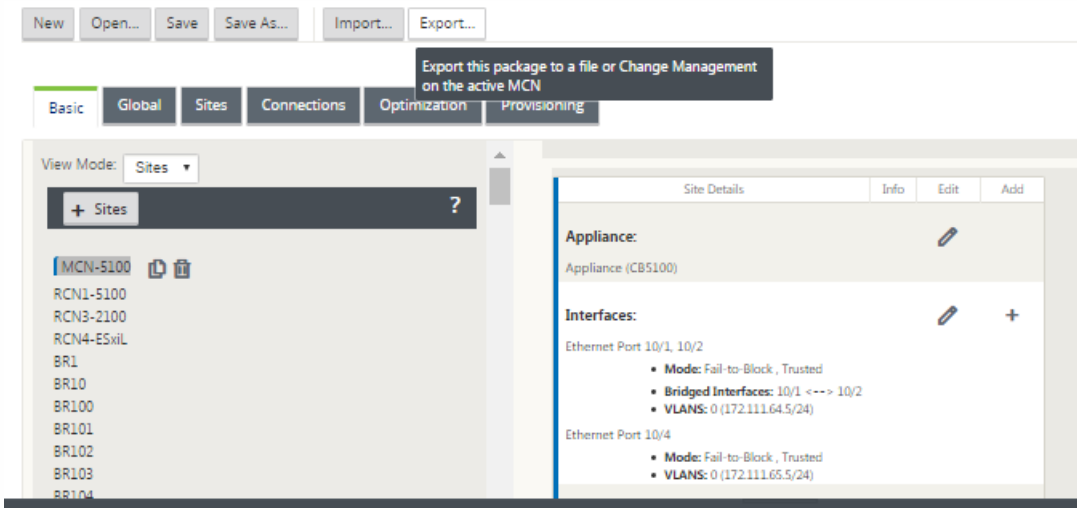
Perform MCN Change Management

Mar 01, 2018

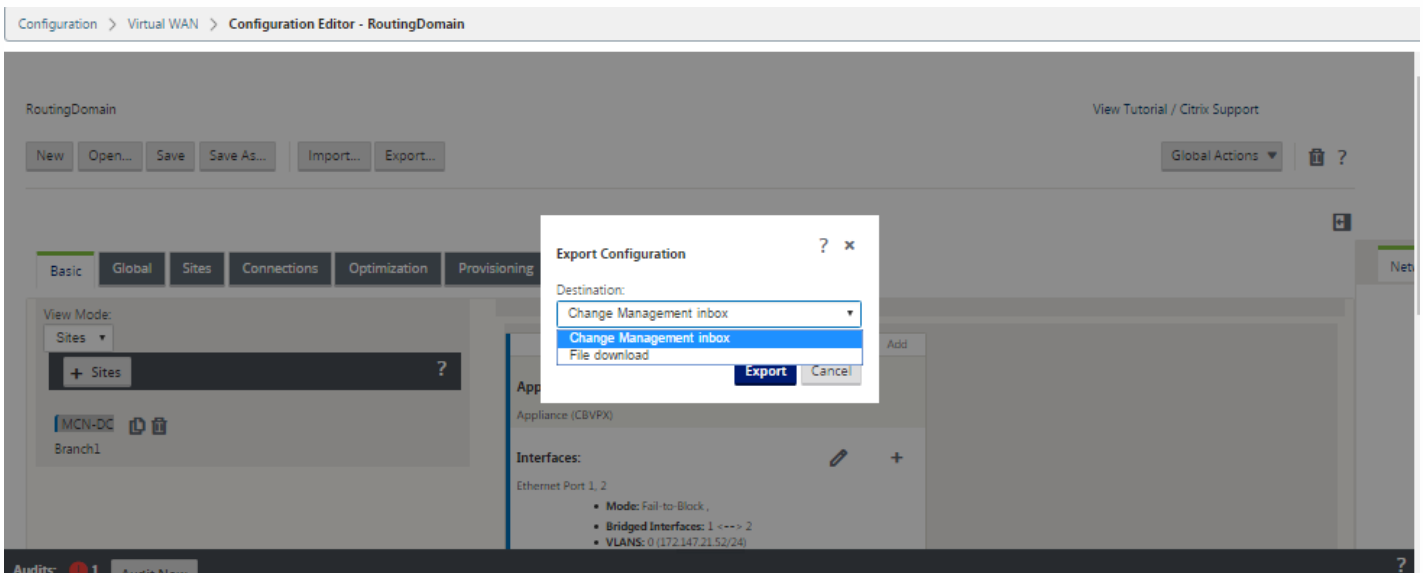
Before you can generate the appliance packages, you must first export the completed configuration package to the Management Web Interface Change Management system.

To export the configuration package to **Change Management**, do the following:

1. In the **Configuration Editor** page, click **Export** (at the top of the page).



This opens the **Export Configuration** dialog box.



2. Select **Change Management Inbox** as the export destination.

Use the drop-down menu in the **Destination:** field to make your selection.

3. Click **Export**.

When the export operation completes, a green success status message displays at the top of the page.

Tip

You can click the blue **Change Management** link in the success message to go directly to the **Change Preparation -- Upload and Verify Files** page (second page) of the **Change Management** wizard. You will need to navigate to this page to perform the next step in the configuration process. However, the success message displays for only a few seconds, after which you must use the navigation tree to open the wizard and then step through to this page. Instructions are provided in the next section.

You are now ready to upload the SD-WAN software packages to the MCN Appliance, and prepare the appliance packages for distribution to the client nodes.

Deploy Configuration to Branches

Mar 01, 2018

After you have prepared the configuration using the configuration editor and exported the configuration package to the change management inbox, the next step is to prepare the SD-WAN Appliance Packages for distribution to the client nodes. To do this, use the **Change Management** wizard in the Management Web Interface on the MCN.

There is a different SD-WAN software package for each SD-WAN Appliance model. An Appliance Package consists of the software package for a specific model, bundled with the configuration package you want to deploy. Consequently, a different Appliance Package must be prepared and generated for each appliance model in your network.

Note

If you have not already downloaded the required SD-WAN software packages to a PC connected to your network, you will need to do so now. For information on acquiring and downloading the software, see the section [Acquiring the SD-WAN Software Packages](#).

To upload and install the package and configuration to the MCN, do the following:

1. Log into the Management Web Interface on the MCN appliance.

Note

You will be uploading the software packages you previously downloaded to the connected PC. For convenience, you might want to use this same PC to connect to the MCN again.

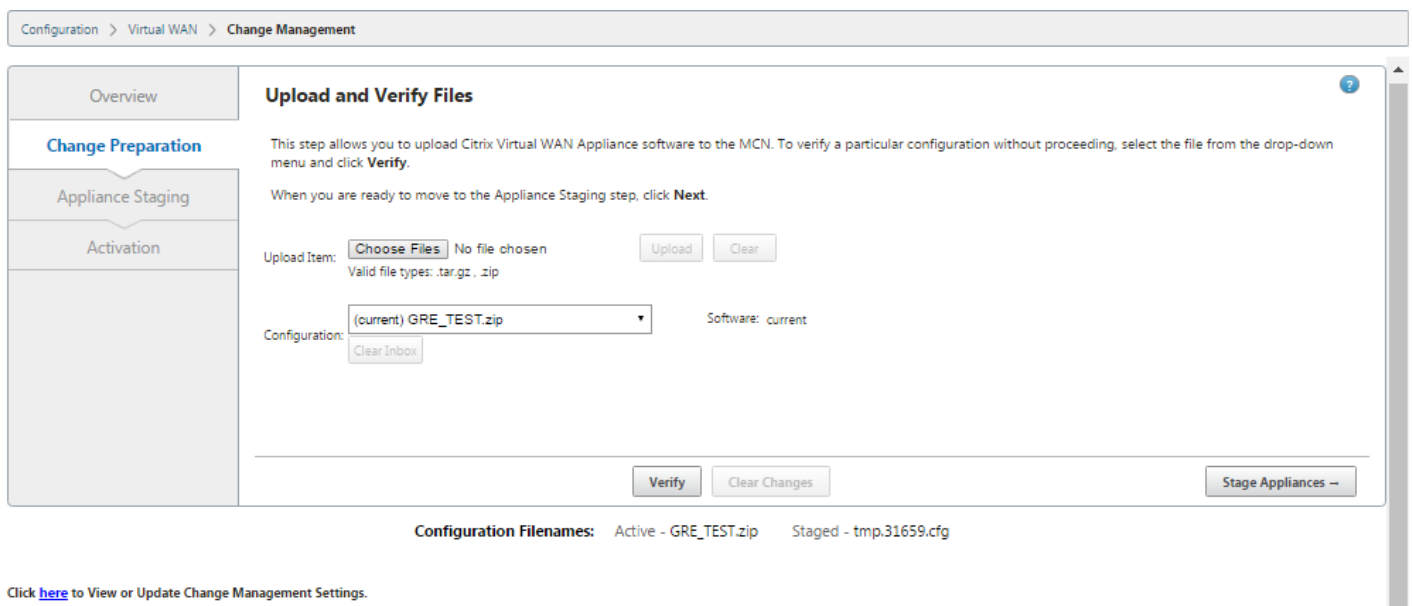
2. Select the **Configuration** tab.
3. In the left pane, open the **Virtual WAN** section, and select **Change Management**.

This displays the first page of the **Change Management** wizard, the **Change Process Overview** page.

The screenshot shows the 'Change Management' wizard interface. On the left is a navigation pane with 'Change Management' selected under the 'Virtual WAN' section. The main area is titled 'Change Process Overview' and contains a three-step process flow: Step 1: Change Preparation (Upload Files to MCN), Step 2: Appliance Staging (Transfer Files to Clients), and Step 3: Activation (Activate Change). Each step has a progress indicator and a button labeled 'MCN' or 'Clients'. At the bottom right, there are 'Activate Staged' and 'Begin --' buttons.

4. Click **Begin**.

This displays the **Change Preparation** page for uploading and verifying the specified configuration and software package(s).



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

5. Upload each of the SD-WAN software packages required for your network.

For each SD-WAN software package you want to deploy, do the following:

a. Click **Choose File** next to the **Upload Item** field.

This opens a file browser for selecting a SD-WAN software package to upload.

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

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

c. Click **Upload**.

d. Repeat steps (a) through (c) for each of the SD-WAN software packages required for your network.

6. In the **Configuration** field drop-down menu, select the new configuration package that you just exported to **Change Management**.

7. Click **Stage Appliance**.

This initiates the following actions:

- Transfers the selected software package and configuration to the MCN.
- Generates an Appliance Package for each appliance model identified in the selected configuration.
- Adds the new Appliance Packages to the list of available packages in the Site-Appliance table.
- Stages the new configuration and appropriate software package on the MCN.

8. Click **Next**. This proceeds to the **Appliance Staging** page.

Appliance Staging

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

Transfer Progress:

100%

Appliance Staging complete. You may now proceed to Activation.

Prepare Packages Stage Packages Done

Abort Ignore Incomplete Next ->

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

Configuration Filenames: Active - GRE_TEST.zip Staged -

When the staging operation completes, the **Site-Appliance** table is populated with the newly staged Appliance Packages information.

Note

If this is an initial deployment, only the MCN is updated and staged at this time. If you are updating an existing deployment and the Virtual Paths are already functioning between the deployed sites, this also distributes the appropriate Appliance Packages to the deployed client nodes, and initiates staging on those nodes. However, if you are adding new client nodes to an existing Virtual WAN deployment, you still must manually upload, stage, and activate the appropriate Appliance Package on each new client, as outlined in the remaining steps in this procedure.

Select ignore incomplete, when adding additional sites to the network or if the site is in **not connected** state. This indicates that the client sites should be ignored for this staging operation, and only the MCN should be updated and staged.

9. Select **Revert on Error** to revert to previous application package on encountering some error. For more information, see Configuration Rollback.

10. Click **Activate Staged**.

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In:

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

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

Revert on Error

Currently Prepared: Configuration - GRE_TEST.zip Software - Current Running
Configuration Filenames: Active - GRE_TEST.zip Staged - GRE_TEST.zip

The results and next steps will differ at this point, depending on whether this is an initial configuration or you are updating or replacing an existing configuration, as follows:

- If you are updating or changing the configuration on an existing deployment:

If this is not an initial configuration, this activates the new configuration and the appropriate Appliance Package on the MCN appliance. The appropriate Appliance Package is then distributed to and automatically activated on each client in your SD-WAN. (This may take several seconds to complete.)

- View Configuration
- Configuration Editor
- Change Management**
- Change Management Settings
- Restart/Reboot Network
- Enable/Disable/Purge Flows
- Dynamic Virtual Paths
- SD-WAN Center Certificates
- System Maintenance

Overview

Change Preparation

Appliance Staging

Activation

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In:

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

Currently Prepared: Configuration - GRE_TEST.zip Software - Current Running
Configuration Filenames: Active - GRE_TEST.zip Staged - GRE_TEST.zip

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

Global Multi-Region Summary

Search:

Region	Total Sites	Not Connected	Staging	Activated	Failed
Default_Region	2	0	0	2	0

Region - Default_Region Details

Show entries Search:

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-DC-Appliance	CBVPX	Done	10.0.0.156.652120	11:23 on 1/23/18	10.0.0.156.652120	22:45 on 1/24/18	0 sec		active / staged
Branch1-Appliance	CB2000	Done	10.0.0.156.652120	11:23 on 1/23/18	10.0.0.156.652120	22:45 on 1/24/18	0 sec		active / staged

When the activation completes, an **Activation complete** status message appears, and the **Done** button is enabled. In addition, the **Configuration Filenames** status line (above the table) now displays the name of newly-activated package in the **Active** field

<https://docs.citrix.com>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

p.169

Click **Done** and proceed to one of the following:

* If you are not adding any new nodes to your SD-WAN, this completes the preparation, distribution, and activation of the new Appliance Packages in your SD-WAN. You can proceed directly to [Enabling the Virtual WAN Service](#).

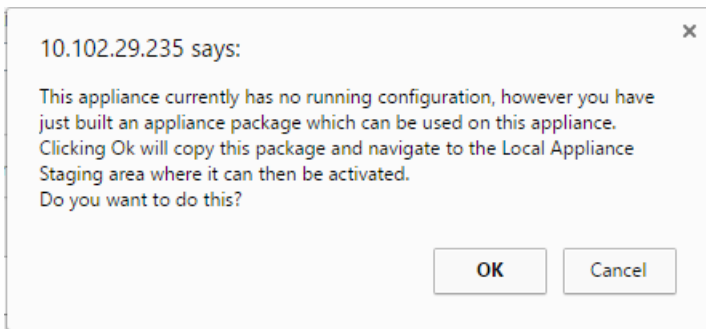
* If you want to add new client nodes to your SD-WAN, please proceed to [Connecting the Client Appliances to Your Network](#).

- If you are activating an initial configuration:

If this is an initial configuration, the new configuration package will not be activated at this point, and there are additional steps you must perform. The next step is to copy the configuration package to the Local Appliance Staging area, in preparation for staging and activating the configuration package on the MCN.

Do the following:

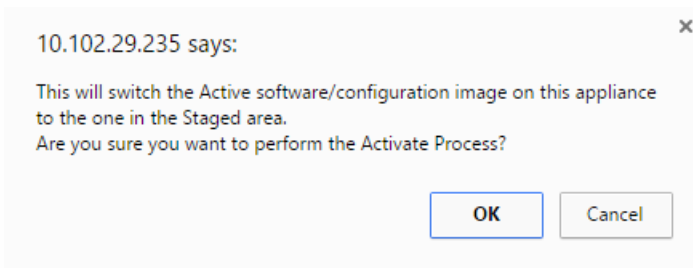
a. Once you click **Activate Staged**, the following message appears .

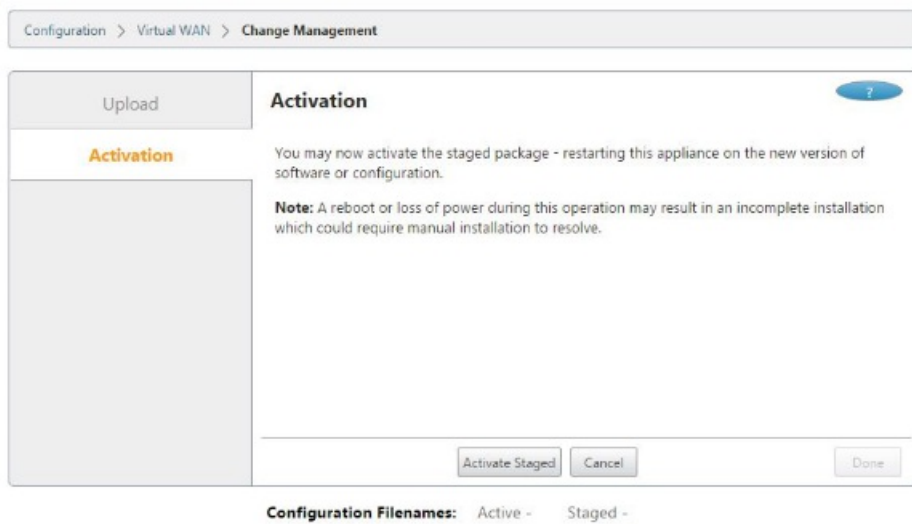


b. Click **OK**.

c. Click **Activate staged**.

This displays a dialog box asking you to confirm the activation operation.





d. Click **OK**.

This initiates activation of the staged configuration package. This process takes several seconds, during which a progress status message displays.

When the activation completes, a status message displays stating activation complete, and the **Done** button is enabled.

e. Click **Done**. This proceeds to the Management Web Interface **Dashboard** page, where you can view the activation results.

You have now completed the preparation of the SD-WAN Appliance Packages on the MCN. Proceed to [Connecting the Client Appliances to Your Network](#).

Tip

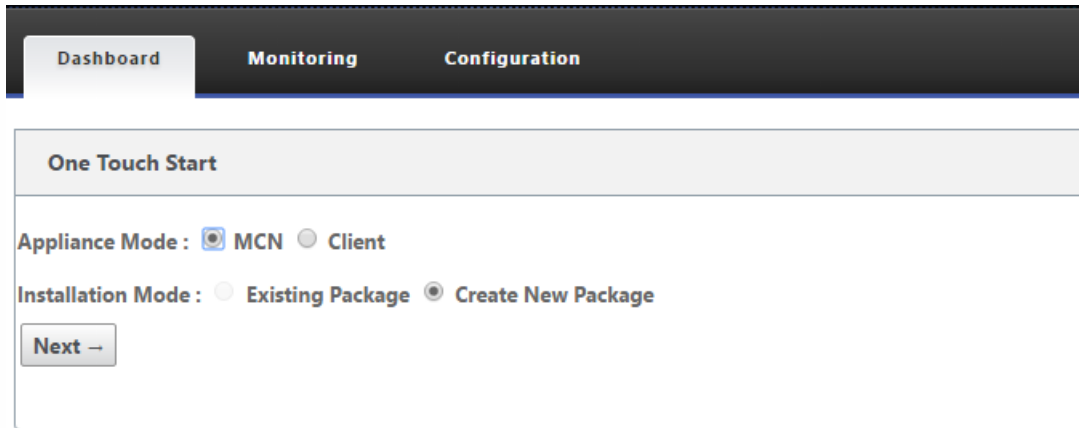
The **Change Management wizard** has an option to search the site- appliance table. This allows you to easily look up sites on a large network with multiple sites and download the required staged configuration. You can also search for error states, for example: 'Fail' or 'Not connected'. This will give you a list of all the sites in that state.

One Touch Start

Mar 01, 2018

Once touch start allows you to easily and quickly configure your SD-WAN appliance as a Client on first time start up.

The one touch start option is displayed when your appliance boots up for the first time.



The screenshot shows the 'One Touch Start' configuration screen. At the top, there is a navigation bar with three tabs: 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' tab is active. Below the navigation bar, the 'One Touch Start' section is displayed. It contains two radio button options for 'Appliance Mode': 'MCN' (selected) and 'Client'. Below that, there are two radio button options for 'Installation Mode': 'Existing Package' and 'Create New Package' (selected). At the bottom of the section, there is a 'Next ->' button.

Note

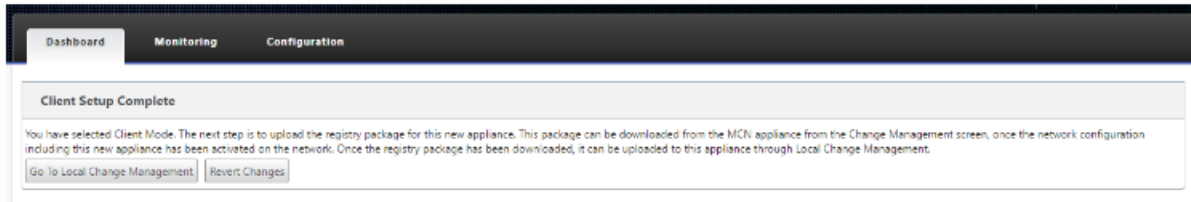
For configuring the SD-WAN appliance as an MCN, create a new configuration or import an existing configuration using the **Configuration Editor**. For more information see, [Preparing the SD-WAN Appliance Packages on the MCN](#).

To configure your SD-WAN appliance as a client using an existing configuration file:

1. Select **Client** as the appliance mode.
2. Select **Existing Package** installation mode. Administrator must periodically save the configuration of the MCN in order to make use of an existing package of the MCN.
3. Click **Choose File** to select the configuration package from your local computer.
4. Click **Upload and Install**.

To configure your SD-WAN appliance as a client using Local Change Management:

1. Select **Client** as the appliance mode.
2. Select **Create New Package** to upload the configuration package for this appliance using Local change management. The package can be downloaded from the MCN appliance from the change Management screen.
3. Click **Next**.
4. Click **Go To Local Change Management**.



Follow the procedure in the topic [Installing the SD-WAN Appliance Packages on the Clients](#).

Connecting the Client Appliances to Your Network

Mar 01, 2018

If this is an initial deployment, or you are adding client nodes to an existing SD-WAN, the next step is for the branch site administrators to connect the client appliances to the network at their respective branch sites. This is in preparation for uploading and activating the appropriate SD-WAN appliance packages to the clients. You will need to contact each branch site administrator to initiate and coordinate these procedures.

To connect the site appliances to the SD-WAN, site administrators should do the following:

1. If you have not already done so, set up the client appliances.

For each appliance you want to add to your SD-WAN, you will need to do the following:

- a. Set up the SD-WAN appliance hardware and any SD-WAN VPX virtual appliances (SD-WAN VPX-SE) you will be deploying.
- b. Set the Management IP Address for the appliance and verify the connection.
- c. Set the date and time on the appliance. Set the console session **Timeout** threshold to a high or the maximum value.
- d. Upload and install the software license file on the appliance.

2. Connect the appliance to the branch site LAN.

Connect one end of an Ethernet cable to a port configured for LAN on the SD-WAN appliance, and the other end of the cable to the LAN switch.

3. Connect the appliance to the WAN.

Connect one end of an Ethernet cable to a port configured for WAN on the SD-WAN appliance, and the other end of the cable to the WAN router.

The next step is for the branch site administrators to install and activate the appropriate SD-WAN appliance package on their respective clients.

Installing the SD-WAN Appliance Packages on the Clients

Mar 01, 2018

After you have prepared the appliance packages and connected the MCN, and the branch site administrators have connected their respective client appliances to the LAN and WAN, the next step is to upload and activate the appropriate SD-WAN appliance package on each client. The Change Management wizard guides you through this process.

To install and activate the software and configuration on a client appliance, do the following

1. On a connected PC, open a browser and log onto the MCN appliance Management Web Interface.

Enter the Management IP Address for the MCN in the browser address field. This displays the Management Web Interface **Dashboard** page for the MCN appliance.

2. Select the **Configuration** tab.

3. In the navigation pane on the left, select **Virtual WAN** and then select **Change Management**.

This displays the **Change Process Overview** page (the first page of the **Change Management** wizard).

Configuration > Virtual WAN > Change Management

Activate

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

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

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

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

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

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

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

Activate Staged Abort Revert on Error Done

Currently Prepared: Configuration - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Software - Current Running

Configuration Filenames: Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Staged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensio_550sites_wantowanforwarding_geoRCN_1kEE.zip

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

Global Multi-Region Summary

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	10	2	0	8	0
r1	552	4	4	547	0
r3	8	2	1	5	0
r4	Data not available				

Region - Default_Region Details

Show 25 entries

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-5100-Appliance	CB5100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR572-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR573-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR574-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR575-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN1-5100-Appliance	CB5100	Transferring Region	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN1-5100-RCN1_HA-Appliance	CB5100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN3-2100-Appliance	CB2100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN3Geo-2100-Appliance	CB2100	Cancelled	Not Connected				Loc Chg Mgt		active / staged
RCN4-ESxIL-Appliance	CBVPXL	Cancelled	Not Connected				Loc Chg Mgt		active / staged

At the bottom of this page, you will see a table listing the individual sites and appliances. At the far right of the table in the **Download Package** column, are links for the **Active** (if available) and **Staged** appliance packages.

Traffic Interruption		Download Package
Expected	Actual	
0 sec		active / staged
Loc Chg Mgt		active / staged

Note

If this is an initial installation, the **Active** links are not yet available, and are replaced by a plain text marker **none**.

- Click the **Staged** link for the package you want to download.

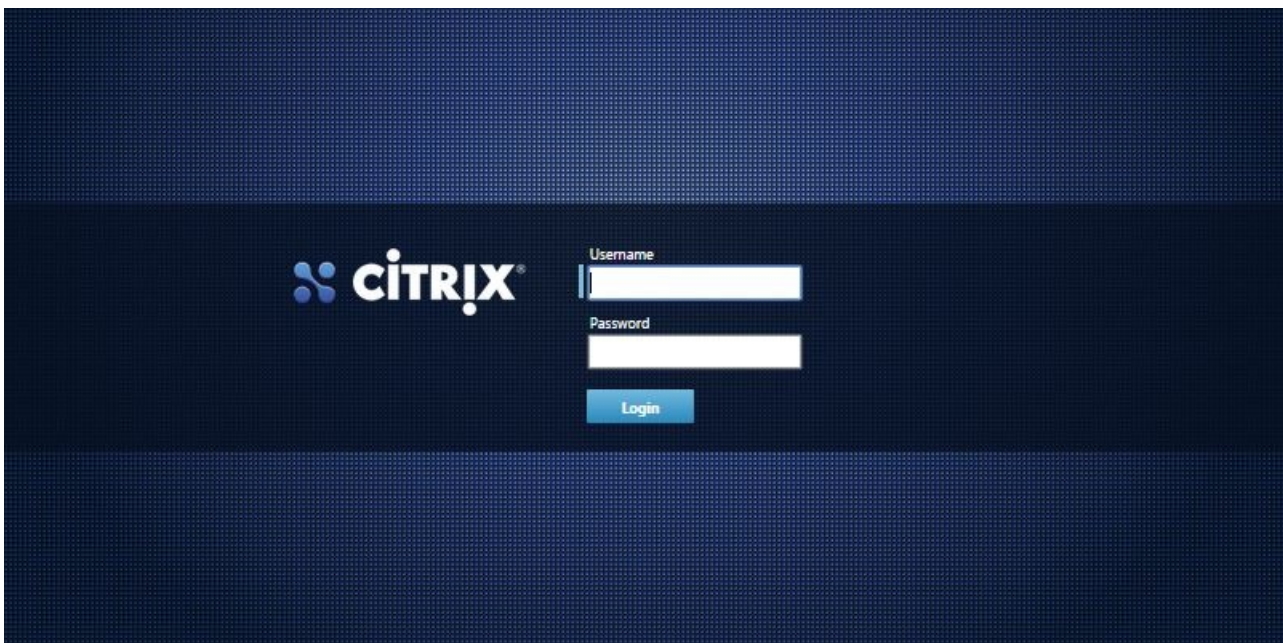
In the **Site-Appliance** table, locate the entry for your site appliance, and click the **Staged** link in the **Download Package** column of that entry. A file browser for selecting the download location (on the local PC) displays.

5. Select the download location and click **OK**.
6. (Optional.) After the download completes, log out of the MCN Management Web Interface.
7. Open a browser, and enter the IP Address for the client to which you want to upload the appliance package .zip file.

Note

Please ignore any browser certificate warnings for the Management Web Interface.

This opens the NetScaler SD-WAN Management Web Interface Login screen on the client appliance.



8. Enter the Administrator user name and password and click **Login**.

The default Administrator user name is *admin*, the default password is *password*.

This displays the Management Web Interface **Dashboard** page for the client appliance.

Dashboard Monitoring Configuration

System Status

Name: MCN-5100
 Model: 5100
 Appliance Mode: MCN
 Serial Number: 4H30GCNPD0
 Management IP Address: 10.199.107.201
 Appliance Uptime: 1 weeks, 4 minutes, 45.3 seconds
 Service Uptime: 1 days, 1 hours, 1 minutes, 42.0 seconds
 Routing Domain Enabled: Default_RoutingDomain

Local Versions

Software Version: 10.0.0.184.657939
 Built On: Feb 13 2018 at 17:32:49
 Hardware Version: 5100
 OS Partition Version: 4,6

Virtual Path Service Status

Virtual Path MCN-5100-BR572: Uptime: 1 hours, 55 minutes, 42.0 seconds.
 Virtual Path MCN-5100-BR573: Uptime: 1 hours, 55 minutes, 44.0 seconds.
 Virtual Path MCN-5100-BR574: Uptime: 1 hours, 55 minutes, 23.0 seconds.
 Virtual Path MCN-5100-BR575: Uptime: 1 hours, 55 minutes, 41.0 seconds.
 Virtual Path MCN-5100-RCN1-5100: Uptime: 21 hours, 40 minutes, 32.0 seconds.
 Virtual Path MCN-5100-RCN3-2100: Uptime: 1 hours, 54 minutes, 49.0 seconds.
 Virtual Path 'MCN-5100-RCN4-ESkil' is currently dead.
 Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.

Note

If this is an initial installation, or if you have temporarily disabled the Virtual WAN Service on this appliance, you will see a goldenrod AuditAlert icon with a status message indicating that the Virtual WAN Service is currently inactive or disabled. You can ignore this alert for now. The alert will remain on the **Dashboard** page until you manually start the service, after completing the installation.

9. Select the **Configuration** tab.

10. Open the System Maintenance branch in the navigation tree (left pane), and select **Local Change Management**.

This displays the **Local Appliance Change Process Upload** page for uploading an Appliance Package.

Dashboard Monitoring Configuration

Configuration > System Maintenance > Local Change Management

Upload

Local Appliance Change Process

The Local Change Management process allows a user to upload a new appliance package to this individual appliance. This two-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied to the appliance in a reliable, fail-safe way.

Note: This process does not update any other appliances on the network. For that purpose, use the Configuration -> Virtual WAN -> Change Management screen on the MCN.

Upload Item: No file chosen
 Valid file types: ".zip"

Configuration Filenames: Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Staged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip

Model	Active Software	Active Config	Staged Software	Staged Config
CB5100	10.0.0.184.657939 download	13:18 on 2/14/18	10.0.0.184.657939 download	14:58 on 2/14/18

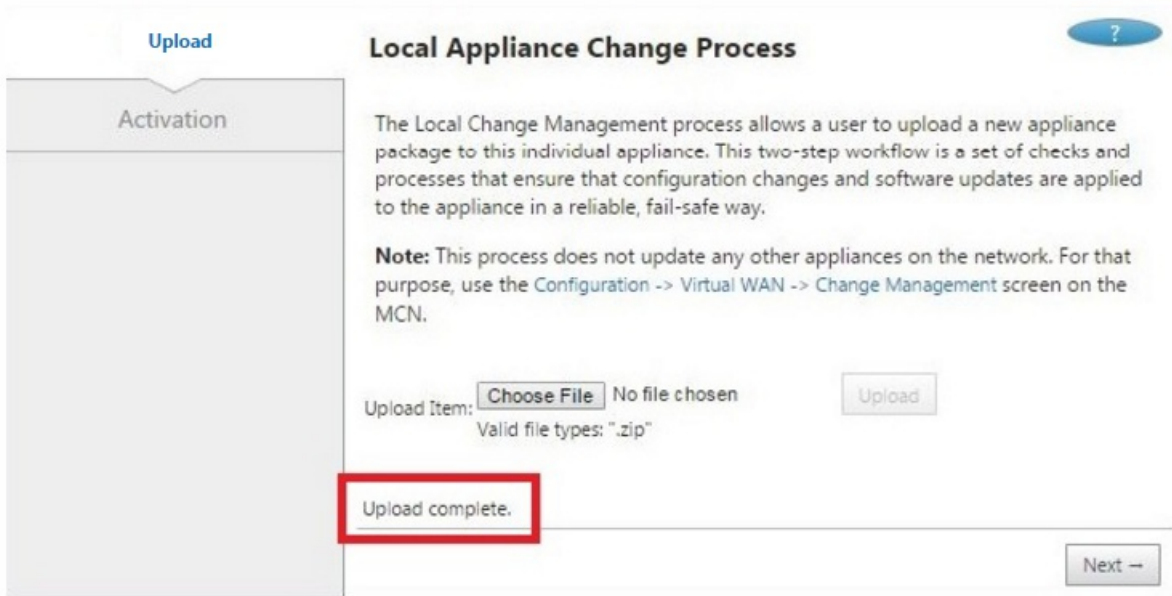
11. Click **Choose File** next to the Upload Item label.

This opens a file browser for selecting the Appliance Package you want to upload to the client.

12. Navigate to the SD-WAN appliance package zip file you just downloaded from the MCN, select it, and click **OK**.

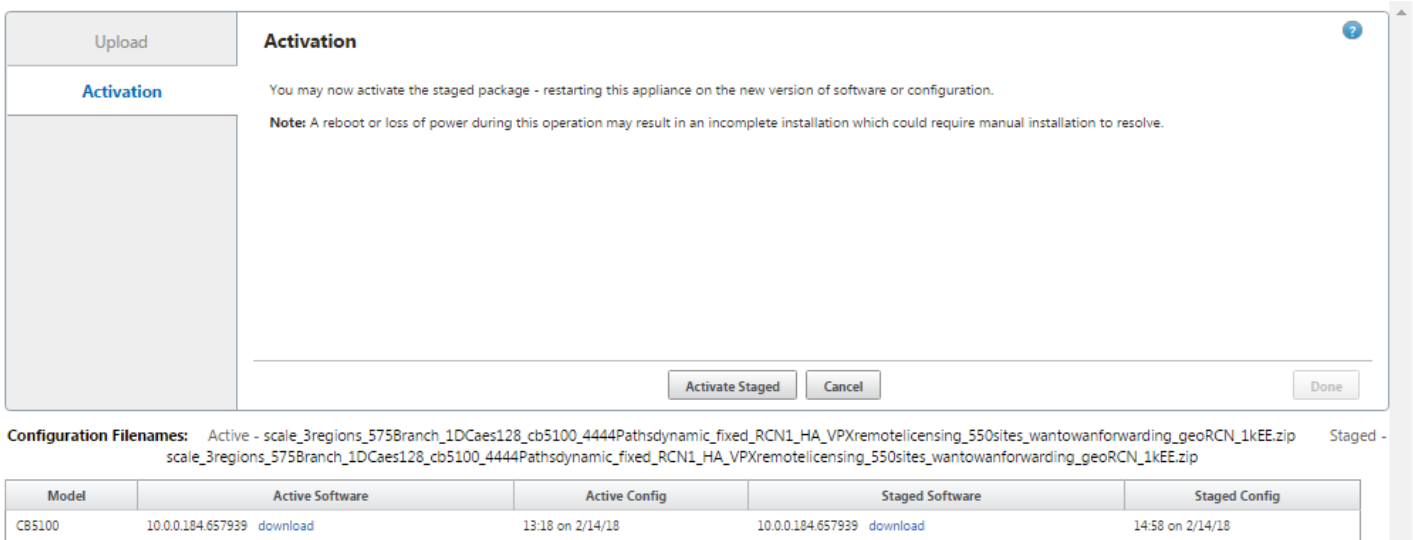
13. Click **Upload**.

The upload process takes a few seconds to complete. When completed, a status message displays (left middle of page), stating **Upload complete.**



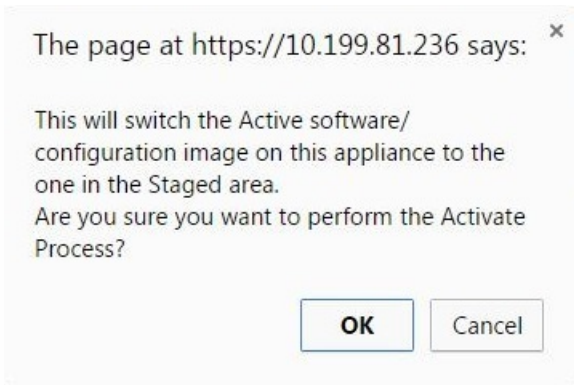
14. Click **Next**.

This uploads the specified software package, and displays the Local Change Management **Activation** page.



15. Click **Activate Staged**.

This displays a dialog box prompting you to confirm the activation operation.



16. Click **OK**.

This activates the newly-installed package and, if this is not an initial deployment, starts the Virtual WAN Service on the client appliance. This process takes several seconds, during which a progress status message displays.

Configuration Filenames: Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Staged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip

Model	Active Software	Active Config	Staged Software	Staged Config
CB5100	10.0.0.184.657939 download	14:58 on 2/14/18	10.0.0.184.657939 download	13:18 on 2/14/18

When the activation completes, a status message displays stating **Activation complete**, and the **Done** button becomes available.

Configuration Filenames: Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Staged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathsdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip

Model	Active Software	Active Config	Staged Software	Staged Config
CB5100	10.0.0.184.657939 download	14:58 on 2/14/18	10.0.0.184.657939 download	13:18 on 2/14/18

17. Click **Done** to exit the wizard and view the activation results.

After the activation completes, click **Done** on the **Activation** page to return to the Management Web Interface **Dashboard** page.

If this is not an initial deployment, this page should now display updated information for the currently active version of the software package, the OS partition, and the status of the CloudBridge Virtual Path. If this is an initial installation, there will be a goldenrod Audit Alert icon, along with a status message indicating that the Virtual WAN Service is currently inactive or disabled. In this case, you must manually enable the service, as described in [Enabling the Virtual WAN Service](#).

The below figure shows a sample client **Dashboard** page displaying the alert icon and status message.

The screenshot displays the Management Web Interface Dashboard with three main 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, 4 minutes, 45.3 seconds, Service Uptime: 1 days, 1 hours, 1 minutes, 42.0 seconds, Routing Domain Enabled: Default_RoutingDomain.
- Local Versions:** Software Version: 10.0.0.184.657939, Built On: Feb 13 2018 at 17:32:49, Hardware Version: 5100, OS Partition Version: 4.6.
- Virtual Path Service Status:** A table listing virtual paths and their uptime. The last two entries are marked as 'currently dead': 'Virtual Path 'MCN-5100-RCN4-ESil1' is currently dead.' and 'Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.'

Virtual Path	Uptime
Virtual Path MCN-5100-8RS72	Uptime: 1 hours, 55 minutes, 42.0 seconds.
Virtual Path MCN-5100-8RS73	Uptime: 1 hours, 55 minutes, 44.0 seconds.
Virtual Path MCN-5100-8RS74	Uptime: 1 hours, 55 minutes, 23.0 seconds.
Virtual Path MCN-5100-8RS75	Uptime: 1 hours, 55 minutes, 41.0 seconds.
Virtual Path MCN-5100-RCN1-5100	Uptime: 21 hours, 40 minutes, 32.0 seconds.
Virtual Path MCN-5100-RCN3-2100	Uptime: 1 hours, 54 minutes, 49.0 seconds.
Virtual Path 'MCN-5100-RCN4-ESil1' is currently dead.	
Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.	

The final step to complete an initial SD-WAN deployment, is to enable the Virtual WAN Service. Instructions are provided in the section [Enabling the Virtual WAN Service](#).

Checklist and How to Deploy

Mar 01, 2018

It is strongly recommended that before beginning the installation, you first read through the Citrix Virtual WAN Deployment Planning Guide. This article discusses the essential Virtual WAN concepts and features, and provides guidelines for planning your deployment. You can find this document on the Citrix Documentation Portal (<http://docs.citrix.com/>).

Prepare for Deployment

The following list outlines the steps and procedures involved in deploying the NetScaler SD-WAN Standard and Enterprise Editions.

1. Gather your NetScaler SD-WAN deployment information.
2. Set up the NetScaler SD-WAN Appliances.

For each hardware appliance you want to add to your SD-WAN deployment, you must complete the following tasks:

- a. Set up the appliance hardware.
- b. Set the Management IP Address for the appliance and verify the connection.
- c. Set the date and time on the appliance.
- d. (Optional) Set the console session **Timeout** interval to a high or the maximum value.
- e. Upload and install the software license file on the appliance.

Installation and Configuration Checklist

Gather the following information for each NetScaler SD-WAN site you want to deploy:

- The licensing information for your product
- Required Network IP Addresses for each appliance to be deployed:
 - * Management IP Address
 - * Virtual IP Addresses
- Site Name
- Appliance Name (one per site)
- SD-WAN Appliance Model (for each appliance to be deployed)
- Deployment Mode (MCN or Client)
- Topology
- Gateway MPLS
- GRE Tunnel information

- Routes
- VLANs
- Bandwidth at each site for each circuit

Deployments

Mar 01, 2018

Following are some of the use case scenarios implemented by using NetScaler SD-WAN appliances:

- [Deploying SD-WAN in Gateway Mode](#)
- [Deploying SD-WAN in PBR mode \(Virtual Inline Mode\)](#)
- [Dynamic Paths for Branch to Branch Communication](#)
- [Static WAN Paths](#)
- [Building an SD-WAN Network](#)
- [Routing for LAN Segmentation](#)
- [Utilizing Enterprise Edition Appliance to Provide WAN Optimization Services Only](#)

Gateway Mode

Mar 01, 2018

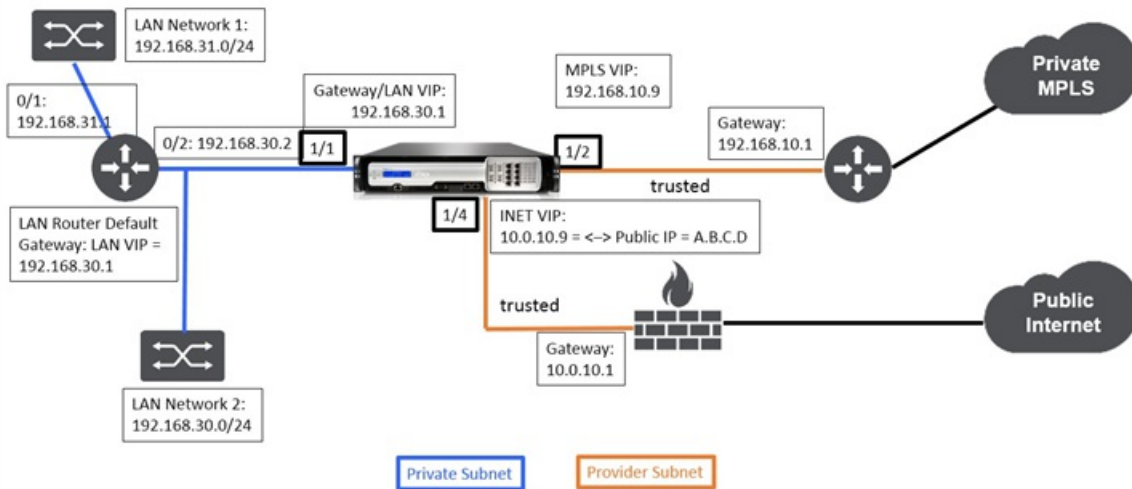
To deploy SD-WAN appliance in Gateway Mode:

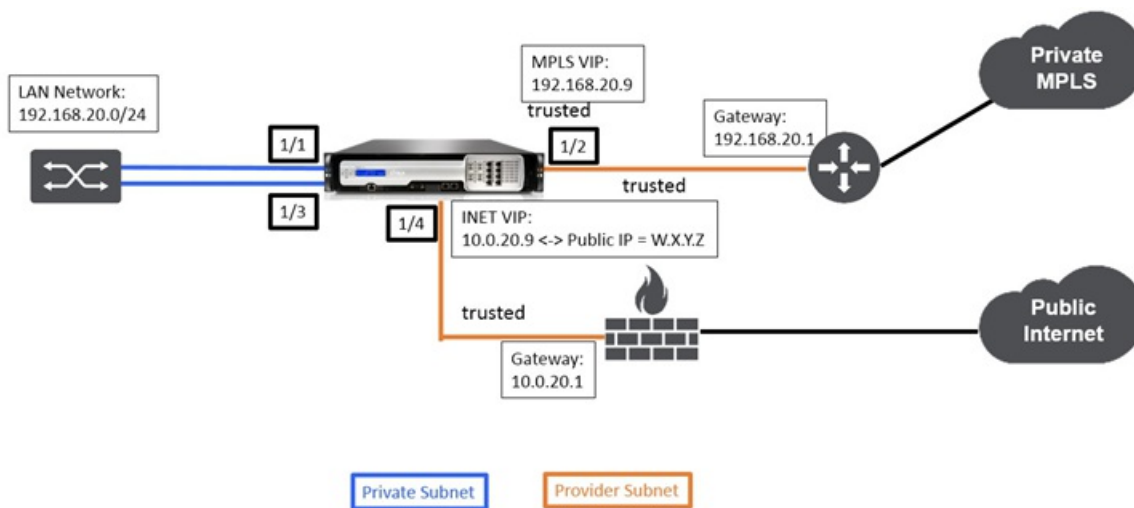
This article provides step-by-step procedure to configure a SD-WAN appliance in Gateway mode in a sample network setup. Inline deployment is also described for the branch side to complete the configuration.

Gateway mode places the SD-WAN appliance physically in the path (two-arm deployment) and requires changes in the existing network infrastructure to make the SD-WAN appliance the default gateway for the entire LAN network for that site.

Note

An SD-WAN deployed in Gateway mode acts as a Layer 3 device and cannot perform fail-to-wire. All interfaces involved will be configured for "Fail-to-block". In the event of appliance failure, the default gateway for the site will also fail, causing an outage until the appliance and default gateway are restored.





Deployment requirements and related information is described below to assist you in building the configuration.

Site Name	DataCenter Site	Branch Site
Appliance Name	A_DC1	A_BR1
Management IP	172.30.2.10/24	172.30.2.20/24
Security Key	If any	If any
Model/Edition	4000	2000
Mode	Gateway	Inline
Topology	2 x WAN Path	2 x WAN Path
VIP Address	192.168.10.9/24 – MPLS 10.0.10.9/24 – Internet (Public IP – A.B.C.D) 192.168.30.1/24 - LAN	192.168.20.9/24 - MPLS 10.0.20.9/24 – Internet (Public IP – W.X.Y.Z)
Gateway MPLS	192.168.10.1	192.168.20.1
Gateway Internet	10.0.10.1	10.0.20.1
Link Speed	MPLS – 100 Mbps Internet – 20 Mbps	MPLS – 10 Mbps Internet – 2 Mbps
Route	Network IP Address - 192.168.31.0/24 Service Type - Local Gateway IP Address - 192.168.30.2	If any
VLANs	If any	If any

- Enable SD-WAN appliance as a Master Control Node.
- Configuration is done only on the Master Control Node (MCN) of the SD-WAN appliance.

To enable an appliance as a Master Control Node:

1. In the NetScaler SD-WAN web management interface, navigate to **Configuration > Appliance Settings > Administrator Interface > Miscellaneous tab > Switch Console**.

Note

If “Switch to Client Console” is displayed, then the appliance is already in MCN mode. There should only be one active MCN in a SD-WAN network.

2. Start Configuration by navigating to **Configuration > Virtual WAN > Configuration Editor**. Click the **New** to begin configuration.

Following are the high-level configuration steps to configure Datacenter site Gateway deployment:

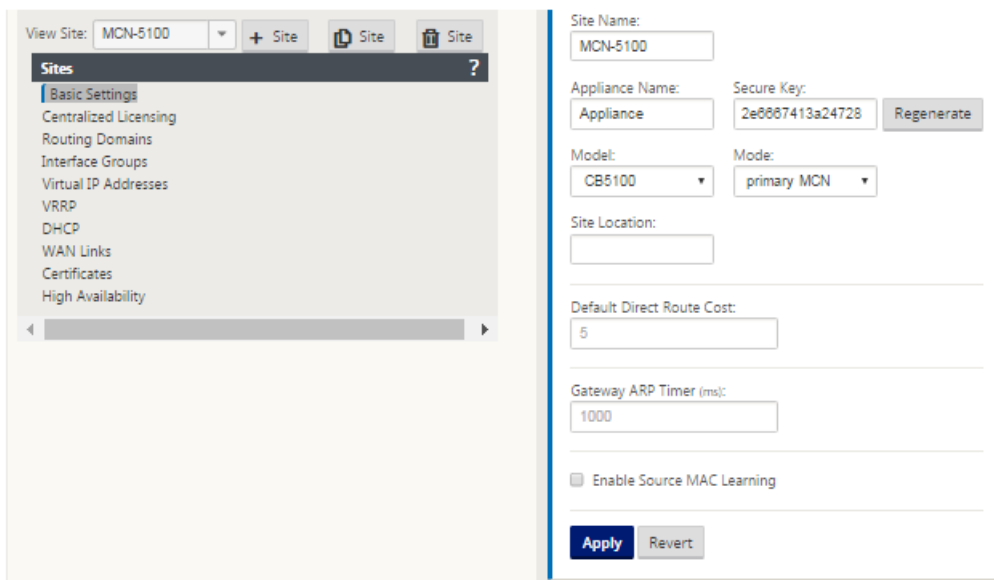
1. Create a new DC site.
2. Populate Interface Groups based on connected Ethernet interfaces.
3. Create Virtual IP address for each virtual interface.
4. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
5. Populate Routes if there are additional subnets in the LAN infrastructure.

1. Navigate to **Configuration Editor - > Sites**, and click the "+" **Add** button.
2. Populate the fields as shown below.
3. Keep default settings unless instructed to change.

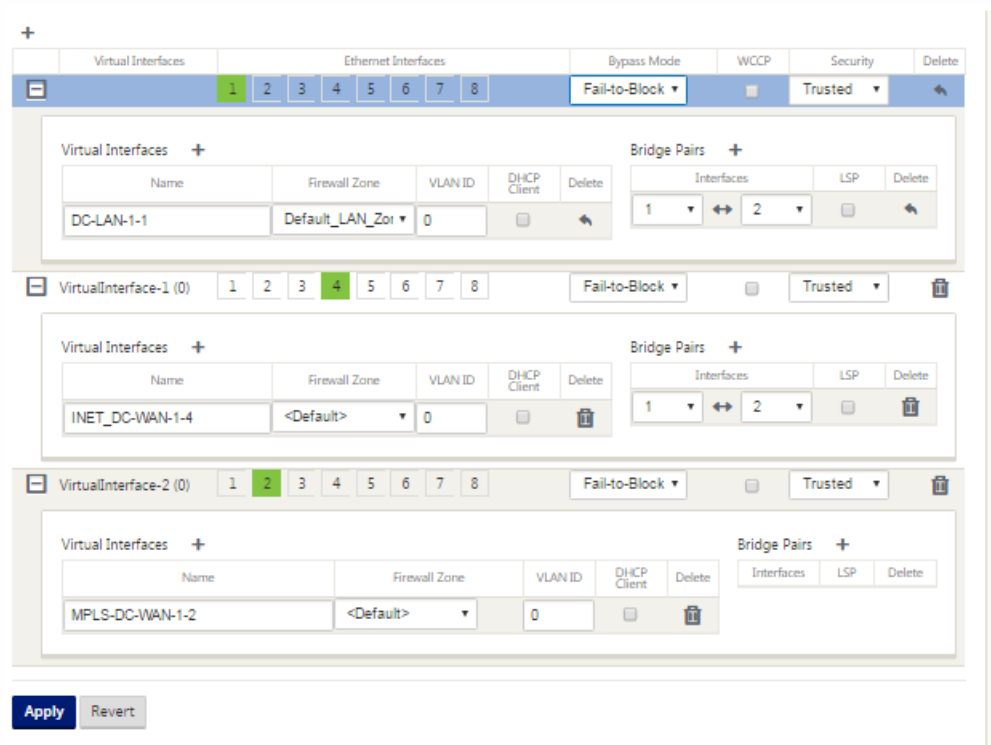
The screenshot shows a modal dialog titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields:

- Site Name:** Text input field containing "DC_Site".
- Region:** Dropdown menu with "r1" selected.
- Site Location:** Text input field containing "APAC".
- Secure Key:** Text input field containing "10871702cbd807ff".
- Model:** Dropdown menu with "CB1000" selected.
- Mode:** Dropdown menu with "primary MCN" selected.

At the bottom right of the dialog, there are two buttons: "Add" (highlighted in blue) and "Cancel".



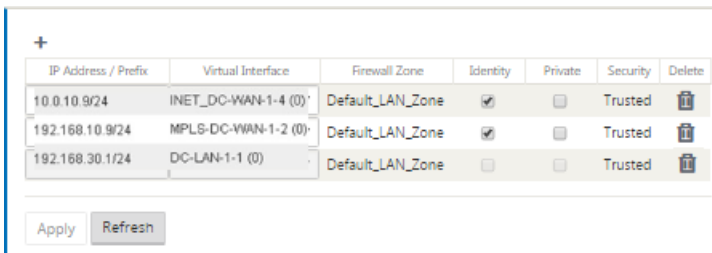
1. In the **Configuration Editor**, navigate to **Sites > View Site > [Site Name] > Interface Groups**. Click “+” to add interfaces intended to be used. For Gateway Mode, each Interface Group is assigned a single Ethernet interface.
2. Bypass mode is set to **fail-to-block** since only one Ethernet/physical interface is used per virtual interface. There are also no Bridge Pairs.
3. In this example three Interfaces Groups are created, one facing the LAN and two others facing each respective WAN Link. Refer to the sample “DC Gateway Mode” topology above and populate the Interface Groups fields as shown below.



1. Create a VIP on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN

appliances in the Virtual WAN environment.

2. Create a Virtual IP Address to be used as the Gateway address for the LAN network

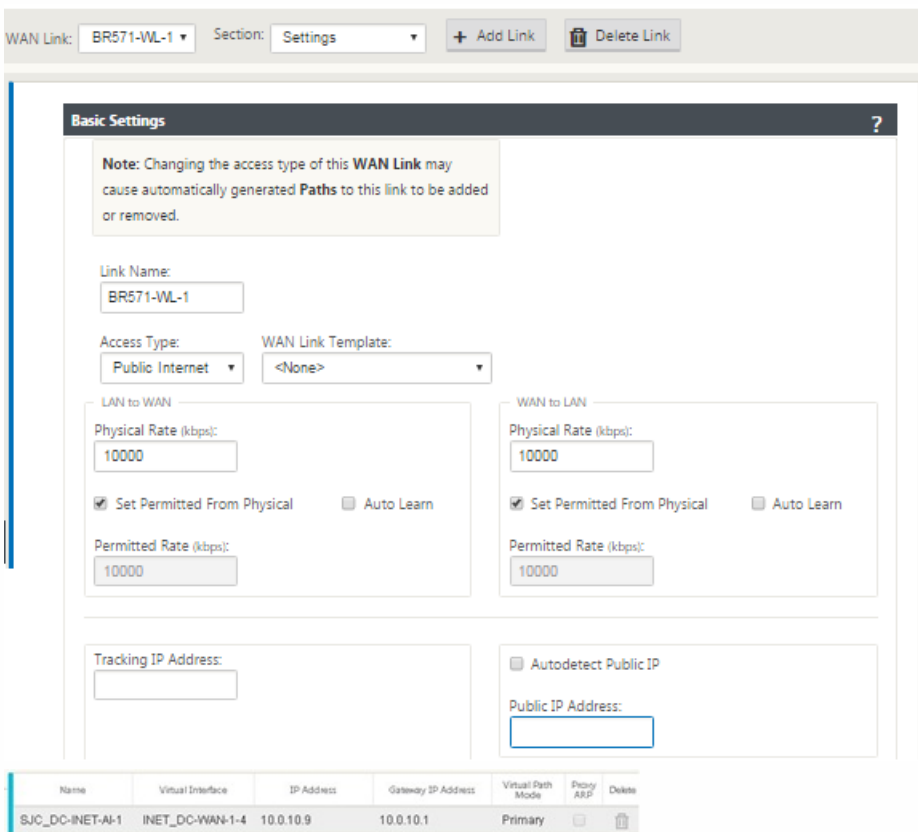


IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.0.10.9/24	INET_DC-WAN-1-4 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.10.9/24	MPLS-DC-WAN-1-2 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input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

To populate WAN links based on physical rate and not on burst speeds using Internet link

1. Navigate to **WAN Links**, click the “+ Add Link” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the supplied Public IP address as shown below. Note that **AutoDetect Public IP** cannot be selected for SD-WAN appliance configured as MCN.
3. Navigate to **Access Interfaces**, from the section drop-down menu, and click the “+ Add” button to add interface details specific for the Internet link.
4. Populate Access Interface for IP and gateway addresses as shown below.



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	Priority ARP	Delete
SJC_DC-INET-AI-1	INET_DC-WAN-1-4	10.0.10.9	10.0.10.1	Primary	<input type="checkbox"/>	

To create MPLS Link

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the MPLS link.
2. Populate MPLS link details as shown below.
3. Navigate to **Access Interfaces**, click the “+” button to add interface detail specific for the MPLS link.
4. Populate Access Interface for IP and gateway addresses as shown below.

Basic Settings ?

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

Link Name: BR571-WL-1

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

LAN to WAN

Physical Rate (kbps): 10000

Set Permitted From Physical

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

Set Permitted From Physical

Permitted Rate (kbps): 10000

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

Routes are auto-created based on the above configuration. The DC LAN sample topology shown above has an additional LAN subnet which is **192.168.31.0/24**. A route needs to be created for this subnet. Gateway IP address must be in the same subnet as the DC LAN VIP as shown below.

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					

Following are the high-level configuration steps to configure Branch site for Inline deployment:

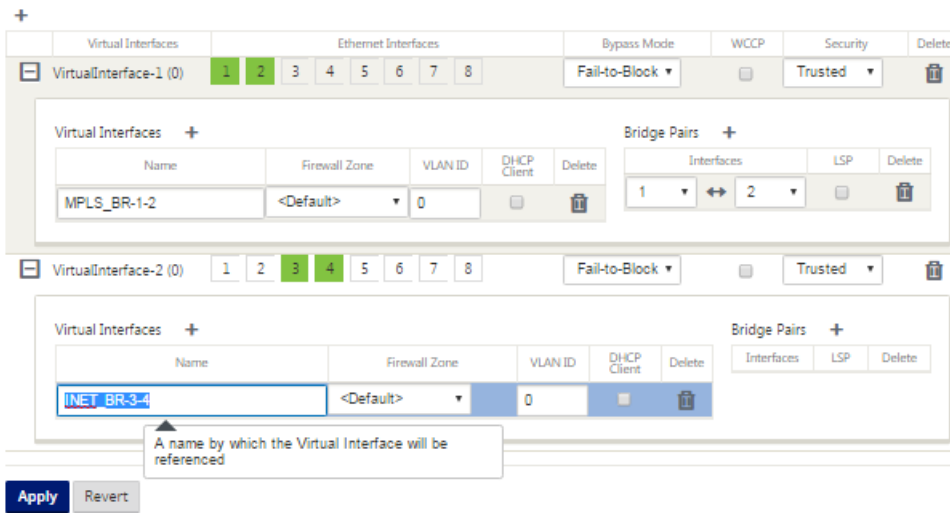
1. Create a new Branch site.
2. Populate Interface Groups based on connected Ethernet interfaces.
3. Create Virtual IP address for each virtual interface.
4. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
5. Populate Routes if there are additional subnets in the LAN infrastructure.

1. Navigate to **Configuration Editor - > Sites**, and click the "+" Add button.
2. Populate the fields as shown below.

3. Keep default settings unless instructed to change.

The image shows two screenshots from the Citrix Configuration Editor. The top screenshot is the 'Add' dialog box, which includes the following fields: Site Name (BR_Site), Region (<Default>), Site Location (APAC), Secure Key (6d10d2ce94552...), Model (CB1000), and Mode (client). The bottom screenshot shows the 'View Site' configuration page for site BR571. The left sidebar lists navigation options: Basic Settings, Centralized Licensing, Routing Domains, Interface Groups, Virtual IP Addresses, VRRP, DHCP, WAN Links, Certificates, and High Availability. The main configuration area includes: Site Name (BR571), Region (Default_Region), Appliance Name (Appliance), Secure Key (ed0b4b910b8bcc4) with a Regenerate button, Model (CB2000), Mode (client), Site Location (empty), Default Direct Route Cost (5), Gateway ARP Timer (ms) (1000), and an unchecked checkbox for Enable Source MAC Learning. Buttons for Apply and Revert are at the bottom.

1. In the **Configuration Editor**, navigate to **Sites > View Site > [Client Site Name] > Interface Groups**. Click “+” to add interfaces intended to be used. For Inline Mode, each Interface Group is assigned two Ethernet interfaces.
2. Bypass mode is set to **fail-to-wire** and Bridge Pair is created using the two Ethernet interfaces.
3. Refer to the sample “Remote Site Inline Mode” topology above and populate the Interface Groups fields as shown below.



1. Create a Virtual IP address on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN appliances in the Virtual WAN environment.

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	
192.113.58.6/24	VirtualInterface-2	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply Refresh

To populate WAN links based on physical rate and not on burst speeds using Internet link

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the AutoDetect Public IP address as shown below.
3. Navigate to **Access Interfaces**, click the “+” button to add interface details specific for the Internet link.
4. Populate Access Interface for IP address and gateway as shown below.

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"/>	

To create MPLS Link

1. Navigate to WAN Links, click the “+” button to add a WAN Link for the MPLS link.
2. Populate MPLS link details as shown below.
3. Navigate to Access Interfaces, click the “+” button to add interface details specific for the MPLS link.
4. Populate Access Interface for IP address and gateway as shown below.

Basic Settings

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

Link Name: BR571-WL-1

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

LAN to WAN

Physical Rate (kbps): 10000

Set Permitted From Physical

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

Set Permitted From Physical

Permitted Rate (kbps): 10000

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-MPLS-...	MPLS_BR-1-2	192.168.20.9	192.168.20.1	Primary	<input checked="" type="checkbox"/>	

Routes are auto-created based on above configuration. In case there are additional subnets specific to this remote branch office, then specific routes need to be added identifying which gateway to direct traffic to in order to reach those backend subnets.

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	65535	Passthrough					

⏪ ⏩ 1 ⏪ ⏩

After completing configuration for DC and Branch sites, you will be alerted to resolve audit error on both DC and BR sites.

By default, the system will generate paths for WAN Links defined as access type Public Internet. You would be required to use the auto-path group function or enable paths manually for WAN Links with an access type of Private Internet. Paths for MPLS links can be enabled by clicking on Add operator (in the green rectangle).

Add Path ✕

From Site: From WAN Link:

To Site: To WAN Link:

Reverse Also

Add
Cancel

After completing all the above steps, proceed to [Preparing the SD-WAN Appliance Packages](#) on the MCN topic.

PBR mode (Virtual Inline)

Mar 01, 2018

In virtual inline mode, the router uses policy based routing rules to redirect incoming and outgoing WAN traffic to the appliance, and the appliance forwards the processed packets back to the router.

The following article describes the step-by-step procedure to configure two SD-WAN (SD-WAN SE) appliances:

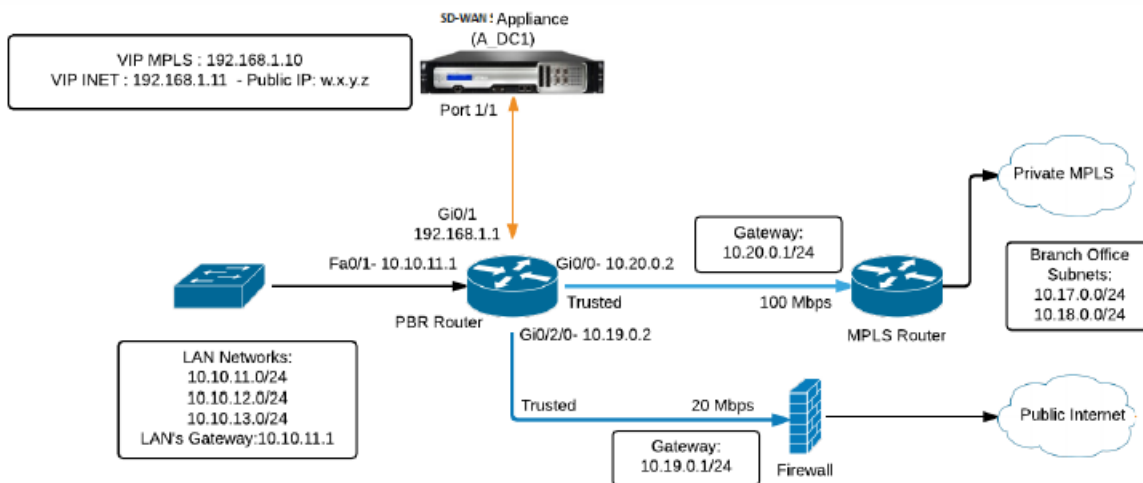
- Data Center Appliance in PBR mode (Virtual Inline Mode)
- Branch Appliance in Inline mode
- PBR needs to be configured either at the core switch or further upstream at the router. The router must monitor the health of the SD-WAN appliance so that the appliance can be bypassed if it fails.
- Virtual Inline Mode places the SD-WAN appliance physically out of path (one-arm deployment) i.e. only a single Ethernet interface to be used (Example: Interface 1/1) with bypass mode set to fail-to-block (FTB).

NetScaler SD-WAN appliance needs to be configured to pass traffic to the proper gateway. Traffic intended for the Virtual Path is directed towards the SD-WAN appliance and then encapsulated and directed to the appropriate WAN link.

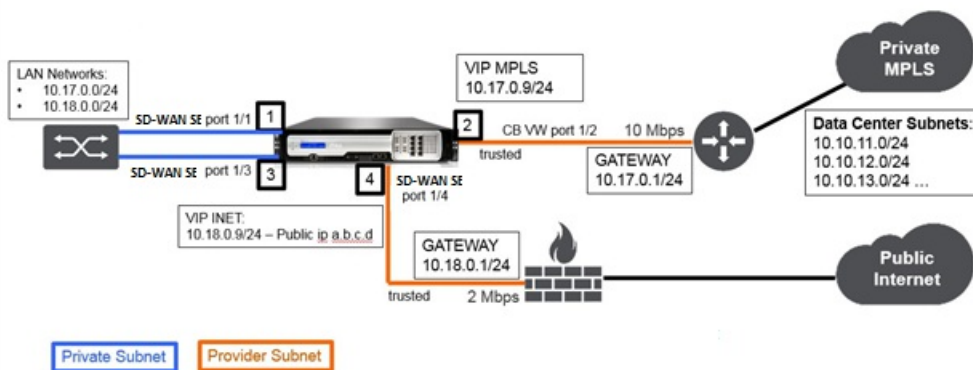
Gathering Information for Configuration

- Accurate network diagram (example diagram show below) of your local and remote site(s) including:
 - Local and Remote WAN links and their bandwidths in both directions, their subnets, Virtual IP Addresses and Gateways from each link, Routes, and VLANs.
- Deployment Table (example diagram shown below)

Data Center Topology – PBR mode (Virtual Inline Mode)



Branch Topology – Inline Mode



Site Name	DataCenter Site	Branch Site
Appliance Name	A_DC1	A_BR1
Management IP	172.30.2.10/24	172.30.2.20/24
Security Key	If any	If any
Model/Edition	4000	2000
Mode	PBR mode (Virtual Inline Mode)	Inline
Topology	2 x WAN Path	2 x WAN Path
VIP Address	192.168.1.10/24 – MPLS 192.168.1.11/24 – Internet*Public IP w.x.y.z	10.17.0.9/24 - MPLS 10.18.0.9/24 – Internet *Public IP a.b.c.d
Gateway MPLS	10.20.0.1	10.17.0.1
Gateway Internet	10.19.0.1	10.18.0.1
Link Speed	MPLS – 100 Mbps Internet – 20 Mbps	MPLS – 10 Mbps Internet – 2 Mbps
Route	Need to add a route on the SD-WAN SE Appliance on how to reach the LAN Subnets (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc) through any of the physical interfaces: Gi0/1 - 192.168.1.1 Configuration > Virtual WAN > Configuration Editor > SJC_DC > Routes. In this example interface 192.168.1.1 was used: <ul style="list-style-type: none"> n/w address: 10.10.13.0/24, 10.10.12.0/24, 10.10.11.0/24 service type: local gateway IP address: 192.168.1.1 	No additional routes were added

Steps to configure a site in Virtual Inline Mode:		Branch Site
Site Name	Data Center Site	

- Enable the MCN functionality.
- Create a New site.
- Create an Interface Group and Virtual Interfaces.
- Assign Virtual IP Address to Virtual Interfaces.
- Create WAN Links and assign IP address.
- Add Routes.
- Troubleshooting.
- Policy Based Routing configuration on the PBR Router.

- Enable SD-WAN appliance as a Master Control Node.
- Configuration is done only on the Master Control Node (MCN) of the SD-WAN appliance.

To enable an appliance as a Master Control Node:

1. In the NetScaler SD-WAN web management interface, navigate to **Configuration > Appliance Settings > Administrator Interface > Miscellaneous tab > Switch Console**.

Note

If “Switch to Client Console” is displayed, then the appliance is already in MCN mode. There should only be one active MCN in a SD-WAN network.

2. Enable Virtual WAN Service. Navigate to **Configuration > Virtual WAN > Enable/Disable/Purge Flows**.

3. Start Configuration by navigating to **Configuration > Virtual WAN > Configuration Editor**. Click **New** to begin configuration.

This operation will create an Untitled_1 initial configuration file which can be renamed [optional] later using the **Save As** button.

Following are the high-level configuration steps to configure Datacenter site in PBR deployment mode:

1. Create a new DC site.
2. Configure Interface Groups based on connected Ethernet interfaces.
3. Configure Virtual IP address for each virtual interface.
4. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
5. Populate Routes if there are additional subnets in the LAN infrastructure.

1. Navigate to **Configuration Editor > Sites**, and click the "+" Add button.
2. Populate the fields as shown below.
3. Keep default settings unless instructed to change.

Add

Site Name: Region:

Site Location:

Secure Key:

Model: Mode:

Add **Cancel**

Site Name:

Appliance Name: Secure Key: **Regenerate**

Model: Mode:

Site Location:

Default Direct Route Cost:

Gateway ARP Timer (ms):

Enable Source MAC Learning

Apply **Revert**

To configure interface groups based on connected Ethernet interfaces

1. In the Configuration Editor, navigate to Sites → [Site Name] → Interface Groups. Click "+" to add interfaces intended to be used. In PBR mode, configuration on only a single Ethernet interface is used i.e. interface connecting the upstream router providing PBR policy implications (Example- Interface 1/1).
2. Bypass mode is set to fail-to-block since only one Ethernet/physical interface is used per virtual interface. There are also no Bridge Pairs.
3. In this example, expand Virtual Interfaces + option and configure the Virtual Interfaces.

Virtual Interfaces

Virtual Interfaces	Ethernet Interfaces	Bypass Mode	WCCP	Security	Delete
VirtualInterface-1 (0)	10/1 10/2 10/3 10/4 10/5 10/6 10/7 10/8	Fail-to-Block		Trusted	

VirtualInterface-1

Name	Firewall Zone	VLAN ID	DHCP Client	Delete
VirtualInterface-1	<Default>	0		

Bridge Pairs

Interfaces	LSP	Delete
10/1 ↔ 10/2		

VirtualInterface-2

Virtual Interfaces	Ethernet Interfaces	Bypass Mode	WCCP	Security	Delete
VirtualInterface-2 (0)	10/1 10/2 10/3 10/4 10/5 10/6 10/7 10/8	Fail-to-Block		Trusted	

Apply **Refresh**

1. Create a **Virtual IP Address** on the appropriate subnet for each WAN Link. VIPs are used for communication between

two SD-WAN appliances in the Virtual WAN environment.

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.111.64.5/24	VirtualInterface-1	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
172.111.65.5/24	VirtualInterface-2	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply Refresh

To populate WAN links based on physical rate and not on burst speeds using Internet and MPLS link:

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the supplied Public IP address as shown below. Note that **AutoDetect Public IP** cannot be selected for SD-WAN appliance configured as MCN.
3. Navigate to **Access Interfaces**, click the “+” button to add interface details specific for the Internet link.
4. Populate Access Interface for IP and gateway addresses as shown below. The **Proxy ARP** is not checked for less than two Ethernet interfaces.

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:

To create MPLS Link

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the MPLS link.
2. Populate MPLS link details as shown below.
3. Navigate to **Access Interfaces**, click the “+” button to add interface detail specific for the MPLS link.
4. Populate Access Interface for MPLS Virtual IP and gateway addresses as shown below.

Basic Settings ?

LAN to WAN

Physical Rate (kbps): 100000

Set Permitted From Physical

Permitted Rate (kbps): 100000

WAN to LAN

Physical Rate (kbps): 100000

Set Permitted From Physical

Permitted Rate (kbps): 100000

Access Type: Private Intranet

Autodetect Public IP

Public IP Address:

Tracking IP Address:

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

Note

The Proxy ARP is not checked for less than two Ethernet interfaces.

On the Data center site, add a route on the SD-WAN SEE appliance to reach the LAN Subnets (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc) through any of the physical interfaces:

0/1/0.1 – 192.168.1.1 on VLAN 10

0/1/0.2 – 192.168.2.1 on VLAN 20

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.10.13.0/24	5	Local		192.168.1.1			
2	10.10.12.0/24	5	Local	BR571	192.168.1.1			
3	10.10.11.0/24	5	Local	BR572	192.168.1.1			
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					

Edit ? x

Network IP Address 10.10.11.0/24	Routing Domain Default_RoutingF	Cost 5	Service Type Local	Gateway IP Address 192.168.1.1
-------------------------------------	------------------------------------	-----------	-----------------------	-----------------------------------

Export Route

Summary Route

Eligibility Based On Path

Path:
<None>

Eligibility Based On Gateway

Apply Cancel

Following are the high-level configuration steps to configure Branch site for Inline deployment:

1. Create a new Branch site.
2. Populate Interface Groups based on connected Ethernet interfaces.
3. Create Virtual IP address for each virtual interface.
4. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
 - Virtual Interface “INTERNET” configured on Bridge pair 1/3 and 1/4
 - Virtual Interface “MPLS” configured con Bridge Pair 1/1 and 1/2
5. Populate Routes if there are additional subnets in the LAN infrastructure.

Add x

Site Name: BR_Site	Region: Default_Region
Site Location: APAC	
Secure Key: 8c07277de5c385f4	
Model: CB1000	Mode: client

Add Cancel

Site Name: Region:

Appliance Name: Secure Key:

Model: Mode:

Site Location:

Default Direct Route Cost:

Gateway ARP Timer (ms):

Enable Source MAC Learning

1. In the **Configuration Editor**, navigate to **Sites** → **[Client Site Name]** → **Interface Groups**. Click “+” to add interfaces intended to be used. For Inline mode configuration, four Ethernet interface are used; interface pair 1/3, 1/4 and interface pair 1/1 and 1/2.
2. Bypass mode is set to fail-to-wire since two Ethernet/physical interfaces are used per virtual interface. There are two bridge Pairs.
3. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
 - Virtual Interface “INTERNET” configured on Bridge pair 1/3 and 1/4
 - Virtual Interface “MPLS” configured con Bridge Pair 1/1 and 1/2.
4. Refer to the sample “Remote Site Inline Mode” topology above and populate the Interface Groups fields as shown below.

Virtual Interfaces	Ethernet Interfaces	Bypass Mode	Security	Delete												
<input type="checkbox"/>	1/1 1/2 1/3 1/4	Fail-to-Wire	Trusted	<input type="button" value="↶"/>												
Virtual Interfaces + <table border="1"> <thead> <tr> <th>Name</th> <th>VLAN ID</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>INET_BR-3-4</td> <td>0</td> <td><input type="button" value="↶"/></td> </tr> </tbody> </table>		Name	VLAN ID	Delete	INET_BR-3-4	0	<input type="button" value="↶"/>	Bridge Pairs + <table border="1"> <thead> <tr> <th colspan="2">Interfaces</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>1/3</td> <td>↔</td> <td>1/4 <input type="button" value="↶"/></td> </tr> </tbody> </table>			Interfaces		Delete	1/3	↔	1/4 <input type="button" value="↶"/>
Name	VLAN ID	Delete														
INET_BR-3-4	0	<input type="button" value="↶"/>														
Interfaces		Delete														
1/3	↔	1/4 <input type="button" value="↶"/>														
<input type="checkbox"/>	1/1 1/2 1/3 1/4	Fail-to-Wire	Trusted	<input type="button" value="↶"/>												
Virtual Interfaces + <table border="1"> <thead> <tr> <th>Name</th> <th>VLAN ID</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>MPLS_BR-1-2</td> <td>0</td> <td><input type="button" value="↶"/></td> </tr> </tbody> </table>		Name	VLAN ID	Delete	MPLS_BR-1-2	0	<input type="button" value="↶"/>	Bridge Pairs + <table border="1"> <thead> <tr> <th colspan="2">Interfaces</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>1/1</td> <td>↔</td> <td>1/2 <input type="button" value="↶"/></td> </tr> </tbody> </table>			Interfaces		Delete	1/1	↔	1/2 <input type="button" value="↶"/>
Name	VLAN ID	Delete														
MPLS_BR-1-2	0	<input type="button" value="↶"/>														
Interfaces		Delete														
1/1	↔	1/2 <input type="button" value="↶"/>														

1. Create a Virtual IP address on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN appliances in the Virtual WAN environment.

Virtual Interfaces	Ethernet Interfaces				Bypass Mode	Security	Delete
+ INET_BR-3-4 (0)	1/1	1/2	1/3	1/4	Fail-to-Wire	Trusted	
+ MPLS_BR-1-2 (0)	1/1	1/2	1/3	1/4	Fail-to-Wire	Trusted	

IP Address / Prefix	Virtual Interface	Security	Delete
10.18.0.9/24	INET_BR-3-4 (0)	Trusted	
10.17.0.9/24	MPLS_BR-1-2 (0)	Trusted	

To populate WAN links based on physical rate and not on burst speeds using Internet link

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the **AutoDetect Public IP address** as shown below.
3. Navigate to **Access Interfaces**, click the “+” button to add interface details specific for the Internet link.
4. Populate Access Interface for Virtual IP address and gateway as shown below.

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC-BR-INET-AI-1	INET_BR-3-4	10.18.0.9	10.18.0.1	Primary	<input checked="" type="checkbox"/>	

To create MPLS Link

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the MPLS link.
2. Populate MPLS link details as shown below.
3. Navigate to **Access Interfaces**, click the “+” button to add interface details specific for the MPLS link.
4. Populate Access Interface for Virtual IP address and gateway as shown below.

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_DC-MPLS-...	DC_MPLS	192.168.1.10	192.168.1.1	Primary	<input type="checkbox"/>	

Routes are auto-created based on above configuration. In case there are additional subnets specific to this remote branch office, then specific routes need to be added identifying which gateway to direct traffic to in order to reach those backend subnets.

Network IP Address	Cost	Service Type	Gateway IP Address	Delete
10.17.0.9/24	5	Local		
10.18.0.9/24	5	Local		
0.0.0.0/0	16	Passthrough		

After completing configuration for DC and Branch sites, you will be alerted to resolve audit error on both DC and BR sites. In this example, we will resolve the Audit Error related to Private Intranet WAN Link [SJC_DC-MPLS].

Note

By default the system will generate paths for WAN Links defined as access type Public Internet (highlighted).

Audit Error:

At Site 'SJC_DC' WAN Link 'SJC_DC-MPLS': no 'add Virtual Path usage' command was successful

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC-BR-MPLS-AI-1	MPLS_BR-1-2	10.17.0.9	10.17.0.1	Primary	<input checked="" type="checkbox"/>	

Audit Error:

WAN link 'SJC_DC-MPLS' has usage for Virtual Path 'SJC-BR-SJC_DC', but no paths were added to or from this WAN link for this Virtual Path

You would be required to use the auto-path group function or enable paths manually for WAN Links with an access type of Private Internet. Paths for MPLS links can be enabled by clicking on the Add operator (in the green rectangle).

Add Path

From Site:

From WAN Link:

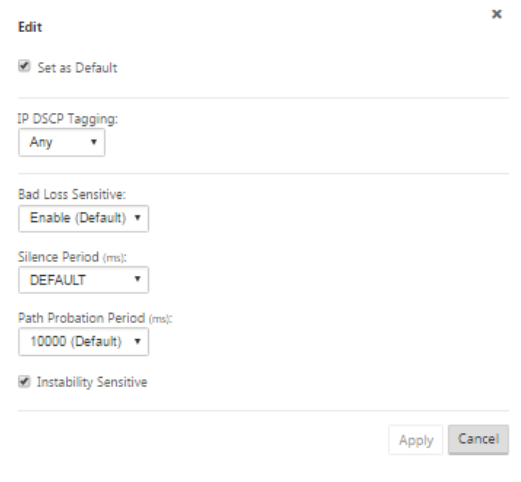
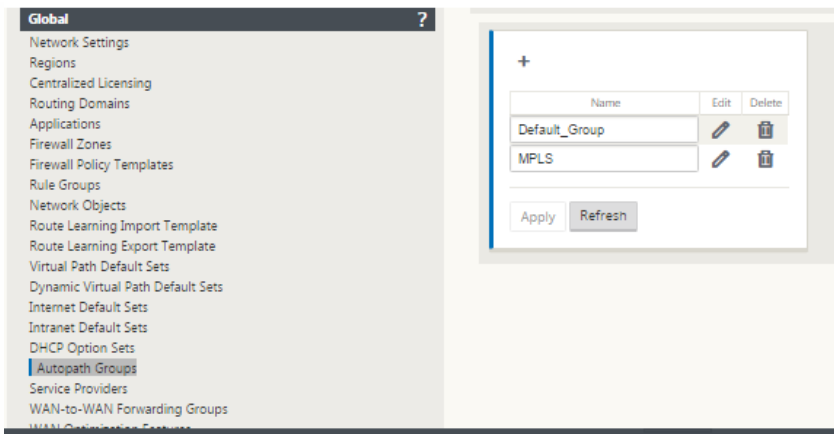
To Site:

To WAN Link:

Reverse Also

Create an Autopath Group

1. Navigate to **Global** tab. Click on the [+] sign next to **Autopath Groups**.
2. Configure the Autopath Group created as per requirement and click **Apply**.

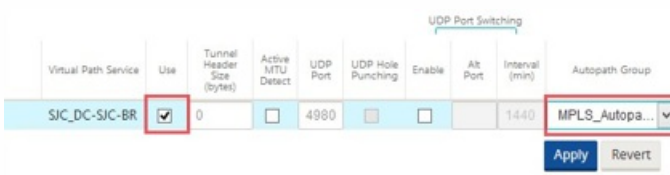


3. Rename the Autopath Group [Optional].

4. Map the Autopath Group to the Virtual Paths of Intranet WAN links at respective sites.

No two Autopath Groups can be marked as default. If marked would lead to an Audit Error.

After mapping the Autopath Group to the Virtual Paths of Intranet WAN, the paths should be automatically populated (highlighted).



1. Select the Virtual Paths under WAN Links for respective sites and no Autopath Group would be mapped.
2. Click the [+] sign next to Paths to add Virtual Paths manually.



3. Select the Virtual Paths WAN Links for each site.

After manually adding the virtual paths for WAN links with access type Private Intranet, it gets populated under Paths (highlighted).

After completing all the above steps, proceed to [Preparing the SD-WAN Appliance Packages](#) on the MCN topic.

Policy Based Routing configuration on the PBR Router

Interface connected to the LAN

- Router# configure terminal
- Router(config)# interface FastEthernet0/1
- Router(config-if)# description ToLAN
- Router(config-if)# ip address 10.10.11.1 255.255.255.0
- Router(config-if)# duplex auto
- Router(config-if)# speed auto

Interface connect to the MPLS WAN Link

- Router# configure terminal
- Router(config)# interface GigabitEthernet0/0
- Router(config-if)# description To-MPLS-WAN
- Router(config-if)# ip address 10.20.0.2 255.255.255.0
- Router(config-if)# duplex auto
- Router(config-if)# speed auto

Interface connected to the INET WAN Link

- Router# configure terminal
- Router(config)# interface GigabitEthernet0/2/0
- Router(config-if)# description To-INET-WAN
- Router(config-if)# ip address 10.19.0.2 255.255.255.0
- Router(config-if)# duplex auto
- Router(config-if)# speed auto

Note: Interface GigabitEthernet0/1 on the PBR router is connected to the SD-WAN port 1/1, it is in 1-arm mode and this one port will serve traffic for MPLS and INET links.

- Router# configure terminal

- Router(config)# interface GigabitEthernet0/1
- Router(config-if)# description To-SDWAN-link
- Router(config-if)# ip address 192.168.1.1 255.255.255.0

Static Route Configuration (Route to the client/remote subnets):

- MPLS 10.17.0.0/24 via next hop WAN router MPLS 10.20.0.1
 - INET 10.18.0.0/24 via next hop WAN router/FW INET 10.19.0.1
-
- Router# configure terminal
 - Router(config)# ip route 10.17.0.0 255.255.255.0 10.20.0.1
 - Router(config)# ip route 10.18.0.0 255.255.255.0 10.19.0.1

Route Map Definition

Access Control List Configuration:

Configure ACL's to define the traffic to be sent to and from the SD-WAN appliance.

1- From LAN to SD-WAN Appliance

As per topology, the LAN subnets are 10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc. To send traffic from LAN to the SD-WAN, configure a unidirectional ACL (from LAN to any).

- Router# configure terminal
- Router(config)# ip access-list extended server_side
- Router(config)# permit ip 10.10.0.0 0.0.255.255 any

2- From SD-WAN Appliance to physical WAN Links

- Router# configure terminal
- Router(config)# ip access-list extended MPLS_Link
- Router(config)# permit ip 192.168.1.10 0.0.0.0 any
- Router# configure terminal
- Router(config)# ip access-list extended INET_Link
- Router(config)# permit ip 192.168.1.11 0.0.0.0 any

Route Map Configuration:

Define the route-map matching the ACL's.

Route map for LAN traffic:

Next hop will be any of SD-WAN Virtual IP's (VIP).

MPLS VIP 192.168.1.10

INET VIP 192.168.1.11

In this case, we chose MPLS VIP 192.168.1.10 as next hop and also added a health check to make sure if the SD-WAN fails,

traffic is not routed to it.

- Router# configure terminal
- Router(config)# route-map server_side_VW_PBR permit 10
- Router(config-route-map)# match ip address server_side
- Router(config-route-map)# set ip next-hop verify-availability 192.168.1.10 10 track 123

Note: The above command configures the route map to verify the reachability of the tracked object. The tracking process provides the ability to track individual objects, such as ICMP ping reachability, routing adjacency, an application running on a remote device, a route in the Routing Information Base (RIB) or to track the state of an interface line protocol.

Route map for WAN traffic:

Next hop will be MPLS Router and Firewall for respective WAN links.

- Router# configure terminal
- Router(config)# route-map WAN_VW_PBR permit 20
- Router(config-route-map)# match ip address MPLS_Link
- Router(config-route-map)# set ip next-hop verify-availability 10.20.0.1 20 track 124
- Router# configure terminal
- Router(config)# route-map WAN_VW_PBR permit 30
- Router(config-route-map)# match ip address INET_Link
- Router(config-route-map)# set ip next-hop verify-availability 10.19.0.1 30 track 125

Apply the Route Map to the interface:

Router# configure terminal

- Router(config)# interface FastEthernet0/1
- Router(config-if)# ip policy route-map server_side_VW_PBR
- Router(config-if)# duplex auto
- Router(config-if)# speed auto
- Router# configure terminal
- Router(config)# interface GigabitEthernet0/1
- Router(config-if)# ip policy route-map WAN_VW_PBR
- Router(config-if)# duplex auto
- Router(config-if)# speed auto

MPLS Router Configuration (Gateway 10.20.0.1)

- Add route on MPLS router to reach MPLS VWAN VIP on the Data Center.
- MPLS VIP subnet 192.168.1.0/24 via next hop PBR router MPLS link 10.20.0.2
- Router# configure terminal
- Router(config)# ip route 192.168.1.0 255.255.255.0 10.20.0.2

Firewall Configuration (Gateway 10.19.0.1)

Add route on Firewall to reach INET VWAN VIP on the Data Center.

INET VIP subnet 192.168.1.0/24 via next hop PBR router INET link 10.19.0.2

- Router# configure terminal
- Router(config)# ip route 192.168.1.0 255.255.255.0 10.19.0.2

Building a SD-WAN Network

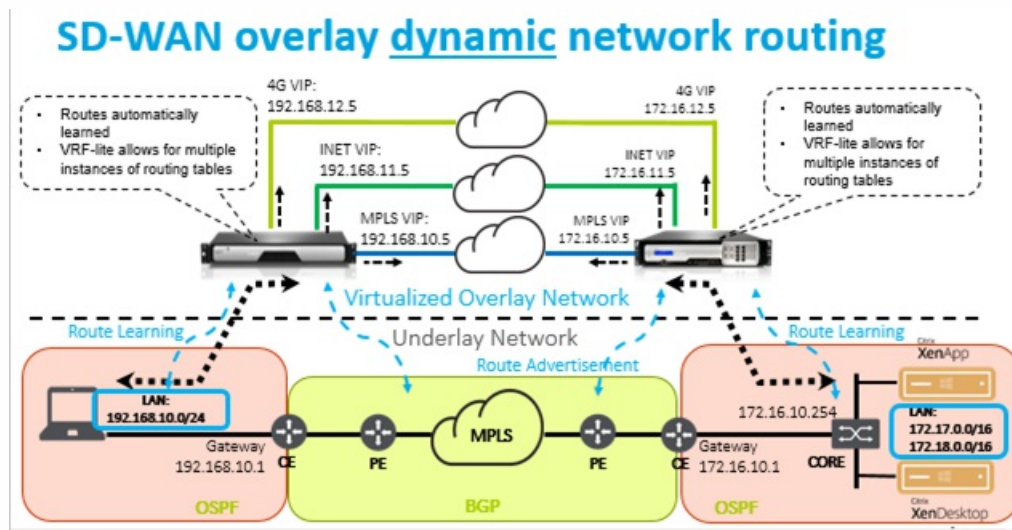
Mar 01, 2018

To build an SD-WAN overlay network without the need to statically build SD-WAN overlay route tables:

1. Create a WAN Path tunnel across each WAN link between two SD-WAN appliances.
2. Configure Virtual IP to represent the endpoint for each WAN link. You can establish encrypted WAN paths through the current L3 Network.

3. Aggregate 2, 3, and 4 WAN paths (physical links) into a single Virtual Path allowing packets to traverse the WAN utilizing the SD-WAN overlay network instead of the existing underlay which is least intelligent and cost inefficient.

- Local – subnet resides at this site (advertised to SD-WAN environment)
- Virtual Path – sent through Virtualized Path to the selected site appliance
- Intranet – sites with no SD-WAN appliance
- Internet – internet bound traffic
- Pass-through – untouched traffic, in one bridge interface out the other
- Default route (0.0.0.0/0) defined. Used for pass-through traffic not captured by the SD-WAN overlay route table, or utilized at the MCN to instruct clients sites to forward all traffic back to MCN node for back-haul of internet traffic.



WAN Optimization Only with Enterprise Edition

Mar 01, 2018

The SD-WAN Enterprise Edition appliances contain fully featured WAN Optimization functionality in addition to WAN Virtualization. Some customers prefer to implement WAN Optimization functionality before migrating to SD-WAN services. This deployment use case provides the steps to utilize Enterprise Edition appliances to utilize WAN optimization services.

NetScaler SD-WAN Product Platform Editions include the following appliances:

- SD-WAN: SD-WAN Standard Edition appliance
- Enterprise: SD-WAN Enterprise Edition appliance
- WANOP: SD-WAN WANOP Edition appliance

To integrate Enterprise Edition appliances into an existing distributed WANOP network, you need to configure SD-WAN (Physical or Virtual) appliance at the DC site as the MCN. The SD-WAN appliance manages all configuration of the network. A Virtual Path is established between the Branch site and MCN at the DC site. This Virtual Path is only used for sending control traffic between the appliances. At the branch appliance, the data traffic is processed as an intranet service. The intranet traffic is not encapsulated and traverses over existing WAN link to reach the DC site. A WANOP appliance at the DC site needs to be in the traffic path to provide end-to-end traffic optimization.

For customer sites that do not have SD-WAN hardware appliance at the head-end, VPX appliances in a HA pair (two Virtual WAN VPXs) can be used as MCN in one-arm mode. For the one-arm mode, PBR rules on the third-party router are required to redirect traffic to the SD-WAN appliance.

This document assumes that the DC site appliances are deployed in HA mode for redundancy. However, note that HA mode is not mandatory for this deployment

Prerequisites

- A pair of WANOP appliances and a pair of SD-WAN appliances deployed in HA mode at the DC site.
- An Enterprise Edition appliance at the Branch site.

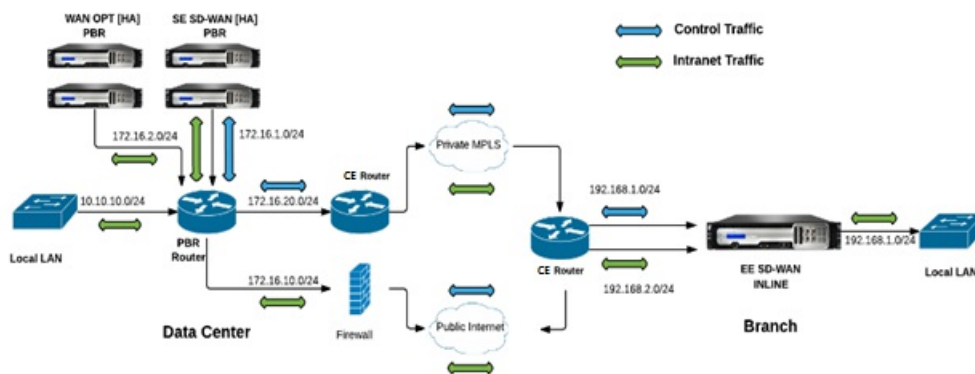
SD-WAN Standard Edition and WANOP Appliances in PBR Deployment

In the below illustration, both the SD-WAN SE and WAN OP appliances at the DC site are deployed in one-arm mode. The SD-WAN appliance supports PBR deployment while the WANOP appliance supports both PBR and WCCP. The control traffic (Virtual Path traffic) received from WAN at the DC site will be redirected to the SD-WAN appliance by the PBR Router. The data traffic will be redirected to WAN Optimization appliance by the PBR Router.

Traffic flow for WAN to DC LAN:

- CE (Customer Edge) Router -> PBR Router -> SD-WAN -> PBR Router -> LAN
- CE (Customer Edge) Router -> PBR Router -> WAN OPT -> PBR Router -> LAN

The same traffic flow will be followed in the reverse direction.



SD-WAN Standard Edition in PBR mode and WANOP in Inline Deployment

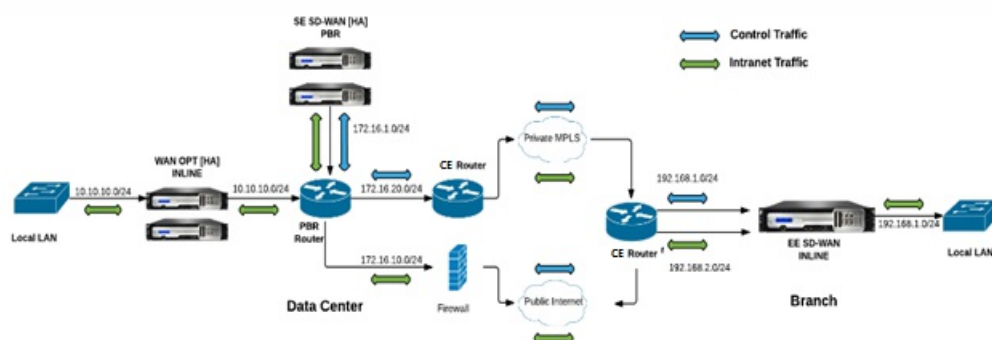
In the below illustration, the SD-WAN appliance at the DC site is deployed in one-arm mode while the WANOP appliance is deployed in inline mode.

The control traffic (Virtual Path traffic) received from WAN at the DC site will be redirected to the SD-WAN appliance by the PBR Router. The data traffic will be forwarded to WAN Optimization appliance (inline) by the PBR Router.

Traffic flow for WAN to DC LAN:

- CE (Customer Edge) Router -> PBR Router -> SD-WAN -> PBR Router -> LAN
- CE (Customer Edge) Router -> PBR Router -> WAN OPT -> LAN

The same traffic flow will be followed in the reverse direction.



1. Configure the SD-WAN Appliance at DC [MCN] to establish Virtual Paths between DC and Branch sites.

See, <http://docs.citrix.com/en-us/netscaler-sd-wan/9-1/configuration-topics/configuring-virtual-path-service-between-mcn-client-sites.html>

2. Configure Intranet Service at the DC site.

a) On the MCN (DC site), go to **Configuration > Virtual WAN > Configuration Editor > Connections > Site (DC) > Intranet Services**. Click the [+] sign to add an Intranet Service.

b) Select the **WAN Link(s)** for Intranet Service, and then click **Apply**.

c) Navigate to **Routes** under the same **Site (DC)**, click [+] sign to add the remote network with cost lower than 5, and select click **Add**.

For example - Enter **192.168.1.0/24** in the **Network IP address** field with cost 4 and select **Service Type** as

Intranet.

Note

Cost at each site should be less than 5 for the intranet route to take precedence.

3. Configure Intranet Service at the Branch site.

a) Repeat sub-steps a to c from **step 2** above on the Branch site.

For example - Enter **172.16.1.0/24** in the Network IP address field with cost 4 and select **Service Type** as **Intranet**.

4. Perform **Change Management** to upload and distribute configuration to the Branch site.

See, [Exporting configuration package and change management](#)

By default, the traffic is sent from Branch to DC through the Virtual Path.

Note

The PBR router needs to be configured to redirect traffic as per the deployment steps provided.

For more information about configuring WAN Optimization, refer to the CloudBridge 9.1 documentation at: [Enabling-configuring-wan-optimization](#)

Hairpin Mode

Mar 01, 2018

With a hairpin deployment, you can implement use of a Remote Hub site for internet access through backhaul or hairpin when local internet services are unavailable or are experiencing a slow traffic. You can leverage high bandwidth routing between client sites by allowing backhauling from specific sites.

The purpose of a hairpin deployment from a non-WAN to a WAN forwarding site is to provide customers with a more efficient deployment process and more streamlined technical implementation. Customers will have the ability to use a remote hub site for internet access when needs arise, and can route flows through the virtual path to the SD-WAN network.

For example, consider an administrator with multiple SD-WAN Sites, A and B. Site A has poor internet service. Site B has usable internet service, with which you want to backhaul traffic from site A to site B only. You can try to accomplish this without the complexity of strategically weighted route costs and propagation to sites that should not receive the traffic.

Also, the route table is not shared across all sites in a Hairpin deployment. For example, if traffic is hairpin'ned between Site A and Site B through Site C, then only Site C would be aware of site A's and B's routes. Site A and Site B will not share each other's route table unlike in WAN-to-WAN forwarding.

When traffic is Hairpin'ned between Site A and Site B through Site C, the static routes are required to be added in Site A and Site B indicating that the next hop for both the sites is the intermediate Site C.

WAN-to-WAN Forwarding and Hairpin deployment have certain differences, namely:

- a. Dynamic Virtual Paths are not configured. At all times, the intermediate site will see all the traffic between the two sites.
- b. Does not participate in WAN-to-WAN Forwarding groups.

WAN-to-WAN Forwarding and Hairpin deployment are mutually exclusive. Only one of them can be configured at any given point in time.

NetScaler SD-WAN SE/EE and VPX (virtual) appliances support hairpin deployment. You can now configure a 0.0.0.0/0 route to hairpin traffic between two locations without affecting any additional locations. If hairpinning used for intranet traffic, specific Intranet routes are added to the client site to forward intranet traffic through the virtual path to the hairpin site. Enabling WAN-to-WAN forwarding to accomplish hairpin functionality is no longer required.

You can configure hairpin deployment through the SD-WAN web management interface from the configuration editor.

DC_CB_vWAN
 Remote_CB_vWAN

Connections

- Default Sets
- Applications
- Autopath Groups
- WAN-to-WAN Forwarding Groups
 - DC_CB_vWAN
 - WAN-to-WAN Forwarding

Group:

Enable WAN-to-WAN Forwarding

Route Cost:

Enable Site as Intermediate Node

If enabled, this Site may serve as a mediator for the creation and destruction of Dynamic Virtual Paths between two or more Sites connected to this Site.

Branch01

- WAN-to-WAN Forwarding
- Virtual Paths
- Internet Services
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall
- Routes

Order	Network IP Address	Routing Domain
1	172.16.1.95/24	Default_RoutingDomain
2	172.16.2.95/24	Green
3	0.0.0.0/0	Default_RoutingDomain
4	0.0.0.0/0	Green

Edit Route

Edit Route

Network IP Address:
 Routing Domain:
 Cost:
 Service Type:
 Gateway IP Address:

Next Hop Site:

Eligibility Based On Path

Path:

Note

Also, note the following points to consider when implementing the two box mode:

- When a routing domain is selected to be redirected to the WANOP appliance from the Configuration Editor, it should be added in the Interface Group for which WCCP is enabled.
- The same routing domain's traffic should be selected on the partner site as well. For example; **MCN > Branch01** to observe WAN optimization benefits.
- If a routing domain is selected in the interface group on which WCCP is enabled, another interface group which contains the bridged interfaces should have the same routing domain configured. Only if WCCP enabled interface group has the routing domain configured it is not enough to transmit the end-to-end traffic flowing with WAN optimization benefits.

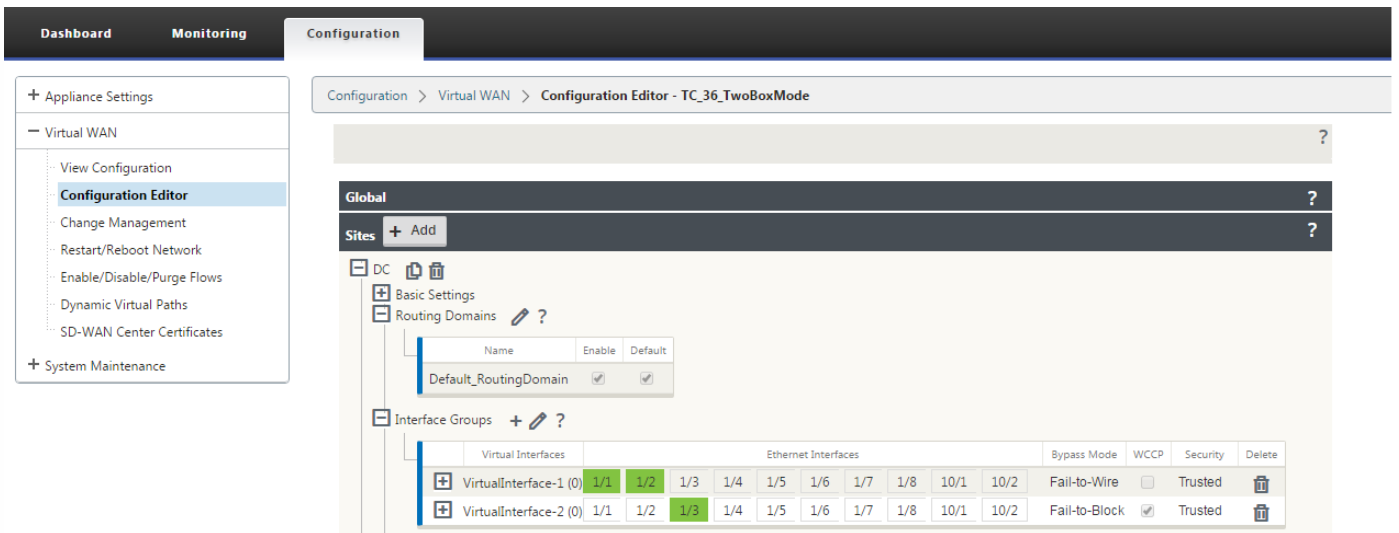
To configure two-box mode solution in the Standard Edition appliance at the DC or Branch site:

1. In the NetScaler SD-WAN SE web management interface, go to **Configuration > Virtual WAN > Configuration Editor**. Open an existing configuration package or create a new package.
2. In the chosen configuration package, go to the **Advanced** tab to view the configuration details.
3. Open **Global** settings and expand **Routing Domains** to view that the **Redirect to WANOP** checkbox is enabled.

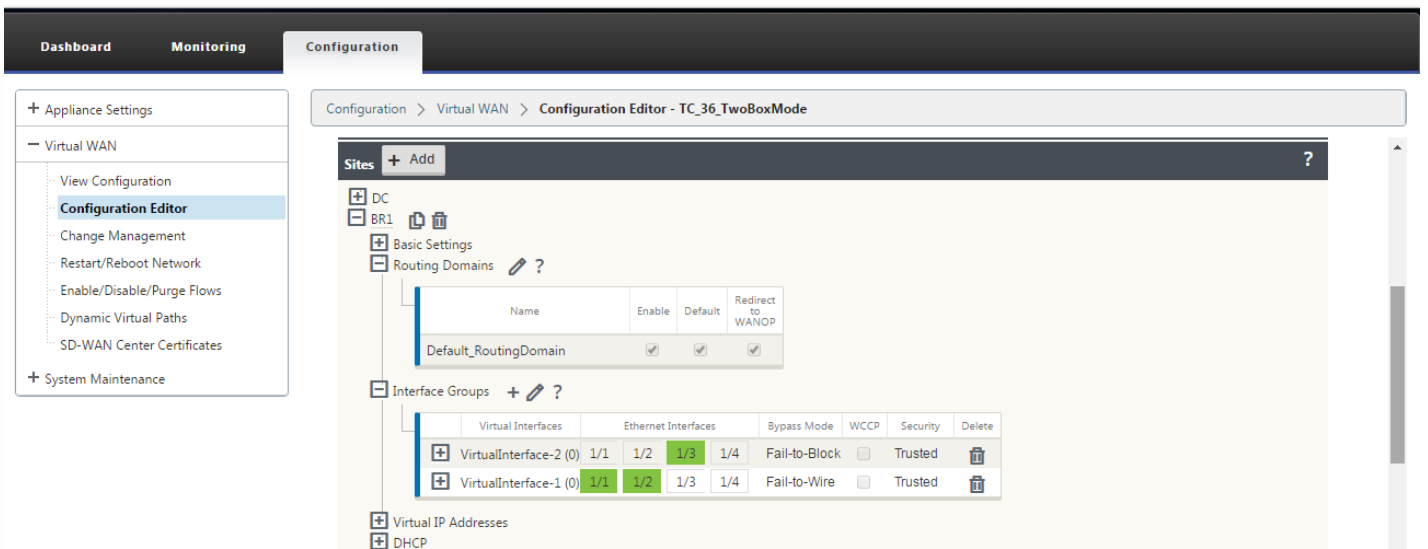
The screenshot shows the NetScaler SD-WAN SE web management interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar shows 'Virtual WAN' settings, with 'Configuration Editor' selected. The main content area displays the 'Configuration Editor - TC_36_TwoBoxMode' page. The 'Global' settings are expanded, and the 'Routing Domains' section is visible. A table shows the 'Default_RoutingDomain' with 'Default' and 'Redirect to WANOP' checkboxes checked.

Name	Default	Redirect to WANOP	Delete
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

4. Expand DC to enable **WCCP** for the **Virtual Interface** under **Interface Group** settings that will signify which virtual network interface the appliance will be enabled for.



5. Expand **Sites+ Add** to view the Branch routing domain and interface group settings. Under the Branch site, the **Redirect to WANOP** checkbox is enabled for Routing Domains.

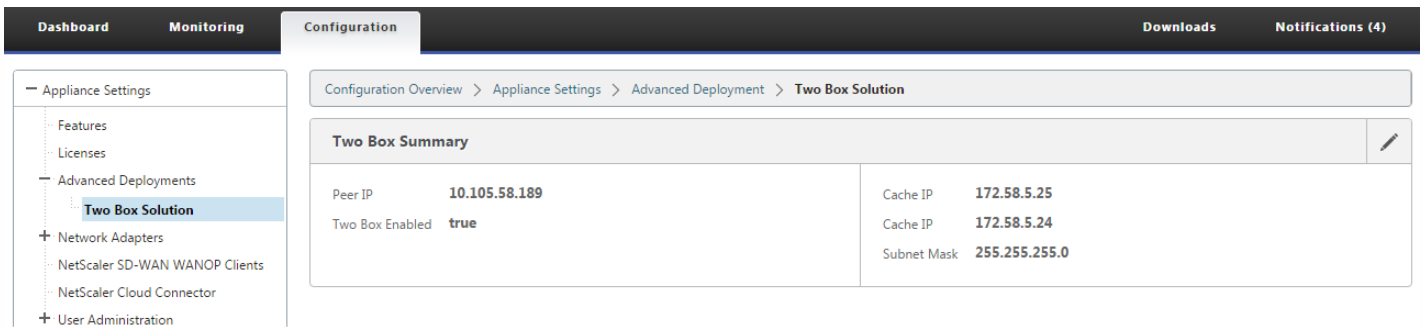


Note

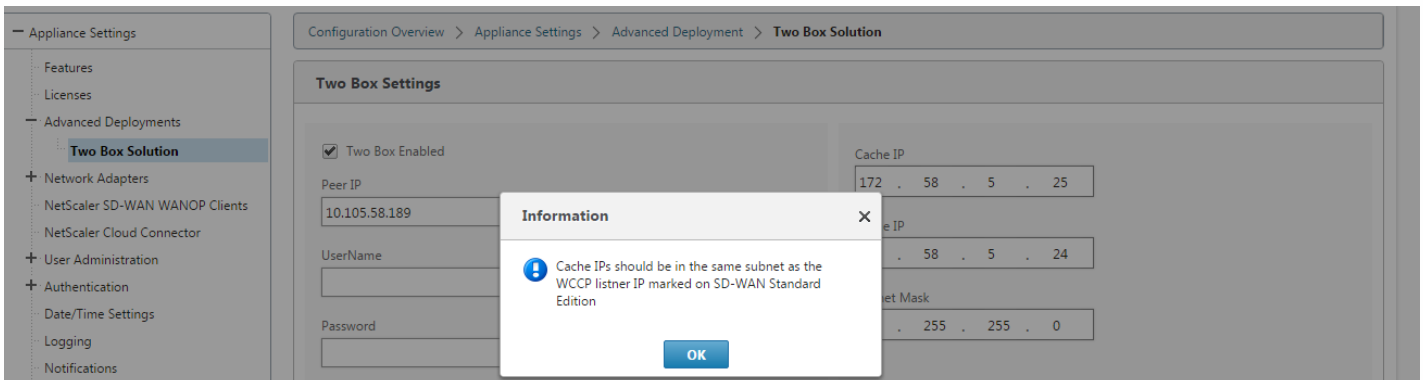
The WCCP listener should be enabled only for those virtual network interfaces which have only ONE Ethernet Interface configured. This indicates that WCCP Listener should not be enabled on a BRIDGED Pair. It is intended to be enabled on the ONE-ARM interface between the SD-WAN SE and SD-WAN WANOP appliances.

To configure two-box deployment mode in the SD-WAN WANOP appliance web GUI:

1. In the NetScaler SD-WAN WANOP web management interface, go to **Configuration > Appliance Settings > Advanced Deployments > Two Box Solution**.



2. Click the Edit icon to edit the two box mode settings. Information dialog about **Cache IPs** is displayed. Click **OK**.



3. Enable the **Two Box Enabled** checkbox.

4. Enter the **Peer IP**. Peer IP is the Netscaler SD-WAN Standard Edition appliance IP address.

5. Enter the user credentials and click **Apply**.

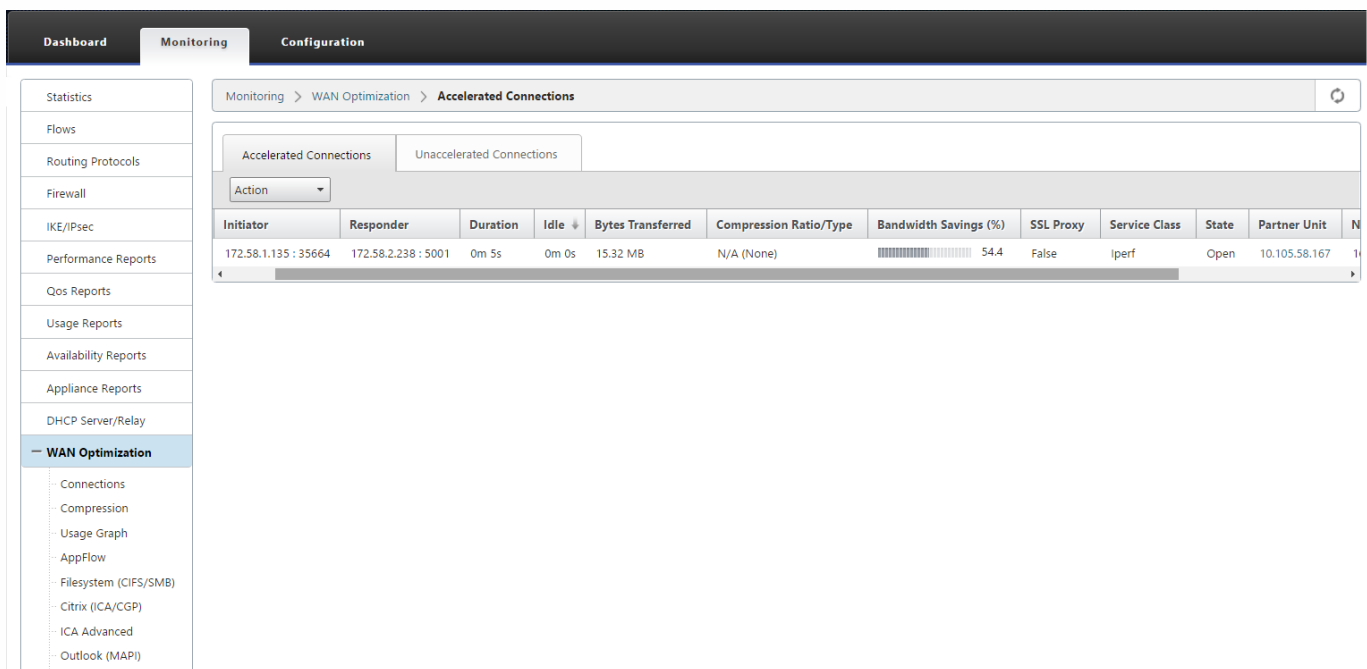


Following are some of the two box mode configuration and manageability points to consider for deployment:

- * SD-WAN WANOP configurations mentioned below can be configured from SD-WAN SE configuration editor as a unified pane

- SERVICE CLASS
- APPLICATION CLASSIFIER
- FEATURES
- SYSTEM TUNING

You can monitor SD-WAN WANOP traffic directly using the Monitoring page of the SD-WAN SE appliance's web UI. This allows for a single pane monitoring of both the SDWAN-SE and SDWAN-WO appliances while processing data traffic. You can view the connection details, secure partner details and so on under the WAN Optimization node in the SDWAN-SE UI.



You can configure APPFLOW directly from the SDWAN-SE **Configuration** page under **APPFLOW** node. This enables SDWAN-SE to act as a single pane for configuration of APPFLOW and other data processing configuration attributes such as Service Class, Application Classifiers and so on. The configuration done on the SDWAN-SE reflects on the SDWAN-WO configuration, maintaining seamless APPFLOW functionality support.

SD-WAN WANOP already discovered by an insight center, if used in Two Box Mode should be isolated and not configured using MAS/Insight until this mode is turned off. This is because the configuration of WANOP for traffic processing is governed by the SD-WAN SE appliance in the Two Box Mode.

Advanced Optimizations or Secure Acceleration should be directly configured on the SDWAN-SE appliance like we would configure on the SDWAN-WO appliance. This helps maintain a single pane of configuration of configurations like Domain Join or Secure Acceleration/SSL Profile creation for Advanced optimizations or SSL Proxy.

* Licensing should be separately managed for each of SD-WAN SE and SD-WAN WANOP appliances.

* Software Upgrade should be separately managed for each of SD-WAN SE and SD-WAN WANOP appliances with the respective software packages. For example, tar.gz for SD-WAN SE and upgrade upg for SD-WAN WANOP.

* Data path integration should be configured between SD-WAN SE and External WANOP appliances through the WCCP deployment mode.

- At data path level both WCCP and Virtual WAN features are offered through data path integration between WANOP and SE externally in one-arm mode to obtain optimization benefits.

Unified Configuration and Monitoring

When you enable the two box mode with SD-WAN SE and SDWAN-WANOP appliances, you can view the configuration in the SD-WAN SE appliance similar to how you can view two box configuration with the SD-WAN-EE appliance.

- a. Go to **Configuration > Virtual WAN > WAN Optimization**
- b. Appflow node under **Configuration > Appliance Settings**
- c. WAN Optimzation node under Configuration.

This information is redirected from the SD-WAN WANOP appliance which is in Two box mode with the SD-WAN SE appliance.

Configuration related to WANOP, such as SSL Acceleration and AppFlow can now be performed from SD-WAN SE web GUI.

Traffic related statistics, such as Connections, Compression, CIFS/SMB , ICA Advanced, MAPI and partners can now be monitored from SD-WAN SE web GUI under **Monitoring > WAN Optimization** similar to the SD-WAN Enterprise edition appliance.

The screenshot displays the Citrix NetScaler SD-WAN 5100-4000-SE web GUI. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' tab is active, showing a breadcrumb 'Configuration > WAN Optimization'. A yellow warning banner indicates 'SSL Optimization status : DISABLED' with an 'Enable' button. Below this, the 'Secure Peering' section shows 'Keystore Status' as 'Opened' and 'Secure Peering Status' as 'Enabled'. At the bottom, there are two icons: 'SSL Profile' and 'Windows Domain'.

Citrix NetScaler SD-WAN 5100-4000-SE

Dashboard | **Monitoring** | Configuration

Monitoring > Statistics

Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Refresh Show latest data.

Path Statistics Summary

Filter: in Any column Apply

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Ser
1	MCN5K-WL-1	Branch-VPX-WL-1	GOOD	GOOD	Static
2	Branch-VPX-WL-1	MCN5K-WL-1	GOOD	GOOD	Static

Showing 1 to 2 of 2 entries
Bandwidth calculated over the last 0.961 seconds

To change the management IP address of SDWAN-WANOP appliance in Two box mode:

1. Execute command `clear_wo_sync` on the SD-WAN SE appliance. This ensures that the SD-WAN WANOP IP address information is cleared for GUI redirection.
2. Disable and enable Two box mode config on the SD-WAN WANOP appliance. The new IP address (changed IP) of SD-WAN WANOP appliance is sent to SD-WAN SE. The new changed IP address is displayed in the URL redirection pages.

The management IP address is used for peer IP address configuration.

To disable or decouple the SD-WAN WANOP and SD-WAN SE appliances from the Two Box mode:

- a. Disable the Two Box mode from SD-WAN WANOP appliance.
- b. It is expected to still see the SD-WAN WANOP appliance two box mode pages in the SD-WAN SE web GUI. To clear these pages, execute the command: `clear_wo_sync`.

High Availability

Apr 12, 2018

This topic covers the High Availability (high availability) deployments and configurations supported by SD-WAN appliances (Standard Edition and Enterprise Edition).

SD-WAN appliances can be deployed in high availability configuration as a pair of appliances in Active/Standby roles. There are three modes of high availability deployment:

- Parallel Inline high availability
- Fail-to-Wire high availability
- One-Arm high availability

These high availability deployment modes are similar to Virtual Router Redundancy Protocol (VRRP) and use a proprietary SD-WAN protocol. Both Client Nodes (Clients) and Master Control Nodes (MCNs) within an SD-WAN network can be deployed in a high availability configuration. The primary and secondary appliance must be the same platform models.

In high availability configuration, one SD-WAN appliance at the site is designated as the Active appliance and is continuously monitored by the Standby appliance. Configuration is mirrored across both appliances. If the Standby appliance loses connectivity with the Active appliance for a defined period, the Standby appliance assumes the identity of the Active appliance and takes over the traffic load. Depending on the deployment mode, this fast failover has minimal impact on the application traffic passing through the network.

One-Arm mode:

In One-Arm mode, the high availability appliance pair is outside of the data path. Application traffic is redirected to the appliance pair with Policy Based Routing (PBR). One-Arm mode is implemented when a single insertion point in the network is not feasible or to counter challenges of fail-to-wire. In the following illustration, the Standby appliance can be added to the same VLAN or subnet as the Active appliance and the router.

In One-Arm mode, it is recommended that the SD-WAN appliances do not reside in the data network subnets. The virtual path traffic does not have to traverse the PBR and avoids route loops. The SD-WAN appliance and router have to be directly connected, either through an Ethernet port or be in the same VLAN.

IP SLA Monitoring for Fall Back

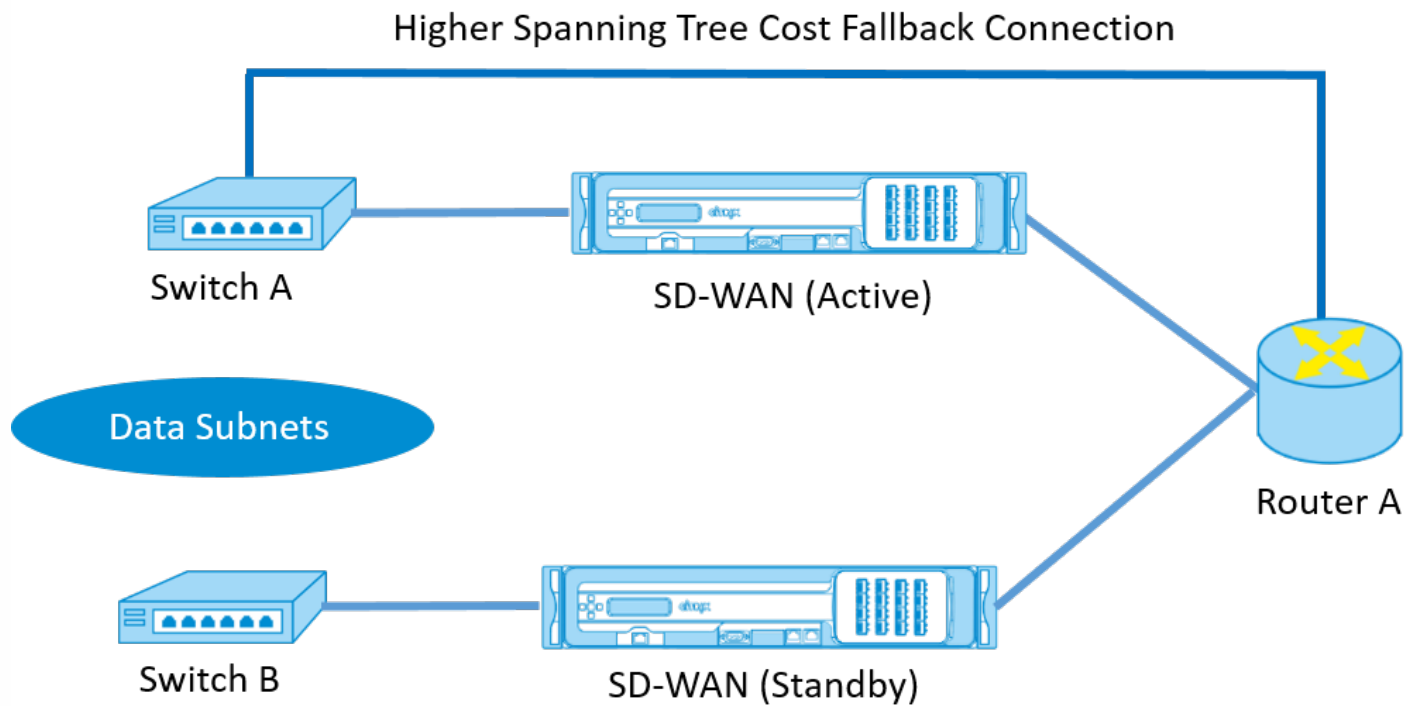
The active traffic flows even if the virtual path is down, as long as one of the SD-WAN appliances is active. The SD-WAN appliance redirects traffic back to the router because Intranet traffic. However, if both active/standby SD-WAN appliances become inactive, the router tries to redirect traffic to the appliances. IP SLA monitoring can be configured at the router to disable PBR, if the next appliance is not reachable. This allows the router to fall back to perform a route lookup and forward packets appropriately.

Parallel Inline high availability mode:

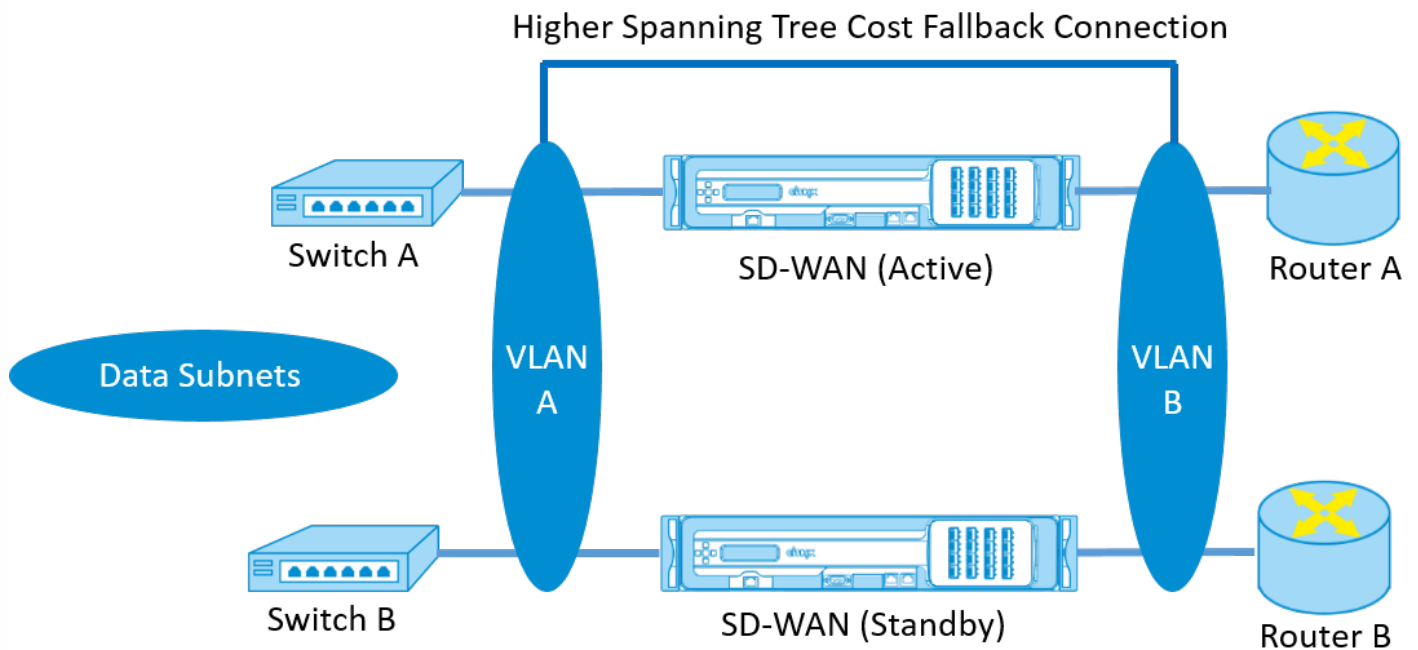
In Parallel Inline high availability mode, the SD-WAN appliances are deployed alongside each other, inline with the data path. Only one path through the Active appliance is used. It is important to note that bypass interface groups are configured to be fail-to-block and not fail-to-wire so that you don't get bridging loops during a failover.

The high availability state can be monitored through the inline interface groups, or through a direct connection between the appliances. External Tracking can be used to monitor the reachability of the upstream or downstream network infrastructure. For example; switch port failure) to direct high availability state change, if needed.

If both active and standby SD-WAN appliances are disabled or fail, a tertiary path can be used directly between the switch and router. This path must have a higher spanning tree cost than the SD-WAN paths so that it is not used under normal conditions. Failover in parallel inline high availability mode is a quick and nearly hitless, because no physical state change occurs. Fallback to the tertiary path is not hitless and can block traffic for 5-30 seconds depending on the spanning tree configuration. If there are out of path connections to other WAN Links, both appliances must be connected to them.



In more complex scenarios, where multiple routers might be using VRRP, non-routable VLANs are recommended to ensure that the LAN side switch and routers are reachable at layer 2.



Fail-to-Wire mode:

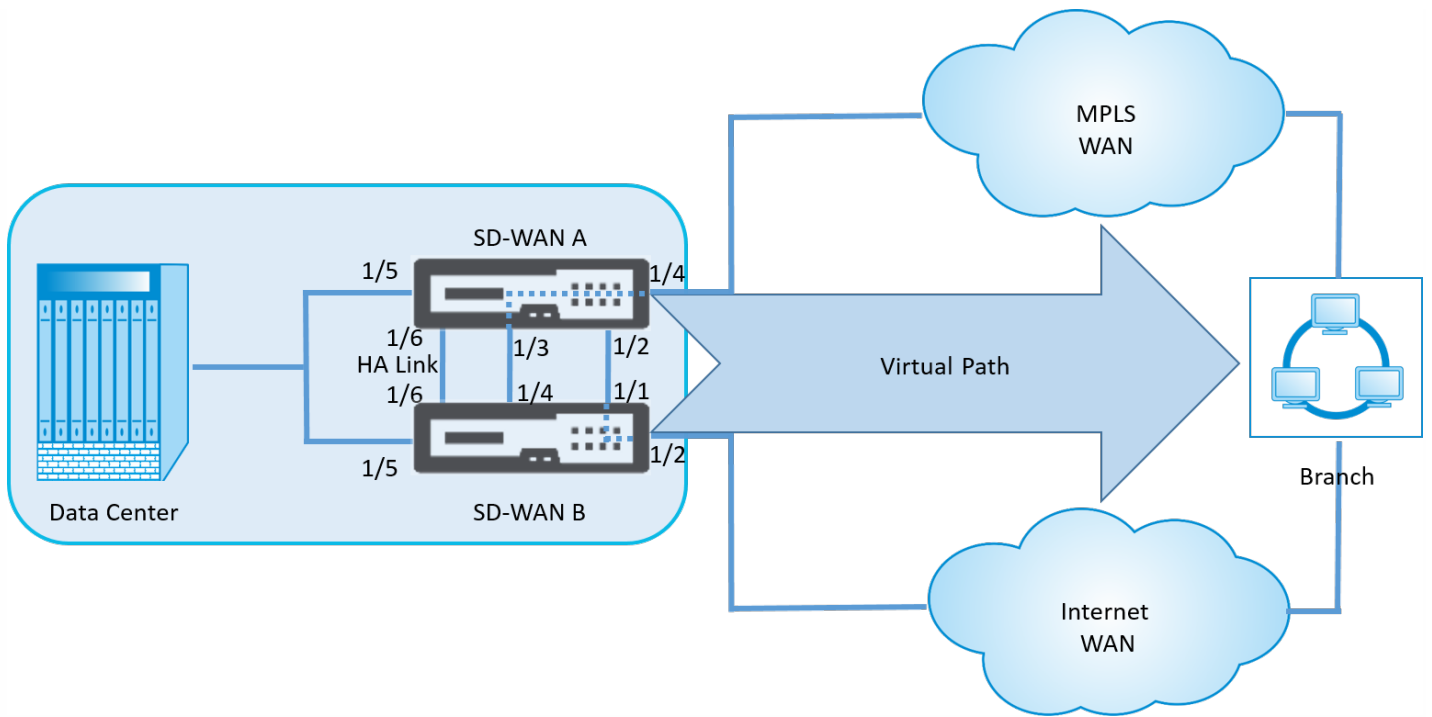
In fail-to-wire mode, the SD-WAN appliances are inline in the same data path. The bypass interface groups should be in the fail-to-wire mode with the Standby appliance in a passthrough or bypass state. A direct connection between the two appliances on a separate port must be configured and used for the high availability interface group.

Note

- High availability switchover in fail-to-wire mode takes longer period, approximately 10–12 seconds because of delay in ports to recover from Fail-to-Wire state.
- If the high availability connection between the appliances fails, both appliances go into Active state and cause a service interruption. This can be mitigated by assigning multiple high availability connections so that there is no single point of failure.
- It is imperative that in high availability Fail-to-Wire Mode, a separate port be used in the hardware appliance pairs for high availability control exchange mechanism to help with state convergence.

- Because of a physical state change when the SD-WAN appliances switch over from Active to Standby, failover can cause partial loss of connectivity depending on how long the auto-negotiation takes on the Ethernet ports.
- It is recommended that Fail-to-Wire mode be used on ports that are auto negotiated, as this increases failover time.

The following illustration shows an example of the Fail-to-Wire deployment.

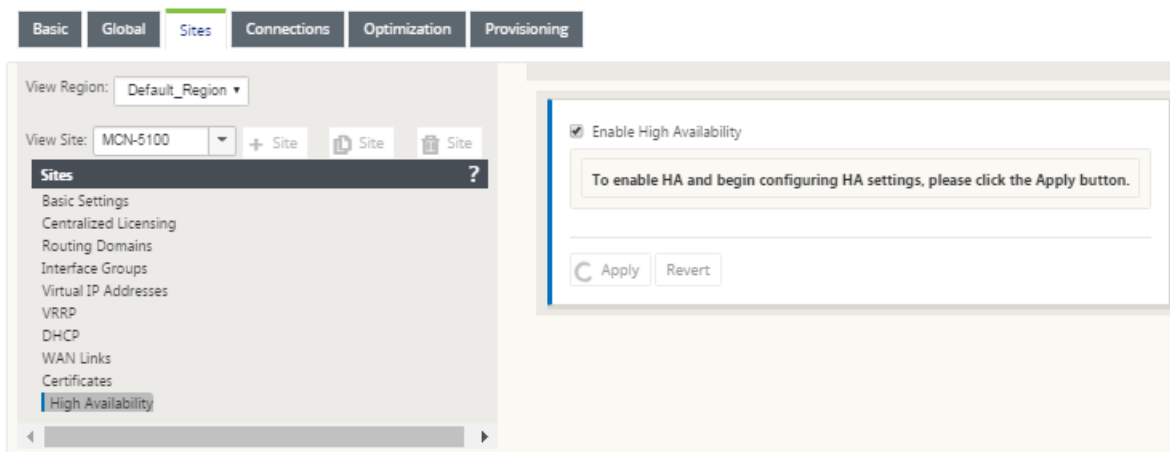


The One-Arm high availability configuration or Parallel Inline high availability configuration is recommended for data centers or Sites that forward a high volume of traffic to minimize disruption during failover.

If minimal loss of service is acceptable during a failover, then Fail-to-Wire high availability mode is a better solution. The Fail-to-Wire high availability mode protects against appliance failure and parallel inline high availability protects against all failures. In all scenarios, high availability is valuable to preserve the continuity of SD-WAN network during a system failure.

To configure high availability:

1. In the Configuration Editor, navigate to **Sites** > site name > **High Availability**. Select **Enable High Availability**, and click **Apply**.



Enable High Availability

HA Appliance Name: MATRIZ-1
Failover Time (ms): 1000
Shared Base MAC: AA:AA:AA:00:00:00

Swap Primary/Secondary Primary Reclaim HA Fail-to-Wire Mode

HA IP Interfaces +

	Virtual Interface	Control IP Addresses		Delete
		Primary	Secondary	
+ LAN (100)		10.0.15.241	10.0.15.240	
+ INET (0)		10.213.16.35	10.213.16.34	

2. Type values for the following parameter:

- **High availability Appliance Name:** This is the name of the high availability (secondary) appliance.
- **Failover Time:** This specifies the wait time (in milliseconds) after contact with the primary appliance is lost, before the standby appliance becomes active.
- **Shared Base MAC:** This is the shared MAC address for the high availability pair appliances. When a failover occurs, the secondary appliance has the same virtual MAC addresses as the failed primary appliance.
- **Swap Primary/Secondary:** When this is selected, if both appliances in the high availability pair come up simultaneously, the secondary appliance becomes the primary appliance, and takes precedence.
- **Primary Reclaim:** When this is selected, the designated primary appliance reclaims control upon restart after a failover event.
- **High availability Fail-to-Wire Mode:** Select this for Fail-to-wire high availability deployment mode.

Note

For hypervisor and cloud based platforms an extra parameter **Disable Shared Base MAC** is available. Choose this to disable the shared virtual MAC address.

Enable High Availability

Note: Below options Disable Shared Base MAC, Shared Base MAC, Swap Primary/Secondary, Primary Reclaim and HA Fail-to-Wire Mode options are Not Supported on cloud platforms.

HA Appliance Name: Failover Time (ms): Disable Shared Base MAC

Swap Primary Reclaim Shared Base MAC:

Primary/Secondary HA Fail-to-Wire Mode

HA IP Interfaces +

Control IP Addresses				
Virtual Interface	Primary	Secondary	Delete	
+ VirtualInterface-2 (0)	172.16.7.10	172.16.7.11		

Note

For hypervisor based platforms ensure that the promiscuous mode is enabled on the hypervisors to allow packet sourcing from high availability shared MAC address. If promiscuous mode is not enabled, you can enable **Disable Shared Base MAC** option.

3. Click + next to **high availability IP Interfaces** to configure interface groups. Type Values for the following parameters:

- **Virtual Interface** – This is the Virtual Interface to be used for communication between the appliances in the high availability pair. This interface monitors the Active appliance for reachability. For One-Arm high availability mode, only one interface group is required.
- **Primary** – This is the unique Virtual IP address for the primary appliance. The secondary appliance uses this for communication with the primary appliance.
- **Secondary** – This is the unique Virtual IP address for the secondary appliance. The primary appliance uses this for communication with the secondary appliance.

4. Click + to the left of the new **high availability IP Interfaces** entry. In the **External Tracking IP Address** field, type the IP Address of the external device that responds to ARP requests to determine the state of the primary appliance.

5. Click **Apply**.

To monitor high availability configuration:

Log in to the SD-WAN web management interface for the Active and Standby appliance's for which high availability is

implemented. View high availability status under the **Dashboard** tab.

The screenshot shows the Dashboard tab selected. The System Status section displays 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

The High Availability Status section displays the following information:

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

The screenshot shows the Dashboard tab selected. The System Status section displays the following information:

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

The High Availability Status section displays the following information:

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

For Network Adapter details of Active and Standby high availability appliances, navigate to **Configuration > Appliance Settings > Network Adapters > Ethernet** tab.

Dashboard Monitoring Configuration

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

Dashboard Monitoring Configuration

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 enabled and the port is included in the Citrix configuration.
The settings for the high speed port 10/1 cannot be changed.

0/1	● MAC Address: 0a:25:90:c5:70:b4	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 1000Mb/s	Duplex: Full
1/1	● MAC Address: b2:1fd0:ab:70:ea	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
1/2	● MAC Address: 36:1f0e:02:91:03	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
1/3	● MAC Address: aa:af:3e:1f:3b:2b	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
1/4	● MAC Address: c2:3e:e5:22:93:05	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
1/5	● MAC Address: ee:6f:d3:aa:6b:bc	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 1000Mb/s	Duplex: Full

Zero Touch

Mar 09, 2018

Note

The Zero Touch Deployment service is supported only on select NetScaler SD-WAN appliances:

- NetScaler SD-WAN 210 Standard Edition
- NetScaler SD-WAN 410 Standard Edition
- NetScaler SD-WAN 2100 Standard Edition
- NetScaler SD-WAN 1000 Standard Edition (reimage required)
- NetScaler SD-WAN 1000 Enterprise Edition (reimage required)
- NetScaler SD-WAN 2000 Standard Edition (reimage required)
- NetScaler SD-WAN 2000 Enterprise Edition (reimage required)
- NetScaler SD-WAN AWS VPX instance

Zero Touch Deployment (ZTD) Cloud Service is a Citrix operated and managed cloud-based service which allows discovery of new appliances in the NetScaler SD-WAN network, primarily focused on streamlining the deployment process for NetScaler SD-WAN at branch or cloud service office locations. The ZTD Cloud Service is publicly accessible from any point in a network via public Internet access. The ZTD Cloud Service is accessed over Secure Socket Layer (SSL) Protocol.

The ZTD Cloud Services securely communicates with backend Citrix services hosting stored identification of Citrix customers who have purchased Zero Touch capable devices (e.g. NetScaler SD-WAN 410-SE, 2100-SE). The backend services are in place to authenticate any Zero Touch Deployment request, properly validating association between the Customer Account and the Serial Numbers of NetScaler SD-WAN appliances.

ZTD High-Level Architecture and Workflow

Data Center Site:

NetScaler SD-WAN Administrator – A user with Administration rights of the NetScaler SD-WAN environment with the following primary responsibilities:

- Configuration creation using NetScaler SD-WAN Center Network Configuration tool, or import of configuration from the Master Control Node (MCN) SD-WAN appliance
- Citrix Cloud Login to initiate the Zero Touch Deployment Service for new site node deployment.

Note

If your SD-WAN Center is connected to the internet through a proxy server, you have to configure the proxy server settings on the SD-WAN Center. For more information, see [How to Configure Proxy Server Settings for Zero Touch Deployment](#).

Network Administrator – A user responsible for Enterprise network management (DHCP, DNS, internet, firewall, etc.)

- If required, configure firewalls for outbound communication to FQDN *sdwanzt.citrixnetworkapi.net* from SD-WAN Center.

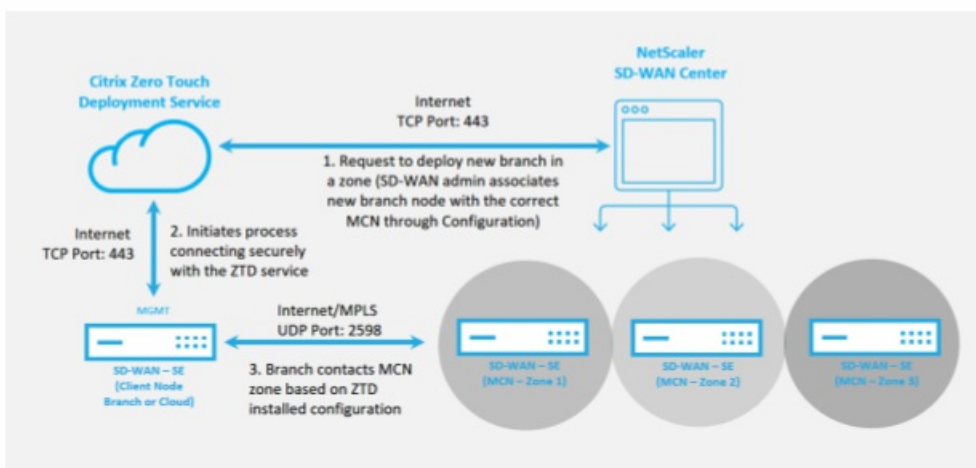
Remote Site:

Onsite Installer – A local contact or hired installer for on-site activity with the following primary responsibilities:

- Physically unpack the NetScaler SD-WAN appliance
- Reimage non-ZTD ready appliances
 - Required for: NetScaler SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
 - Not required for: NetScaler SD-WAN 410-SE, 2100-SE
- Power cable the appliance
- Cable the appliance for internet connectivity on the Management interface (e.g. MGMT, or 0/1)
- Cable the appliance for WAN link connectivity on the Data interfaces (e.g. apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, etc)

Note

The interface layout will be different each model, so please reference the documentation for identification of data and management ports.



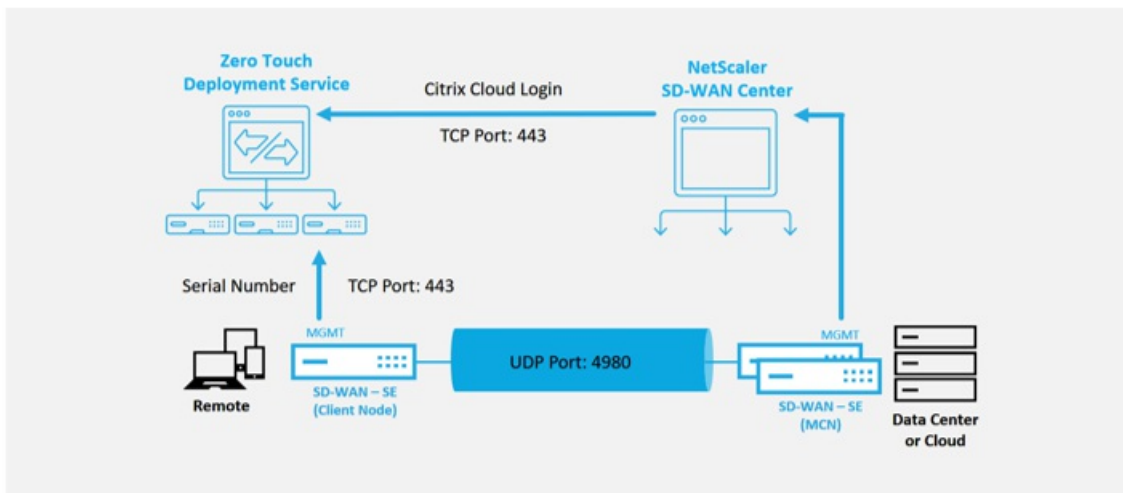
The following prerequisites are required before starting any Zero Touch Deployment service:

- Actively running NetScaler SD-WAN promoted to Master Control Node (MCN).
- Actively running NetScaler SD-WAN Center with connectivity to the MCN through Virtual Path.
- Citrix Cloud Login credentials created on <https://onboarding.cloud.com> (reference the instruction below on account

creation).

- Management network connectivity (SD-WAN Center and SD-WAN Appliance) to the Internet on port 443, either directly or through a proxy server.
- (optional) At least one actively running NetScaler SD-WAN appliance operating at a branch office in Client Mode with valid Virtual Path connectivity to MCN to help validate successful path establishment across the existing underlay network.

The last prerequisite is not a requirement, but allows the NetScaler SD-WAN Administrator to validate that the underlay network will successfully allow Virtual Paths to be successfully established as soon as the Zero Touch Deployment is complete with any newly added site. Primarily, this validates that the appropriate Firewall and Route policies are in place to either NAT traffic accordingly or confirm ability for UDP port 4980 can successfully penetrate the network to reach the MCN.



Zero Touch Deployment Service Overview

The Zero Touch Deployment Service works in tandem with the NetScaler SD-WAN Center to provide an easier deployment of branch office SD-WAN appliances. SD-WAN Center is configured and used as the central management tool for the SD-WAN Standard and Enterprise Edition appliances. To utilize the Zero Touch Deployment Service (or ZTD Cloud Service), an Administrator must begin by deploying the first NetScaler SD-WAN device in the environment, then configure and deploy the SD-WAN Center as the central point of management. When the SD-WAN Center, release 9.1 or later, is installed with connectivity to the public internet on port 443, SD-WAN Center will automatically call home to the Cloud Service and install necessary components to unlock the Zero Touch Deployment features and to make the Zero Touch Deployment option available in the GUI of SD-WAN Center. Zero Touch Deployment is not available by default in the SD-WAN Center software. This is purposely designed to make sure the proper preliminary components on the underlay network are present before allowing an Administrator to initiate any on-site activity involving Zero Touch Deployment.

After a working SD-WAN environment is up and running registration into the Zero Touch Deployment Service is accomplished through creating a Citrix Cloud account login. With SD-WAN Center able to communicate with the ZTD service, the GUI will expose the Zero Touch Deployment options under the Configuration tab. Logging into the Zero Touch Service authenticates the Customer ID associated with the particular NetScaler SD-WAN environment and registers the SD-WAN Center, in addition to unlocking the account for further authentication of ZTD appliance deployments.

Using the Network Configuration tool in NetScaler SD-WAN Center, the SD-WAN Administrator will then need to utilize the templates or clone site capability to build out the SD-WAN Configuration to add new sites. The new configuration will be used by the SD-WAN Center to initiate the deployment of ZTD for the newly added sites. When the SD-WAN Administrator initiates a site for deployment using the ZTD process, he or she will have the option to pre-authenticate the appliance to be used for ZTD by pre-populating the serial number, and initiating email communication to on-site installer to begin on-site activity.

The Onsite Installer will receive email communication that the site is ready for Zero Touch Deployment and can begin the installation procedure of powering on and cabling the appliance for DHCP IP address assignment and internet access on the MGMT port. Also, cabling in any LAN and WAN ports. Everything else will be automated by the ZTD Service and progress can be monitored by the utilizing the activation URL. In the event the remote node to be installed is a cloud instance, opening up the activation URL will begin the workflow to automatically install the instance in the designated cloud environment, no action is needed by a local installer.

The Zero Touch Deployment Cloud Service will automate the following actions:

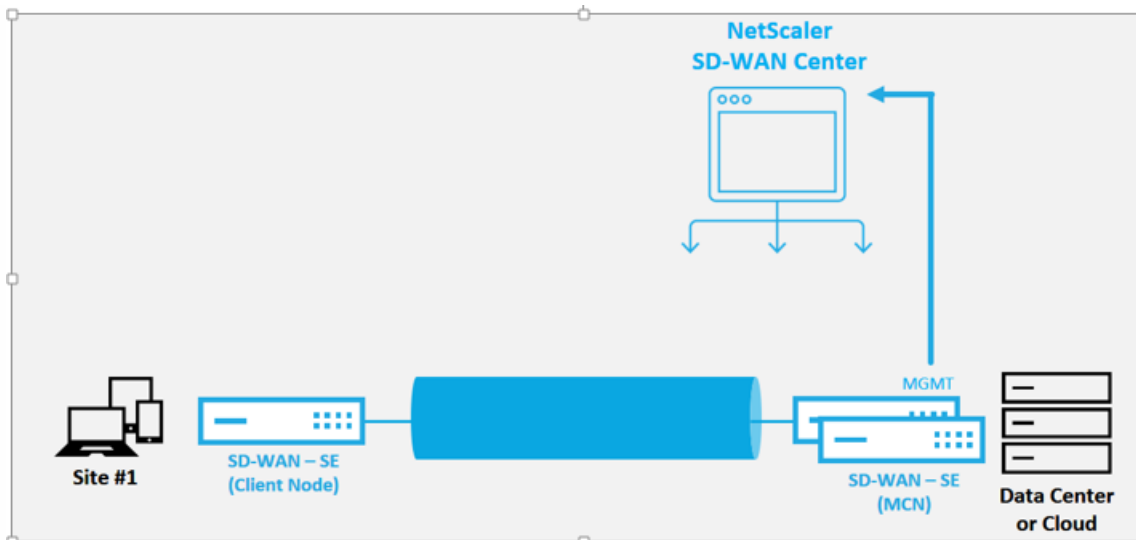
Download and Update the ZTD Agent if new features are available on the branch appliance.

- Authenticate the branch appliance by validating the serial number
- Authenticate that the SD-WAN Administrator accepted the site for ZTD using the SD-WAN Center
- Pull the configuration file specific for the targeted appliance from the SD-WAN Center
- Push the configuration file specific for the targeted appliance to the branch appliance
- Install the configuration file on the branch appliance
- Push any missing SD-WAN software components or required updates to the branch appliance
- Push a temporary 10Mbps license file for confirmation of Virtual Path establishment to the branch appliance
- Enable the SD-WAN Service on the branch appliance

Additional steps are required of the SD-WAN Administrator to install a permanent license file on the appliance.

The following procedure detail the steps required to successfully deploy a new site using the Zero Touch Deployment Service. It is recommended to have a running MCN and one client node already working with proper communication to NetScaler SD-WAN Center, as well as established Virtual Paths confirming connectivity across the underlay network.

The following steps are required of the SD-WAN Administrator to initiate the deployment of zero touch:



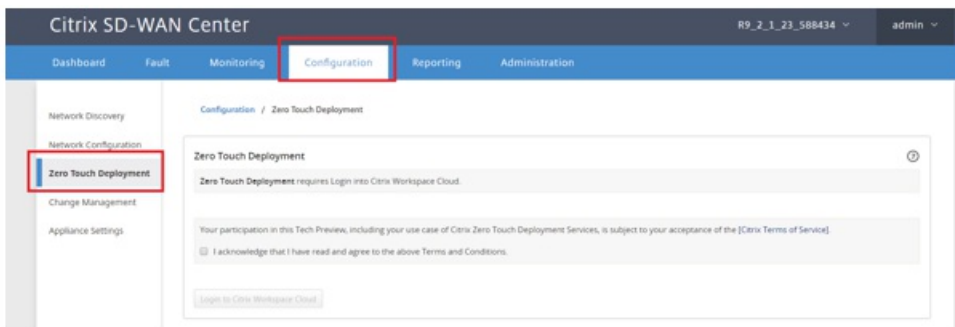
The SD-WAN Center has the functionality to accept requests from newly connected appliances to join the SD-WAN Enterprise network. The request is forwarded to the web interface through the zero touch deployment service. Once the appliance connects to the service, configuration and software upgrade packages are downloaded.

Configuration workflow:

- Access **SD-WAN Center** > **Create New site configuration** or Import existing configuration and save it.
- Login to Citrix Workspace Cloud to enable ZTD service. The Zero Touch Deployment menu option is now displayed in the SD-WAN center web management interface.
- In SD-WAN Center, navigate to **Configuration** > **Zero Touch Deployment** > **Deploy New Site**.
- Select an appliance, click **Enable** and click **Deploy**.
- Installer receives activation email > Enter the serial number > **Activate** > Appliance is deployed successfully.

To configure Zero Touch Deployment service:

1. Install SD-WAN Center with enabled Zero Touch Deployment capabilities:
 - a) Install NetScaler SD-WAN Center with DHCP assigned IP address.
 - b) Verify SD-WAN Center is assignment a proper management IP address and network DNS address with connectivity to the public internet across the management network.
 - c) Upgrade the NetScaler SD-WAN Center to the latest 9.2 firmware.
 - d) With proper internet connectivity, the SD-WAN Center will call home to the Zero Touch Deployment (ZTD) Cloud Service and automatically download and install any firmware updates specific to ZTD, if this call home procedure fails the following Zero Touch Deployment option will not be available in the GUI.



e) Read the Terms and Conditions, and then select “I acknowledge that I have read and agree to the above Terms and Conditions.”

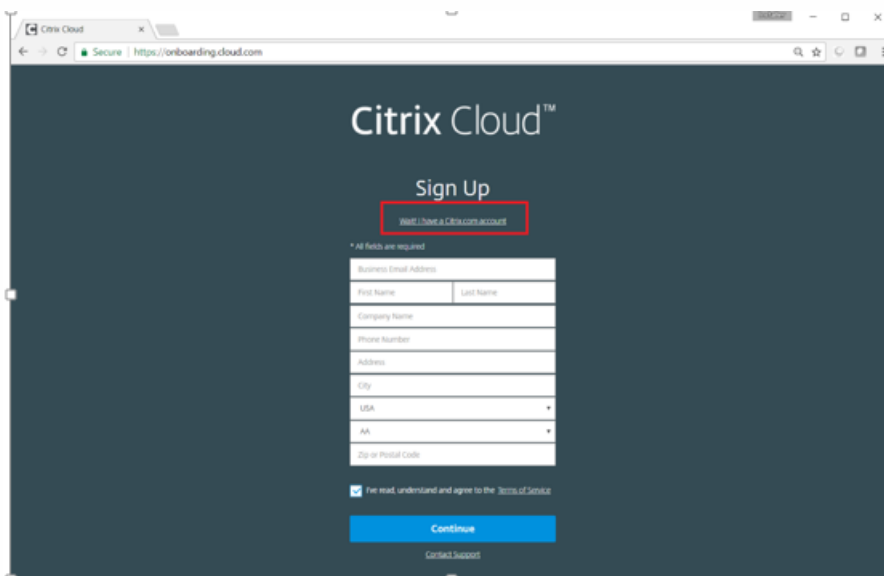
f) Click the “Login to Citrix Workspace Cloud” button if a Citrix Cloud account has leady been created.

g) Login into the Citrix Cloud account, and upon receiving the following message of successful login, **PLEASE DO NOT CLOSE THIS WINDOW UP, THE PROCESS REQUIRES ANOTHER ~20 SECONDS FOR THE SD-WAN CENTER GUI TO BE REFRESHED.** The window should close on its own when it is complete.

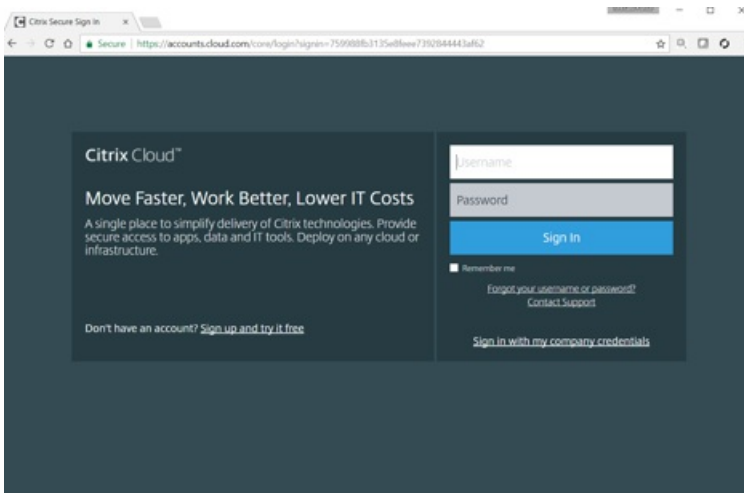


h) To create a Cloud Login account follow the below procedure:

- Open a web browser to <https://onboarding.cloud.com>
- Click on the link for “Wait, I have a Citrix.com account”.



i) Sign in with an existing Citrix account.



j) Once logged into SD-WAN Center Zero Touch Deployment page, you may notice no sites are available for ZTD deployment, this could be because of the following reasons:

- The active configuration has not been selected from the Configuration drop-down menu
- All the sites for the current active configuration have already been deployed
- The configuration was not built using the SD-WAN Center, but rather the Configuration Editor available on the MCN
- Sites were not built in the configuration referencing zero touch capable appliances (e.g. 410-SE, 2100-SE, Cloud VPX)

2. Update the configuration to add a **new remote** site with a **ZTD capable SD-WAN appliance** using SD-WAN Center Network Configuration.

If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure should be used to add a new site targeted for zero touch deployment.

a) Design the new site for SD-WAN appliance deployment by first outlining the details of the new site (i.e. Appliance Model, Interface Groups usage, Virtual IP Addresses, WAN Link(s) with bandwidth and their respective Gateways).

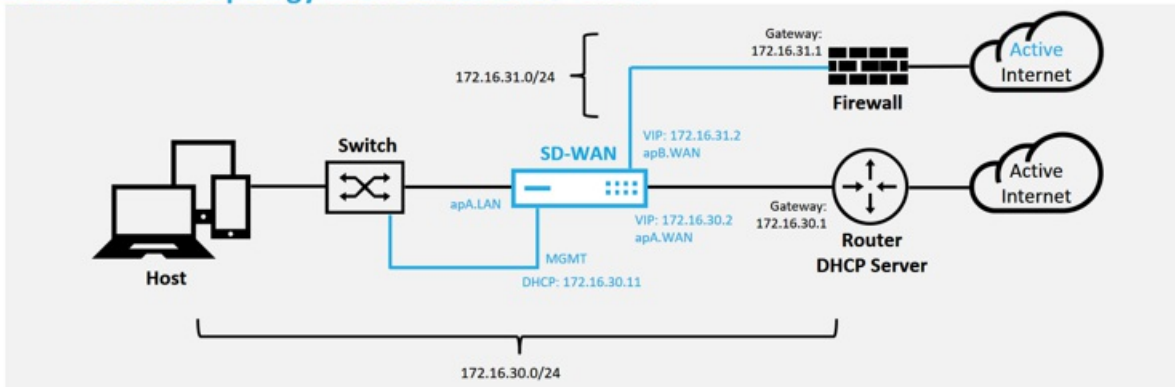
Important

You may notice any site node that has VPX selected as the model will also be listed, but currently ZTD support is only available for the AWS VPX instance.

Note

- Make sure that you are using a support web browser for Citrix SD-WAN Center
- Make sure the web browser is not blocking any pop-up windows during the Citrix Workspace Login

Branch Office Topology with NetScaler SD-WAN



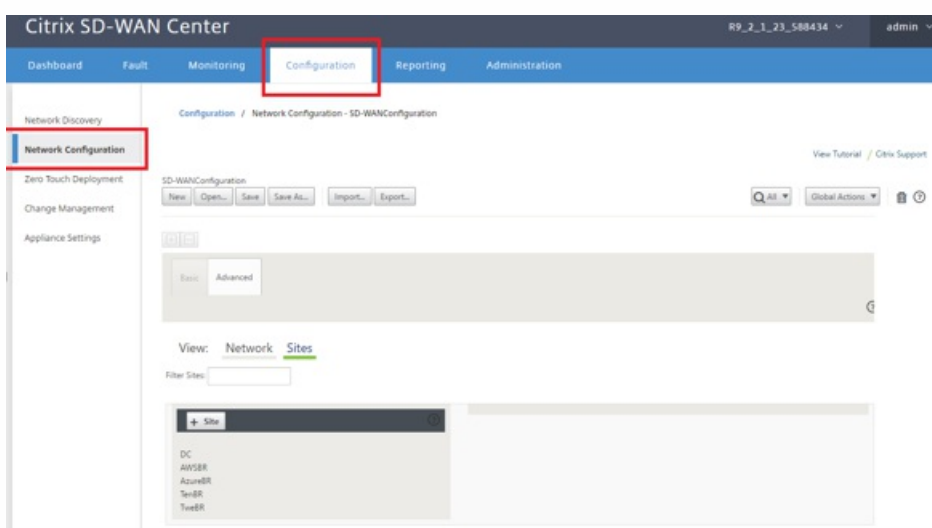
This is an example deployment of a branch office site, the NetScaler SD-WAN appliance is deployed physically in path of the existing MPLS WAN link across a 172.16.30.0/24 network, and leveraging an existing backup link by enabling it into an active state and terminating that second WAN link directly into the NetScaler SD-WAN appliance on a different subnet 172.16.31.0/24.

Note

The NetScaler SD-WAN appliances automatically assign a default IP address of 192.168.100.1/16. With DHCP enabled by default, the DHCP Server in the network may provide the appliance a second IP address in a subnet that overlaps the default. This can possibly result in a routing issue on the appliance where the appliance may fail to connect to the ZTD Cloud Service. It is recommended to configure the DHCP server to assign IP addresses outside of the range of 192.168.0.0/16.

There are various different deployment modes available for NetScaler SD-WAN product placement in a network. In the above example, SD-WAN is being deployed as an overlay on top of existing networking infrastructure. For new sites, SD-WAN Administrators may choose to deploy the NetScaler SD-WAN in Edge or Gateway Mode deployment, eliminating the need for a WAN edge router and firewall, and consolidating the network needs of edge routing and firewall onto the NetScaler SD-WAN solution.

a) Open the SD-WAN Center web management interface and navigate to the **Configuration > Network Configuration** page.

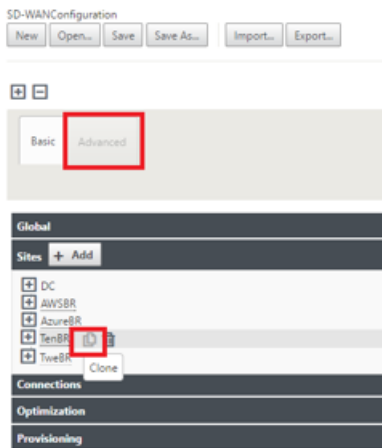


b) Make sure a working configuration is already in place, or import the configuration from the MCN.

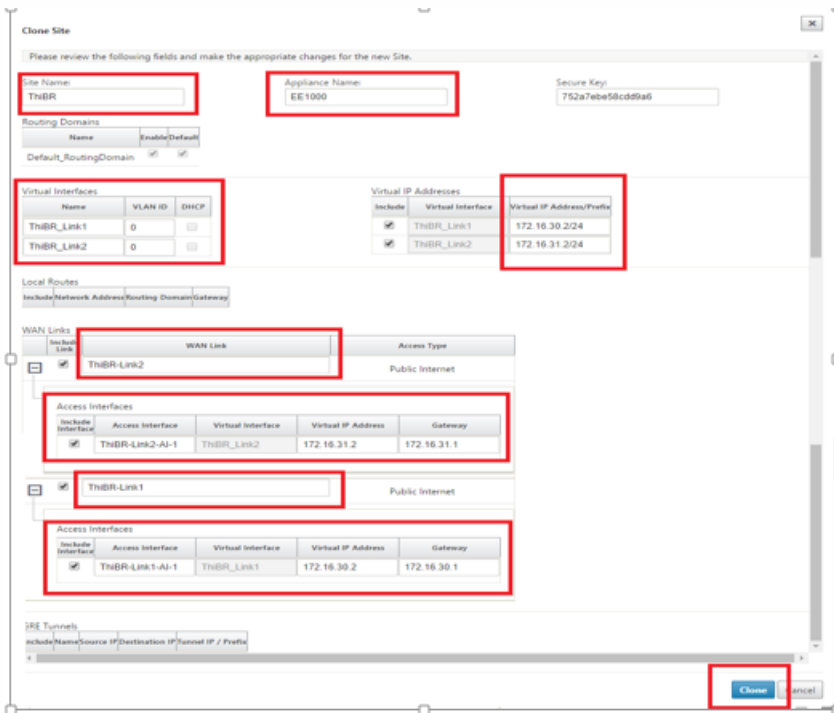
c) Navigate to the Advanced tab to create a new site.

d) Open the Sites tile to display the currently configured sites.

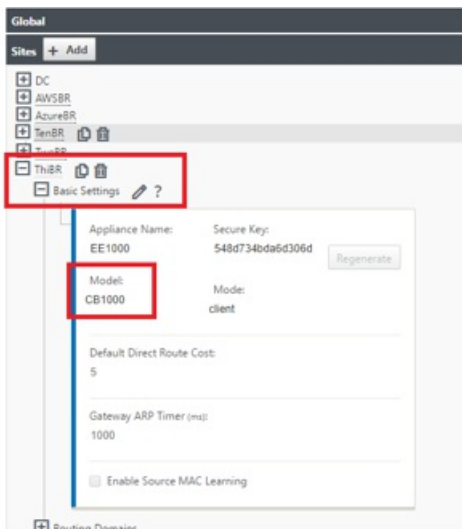
e) Quickly built the configuration for the new site by utilizing the clone feature of any existing site.



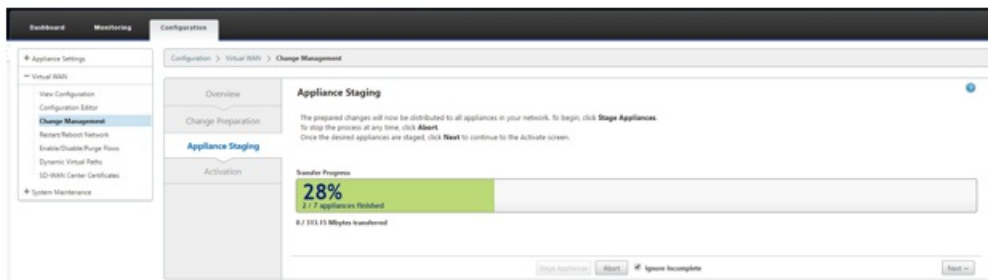
f) Populate all the required fields from the topology designed for this new branch site



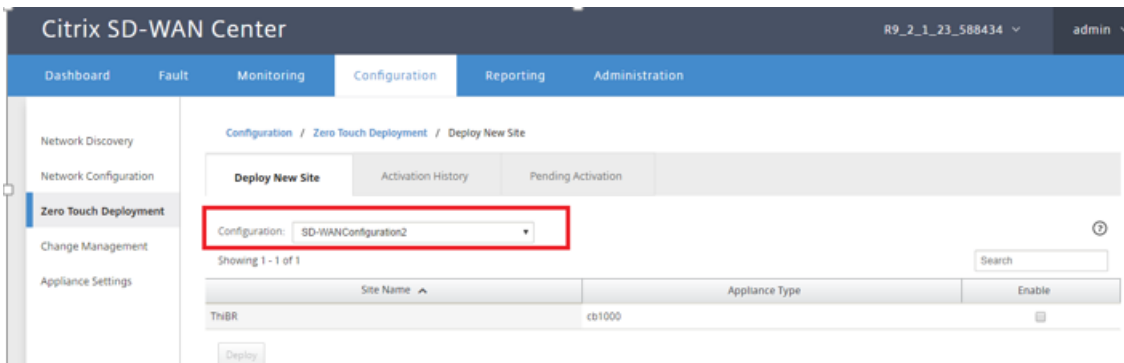
g) After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.



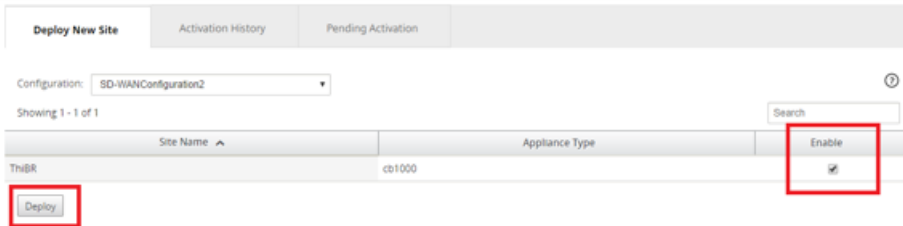
- h) The SD-WAN model for the site can be updated, but do be aware that the Interface Groups may have to be redefined since the updated appliance may have a new interface layout then what was used to clone.
- i) Save the new configuration on SD-WAN Center, and use the export to the “Change Management inbox” option to push the configuration using Change Management.
- j) Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you will need to utilize the “Ignore Incomplete” option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.



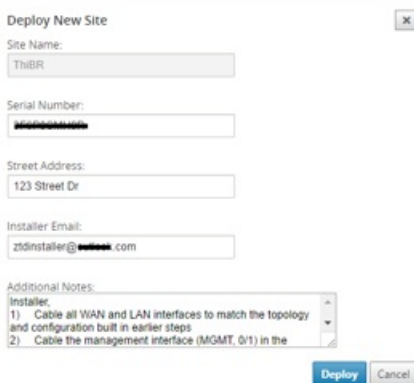
3. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site will be available for deployment.
 - a) In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file
 - b) After the running configuration file is selected, the list of all the branch sites with undeployed NetScaler SD-WAN devices that are supported for zero touch will be displayed



c). Select the branch sites you want to configure for Zero Touch service, click **Enable**, and then **Deploy**.



d) A Deploy New Site pop-up window will appear, where the Admin can provide the Serial Number, branch site Street Address, Installer Email address, and Additional Notes, if required.



Note

The Serial Number entry field is optional and depending if it is populated or not, will result in a change in on-site activity the Installer is responsible for.

- If Serial Number field is populated – The installer is not required to enter serial number into the activation URL generated with the deploy site command
- If Serial Number field is left blank – The installer will be responsible for entering in the correct serial number of the appliance into the activation URL generated with the deploy site command

e) After clicking the **Deploy** button, a message will appear indicating that “The Site configuration has been deployed”.

f) This action triggers the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this particular site to be temporarily stored in the ZTD Cloud Service.

g) Navigate to the Pending Activation tab to confirm that the branch site information populated successfully and was put into a pending installer activity status.

Site Name	Serial No	Installer Email	Address	Status	Action
ThiBR		ztainstaller@...com	123 Street Dr	Connecting	

Note

A zero touch deployment in the Pending Activation state can optionally be chosen to Delete or Modify if information is seen to be incorrect. If a Site is deleted from the pending activation page, it will become available to be deployed in the Deploy New Site tab page. Once you choose to delete the branch site from Pending activation, the activation link send to the installer will become invalid.

If the Serial Number field was not populated by the SD-WAN Administrator, the Status Field will indicate “Waiting for Installer” instead of “Connecting”.

4. The next series of activities will be conducted by the On-site Installer.

a) The Installer will need to check the mailbox of the email address the SD-WAN Administrator used when deploying the site.

NetScaler SD-WAN Cloud Service Activation Link @ThiBR

 Citrix Zero Touch Service <sdwanservice@citrix.com>
Thu, 5/10/2017 1:47 PM
To: ThiBR (ztainstaller@outlook.com); A



Your NetScaler SD-WAN Appliance Activation Information for: ThiBR

Hello,

To activate your appliance please use the following URL:
<https://sdwanzt.citrixnetworkapi.netroot/sdwanztv1/appliance/activate?activationcode=3720fe45-fa1b-4662-bab1-ff3bbd40d357>

Installer Notes from the Admin:
Installer, Please power and cable the appliance for internet.

Site Name:
ThiBR

Address:
123 Street Dr

Cheers,

The team at Citrix Cloud Services

b) Open the zero touch deployment Activation URL in an internet browser window (e.g. <https://sdwanzt.citrixnetworkapi.net>).

c) If the SD-WAN Administrator did not pre-populate the serial number in the deploy site step, then the Installer would be responsible for locating the serial number on the physical appliance and entering the serial number manually into the activation URL, then click the **Activate** button.



d) If the Admin pre-populating the Serial Number information, the Activation URL will have already progressed to the next step.



e) The installer must physically be on-site to perform the following actions:

- Cable all WAN and LAN interfaces to match the topology and configuration built in earlier steps.
- Cable the management interface (MGMT, 0/1) in the segment of the network that will provide DHCP IP address and connectivity to the Internet with DNS and FQDN to IP address resolution.
- Power cable the SD-WAN appliance.
- Turn on the power switch of the appliance.

Note

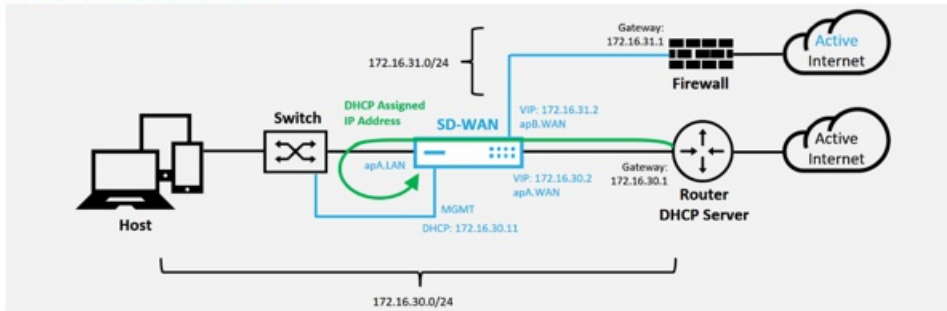
Most appliances will automatically power on as soon as the power cable is attached. Some appliance may have to be powered on using the power switch on the front of the appliance, others may have the power switch on the rear of the appliance. Some power switches require holding the power button until the unit powers up.

5. The next series of steps are automated with the help of the Zero Touch Deployment service, but requires that the following pre-requisites are available.

- The branch appliance should be powered up
- DHCP must be available in the existing network to assign management and DNS IP address
- Any DHCP assigned IP address will require connectivity to the internet with ability to resolve FQDNs
- IP assignment can be configured manually, as long as the other pre-requisites are meet

a) The appliance obtains an IP address from the networks DHCP Server, in this example topology this is achieved through the bypassed data interfaces of a factory default state appliance.

Power on NetScaler SD-WAN



- b) As the appliance obtains the web management and DNS IP addresses from the underlay network DHCP Server, the appliance will call home to the Zero Touch Deployment Service and download any ZTD related software updates.
- c) With successful connectivity to the ZTD Cloud Service, the deployment process will automatically perform the following:
- Download the Configuration File that was stored earlier by the SD-WAN Center
 - Applying the Configuration to the local appliance
 - Download and Install a temporary 10 MB license file
 - Download and Install any software updates if needed
 - Activate the SD-WAN Service



- d) Further confirmation can be done in the SD-WAN Center web management interface, the Zero Touch Deployment menu will display successfully activated appliances in the **Activation History** tab.

Site Name	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
TheBR	3F6P82307	ztdinstaller@outlook.com	123 Street Dr	Appliance Activated	May 11 22:18:03 2017 UTC	Activated	

- e) The Virtual Paths may not immediately show in a connected state, this is because the MCN may not trust the configuration handed down from the ZTD Cloud Service, and will report "Configuration version mismatch" in the MCN Dashboard.

Dashboard Monitoring Configuration

System Status

Name: DC
 Model: VPX
 Appliance Mode: MCN
 Serial Number: 1079975b-b067-ae77-1718-d7bd0375a2b
 Management IP Address: 172.16.10.51
 Appliance Uptime: 3 weeks, 5 days, 22 hours, 45 minutes, 35.2 seconds
 Service Uptime: 1 weeks, 2 days, 20 hours, 58 minutes, 57.0 seconds
 Routing Domain Enabled: Default_RoutingDomain

Local Versions

Software Version: 9.2.1.23.588434
 Built On: Apr 21 2017 at 05:23:29
 Hardware Version: VPX
 OS Partition Version: 4.6

Virtual Path Service Status

Virtual Path DC-AWSBR: Uptime: 1 hours, 12 minutes, 48.0 seconds.
 Virtual Path 'DC-AzureBR' is currently dead.
 Virtual Path 'DC-THBR' is currently dead (Configuration version mismatch)
 Virtual Path 'DC-IRCON' is currently dead.
 Virtual Path 'DC-FouBR' is currently dead.

f) The configuration will automatically be redelivered to the newly installed branch office appliance, the status of this can be monitoring on the MCN > Configuration > Virtual WAN > Change Management page (this process can take several minutes to complete).

Dashboard Monitoring Configuration

Configuration > Virtual WAN > Change Management

Change Process Overview

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

Step 1: Change Preparation (Upload File to MCN) — MCN — MCN — Clients — MCN — Clients

Step 2: Appliance Staging (Transfer File to Clients) — Clients — MCN — Clients

Step 3: Activation (Activate Change) — Clients

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

Configuration Filenames: Active - %2-2TD-fenTuaThuWSAque-DO-NOT-4ZTER.ftg Staged - SD-WANConfiguration.zip

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
DC-494	CB494	Active	9.2.1.23.588434	2019-05-31 11:17	9.2.1.23.588434	1641 on 5/11/17	<1 min	108 min	active / staged
AzureBR-485-648	CB485	Not Connected	9.2.1.23.588434	2019-05-31 11:17	9.2.1.23.588434	1641 on 5/11/17	<3 min	82 s	active / staged
AzureBR-486-654	CB486	Not Connected					Loc Chg Mgt		active / staged
FouBR-02410	CB410	Not Connected					Loc Chg Mgt		active / none
IRCON-421000	CB1000	Not Connected					Loc Chg Mgt		active / staged
THBR-421000	CB1000	40%	9.2.1.23.588434	2148 on 5/11/17			Loc Chg Mgt		active / staged
THBR-02410	CB410	Not Connected					Loc Chg Mgt		active / staged

g) The SD-WAN Administrator can monitor the head-end MCN web management page for the established Virtual Paths of the remote site.

Dashboard Monitoring Configuration

Monitoring > Statistics

Statistics

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

Path Statistics Summary

Filter: in Any column Apply

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path
13	DC-A5	ThiBR-Wifi	GOOD	GOOD	Static
14	DC-B4	ThiBR-4G	GOOD	GOOD	Static
15	ThiBR-4G	DC-B4	GOOD	GOOD	Static
16	ThiBR-Wifi	DC-A5	GOOD	GOOD	Static

Showing 1 to 4 of 4 entries (filtered from 24 total entries)
Bandwidth calculated over the last 4.762 seconds

h) SD-WAN Center can also be utilized to identify the DHCP assigned IP address of the on-site appliance from the Configuration > Network Discovery > Inventory and Status page.

Dashboard Fault Monitoring Configuration Reporting Administration

Configuration / Network Discovery / Inventory And Status

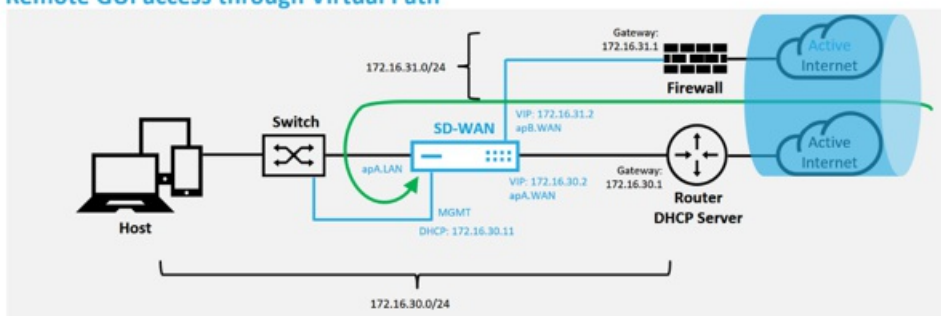
SSL Certificate Discovery Settings Inventory And Status

Showing 1 - 7 of 7

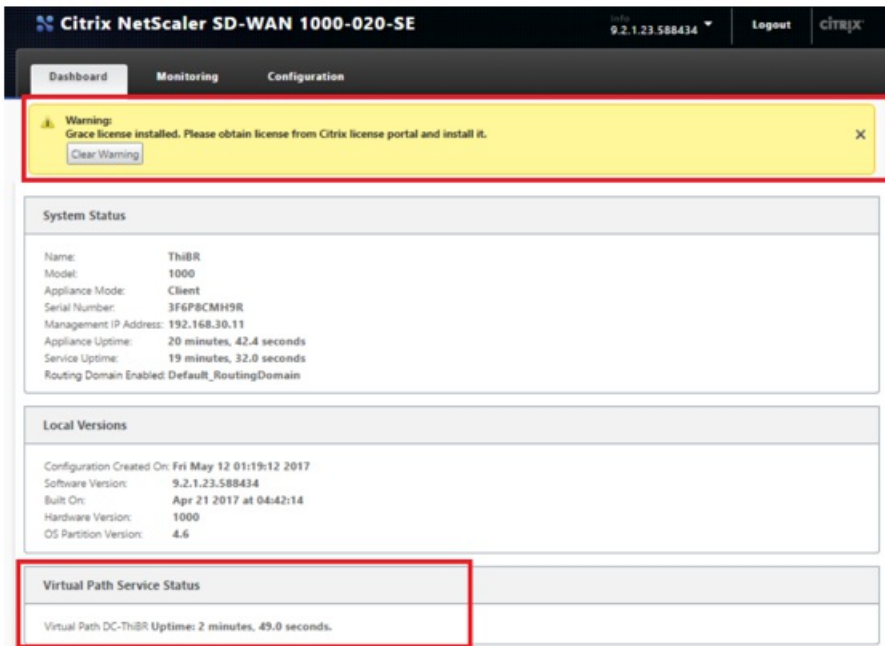
Pool	State	Name	MGT IP Address	Model	Serial Number	Software	Registry Timestamp	Last Successful Poll	Latest Record	Download
✓	Stats in Sync	DC	172.16.10.51	ctbrpx	1079975b-5067-ae77-1718-d7be0f0375a2b	R9_2_1_33_588434	1494551952	05/11/17 19:02	05/11/17 19:01	Download
✓	Unknown	AW5BR								Download
✓	Not Reachable	AzureBR	192.168.202.4							Download
✓	Unknown	Fou5BR								Download
✓	Not Reachable	Ter5BR	192.168.10.11							Download
✓	Not Reachable	Th5BR	192.168.30.11							Download
✓	Unknown	Twe5BR								Download

i) At this point the SD-WAN Network Administrator can gain web management access to on-site appliance utilizing the SD-WAN overlay network.

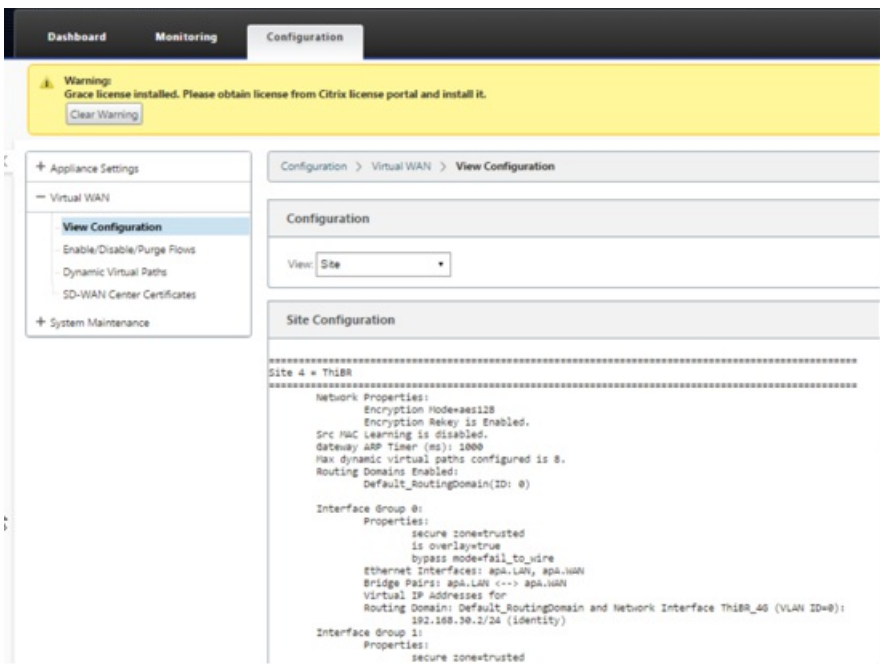
Remote GUI access through Virtual Path



j) Web management access to the remote site appliance will indicate that the appliance has been installed with a temporary Grace License at 10Mbps, which enables the ability for the Virtual Path Service Status to report as active.



k) The appliance configuration can be validated using the **Configuration > Virtual WAN > View Configuration** page.



l) The appliance license file can be updated to a permanent license using the **Configuration > Appliance Settings > Licensing** page.

The screenshot shows the Citrix NetScaler Configuration page. At the top, there are tabs for Dashboard, Monitoring, and Configuration. A yellow warning banner at the top left states: "Warning: Grace license installed. Please obtain license from Citrix license portal and install it." with a "Clear Warning" button. The left sidebar shows the "Appliance Settings" menu with "Licensing" selected. The main content area is titled "Configuration > Appliance Settings > Licensing".

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

m) After uploading and installing the permanent license file, the Grace License warning banner is will disappear, and during the license install process no loss in connectivity to the remote site will occur (zero pings are dropped).

On-Prem Zero Touch

Mar 01, 2018

For instructions about how to deploy an SD-WAN appliance with Zero Touch Service, see the topic; [How to Configure Zero Touch Deployment Service](#).

AWS

Mar 01, 2018

Deploying in AWS

With NetScaler SD-WAN release 9.3, zero touch deployment capabilities have extended to Cloud instances. The procedure to deploy zero touch deployment process four cloud instances is slightly different from appliance deployment for zero touch service.

1. Update the configuration to add a new remote site with a ZTD capable SD-WAN cloud device using SD-WAN Center Network Configuration.

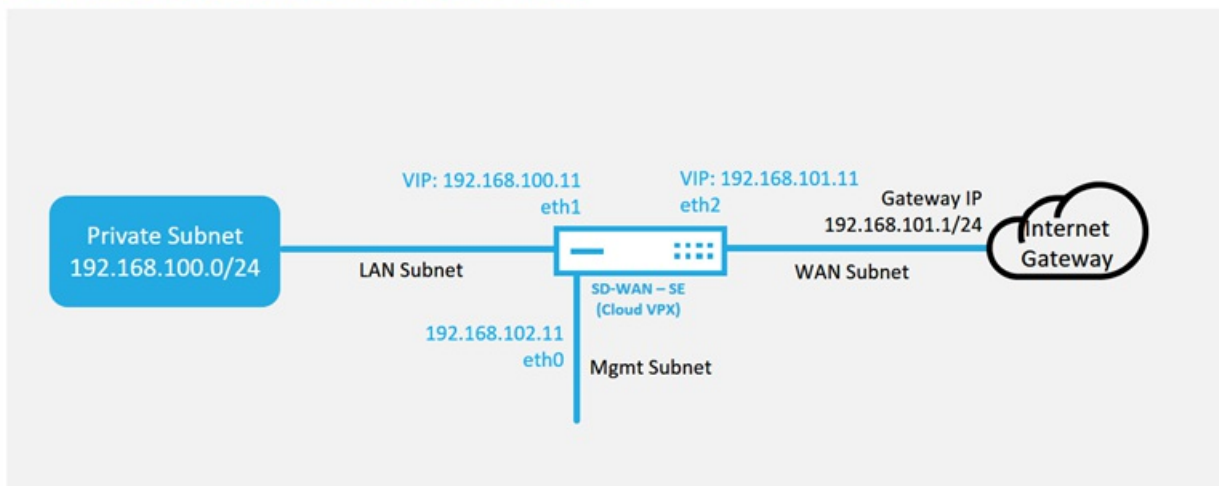
If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure should be used to add a new cloud node targeted for zero touch deployment.

a) Design the new site for SD-WAN cloud deployment by first outlining the details of the new site (i.e. VPX size, Interface Groups usage, Virtual IP Addresses, WAN Link(s) with bandwidth and their respective Gateways).

Note

- Cloud deployed SD-WAN instances must be deployed in Edge/Gateway mode.
- The template for the cloud instance is limited to three interfaces; Management, LAN, and WAN (in that order).
- The available cloud templates for SD-WAN VPX are currently hard-set to obtain the #.#.#.#.11 IP address of the available subnets in the VPC .

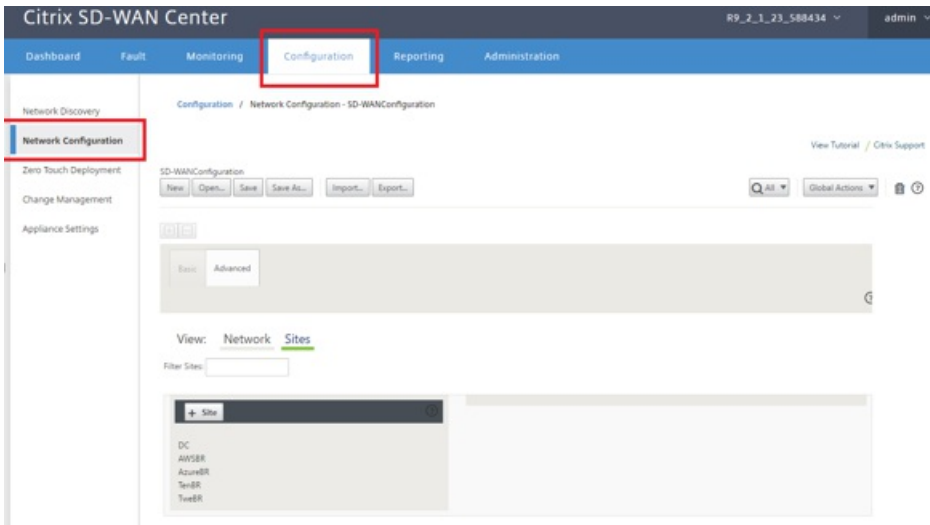
Cloud Topology with NetScaler SD-WAN



This is an example deployment of a SD-WAN cloud deployed site, the NetScaler SD-WAN device is deployed as the edge device servicing a single Internet WAN link in this cloud network. Remote sites will be able to leverage multiple distinct Internet WAN links connecting into this same Internet Gateway for the cloud, providing resiliency and aggregated bandwidth connectivity from any SD-WAN deploy site to the cloud infrastructure. This provides cost effective and highly

reliable connectivity to the cloud.

b) Open the SD-WAN Center web management interface and navigate to the **Configuration > Network Configuration** page.

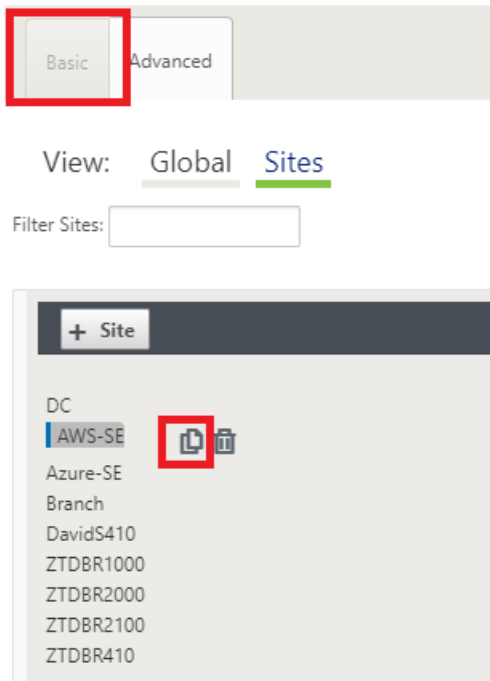


c) Make sure a working configuration is already in place, or import the configuration from the MCN.

d) Navigate to the Basic tab to create a new site.

e) Open the Sites tile to display the currently configured sites.

f) Quickly built the configuration for the new cloud site by utilizing the clone feature of any existing site, or manually build a new site.



g) Populate all the required fields from the topology designed earlier for this new cloud site

Keep in mind that the template available for cloud ZTD deployments are hard-set to utilize the `###.11` IP address for the Mgmt, LAN, and WAN subnets. If the configuration is not set to match the expected `.11` IP host address for each

interface, then the device will not be able to properly establish ARP to the cloud environment gateways and IP connectivity to the Virtual Path of the MCN.

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name:

AWS-SE 

Appliance Name:

AWS-SE-CBVPX

Secure Key:

4a460b14f0228091



Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
E1Vlan0	0	<input type="checkbox"/>
E2Vlan0	0	<input type="checkbox"/>



Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	E1Vlan0	192.168.100.11/2 
<input checked="" type="checkbox"/>	E2Vlan0	192.168.101.11/2 



Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

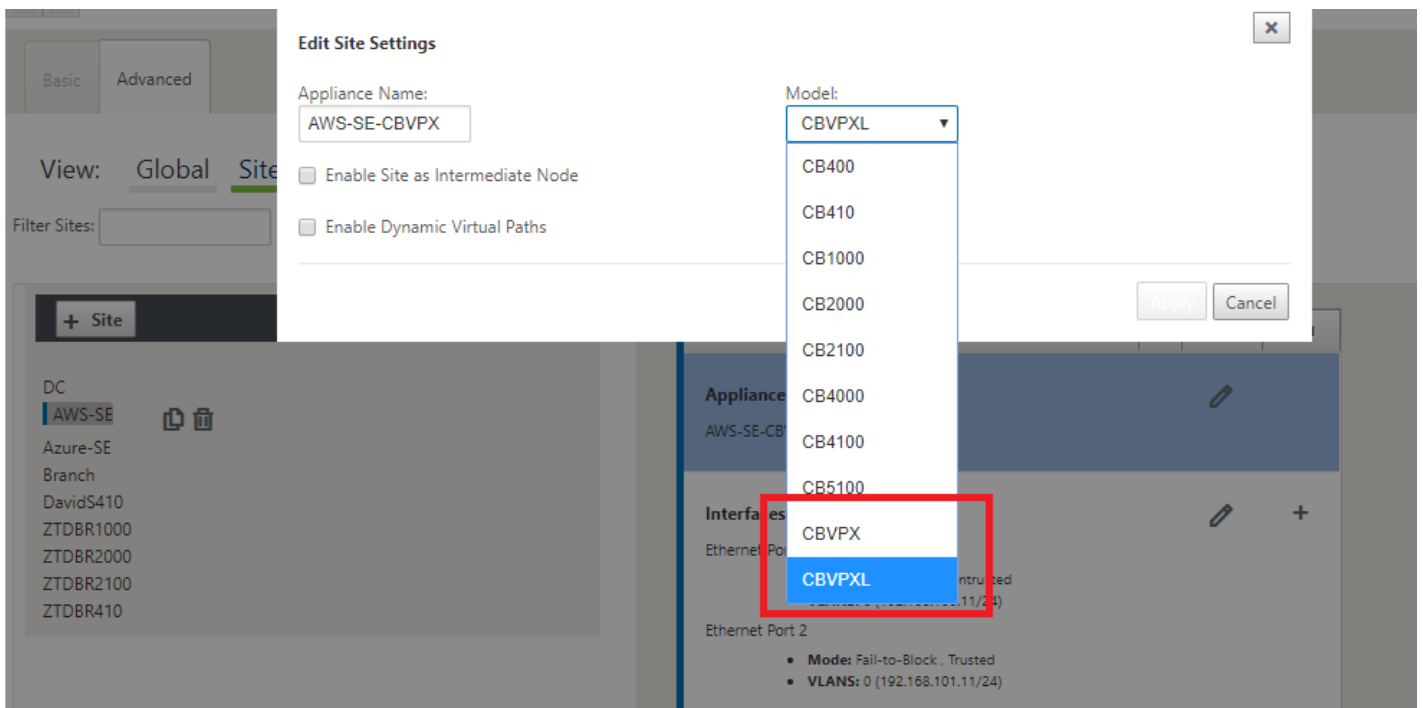
WAN Links

	Include Link	WAN Link	Access Type
	<input checked="" type="checkbox"/>	AWS-INET 	Public Internet

Access Interfaces

Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	AWS-INET-AI-1	E2Vlan0	192.168.101.11 	192.168.101.1 

h) After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.



i) Save the new configuration on SD-WAN Center, and use the export to the “Change Management inbox” option to push the configuration using Change Management.

j) Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you will need to utilize the “*Ignore Incomplete*” option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.



3. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site will be available for deployment.

- a) In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file.
- b) After the running configuration file is selected, the list of all the branch sites with undeployed NetScaler SD-WAN devices that are supported for zero touch will be displayed.

Citrix SD-WAN Center R9_3_0_161_612290

Dashboard | Fault | Monitoring | **Configuration** | Reporting | Administration

Configuration / Zero Touch Deployment / Prepare New Site

Prepare New Site | Activation History | Pending Activation

Configuration: OnPremAppliance-ZTDv5

Showing 1 - 7 of 7

Site Name ^	Appliance Type	Enable
Azure-SE	cbvpxl	<input type="checkbox"/>
Branch	cbvpx	<input type="checkbox"/>
DavidS410	cb410	<input type="checkbox"/>
ZTDBR1000	cb1000	<input type="checkbox"/>
ZTDBR2000	cb2000	<input type="checkbox"/>
ZTDBR2100	cb2100	<input type="checkbox"/>
ZTDBR410	cb410	<input type="checkbox"/>

c). Select the target cloud site you want to deploy using the Zero Touch service, click **Enable**, and then **Provision and Deploy**.

Site Name ^	Appliance Type	Enable
AWS-SE	cbvpxl	<input checked="" type="checkbox"/>
Azure-SE	cbvpxl	<input type="checkbox"/>
Branch	cbvpx	<input type="checkbox"/>
DavidS410	cb410	<input type="checkbox"/>
ZTDBR1000	cb1000	<input type="checkbox"/>
ZTDBR2000	cb2000	<input type="checkbox"/>
ZTDBR2100	cb2100	<input type="checkbox"/>
ZTDBR410	cb410	<input type="checkbox"/>

Deploy Provision and Deploy

d) A pop-up window will appear, where the NetScaler SD-WAN Admin can initiate the deployment for Zero Touch. Populate an email address where the activation URL can be delivered, and select the **Provision Type** for the desired Cloud.

Provision and Deploy ✕

Site Name:

Installer Email:

Provision Type:

Next

e) After clicking **Next**, Select the appropriate Region, Instance size, populate the SSH Key name and Role ARN fields appropriately.

Provision and Deploy AWS ✕

AWS Region

AWS Instance Size

SSH Key Name:
 ?

Role ARN:
 ?

Note

Make use of the help links for guidance on how to setup the SSH Key and Role ARN on the Cloud account. Also make sure the select region matches what is available on the account and that the selected Instance Size matches VPX or VPXL as the selected model in the SD-WAN configuration.

f) Click **Deploy**, triggering the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this site to be temporarily stored in the ZTD Cloud Service.

g) Navigate to the **Pending Activation** tab to confirm that the site information populated successfully and was put into a provisioning status.

Configuration / Zero Touch Deployment / Pending Activation

Prepare New Site Activation History **Pending Activation**

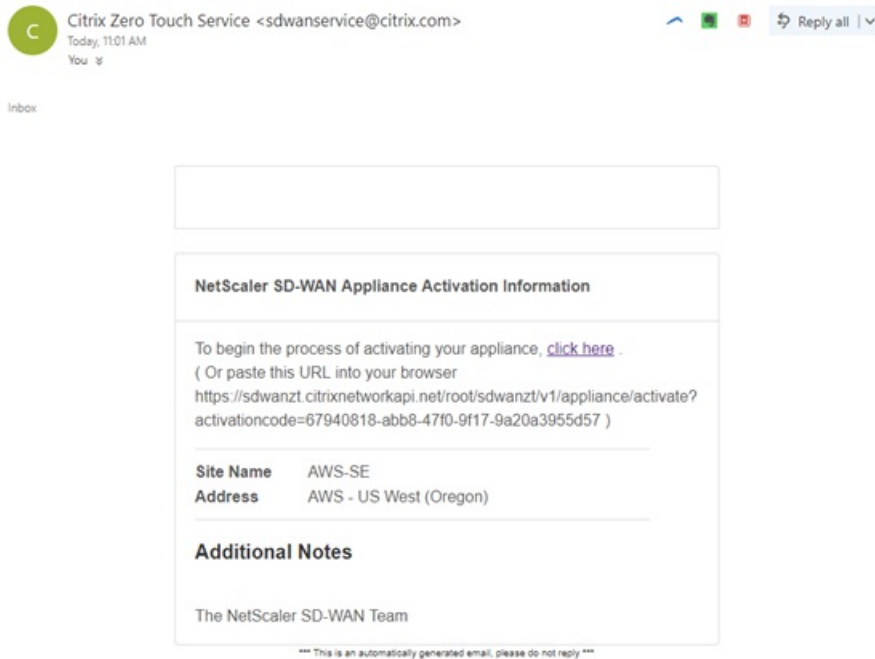
Showing 1 - 1 of 1 Search

Site Name ^	Serial No	Installer Email	Address	Status	Action
AWS-SE	2E20EFCF-1A26-42DC-86D0-5624FD27C37F	ztdinstaller@outlook.com	AWS - US West (Oregon)	Provisioning	

4. Initiate the Zero Touch Deployment process as the Cloud Admin.

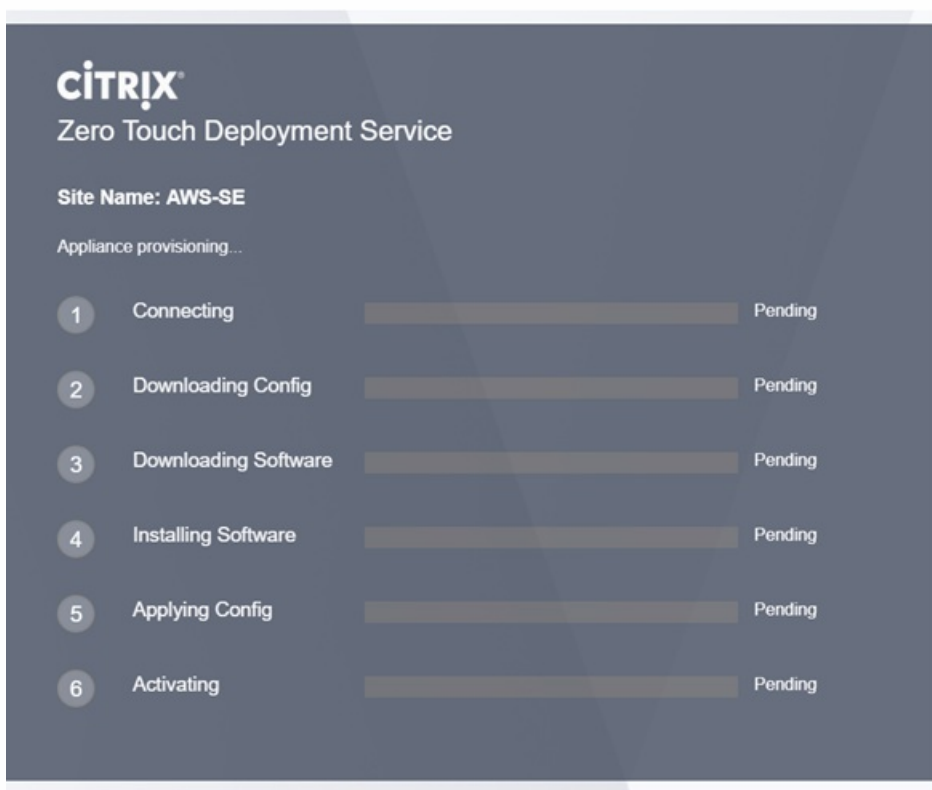
a) The Installer will need to check the mailbox of the email address the SD-WAN Administrator used when deploying the site.

NetScaler SD-WAN Cloud Service Activation Link @AWS-SE

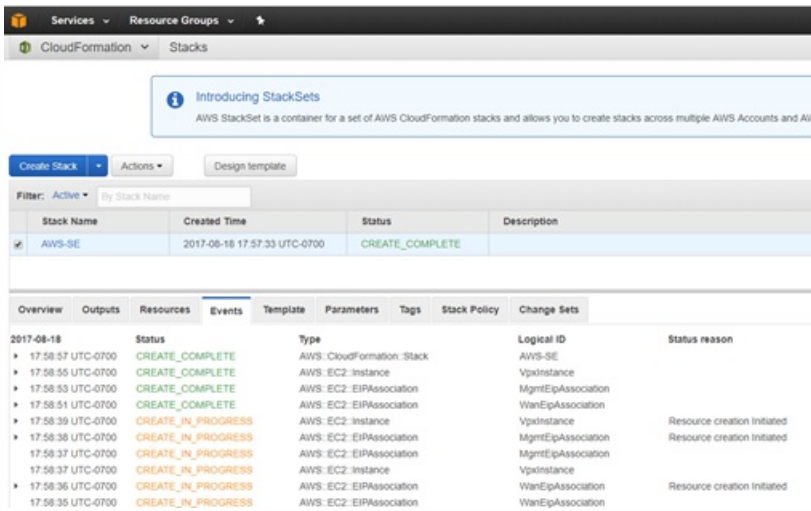


b) Open the activation URL found in the email in an internet browser window (example; <https://sdwanzt.citrixnetworkapi.net>).

c) If the SSH Key and Role ARN are properly inputted, the Zero Touch Deployment Service will immediately start provisioning the SD-WAN instance, otherwise connections errors will immediately be displayed.



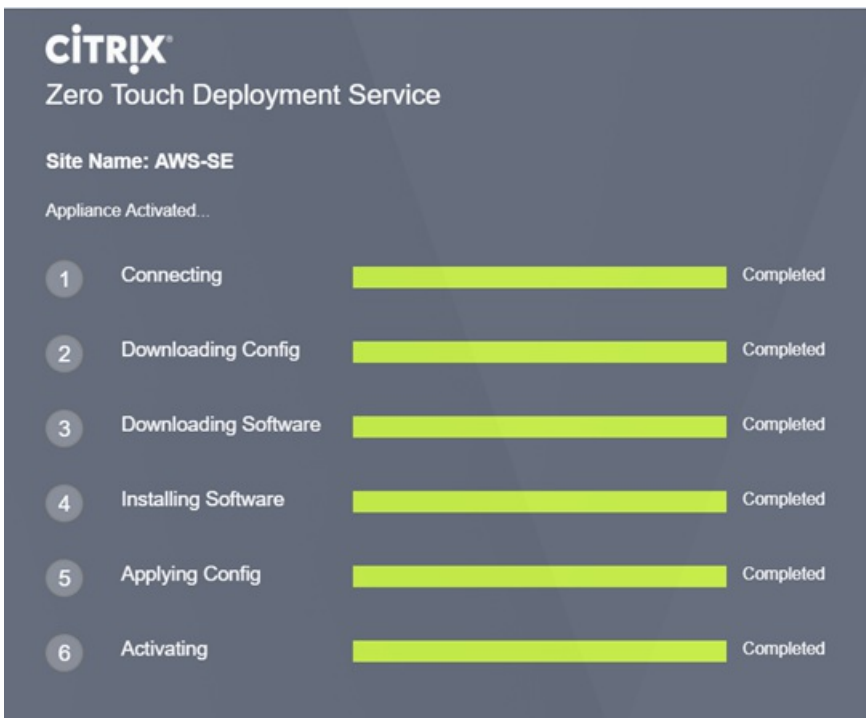
d) For additional troubleshooting on the AWS console, the Cloud Formation service can be utilized to catch any events that occur during the provisioning process.



e) Allow the provisioning process ~8-10 minutes and activation another ~3-5 minutes to fully complete.

f) With successful connectivity of the SD-WAN cloud instance to the ZTD Cloud Service, the service will automatically perform the following:

- Download the site-specific Configuration File that was stored earlier by the SD-WAN Center
- Applying the Configuration to the local instance
- Download and Install a temporary 10 MB license file
- Download and Install any software updates if needed
- Activate the SD-WAN Service



g) Further confirmation can be done in the SD-WAN Center web management interface; the Zero Touch Deployment menu will display successfully activated appliances in the **Activation History** tab.

Citrix SD-WAN Center R9_3_0_161_612290 admin

Dashboard Fault Monitoring **Configuration** Reporting Administration

Configuration / Zero Touch Deployment / Activation History

Prepare New Site **Activation History** Pending Activation

Showing 1 - 1 of 1

Site Name	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
AWS-SE	2E20EFCF-1A26-42DC-86D0-5624FD27C37F	ztdinstaller@outlook.com	AWS - US West (Oregon)	Appliance Activated	Aug 19 01:16:55 2017 UTC	Activated	

h) The Virtual Paths may not immediately show in a connected state, this is because the MCN may not trust the configuration handed down from the ZTD Cloud Service, and will report "*Configuration version mismatch*" in the MCN Dashboard.

Dashboard **Monitoring** Configuration

System Status

Name: **DC**
 Model: **VPX**
 Appliance Mode: **MCN**
 Serial Number: **b536a38c-5f48-b720-4f8d-b3f50b23f69f**
 Management IP Address: **172.16.10.30**
 Appliance Uptime: **1 weeks, 2 days, 3 hours, 50 minutes, 18.3 seconds**
 Service Uptime: **1 weeks, 2 days, 3 hours, 42 minutes, 19.0 seconds**
 Routing Domain Enabled: **Default_RoutingDomain**

Local Versions

Software Version: **9.3.0.161.612290**
 Built On: **Aug 8 2017 at 14:45:01**
 Hardware Version: **VPX**
 OS Partition Version: **4.6**

Virtual Path Service Status

Virtual Path DC-Branch: **Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.**
 Virtual Path 'DC-DavidS410' is currently dead.
 Virtual Path DC-ZTDBR1000: **Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.**
 Virtual Path 'DC-ZTDBR2000' is currently dead.
 Virtual Path 'DC-ZTDBR2100' is currently dead.
 Virtual Path 'DC-ZTDBR410' is currently dead.
Virtual Path 'DC-AWS-SE' is currently dead (Configuration version mismatch)
 Virtual Path 'DC-Azure-SE' is currently dead.

i) The configuration will automatically be redelivered to the newly installed branch office appliance, the status of this can be monitoring on the **MCN > Configuration > Virtual WAN > Change Management** page (depending on the connectivity, this process can take several minutes to complete).

Configuration > Virtual WAN > Change Management

Overview

- Change Preparation
- Appliance Staging
- Activation

Change Process Overview

The Change Management process allows a user to upload changes to the network, whether it processes that ensure that configuration changes and software updates are applied in a reliable manner.

Step 1: Change Preparation
Upload Files to MCN

Step 2: Appliance Staging
Transfer Files

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a previously staged configuration.

Configuration Filenames: Active - OnPremAppliance-ZTDv5.zip Staged

Site-Appliance	Model	State	Currently Active		Current
			Software	Config	Software
DC-DC_SDWAN	CBVPX		9.3.0.161.612290	10:55 on 8/18/17	9.3.0.161.612290
AWS-SE-AWS-SE-CBVPX	CBVPXL	6%	9.3.0.161.612290		
Azure-SE-Azure-SE-CBVPX	CBVPXL	Not Connected			
Branch-Branch_SDWAN	CBVPX		9.3.0.161.612290	10:55 on 8/18/17	9.3.0.161.612290

j) The SD-WAN Administrator can monitor the head-end MCN web management page for the established Virtual Paths of the newly added cloud site.

Monitoring > Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Start Show latest data.

Path Statistics Summary

Filter: AWS in Any column Apply Show 100 entries

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
27	DC-INET	AWS-INET	GOOD	GOOD	Static	26	2	0.00	16.20	NO
28	AWS-INET	DC-INET	GOOD	GOOD	Static	26	2	0.00	15.13	NO

Showing 1 to 2 of 2 entries (filtered from 30 total entries)
Bandwidth calculated over the last 0.956 seconds

k) If troubleshooting is required, open the SD-WAN instances user interface using the public IP assigned by the cloud environment during provisioning, and utilize the ARP table in the **Monitoring > Statistics** page to identify any issues

connecting to the expected gateways, or utilize the trace route and packet capture options in diagnostics.

The screenshot shows the Citrix NetScaler SD-WAN VPXL-10-SE interface. At the top, there is a navigation bar with 'Dashboard', 'Monitoring', and 'Configuration' tabs. A warning banner at the top left states: 'Warning: Grace license installed. Please obtain license from Citrix license portal and install it.' Below this, the 'Monitoring > Statistics' section is active. The 'Statistics' section includes a dropdown menu set to 'ARP', an 'Enable Auto Refresh' checkbox, a '5 seconds' refresh interval, and a 'Refresh' button. The 'ARP Statistics' section shows a 'Gateway ARP Timer: 1000 ms' and a filter input field. The main content is a table with 7 columns: Num, Interface, VLAN, IP Addr, MAC Addr, State, and Reply Age(mS). The table contains two entries. Navigation buttons for 'First', 'Previous', 'Next', and 'Last' are present at the bottom of the table.

Num	Interface	VLAN	IP Addr	MAC Addr	State	Reply Age(mS)
1	1	0	192.168.100.1	06:83:d9:d7:a8:02	READY_INACTIVE	19174
2	2	0	192.168.101.1	06:e3:b3:cb:bb:14	READY_ACTIVE	104

Azure

Mar 01, 2018

With NetScaler SD-WAN release 9.3, zero touch deployment capabilities have extended to Cloud instances. The procedure to deploy zero touch deployment process for cloud instances is slightly different from appliance deployment for zero touch service.

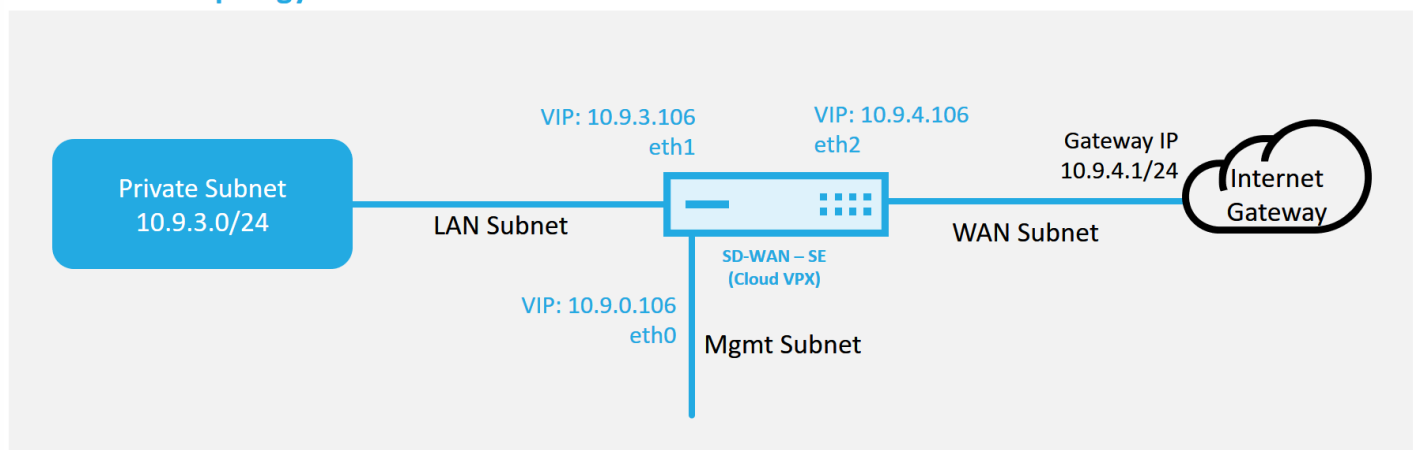
If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure should be used to add a new cloud node targeted for zero touch deployment.

a) Design the new site for SD-WAN cloud deployment by first outlining the details of the new site (i.e. VPX size, Interface Groups usage, Virtual IP Addresses, WAN Link(s) with bandwidth and their respective Gateways).

Note

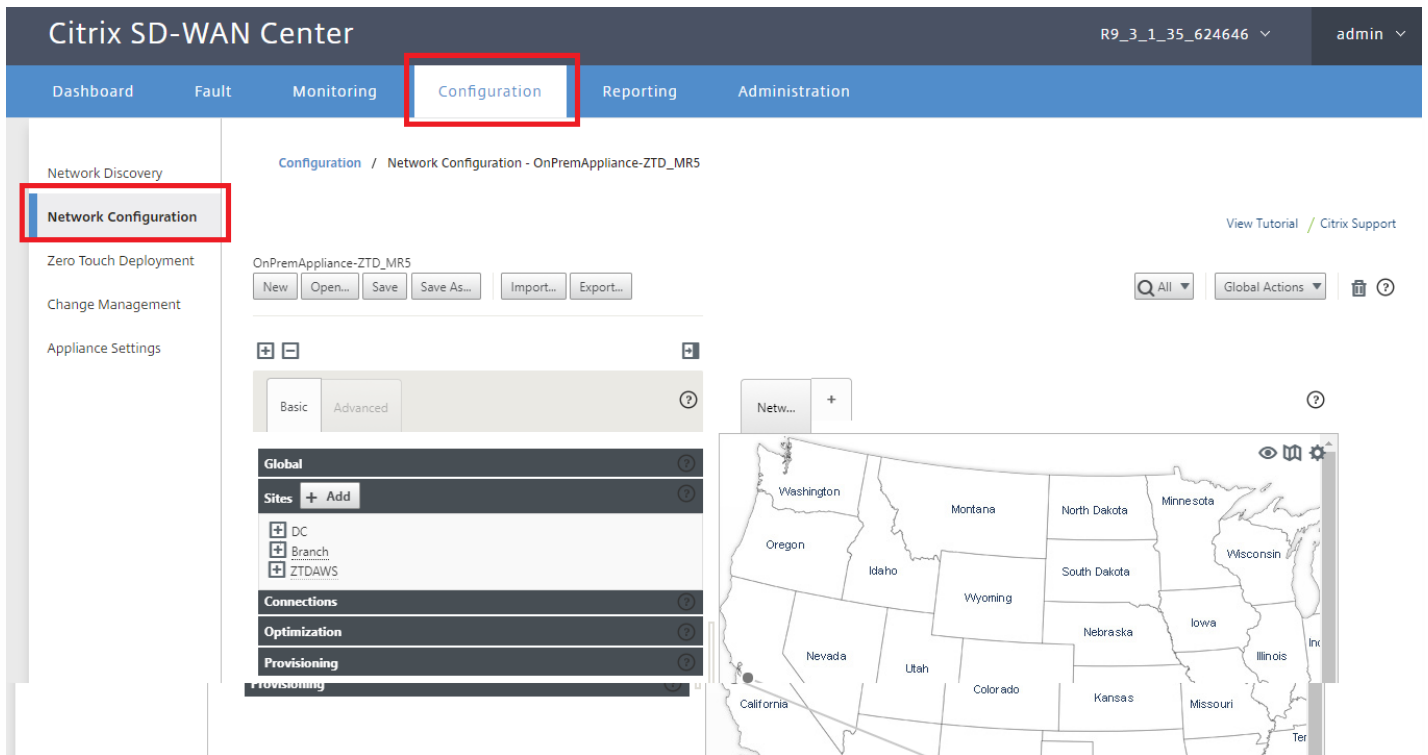
- Cloud deployed SD-WAN instances must be deployed in Edge/Gateway mode.
- The template for the cloud instance is limited to three interfaces; Management, LAN, and WAN (in that order).
- The available Azure cloud templates for SD-WAN VPX are currently hard-set to obtain the 10.9.4.106 IP for the WAN, 10.9.3.106 IP for the LAN, and 10.9.0.16 IP for the Management address. The SD-WAN configuration for the Azure node targeted for Zero Touch must match this layout.
- The Azure site name in the configuration must be all lowercase with no special characters (e.g. ztdazure).

Azure Cloud Topology with NetScaler SD-WAN



This is an example deployment of a SD-WAN cloud deployed site, the NetScaler SD-WAN device is deployed as the edge device servicing a single Internet WAN link in this cloud network. Remote sites will be able to leverage multiple distinct Internet WAN links connecting into this same Internet Gateway for the cloud, providing resiliency and aggregated bandwidth connectivity from any SD-WAN deploy site to the cloud infrastructure. This provides cost effective and highly reliable connectivity to the cloud.

b) Open the SD-WAN Center web management interface and navigate to the **Configuration > Network Configuration** page.

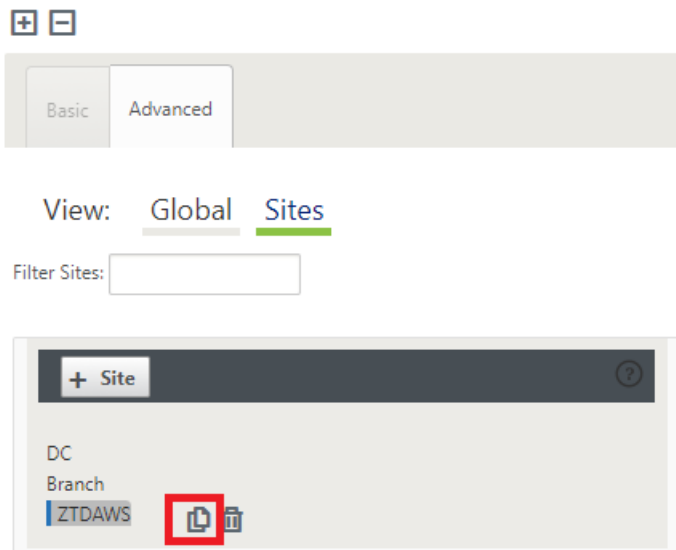


c) Make sure a working configuration is already in place, or import the configuration from the MCN.

d) Navigate to the Basic tab to create a new site.

e) Open the Sites tile to display the currently configured sites.

f) Quickly built the configuration for the new cloud site by utilizing the clone feature of any existing site, or manually build a new site.



g) Populate all the required fields from the topology designed earlier for this new cloud site.

Keep in mind that the template available for Azure cloud ZTD deployments is currently hard-set to obtain the 10.9.4.106 IP

for the WAN, 10.9.3.106 IP for the LAN, and 10.9.0.16 IP for the Management address. If the configuration is not set to match the expected VIP address for each interface, then the device will not be able to properly establish ARP to the cloud environment gateways and IP connectivity to the Virtual Path of the MCN.

It is import that the site name be compliant with what Azure expects. The site name must be in all lower case, at least 6 characters, with no special characters, it must confirm to the following regular expression $^[a-z][a-z0-9-]{1,61}[a-z0-9]$.$

Clone Site ✕

Please review the following fields and make the appropriate changes for the new Site.

Site Name:
ztdazure

Appliance Name:
azure-CBVFXL

Secure Key:
f6796bba4d1c8da2

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
E1Vlan0	0	<input type="checkbox"/>
E2Vlan0	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	E1Vlan0	10.9.3.106/24
<input checked="" type="checkbox"/>	E2Vlan0	10.9.4.106/24

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type
<input checked="" type="checkbox"/>	Azure-INET	Public Internet

Access Interfaces

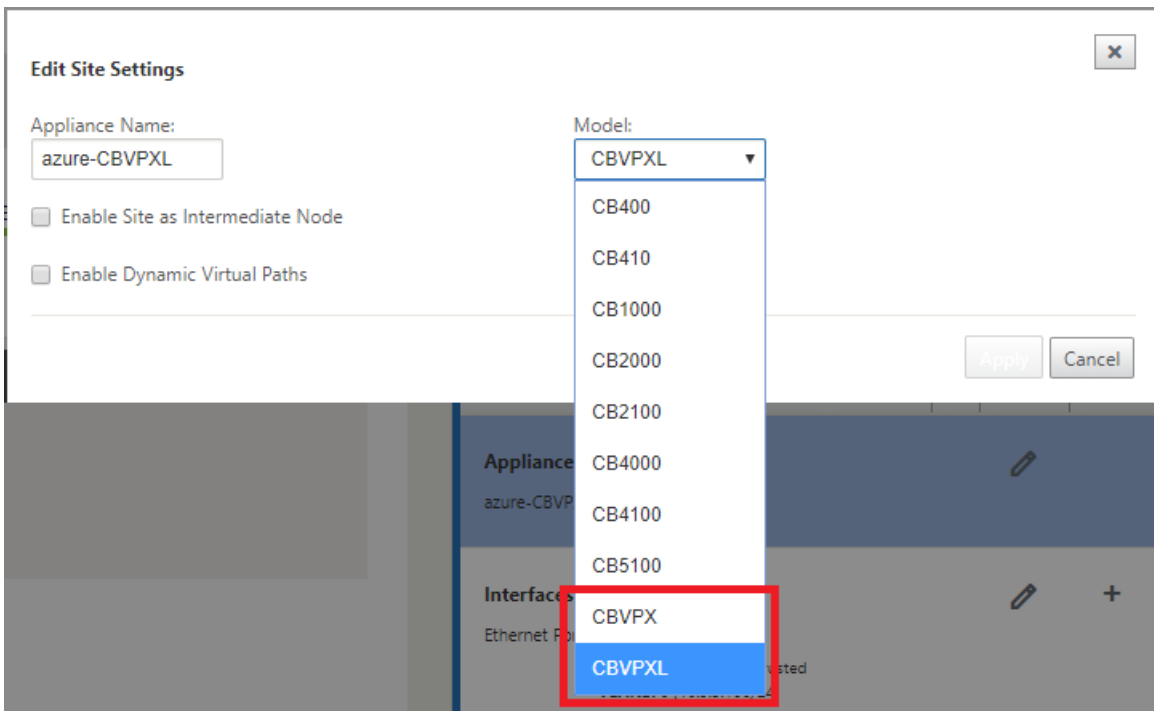
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	Azure-WL-1-AI-1	E2Vlan0	10.9.4.106	10.9.4.1

GRE Tunnels

Include	Name	Source IP	Destination IP	Tunnel IP / Prefix
---------	------	-----------	----------------	--------------------

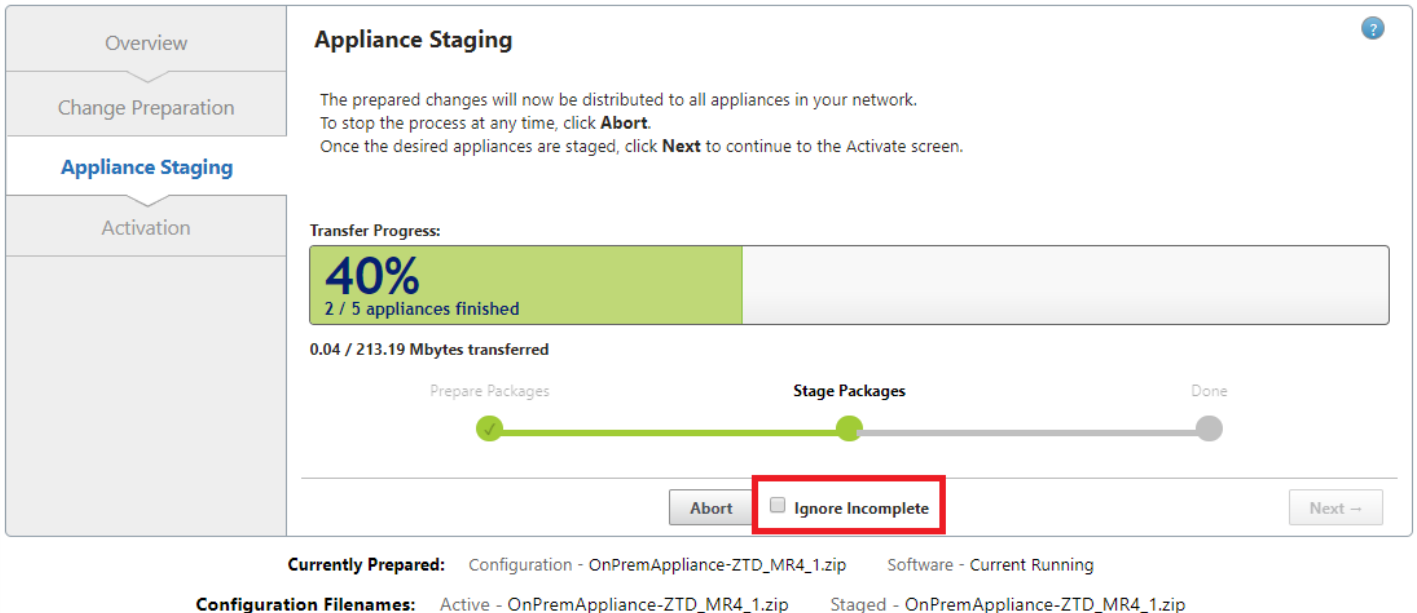
Clone
Cancel

h) After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.



i) Save the new configuration on SD-WAN Center, and use the export to the “Change Management inbox” option to push the configuration using Change Management.

j) Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you will need to utilize the “*Ignore Incomplete*” option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.



a) In the Zero Touch Deployment page, login with your Citrix account credentials. Under the **Deploy New Site** tab, select the running network configuration file.

b) After the running configuration file is selected, the list of all the branch sites with ZTD capable NetScaler SD-WAN

devices will be displayed.

The screenshot shows the Citrix SD-WAN Center interface. The top navigation bar includes Dashboard, Fault, Monitoring, Configuration (selected), Reporting, and Administration. The left sidebar lists Network Discovery, Network Configuration, Zero Touch Deployment (highlighted with a red box), Change Management, and Appliance Settings. The main content area is titled 'Configuration / Zero Touch Deployment / Prepare New Site'. It features a 'Prepare New Site' tab, a configuration dropdown set to 'OnPremAppliance-ZTD_MR5' (highlighted with a red box), and a table with three rows: Branch, ZTDAWS, and ztdazure. The 'Enable' column for 'ztdazure' has a checked checkbox (highlighted with a red box). Below the table are 'Deploy' and 'Provision and Deploy' buttons.

c) Select the target cloud site you want to deploy using the Zero Touch service, click **Enable**, and then **Provision and Deploy**.

This screenshot is similar to the previous one, showing the 'Prepare New Site' configuration. The 'Enable' checkbox for the 'ztdazure' site is checked and highlighted with a red box. The 'Provision and Deploy' button is also highlighted with a red box.

d) A pop-up window will appear, where the NetScaler SD-WAN Admin can initiate the deployment for Zero Touch. Validate that the site name complies with the requirements on Azure (lowercase with no special characters). Populate an email address where the activation URL can be delivered, and select Azure as the **Provision Type** for the desired Cloud, before clicking **Next**.

The screenshot shows a 'Provision and Deploy' pop-up window. It contains a 'Site Name' field with 'ztdazure', an 'Installer Email' field with 'ztdinstaller@outlook.com', and a 'Provision Type' dropdown menu set to 'AZURE' (highlighted with a red box). A 'Next' button is located at the bottom right.

e) After clicking **Next**, the Provision and Deploy Azure (step 1of 2) window will require input of obtained from the Azure

account.

Copy and paste each required field after obtaining the information from your Azure account. The steps below outline how to obtain the required Subscription ID, Application ID, Secret Key, and Tenant ID from your Azure account, then proceed by clicking **Next**.

Provision and Deploy Azure (step 1 of 2) [X]

Subscription ID:
52dd5bd9-2671-4cd3-8029-0f7d68108d53

Application ID:
2382ebde-09b4-4ec8-9098-0bdd6e113a54

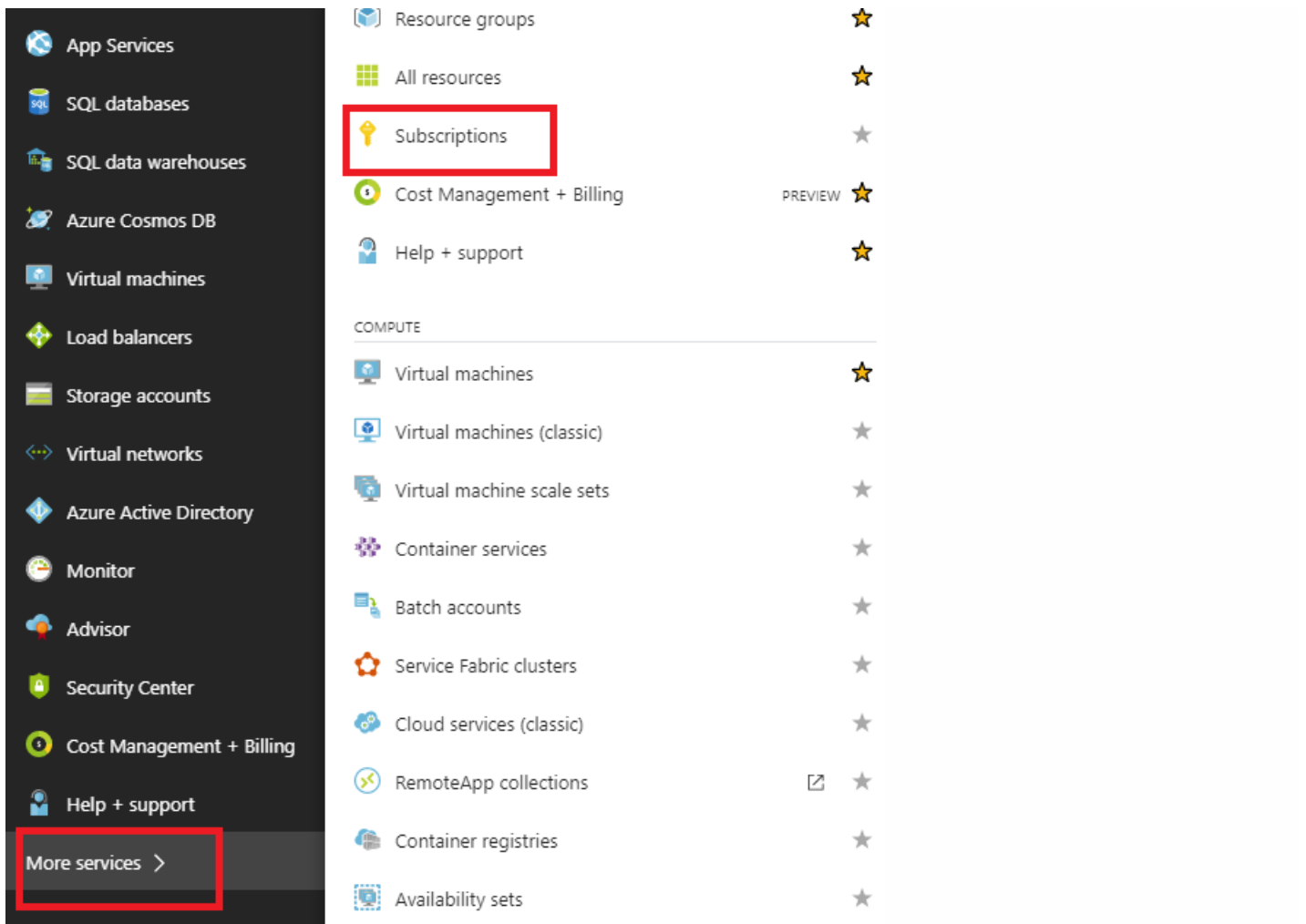
Secret Key:
om5RZX9bY2T+GzJbP0qoCgtm1fBEMS...

Tenant ID:
335836de-42ef-43a2-b145-348c2ee9ca5b

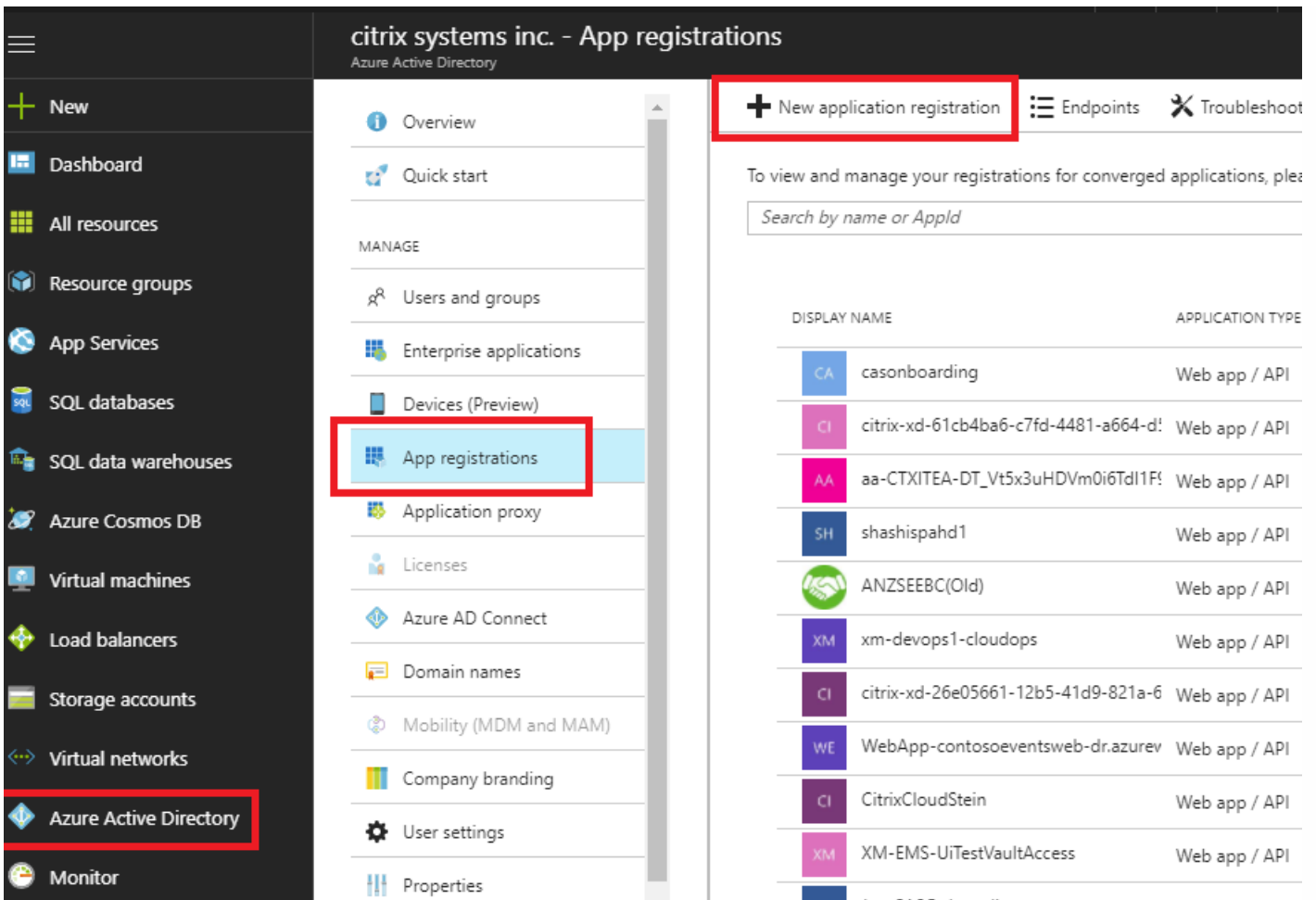
SSH Public Key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEA...
s2piG3uv2lshYlBaE4nH3y3lazetEhhl6Ng4rAf+LPSoZcBjLHh3
nAEAJmcyJTfvmt61Yd4y339ciasEDmPEWEzqcyFGaQ0i/DFI

[Back] [Next]

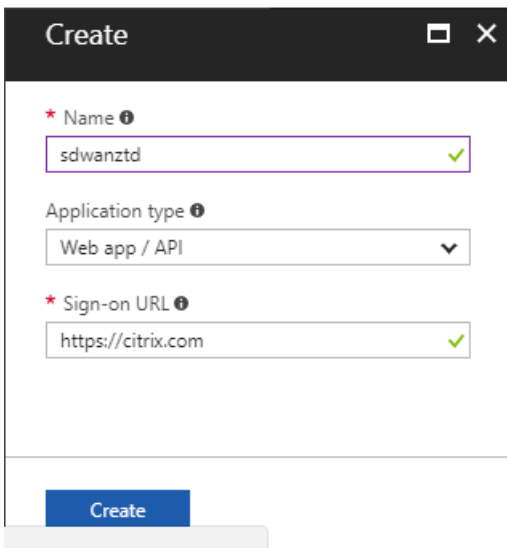
1. On the Azure account, we can identify the required *Subscription ID* by navigating to “More Services” and select **Subscriptions**.



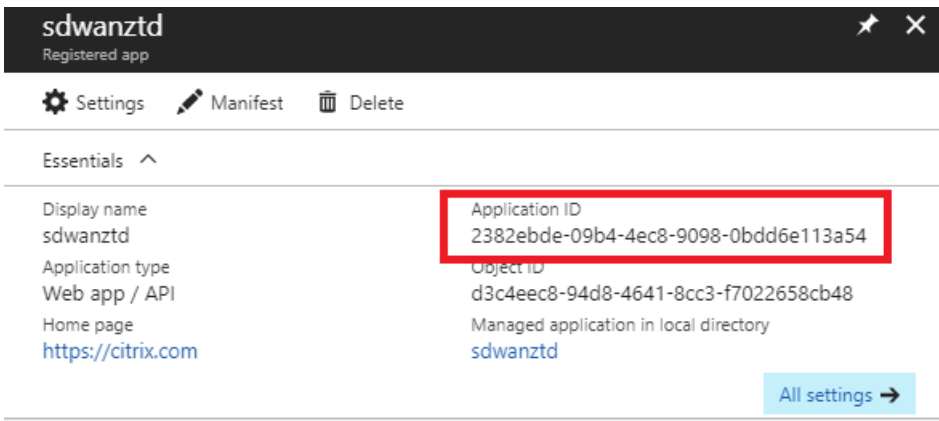
2. To identify the required *Application ID*, navigate to Azure Active Directory, Application registrations, and click **New application registration**.



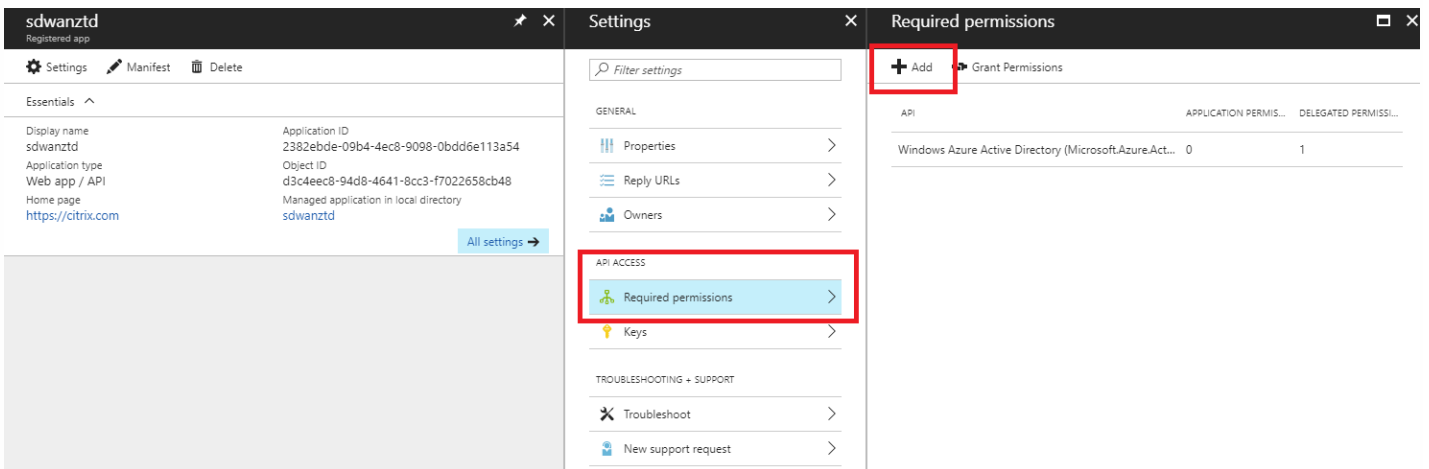
3. In the app registration create menu, enter a Name and a Sign-on URL (this can be any URL, the only requirement is that it must be valid), then click **Create**.



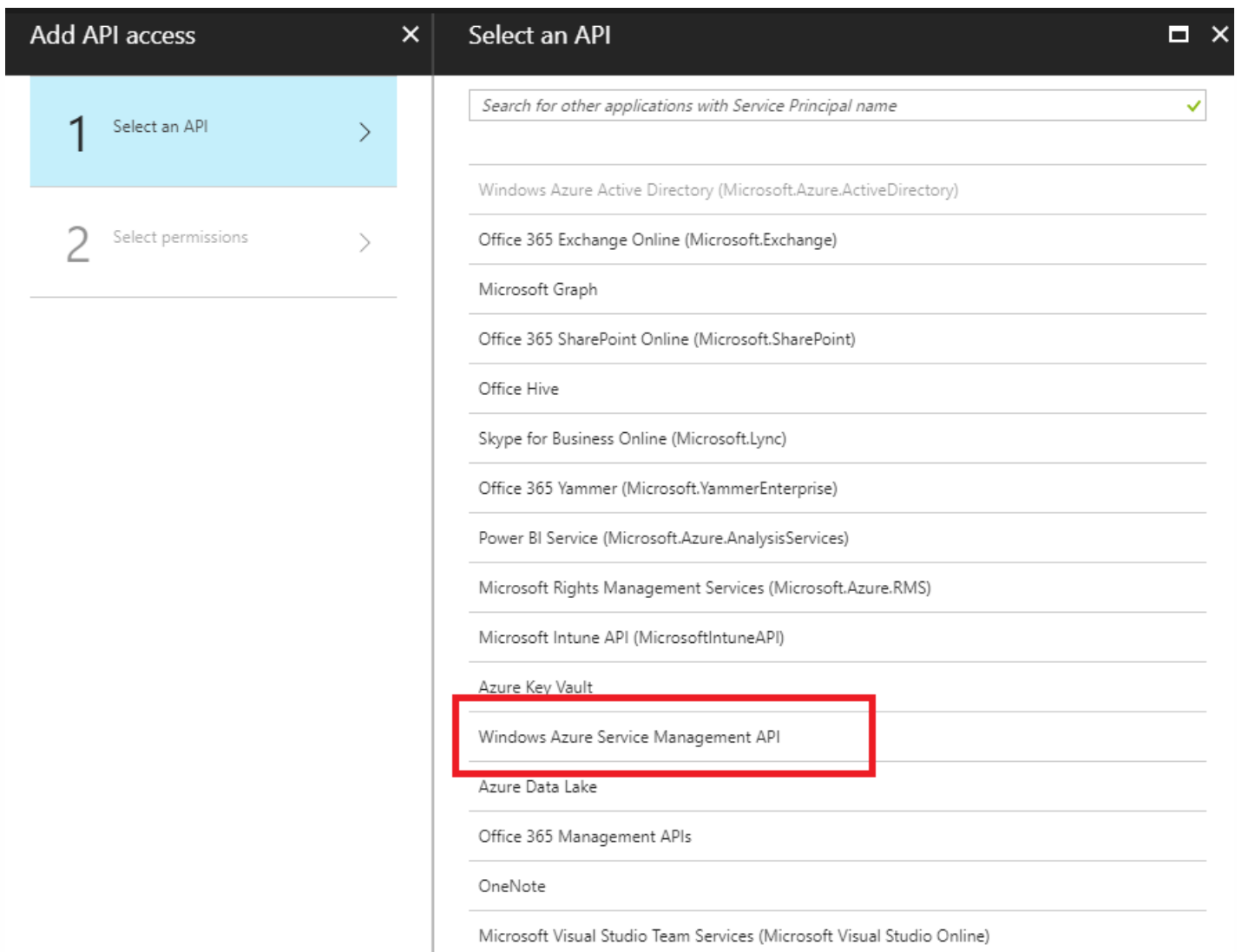
4. Search for and open the newly created Registered App, and note the Application ID.



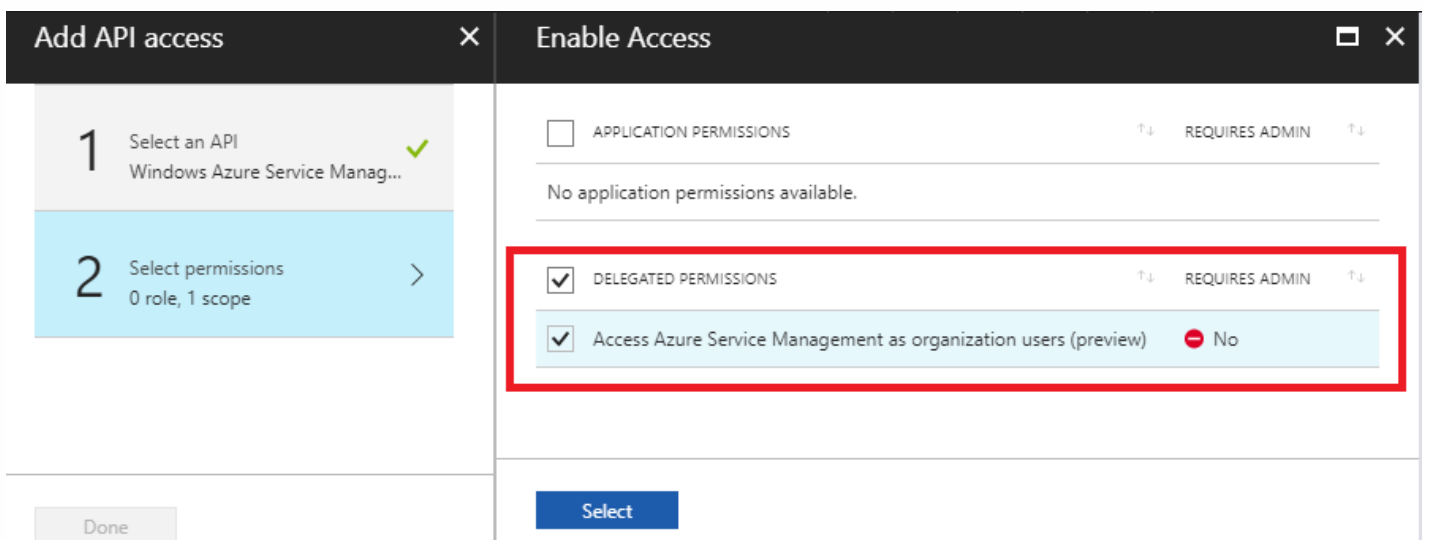
5. Again open the newly created Registration App, and to identify the required *Security Key*, under API Access, select **Required permissions**, to allow a third party to provision and instance. Then select **Add**.



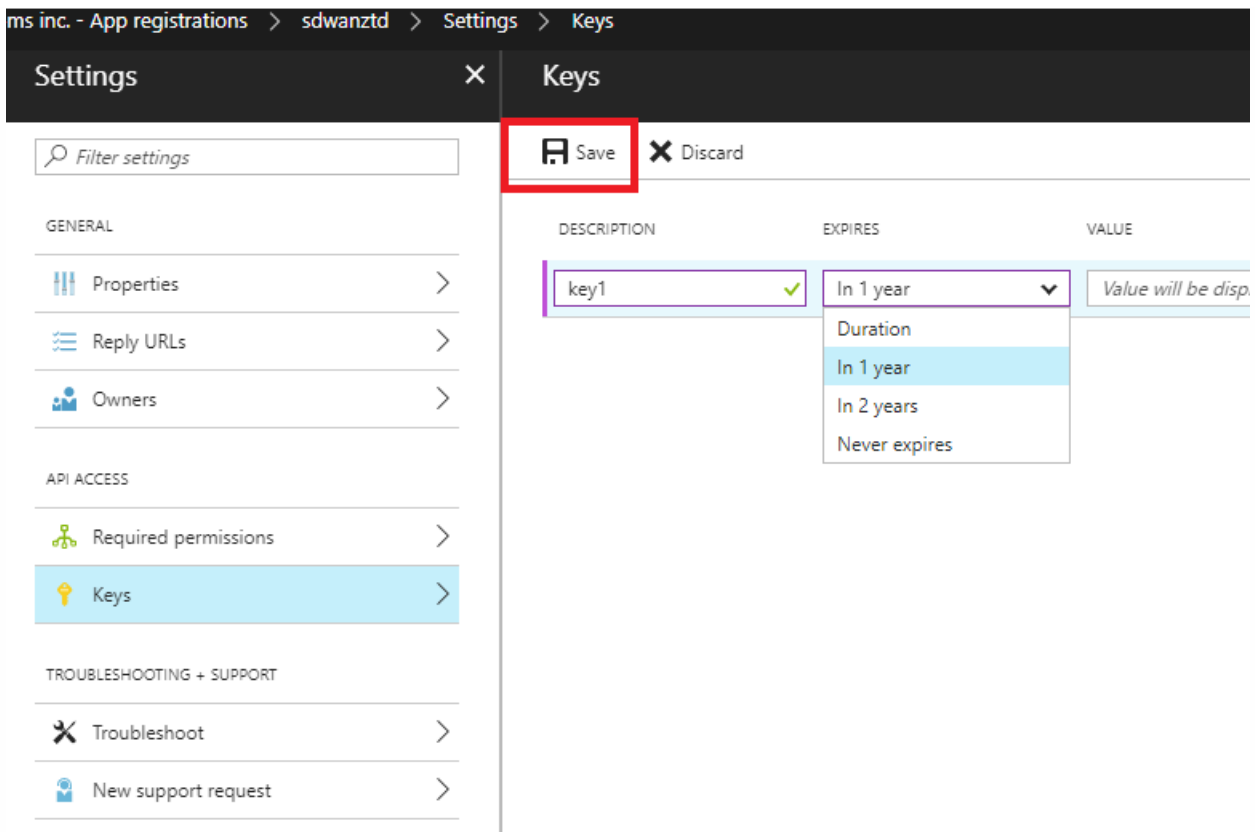
6. When adding the Required permissions, Select an API, then highlight **Windows Azure Service Management API**.



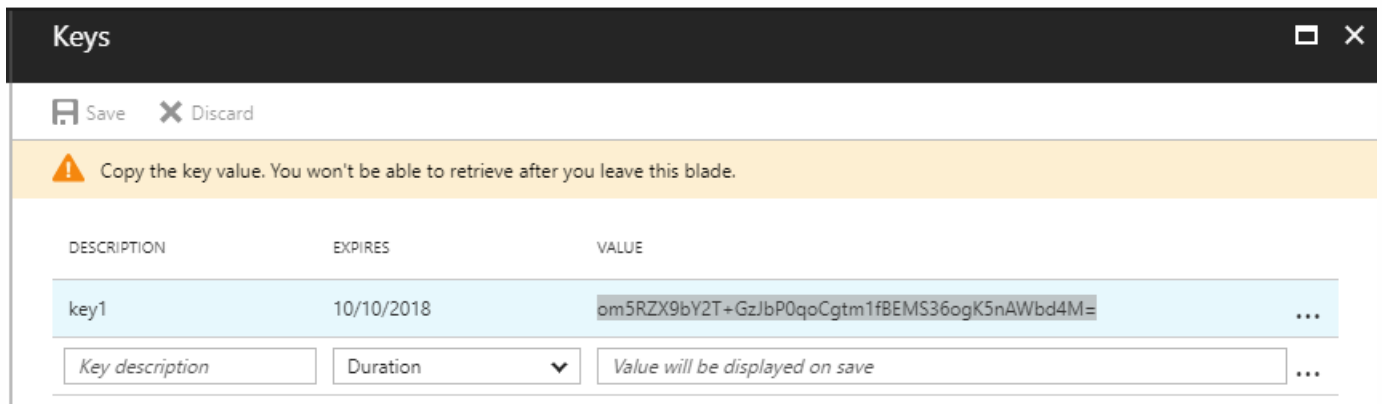
7. Enable Delegate Permissions to provision instances, then click **Select** and **Done**.



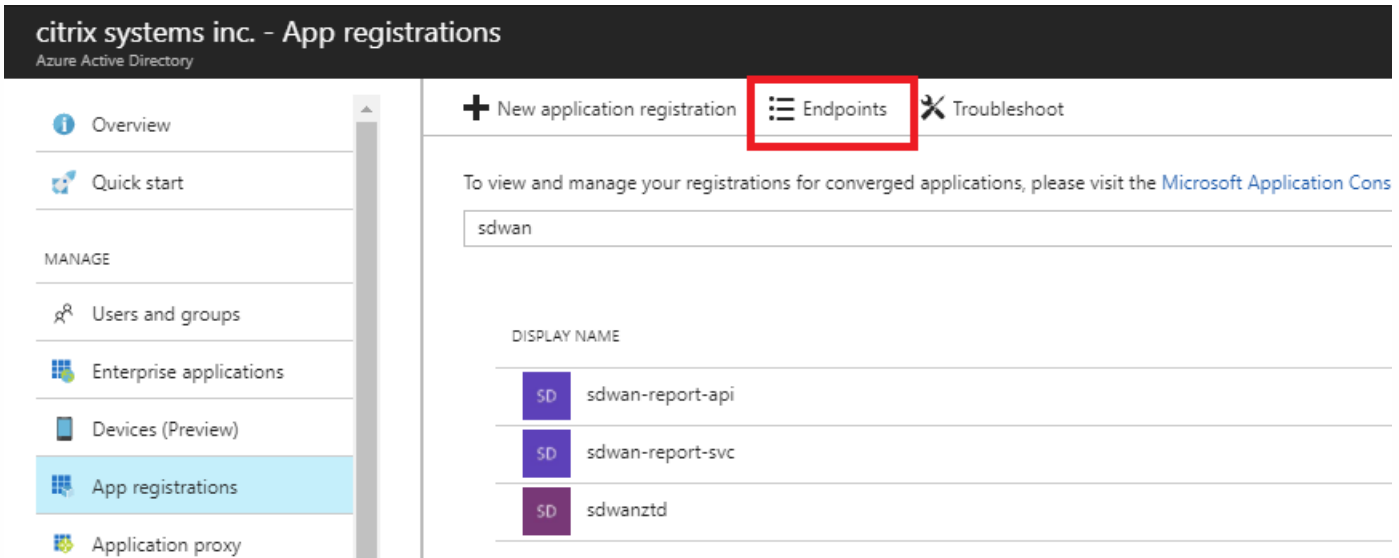
8. For this Registered App, under API Access, select **Keys**, and create a secret **key description** and the desired **duration** for the key to be valid. Then click **Save** which will produce a **secret key** (the key is only required for the provisioning process, it can be deleted after the instance is made available).



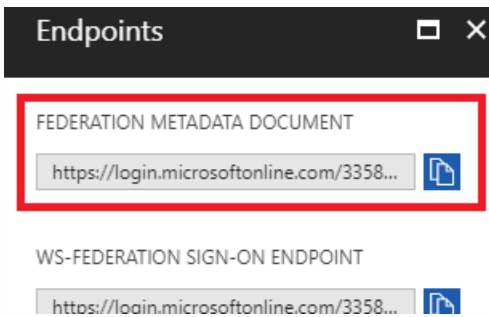
9. Copy and save the secret key (note you will not be able to retrieve this later).



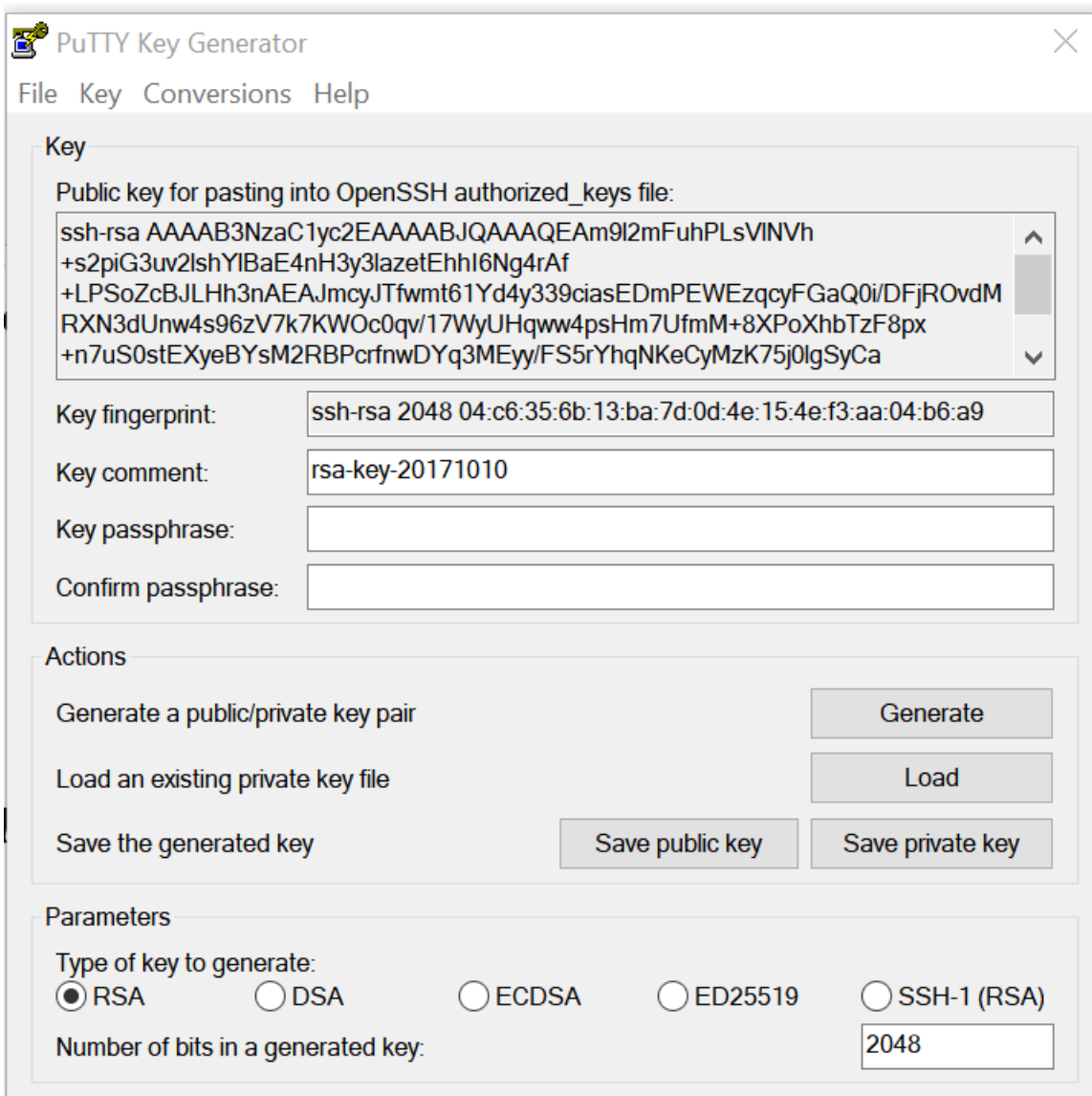
10. To identify the required *Tenant ID*, navigate back to the App registration pane, and select Endpoints.



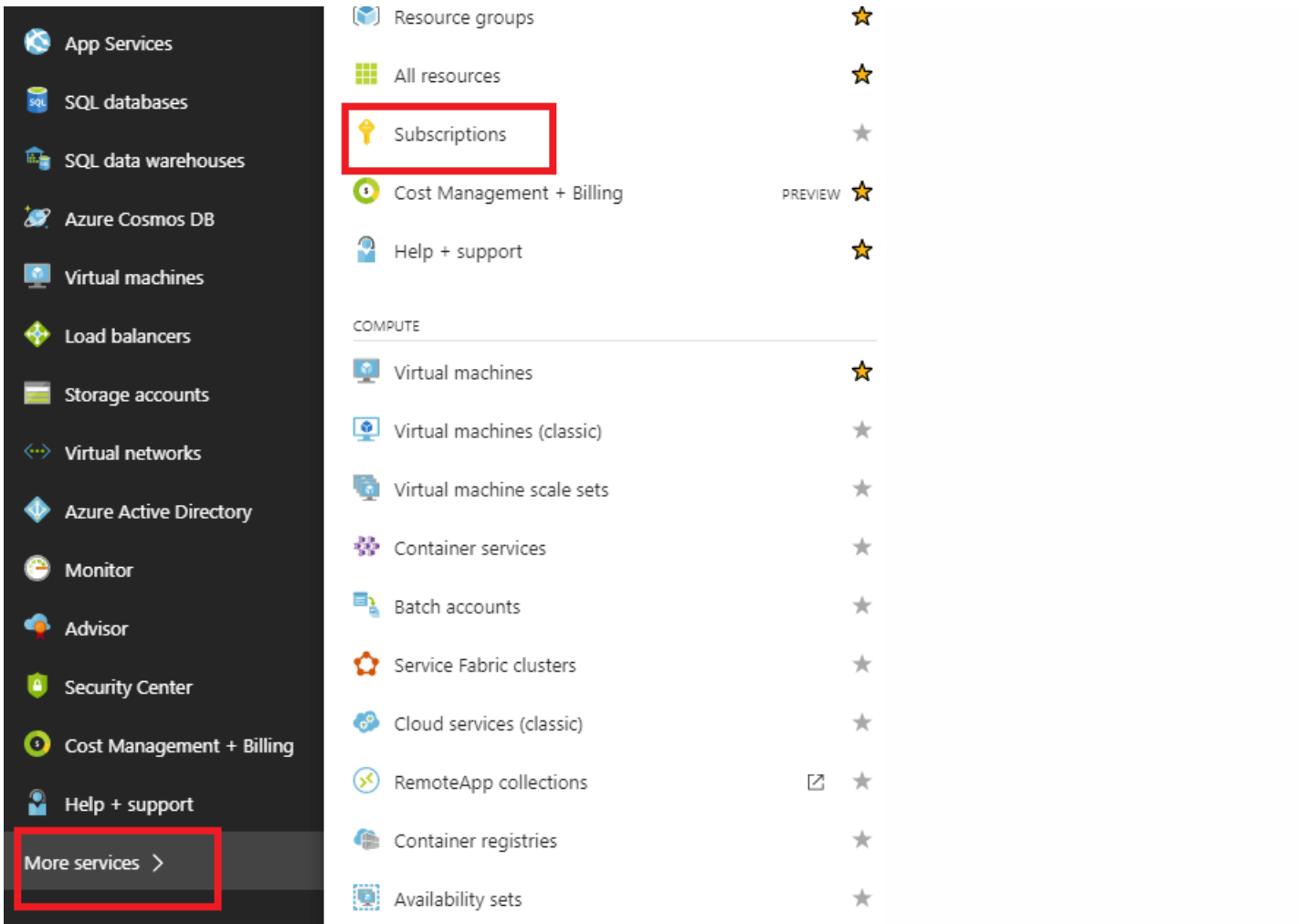
11. Copy the **Federation Metadata Document**, to identify your Tenant ID (note the Tenant ID is 36-character string located between the “online.com/” and the “/federation” in the URL).



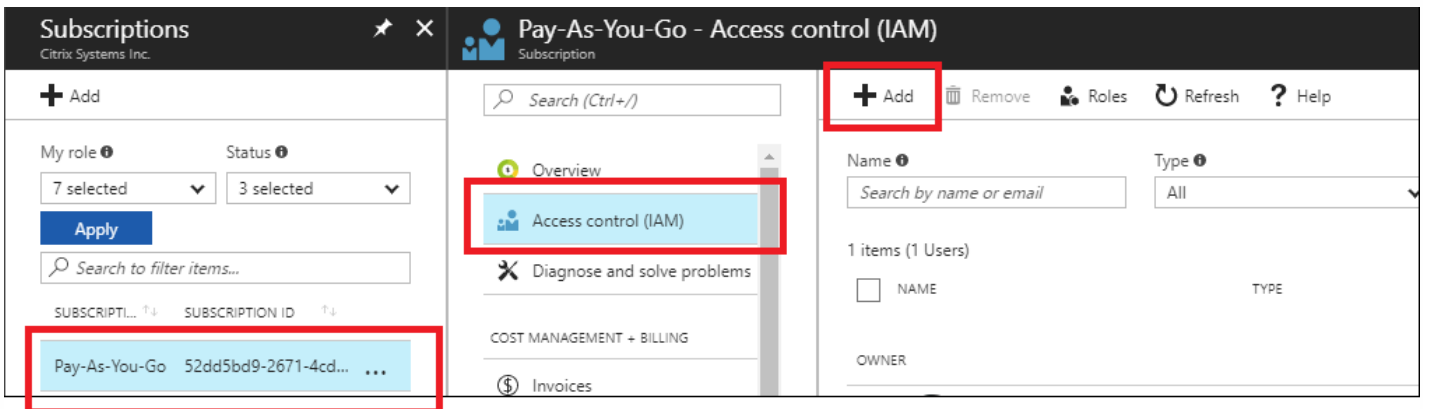
12. The last item required is the **SSH Public Key**. This can be created using Putty Key Generator or ssh-keygen and will be utilized for authentication, eliminating the need for passwords to log in. The SSH public key can be copied (including the heading ssh-rsa and trailing rsa-key strings). This public key will be shared through SD-WAN Center input to the Citrix Zero Touch Deployment Service.



13. Additional steps are required to assign the application a role. Navigate back to More Services, then Subscriptions.

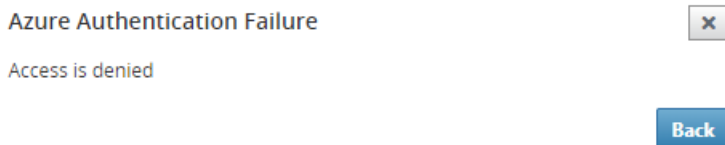


14. Select the active subscription, then **Access control (IAM)**, next click **Add**.



15. In the add permissions pane, select **“Owner”** role, assign access to **“Azure AD user, group, or application”** and search for the registered app in the Select field to allow the Zero Touch Deployment Cloud Service to create and configure the instance on the Azure subscription. Once the app is identified, select it and make sure it populates as a Selected member before clicking **Save**.

16. After collecting the required inputs and entering them into SD-WAN Center, click **Next**. If the inputs are not correct, you will encounter an authentication failure.



a) Once the Azure authentication is successful, populate the appropriate fields to select the desired Azure Region, and the appropriate Instance Size, then click **Deploy**.

Provision and Deploy Azure (step 2 of 2)

Azure Region

West US

Azure Instance Size

Standard_D4_v2

WAN subnet address prefix:

10.9.4.0/24

LAN subnet address prefix:

10.9.3.0/24

Management subnet prefix:

10.9.0.0/24

Back

Deploy

b) Navigating to the **Pending Activation** tab in SD-WAN Center, will help track the current status of the deployment.

The screenshot shows the Citrix SD-WAN Center interface. The top navigation bar includes Dashboard, Fault, Monitoring, Configuration, Reporting, and Administration. The Configuration tab is active, and the breadcrumb trail is Configuration / Zero Touch Deployment / Pending Activation. Below the breadcrumb, there are three tabs: Prepare New Site, Activation History, and Pending Activation. The Pending Activation tab is highlighted with a red box. Below the tabs, there is a table with one entry. The table has columns for Site Name, Serial No, Installer Email, Address, Status, and Action. The Status column for the entry is highlighted with a red box and shows 'Provisioning'. Below the table, there are 'Delete' and 'Modify' buttons.

Site Name	Serial No	Installer Email	Address	Status	Action
ztdazure	B0F20EC1-9DEE-4902-B072-D593536C6C02	ztdinstaller@outlook.com	AZURE - West US 2	Provisioning	

c) An email with an activation code will be delivered to the email address inputted in step 1, obtain the email and open the **activation URL** to trigger the process and check the activation status.

Focused Other Filter

NetScaler SD-WAN Cloud Service Activation Link @uswestazure

NetScaler SD-WAN Team
NetScaler SD-WAN Cloud Service A 3:44 PM
NetScaler SD-WAN Appliance Activation Info...

NT NetScaler SD-WAN Team <sdwanservice@citrix.com>
Today, 3:44 PM
You

CITRIX®

NetScaler SD-WAN Appliance Activation Information

To check the activation status, [click here](#)
(Or copy and paste this link into your Browser's address bar
`https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate?activationcode=4f19b443-7e89-4b69-9872-0f7ebeaa8ac2`).

Site Name	uswestazure
Address	AZURE - West US

Additional Notes

The NetScaler SD-WAN Team

*** This is an automatically generated email, please do not reply ***

d) An email with an activation URL will be delivered to the email address inputted in step 1. Obtain the email and open the **activation URL** to trigger the process and check the activation status.

CITRIX[®]

Zero Touch Deployment Service

Site Name: ztdazure

Appliance provisioning...

Connecting Pending

Downloading config Pending

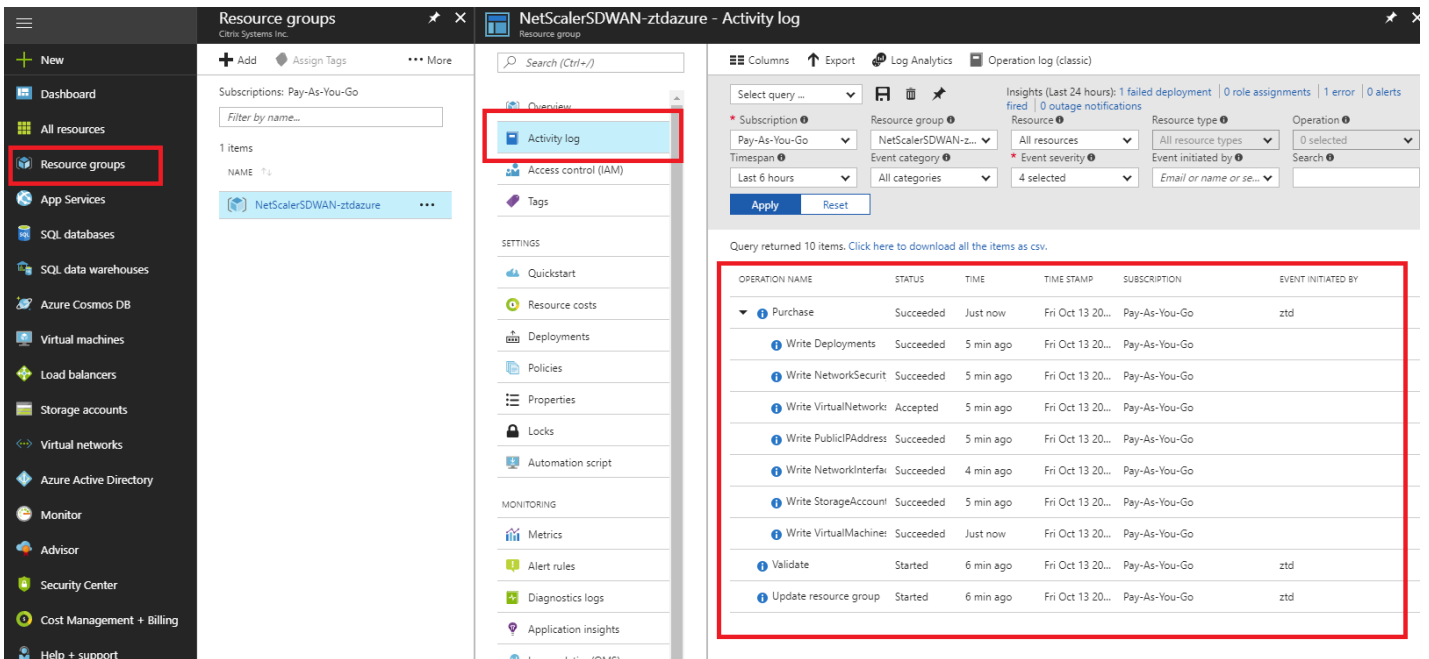
Downloading software Pending

Installing software Pending

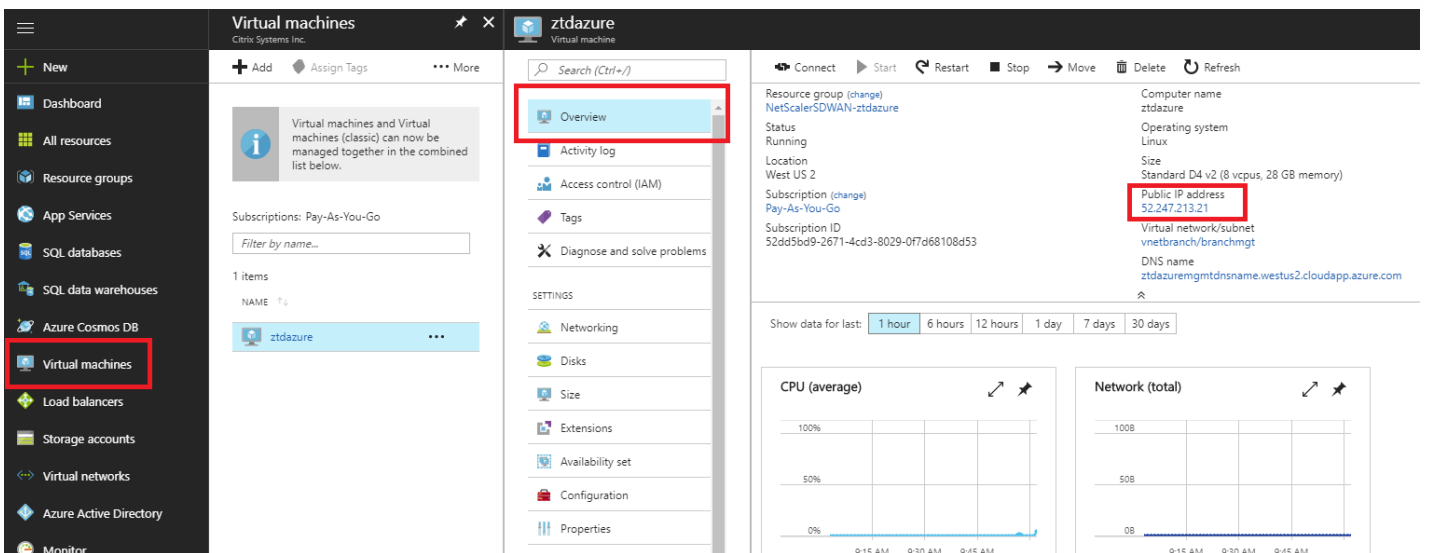
Applying config Pending

Activating Pending

e) It will take a few minutes for the instance to be provisioned by the SD-WAN Cloud Service. You can monitor the activity on the Azure portal, under **Activity log** for the **Resource Group** which is automatically created. Any issues or errors with the provisioning will be populated here, as well as replicated to SD-WAN Center in the Activation Status.



f) In the Azure portal, the successfully launched instance will be available under **Virtual Machines**. To obtain the assigned public IP, navigate to the Overview for the instance.



g) After the VM is in a running state, give it a minute before the service will reach out and start the process of downloading the configuration, software and license.

Zero Touch Deployment Service

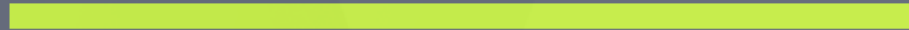
Site Name: ztdazure

Appliance Activated...

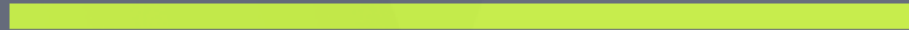
Connecting Completed



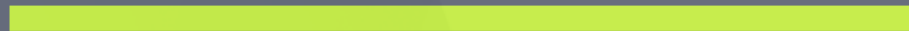
Downloading config Completed



Downloading software Completed



Installing software Completed



Applying config Completed



Activating Completed



h) After each of the SD-WAN Cloud service steps are automatically complicated, log in to the SD-WAN instances web interface using the public IP obtained from the Azure portal.

Citrix NetScaler SD-WAN VPXL-10-SE Info: 9.3.1.35.624646 **Logout**

Dashboard | **Monitoring** | **Configuration**

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

System Status

Name: **ztdazure**
 Model: **VPXL**
 Appliance Mode: **Client**
 Serial Number: **0000-0005-7786-4927-4958-4331-78**
 Management IP Address: **10.9.0.106**
 Appliance Uptime: **6 minutes, 52.3 seconds**
 Service Uptime: **1 minutes, 58.0 seconds**
 Routing Domain Enabled: **Default_RoutingDomain**

Local Versions

Configuration Created On: **Fri Oct 13 16:30:55 2017**
 Software Version: **9.3.1.35.624646**
 Built On: **Oct 2 2017 at 21:01:31**
 Hardware Version: **VPXL**
 OS Partition Version: **4.6**

Virtual Path Service Status

Virtual Path DC-ztdazure Uptime: **1 minutes, 15.0 seconds.**

i) The NetScaler SD-WAN Monitoring Statistics page will identify successful connectivity from the MCN to the SD-WAN instance in Azure.

Citrix NetScaler SD-WAN VPXL-10-SE Info: 9.3.1.35.624646 **Logout**

Dashboard | **Monitoring** | **Configuration**

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

Monitoring > Statistics

Statistics

Show: **Paths (Summary)** Enable Auto Refresh **5** seconds Show latest data.

Path Statistics Summary

Filter: in **Any column** Show **100** entries

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	Azure-INET	DC-INET	GOOD	GOOD	Static	2	2	0.00	10.83	NO
2	DC-INET	Azure-INET	GOOD	GOOD	Static	2	2	0.00	17.60	NO

Showing 1 to 2 of 2 entries

Bandwidth calculated over the last 0.851 seconds

j) Furthermore, the successful (or unsuccessful) provisioning attempt will be logged in the SD-WAN Center's Activation History page.

- Network Discovery
- Network Configuration
- Zero Touch Deployment
- Change Management
- Appliance Settings

Configuration / Zero Touch Deployment / Activation History

Prepare New Site **Activation History** Pending Activation

Showing 1 - 1 of 1

Site Name	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
ztdazure	C736A440-0A37-4676-AF5D-CCDB74220783	ztdinstaller@outlook.com	AZURE - West US	Appliance Activated	Oct 14 15:10:13 2017 UTC	Activated	<input type="checkbox"/>

Configure 210-SE LTE

Jun 08, 2018

The following procedure describes the steps and workflow to configure a 210-SE LTE appliance.

Prerequisites

1. Have a standard or 2FF SIM card (15 x 25 mm) from the preferred carrier.
2. Have the Access Point Name (APN) information from the preferred carrier, if different from the default APN settings. The APN information varies from carrier to carrier.

Note

See the [210-SE LTE QSG](#) for more information about installing the appliance.

Add and Configure 210-SE LTE Appliance in the Network

1. Insert the SIM card into the SIM card slot of the appliance. Only a standard or 2FF SIM card (15x25 mm) is supported.
2. In the SD-WAN appliance GUI, navigate to **Configuration > Appliance Settings > Network Adapters > Mobile Broadband**.
 - a. If the APN settings are not the default, type the APN settings details.

The screenshot shows a web form titled "APN Settings". It contains three text input fields: "APN:", "Username:", and "Password:". Below these fields is a button labeled "Change APN Settings".

- b. Verify the status info page.

- Status: Enabled means modem tries to establish the data session.
- Card state: If present, it indicates that SIM is properly inserted.
- Signal strength: Excellent, Good, Fair, Poor, or no signal.
- Home network: Carrier of the SIM you inserted.
- APN name: APN used by the LTE modem.
- Session state: Connected indicates that the device has joined the network.

If the session state is disconnected, check with carrier whether:

- The account has been activated.
- The data plan is enabled or not.

Status Info Refresh

<p>Modem</p> <p>Type : 210-LTE-R1</p> <p>IMEI Number : 354324070049180</p> <p>Status : Enabled</p> <p>Active Firmware: 02.24.05.06_VERIZON</p>	<p>Cellular network</p> <p>Home Network : Verizon Wireless</p> <p>Radio Interface : LTE</p> <p>Signal Strength : Excellent</p> <p>Session State : CONNECTED</p> <p>APN Name : pwsdia.gw8.vzwentp</p> <p>Profile Name :</p>	<p>Network</p> <p>IP Address/Gateway : 100.87.12.193/ 100.87.12.194</p> <p>Primary/Secondary DNS : 198.224.160.135/ 198.224.164.135</p>
---	--	--

Detailed info

Status Info Refresh

Modem

Manufacture: **Sierra Wireless, Incorporated**

Modem Type: **210-LTE-R1**

Modem Status: **Enabled**

Active Firmware: **02.24.05.06_VERIZON**

Model Id: **EM7455**

Firmware Revisions: **SWI9X30C_02.24.05.06_r7040 CARMD-EV-FRMWR2 2017/05/19 06:23:09**

Boot Revisions: **SWI9X30C_02.24.05.06_r7040 CARMD-EV-FRMWR2 2017/05/19 06:23:09**

PRI Revisions: **9904802 001.003 Generic-Laptop**

PRL Version: **15569**

PRL Preference: **1**

IMSI Number: **311480993245597**

ICCID Number: **8914800003218542467**

ESN Number: **0**

IMEI Number: **354324070049180**

MEID Number: **35432407004918**

Hardware Revision: **1.0**

Device State: **READY**

Cellular Network

Home Network: **Verizon Wireless**

Roaming Status: **Home**

Session State: **CONNECTED**

Data Bearer: **GPRS**

Dormancy Status: **Traffic Channel Active**

LU Reject Cause: **0**

Card State: **Present**

Call Statistics

Call Status: **CONNECTED**

Bytes Transferred: **684528**

Bytes Received: **571824**

RF Information

Radio Interface: **LTE**

Active Band Class: **121**

Active Channel: **1150**

Signal Strength: **Excellent**

ECIO: **0**

IO: **0**

SINR: **0**

RSRQ: **-11**

Profile

PDP Type: **IPv4**

Authentication: **0**

Profile Name:

APN Name: **pwsdia.gw8.vzwentp**

User Name:

IP Address: **100.87.12.193**

Gateway Address: **100.87.12.194**

Primary DNS: **198.224.160.135**

Secondary DNS: **198.224.164.135**

Show less

Manage Firmware

The AUTO-SIM option allows the LTE modem to choose the most matching firmware based on the SIM card inserted. Choose **AUTO-SIM**, if you are unsure which firmware to use. You can upload new firmware if available, using the **Upload** option.

Manage Firmware

Filename: No file chosen

Available Firmwares

AUTO-SIM ▼

- AUTO-SIM
- 02.24.03.00_VODAFONE
- 02.24.05.06_BELL
- 02.24.05.06_GENERIC
- 02.24.05.06_ROGERS
- 02.24.05.06_VERIZON

Enable/Disable Modem

Enable/disable modem depending on your intent to use the LTE functionality. By default, the LTE modem is enabled.

Reboot Modem

Reboots the modem. It can take up to 3-5 minutes for the reboot operation to complete.

Refresh SIM

Use this option when you hot swap the SIM card to detect the new SIM card by the 210-SE LTE modem.

Manage Firmware

Filename: No file chosen

Available Firmwares

AUTO-SIM ▼

Enable/Disable Modem

Reboot Modem

SIM Card

Configure 210-SE LTE Using CLI

To configure 210-SE LTE modem using the CLI:

1. Log in to the SD-WAN appliance console.
2. At the prompt, type the user name and password to gain CLI interface access.
3. At the prompt, type the command lte. Type >help. This displays the list of LTE commands available for configuration.

```

admin@10.216.139.21's password:
=====
      Operating System 4.6 on CB210v1
      Host IP = 10.216.139.21
=====
Last login: Thu May  3 09:28:48 2018 from 10.252.241.81
Console to Citrix acquired

lte1>lte
lte>help
status                # Show status
show                  # Show settings
disable               # Disable LTE modem
enable                # Enable LTE modem
apn <apn> [<user name> [<password>]] # Set APN
sim-power <off|on|reset> # Off, on, reset SIM card power
reboot                # Reboot modem
ping                  # Check if modem manager ready
list-fw               # List available firmware
apply-fw <fw>        # Apply the specified firmware
lte>

```

The following table lists the LTE command descriptions.

Command	Description
Help {lte>help}	Lists the available LTE commands and parameters
Status {lte>status}	Displays LTE connectivity status
Show {lte>show}	Displays LTE settings
Disable {lte>disable}	Disables LTE modem
Enable {lte>enable}	Enables LTE modem
Apn {lte>apn}	Configures APN settings information
Sim-power <off on reset> {lte>sim-power}	Powers off sim card, Power on sim card, Refresh sim card
Reboot {lte>reboot}	Restarts LTE modem
Ping {lte>ping}	Pings LTE modem
List-fw {lte>list-fw}	Lists firmware available on the R1 or R2 LTE modems
Apply-fw <fw> {lte>apply-fw}	Applies firmware specific to a carrier

Configure MCN for LTE

To configure an MCN:

1. Log in to the SD-WAN appliance GUI. Go to **Configuration Editor**. Complete configuration for the MCN site, see; [Configure MCN](#).
2. Ensure that you select the **Sub Model** as **LTE** for the 210-SE appliance client site configuration.
3. Ensure that you provide routable public IP address as part of WAN link configuration.

You do not have to configure public IP address for client appliances.

Site Name: LTE

Secure Key: 38b9fd3adb98a915

Model: CB210

Sub Model: LTE

Mode: client

Enable Site as Intermediate Node

Enable Dynamic Virtual Paths

Add Cancel

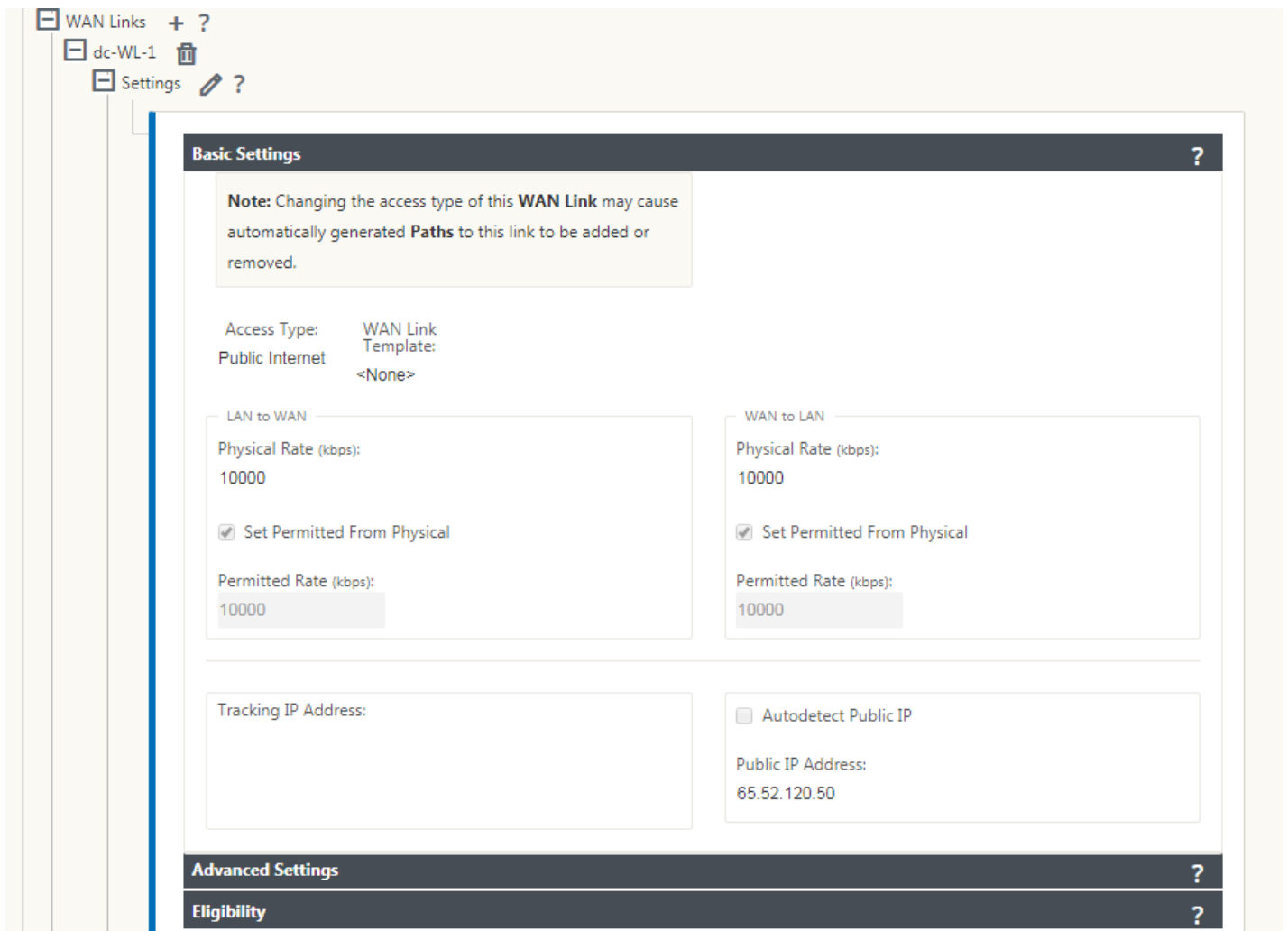
Note

If you configured network with a 210-SE appliance with release 9.3 version 5, it is possible to misconfigure the 210-SE appliance with incorrect hardware. For instance, during the change management process, a 210-SE appliance with no LTE port can still turn on the LTE port in the configuration and push that change to the non LTE 210-SE appliance.

To prevent misconfiguring incorrect 210-SE appliance, you have to update the network to release 10.0 version 2. Ensure that

- Any 210-SE LTE appliances in the network have the "LTE" sub-model configured or selected for those sites.
- Any 210-SE base (non-LTE) appliances in the network have the "BASE" sub-model configured at those sites.

Any 210-SE appliance with the "LTE" port enabled in release 9.3 version 5 automatically translates to the 210-SE LTE sub-model after migrating to release 10.0 version 2.



Configure Branch for LTE

To configure the 210-SE LTE appliance as a branch site:

1. In the SD-WAN appliance GUI, go to configuration editor. See; [Configure Branch](#).

a. Create Interface Groups.

b. Create up to one Virtual Interface and one Interface Group for the LTE adapter to configure WAN link by selecting the following:

- i. Ethernet Interface – LTE 1
- ii. Security- untrusted (default)
- iii. DHCP client - Enabled (default)

Interface Groups + ?

	Virtual Interfaces	Ethernet Interfaces					Bypass Mode	WCCP	Security	Delete
+ VirtualInterface-1 (0)	1/1	1/2	1/3	1/4	1/5	LTE-1	Fail-to-Wire	<input type="checkbox"/>	Trusted	
+ VirtualInterface-2 (206)	1/1	1/2	1/3	1/4	1/5	LTE-1	Fail-to-Block	<input type="checkbox"/>	Trusted	
+ VirtualInterface-3 (0)	1/1	1/2	1/3	1/4	1/5	LTE-1	Fail-to-Block	<input type="checkbox"/>	Trusted	
- VirtualInterface-4 (0)	1/1	1/2	1/3	1/4	1/5	LTE-1	Fail-to-Block	<input type="checkbox"/>	Untrusted	

Virtual Interfaces +					Bridge Pairs +		
Name	Firewall Zone	VLAN ID	DHCP Client	Delete	Interfaces	LSP	Delete
VirtualInterface-4	Untrusted_Internet_Zone	0	<input checked="" type="checkbox"/>				

2. Enable **AutoDetect Public IP** for WAN link configuration when configuring WAN link using the virtual interface created for LTE interface.

br210-WL-4

Settings ?

Basic Settings ?

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

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

<p>LAN to WAN</p> <p>Physical Rate (kbps): 10000</p> <p><input checked="" type="checkbox"/> Set Permitted From Physical <input type="checkbox"/> Auto Learn</p> <p>Permitted Rate (kbps): 10000</p> <p>Tracking IP Address:</p>	<p>WAN to LAN</p> <p>Physical Rate (kbps): 10000</p> <p><input checked="" type="checkbox"/> Set Permitted From Physical <input type="checkbox"/> Auto Learn</p> <p>Permitted Rate (kbps): 10000</p> <p><input checked="" type="checkbox"/> Autodetect Public IP</p> <p>Public IP Address:</p>
--	--

Advanced Settings ?

3. By default, when you try to configure WAN link using LTE interface, the WAN link is marked as Metered link and **Last-Resort** Standby mode. You can change these default settings, if necessary.

Advanced Settings	?
Eligibility	?
Metered/Standby Link	?
Metering <input checked="" type="checkbox"/> Enable Metering Data Cap (MB): <input type="text" value="0"/> Billing Cycle: <input type="text" value="Monthly"/> Starting From: <input type="text" value="MM/DD/YYYY"/>	
Standby Standby Mode: <input type="text" value="Last-Resort"/> Priority: <input type="text" value="1"/>	

Note

Configure the **active MTU detect** option for the WAN links created using the LTE interface. Establishing dynamic virtual paths using LTE interface is not supported.

Ignore configuring the IP address and gateway address for the Access Interface of the WAN link. This information is obtained from the carrier through DHCP.

Access Interfaces + ?						
Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
br-WL-1-AI-1	V2			Primary	<input type="checkbox"/>	

Apply Revert

4. Complete rest of the required Branch configuration for the 210-SE LTE appliance. See; [configure Branch](#).
5. Perform Change Management by uploading the SD-WAN software. See the [Change Management](#) procedure.
6. Activate configuration through the Local Change Management process. When you perform Change Management, configuration is activated and required configuration is applied.

Important

When you perform Local Change Management and install a package where the sub model of the package does not match the actual sub model of the appliance, validation fails and the following message is displayed:

"Appliance sub_model (BASE) does not match the sub_model this package is prepared for (LTE)"

Configuration > System Maintenance > Local Change Management

Upload

Local Appliance Change Process

The Local Change Management process allows a user to upload a new appliance package to this individual appliance. This two-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied to the appliance in a reliable, fail-safe way.

Note: This process does not update any other appliances on the network. For that purpose, use the Configuration -> Virtual WAN -> Change Management screen on the MCN.

Upload Item: No file chosen
Valid file types: ".zip"

Error: The uploaded file failed validation. Appliance sub_model (BASE) does not match the sub_model this package is prepared for (UNKNOWN).

Configuration Filenames: Active – Basic_RCN_cfg_fast_210_210LTE.db Staged – Basic_RCN_cfg_fast.db

Model	Active Software	Active Config	Staged Software	Staged Config
CBVPX	10.0.2.28.684046 download	15:12 on 6/1/18	10.0.2.28.684046 download	14:54 on 6/1/18

Note

High availability is supported on the 210-SE LTE platform.

Inline helptext describing the LTE settings is added in the SD-WAN 210-SE LTE appliance GUI.

Help ✕

The "Mobile Broadband" section will help manage the LTE settings on the appliance.

Available Sections

- **Status Info:** Provides status information of your Modem, Cellular Data, Profile etc.
- **APN Settings:** The user can modify APN Name, Username and Password under this section.
- **Manage Firmware:** Each appliance (that has LTE enabled) will have a set of available firmwares. This section contains a listing of all the available firmwares on that modem. User can also modify the active firmware and also chose to delete a firmware file. There is also a way to upload new firmware files if the user wishes to.
- **Enable/Disable Modem:** This button will enable or disable the Mobile Broadband on the appliance.
- **Reboot Modem:** User can Reboot the modem by clicking on this button.
- **SIM Card:** User can Refresh the SIM Card in this section.

ZTD over LTE

Pre-requisites for enabling ZTD service over LTE:

1. Install antenna and the SIM card for the 210-SE LTE appliance.
2. Ensure that the SIM card has an activated data plan.
3. Ensure that the management port is not connected.
 - If the management port is connected, disconnect the management port and then restart the appliance.
 - Configure the Management Interface with DHCP, if a static IP address on the Management Interface is configured. Apply the configuration, and then disconnect the Management port, and restart the appliance.
4. Ensure that the 210-SE appliance configuration has internet service defined for LTE interface.

The ZTD service uses the LTE port to obtain latest SD-WAN software and SD-WAN configuration when:

- Appliance is powered on.
- Management port is not connected.

You can use the SD-WAN Center GUI to deploy and configure 210-SE LTE appliance for the ZTD service.

See the [ZTD procedure](#) for more information about deploying and configuring 210-SE LTE appliance using SD-WAN Center.

ZTD Service over Management Interface for 210-SE LTE Appliance

Connect the Management Port and use the standard [ZTD procedure](#) that is supported on all other non-LTE platforms.

Manage 210-SE LTE Using SD-WAN Center

The **Mobile Broadband** page under the **Configuration** tab in the SD-WAN Center GUI displays information about the LTE modem configuration. You can perform the LTE modem operations using the same options or buttons displayed in the SD-WAN 210-SE appliance GUI configuration for mobile broadband settings. LTE summary table lists 210-SE LTE appliances and you can select either single or multiple appliances to perform LTE modem operations.

Note

Multi region support in SD-WAN Center is added for the region-level architecture in SD-WAN release 10.0.2 and beyond.

For multi region networks:

Head end SD-WAN Center shows data and summary from all LTE sites in the network. All modem operations, except upload, can be performed on site of any region from Head end SD-WAN Center. Upload operation can be performed on a site from respective Collector SD-WAN Center. The Head end can only perform upload operation for sites in “Default Region” and Collector can perform upload operation for the sites in its region.

Collector SD-WAN Center has a Mobile Broadband tab page, which shows data and summary from LTE Sites in its region. You can perform modem operations on any LTE sites in the region from the Collector.

Network Configuration
Zero Touch Deployment
Change Management
Appliance Settings
Mobile Broadband

Remote Management and LTE Site Support

Modem Actions:

Show entries Showing 1 to 1 of 1 entries 1 row selected Search:

Site Name	Available Firmware	Model	Modem Status	Radio Interface	Home Network	Signal Strength	APN	Session State	IP Address	IMEI	Active Firmware	Details
br210	AUTO-SIM	210-LTE-R2	Enabled	UMTS	AT&T	Excellent	nxtgenphone	CONNECTED	10.2.122.72	359075060212577	02.24.05.06_ATT	

Modem

Manufacturer: Sierra Wireless, Incorporated Model ID: EM7430 Firmware Revisions: SWI9X30C_02.24.05.06 r7040 CARMD-EV-FRMWR2.2017/05/19 06:23:09

Boot Revisions: SWI9X30C_02.24.05.06 r7040 CARMD-EV-FRMWR2.2017/05/19 06:23:09 PRI Revision: 9905178.001.004 Generic PRL Version: 1

PRL Preference: 0 IMSI: 310410090919083 ESN Number: 0

IMEI Number: 359075060212577 ICCID Number: 89014103270909190837 MEID Number: 35907506021257

Hardware Revision: 1.0 Modem State: READY

Cellular Network

Home Network: AT&T Roaming Status: Home Session State: CONNECTED

Data Bearer: CDMA 1XRTT Dormancy Status: Traffic Channel Active LU Reject Cause: 0

Card State: Present

RF Information

Radio Interface: UMTS Active Band Class: 84 Active Channel: 4385

Signal Strength: Excellent ECIO: 5 IO: 0

SINR: 0 RSRQ: 0

Profile

PDP Type: IPv4 Authentication: 0 Profile Name:

APN Name: nxtgenphone User Name: IP Address: 10.2.122.72

Primary DNS: 172.26.38.1 Secondary DNS: 255.255.255.255 Gateway Address: 10.2.122.73

Call Statistics

Call Status: CONNECTED Bytes Transferred: 10256352 Bytes Received: 0

Previous Next

For information about LTE REST API, navigate to the SD-WAN GUI and go to **Configuration > Appliance Settings > NITRO API**. Click **Download Nitro API Doc**.

Dashboard **Monitoring** **Configuration**

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

Configuration > Appliance Settings > **NITRO API**

CITRIX NetScaler SD-WAN NITRO API DOC

Single Region Deployment

Mar 01, 2018

Regions allow you to define a network hierarchy with distributed management. A Region must define a Regional Control Node (RCN) which will take over functions performed by the Network Control Node (MCN) for its Region. The MCN is the controller for the Default Region.

Static and Dynamic Virtual Paths are not permitted between Regions. Traffic between Regions is managed by RCNs.

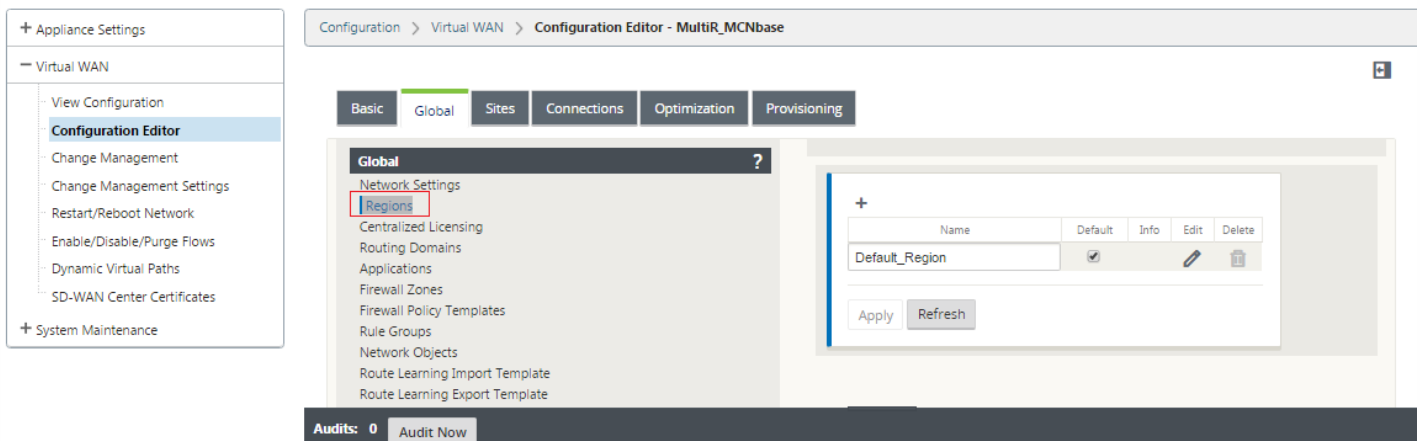
A single region deployment in an SD-WAN network can support network sites less than 550.

You can configure default region in the Configuration Editor of the SD-WAN appliance GUI. The Basic editor is useful to create only a small network with MCN and Client SD-WAN nodes. For configuring multi-region network with MCN, RCN, Clients or advanced features, you should use other configuration options in the configuration editor.

To configure single region deployment:

1. Navigate to the **Global** tab in the Configuration Editor. Select **Regions**. The default region configuration options are displayed.

You can change the name and description for the default region by editing it.



2. Edit the **Default_Region** to change the name and configure subnets.

3. Enable Interval VIP matching based on whether you want **Forced Internal VIP Matching** or **Allow External VIP Matching**.

- Forced Internal VIP: When enabled, all non-private Virtual IP addresses in the Region will be forced to match the configured subnets.

- Allowed External VIP - When enabled, non-private Virtual IP addresses from other regions will be allowed to match the configured subnets.

4. Click + to add subnets.

Edit

Name:

Default_Region

Description:

Force Internal VIP Matching

Allow External VIP Matching

Subnets +

Routing Domain	Network	Delete
Default_RoutingDomain ▾	*	

Apply

Cancel

5. Select a **Routing Domain**, enter the **Network** address. Click **Apply**. This is the IP address and mask for the subnet.

Multi Region Deployment

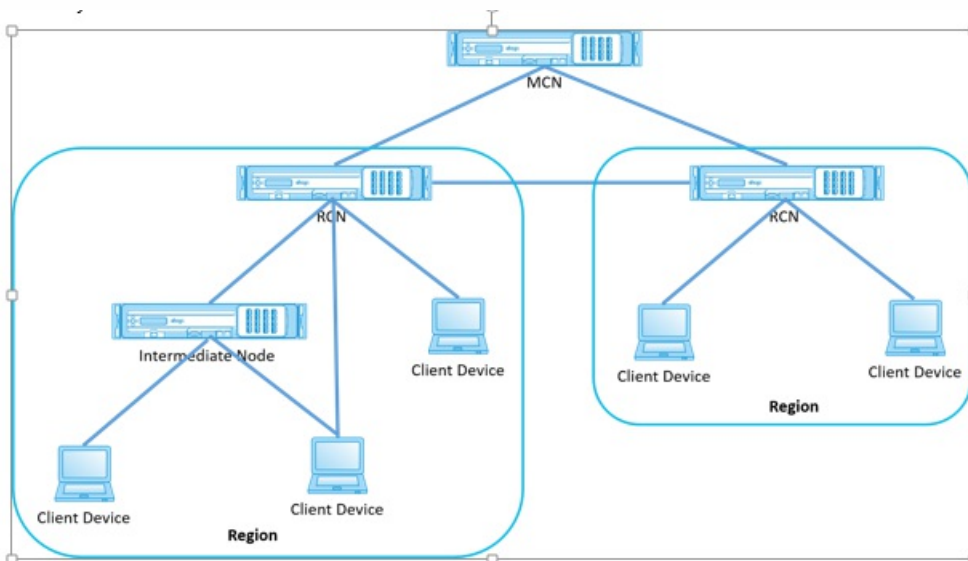
May 03, 2018

An SD-WAN appliance configured as Master Control Node (MCN) supports multi-region deployment. The MCN manages multiple Regional Control Nodes (RCNs). Each RCN, in turn, manages multiple client sites. The MCN can also be used to manage some of the client sites directly.

With MCN as the control node of the network and RCNs as the control nodes of the regions, SD-WAN can manage more than 2500 sites.

This enables you to fragment network into regions and set up a tiered network; such as branch (client) > RCN > MCN.

In NetScaler SD-WAN 10.0, an MCN with single region can be configured with maximum of 550 sites. You can keep the existing sites in the default region and add new regions with RCNs and their sites for multi-region deployment.



The table below provides list of platforms supported for configuring primary and secondary MCN/RCN.

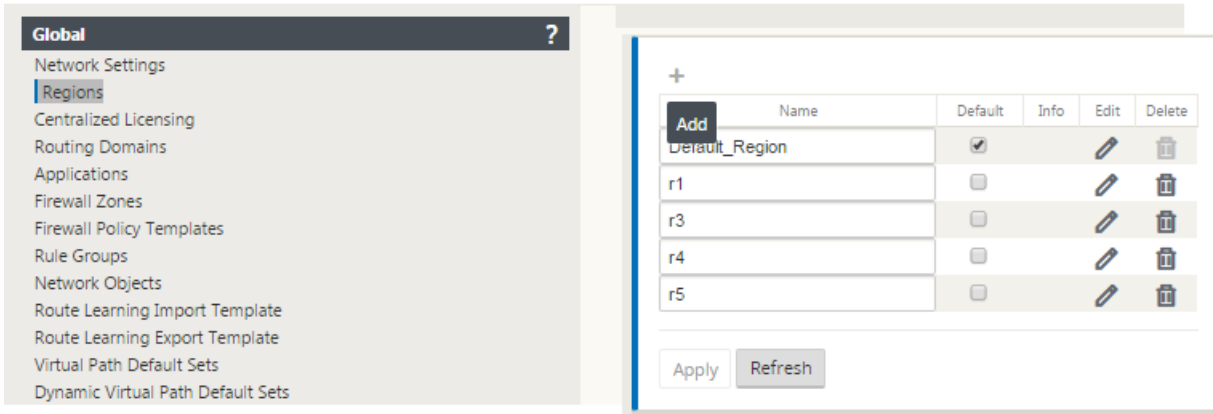
Platform Edition	Primary/Secondary MCN	Primary/Secondary RCN
210-SE	No	No
400-SE	Yes	No
410-SE	Yes	No
1000-SE, 1000-EE	Yes	No
VPX-SE, VPXL-SE	Yes	Yes
2000-SE, 2000-EE, 2100-SE, 2100-EE, 4000-SE, 4100-SE, 5100-SE	Yes	Yes

To configure multi-region deployment for an SD-WAN network:

1. Navigate to the **Global** tab in the Configuration Editor. Select **Regions**. The default region configuration options are displayed.

You can change the name and description for the default region by editing it.

2. Click **+ Add** to add a new region.



Add ? x

Name:

Description:

Force Internal VIP Matching

Allow External VIP Matching

Subnets +

2. Enter a Name and Description for the region.

3. Enable Interval VIP matching based on whether you want **Forced Internal VIP Matching** or **Allow External VIP Matching**.

- Forced Internal VIP: When enabled, all non-private Virtual IP addresses in the Region will be forced to match the configured subnets.

- Allowed External VIP - When enabled, non-private Virtual IP addresses from other regions will be allowed to match the configured subnets.

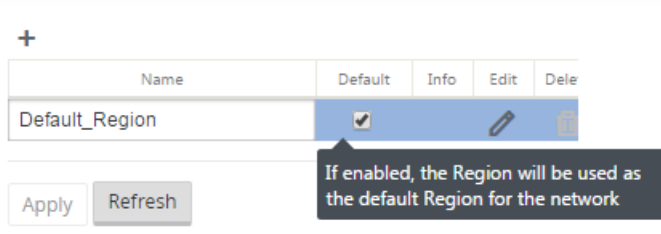
4. Click **+** to add subnets. Choose a routing domain.

Subnets +

Routing Domain	Network	Delete
<Default>	<input type="text" value="*"/>	
<Default>		
Default_RoutingDomain		
WCCP_RoutingDomain		

5. Enter a **Network** address. Click **Add**. This is the IP address and mask for the subnet. The newly created region is added to the existing list of regions.

You can select the **Default** checkbox to use a desired region as the Default.



Note

You can clone MCN to a GEO or client site.

SD-WAN Center supports multi-region deployment. For more information, see [SD-WAN Center Multi-Region Deployment and Reporting](#).

Change Management Summary View

When you perform Change Management process for appliances configured in multi-region deployment, the change management summary table is displayed in the SD-WAN appliance GUI.

The Region column displays a list of regions currently configured in the network. You can view change management summary for specific region by selecting it in the summary table.

Default Region Summary

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - Default_Region Details

Show entries Search

Customize Refresh ?

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 min		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
BR1-BR1-CBVPXL	CBVPXL	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
AMER-1RCN-5100-AMER-1RCN-5100	CB5100	Not Needed	Not Connected					Loc Chg Mgt	none / staged

Previous 1 Next

Region Summary

Global Multi-Region Summary

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - AMEA_r1 Details

Show entries Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
AMEA_r1_vpx01-AMEA_r1_vpx01	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx02-AMEA_r1_vpx02	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx03-AMEA_r1_vpx03	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx04-AMEA_r1_vpx04	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx05-AMEA_r1_vpx05	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx06-AMEA_r1_vpx06	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx07-AMEA_r1_vpx07	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx08-AMEA_r1_vpx08	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx13-AMEA_r1_vpx13	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx14-AMEA_r1_vpx14	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx15-AMEA_r1_vpx15	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx16-AMEA_r1_vpx16	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx17-AMEA_r1_vpx17	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx18-AMEA_r1_vpx18	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx19-AMEA_r1_vpx19	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx20-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx33-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx34-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx35-vpx35	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx36-vpx36	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx37-vpx37	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx38-vpx38	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx39-vpx39	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx40-vpx40	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx49-vpx49	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged

Previous Next

Note

In some instances, the **Total Sites** value displayed in the **Global Multi-Region Summary** table is less than the sum of the remaining columns. For example; when a branch node is not connected, it is possible that the branch is counted twice; once as “Not Connected” and once as “Preparing/Staging”.

Active Bandwidth Testing

Mar 01, 2018

Active Bandwidth Testing enables you the ability to issue an instant path bandwidth test through public internet WAN link, or to schedule public internet WAN link bandwidth testing to be completed at specific times on a recurring basis. This feature is useful for demonstrating how much bandwidth is available between two locations during new and existing installations, also for testing paths to determine the outcome of setting and confirmation changes, such as adjusting DSCP tag settings or bandwidth Permitted Rates.

To use the active bandwidth testing feature:

1. Navigate to **System Maintenance > Diagnostics > Path Bandwidth**.
2. Select the desired **Path** and click **Test**.

Dashboard Monitoring Configuration

Configuration > System Maintenance > Diagnostics

Ping Traceroute Packet Capture Path Bandwidth System Info Diagnostic Data Events Alarms Diagnostics Tool

Instant Path Bandwidth Testing

Path: MCN-5100-WL-2->BR572-1

Test

Results

Minimum Bandwidth: 936564 kbps
 Maximum Bandwidth: 1213863 kbps
 Average Bandwidth: 1189046 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	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 2:01:03 PM	2883972	5099707	4357330
2	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 4:01:03 PM	3109115	3872000	3616157
3	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 6:01:04 PM	3041280	4119960	3518949
4	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 8:01:04 PM	2769377	3700672	3276124
5	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 10:01:04 PM	409245	3574153	2489269
6	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:04 AM	2481756	4001684	3198214
7	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 AM	2549853	3872000	3236546
8	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 AM	3204413	3982628	3642643
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	2173340	3684370	2929146
15	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 PM	2613600	3589493	3021890
16	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:03 PM	1676056	3499380	2655280
17	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:03 PM	1954093	3558944	2975884
18	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 AM	2161116	3784398	2902088
19	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 AM	2986971	4079765	3821158
20	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:04 AM	3514084	4181760	3893381
21	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 6:01:03 AM	3358843	4059961	3756691
22	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 8:01:03 AM	3216738	4245441	3716351
23	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 10:01:04 AM	3558944	4202773	3932908
24	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 PM	3427672	4267102	3838552
25	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 PM	2874061	4224000	3608676
26	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:03 PM	2816000	6288360	4165337
27	MCN-5100-WL-2	BR572-WL-1	2/19/2018, 5:23:04 PM	936564	1213863	1109046

Showing 1 to 27 of 27 entries

The output displays average bandwidth used as value to set as the permitted rate for the WAN Link minimum and maximum bandwidth results of the test. Along with the ability to test the bandwidth, you can now change the configuration file to use the learned bandwidth. This is accomplished through the Auto Learn option is under **Site > [Site Name] > WAN Links > [WAN Link Name] > Settings** and if enabled, the system will use the learned bandwidth.

You can also schedule recurring tests of path bandwidth in weekly, daily, or hourly intervals.

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute	
DC_MPLS2->Branch_	every day	Sunday	0	0	X
	every day	Sunday	0	0	↶

Apply Settings

Note

A history of the path bandwidth testing results is displayed at the bottom of this page and results are archived every 7 days.

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute	

Apply Settings

History Path Bandwidth Testing Result

Show entries Showing 1 to 14 of 14 entries

First Previous 1 Next Last

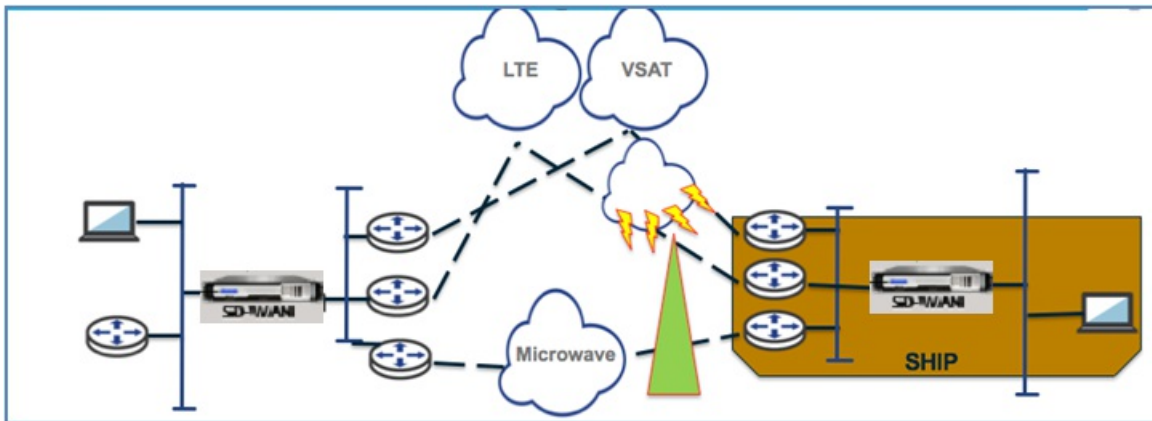
Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	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 Bandwidth Detection

Mar 01, 2018

This feature is applicable to networks with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, for which the available bandwidth varies based on weather and atmosphere conditions, location, and line of site obstructions. It allows the NetScaler SD-WAN appliances to adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth without marking the paths BAD.

- Greater bandwidth reliability (Over VSAT, Microwave, 3G/4G, and LTE)
- Greater predictability of adaptive bandwidth over user configured settings



To enable adaptive bandwidth detection:

This feature needs Bad loss sensitivity option to be enabled (default/custom) as a prerequisite. You can enable it under **Global > Autopath Groups > [Autopath Group Name] > Bad Loss Sensitive**.

1. Enable **Adaptive Bandwidth Detection** under **Global > Autopath Groups > [Autopath Group Name] > Bad Loss Sensitive**.
2. Navigate to **Configuration Editor > Sites > [Site Name] > WAN Links > [WAN Link Name] > Settings > Advanced Settings**.

View Region: Default_Region

View Site: BR572

WAN Link: BR572-WL-2 Section: Settings

Basic Settings

Advanced Settings

Provider ID: Frame Cost (bytes): 0

Congestion Threshold (μ s): 20000 MTU Size (bytes): 1500

Adaptive Bandwidth Detection

Minimum Acceptable Bandwidth (%): 30

This feature is for a WAN link whose bandwidth level has a wide variance. When loss is detected, we attempt to use the wan link at a reduced bandwidth rate first. When the available bandwidth is below the configured Minimum Acceptable Bandwidth, then we mark the path as bad. We recommend that custom bad loss sensitivity to be used under path or auto path group in conjunction with this feature.

For adaptive bandwidth detection, when available bandwidth is below this amount, paths will be marked bad. This is a percentage of WAN to LAN Permitted rate. The minimum kbps is different on each side of a virtual path. The value can be in the range 10%-50% and the default being 30%.

3. Check the **Adaptive Bandwidth Detection** box and enter a value in the **Minimum Acceptable Bandwidth** field.

4. View the **Usage and Permitted Rates** table by navigating to **Monitor > Statistics > WAN Link Usage > Usage and Permitted Rates**.

Usages and Permitted Rates

Filter: in **Any column**

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

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Recv	5437658	3467411.62	0	0	0	25	NO
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Send	7598365	559484464	118	8.39	12.69	5905	N/A
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Recv	58537274	41745181.34	6562	5203.86	7872.71	8105	NO
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Send	20640095	1497892080	229	17.25	26.1	5880	N/A

Showing 1 to 4 of 4 entries

DHCP Server and DHCP Relay

Mar 01, 2018

NetScaler SD-WAN introduces the ability to use Standard or Enterprise Edition appliances as either DHCP Servers or DHCP Relay agents. You can configure your appliance to issue IP addresses using DHCP or forward DHCP packets between clients and servers.

Note

- DHCP Server supports only IP Pool based address assignment
- DHCP Relay does not support multiple DHCP Server IP address assignment

See [DHCP Management](#) for more information.

How To Enable DHCP Server

NetScaler SD-WAN appliances can be configured as DHCP server that assigns and manages IP addresses from specified address pools within the network to DHCP clients. The DHCP server can be configured to assign additional parameters such as the IP address of the Domain Name System (DNS) server and the default router. DHCP server accepts address assignment requests and renewals. The DHCP server also accepts broadcasts from locally attached LAN segments or from DHCP requests that have been forwarded by other DHCP relay agents within the network.

To enable DHCP server:

1. Navigate to **Configuration > Appliance Settings > Network Adapters**. In the Network Adapters page, look for the Management Interface DHCP Server pane.
2. Click the **Enable DHCP Server** checkbox to start the server, then enter the **Lease Time** (in minutes), the **Domain Name**, and define the **IP Address** range by entering a **Start IP Address** and an **End IP Address**.

Note

The server IP address pool should be within the management network.

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:

3. Click the **Change Settings** button to finish configuring the DHCP Server.

Note

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

4. Click **Show Client** to view the current DHCP clients, and click **Clear Clients** to release the DHCP Client leases.

How To Enable DHCP Relay

A DHCP relay agent is a host or router that forwards DHCP packets between clients and servers. Network administrators can use the DHCP Relay service on the management port of the SD-WAN (Standard or Enterprise Editions) appliances to relay requests and replies between local DHCP Clients and a remote DHCP Server. This allows local hosts to acquire dynamic IP addresses from the remote DHCP Server. Relay agent receives DHCP messages and generates a new DHCP message to send out on another interface.

To enable DHCP relay service:

1. Navigate to **Configuration > Appliance Settings > Network Adapters**. In the Network Adapters page, look for the **Management Interface DHCP Relay** pane.
2. Click the **Enable DHCP Relay** checkbox to enable the service. Enter the **DHCP Server IP Address** and click the **Change Settings** button to begin using your appliance as a DHCP Relay Agent.

Note

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

Management Interface DHCP Relay

Enable DHCP Relay:

DHCP Server IP Address:

How To Monitor DHCP Client WAN Links

The runtime Virtual IP address, Subnet Mask, and Gateway settings are logged and archived in a log file called “*SDWANVW_ip_learned.log*”. Events are generated when Dynamic Virtual IPs are learned, released, or expired, and when there is a communication issue with the learned Gateway or DHCP server; or when duplicate IP addresses are detected in the archived log file. If duplicate IPs are detected at a site, Dynamic Virtual IP addresses are released and renewed until all Virtual Interfaces at the site obtain unique Virtual IP addresses.

To monitor DHCP client WAN links:

1. In the **Virtual WAN > Enable/Disable/Purge Flows** page, the DHCP Client WAN Links table provides the status of learned IPs.
2. You can request to renew the IP, which refreshes the lease time. You can also choose to **Release Renew**, which will issue a new IP address with a new lease.

DHCP Client WAN Links

Ethernet Interface	Virtual Interface	WAN Link	IP Address / Prefix	Gateway IP Address	Lease Duration Seconds	Remaining Seconds	Expiration Date	Action
X2	VLAN349	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew <input type="button" value="v"/> <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="v"/> <input type="button" value="Submit"/>

DHCP Management

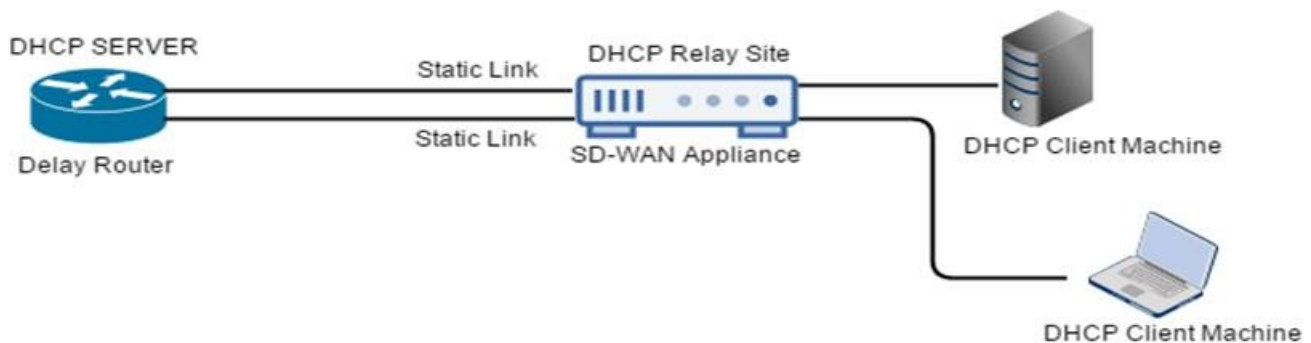
Jul 26, 2018

Devices on the same network as the SD-WAN appliance's LAN/WAN interface can now use the SD-WAN DHCP Relay & DHCP Server features to provide those devices with their IP configuration. These features help to simplify the client site network by reducing the amount of equipment necessary.

- Reduce equipment at client site
- Replace router at client site (Easy deployment of edge router services)
- Simplify the client site network
- Configuration of Router without CLI commands
- Use of Dynamic Host Configuration Protocol (DHCP) on Internet Protocol (IP) networks to request IP addresses and networking parameters automatically reducing manual configuration needs by network admin on simple client sites

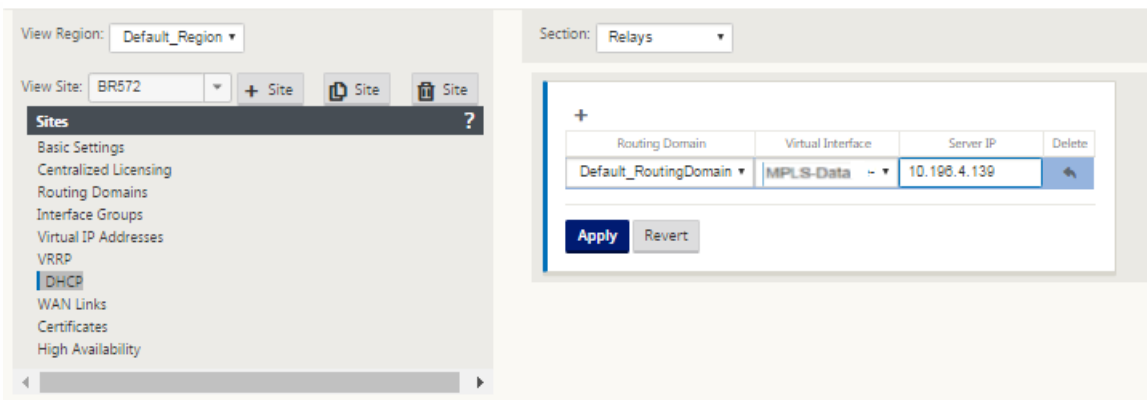
DHCP Relay

Network administrators can now use the DHCP Relay service of the SD-WAN appliance to relay requests and replies between local DHCP clients and a remote DHCP Server. This allows local hosts to acquire dynamic IP addresses from the remote DHCP Server.



To configure DHCP Relay:

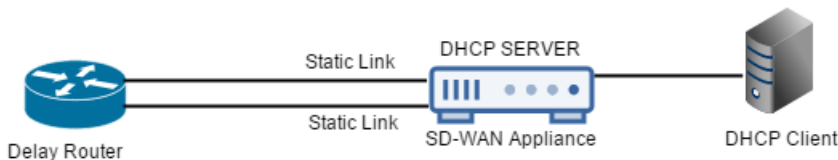
1. In the SD-WAN web management interface, navigate to **Configuration Editor > Sites > [Site Name] > DHCP > Relays**. Expand Relays, and then specify the server IP address.
2. Select the **Virtual Interface** to be used.
3. Configure a static route to reach the DHCP Server.



Important

You can configure multiple DHCP servers as a DHCP relay.

DHCP Server

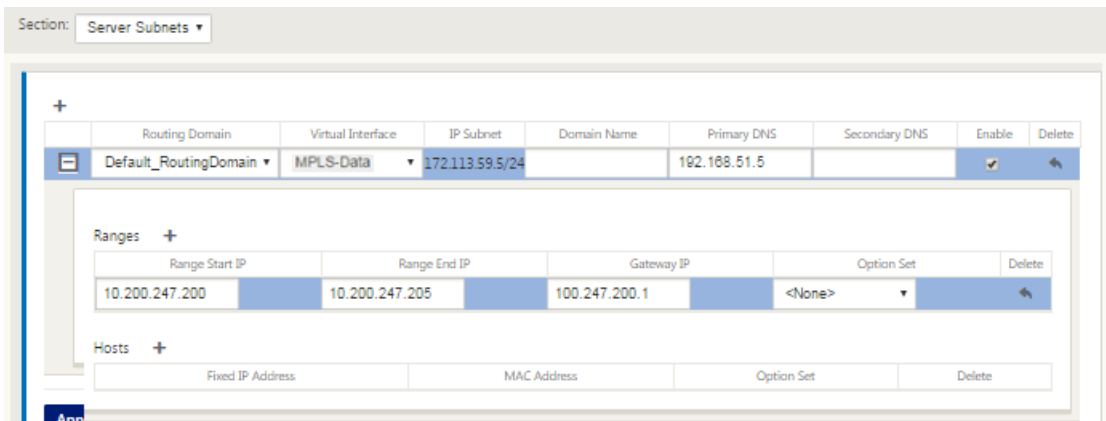


Network administrators can use the DHCP Server feature on data ports of an SD-WAN appliance to allow local hosts to acquire dynamic or static IP addressing directly from the SD-WAN appliance.

To configure DHCP Server:

1. In the SD-WAN web management interface, navigate to **Configuration Editor > Sites > [Site Name] > DHCP > Server Subnets**.
2. Select the Virtual Interface to be used and specify the range of IP addresses allowed to be dynamically assigned to local hosts.
3. Optionally, specify settings for configuring the hosts, such as gateway IP address, DNS address, and an Option Set (described below).

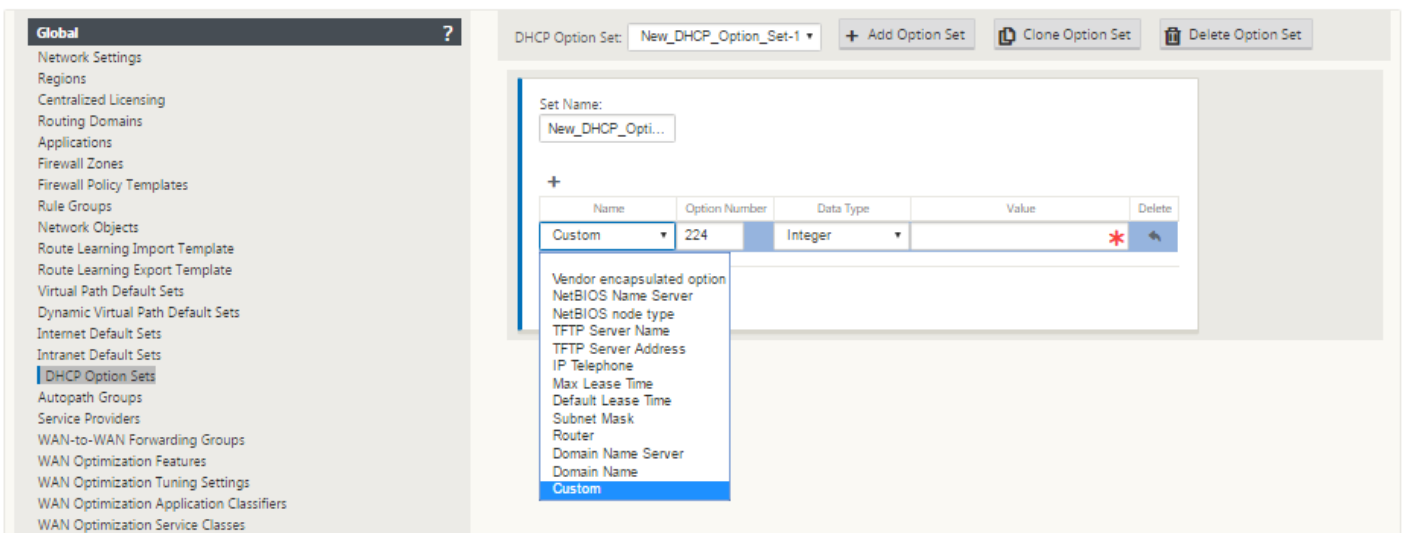
The Hosts option of this drop-down gives users an option to manually associate specific IP addresses with specific hosts through the host MAC addresses.



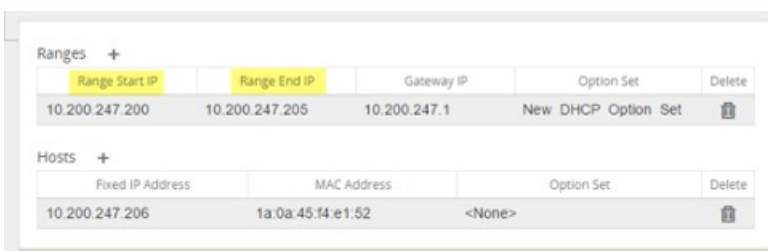
Note

The following feature is optional, not required.

DHCP Option Sets are groups of DHCP settings that can be applied to individual IP address ranges. To create DHCP Option Sets, navigate to the **Global** section of the configuration and expand **DHCP Options Sets**. Enter the settings that you would like to include in the set, and then click **Apply**.



Your DHCP Option Set must then be assigned to a DHCP range. Do this in the Sites section where the IP address range was defined. The DHCP Option Set defined globally takes precedence over local configuration for some parameters configured for the DHCP Server pool.



To view a list of Clients from the DHCP Server Database, in the web management interface, navigate to **Monitor > DHCP Server/Relay**.

Show DHCP Server Client Database ✕						
Routing Domain	Client IP Address	Lease Start Time	Lease End Time	Client MAC Address	Client Hostname	State
Default_RoutingDomain	10.200.247.200	Mon Jul 11 15:23:23 2016	Mon Jul 11 15:29:23 2016	3a:1a:dc:67:ca:b4	TexasF_Angelina2_TN	active

Close

DHCP Client for Data Port

Mar 01, 2018

NetScaler SD-WAN appliances support WAN Link IP address learning through DHCP Clients. This functionality reduces the amount of manual configuration to deploy SD-WAN appliances and reduces ISP costs by eliminating the need to purchase static IP addresses. SD-WAN appliances can obtain dynamic IP addresses for WAN Links on untrusted interfaces eliminating the need for an intermediary WAN router to perform this function.

Note

- DHCP Client can only be configured for untrusted non-bridged interfaces configured as Client Nodes.
- DHCP Client for Data Port can be enabled only on non-MCN sites.
- One-Arm or Policy Based Routing (PBR) deployment is not supported on the site with DHCP Client configuration.
- DHCP events are logged from the client's perspective only and no DHCP server logs are generated.

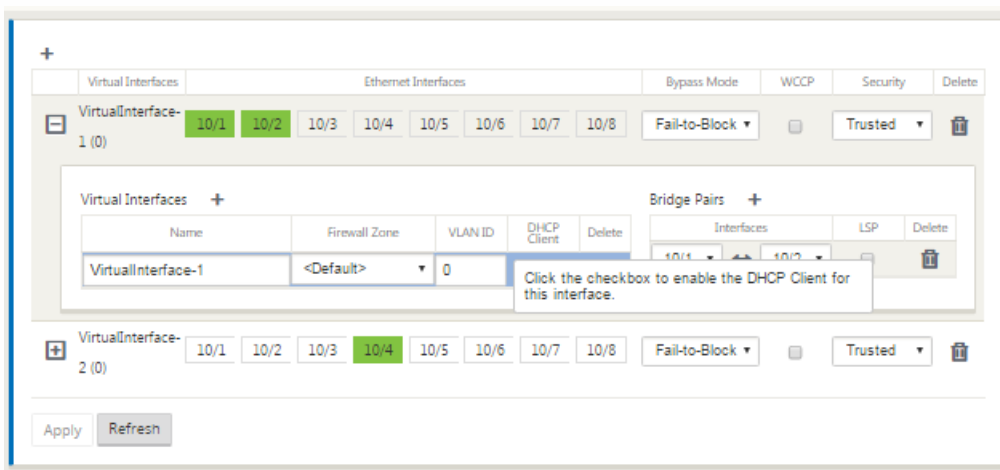
How To Configure DHCP Client

To configure DHCP for an untrusted virtual interface:

1. In the **Configuration Editor**, go to **Sites > [Site Name] > Interface Groups > Virtual Interfaces**.

Note

The physical interface in the interface group should be a non-bridged pair on a single interface.



2. Navigate to **WAN Links → [WAN Link Name] → Settings → Basic Settings**.

3. Click the **Autodetect Public IP** checkbox to enable the MCN to detect the Public IP Address used by the Client. This is required when DHCP Client mode is configured for the WAN Link.

View Region: Default_Region | WAN Link: BR571-WL-1 | Section: Settings | + Add Link | Delete Link

View Site: BR571 | + Site | Site | Site

Sites ?

- Basic Settings
- Centralized Licensing
- Routing Domains
- Interface Groups
- Virtual IP Addresses
- VRRP
- DHCP
- WAN Links**
- Certificates
- High Availability

Basic Settings ?

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

Link Name:

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

LAN to WAN

Physical Rate (kbps):

Set Permitted From Physical | Auto Learn

Permitted Rate (kbps):

WAN to LAN

Physical Rate (kbps):

Set Permitted From Physical | Auto Learn

Permitted Rate (kbps):

Tracking IP Address:

Autodetect Public IP

Click the checkbox to enable the MCN to detect the Public IP Address used by the Client (required when DHCP Client mode is configured for the WAN Link)

GRE Tunnel

Mar 01, 2018

The SD-WAN GRE Tunnel settings enable you to configure SD-WAN Appliances to terminate GRE tunnels on the LAN. If you do not want to configure site as a GRE Tunnel termination node, you can skip this step, and proceed to the section, [Configuring the WAN Links for the MCN Site](#).

To configure a GRE Tunnel, do the following:

1. Continuing in the **Sites** view for the new MCN site, click **+** to the left of the **GRE Tunnels** label.

This opens the **GRE Tunnels** table for the new site.

Configure GRE Tunnels for the MCN Site (Optional)

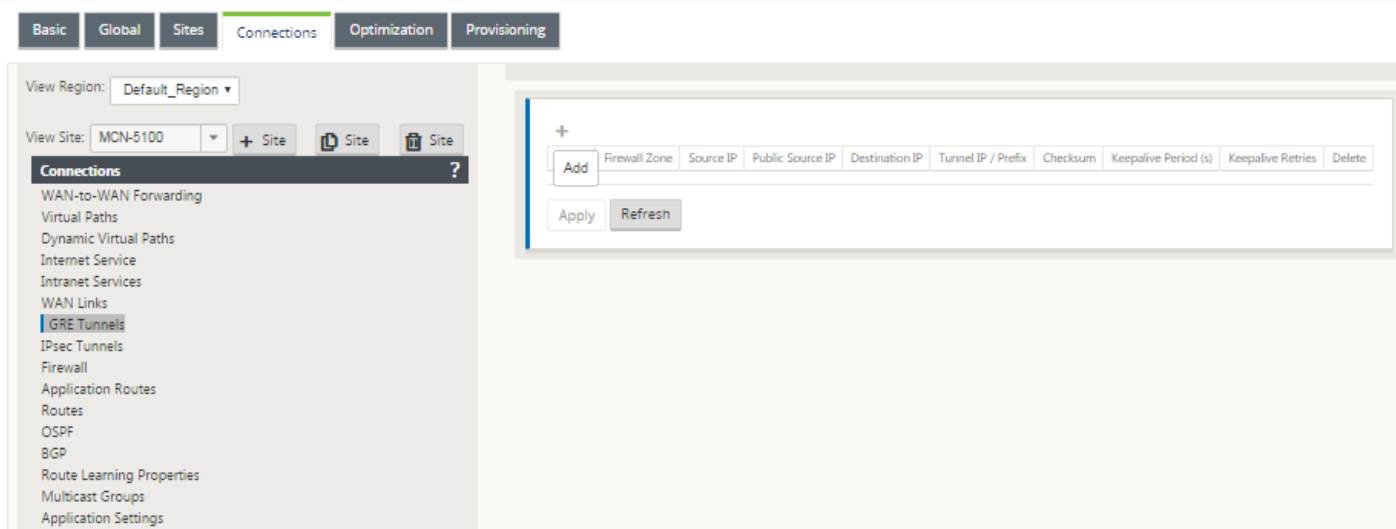
Mar 01, 2018

The SD-WAN GRE Tunnels settings enable you to configure SD-WAN Appliances to terminate GRE tunnels on the LAN. If you do not want to configure this site as a GRE Tunnel termination node, you can skip this step, and proceed to the section, [Configuring the WAN Links for the MCN Site](#).

To configure a GRE Tunnel, do the following:

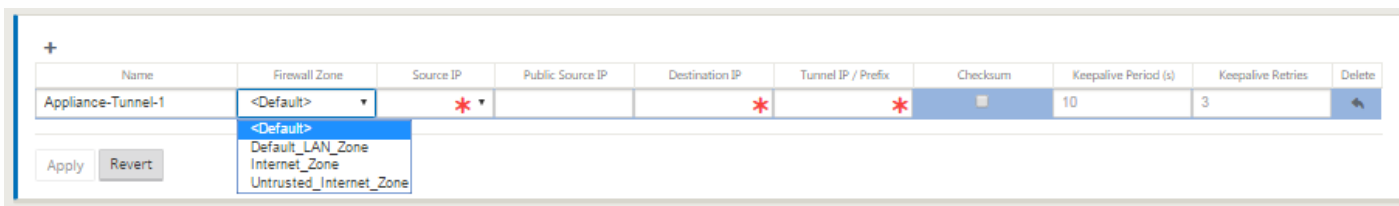
1. Continuing in the connections tab for the new MCN site, click **GRE Tunnels**.

This opens the **GRE Tunnels** table for the new site.



2. Click **+** to the right of the **GRE Tunnels**.

This adds a new blank GRE Tunnel entry to the table and opens it for editing.



3. Configure the GRE Tunnel settings.

Enter the following:

- **Name** – Enter a name for the new GRE tunnel, or accept the default. The default uses the following naming format:

*Appliance-Tunnel-**<number>***

Where **<number>** is the number of GRE Tunnels configured for this site, incremented by one.

- **Firewall Zone** - Select the file zone for the GRE tunnel to you.

- **Source IP** – Select a source IP Address for the tunnel from the drop-down menu for this field. The menu options will be the list of Virtual Interfaces configured for this site. You must configure at least one Virtual Interface before you can configure a GRE Tunnel. For instructions, see [Configuring the Virtual Interface Groups for the MCN Site](#) and [Configuring the Virtual IP Addresses for the MCN Site](#).

- **Public Source IP**: Enter the public source IP Address for the tunnel.

- **Destination IP** – Enter the destination IP Address for the tunnel.

- **Tunnel IP / Prefix** – Enter the tunnel IP Address and prefix.

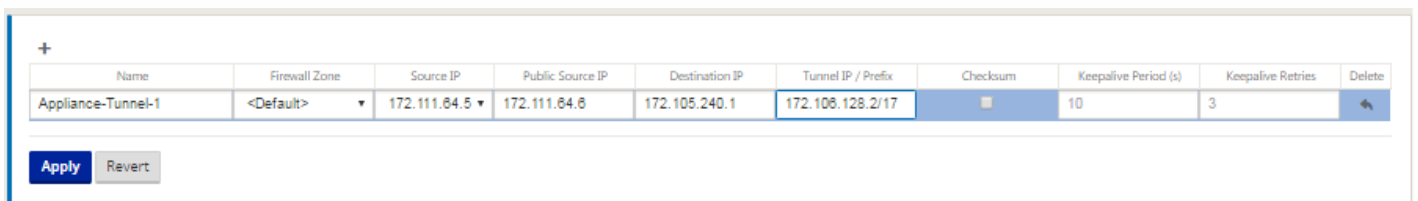
- **Checksum** – Select this to enable Checksum for the tunnel GRE header.

- **Keepalive Period(s)** – Enter the wait time interval (in seconds) between keepalive messages. If configured to 0, no keepalive packets will be sent, but the tunnel will remain up. The default is 10.

- **Keepalive Retries** – Enter the number of keepalive retries the Virtual WAN Appliance should attempt before it brings down the tunnel. The default is 3.

4. Click **Apply**.

This submits your settings and adds the new GRE Tunnel to the table.



Name	Firewall Zone	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	<Default>	172.111.84.5	172.111.84.8	172.105.240.1	172.108.128.2/17	<input checked="" type="checkbox"/>	10	3	

Apply

5. To configure additional GRE Tunnels, click **+** to the right of the **GRE Tunnels**, and proceed as above.

The next step is to configure the [WAN links for the MCN site](#).

Configure GRE Tunnels for a Branch Site

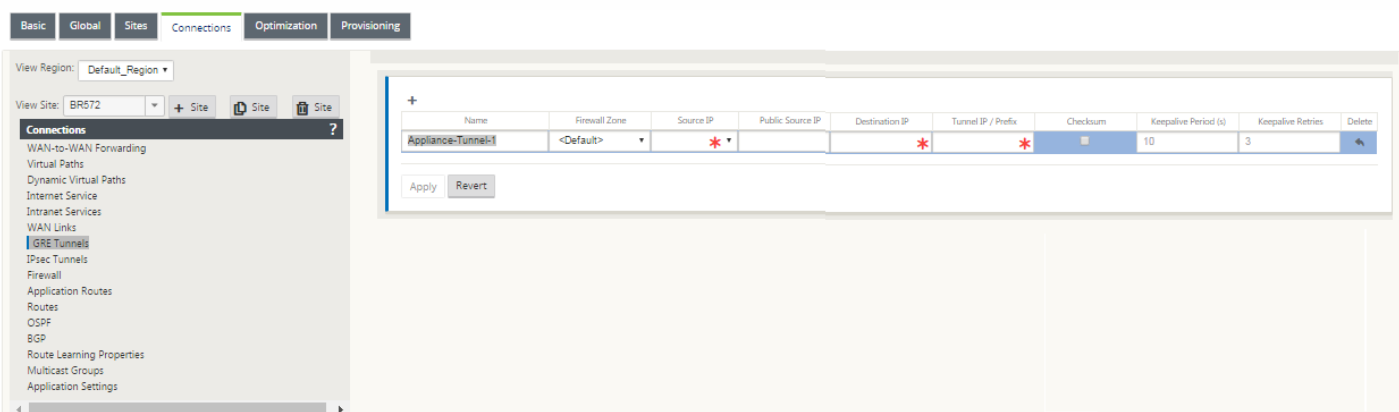
Mar 01, 2018

The Virtual WAN LAN GRE Tunnels settings enable you to configure Virtual WAN Appliances to terminate GRE tunnels on the LAN. If you do not want to configure this branch site as a LAN GRE Tunnel termination node, you can skip this step, and proceed to the section, [Configuring WAN Links for the Branch Site](#).

To configure a LAN GRE Tunnel for the branch site, do the following:

1. Continuing in the connections view for the new branch site, click **GRE Tunnels**. This opens the **GRE Tunnels** view for the new site.
2. Click **+** to the right of the **GRE Tunnels**.

This adds a new blank GRE Tunnel entry to the table and opens it for editing.



3. Configure the GRE Tunnel settings.

Enter the following:

- **Name** – Enter a name for the new GRE tunnel, or accept the default. The default uses the following naming format:

*Appliance-Tunnel-**<number>***

Where **<number>** is the number of GRE Tunnels configured for this site, incremented by one.

- **Firewall Zone** - Select a firewall zone for the GRE tunnel.

- **Source IP** – Select a Source IP Address for the tunnel from the drop-down menu for this field. The menu options will be the list of Virtual IP Addresses that you configured for this site. You must configure at least one Virtual Interface and one Virtual IP Address before you can configure a LAN GRE Tunnel. For instructions, see the sections, [Configuring the Virtual Interface Groups for the Branch Site](#) and [Configuring the Virtual IP Addresses for the Branch Site](#).

- **Public Source IP** - Enter the public source IP Address for the tunnel.

- **Destination IP** – Enter the destination IP Address for the tunnel.

- **Tunnel IP / Prefix** – Enter the tunnel IP Address and prefix.

- **Checksum** – Select this to enable Checksum for the tunnel GRE header.
- **Keepalive Period(s)** – Enter the wait time interval (in seconds) between keepalive messages. If configured to 0, no keepalive packets will be sent, but the tunnel will remain up. The default is 10.
- **Keepalive Retries** – Enter the number of keepalive retries the Virtual WAN Appliance should attempt before it brings down the tunnel. The default is 3.

4. Click **Apply**. This submits your settings and adds the new GRE Tunnel entry to the table.

Name	Firewall Zone	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	Default_LAN_Zo ▾	192.113.59.5 ▾	192.113.59.6	10.199.81.237	10.199.106.2/20	<input checked="" type="checkbox"/>	10	3	

Apply Revert

5. To configure additional GRE Tunnels, click **+** to the right of the **GRE Tunnels** label, and proceed as above.

The next step is to configure the [WAN links for the branch site](#).

Internet Access

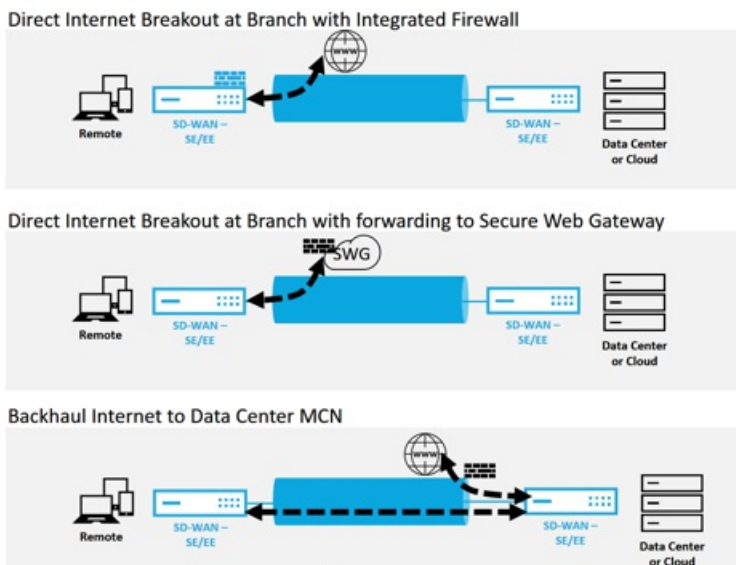
Mar 01, 2018

The Internet Service is used for traffic between an end-user site and sites on the public internet. Internet service traffic is not encapsulated by NetScaler SD-WAN and does not have the same capabilities as traffic that is delivered across the Virtual Path Service. However, it is important to classify and take account for this traffic on the NetScaler SD-WAN. Traffic that is identified as Internet Service enables the added ability of SD-WAN being able to actively manage WAN link bandwidth by rate-limiting Internet traffic relative to traffic delivered across the Virtual Path and Intranet traffic per the configuration established by the administrator. In addition to bandwidth provisioning capabilities, SD-WAN has the added capability to load balance traffic delivered across the Internet Service making use of multiple Internet WAN links, or optionally, utilizing the Internet WAN links in a primary or secondary configuration.

Internet traffic control using the Internet Service on NetScaler SD-WAN can be configured in the following deployment modes:

- Direct Internet Breakout at Branch with Integrated Firewall
- Direct Internet Breakout at Branch forwarding to Secure Web Gateway
- Backhaul Internet to Data Center MCN

Internet Traffic Control

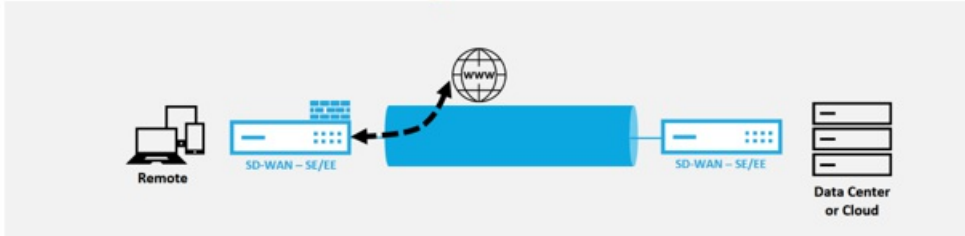


DIA with Integrated Firewall

Mar 01, 2018

Direct Internet Breakout at Branch with Integrated Firewall

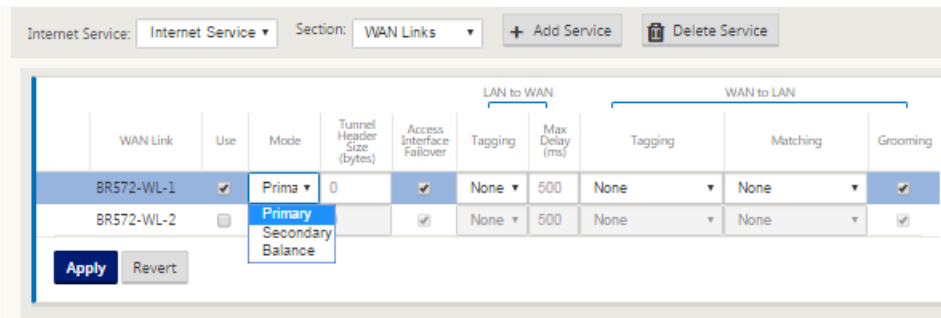
Direct Internet Breakout at Branch with Integrated Firewall



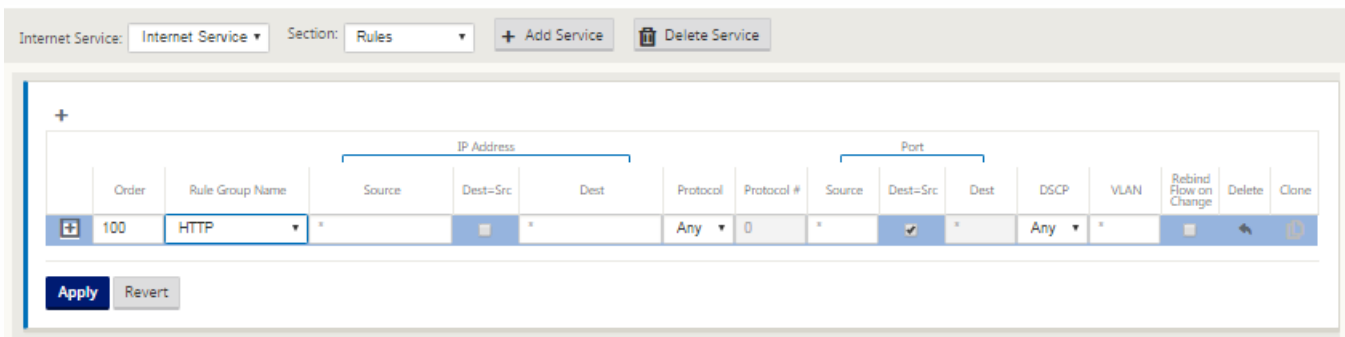
Perform the following steps to enable Internet Service for any site (Client node or MCN):

1. In the **Configuration Editor**, navigate to the **Connections** tile. Click the add (+) icon to add an Internet Service for that site. Only one Internet Service can be created per site.
2. In the **Basic Settings** for the Internet Service, there are several options on how you want the Internet Service to behave during unavailability of WAN links. An Internet Default Set can be defined in the Global tile with a set of Rules that can be applied to any node in the configuration which has Internet Service enabled, giving central control for Internet Service management without having to configure each node separately.

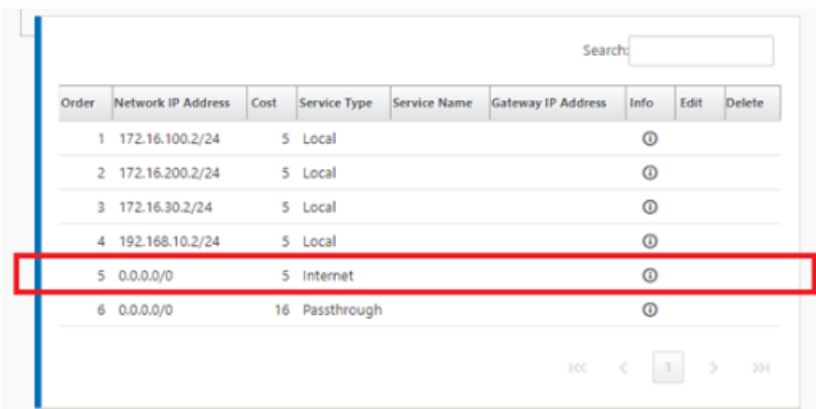
3. In the Internet Service WAN Links node, the WAN links built in the Site tile are made available to select which WAN link you would like to use for Internet traffic. In addition to other options, the Modes available are Primary, Secondary and Balanced, allowing the admin to use the available WAN links simultaneously or in an active/passive role.



4. Site node specific Rules are available, enabling the capability of customization of each site uniquely overriding any general settings configured in the global default set. Modes include desired delivery over a specific WAN link, or as an Override Service allowing for passthrough or discard of the filtered traffic.



As an Internet Service is created for a node, the Route table for that particular node is automatically updated with a 0.0.0.0/0 route for Service Type equal Internet and a Route cost of 5, otherwise the default route with cost 16 with Passthrough as the Service Type would be enacted and Internet traffic would be handed off to the underlay network to route.



With Internet Service being enabled for a site node, the Provisioning tile is made available to allow for the bidirectional (LAN to WAN / WAN to LAN) distribution of bandwidth for a WAN link among the various services utilizing the WAN link. The Services section allows for users to further fine-tune bandwidth allocation. In addition, fair share can be enabled, allowing for all services to receive their minimum reserved bandwidth before fair distribution is enacted.

Filter by Group: LAN to WAN Permitted Rate (kbps): 6000 WAN to LAN Permitted Rate (kbps): 6000
 <ALL>

Name	Group	LAN to WAN				WAN to LAN			
		Min (kbps)	Max (kbps)	Shares of Group	Fair (kbps)	Min (kbps)	Max (kbps)	Shares of Group	Fair (kbps)
DC	Default	80	no limit	1000	2990	80	no limit	1000	2990
Internet	Default	100	no limit	1000	3010	100	no limit	1000	3010
Totals:		180	0	2000	6000	180	0	2000	6000

The Internet Service can be utilized in the various deployment modes supported by NetScaler SD-WAN.

- Inline Deployment Mode (SD-WAN Overlay)

NetScaler SD-WAN can be deployed as an overlay solution in any network. As an overlay solution, SD-WAN generally is deployed behind existing edge routers and/or firewalls. If SD-WAN is deployed behind a network firewall, the interface can be configured as trusted and Internet traffic can be delivered to the firewall as an internet gateway.

- Edge or Gateway Mode

NetScaler SD-WAN can be deployed as the edge device, replacing existing edge router and/or firewall devices. Onboard firewall feature allows SD-WAN to protect the network from direct internet connectivity. In this mode, the interface connected to the public internet link is configured as untrusted, forcing encryption to be enabled, and firewall and Dynamic NAT features are enabled to secure the network.

DIA with Secure Web Gateway

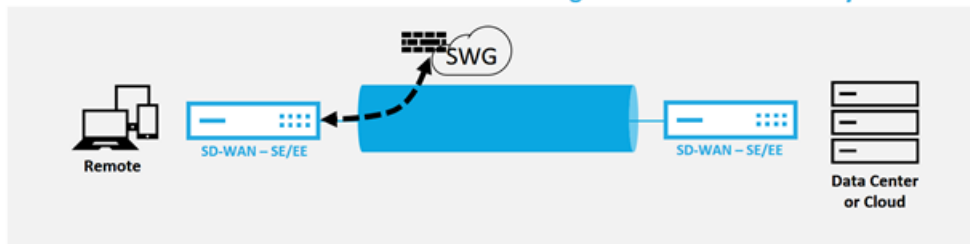
Jun 12, 2018

To secure traffic and enforce policies, enterprises often use MPLS links to backhaul branch traffic to the corporate data center. The data center applies security policies, filters traffic through security appliances to detect malware, and routes the traffic through an ISP. Such backhauling over private MPLS links is expensive. It also results in significant latency, which creates a poor user experience at the branch site. There is also a risk that users will bypass your security controls.

An alternative to backhauling is to add security appliances at the branch. However, the cost and complexity increases as you install multiple appliances to maintain consistent policies across the sites. Most significantly, if you have a large number of branch offices, cost management becomes impractical.

One alternative is to enforce security without adding cost, complexity, or latency would be to route all branch Internet traffic utilizing NetScaler SD-WAN to the to a Secure Web Gateway service. A third-party secure web gateway service enables granular and central security policy creation to be utilizing by all connected networks. The policies are applied consistently whether the user is at the data center or a branch site. Because secure web gateway solutions are cloud based, you don't have to add additional costly security appliances to the network.

Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



NetScaler SD-WAN supports the following secure web gateway solutions:

- [Zscaler](#)
- [Foreceptpoint](#)

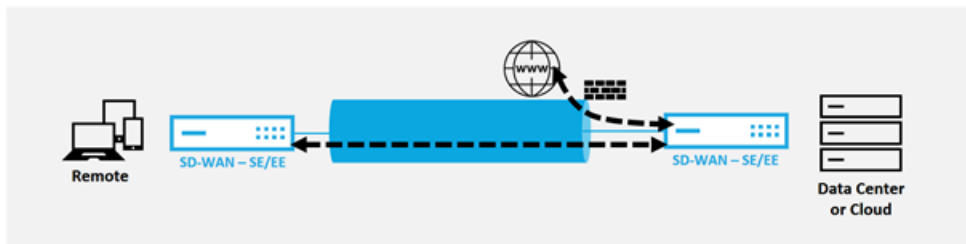
Backhaul Internet

Mar 01, 2018

The NetScaler SD-WAN solution provides the ability to backhaul Internet traffic to the MCN site or other NetScaler SD-WAN client-node sites for access to the Internet. The term “backhaul” indicates traffic destined for the Internet will be sent back to another predefined site which has access to the Internet via a WAN link. This may be the case for networks that do not allow Internet access directly at a branch office because of security concerns, or due to the underlay networks topology. An example would be a remote site that lacks an external firewall where the on-board NetScaler SD-WAN firewall does not meet the security requirements for that site. For some environments, backhauling all remote site internet traffic through the hardened DMZ at the Data Center may be the most desired approach to providing Internet access to users at remote offices. This approach does however have its limitations to be aware of following and the underlay WAN links size appropriately.

- Backhaul of internet traffic adds latency to internet connectivity and is variable depending on the distance of the branch site with respect to the data center
- Backhaul of internet traffic will consume bandwidth on the Virtual Path and should be accounted for in sizing of WAN links
- Backhaul of internet traffic may over-subscribe the Internet WAN link at the Data Center

Backhaul Internet to Data Center MCN



All NetScaler SD-WAN devices can terminate up to 8 distinct Internet WAN links into a single device. Licensed throughput capabilities for the aggregated WAN links are listed per respective appliance on the NetScaler SD-WAN datasheet.

The NetScaler SD-WAN solution supports the backhaul of internet traffic with the following configuration.

1. Enable Internet Service at the MCN site node, or any other site node where Internet Service is desired.

WAN Link	Use	Mode	Tunnel Header Size (Bytes)	Access Interface Failover	LAN to WAN		WAN to LAN		
					Tagging	Max Delay (ms)	Tagging	Matching	Grooming
DC-INET	<input checked="" type="checkbox"/>	Primary	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>
DC-MPLS	<input type="checkbox"/>	Primary	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>

2. On the branch nodes where internet traffic will be backhauled, manually add a 0.0.0.0/0 route to default all default traffic to the Virtual Path Service with the next hop denoted as the MCN, or intermediary site.

Add Route ?

Network IP Address: Cost: Service Type: Gateway IP Address:

Next Hop Site:

Eligibility Based On Path

Path:

3. Verify that the route table of the branch site does not have any other lower cost routes that would steer traffic other than the desired backhaul route through the Virtual Path.

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	172.16.100.2/24	5	Local					
2	172.16.30.2/24	5	Local					
3	192.168.10.2/24	5	Local					
4	0.0.0.0/0	5	Virtual Path	DC				
5	0.0.0.0/0	16	Passthrough					

<<< < 1 > >>>

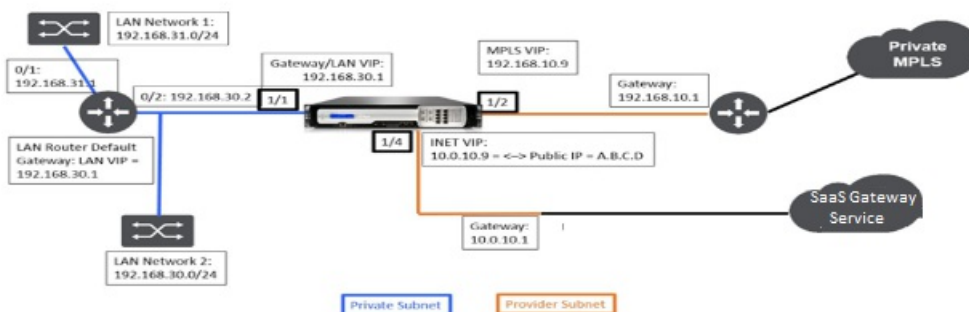
Citrix SaaS Gateway Service

Jun 04, 2018

Note

The Citrix SaaS Gateway Service is currently available as a "Technical Preview" feature only. For more information, please consult the Citrix Sales team.

The Citrix SD-WAN SaaS Gateway Service delivers SD-WAN functionalities as a service through reliable and secure delivery for all internet-bound traffic regardless of the host environment (data center, cloud, and internet). This improves network visibility and management. It enables partners to offer managed SD-WAN services for business critical SaaS applications to their end customers.



Citrix SaaS Gateway Service Workflow

Before you begin to use the SaaS Gateway Service, ensure that the following steps are completed:

1. Have a 410-SE platform edition appliance with SD-WAN release version 9.3.3 or higher.
2. Perform the [single step upgrade](#) procedure to install the software version that supports SaaS Gateway Service.
3. Configure MCN appliance and setup 410-SE branch appliance:
 - a. Enable SaaS Gateway Service in the 410-SE appliance SD-WAN GUI.
 - b. Perform change management process on the MCN appliance:
 - Create Intranet Service or use existing Intranet Service. It is recommended to configure two WAN links, with one as primary and other as secondary.
 - Create Application object for application based routes.
 - Create Application routes or IP based routes for a selected SaaS application.

Site Configuration

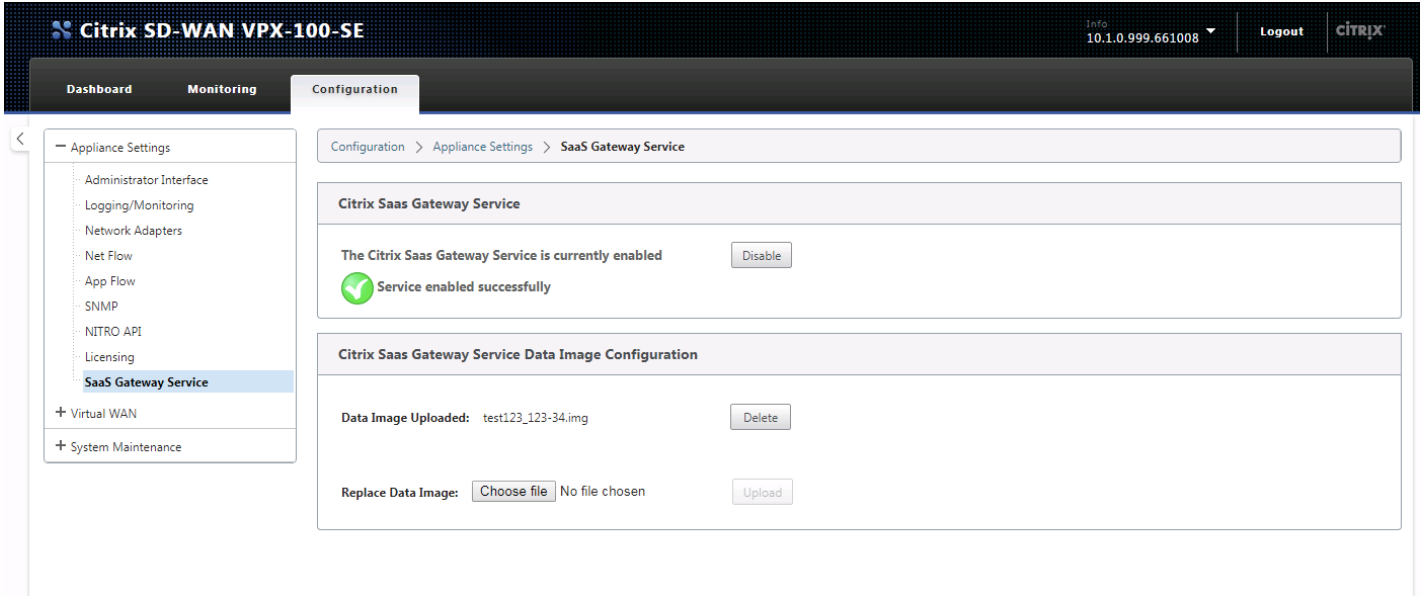
Configure the MCN and branch (410-SE) site appliances.

- **Primary MCN:** The primary Master Control Node of the SD-WAN network. The MCN is responsible for managing the SD-WAN configurations and software versions for all the clients and serves as a mediator between clients.

- **Client:** A client receives its appliance configuration from an MCN and participates in the SD-WAN network as described by the Configuration.

To configure 410-SE appliance to use Citrix SaaS Gateway Service:

1. In the SD-WAN GUI, navigate to **Configuration > Appliance Settings > SaaS Gateway Service**. Click **Enable**.

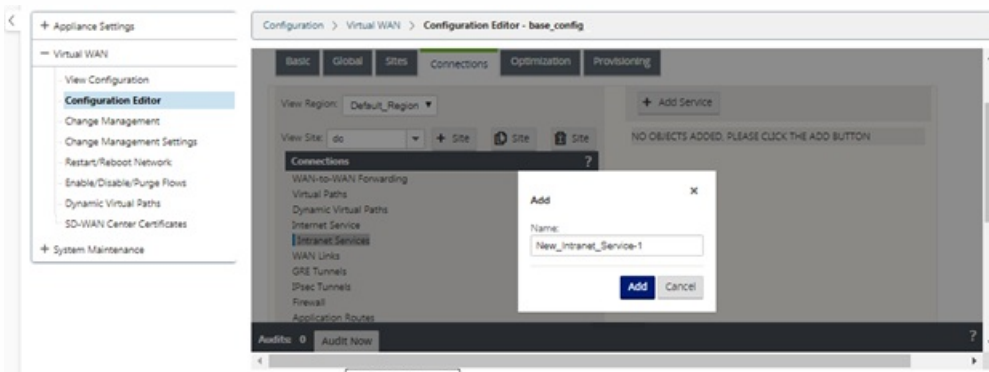


2. On the MCN appliance, navigate to **Configuration > Virtual WAN > Configuration Editor**. The Basic tab page is displayed.

3. Select the Site for which you want to configure Intranet Service. Click the **Connections** tab. Complete Intranet Service configuration.

Configure Intranet Service and WAN Links

1. Navigate to **Intranet Services**. Click **Add Service**. Type a name for the intranet service and click **Add**.



2. Select a **Firewall Zone** and click **Apply**.

Name:

Firewall Zone:

Enable Primary Reclaim

Default Set:

Ignore WAN Link Status

3. Go to **WAN Links**. Configure one or two WAN links, and click **Apply**. See Configure [WAN Links](#) for branch site, for more information.

Intranet Service: Section:

Basic Settings

WAN Links

Rules

WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Failover	Tag	Tagging	Matching	Grooming
dc-WL-	<input checked="" type="checkbox"/>	Prim	0	<input checked="" type="checkbox"/>	None	500	None	<input checked="" type="checkbox"/>

Configure Application Objects and Application Routes

To configure application objects and routes; go to **Global > Applications**. Select **Application Objects** and configure applications to be directed using the SaaS Gateway Service.

See [Application Routes](#), for more information about configuring Application objects and routes.

Basic Global Sites Connections Optimization Provisioning

Global ? Section:

Network Settings

Regions

Centralized Licenses

Routing Domains

Applications

Firewall Zones

Firewall Policy Templates

Rule Groups

Network Objects

Route Learning Intents

Route Learning Exclusions

Virtual Path Defaults

Dynamic Virtual Paths

Internet Default Settings

Intranet Default Settings

Audits:

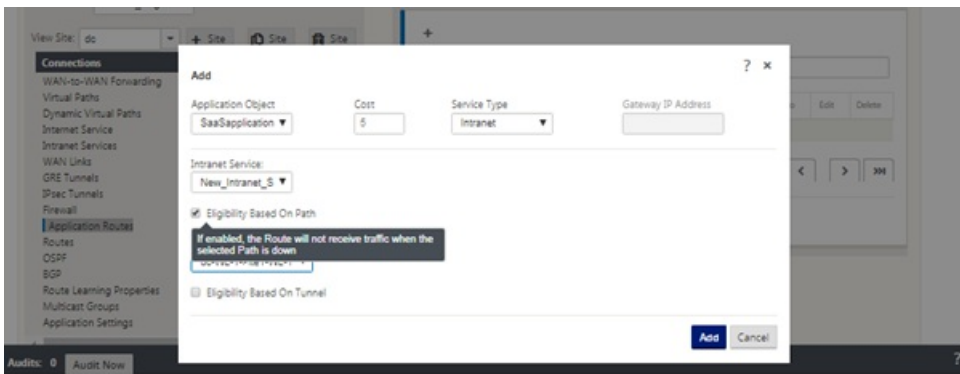
Edit ? x

Name: Priority: Enable Reporting

Application Match Criteria +

Match Type	Application Family	Application	Protocol	Network IP Address 1
Application			Any	*

To configure Application Routes, go to **Connections > Application Routes**. Add required application routes.



Configuration Deployment

After adding and configuring sites with Intranet service and application routes, you can push the configuration files to the site appliances by performing **Change Management**.

Ensure that all the site appliances are powered on and connected.

To deploy configuration:

1. Navigate to **Configuration > Virtual WAN > Change Management**. Begin the change management procedure to deploy Citrix SaaS Gateway Service enabled SD-WAN Intranet Service configuration to the branch site appliances, and the SD-WAN Center management dashboard.
2. After successful deployment, the SD-WAN GUI dashboard for the site appliance displays the Citrix SaaS Gateway Service configuration.

Link State Propagation

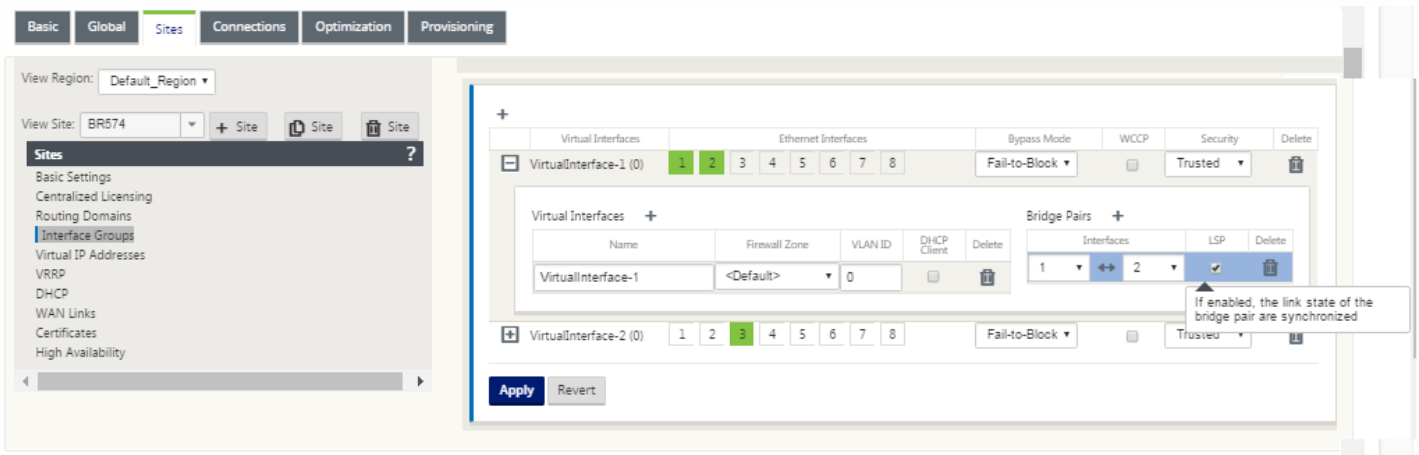
Mar 01, 2018

Link State Propagation feature allows network administrators to keep the link state of a bypass pair synchronized allowing attached devices on the other side of the link to view when links are inactive. When one port of a bypass pair becomes inactive, the coupled link is de-activated administratively. If your network architecture includes a parallel failover network, this forces traffic to transition to that network. Once the disrupted link is restored, its corresponding link will automatically become active.

How To Configure Link State Propagation

To configure Link State Propagation:

1. Navigate to **Configuration Editor > Sites > [Site Name] > Interface Groups**.
2. Expand **Virtual Interfaces** and under **Bridge Pairs**, click the **LSP** checkbox to enable **Link State Propagation** for a Bridge Pair. Click **Apply** to save the settings.



Monitoring Link Statistics

To monitor Link statistics:

1. In the **Monitor > Statistics** page, choose **Ethernet** from the **Show** drop-down menu to view the status of the bypass port pair with Link State Propagation enabled. Observe that the LAN side link is down and subsequently the WAN side link of the bypass pair is administratively DISABLED.

The screenshot shows the 'Statistics' page with 'Ethernet' selected. The 'Ethernet Statistics' table displays the following data:

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

2. Navigate to **Configuration → Appliance Settings → Network Adapters → Ethernet** tab. The ports that are administratively down are indicated by a red asterisk (*) in the **Ethernet Interface Settings** list.

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](#)

Metering and Standby WAN Links

Mar 01, 2018

NetScaler SD-WAN supports enabling metered links, which can be configured such that user traffic is only transmitted on a specific Internet WAN Link when all other available WAN Links are disabled.

Metered links conserve bandwidth on links that are billed based on usage. With the metered links you can configure the links as the Last Resort link, which disallows the usage of the link until all other non-metered links are down or degraded. Set Last Resort is typically enabled when there are three WAN Links to a site (i.e. MPLS, Broadband Internet, 4G/LTE) and one of the WAN links is 4G/LTE and may be too costly for a business to allow usage unless it is absolutely necessary. Metering is not enabled by default and can be enabled on a WAN link of any access type (Public Internet / Private MPLS / Private Intranet). If metering is enabled, you can optionally configure the following:

- data cap
- billing frequency (weekly/monthly)
- start date of the billing cycle
- active heartbeat interval

- interval at which a heartbeat message is sent by an appliance to its peer on the other end of the virtual path when there has been no traffic (user/control) on the path for at least a heartbeat interval

- configurable values: default 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s

With a local metered link, the dashboard of an appliance shows a **WAN Link Metering** table at the bottom with metering information.

Bandwidth usage on a local metered link is tracked against the configured data cap. When the usage exceeds 50%, 75% or 90% of the configured data cap, the appliance generates an event to alert the user and a warning banner is displayed across the top of the dashboard of the appliance. This usage alert event can also be viewed in SD-WAN center. A metered path can be formed with 1 or 2 metered links. If a path is formed between 2 metered links, the active heartbeat interval used on the metered path is the larger of the two configured active heartbeat intervals on the links.

A metered path is a non-standby path and is always eligible for user traffic. When there is at least 1 non-metered path that is in GOOD state, a metered path carries reduced amount of control traffic and is avoided when the forwarding plane searches for a path for a duplicate packet.

Standby Mode

The standby mode of a WAN link is disabled by default. To enable standby mode, you must specify in which one of the following two modes the standby link operates:

On-demand - a standby link that becomes active when one of the conditions is met:

When the available bandwidth in the virtual path is not greater than the configured on-demand bandwidth limit AND there is sufficient usage. Sufficient usage is currently defined as more than 95% (ON_DEMAND_USAGE_THRESHOLD_PCT) of the current available bandwidth, or the difference between current available bandwidth and current usage is less than 250 kbps (ON_DEMAND_THRESHOLD_GAP_KBPS) both parameters can be changed using t2_variables when all the non-standby paths are dead or disabled.

Last-resort - a standby link that becomes active only when all non-standby links and on-demand standby links are dead or

disabled.

When configuring a standby link, you can specify standby priority and two heartbeat intervals:

- standby priority indicates the order in which a standby link becomes active, if there are multiple standby links:
 - a priority 1 standby link becomes active first whereas a priority 3 standby link becomes active last
 - multiple standby links can be assigned the same priority
- active heartbeat interval - the heartbeat interval used when the standby path is active (default 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- standby heartbeat interval - the heartbeat interval used when the standby path is inactive (default 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/disabled)

A standby path is formed with 1 or 2 standby links.

- An on-demand standby path is formed between:
 - a non-standby link and an on-demand standby link
 - 2 on-demand standby links
- A last-resort standby path is formed between
 - a non-standby link and a last-resort standby link
 - an on-demand standby link and a last-resort standby link
 - 2 last-resort standby links

The heartbeat intervals used on a standby path are determined as follows:

- If standby heartbeat is disabled on at least 1 of the 2 links, heartbeat is disabled on the standby path while inactive.
- If standby heartbeat is not disabled on either link, then the larger of the two values is used when the standby path is standby.
- If active heartbeat interval is configured on both links, then the larger of the two values is used when the standby path is active.

Heartbeat (keep alive) messages:

- On a non-standby path, heartbeat messages are sent only when there has been no traffic (control or user) for at least a heartbeat interval. The heartbeat interval varies depending on the path state. For **non-standby, non-metered** paths:
 - 50ms when the path state is GOOD
 - 25 ms when the path state is BAD

On an **standby** path, the heartbeat interval used depends on the activity state and the path state:

- While inactive, if heartbeat is not disabled, heartbeat messages are sent regularly at the configured standby heartbeat interval since no other traffic is allowed on it.
 - the configured active heartbeat interval is used when the path state is GOOD.
 - 1/2 the configured active heartbeat interval is used when the path state is BAD.

- While active, like non-standby paths, heartbeat messages are sent only when there has been no traffic (control or user) for at least the configured active heartbeat interval.

- the configured standby heartbeat interval is used when the path state is GOOD.

- 1/2 the configured standby heartbeat interval is used when the path state is BAD.

While inactive, standby paths are not eligible for user traffic. The only control protocol messages sent on inactive standby paths are heartbeat messages, which are for connectivity failure detection and quality metrics gathering. When standby paths are active, they are eligible for user traffic with added time cost. This is done so that the non-standby paths, if available, are favored during forwarding path selection.

The path state of a standby path with disabled heartbeat, while inactive, is assumed to be GOOD and it is displayed as GOOD in the Path Statistics table under Monitoring. When it becomes active, unlike a non-standby path that starts in DEAD state until it hears from its Virtual Path peer, it starts in GOOD state. If connectivity with the Virtual Path peer is not detected, the path will go BAD and then DEAD. If connectivity with the Virtual Path peer is re-established, the path will go BAD and then GOOD again.

If such standby path goes DEAD and then becomes inactive, the path state does not immediately change to (assumed) GOOD. Instead, it is kept in DEAD state for a period of time so that it cannot be used immediately. This is to prevent activity from oscillating between a lower priority path group with assumed good DEAD paths and a higher priority path group with actually GOOD paths. This on-hold period (NO_HB_PATH_ON_HOLD_PERIOD_MS) is currently set to 5 min and can be changed via `t2_variables`.

If path MTU discovery is enabled on a Virtual Path, the standby path's MTU is not used to calculate the Virtual Path's MTU while the path is standby. When the standby path becomes active, the Virtual Path's MTU is re-calculated taking into consideration the standby path's MTU. (The Virtual Path's MTU is the smallest path MTU among all active paths within the Virtual Path).

Events and log messages are generated when a standby path transitions between standby and active.

Configuration pre-requisites:

- A meter link may be of any access type.

- All links at a site can be configured with metering enabled.

- A standby link may be of Public Internet or Private Intranet access type. A WAN link of Private MPLS access type cannot be configured as a standby link.

- At least one non-standby link must be configured per site. A maximum of 3 standby links per site is supported.

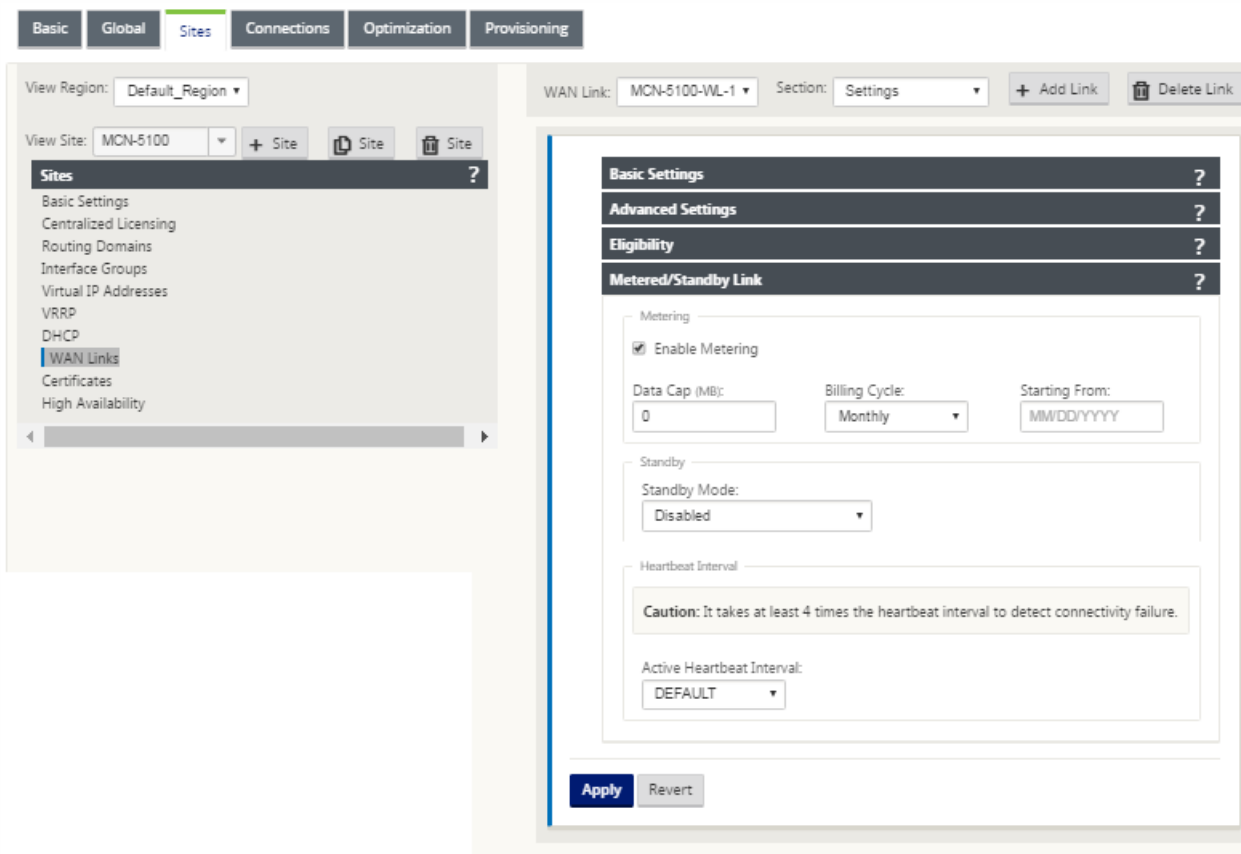
- Internet/Intranet services may not be configured on on-demand standby links. On-demand standby links support Virtual Path service only.

- Internet service may be configured on a last-resort standby link, but only load balance mode is supported.

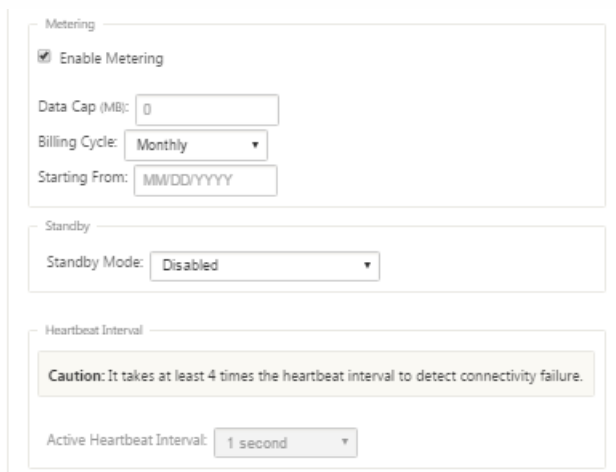
- Intranet service may be configured on a last-resort standby link, but only secondary mode is supported and primary reclaim must be enabled.

To configure metered links:

1. In the SD-WAN web management interface, navigate to **Configuration Editor > Sites > WAN Links > Settings**. Click **Metered/Standby Link** to expand it.



2. Check the **Enable Metering** checkbox. You can provide values for data cap, billing frequency, billing cycle start date and the active heartbeat interval.



To configure standby links:

1. In the SD-WAN web management interface, navigate to **Configuration Editor > Sites > WAN Links > Settings**. Click **Metered/Standby Link** to expand it.

2. By default, standby mode of a WAN link is disabled. To configure the WAN link as standby, click the pencil icon next to **Settings** to enter edit mode and select one of the standby modes.

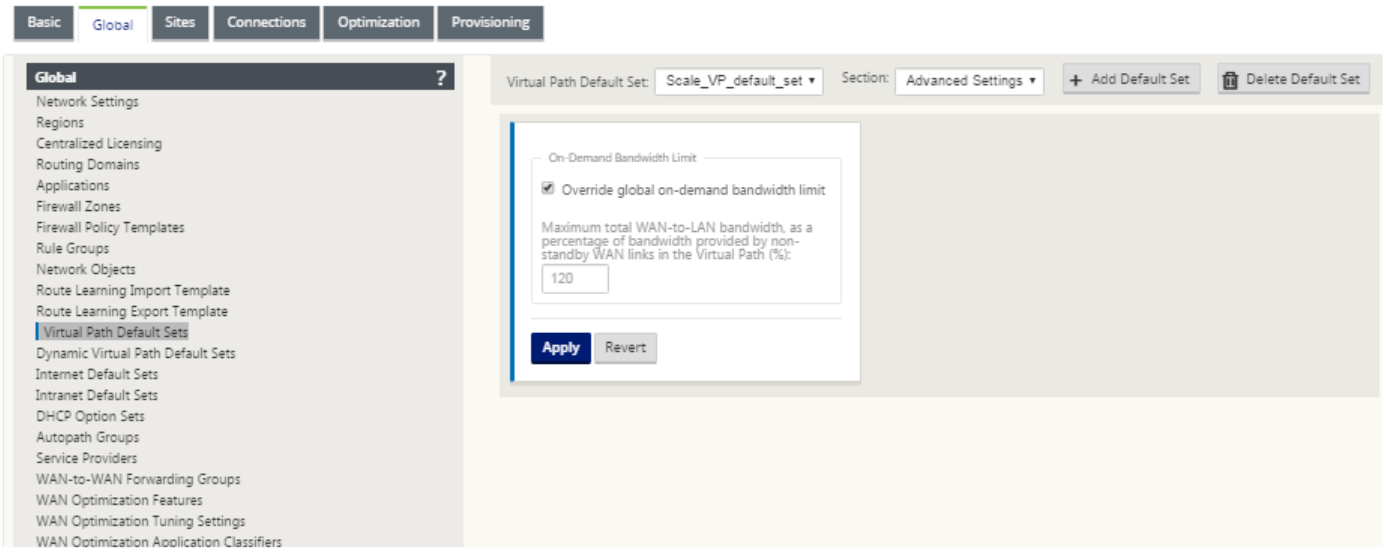
3. Once a standby mode is selected, select the standby priority, active heartbeat interval, and standby heartbeat interval as appropriate. Click **apply** to validate the configuration.

4. If an on-demand standby link is configured, the global default on-demand bandwidth limit (120%) is applied to the Virtual Path. This specifies the maximum WAN-to-LAN bandwidth allowed for the Virtual Path. It is expressed as a percentage of the total bandwidth provided by all non-standby links in the Virtual Path. As long as the available bandwidth in the Virtual Path is below the limit and if there is sufficient usage, the appliance will attempt to activate on-demand paths to supplement bandwidth.

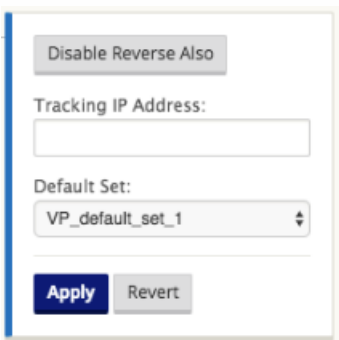
a. To view or change the global default on-demand bandwidth limit, open the sections **Global > Virtual WAN Network Settings**.

b. If you want to apply an on-demand bandwidth limit specific to a Virtual Path and keep the global default setting

unchanged, a Virtual Path Default Set needs to be created and the on-demand bandwidth limit in the Advanced Settings can be changed.



C. To apply settings for a specific Virtual Path, the user should navigate to the section **Connections > Site > Virtual Paths > Basic Settings** and select the default set for the particular Virtual Path.



How To Monitor Metered and Standby WAN Links

1. When path statistics (**Monitoring > Statistics > Paths**) are displayed, metered links and standby links are marked as shown below.

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.										
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	RL-TB-CL1-WL-1	RL-TB-MCN-WL-1	GOOD	GOOD	Static	2	2	0.00	12.42	NO
2	RL-TB-CL1-WL-1	RL-TB-MCN-WL-2	GOOD	GOOD	Static	2	2	0.00	21.48	NO
3	RL-TB-CL1-WL-2 (metered)	RL-TB-MCN-WL-1	GOOD	GOOD	Static	2	2	0.00	0.23	NO
4	RL-TB-CL1-WL-2 (metered)	RL-TB-MCN-WL-2	GOOD	GOOD	Static	2	2	0.00	0.23	NO
5	RL-TB-MCN-WL-1	RL-TB-CL1-WL-1	GOOD	GOOD	Static	2	2	0.00	11.93	NO
6	RL-TB-MCN-WL-1	RL-TB-CL1-WL-2 (metered)	GOOD	GOOD	Static	2	2	0.00	0.23	NO
7	RL-TB-MCN-WL-2	RL-TB-CL1-WL-1	GOOD	GOOD	Static	2	2	0.00	17.36	NO
8	RL-TB-MCN-WL-2	RL-TB-CL1-WL-2 (metered)	GOOD	GOOD	Static	2	2	0.00	0.23	NO

Showing 1 to 8 of 8 entries

Bandwidth calculated over the last 5 seconds

Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Show latest data.

Path Statistics Summary

Filter: in Any column 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	RL-TB-CL2-WL-1	RL-TB-MCN-WL-1	GOOD	GOOD	Static	2	2	0.00	17.01	NO
2	RL-TB-CL2-WL-1	RL-TB-MCN-WL-2	GOOD	GOOD	Static	2	2	0.00	12.34	NO
3	RL-TB-CL2-WL-2 (standby)	RL-TB-MCN-WL-1	GOOD	GOOD	Static	9999	0	0.00	0.00	NO
4	RL-TB-CL2-WL-2 (standby)	RL-TB-MCN-WL-2	GOOD	GOOD	Static	9999	0	0.00	0.00	NO
5	RL-TB-MCN-WL-1	RL-TB-CL2-WL-1	GOOD	GOOD	Static	2	2	0.00	12.91	NO
6	RL-TB-MCN-WL-1	RL-TB-CL2-WL-2 (standby)	GOOD	GOOD	Static	9999	0	0.00	0.00	NO
7	RL-TB-MCN-WL-2	RL-TB-CL2-WL-1	GOOD	GOOD	Static	2	2	0.00	11.83	NO
8	RL-TB-MCN-WL-2	RL-TB-CL2-WL-2 (standby)	GOOD	GOOD	Static	9999	0	0.00	0.00	NO

Showing 1 to 8 of 8 entries

Bandwidth calculated over the last 4.988 seconds

2. If the appliance has a Virtual Path that has a local or remote on-demand standby link, when WAN link usage statistics are viewed, an additional table showing on-demand bandwidth is displayed at the bottom of the page (**Monitoring > Statistics > WAN Link Usage**).

Local WAN-to-LAN On Demand WAN Link Usages

Filter: in Any column

Show 100 entries Showing 1 to 2 of 2 entries

WAN Link	WAN Link Mode	Standby Priority	Configured	Adaptive Bandwidth Detection			Virtual Path Name	Virtual Path On Demand Bandwidth Limit Kbps	Virtual Path Available Bandwidth Kbps	In Use
				Minimum Acceptable BW Kbps	Maximum Allowed BW Kbps	Current Allowed BW Kbps				
RL-TB-CL2-WL-1	Regular-Active	N/A	No	N/A	N/A	N/A	RL-TB-MCN-RL-TB-CL2	11760	9500	Yes
RL-TB-CL2-WL-2 (standby)	On-Demand	1	No	N/A	N/A	N/A	RL-TB-MCN-RL-TB-CL2	11760	9500	No

Showing 1 to 2 of 2 entries

Bandwidth calculated over the last 4.964 seconds

3. When the usage on a metered link exceeds 50% of the configured data cap, a warning banner is displayed across the top of the dashboard. In addition, if the usage exceeds 75% of the configured data cap, the numerical metering information toward the bottom of the dashboard will be highlighted.

Dashboard Monitoring Configuration

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

- RL-TB-CL1-WL-2 : 100%

System Status

Name: RL-TB-CL1
 Model: VPX
 Appliance Mode: Client
 Serial Number: c4ec4b39-04db-2633-5ed4-38b3ad3f52d2
 Management IP Address: 10.200.32.236
 Appliance Uptime: 2 weeks, 3 days, 20 hours, 7 minutes, 22.6 seconds
 Service Uptime: 2 hours, 1 minutes, 52.0 seconds
 Routing Domain Enabled: Default_RoutingDomain

Local Versions

Configuration Created On: Fri May 26 11:42:15 2017
 Software Version: 9.3.0.43.594998
 Built On: May 26 2017 at 03:42:20
 Hardware Version: VPX
 OS Partition Version: 4.6

Virtual Path Service Status

Virtual Path RL-TB-MCN-RL-TB-CL1 Uptime: 2 hours, 55.0 seconds.

WAN Link Metering

WAN Link Name: RL-TB-CL1-WL-2
 Data Usage: **6921.72 MBs of 5000 MBs**
 Usage(in %): 138
 Billing Cycle: MONTHLY
 Starting From: 05/20/2017
 Days Elapsed: 7 days of 31 days

A WAN link usage event is also generated at the appliance when the usage exceeds 50%, 75% and 90% of the configured data cap.

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

4. When a standby path transitions between standby and active state, an event is generated by the appliance.

24640	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-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-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-WL-2->RL-TB-CL2-WL-1 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-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to GOOD.
24636	2	RL-TB-MCN-WL-1->RL-TB-CL2-WL-1	VIRTUAL PATH	2017-05-26 10:18:27	GOOD	NOTICE	The state of Virtual Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 has changed from BAD to GOOD.
24635	0	RL-TB-MCN-WL-1->RL-TB-MCN-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-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-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-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-WL-1->RL-TB-CL2-WL-2 has become active

5. The configured active and standby heartbeat intervals for each path can be viewed at **Configuration > Virtual WAN > View Configuration > Paths**.

Path Configuration										
Paths on virtual path 1 'RL-TB-MCN-WL-2->RL-TB-CL2-WL-2'										
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	Sr
0	RL-TB-MCN-WL-1	RL-TB-CL1-WL-1	192.168.15.2	192.16.152.2	-	-	4980	4980	-	4980
3	RL-TB-MCN-WL-2	RL-TB-CL1-WL-2	192.168.15.2	192.168.16.194	-	-	4980	4980	-	4980
1	RL-TB-MCN-WL-1	RL-TB-CL1-WL-2	192.16.124.2	192.168.16.194	-	-	4980	4980	-	4980
2	RL-TB-MCN-WL-2	RL-TB-CL1-WL-1	192.168.15.2	192.16.152.2	-	-	4980	4980	-	4980
0	RL-TB-CL1-WL-1	RL-TB-MCN-WL-1	192.16.152.2	192.16.124.2	-	-	4980	4980	-	4980
3	RL-TB-CL1-WL-2	RL-TB-MCN-WL-2	192.168.16.194	192.168.15.2	-	-	4980	4980	-	4980
1	RL-TB-CL1-WL-1	RL-TB-MCN-WL-2	192.16.152.2	192.168.15.2	-	-	4980	4980	-	4980
2	RL-TB-CL1-WL-2	RL-TB-MCN-WL-1	192.168.16.194	192.16.124.2	-	-	4980	4980	-	4980

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
RL-TB-MCN-WL-1	RL-TB-CL1-WL-1	YES	YES	YES	0	n/a	n/a
RL-TB-MCN-WL-2	RL-TB-CL1-WL-2	YES	YES	YES	0	n/a	2000
RL-TB-MCN-WL-1	RL-TB-CL1-WL-2	YES	YES	YES	0	n/a	2000
RL-TB-MCN-WL-2	RL-TB-CL1-WL-1	YES	YES	YES	0	n/a	n/a
RL-TB-CL1-WL-1	RL-TB-MCN-WL-1	YES	YES	YES	0	n/a	n/a
RL-TB-CL1-WL-2	RL-TB-MCN-WL-2	YES	YES	YES	0	n/a	2000
RL-TB-CL1-WL-1	RL-TB-MCN-WL-2	YES	YES	YES	0	n/a	n/a
RL-TB-CL1-WL-2	RL-TB-MCN-WL-1	YES	YES	YES	0	n/a	2000

Path Configuration											
Paths on virtual path 2 'RL-TB-MCN-WL-1->RL-TB-CL2-WL-2'											
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
0	RL-TB-CL2-WL-1	RL-TB-MCN-WL-1	192.16.152.2	192.16.124.2	-	-	4980	4980	-	-	*
3	RL-TB-CL2-WL-2	RL-TB-MCN-WL-2	192.168.17.2	192.168.15.2	-	-	4980	4980	-	-	*
1	RL-TB-CL2-WL-1	RL-TB-MCN-WL-2	192.16.152.2	192.168.15.2	-	-	4980	4980	-	-	*
2	RL-TB-CL2-WL-2	RL-TB-MCN-WL-1	192.168.17.2	192.16.124.2	-	-	4980	4980	-	-	*
0	RL-TB-MCN-WL-1	RL-TB-CL2-WL-1	192.16.152.2	192.16.124.2	-	-	4980	4980	-	-	*
3	RL-TB-MCN-WL-2	RL-TB-CL2-WL-2	192.168.17.2	192.168.15.2	-	-	4980	4980	-	-	*
1	RL-TB-MCN-WL-1	RL-TB-CL2-WL-2	192.16.152.2	192.168.15.2	-	-	4980	4980	-	-	*
2	RL-TB-MCN-WL-2	RL-TB-CL2-WL-1	192.168.17.2	192.16.152.2	-	-	4980	4980	-	-	*

From Link	To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)
RL-TB-CL2-WL-1	RL-TB-MCN-WL-1	YES	YES	YES	0	n/a	n/a
RL-TB-CL2-WL-2	RL-TB-MCN-WL-2	YES	YES	YES	1	0	1000
RL-TB-CL2-WL-1	RL-TB-MCN-WL-2	YES	YES	YES	0	n/a	n/a
RL-TB-CL2-WL-2	RL-TB-MCN-WL-1	YES	YES	YES	1	0	1000
RL-TB-MCN-WL-1	RL-TB-CL2-WL-1	YES	YES	YES	0	n/a	n/a
RL-TB-MCN-WL-2	RL-TB-CL2-WL-2	YES	YES	YES	1	0	1000
RL-TB-MCN-WL-1	RL-TB-CL2-WL-2	YES	YES	YES	1	0	1000
RL-TB-MCN-WL-2	RL-TB-CL2-WL-1	YES	YES	YES	0	n/a	n/a

Quality of Service

Mar 01, 2018

The network between the data center and branch offices transport a multitude of applications and data, such as high quality video or real-time voice. The network capabilities and resources are stretched by bandwidth sensitive applications. The SD-WAN network provides guaranteed, secure, measurable and predictable services. This is achieved by managing the delay, jitter, bandwidth and packet loss on the network.

NetScaler SD-WAN solution has a sophisticated application QoS engine that accesses the application traffic and prioritize it against other applications. It also understands the requirements with respect to the WAN network quality, and picks a network path based on the quality characteristics in real time.

The topics in the following sections discuss QoS classes, IP rules, application QoS rules and other components that are required to define application QoS.

Customizing Classes

Mar 01, 2018

The SD-WAN configuration provides a default set of application-classification, rule-filtering, and class-assignment settings that can be applied to any virtual path service in the SD-WAN environment. You can also customize these settings.

Using classes, you can classify a specific type of traffic on the virtual path, and then you can apply rules to handle this traffic. Traffic is assigned to a specific class, as defined in the rule.

For more information about creating rules, see [Rules by IP Address and Port Number](#).

The SD-WAN system provides 17 classes (0-16). Classes 0-3 are predefined for Citrix HDX QoS prioritization. To use this feature, enable the following options:

- **WAN Optimization**, available under **Optimization > Features**.
- **HDX QoS Priorities**, available under **Optimization > Features**.
- **ICA Service Class**, available under **Optimization > Service Classes**.

These classes are used to classify HDX traffic with different ICA priority tags. You can edit the class types and their assigned bandwidth sharing to obtain the optimal quality of service, but you cannot edit the names of the classes.

Classes 10-16 are predefined and are associated with Realtime, Interactive, and Bulk class types. Each type can be configured further to optimize quality of service for its type of traffic. Classes 4-9 can be used to specify user defined classes. Classes are of one of the following three types:

- **Realtime**: Used for low latency, low bandwidth, time-sensitive traffic. Real-time applications are time sensitive but don't really need high bandwidth (for example voice over IP). Real-time applications are very sensitive to latency and jitter, but can tolerate some loss.
- **Interactive**: Used for interactive traffic with low to medium latency requirements and low to medium bandwidth requirements. Interactive applications involve human input in the form of mouse clicks or cursor moves. The interaction is typically between a client and a server. The communication might not need high bandwidth but is sensitive to loss and latency. However, server to client does need high bandwidth to transfer graphical information, which might not be sensitive to loss.
- **Bulk**: Used for high bandwidth traffic that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as bulk class. These applications involve very little human interference and are mostly handled by the systems themselves.

To customize classes:

1. In the SD-WAN Configuration Editor, navigate to **Global > Virtual Path Default Sets**.
2. Click **Add Default Set**, enter a name for the default set and click **Add**. In the **Section** field select **Classes**.

Virtual Path Default Set: New_Default_Set-1 Section: Classes + Add Default Set Delete Default Set

ID	Name	Type	Initial				Sustained		Reset
			Period	Rate	%/Kbps	Share %	Rate	Share %	
0	HDX_priority_tag_0	Realtime	0	30	%	0	30	0	↔
1	HDX_priority_tag_1	Interactive	0	0	%	20	0	20	↔
2	HDX_priority_tag_2	Interactive	0	0	%	6	0	6	↔
3	HDX_priority_tag_3	Interactive	0	0	%	2	0	2	↔
4	class_4	Bulk		0	%	0	0	0	↔
5	class_5	Bulk		0	%	0	0	0	↔
6	class_6	Bulk		0	%	0	0	0	↔
7	class_7	Bulk		0	%	0	0	0	↔
8	class_8	Bulk		0	%	0	0	0	↔
9	class_9	Bulk		0	%	0	0	0	↔
10	realtime_class	Realtime	0	30	%	0	30	0	↔
11	interactive_high_class	Interactive	0	0	%	20	0	20	↔
12	interactive_medium_class	Interactive	0	0	%	13	0	13	↔
13	interactive_low_class	Interactive	0	0	%	6	0	6	↔
14	interactive_very_low_class	Interactive	0	0	%	3	0	3	↔
15	bulk_background_class	Bulk		0	%	0	0	100	↔
16	bulk_unused_class	Bulk		0	%	0	0	0	↔

Apply Revert

3. In the **Name** field, either leave the default name or enter a name of your choice.

4. In the **Type** field, select the class type (Realtime, Interactive or Bulk).

5. For realtime classes, you can specify the following attributes:

- * **Initial Period:** The time period in milliseconds to apply an initial rate before switching to a sustained rate.
- * **Initial Rate:** Maximum rate at which packets leave the queue during the initial period.
- * **Sustained Rate:** Maximum rate at which the packets leave the queue after the initial period.

When in contention, the scheduler ensures that the realtime class receives the **Initial Rate** and the **Sustained Rate** that you specify, plus a small percentage of the available bandwidth that is shared with interactive and bulk classes.

6. For interactive classes, you can specify the following attributes:

- * **Initial Period:** The time period, in milliseconds, during which to apply initial percentage of the available bandwidth before switching to the sustained percentage. Typically, 20 ms.
- * **Initial Share %:** The maximum share of virtual-path bandwidth during the initial period.
- * **Sustained Share %:** The maximum share of virtual-path bandwidth after the initial period.

Interactive classes use the remaining bandwidth after the real-time traffic has been serviced.

7. For bulk classes, you can specify only the **Sustained Share%**, which determines the remaining virtual path bandwidth to be used for a bulk class.

Bulk traffic is serviced after real-time and interactive traffic are serviced. Typically, a bulk class gets a lower sustained share % than an interactive class.

8. Click **Apply**.

Note

Save the configuration, export it to the change management inbox, and initiate the change management process.

Rules by IP Address and Port Number

Mar 01, 2018

Using the configuration editor, you can create rules for traffic flow and associate the rules with applications and classes. You can specify criteria to filter traffic for a flow, and can apply general behavior, LAN to WAN behavior, WAN to LAN behavior, and packet inspection rules.

To create rules:

1. In the SD-WAN Configuration Editor, navigate to **Global > Virtual Path Default Sets**.
2. Click **Add Default Set**, enter a name for the default set and click **Add**. In the **Section** field select **Rules**. Click **+**.
3. In the **Order** field, enter the order value to define when the rule is applied in relation to other rules.
4. In the **Rule Group Name** field, select a rule group. The statistics for rules with the same rule group will be grouped together and can be viewed together.

For viewing rule groups, navigate to **Monitoring > Statistics**, and in the **Show** field select **Rule Groups**.

You can also add custom rule groups. For more information, see [Add Rule Groups and Enable MOS](#).

5. In the **Routing Domain** field, choose one of the configured routing domains.
6. You can define rule matching criteria to filter services on the basis of the parameters listed below. After the filtering, the rule settings are applied to the services matching these criteria.

- * **Source IP Address:** Source IP address and the subnet mask to match against the traffic.
- * **Destination IP Address:** Destination IP address and the subnet mask to match against the traffic.

Note

Select **Dest=Src**, if the source and destination IP address are the same.

- * **Protocol:** Protocol to match against the traffic.
 - * **Source Port:** Source port number or port range to match against the traffic.
 - * **Destination Port:** Destination port number or port range to match against the traffic.
 - * **DSCP:** The **DSCP** tag in the IP header to match against the traffic.
 - * **VLAN:** The **VLAN ID** to match against the traffic.
7. Click the add (+) icon next to the new rule.
 8. Click **Initialize Properties Using Protocol** to initialize the rule properties by applying the rule defaults and recommended settings for the protocol. This will populate the default rule settings. You can also customize the settings manually, as shown in the following steps.

9. Click the **WAN General** tile to configure the following properties.

* **Transmit Mode:** Select one of the following transmit modes.

- **Load Balance Path:** Traffic for the flow will be balanced across multiple paths for the service. Traffic will be sent through the best path until that path is completely used. Leftover packets will be sent through the next best path.

- **Persistent Path:** Traffic for the flow will remain on the same path until the path is no longer available.

- **Duplicate Path:** Traffic for the flow is duplicated across multiple paths, increasing reliability.

- **Override Service:** Traffic for the flow will override to a different service. In the Override Service field, select the service type to which the service will override. For example, a virtual path service could override to an intranet, internet, or pass-through service.

* **Retransmit Lost Packets:** Send traffic that matches this rule to the remote appliance over a reliable service and retransmit lost packets.

* **Enable TCP Termination:** Enable TCP termination of traffic for this flow. This reduces the round-trip time for acknowledgement packets and therefore improves throughput.

* **Preferred WAN Link:** The WAN link that the flows should use first.

* **Persistent Impedance:** The minimum time in milliseconds for which the traffic would remain in the same path, until wait time on the path is longer than the configured value.

* **Enable IP, TCP and UDP:** Compress headers in IP, TCP and UDP packets.

* **Enable GRE:** Compress headers in GRE packets.

* **Enable Packet Aggregation:** Aggregate small packets into larger packets.

* **Track Performance:** Records performance attributes of this rule in a session data base (for example, loss, jitter, latency and bandwidth).

WAN General

Transmit Mode:
Load Balance Paths Retransmit Lost Packets

Override Service: Preferred WAN Link Persistent Impedance(ms):
<N/A> Any 50

Traffic Optimization

Enable TCP Termination: Header Compression
<Default> Enable IP, TCP and UDP Enable GRE

Enable Packet Aggregation

Track Performance

10. Click the **LAN to WAN** tile, to configure LAN to WAN behavior for this rule.

* **Class:** Select a class with which to associate this rule.

Note

You can also customize classes before applying rules, for more information, see [How to Customize Classes](#).

* **Large Packet Size:** Packets smaller than or equal to this size are assigned the **Drop Limit** and **Drop Depth** values specified in the fields to the right of the **Class** field.

The screenshot shows the 'LAN to WAN' configuration page. It is divided into 'General' and 'Reassign' sections. In the 'General' section, the 'Class' is set to '<Default>'. The 'Large Packet Size (bytes)' is 0. The 'Drop Limit (ms)' is 50 and 'Drop Depth (bytes)' is 128000. In the 'Reassign' section, the 'Reassign Class' is 'Disabled <Default>', 'Reassign Size (bytes)' is 2000, and 'Large Packet Size (bytes)' is 0. The 'Drop Limit (ms)' and 'Drop Depth (bytes)' are also 50 and 128000 respectively. The 'Enable RED' checkbox is unchecked in both sections.

Packets larger than this size are assigned the values specified in the default **Drop Limit** and **Drop Depth** fields in the **Large Packets** section of the screen.

This screenshot is identical to the one above, showing the 'LAN to WAN' configuration page. In this view, the 'Drop Limit (ms)' and 'Drop Depth (bytes)' fields in the 'Large Packets' section of the 'General' section are highlighted with a red box, showing values of 0 and 0 respectively.

* **Drop Limit:** Length of time after which packets waiting in the class scheduler are dropped. Not applicable for a bulk class.

* **Drop Depth:** Queue depth threshold after which packets are dropped.

- * **Enable RED:** Random Early Detection (RED) ensures fair sharing of class resources by discarding packets when congestion occurs.
- * **Reassign Size:** Packet length that, when exceeded, causes the packet to be reassigned to the class specified in the Reassign Class field.
- * **Reassign Class:** Class used when the packet length exceeds the packet length specified in the Reassign Size field.
- * **Disable Limit:** Time for which duplication can be disabled to prevent duplicate packets from consuming bandwidth.
- * **Disable Depth:** The queue depth of the class scheduler, at which point the duplicate packets will not be generated.
- * **TCP Standalone ACK class:** High priority class to which TCP standalone acknowledgements are mapped during large file transfers.

LAN to WAN

General

Class: 3 (citrix_class_3) Drop Limit (ms): 80

Large Packet Size (bytes): 0 Enable RED

Large Packets **Duplicate Packets**

Drop Limit (ms): 50 Drop Depth (bytes): 128000 Disable Limit (ms): 0 Disable Depth (bytes): 128000

Reassign

Reassign Class: 1 (citrix_class_1) Drop Limit (ms): 50

Reassign Size (bytes): 2000 Large Packet Size (bytes): 0 Enable RED

Large Packets **Duplicate Packets**

Drop Limit (ms): 1 Drop Depth (bytes): 0 Disable Limit (ms): 0 Disable Depth (bytes): 128000

TCP Standalone ACK

TCP Standalone ACK Class: Disabled <Default> Drop Limit (ms): 50

Large Packet Size (bytes): 0 Enable RED

Large Packets

Drop Limit (ms): 0 Drop Depth (bytes): 0

11. Click the **WAN to LAN** tile to configure WAN to LAN behavior for this rule.

- * **Enable Packets Resequencing:** Sequences the packets into the correct order at the destination.
- * **Hold Time:** Time interval for which the packets are held for resequencing, after which the packets are sent to the LAN.
- * **Discard Late Resequencing Packets:** Discard out-of-order packets that arrived after the packets needed for resequencing have been sent to the LAN.

* **DSCP Tag:** DSCP tag applied to the packets that match this rule, before sending them to the LAN.

The screenshot shows a configuration window titled "WAN to LAN". It contains two main sections. The first section is "Packet Resequencing", which includes two checked checkboxes: "Enable Packet Resequencing" and "Discard Late Resequencing Packets". To the right of these checkboxes is a "Hold Time (ms):" label and an empty input field. The second section is "DSCP Tag:", which features a dropdown menu with "af12" selected and a downward arrow icon.

12. Click **Deep Packet Inspection** tile and select **Enable Passive FTP Detection** to allow the rule to detect the port used for FTP data transfer and automatically apply the rule settings to the detected port.

13. Click **Apply**.

Note

Save the configuration, export it to the change management inbox, and initiate the change management process.

Rules by Application Name

Jun 12, 2018

The Application classification feature allows the NetScaler SD-WAN appliance to parse incoming traffic and classify them as belonging to a particular application or application family. This classification allows us to enhance the QoS of individual application or application families by creating and applying application rules.

You can filter traffic flows based on application, application family, or application object match-types and apply application rules to them. The application rules are similar to Internet Protocol (IP) rules. For information on IP rules see, [Rules by IP Address and Port Number](#).

For every application rule, you can specify the mode of transmission. The following are the available transmit modes:

- **Load Balance Path:** Application traffic for the flow is balanced across multiple paths. Traffic is sent through the best path until that path is completely used. The remaining packets are sent through the next best path.
- **Persistent Path:** Application traffic remains on the same path until the path is no longer available.
- **Duplicate Path:** Application traffic is duplicated across multiple paths, increasing reliability.

The application rules are associated to classes. For information on classes, see [Customizing Classes](#).

By default, the following five pre-defined application rules are available for Citrix ICA applications:

Rule	Class	Transmit Mode	Retransmit Lost Packets	Enable Packet Resequencing	Discard Late Resequencing Packets
HDX_Priority_0	HDX_priority_tag_0	Load Balance Path	Enabled	Enabled	Enabled
HDX_Priority_1	HDX_priority_tag_1	Load Balance Path	Enabled	Enabled	Enabled
HDX_Priority_2	HDX_priority_tag_2	Load Balance Path	Enabled	Enabled	Enabled
HDX_Priority_3	HDX_priority_tag_3	Load Balance Path	Enabled	Enabled	Enabled
HDX	interactive_high_class	Load Balance Path	Enabled	Enabled	Enabled

How Application Rules are Applied?

In the SD-WAN network, when the incoming packets reach the SD-WAN appliance, the initial few packets do not undergo

DPI classification. At this point, the IP rule attributes such as Class, TCP termination and so on are applied to the packets. After DPI classification, the application rule attributes such as Class, transmit mode and so on override the IP rule attributes.

The IP rules have more number of attributes as compared to the application rules. The application rule overrides only a few IP rule attributes, the rest of the IP rule attributes remain processed on the packets.

For example, consider you have specified an application rule for a webmail application such as Google Mail that uses the SMTP protocol. The IP rule set for SMTP protocol is applied initially before DPI classification. After parsing the packets and classifying it as belonging to Google Mail application, the application rule specified for the Google Mail application is applied.

Creating Application Rules

To create application rules:

1. In the SD-WAN Configuration Editor, navigate to **Global > Virtual Path Default Sets**.
2. Click **Add Default Set**, enter a name for the default set and click **Add**. In the **Section** field select **Application QoS**. Click **+**.

Note

You can also create application rules by navigating to **Connections > Virtual Paths > Application QoS** or **Global > Dynamic Virtual Path Default Set > Application QoS**.

? x

Add

Order: Match Type: Application Objects: Rule Group Name:

Source IP Address: Destination IP Address: Src = Dest

Source Port: Destination Port: Src = Dest

WAN General

Transmit Mode: Retransmit Lost Packets Persistent Impedance(ms):

LAN to WAN

Class: Drop Limit (ms): Drop Depth (bytes): Enable RED

Duplicate Packets

Disable Limit (ms): Disable Depth (bytes):

WAN to LAN

Enable Packet Resequencing Resequence Hold Time (ms): Discard Late Resequenced Packets

DSCP Tag:

3. In the **Order** field, type the order value to define when the rule is applied in relation to other rules.
4. In the **Match Type** field, choose one of the following match types:
 - **Application** – If this match type is selected, specify the application that is used as a match criteria for this filter.
 - **Application Family** – If this match type is selected, select an application family that is used as a match criteria for this filter.
 - **Application Object** – If this match type is selected, select an application family that is used as a match criteria for this filter.

For more information on application, application family and application object, see [Application Classification](#).

5. In the **Rule Group Name** field, select a rule group. The statistics for rules with the same rule group will be grouped together and can be viewed together.

For viewing rule groups, navigate to **Monitoring > Statistics**, and in the **Show** field select **Rule Groups**.

You can also add custom rule groups. For more information, see [Add Rule Groups and Enable MOS](#).

6. Specify the following application rule matching criteria to filter the application traffic. After the filtering, the rule settings are applied to the services matching these criteria.
 - **Source IP Address:** Source IP address and the subnet mask to match against the traffic.
 - **Destination IP Address:** Destination IP address and the subnet mask to match against the traffic.
 - **Source Port:** Source port number or port range to match against the traffic.
 - **Destination Port:** Destination port number or port range to match against the traffic.

Note

Choose **Src = Dest**, if the source and destination internet protocol address are the same.

7. Configure the following general WAN settings:

- In the **Transmit Mode** field, choose one of the following transmit modes:
 - **Load Balance Path**: Application traffic for the flow is balanced across multiple paths. Traffic is sent through the best path until that path is completely used. The remaining packets are sent through the next best path.
 - **Persistent Path**: Application traffic remains on the same path until the path is no longer available.
In the **Persistent Impedance** field, specify the minimum time in milliseconds for which the traffic would remain in the same path, until wait time on the path is longer than the configured value.
 - **Duplicate Path**: Application traffic is duplicated across multiple paths, increasing reliability.
- Check **Retransmit Lost Packets** to send traffic that matches this rule to the remote appliance over a reliable service and retransmit lost packets.

8. Configure the LAN to WAN settings:

- **Class**: Select a class with which to associate this rule.

You can also customize classes before applying rules, for more information, see [Customizing Classes](#).
- **Drop Limit**: Length of time after which packets waiting in the class scheduler are dropped. Not applicable for a bulk class.
- **Drop Depth**: Queue depth threshold after which packets are dropped.
- **Enable RED**: Random Early Detection (RED) ensures fair sharing of class resources by discarding packets when congestion occurs.
- **Disable Limit**: Time for which duplication can be disabled to prevent duplicate packets from consuming bandwidth.
- **Disable Depth**: The queue depth of the class scheduler, at which point the duplicate packets will not be generated.

9. Configure the following WAN to LAN behavior for this rule:

- **Enable Packets Resequencing**: Sequences the packets in the correct order at the destination.
- **Resequence Hold Time**: Time interval for which the packets are held for resequencing, after which the packets are sent to the LAN.
- **Discard Late Resequencing Packets**: Discard out-of-order packets that arrived after the packets needed for resequencing have been sent to the LAN.

10. Click **Apply**.

To confirm if application rules are applied to traffic flow, navigate to **Monitoring > Flows**.

Make a note of the app rule id and check if the class type and transmission mode are as per your rule configuration.

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
172.186.30.74	172.186.10.89	LAN to WAN	35118	5001	UDP	default	4961	Virtual Path	DC-Client-1	LOCAL	0	4959	7428582	292.687	3507.565	126.441	0.000	48	0	11	INTERACTIVE	DC-WL-1->Client-1-WL-1	N/A	Duplicate

You can monitor the application QoS such as no of packets / bytes uploaded, downloaded, or dropped at each site by navigating to **Monitoring > Statistics > Application QoS**.

The **Num** parameter indicates the app rule id. Check for the app rule id obtained from the flow.

Creating Custom Applications

In SD-WAN 10.0, you can use application objects to define custom applications based on the following match types:

- IP protocol
- Application name
- Application family

The DPI classifier analyzes the incoming packets and classifies it as applications based on the specified match criteria. You can use these classified custom applications in QoS, firewall, and application routing.

Tip

You can specify one or more match types.

You can view the reports for the classified custom applications in SD-WAN Center. For more information, see [How to View Application Statistics](#).

To create custom applications:

1. In the Configuration Editor, navigate to **Global > Applications > Custom Applications** and click **+**.

Add ? x

Name: Priority: Enable Reporting

Application Match Criteria +

Match Type	Application Family	Application	Protocol	Network IP Address 1	Port 1
IP Protocol ▼	▼		TCP (6) ▼	*	*

Add Cancel

2. Set the following parameters:

- **Name:** Name for the custom application
- **Enable Reporting:** Allows viewing custom application reports in SD-WAN Center. For more information see, [How to View Application Statistics](#).
- **Priority:** The priority of the custom application. When the incoming packets match two or more custom application definitions, the custom application definition with the highest priority is applied.

3. Click + in the **Application Match Criteria** section.

4. Select one of the following match types:

- **IP Protocol:** Specify the protocol, network IP address, port number, and, DSCP tag.
- **Application:** Specify the application name, network IP address, port number, and, DSCP tag.
- **Application Family:** Select an application family and specify the network IP address, port number, and, DSCP tag.

5. Click + to add more application match criteria.

6. Click **Apply**.

Add Rule Groups and Enable MOS

Jun 12, 2018

A particular application in the network can be defined by the group of rules that is applied to it. The SD-WAN configuration editor provides a default list of rule groups. You can also create custom rule groups and tag individual IP rules or application QoS rules to applications.

For more information about rules, see [Rules by IP Address and Port Number](#) and [Rules by Application Name](#).

The statistics for rules with the same rule group will be grouped together and can be viewed together.

For viewing statistics based on rule groups, navigate to **Monitoring > Statistics**, and in the **Show** field select **Rule Groups**.

The mean opinion score (MOS) is a numerical measure of the quality of the experience that an application delivers to end users. It is primarily used for VoIP applications. In SD-WAN, MOS is also used to assess the quality of non-VoIP applications by judging the traffic as if it were a VoIP call.

The average MoS Score is calculated with a sampling interval of 1 minute. MoS score calculated by other third party tools may vary, depending on the sampling interval used.

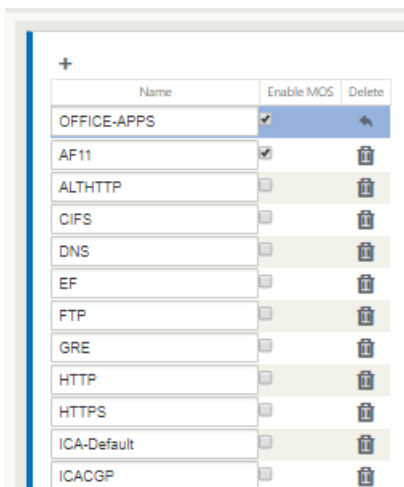
SD-WAN Center displays the MOS for existing traffic that passes through the virtual path. For more information about viewing MOS in SD-WAN Center, see [How to View MOS for Applications](#).

To add a custom rule group:

1. In the Configuration Editor, navigate to **Global > Rule Groups**.

The default list of rule groups appears.

2. Click the add (+) icon.
3. Enter the application name.
4. Click the edit icon and select **Enable MOS**.



Name	Enable MOS	Delete
OFFICE-APPS	<input checked="" type="checkbox"/>	
AF11	<input checked="" type="checkbox"/>	
ALTHHTTP	<input type="checkbox"/>	
CIFS	<input type="checkbox"/>	
DNS	<input type="checkbox"/>	
EF	<input type="checkbox"/>	
FTP	<input type="checkbox"/>	
GRE	<input type="checkbox"/>	
HTTP	<input type="checkbox"/>	
HTTPS	<input type="checkbox"/>	
ICA-Default	<input type="checkbox"/>	
ICACGP	<input type="checkbox"/>	

5. Click **Apply**.

Note

You can also enable MOS estimation for the default applications, by selecting **Enable MOS**.

Note

Enable the Track Performance option under Rules to estimate MOS for applications and display it in SD-WAN Center. For more information about rules, see [How to View MOS for Applications](#).

Application Classification

Mar 01, 2018

NetScaler SD-WAN has an integrated Deep Packet Inspection (DPI) library that enables real-time discovery and classification of applications. Using the DPI technology, the SD-WAN appliance analyses the incoming packet and classifies it as belonging to a particular application or application family.

NetScaler SD-WAN also has the ability to classify the following features of HDX traffic as ICA application with “Citrix Protocol”.

- ICA
- ICA-CGP
- Single Stream ICA
- Multi-Stream ICA
- ICA over TCP
- ICA over UDP/UDT
- ICA over non-standard ports (Multi-ports)
- HDX Adaptive Transport protocol
- HTML5 receivers

Note

Classification of ICA over SSL is currently not supported. HDX priority tag based QoS will continue to be supported on SD-WAN Enterprise Edition appliances.

Classification of network traffic is done during initial connections or flow establishment, therefore, pre-existing connections will not be classified as ICA. Classification of connection will also be lost when connection table is cleared manually.

Legacy FrameHawk HDX traffic, which is getting replaced with HDX Adaptive Transport Protocol, is not classified as HDX applications. It is reported as either UDP or ‘Unknown Protocol’. Similarly, audio over RTP/UDP, if configured, is not classified as ICA traffic.

Once classified, ICA application can be used in application rules and to view application statistics similar to other classified applications.

There are five default application rules for ICA applications one each for the following priority tags:

- ICA
- ICA Priority 0 (ICA Real-Time)
- ICA Priority 1 (ICA Interactive)
- ICA Priority 2 (ICA Bulk-Transfer)
- ICA Priority 3 (ICA Background)

For more information, see [Rules by Application Name](#).

As priority tag based HDX classification is not available in SD-WAN Standard Edition appliances the four App rules; ICA priority 0 to 3 are not in effect.

To classify HDX on non-standard ports as configured in XA/XD server policy you must add those ports in ICA port configurations. Additionally, in order to match traffic on those ports to valid IP rules, you must update ICA IP rules.

In ICA IP and port list you can specify non-standard ports used in XA/XD policy to process for HDX classification. IP address is used to further restrict the ports to specific destination. Use '*' for port destined to any IP address. IP address with combination of SSL port is also used to indicate that the traffic is likely ICA even though traffic is not finally classified as ICA. This indication is used to send L4 AppFlow records to support multi-hop reports in MAS.

Classifying Encrypted Traffic

NetScaler SD-WAN detects and reports encrypted traffic, as part of application reporting, in the following two methods:

- For HTTPS traffic, the DPI engine inspects the SSL certificate to read the common name, which carries the name of the service (for example - Facebook, Twitter). Depending on the application architecture only one certificate may be used for several service types (for example - email, news and so on). If different services utilize different certificates, the DPI engine would be able to differentiate between services.
- For applications that utilize their own encryption protocol, the DPI engine looks for binary patterns in the flows, for instance in case of Skype the DPI engine looks for a binary pattern inside the certificate and determines the application.

To configure application classification settings:

1. In the **Configuration Editor**, click **Global > Applications > Settings**.

Settings

Enable Deep Packet Inspection

Enable Deep Packet Inspection for Citrix ICA Applications

Citrix ICA Deep Packet Inspection Settings

Enable Multi-Stream ICA

DPI ICA IP and Port List

DPI ICA IP-1:	DPI ICA Port-1:
<input type="text" value="192.168.29.2/4"/>	<input type="text" value="2599"/>
DPI ICA IP-2:	DPI ICA Port-2:
<input type="text" value="192.170.29.3/5"/>	<input type="text" value="2600"/>
DPI ICA IP-3:	DPI ICA Port-3:
<input type="text" value="192.170.100.3/5"/>	<input type="text" value="2601"/>
DPI ICA IP-4:	DPI ICA Port-4:
<input type="text" value="192.160.23.3/5"/>	<input type="text" value="8008"/>
DPI ICA IP-5:	DPI ICA Port-5:
<input type="text"/>	<input type="text"/>

Apply

Revert

2. Select **Enable Deep Packet Inspection**. This enables application classification on the appliance. You can, view, and monitor application statistics on the SD-WAN Center. For more information, see [How to View Application Statistics](#).

Note

By default, **Enable Deep Packet Inspection** will collect statistics for classified data.

3. Select **Enable Deep Packet Inspection for Citrix ICA Applications**. This enables classification of Citrix ICA applications and collects statistics for user, sessions and flow counts. Without this option enabled, some of the flavor of HDX traffic may still be classified and QoE calculated but statistics on SD-WAN center will not be available. You can, view, and monitor ICA application statistics on the SD-WAN Center. This option is enabled by default. For more information, see [How to View HDX Reports](#).

4. Select **Enable Multi-stream ICA** to allow multiple ICA streams in a session. This option is disabled by default and should only be enabled to provide QoS per stream type.

5. In **DPI ICA Port**, specify non-standard ports used in XA/XD policy to process for HDX classification. Do not include standard port numbers 2598 or 1494 in this list, as these are already included internally.

6. In **DPI ICA IP**, specify the IP address to be used to further restrict the ports to specific destination.

Note

Use '*' for port destined to any IP address.

7. Click **Apply**

You can configure application classification settings at each site individually. Click **Connections**, select a site and click **Applications Settings**. You can also choose to use the global application settings.

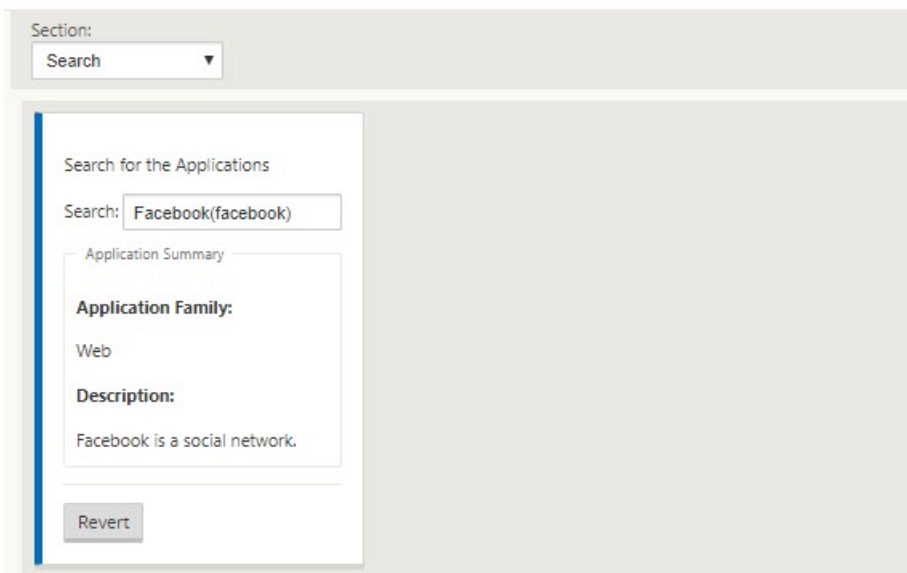
Search Applications

You can search for an application to determine the application family name. A brief description of the application is also provided.

To search for an application:

1. In the Configuration Editor, click **Global > Applications > Search**.
2. In the **Search** field type the name of the application and hit enter.

A brief description of the Application and the Application Family name appears.



Note

For information on applications that the SD-WAN appliance can identify using Deep Packet Inspection, see [Application Signature Library](#).

Application Objects

Application objects enable you to group different types of match criteria into a single object that can be used in firewall policies and application steering. IP Protocol, Application, and Application Family are the available match types.

To create an application object:

1. In the Configuration Editor, click **Global > Applications > Application Objects**.
2. Click **Add** and, in the **Name** field, enter a name for the object.

Match Type	Application Family	Application	Protocol	Network IP Address 1	Port 1
Application		Salesforce(salesforce)	Any	192.168.3.4/3	*
Application		Onjira.com (JIRA)(jira)	Any	192.168.4.4/3	*

3. Select **Enable Reporting** to enable viewing custom application reports in SD-WAN Center. For more information see, [How to View Application Statistics](#).

4. In the **Priority** field, enter the priority of the application object. When the incoming packets match two or more

application object definitions, the application object definition with the highest priority is applied.

5. Click **+** in the **Application Match Criteria** section.
6. Select one of the following match types:
 - **IP Protocol:** Specify the protocol, network IP address, port number, and, DSCP tag.
 - **Application:** Specify the application name, network IP address, port number, and, DSCP tag.
 - **Application Family:** Select an application family and specify the network IP address, port number, and, DSCP tag.
7. Click **+** to add more application match criteria.
8. Click **Add**.

Using Application Classification with a Firewall

The classification of traffic as applications and application families enables you to use the application, application families and application objects as match types to filter traffic and apply firewall policy and rules. This applies for all Pre, Post and local policies. For more information about firewall, see [Stateful Firewall and NAT Support](#).

Edit Firewall Policy ? x

Priority: 100

From Zones

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

To Zones

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

Action: Allow Log Interval (s): 0 Log Start Log End Connection State Tracking: Use Site Setting

Match Type: IP Protocol Application Application Family Application Objects

Application Objects: Any Application: Application Family:

DSCP: Any Allow Fragments Reverse Also Match Established

Source Service Type: Any Source Service Name: Any Source IP: * Source Port: *

Dest Service Type: Any Dest Service Name: Any Dest IP: * Dest Port: *

Apply Cancel

QoS Fairness (RED)

Mar 01, 2018

The QoS fairness feature improves the fairness of multiple virtual path flows by using QoS classes and Random Early Detection (RED). A virtual path can be assigned to one of 16 different classes. A class can be one of three basic types:

- Realtime classes serve traffic flows that demand prompt service up to a certain bandwidth limit. Low latency is preferred over aggregate throughput.
- Interactive classes have lower priority than realtime but have absolute priority over bulk traffic.
- Bulk classes get what is left over from realtime and interactive classes, because latency is less important for bulk traffic.

Users specify different bandwidth requirements for different classes, which enables the virtual path scheduler to arbitrate competing bandwidth requests from multiple classes of the same type. The scheduler uses the Hierarchical Fair Service Curve (HFSC) algorithm to achieve fairness among the classes.

HFSC services classes in first-in, first-out (FIFO) order. Before scheduling packets, NetScaler SD-WAN examines the amount of traffic pending for the packets' class. When excessive traffic is pending, the packets are dropped instead of being put into the queue (tail dropping).

Why Does TCP Cause Queuing?

TCP cannot control how quickly the network can transmit data. To control bandwidth, TCP implements the concept of a bandwidth window, which is the amount of unacknowledged traffic that it will allow in the network. It initially starts with a small window and doubles the size of that window whenever acknowledgments are received. This is called the slow start or exponential growth phase.

TCP identifies network congestion by detecting dropped packets. If the TCP stack sends a burst of packets that introduce a 250 ms delay, TCP does not detect congestion if none of the packets are discarded, so it continues to increase the size of the window. It might continue to do so until the wait time reaches 600-800 ms.

When TCP is not in the slow start mode, it reduces the bandwidth by half when packet loss is detected, and increases the allowed bandwidth by one packet for each acknowledgment received. TCP therefore alternates between putting upward pressure on the bandwidth and backing off. Unfortunately, if the wait time reaches 800ms by the time packet loss is detected, the bandwidth reduction causes a transmission delay.

Impact on QoS Fairness

When TCP transmission delay occurs, providing any kind of fairness guarantee within a virtual-path class is difficult. The virtual path scheduler must apply tail-drop behavior to avoid holding enormous amounts of traffic. The nature of TCP connections is such that a small number of traffic flows to fill the virtual path, making it difficult for a new TCP connection to achieve a fair share of the bandwidth. Sharing bandwidth fairly requires making sure that bandwidth is available for new packets to be transmitted.

Random Early Detection

Random Early Detection (RED) prevents traffic queues from filling up and causing tail-drop actions. It prevents needless queuing by the virtual path scheduler, without affecting the throughput that a TCP connection can achieve.

How To Use RED

1. Start a TCP session to create the virtual path. Verify that with RED enabled, the wait time on that class stays at around 50 ms in the steady state.
2. Start a second TCP session and verify that the both TCP sessions share the virtual path bandwidth evenly. Verify that the wait time on the class stays at the steady state.
3. Verify that the Configuration Editor can be used to enable and disable RED and that it displays the correct value for the parameter.
4. Verify that the View Configuration in the SD-WAN GUI page displays whether RED is enabled for a rule.

How To Enable RED

1. Navigate to **Configuration editor > Connections > Virtual Paths > [Select Virtual Path] > Rules > Select Rule**, for example; **(VOIP)**.
2. Expand the **LAN to WAN** pane. Under **LAN to WAN** section, click the **Enable RED** checkbox to enable it for TCP based rules.

Virtual Path to Site: NSSDWANVPX_MCN-NSSDWAN1kBranch Section: Rules + Add Virtual Path Delete Virtual Path

Order	Rule Group Name	IP Address			Protocol	Protocol #	Port			DSC
		Source	Dest=Src	Dest			Source	Dest=Src	Dest	
100	IPERF	10.102.29.3/5	<input checked="" type="checkbox"/>	*	Any	0	*	<input checked="" type="checkbox"/>	*	Any

Initialize Properties Using Protocol

WAN General

LAN to WAN

General

Class: <Default>

Drop Limit (ms): 50 Drop Depth: 128000

Large Packet Size (bytes): 0

Enable RED

Large Packets

Drop Limit (ms): 0 Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0 Disable Depth (bytes): 128000

MPLS Queues

Mar 01, 2018

This feature simplifies creating SD-WAN configurations when adding a Multiprotocol Label Switching (MPLS) WAN Link. Previously, each MPLS queue required one WAN Link to be created. Each WAN Link required a unique Virtual IP Address (VIP) to create the WAN Link and a unique Differentiated Services Code Point (DSCP) tag corresponding to the provider's queuing scheme. After defining a WAN Link for each MPLS queue, the Intranet Service to map to a specific queue is defined.

Currently, a new MPLS specific WAN Link definition (i.e., Access Type) is available. When a new Private MPLS Access Type is selected, you can define MPLS queues associated with the WAN Link. This allows a single VIP with multiple DSCP tags that correspond to the provider's queuing implementation for the MPLS WAN Link. This maps the Intranet Service to multiple MPLS Queues on a single MPLS WAN Link.

Allows MPLS providers to identify traffic based on DSCP markings so that class of service can be applied by the provider.

Note

If you have existing MPLS configurations and would like to implement the Private MPLS Access Type, please contact Citrix Support for assistance.

Configuring Private MPLS WAN Links

1. Define the WAN Link Access Type as Private MPLS.
2. Define the MPLS Queues corresponding to the Service Provider MPLS queues.
3. Enable the WAN Link for virtual path service (enabled by default for Private MPLS WAN Links).
4. From the virtual path on a WAN Link, assign an Autopath group.

Note

If the Autopath Group is assigned from the WANLink level, SD-WAN creates paths automatically between the MCN and Client MPLS Queues based on matching DSCP tags. If the Autopath Group is assigned from the MPLS Queue level, SD-WAN creates paths automatically regardless of whether or not the DSCP tags match.

5. Ensure that the same Autopath Group is configured at the MCN and Client.
6. Verify that the Paths for the WAN Link are built automatically.
7. Assign Intranet Service to a specific queue, if needed.

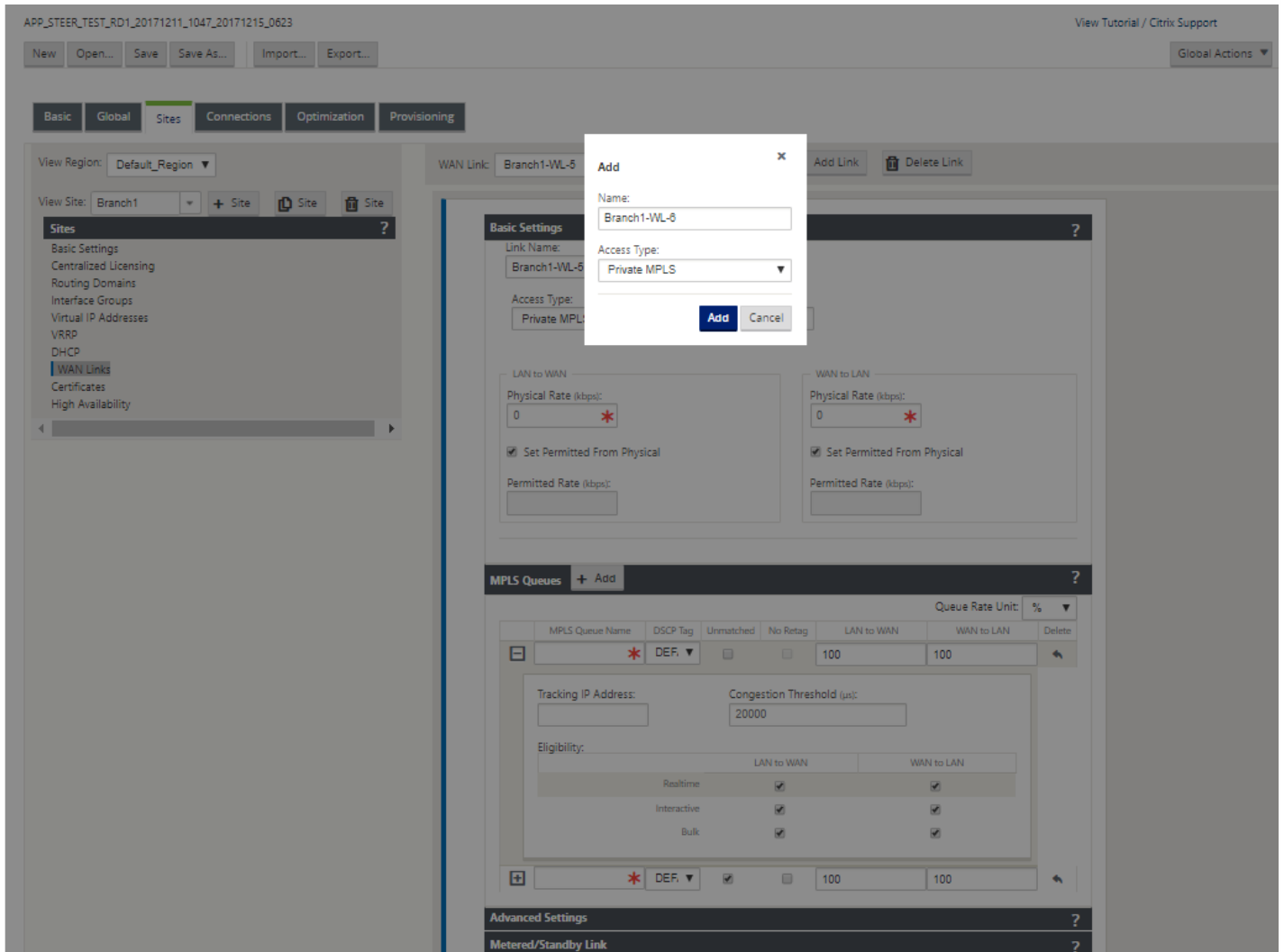
Note

The SD-WAN configuration may not have a one-to-one mapping for provider-based queues. This is based on specific deployment scenarios. You cannot create Autopath Groups between different Private Access Types. For instance, you cannot create Autopath Groups between a Private Internet Access Type and a Private MPLS Access Type.

How to Add Private MPLS WAN LINK

To configure new WAN Link Access Type for Private MPLS

1. In the Configuration Editor, navigate to **Sites > [Site Name] > WAN Links**. Click **Add Link**. Enter WAN Link name and select **Private MPLS** as the Access Type.



2. Under the **Basic Settings**, there is now a new **MPLS Queues** tab. Click + Add to add specific MPLS Queues. These should correspond with the queues defined by the Service Provider.

Field	Description
MPLS Queue Name	The MPLS queue name
DSCP Tag	Service Provider's DSCP tag setting for the queue.
Unmatched	When enabled, any frames arriving that do not match defined tags within the configuration file are mapped to this queue and the bandwidth defined for this queue.

Field	Description
Rate (kbps)	defined physical upload rate of the WAN Link.
WAN to WAN Permitted Rate (kbps)	The amount of bandwidth that SD-WAN devices are permitted to use for download, which cannot exceed the defined physical download rate of the WAN Link.

Expand the MPLS Queue definition (by clicking the +), and additional options appear. These options include:

Field	Description
Tracking IP Address	WAN Link tracking address
Congestion Threshold	The defined amount of time for congestion (in microseconds) after which the MPLS Queue will throttle packet transmission to avoid additional congestion. When congestion exceeds the set Threshold, SD-WAN backs off the sending rate.
Eligibility	The MPLS Queue's eligibility to process specific classes of traffic. When eligibility is disabled for a specific class of traffic, that class of traffic is unlikely to route through the MPLS Queue unless network conditions require it.

Configure the MPLS Queues that correspond to the existing Service Provider WAN Link queue definitions.

Note

Any existing MPLS WAN Links that are configured prior to SD-WAN 9.1 are not impacted.

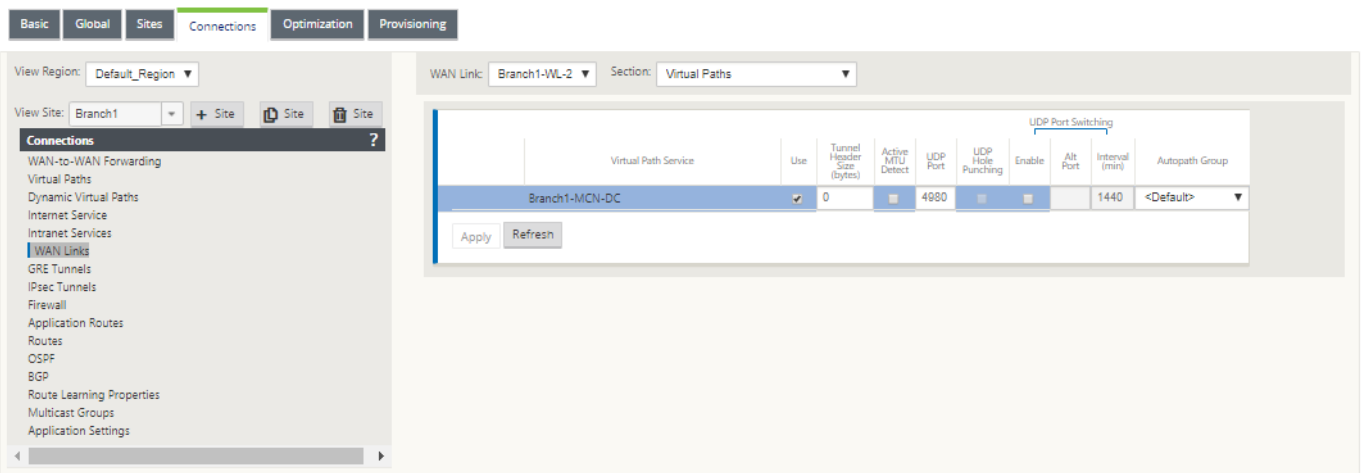
Define WAN Link Properties for Private MPLS

Once the Private MPLS WAN Link with its MPLS Queues is defined, you should assign an Autopath Group for the WAN Link under a specific Virtual Path definition.

To assign autopath group

1. Go to **Connections** > [Site Name] > **WAN Links** > [MPLS WAN Link Name] > **Virtual Paths** > [Virtual Path Name] > [Local Site] > **WAN Links** and click **Edit** ().

2. Click the **Autopath Group** drop-down menu and choose from the available groups. By default, MPLS Queues inherit the Autopath Group assigned to the MPLS WAN Link. You may choose to set the individual MPLS Queues to Inherit the chosen Autopath Group or choose an alternate from the Autopath Group drop-down menu for each MPLS Queue.



Note

If there is no one-to-one mapping, based on DSCP tag, between queues at the local site and the remote site, you must map MPLS Queues to specific Autopath Groups. Inheriting an Autopath Group from the MPLS WAN Link will only automatically generate paths between queues with matching DSCP tags.

Assign Autopath Group to Virtual Path-WAN Link

The Autopath Group defined is the same for the MCN and Client appliance. This allows the system to build the Paths automatically. At the MCN site you can also expand the WAN Link associated with the virtual path.

View Permitted Rate and Congestion for WAN Links

The SD-WAN web interface now allows you to view the permitted rate for WAN Links and WAN Link Usages and whether a WAN Link, Path, or Virtual Path may be in a congested state. In the previous releases, this information was only available in SD-WAN log files and through the CLI. These options are now available in the web interface to assist in troubleshooting.

View Permitted Rate

Permitted Rate is the amount of bandwidth that a particular WAN Link, Virtual Path Service, Intranet Service, or Internet Service is permitted to use at a given point in time. The permitted rate for a WAN Link is static, and is defined explicitly in the SD-WAN configuration. The permitted rate for a Virtual Path Service, Intranet Service, or Internet Service will fluctuate over time, in response to congestion, user demand, and Fair Shares, but will always be greater than or equal to the Minimum Reserved Bandwidth for the Service.

Monitor WAN Link

Go to **Monitor** > **Statistics**, and select **WAN Link** from the **Show** drop-down menu.

Monitoring > Statistics

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 5 of 5 entries First Previous 1 Next Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
BRANCH1-WL-1	N/A	172.186.20.7	N/A	N/A	N/A	N/A
BRANCH1-WL-2	N/A	172.186.30.2	N/A	N/A	N/A	N/A
BRANCH2-WL-1	N/A	172.186.75.2	N/A	N/A	N/A	N/A
DC-WL-1	DC-WL-1-AI-1	172.186.40.2	N/A	DISABLED	N/A	N/A
DC-WL-2	DC-WL-2-AI-1	172.186.50.2	N/A	DISABLED	N/A	N/A

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

Monitor MPLS Queues

Go to **Monitor > Statistics**, and select **MPLS Queues** from the **Show** drop-down menu.

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

MPLS Queue Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries Processing... First Previous 1 Next Last

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

Showing 1 to 4 of 4 entries First Previous 1 Next Last

Virtual Path Service Data Rates

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

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

Showing 1 to 4 of 4 entries First Previous 1 Next Last

Reporting

Mar 01, 2018

[Application QoE](#)

[Multiple Net Flow Collectors](#)

Application Quality of Experience (QoE)

Mar 01, 2018

Network parameters such as latency, jitter and packet drop affect the user experience of HDX users. Quality of Experience (QoE) is introduced to help the users understand and check their ICA quality of experience. QoE is a calculated index, which indicates the ICA traffic performance. The users can tune the rules and policy to improve the QoE.

The QoE is a numeric value between 0–100, the higher the value the better the user experience. QoE is enabled by default for all ICA / HDX applications.

The parameters used to calculate QoE is measured between the two SD-WAN appliances at the client side and server side and not, end to end, between the sever and the client. Latency, jitter and packet drop are measured at the flow level and it could be different from the statistics at the link level. The end host (client or server) application may never know that there is a packet loss on the WAN. If the retransmit succeeds, the flow level packet loss rate is lower than the link level loss. However, as a result, it may increase latency and jitter a bit.

Default configuration for HDX traffic enables SD-WAN to re-transmit packets, thus improves the QoE index value that was lost due to packet loss in the network.

In the SD-WAN Center dashboard, you can view a graphical representation of the overall quality of HDX applications. The HDX applications are classified into the following three quality categories:

Quality	QoE Range
Good	80–100
Fair	50–80
Poor	0–50

A list of the bottom five sites with the least QoE is also displayed in the NetScaler SD-WAN Center dashboard.

A graphical representation of the QoE for different time intervals allows you to monitor the performance of HDX applications at each site.

For more information, see [SD-WAN Center Dashboard](#).

You can also view the detailed HDX reports of each site on the NetScaler SD-WAN Center. For more information see, [How to View HDX Reports](#).

Note

- *Do not expect the WAN link latency, jitter, and packet drop would always match application latency, jitter and packet drop. WAN Link loss correlates to the actual WAN packet loss, while application loss is after retransmit, which is usually lower than WAN link loss.*
- *WAN Link latency displayed in the GUI is BOWT (Best One Way Time). It is the best metrics of the link as a means to gauge the health of the link. The application QoE tracks and calculates the total and average latency of all the packets for that application.*

This often does not match the link BOWT.

- *When an MSI session starts, during ICA handshake, the session might be temporarily counted as 4 SSI instead of 1 MSI. After the handshake is complete, it will converge to 1 MSI. If the conversion happens before the SQL table is updated, it may show up in ICA_Summary for that minute.*
- *On session reconnect, since initial protocol information is not exchanged, SD-WAN is not able to identify MSI, hence each connection is counted as SSI information.*
- *For UDP connections, after the connection is closed, it could take up to 5 minutes for the connection to show as closed and updated in ICA_Summary. For TCP connections, after the connection is closed, it could take up to 2 minutes to show as closed in ICA_Summary.*
- *QoE of TCP sessions and UDP sessions may not be the same on the same path due to the inherent difference between TCP and UDP.*
- *If one user launches two virtual desktops, the number of users is counted as two.*

Multiple Net Flow Collectors

Mar 01, 2018

Net Flow Collectors provide the ability to collect IP network traffic as it enters or exits an SD-WAN interface. By analyzing the data provided by Net Flow, you can determine the source and destination of traffic, class of service, and the causes for traffic congestion. Citrix SD-WAN devices can be configured to send basic NetFlow version 5 statistical data to the configured NetFlow collector. Citrix SD-WAN provides NetFlow support for traffic flows that are obscured by the transport reliable protocol. Devices on the WAN edge of the solution lose capability to collect NetFlow records since they will only see the SD-WAN encapsulated UDP packets. NetFlow is supported on the Citrix SD-WAN Standard and Enterprise Edition appliances.

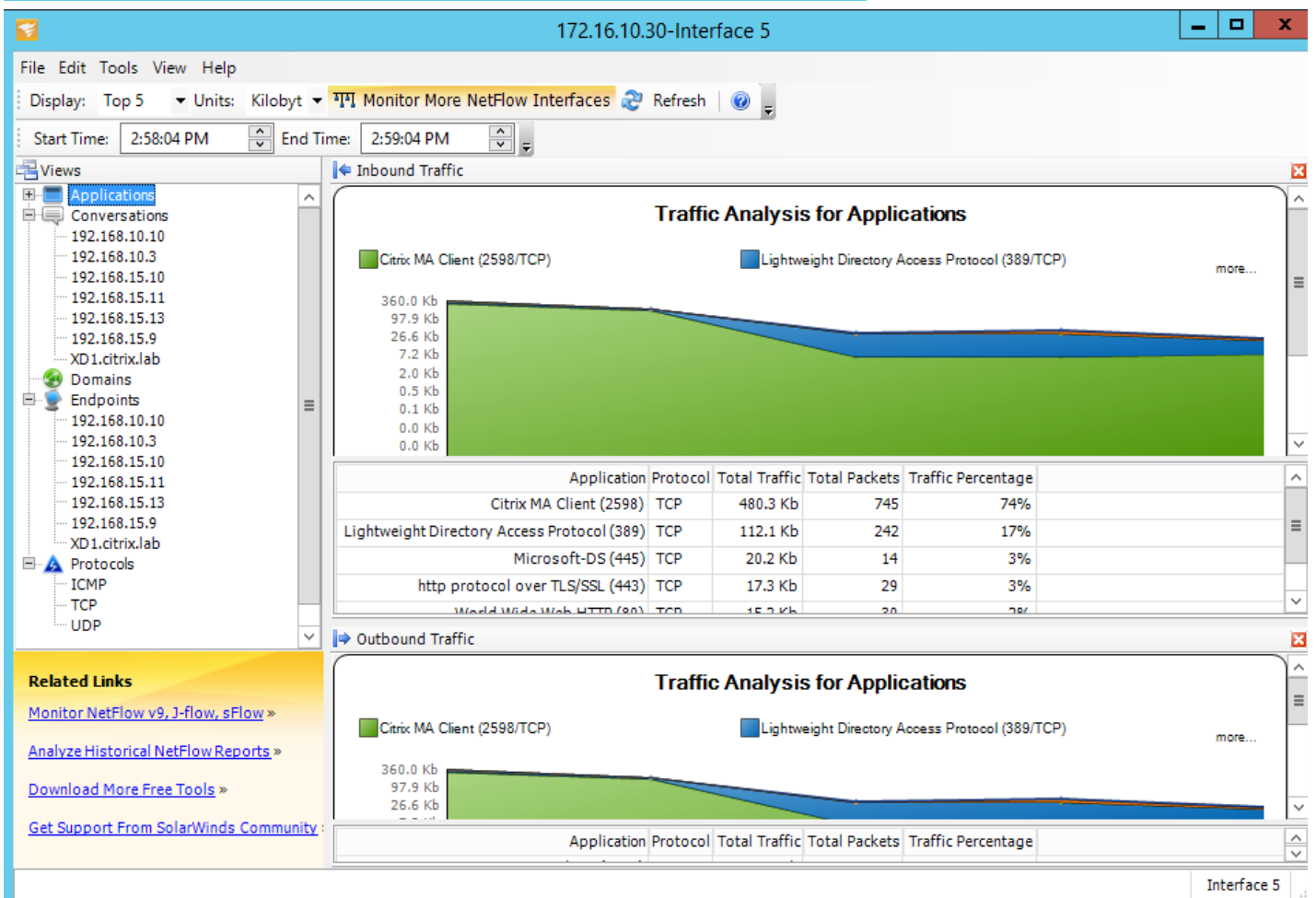
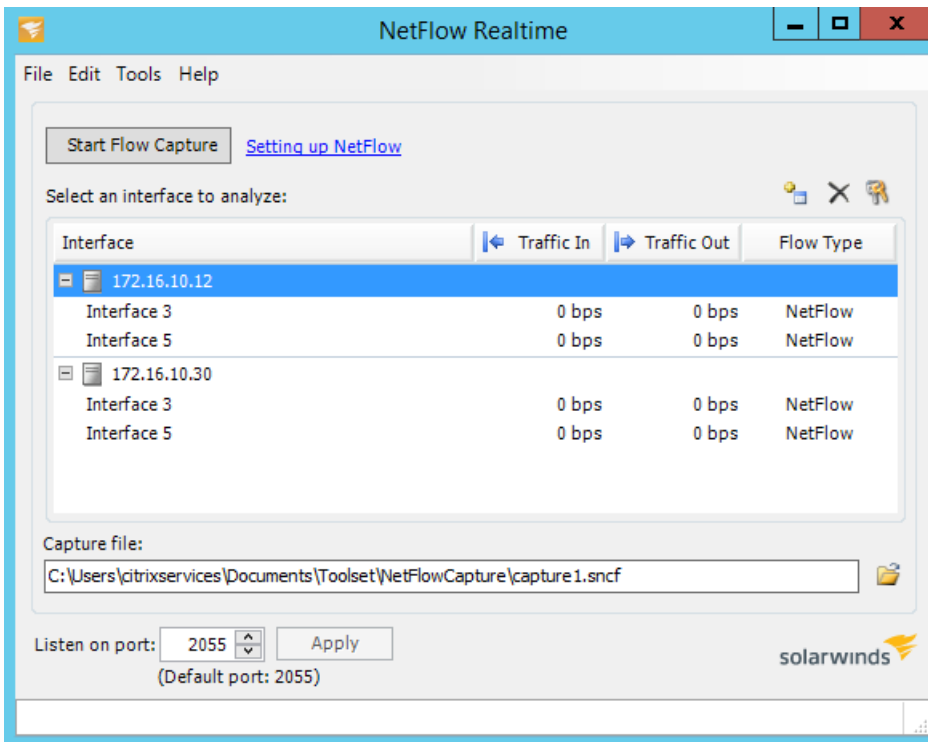
To configure Net Flow Hosts:

1. Navigate to **Configuration** → **Appliance Settings** → **Net Flow** → **Netflow Host Settings** page. Click the **Enable Netflow** checkbox, and enter the **IP Address**, and **Port** numbers for up to three Net flow Hosts, then click **Apply Settings** to save the changes.

The screenshot shows the 'NetFlow Host Settings' configuration page. The breadcrumb trail is 'Configuration > Appliance Settings > Net Flow'. The page title is 'NetFlow Host Settings'. There is a checkbox labeled 'Enable NetFlow' which is checked. Below this, there are three sections for configuring NetFlow hosts. The first section is 'NetFlow Host 1:' with an 'IP Address' field containing '192.168.15.10' and a 'Port' field containing '2055'. The second section is 'NetFlow Host 2: (Optional - can be left blank.)' with empty 'IP Address' and 'Port' fields. The third section is 'NetFlow Host 3: (Optional - can be left blank.)' with empty 'IP Address' and 'Port' fields. At the bottom of the form is a blue 'Apply Settings' button. On the left side of the interface, there is a navigation menu with 'Appliance Settings' expanded, and 'Net Flow' selected.

NetFlow Export

Netflow data is exported from the management port of the SD-WAN device. On your NetFlow collector tool, the SD-WAN devices will be listed as the configured management IP address, if SNMP is not configured. The interfaces will be listed as one for incoming and a second for outgoing (Virtual Path traffic).



NetFlow Limitations

- With NetFlow enabled on SD-WAN Standard and Enterprise Edition appliances, Virtual Path data is streamed to the

designated NetFlow collectors. One limitation with this is that one cannot differentiate which physical WAN link is being used by SD-WAN, as the solution reports aggregated Virtual Path information (A Virtual Path may comprise of multiple distinct WAN Paths), there is no way to filter the NetFlow records for the distinct WAN paths.

- TCP Control Bits report as N/A which indicates SD-WAN does not follow the internet standard for NetFlow exports based on [RFC 7011](#) which has element ID 6 for tcpControlBits ([IANA](#)). Without TCP Flags, calculating route trip time (RTT), latency, jitter, and other performance metrics in the flow data will not be possible. From the security side, without TCP flags, the NetFlow collector cannot determine if there are FIN, ACK/RST, or SYN scans occurring.

Routing

Mar 01, 2018

Virtual Routing and Forwarding (VRF)

VRF is an IP technology that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices.

Dynamic Routing

NetScaler SD-WAN introduces support for Dynamic Routing protocols. This feature facilitates discovery of LAN subnets, advertise virtual path routes to work more seamlessly within networks using the BGP and OSPF protocols, allowing SD-WAN to be seamlessly deployed in an existing environment without the need for static route configurations and graceful router failover.

Route Filtering

For networks with Route Learning enabled, NetScaler SD-WAN provides more control over which SD-WAN routes are advertised to routing neighbors rather than advertising all or no routes. Export Filters are used to include or exclude routes for advertisement using OSPF and BGP protocols based on specific match criteria. Route filtering is implemented on LAN routes in an SD-WAN network (Data Center/Branch) and are advertised to a non-SD-WAN network through eBGP.

Route Summarization

Route summarization reduces the number of routes that a router must maintain. A summary route is a single route that is used to represent multiple routes. It saves bandwidth by sending a single route advertisement, reducing the number of links between routers. It saves memory because only one route address is maintained. The CPU resources are used more efficiently by avoiding recursive lookups.

VRRP

Virtual Router Redundancy Protocol (VRRP) is a widely used protocol that provides device redundancy to eliminate the single point of failure inherent in the static default-routed environment. VRRP allows you to configure two or more routers to form a group. This group appears as a single default gateway with one virtual IP address and one virtual MAC address.

NetScaler SD-WAN 10.0 supports VRRP version 2 and version 3 to inter-operate with any third party routers. The SD-WAN appliance acts as a master router and direct the traffic to use Virtual Path Service between sites. You can configure the SD-WAN appliance as the VRRP master by configuring the Virtual Interface IP as the VRRP IP and by manually setting the priority to a higher value than the peer routers. You can configure the advertisement interval and the preempt option.

Using CLI to Access Routing Functionality

In NetScaler SD-WAN 10.0, you can view additional information related to dynamic routing and the protocol status. Type the following command and syntax to access routing daemon and view the list of commands.

Code

COPY

dynamic_routing?

SD-WAN Overlay Routing

Mar 01, 2018

Introduction

NetScaler SD-WAN provides resilient and robust connectivity between remote sites, data centers, and cloud networks. The SD-WAN solution can accomplish this by establishing tunnels between SD-WAN appliances in the network enabling connectivity between sites by leveraging route tables that overlay the existing underlay network. SD-WAN route tables can fully replace or coexist with the existing routing infrastructure. This article below provides detailed routing configuration within the NetScaler SD-WAN network.

NetScaler SD-WAN Route Table

The SD-WAN configuration allows static route entries for specific sites, and route entries learned from the underlay network through supported routing protocols; such as OSPF, eBGP, and iBGP. Routes are not only defined by their next hop but by their service type. This determines how the route is forwarded. Below are the main service types in use:

- **Local Service:** This service denotes any route or subnet local to the SD-WAN appliance. This includes the Virtual Interface subnets (automatically creates local routes), and any local route defined in the route table (with a local next hop). The route is advertised to other SD-WAN appliances that have a Virtual Path to this local site where this route is configured when trusted as a partner.

Note

Be cautious when adding default routes, and summary routes as local routes as these can result in virtual path routes at other sites. Always check the route tables to make sure the correct routing is in effect.

- **Virtual Path** – This denotes any local route learned from a remote SD-WAN site; that is what is reachable down the virtual paths. These routes are normally automatic, however a virtual path route can be added manually at a site. Any traffic for this route is forwarded to the defined Virtual Path for this destination route (subnet).
- **Intranet** – This service denotes routes that are reachable through a private WAN link (MPLS, P2P, VPN etc.). For example, a remote branch that is on the MPLS network but does not have an SD-WAN appliance. It is assumed that these routes need to be forwarded to a certain WAN router. Intranet Service is not enabled by default. Any traffic matching this route (subnet) is classified as intranet for this appliance for delivery to a site that does not have an SD-WAN solution.

Note

Notice that when adding an Intranet route there is no next hop, but rather a forward to an IntranetService. The Service is associated with a given WAN link.

- **Internet** – This is similar to Intranet but is used to define traffic flowing to public Internet WAN links rather than private WAN links. One unique difference is that the Internet service can be associated with multiple WAN links and set to load

balance (per flow) or be active/backup. A default Internet routes gets created when internet service is enabled (it is off by default). Any traffic matching this route (subnet) is classified as Internet for this appliance for delivery to public internet resources.

Note

Internet Service routes can be advertised to the other SD-WAN appliances or prevented from being exported depending on whether you are backhauling Internet access over the Virtual Paths.

- **Passthrough** – This service acts as a last resort or override service when an appliance is in-line mode. If a destination IP address fails to match with any other route, then the SD-WAN appliance simply forwards it onto the WAN link next hop. A default route: 0.0.0.0/0 cost of 16 pass-through route is created automatically. Passthrough does not work when the SD-WAN appliance is deployed out of path or in Edge/Gateway mode. Any traffic matching this route (subnet) is classified as passthrough for this appliance. It is recommended that passthrough traffic be limited as much as possible.

Note

Passthrough can be useful when conducting a POCs to avoid having to configure a lot of routing, however be very careful in production because SD-WAN does not account for WAN link utilization for traffic sent to passthrough. It is also helpful when troubleshooting issues and you want to take a certain IP flow out of delivery over the Virtual Path.

- **Discard** - This is not a service but a last resort route that drops the packets if it matches. Normally this does not occur expect when the SD-WAN appliance is deployed out of path. You must have an Intranet service or local route as a catch all route, otherwise the traffic will be discarded as there is no passthrough service (even though a passthrough default route will be present).

The SD-WAN Configuration Editor enables route table customization for each available site:

The screenshot shows the Citrix SD-WAN configuration interface. The top navigation bar includes tabs for Basic, Global, Sites, Connections, Optimization, and Provisioning. The 'Connections' tab is active. On the left, there is a sidebar with a 'View Region' dropdown set to 'Default_Region' and a 'View Site' dropdown set to 'MCN1'. Below these are buttons for '+ Site', 'Site', and 'Site'. The sidebar menu includes 'Connections', 'WAN-to-WAN Forwarding', 'Virtual Paths', 'Dynamic Virtual Paths', 'Internet Service', 'Intranet Services', 'WAN Links', 'GRE Tunnels', 'IPsec Tunnels', 'Firewall', 'Application Routes', 'Routes', 'OSPF', 'BGP', 'Route Learning Properties', 'Multicast Groups', and 'Application Settings'. The main area displays a table of route table entries with columns for Order, Network IP Address, Cost, Service Type, Service Name, Gateway IP Address, Info, Edit, and Delete. The table contains 12 entries. At the bottom of the main area are 'Apply' and 'Refresh' buttons.

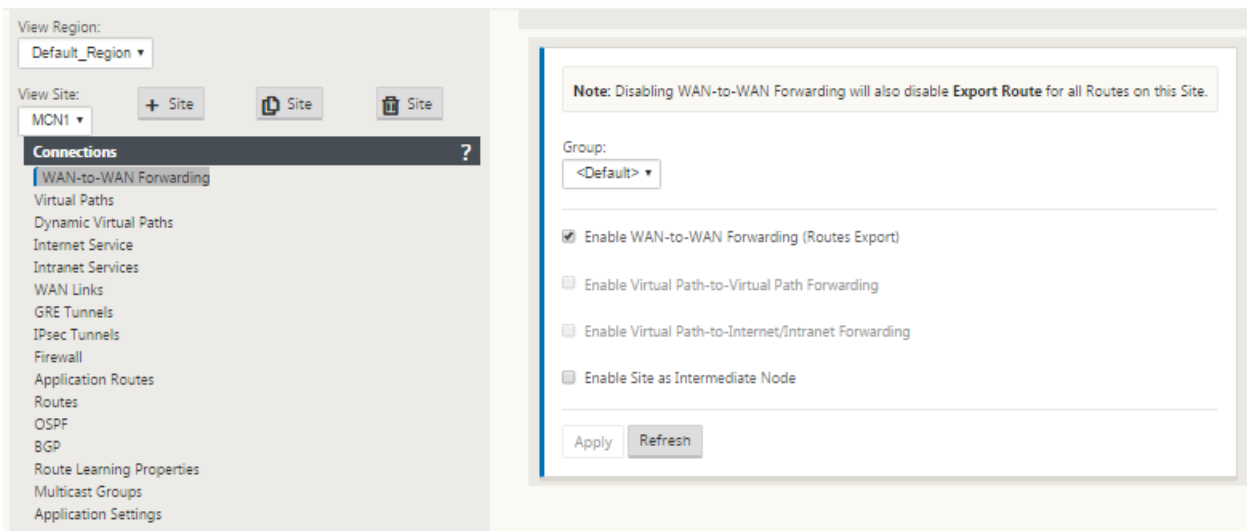
Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	172.120.21.100/32	5	Passthrough			ⓘ	✎	🗑️
2	172.120.21.64/32	4	Internet			ⓘ	✎	🗑️
3	172.120.21.65/32	4	Passthrough			ⓘ	✎	🗑️
4	172.120.24.64/32	4	Internet			ⓘ	✎	🗑️
5	10.101.0.0/22	5	Virtual Path	BR1		ⓘ	✎	🗑️
6	224.225.1.1/32	5	Multicast			ⓘ	✎	🗑️
7	224.225.1.2/32	5	Multicast			ⓘ	✎	🗑️
8	224.225.1.3/32	5	Multicast			ⓘ	✎	🗑️
9	172.120.24.7/24	5	Local			ⓘ	✎	🗑️
10	182.120.24.7/24	5	Local			ⓘ	✎	🗑️
11	0.0.0.0/0	5	Internet			ⓘ	✎	🗑️
12	0.0.0.0/0	65535	Passthrough			ⓘ	✎	🗑️

Route table entries are populated from different inputs:

- Configured Virtual IP Address (VIP) auto-populate as Service Type Local route. The Configuration Editor will prevent the same VIP assignment to different site nodes.
- Internet Services enabled at a local site will auto-populate a default route (0.0.0.0/0) locally for direct internet breakout.
- Admin defined static routes on a per site basis, which will also be defined as a Service Type Local route.
- A default (0.0.0.0/0) catch all route with cost 16 defined as Passthrough

Administrators can configure one of the above routes, but also include a service type, next hop, or gateway depending on the service type, in addition to route cost. A default route cost will automatically be added to each route type (reference the table below for default route costs). Additionally, only trusted routes are advertised to other SD-WAN appliances. Untrusted routes are only used by the local appliance.

Client node routes are only advertised to the MCN node and no other client nodes by default. In order for client node routes to be visible to another client nodes WAN to WAN Forwarding needs to be enabled at the MCN node.



With WAN-to-WAN Forwarding (Routes Export Template) enabled under Global settings, the MCN site will share the advertised routes to all clients participating in the SD-WAN overlay. Turning on this feature enables IP connectivity between hosts at different client node sites with the communication traveling through the MCN. The route table for the local client node can be monitored on the **Monitoring > Statistics** page with Routes selected for the **Show** drop-down.

- Statistics
- Flows
- Routing Protocols
- Firewall
- IKE/IPsec
- IGMP
- Performance Reports
- Qos Reports
- Usage Reports
- Availability Reports
- Appliance Reports
- DHCP Server/Relay
- VRRP Protocol

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh [Purge dynamic routes](#)

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 54 of 54 entries

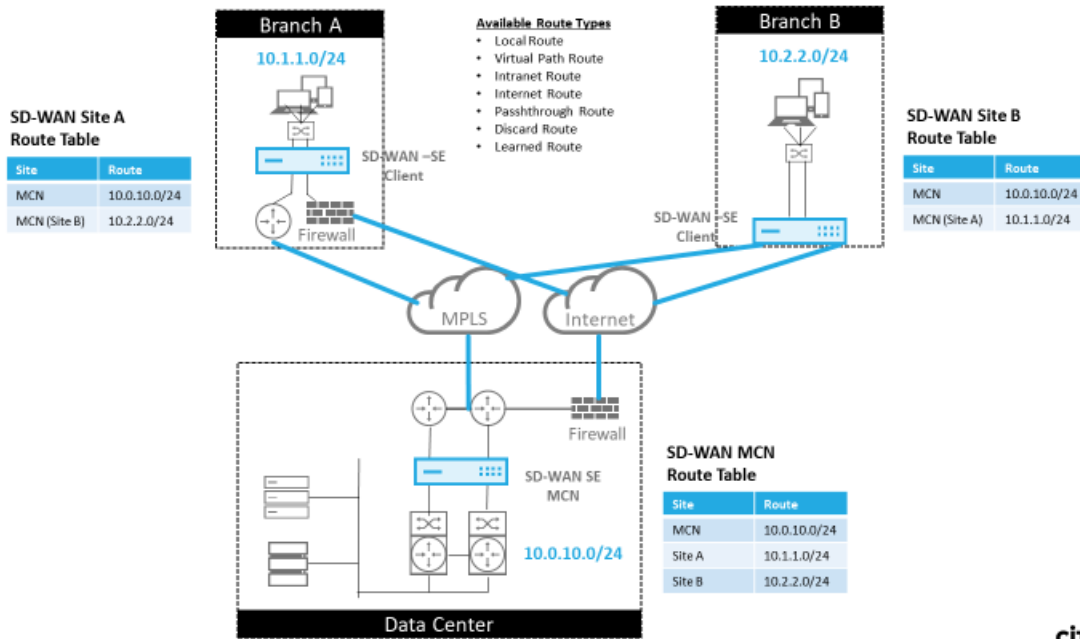
Num#	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
2	172.120.21.65/32	*	Passthrough	Any	YES	*	*	Static	-	-	4	0	YES	N/A	N/A
3	224.225.1.1/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
4	224.225.1.2/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
5	224.225.1.3/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
6	172.120.21.100/32	*	Passthrough	Any	YES	*	*	Static	-	-	5	0	YES	N/A	N/A
7	172.120.24.64/32	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	9	0	YES	N/A	N/A
8	172.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	3458	YES	N/A	N/A
9	182.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
10	172.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
11	172.120.21.0/24	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
12	182.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
13	192.168.255.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
14	192.172.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
15	192.172.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
16	192.172.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
17	192.172.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
18	192.172.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
19	192.172.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
20	192.172.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
21	192.172.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
22	192.172.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
23	192.172.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
24	192.172.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
25	192.172.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
26	192.172.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
27	192.172.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
28	192.172.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
29	192.172.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
30	192.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
31	172.108.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
32	172.108.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
33	172.108.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
34	172.108.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
35	172.108.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
36	172.108.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
37	172.108.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
38	172.108.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
39	172.108.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
40	172.108.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
41	172.108.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
42	172.108.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
43	172.108.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
44	172.108.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
45	172.108.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
46	172.108.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
47	10.101.0.0/22	*	MCN1-BR1	Any	YES	*	BR1	Static	-	-	5	0	YES	N/A	N/A
48	10.101.0.0/22	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
49	172.105.96.0/20	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
50	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	5	401109	YES	N/A	N/A
51	0.0.0.0/0	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
52	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	40031844	YES	N/A	N/A
53	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

Showing 1 to 54 of 54 entries

Each route for remote branch office subnets is advertised as a Service through the Virtual Path connecting through the MCN, with the Site column populated with the client node where the destination resides as a local subnet.

In the below example, with “**WAN-to-WAN Forwarding** (Routes Export)” enabled, Branch A has a route table entry for the Branch B subnet (10.2.2.0/24) through the MCN as a next hop.

SD-WAN Overlay Route Tables



35 © 2017 Citrix

CITRIX

How NetScaler SD-WAN Traffic Matches on Defined Routes

The match process for defined routes on NetScaler SD-WAN is based on longest prefix match for destination subnet (similar to a router operation). The more specific the route, the higher the change on it being matched. Beyond that, sorting is done in the following order:

1. Longest prefix match
2. Cost
3. Service

Therefore a /32 route always precedes a /31 route. For two /32 routes, a cost 4 route always precedes a cost 5 route. For two /32 cost 5 routes, routes are chosen based on ordered IP host. Service order is as follows: Local, Virtual Path, Intranet, Internet, Passthrough, Discard.

As an example, consider the following two routes below:

- 192.168.1.0/24 Cost 5
- 192.168.1.64/26 Cost 10

A packet destined for 192.168.1.65 host would use the latter route even though the cost is higher. Based on this, it is common for configuration to be in place for only the routes intended to be delivered over the Virtual Path overlay with other traffic falling into catch all routes such as a default route to the passthrough service.

Routes can be configured in a site node route table that have the same prefix. The tie break then goes to the route cost, the service type (Virtual Path, Intranet, Internet, etc.) and the next hop IP.

NetScaler SD-WAN Routing Packet Flow

- LAN to WAN (Virtual Path) Traffic Route Matching:
 1. Incoming traffic is received by the LAN interface and is processed.
 2. The received frame is compared to the route table for the longest prefix match.
 3. If a match is found, the frame is then processed by the rule engine and a flow is created in the flow database.
- WAN to LAN (Virtual Path) Traffic Route Matching:
 1. Virtual Path traffic is received by SD-WAN from the tunnel and is processed.
 2. The appliance compares the source IP address to see if the source is local.
 - If yes – then WAN eligible and match IP destination to routing table/Virtual Path.
 - If no – then WAN to WAN forwarding enabled check.
 3. (WAN to WAN Forwarding disabled) Forward to LAN based on local routes.
 4. (WAN to WAN Forwarding enabled) Forward to Virtual Path based on route table.
- Non Virtual Path Traffic:
 1. Incoming traffic is received on LAN interface and is processed.
 2. The received frame is compared to the route table for the longest prefix match.
 3. If a match is found, the frame is then processed by the rule engine and a flow is created in the flow database.

NetScaler SD-WAN Routing Protocol Support

NetScaler SD-WAN release 9.1 introduced OSPF and BGP routing protocols into the configuration. Introducing routing protocols to SD-WAN enabled easier integration of SD-WAN in more complex underlay networks where routing protocols are actively in use. With the same routing protocols enabled on SD-WAN, configuration of subnets denoted to make use of the SD-WAN overlay was made easier. In addition, the routing protocols enable communication between SD-WAN and non-SD-WAN sites with direct communication to existing customer edge routers using the common routing protocol.

NetScaler SD-WAN participating in routing protocols operating in the underlay network can be done regardless of the deployment mode of SD-WAN (Inline mode, Virtual Inline mode, or Edge/Gateway mode). Additionally, SD-WAN can be deployed in “learn only” mode where SD-WAN can receive routes but not advertise routes back to the underlay. This can be useful when introducing the SD-WAN solution into a network where the routing infrastructure is complex or uncertain.

Important

It is very easy to accidentally leak unwanted route, if you are not careful.

The SD-WAN Virtual Path route table works as an External Gateway Protocol (EGP), very similar to BGP (think site-to-site). For example, when SD-WAN advertises routes from the SD-WAN appliance to OSPF they are typically considered external

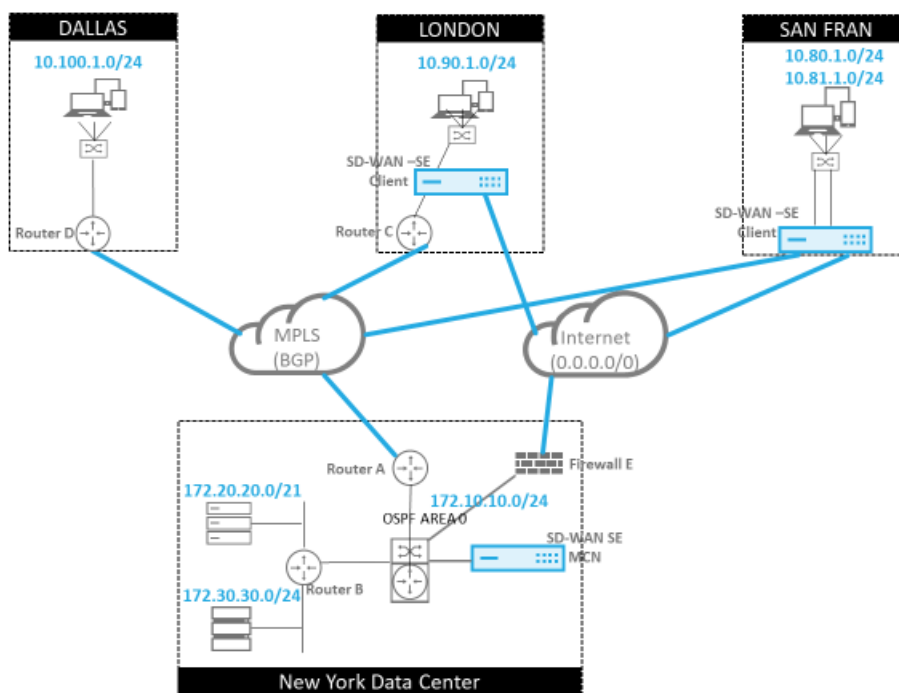
to site and protocol.

Note

Be aware of environments that have IGP across the entire infrastructure (across the WAN) as it does complicate how SD-WAN advertised routes are used. EIGRP is extensively used in the market and SD-WAN does not interop with that protocol.

One challenge in introducing Routing Protocols to an SD-WAN deployment is that the route table is not available until the SD-WAN service is enabled and operation in the network, therefore it is not recommended to enable advertise routes from the SD-WAN appliance initially. Use the import and export filters for a gradual introduction of routing protocols on SD-WAN.

Let us take a closer look by reviewing the following example:



37 © 2017 Citrix

CITRIX

In this example, we will examine a routing protocol use case. The above network has four locations; New York, Dallas, London, and San Francisco. We will deploy SD-WAN appliances at three of these locations, and utilize SD-WAN to create a hybrid WAN network where MPLS and Internet WAN Links will be used to provide a Virtualized WAN. Since Dallas will not have an SD-WAN device, we need to consider how to best integrate with existing route protocols to that site to ensure full connectivity between underlay and SD-WAN overlay networks.

In the example network, eBGP is used between all four locations across the MPLS network. Each location has its own Autonomous System Number (ASN).

In the New York Data Center, OSPF is running to advertise the core Data Center subnets to the remote sites and also announce a default route from the New York Firewall (E). In this example, all internet traffic is backhauled to the datacenter, even though London and San Francisco Branches have a path to the internet.

The San Francisco site also should be noted to not have a router. SD-WAN will be deployed in Edge/Gateway mode with that appliance being the default gateway for the San Francisco subnet and also participating in eBGP to the MPLS.

- With the New York Data Center, take note that the SD-WAN is deployed in Virtual Inline mode. The intent is to participate in the existing OSPF routing protocol to get traffic forwarded to the appliance as the preferred gateway.
- The London site is deployed in traditional inline mode. The upstream WAN Router (C) will still be the default gateway for the London subnet.
- The San Francisco site will be a newly introduced site to this network and the SD-WAN is planned to be deployed in Edge/Gateway mode and act as the default gateway for the new San Francisco subnet.

First, we will take a look at some of the existing underlay route tables before implementing SD-WAN.

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
```

The local New York subnets (172.x.x.x) are available on router B as directly connected, and from the route table we identify that the default route is 172.10.10.3 (Firewall E). Also, we can see that Dallas (10.90.1.0/24) and London (10.100.1.0/24) subnets are available via 172.10.10.1 (MPLS Router A). Note the route costs indicate they were learned from eBGP.

Note

In the example provided, San Francisco is not listed as a route, because we have not yet deployed the site with SD-WAN in Edge/Gateway mode for that network.

```

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

```

For the New York WAN Router (A), OSPF learned routes and routes learned across the MPLS through eBGP are listed routes. Note the route costs. BGP is lower administrative domain and cost by default 20/1 compared to OSPF 110/10.

Dallas Router D:

For the Dallas WAN Router (D) all routes are learned across the MPLS.

```

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

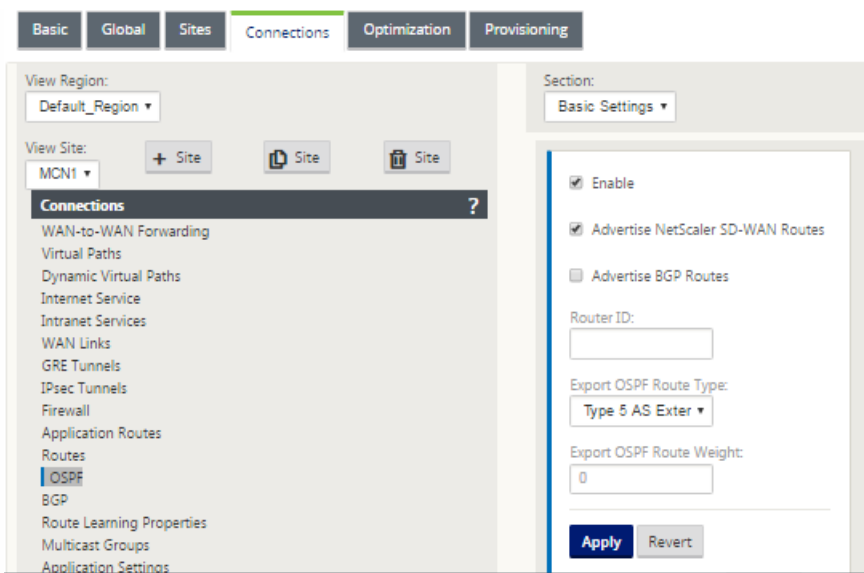
B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:10:17
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h10m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 1d23h10m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0

```

Note

In this example, you can ignore the 192.168.65.0/24 subnet. This is a management network and not pertinent to the example. All the Routers are connected to the management subnet but the is not advertised in any routing protocol.

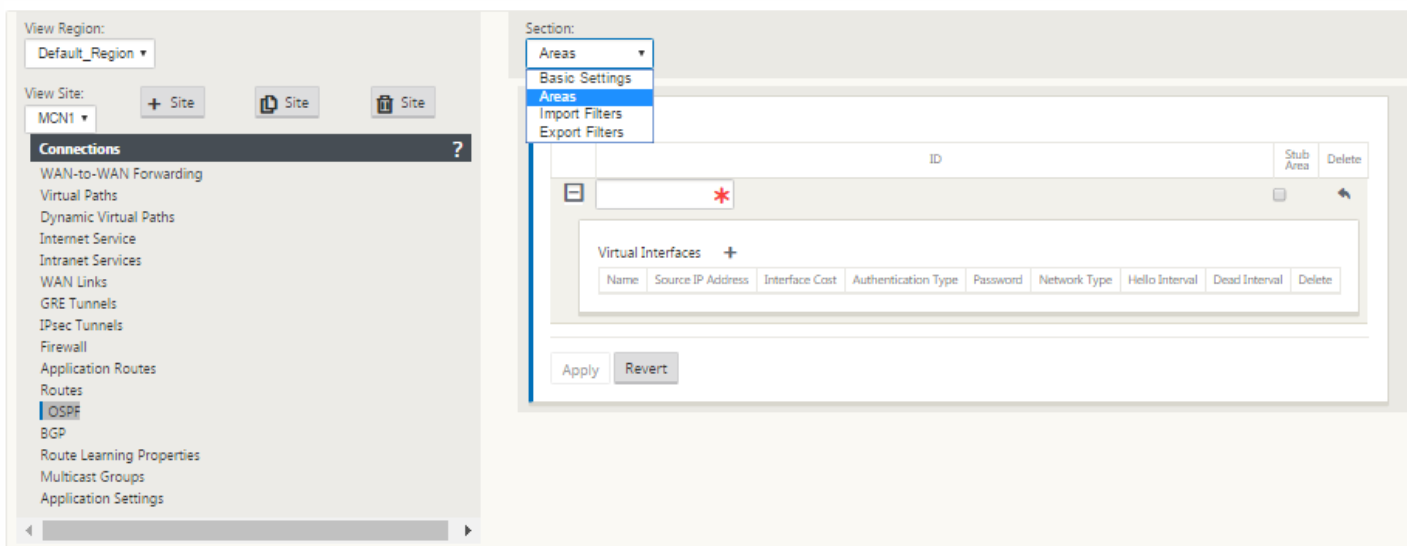
In NetScaler SD-WAN, we can add the SD-WAN overlay by enabling OSPF on the SD-WAN located in the New York site under **Connections > View Site > OSPF > Basic Settings**:



Note

The **Export OSPF Route Type** is Type 5 External by default. This is because SD-WAN routing table is considered external to the OSPF protocol and so OSPF will prefer a route learned internal (intra-area), therefore routes advertised by SD-WAN may not take precedence.

When OSPF is used across the WAN (i.e. MPLS networks), then this can be changed to Type 1 intra-area. OSPF areas can be configured as shown below.



Area 0 added with the local network derived from the Virtual Interface (172.10.10.0), all other settings were left default.

For the new San Francisco site, we will need to enable eBGP since it will be directly connected to the MPLS network and operating as the customer edge route for the site. BGP can be enabled under **Connections > View Site > BGP > Basic Settings**.

Note the Autonomous System number of 13.

Section: Basic Properties

Enable

Advertise NetScaler SD-WAN Routes

Advertise OSPF Routes

Router ID:
192.168.10.4

Local Autonomous System:
13

Apply Revert

Section: Neighbors

	Virtual Interface	Source IP	Neighbor IP	Neighbor AS	Hold Time(s)	Local Preference	IGP Metric	Multi Hop	Password	Delete
	V1	192.168.10.4	192.168.10.1	65011	3600	100		<input checked="" type="checkbox"/>		
Policies +										
	Order	Network Address	BGP Community(AA:NN)		AS Path	BGP Policy	Direction	Delete		
	(auto)	<Manual>	*	<Manual>	*	*	<Accept>			
	V1	192.168.10.4	192.168.10.2	65012	3600	100		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

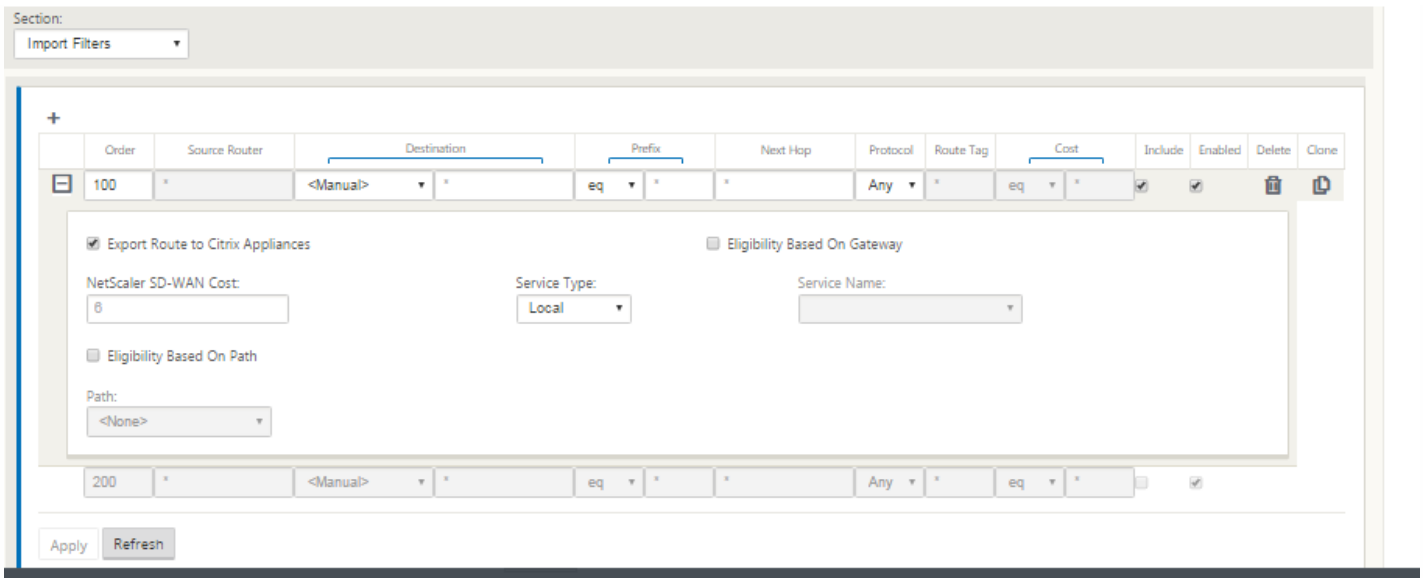
Apply Refresh

The eBGP peers with each other location. Note that each ASN is different.

It is important to understand how routes are passed between the Virtual Path routing table and the dynamic route protocols in use. It is easy to create routing loops or advertise routes in an adverse way. The filter mechanism gives us the ability to control what gets into and out of the routing table. We will consider each location in turn.

- The San Francisco location has two local subnets **10.80.1.0/24** and **10.81.1.0/24**. We want to advertise them through eBGP so that sites like Dallas can still reach the San Francisco site over the underlay network and also sites like London and San Francisco can still reach San Francisco over the Virtual Path overlay network. We also want to learn from eBGP reachability to all sites in case the SD-WAN Virtual Path overlay goes down and the environment needs to fall back to using just the MPLS. We also do not want to re-advertise anything SD-WAN learns from eBGP to the SD-WAN routers. In order to accomplish this, the filters need to be configured as follows:

- Import all routes from eBGP. Do not re-advertise/export routes to SD-WAN appliances.



- Export local routes to eBGP

The default rule for export is to export everything. Rule 200 is used to override the fault rule in order to not re-advertise the routes. Any route matching any prefix SD-WAN has learned across the Virtual Paths.

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

After the NetScaler SD-WAN appliances have been deployed, we can take a refreshed look at the route tables for the BGP router at the Dallas site. We see 10.80.1.0/24 and 10.81.1.0/24 subnets are being seen correctly through eBGP from the San Francisco SD-WAN.

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
```

Further, the NetScaler SD-WAN route table can be viewed on the **Monitoring > Statistics > Show Routes** page.

San Francisco NetScaler SD-WAN:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 16 of 16 entries

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 16 of 16 entries

NetScaler SD-WAN shows all the routes learned, including routes available through the Virtual Path overlay.

Let us consider 172.10.10.0/24, which is located in New York Data Center. This route is being learned in two ways:

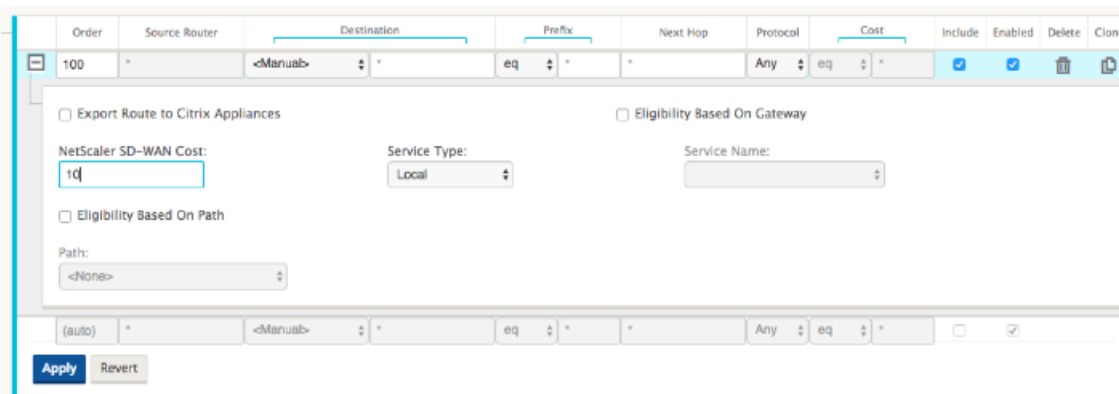
- As a Virtual Path route (Num 3), service = NYC-SFO with a cost of 5 and type static. This is a local subnet being advertised by SD-WAN appliance in New York. It is static in that it is either directly connected to the appliance or it is a manual static route entered in the configuration. It is reachable because the Virtual Path between the sites is in a working/up state.
- As an advertised route through BGP (Num 6), with a cost of 6. This is now considered a fallback route.

Since the prefix is equal and cost is different, SD-WAN will use the Virtual Path route unless it becomes unavailable, in which case the fallback route is learned through BGP.

Now, let us consider the route 172.20.20.0/24.

- This is learned as a Virtual Path route (Num 9) but has a type of dynamic and a cost of 6. This means the remote SD-WAN appliance learned this route through a routing protocol, in this case OSPF. By default the route cost is higher.
- SD-WAN also learns this route through BGP with the same cost, so in this case this route may be preferred over the Virtual Path route.

In order to ensure correct routing, we must increase the BGP route cost to make sure if we have a Virtual Path route and it will be the preferred route. This can be done by adjusting the import filter route weight to be higher than the default of 6.



After making the adjustment, we can refresh the SD-WAN route table on the San Francisco appliance to see the adjusted route costs. Make use of the filter option to focus the displayed list.

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)

Finally, let us look at the learned default route on the San Francisco SD-WAN. We want to backhaul all internet traffic to New York. We can see that we will send it using the Virtual Path, if it is up, or through the MPLS network as a 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)

We also see a passthrough and discard route with cost 16. These are automatic routes that cannot be removed. If the device is inline, the passthrough route is used as a last resort so if a packet cannot be matched to a more specific route, SD-WAN will pass it along to the next hop of the interface group. If the SD-WAN is out of path or in edge/gateway mode, there is no passthrough service, in which case SD-WAN drops the packet using the default discard route. The Hit Count indicates the number of packets that are hitting each route, which can be valuable when troubleshooting.

Now focusing on the New York site, we want to get traffic destined for remote sites (London and San Francisco) to be directed to the SD-WAN appliance when the Virtual Path is active.

There are multiple subnets available in the New York site:

- 172.10.10.0/24 (directly connected)
- 172.20.20.0/24 (advertised via OSPF from the core router B)
- 172.30.30.0/24 (advertised via OSPF from the core router B)

We also are required to still provide traffic flow to Dallas (10.100.1.0/24) through MPLS.

Lastly, we want all internet bound traffic route to the Firewall E through 172.10.10.3 as a next hop. SD-WAN learns this default route through OSPF and will need to advertise this across the Virtual Path. The filters for the New York site are:

Order	Source Router	Destination	Prefix	Next Hop	Protocol	Cost	Include	Enabled	Delete	Clone	
100	*	<Manual> 192.168.85.0/24	eq *	*	Any	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
<div style="border: 1px solid #ccc; padding: 5px;"> <input type="checkbox"/> Export Route to Citrix Appliances <input type="checkbox"/> Eligibility Based On Gateway NetScaler SD-WAN Cost: 6 Service Type: Local Service Name: <input type="checkbox"/> Eligibility Based On Path Path: <None> </div>											
+	200	*	<Manual> 192.168.10.0/24	eq *	*	Any	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
+	300	*	<Manual> *	eq *	*	Any	eq *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
	(auto)	*	<Manual> *	eq *	*	Any	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

The New York SD-WAN site will import all routes for the management network. This can be ignored. We can focus on filter 200.

Order	Source Router	Destination	Prefix	Next Hop	Protocol	Cost	Include	Enabled	Delete	Clone
200	*	<Manual> 192.168.10.0/24	eq *	*	Any	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<div style="border: 1px solid #ccc; padding: 5px;"> <input type="checkbox"/> Export Route to Citrix Appliances <input type="checkbox"/> Eligibility Based On Gateway NetScaler SD-WAN Cost: 6 Service Type: Local Service Name: <input type="checkbox"/> Eligibility Based On Path Path: <None> </div>										

Filter 200 is used to import 192.168.10.0/24 (our MPLS core) for reachability but it is not advertised across the Virtual Path overlay. All other routes are then included.

For the export filters, we can exclude route for 192.168.10.0/24. This is because, as a directly connected subnet in San Francisco site, we cannot filter this route out at the source, so it is suppressed at this end.

Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone	
+	100	<Manual> 192.168.10.0/24	eq *	eq *	Any	<Any>	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
	(auto)	<Manual> *	eq *	eq *	Any	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Now let us review the refreshed route table starting at the core route in New York site.

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

```

We can see the subnets for San Francisco (10.80.1.0 & 10.81.1.0) and London (10.90.1.0) now being advertised via the New York SD-WAN Appliance (172.10.10.10). The route 10.100.1.0/24 is still being advertised through the underlay MPLS Router A. Let us review the New York site SD-WAN route table.

New York site SD-WAN Route Table:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 11 of 11 entries

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

We can see the correct routes for both the local subnets learned via OSPF, a route to Dallas site learned from the MPLS Router A and the remote subnets for San Francisco and London sites. Lastly, let us look at the MPLS Router A. This router is participating in OSPF and 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

```

From the route table this Router A is learning the remote subnets through BGP and OSPF with the Administrative distance and cost of the BGP route (20/5) being lower than OSPF (110/10) and hence preferred. In this example, network where there is only one core route, this may not cause concern. However, traffic arriving here would be delivered via the MPLS network rather than being sent to the SD-WAN Appliance (172.10.10.10). If we want to maintain complete routing symmetry, we would need a route map to adjust the AD/Metric cost so that there is route preference from the route coming from 172.10.10.10 rather than the route learned via eBGP.

Alternatively, a “backdoor” route can be configured to force the router to prefer the OSPF route over the BGP route. astly, notice the static route for the SD-WAN Virtual IP address to the London site SD-WAN appliance.

```
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
```

This is necessary to ensure the Virtual Path is re-routed back to the New York site SD-WAN appliance if the MPLS path goes down. Since there is a route for the 10.90.1.0/24 being advertised via 172.10.10.10 (New York SD-WAN). It is also recommended to create an override service rule to drop any UDP 4980 packets at the SD-WAN appliance to prevent the Virtual Path from coming back to itself.

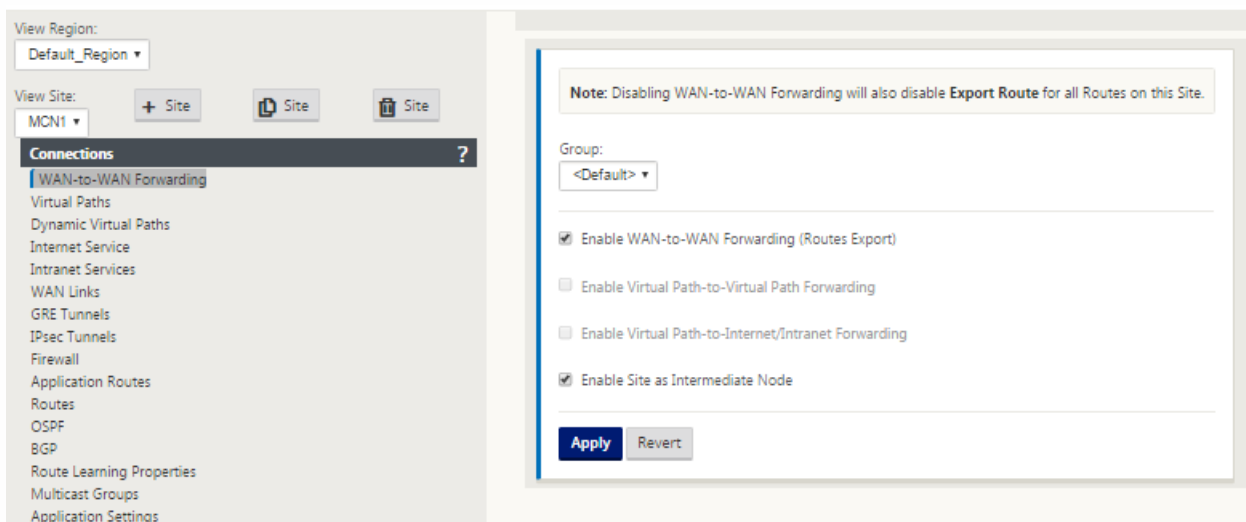
Dynamic Virtual Paths

Dynamic Virtual Paths can be allowed between two client nodes to build on-demand virtual paths for direct communication between two sites. The advantage of a dynamic virtual path is that traffic can flow directly from one client node to second without having to traverse the MCN or two virtual paths, which could add latency to the traffic flow. Dynamic virtual paths are built and removed dynamically based on user-defined traffic thresholds. These thresholds are defined as either packets per second (pps) or bandwidth (kbps). This functionality enables a dynamic full mesh SD-WAN overlay topology.

Once the thresholds for dynamic virtual paths are met, the client nodes dynamically create their virtualized path to one another leveraging all available WAN paths between the sites and make full use of it in the following manner:

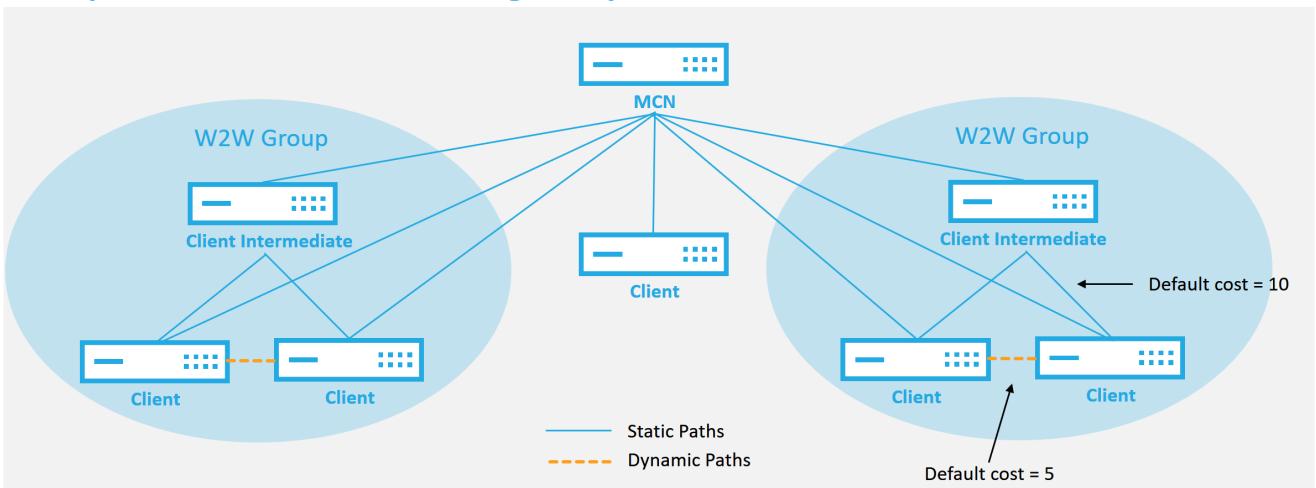
- Send Bulk data if any exists and verify no loss, then
- Send Interactive data and verify no loss, then
- Send Real Time data after the Bulk and Interactive data are considered stable (no loss or acceptable levels)
- If there is no Bulk or interactive data send Real Time Data after the Dynamic Virtual Path has been stable for a period of time
- If the user data falls below the configured thresholds for a user defined period of time, the dynamic virtual path is torn down

Dynamic Virtual Paths have the concept of an Intermediate site. The intermediate site could be an MCN site or any other site in the network that has Static Virtual Path configured and connected to two or more other client nodes. Another design consideration requirement is to have WAN-to-WAN Forwarding enabled, allowing all routes from all sites to be advertised to the client nodes where the dynamic virtual path is desired. **“Enable Site as Intermediate Node”** must be enabled in addition to **WAN-to-WAN Forwarding** in order for this intermediate site to monitor client node communication and to dictate when the dynamic path needs to be established and torn down.



Multiple WAN-to-WAN Forwarding Groups can be allowed in the SD-WAN configuration, enabling full control to path establishment between certain client nodes and not others.

Multiple WAN to WAN Forwarding Groups



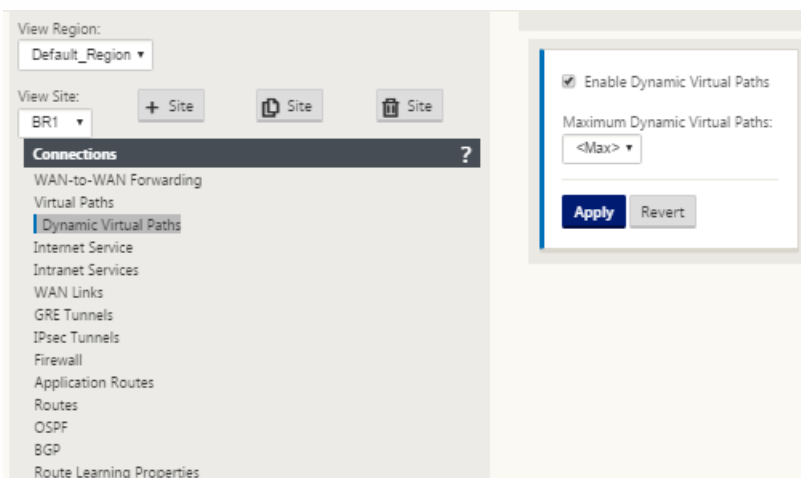
WAN to WAN Forwarding Group:

- 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

For client nodes to operate as Intermediate sites, a static Virtual Path is required to be configured between it and the clients that are associated with that **WAN-to-WAN Forwarding Group**. In addition, client nodes will need **Enable Dynamic Virtual Path** option turned on for each client node.



Each SD-WAN device will have its own unique route table with the following details defined for each route:

- Num – order of route of this appliance based on match process (lowest Num processed first)
- Network address – subnet or host address
- Gateway if required
- Service – what service is applied for this route
- Firewall Zone – the firewall zone classification of the route
- Reachable – Identifies if the Virtual Path state is active for this site

- Site – The name of the site where the route is expected to exist
- Type – Identification of route type (Static or Dynamic)
- Neighbor Direct
- Cost - cost of the specific route
- Hit Count – how many times the route has been used per packet. This would be used to verify that a route is being hit correctly.
- Eligible
- Eligibility Type
- Eligibility Value

Below is an example SD-WAN site route table:

Routes for routing domain : Default_RoutingDomain

Filter: in

Show entries Showing 1 to 13 of 13 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 13 of 13 entries

Notice from the above SD-WAN route table that there are additional elements not normally availability in traditional routers. Most notable is the “Reachable” column, which renders the route either active or inactive (yes/no) depending on the WAN path state. Routes listed here are suppressed based on various states of the service (the Virtual Path being down as an example). Other events that can force a route to be ineligible are path down state, next hop unreachable or WAN link down.

From the above table, we can see fourteen defined routes. A description of the routes or groups of routes is described below:

- Route 0 – On the MCN this is a Host subnet route that resides at the DC site. 172.16.10.0/24 resides in the DC LAN and 192.168.15.1 is the gateway on the LAN that is the next hop that will get to that subnet.
- Route 1 – This is a local route to this SD-WAN device that displaying the route table.
- Route 2-4 – These are the subnets that are part of the virtual interfaces configured for the DC site SD-WAN. These subnets are derived from the trusted virtual interfaces defined.
- Route 5 – This is a shared route to another client node that is shared by the MCN with a Reachability status of No due

to the down Virtual Path between that site and the MCN.

- Route 6-9 – These routes exist at another client site. For this route, a Virtual Path route is created for matching WAN ingress traffic destined for the remote site on the Virtual Path.
- Route 10 – With the Internet Service defined, the system adds a catch all route for direct internet breakout for this local site.
- Route 11 – Passthrough is default route the system always adds to allow packets to flow through in case there is no match on any existing routes. The Passthrough is not groomed, typically local broadcasts and ARP traffic will be mapped to this service.
- Route 12 – Discard is default route the system always adds to drop anything undefined.

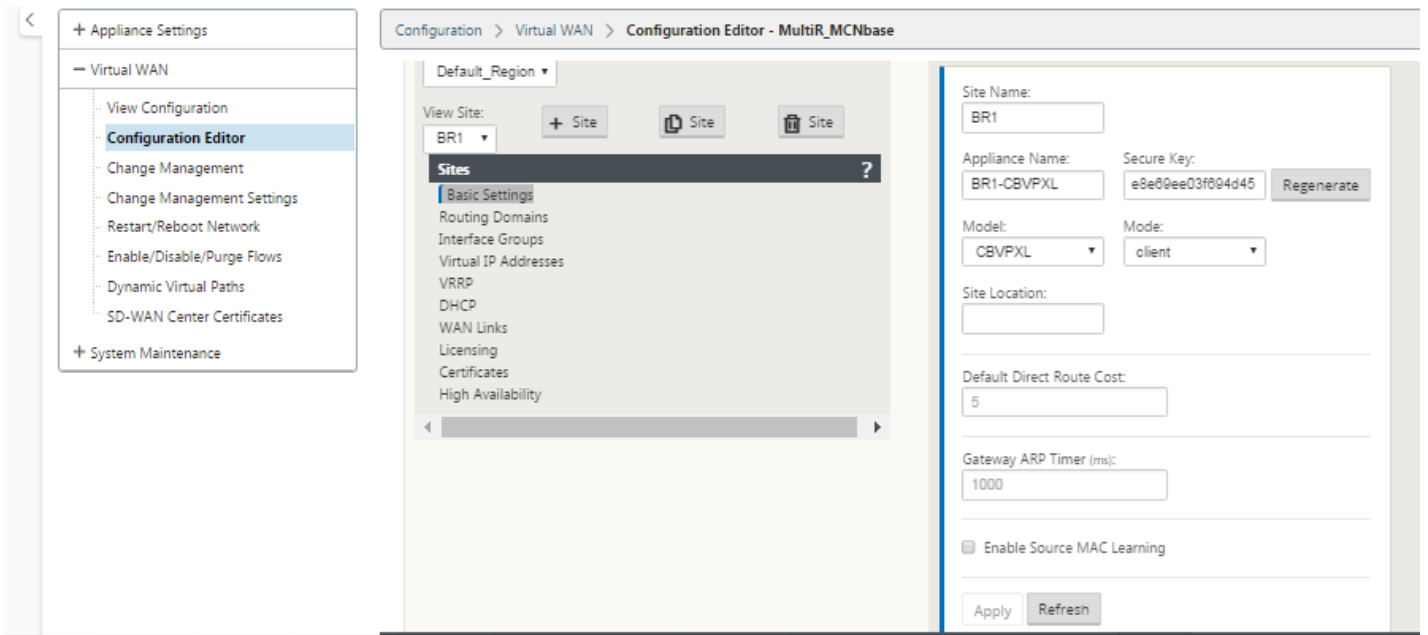
Default Route Cost Values:

- WAN to WAN Forwarding – 10
- Default Direct Route Cost – 5
- Auto Generated Routes – 5
- Virtual Path – 5
- Local – 5
- Intranet – 5
- Internet – 5
- Passthrough – 5
- Optional – route is 0.0.0.0/0 defined as a service level

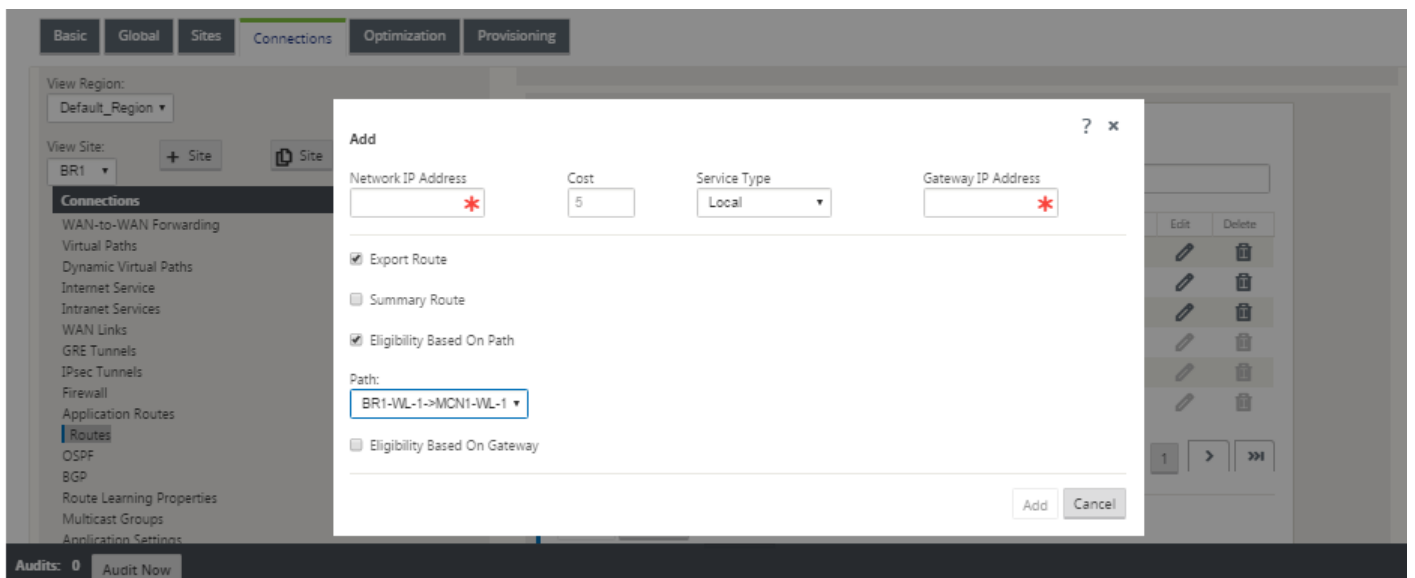
After defining these routes, it is important to understand how the traffic flows using the defined routes. These traffic flows will be broken into the following flows:

- LAN to WAN (Virtual Path) – Traffic going into the SD-WAN overlay tunnel
- WAN to LAN (Virtual Path) – Traffic existing the SD-WAN overlay tunnel
- Non-Virtual Path Traffic – Traffic routed to the underlay network

The default route cost can be altered on a per-site basis. The configuration can be found under **View Site > Basic Settings**:



Static routes can be defined per site under the **Connections > Site > Routes** node:



You will notice that routes can be tied to the Virtual Path or Gateway IP availability. Internet routes can be exported to the Virtual Path overlay or not depending on desired behavior. You can also create static Virtual Path routes to force traffic to a Virtual Path even though we are not getting the prefix advertised to SD-WAN (i.e. a higher cost route of last resort). SD-WAN can also suppress local subnets from being advertised by making the Virtual IP Address (VIP) private.

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.10.10.10/24	E1Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Trusted	
172.10.10.11/24	E1Vlan0	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply Revert

Note

The configuration does require at least one non-private VIP in each route domain.

Intranet and Internet Routes

For the Intranet and Internet service types, the user must have defined a SD-WAN WAN Link to support those types of services. This is a pre-requisite for any defined routes for either of these services. If the WAN link is not defined to support the Intranet Service it will be considered as a local route. The Intranet, Internet and Passthrough routes are only relevant to the site/appliance they are configured for.

When defining Intranet, Internet or Passthrough routes the following are design considerations:

- Must have service defined on the WAN link (Intranet/Internet – required)
- For Intranet/Internet must have gateway defined for the WAN link
- Relevant to local SD-WAN device
- Intranet routes can be learned via the Virtual Path but are done so at a higher cost
- With Internet Service, there is automatically a default route created (0.0.0.0/0) catch all route with a max cost
- Do not assume Passthrough will work, this should be tested/verified, also test with Virtual Path down/disabled to verify desired behavior
- Route tables are static unless route learning feature is enabled

Below is the maximum supported limit for multiple routing parameters:

- Maximum Routing Domains: 255
- Maximum Access Interfaces per WAN Link: 64
- Maximum BGP neighbors per site: 255
- Maximum OSPF area per site: 255
- Maximum Virtual Interfaces per OSPF area: 255
- Maximum Route Learning import filters per site: 512
- Maximum Route Learning export filters per site: 512
- Maximum BGP routing policies: 255
- Maximum BGP community string objects: 255

Virtual Routing and Forwarding

Mar 01, 2018

NetScaler SD-WAN allows segmenting networks for additional security and manageability by using VRF. For example, you can separate guest network traffic from employee traffic, create distinct routing domains to segment large corporate networks, and segment traffic to support multiple customer networks. Each routing domain has its own routing table and enables the support for overlapping IP subnets.

NetScaler SD-WAN appliances implement OSPF and BGP routing protocols for the routing domains to control and segment network traffic.

A Virtual Path can communicate using all routing domains regardless of the definition of the access point. This is possible because SD-WAN encapsulation includes the routing domain information for the packet. Therefore, both end networks know where the packet belongs to. It is not necessary to create a new WAN Link or an Access Interface for each routing domain.

Following are the list of points to consider when configuring the VRF functionality:

- By default, routing domains are enabled on an MCN.
- Routing domains have to be enabled on the Branch sites.
- Each enabled routing domain should have a virtual interface and virtual IP associated with it.
- Routing selection is part of all the following configurations:
 - Interface group
 - Virtual IP
 - GRE
 - WAN Link -> Access Interface
 - IPsec tunnels
 - Routes
 - Rules
- Routing domains are exposed in the web interface configuration only when multiple domains are created.
- For a Public Internet link, only one primary and secondary access interfaces can be created.
- For a Private Intranet/MPLS link, one primary and secondary access interface can be created per routing domain.

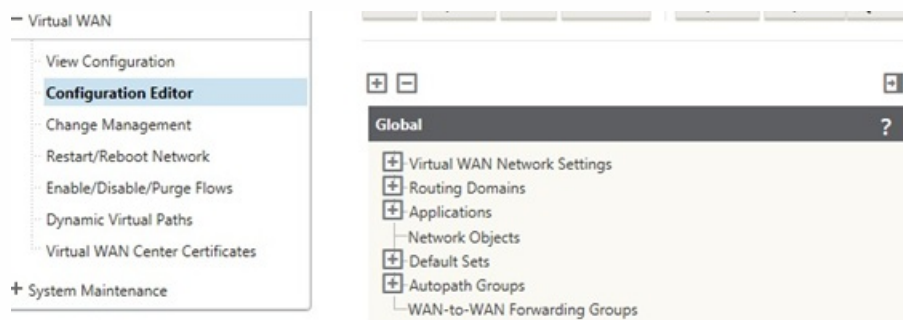
Configure Routing Domain

Mar 01, 2018

NetScaler SD-WAN appliances enable configuring routing protocols providing single point of administration to manage a corporate network, or a branch office network, or a data center network.

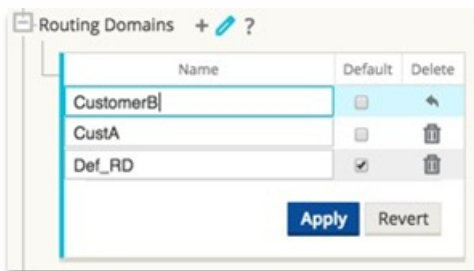
To configure routing domain:

1. In the SD-WAN web interface, navigate to **Configuration** → **Virtual WAN** → **Configuration Editor**. In the **Configuration Editor**, navigate to **Global** → **Routing Domains**, click **Add (+)** and enter a Name for your new Routing Domain.



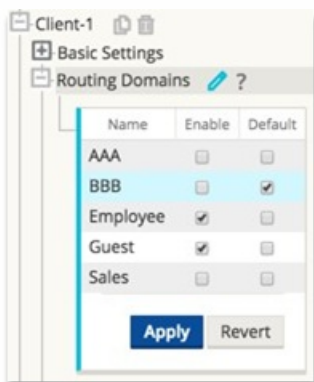
2. If you want to default to this Routing Domain, click the **Default** checkbox. Click **Apply** to save the changes. If you plan to implement a single Routing Domain, no explicit configuration is required.

All new configurations are automatically populated with a default Routing Domain.



3. Navigate to **Sites** → **[Client Site Name]** → **Routing Domains**. Click the **Enable** checkbox to enable a configured Routing Domain for the Site.

4. Click the **Default** checkbox to make that Routing Domain the default for the Site. Click **Apply** to save the changes.



Note

Unchecking **Enable** for a Routing Domain will make it unavailable for use at the Site.



Select Routing Domain for Intranet Service

Mar 01, 2018

To select routing domain for intranet service:

1. In the **Configuration Editor**, navigate to **Connections** → **[Site Name]** → **Intranet Services** → **[Intranet Service Name]** → **Basic Settings** click the **Edit** () icon.
2. Choose a **Routing Domain** from the drop-down menu.



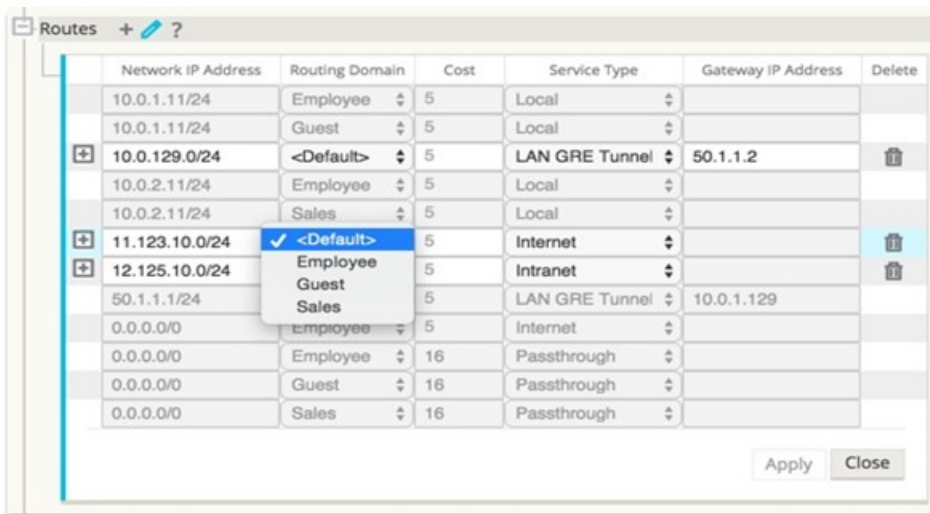
Configure Routes

Jun 11, 2018

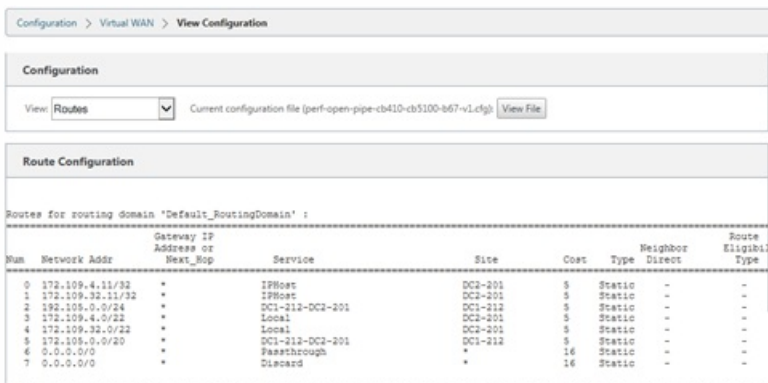
To configure routes:

1. In the **Configuration Editor**, navigate to **Connections > [Site Name] > Routes**.
2. Choose a **Routing Domain** from the drop-down menu. New Routes are automatically associated with the default Routing Domain.

For detailed instructions, see [configuring MCN](#).



3. After you configure routes, validate the route tables for the configured routing domain by navigating to **Configuration → Virtual WAN → View → Routes**.



Use CLI to Access Routing

Mar 01, 2018

In NetScaler SD-WAN release version 10.0, you can view additional information related to dynamic routing and the protocol status. Type the following command and syntax to access routing daemon and view the list of commands.

dynamic_routing?

Dynamic Routing

Mar 01, 2018

OSPF Overview

OSPF is a routing protocol developed for Internet Protocol (IP) networks by the Interior Gateway Protocol (IGP) group of the Internet Engineering Task Force (IETF). It includes the early version of OSI's Intermediate System to Intermediate System (IS-IS) routing protocol.

OSPF protocol is open, which means that its specification is in the public domain (RFC 1247). OSPF is based on the Shortest Path First (SPF) algorithm called Dijkstra. It is a link-state routing protocol that calls for sending Link-State Advertisements (LSAs) to all other routers within the same hierarchical area. Information on attached interfaces, metrics used, and other variables are included in OSPF LSAs. OSPF routers accumulate link-state information, which is used by the SPF algorithm to calculate the shortest path to each node.

You can now configure NetScaler SD-WAN appliances (Standard and Enterprise Editions) to learn routes and advertise routes using OSPF.

Note

- NetScaler SD-WAN appliances do not participate as Designated Router (DR) and BDR (Backup Designated Router) on each multi-access network since the default DR priority is set to "0".
- NetScaler SD-WAN appliances does not support summarization as an Area Border Router (ABR).

How To Configure OSPF

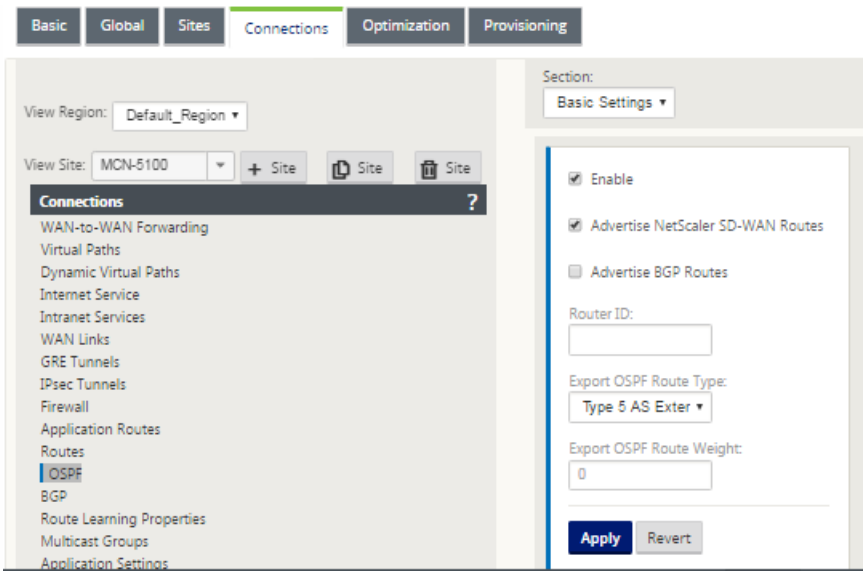
To configure OSPF:

1. In the **Configuration Editor**, navigate to **Connections > View Region > View Site > [Site Name] > OSPF > Section > Basic Settings**.
2. Click the **Enable** checkbox, enter an optional **Router ID**.

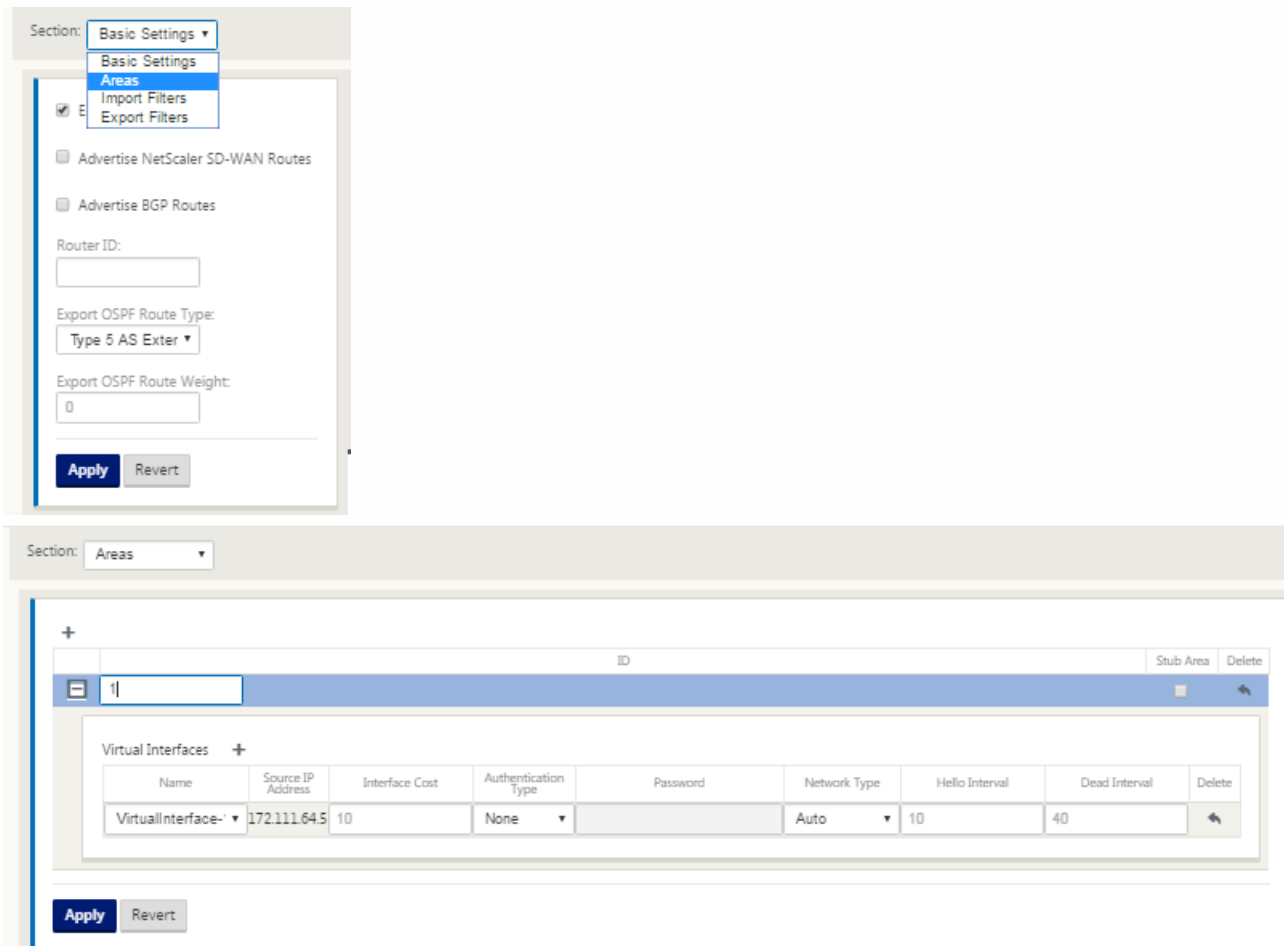
Note

If the Router ID is not specified, it will be auto-selected as the lowest Virtual IP hosted in the SD-WAN network.

3. Click the **Advertise NetScaler SD-WAN Routes** checkbox if you wish to advertise NetScaler SD-WAN Routes, and click **Apply** to enable OSPF. The routes advertise or redistribute the SD-WAN virtual path routes to peer routes with whom adjacency or peering is established so that the peer routes are aware of being able to reach those network prefixes through the SD-WAN network.



4. Expand **OSPF** -> **Area**, and click **Edit**.



5. Enter an **area ID** to learn routes from and advertise to.

6. For sites with multiple Routing Domains, from the **Virtual Interfaces** panel, choose a **Routing Domain** from the drop-down menu as illustrated in the figure. The Routing Domain determines which Virtual Interfaces are available.

Note

If there is only one Routing Domain configured, the Routing Domain column will not appear. If Identity is not checked for a specific Virtual IP Address, the associated Virtual Interface will not be available for IP services. For more information, see the Virtual IP Address Identity section.

7. Choose one of the available Virtual Interfaces from the **Name** drop-down menu. The Virtual Interface will determine the **Source IP Address**.
8. Enter the **Interface Cost** (10 is the default).
9. Choose an **Authentication Type** from the drop-down menu.
10. If you chose **Password** or **MD5** in step 8, enter the Password associated text field.
11. In the **Hello Interval** field, enter the amount of time to wait between sending Hello protocol packets to directly connected neighbors (10 seconds is the default).
12. In the **Dead Interval** field, enter the amount of time to wait to receive a Hello protocol packet before marking a router as dead (40 seconds is the default).
13. Click **Apply** to save your changes.

Stub Area

Stub areas are shielded from external routes and receive information about networks that belong to other areas of the same OSPF domain.

Enable the **Stub Area** check box.

ID	Stub Area	Delete
1	<input type="checkbox"/>	

Name	Source IP Address	Interface Cost	Authentication Type	Password	Network Type	Hello Interval	Dead Interval	Delete
VirtualInterface-1	172.111.64.5	10	None		Auto	10	40	

BGP Overview

BGP is an inter-autonomous system routing protocol. An autonomous network or group of networks is managed under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet Service Providers (ISPs). Customer networks deploy an Interior Gateway

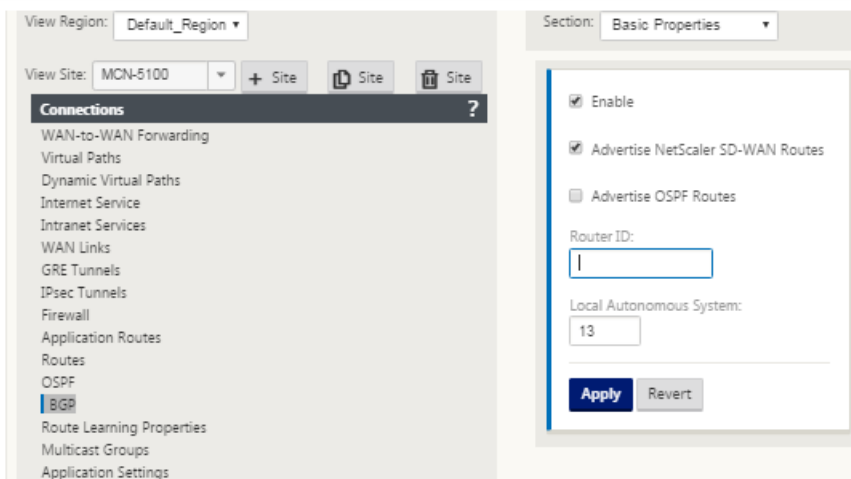
Protocol (IGP) such as RIP or OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between Autonomous Systems (AS), the protocol is called External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is called Interior BGP (IBGP).

BGP is a robust and scalable routing protocol deployed on the Internet. To achieve scalability, BGP uses many route parameters called attributes to define routing policies and maintain a stable routing environment. BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and advertise only the optimal path to a destination network. You can configure NetScaler SD-WAN appliances to learn routes and advertise routes using BGP.

How To Configure BGP

To configure BGP:

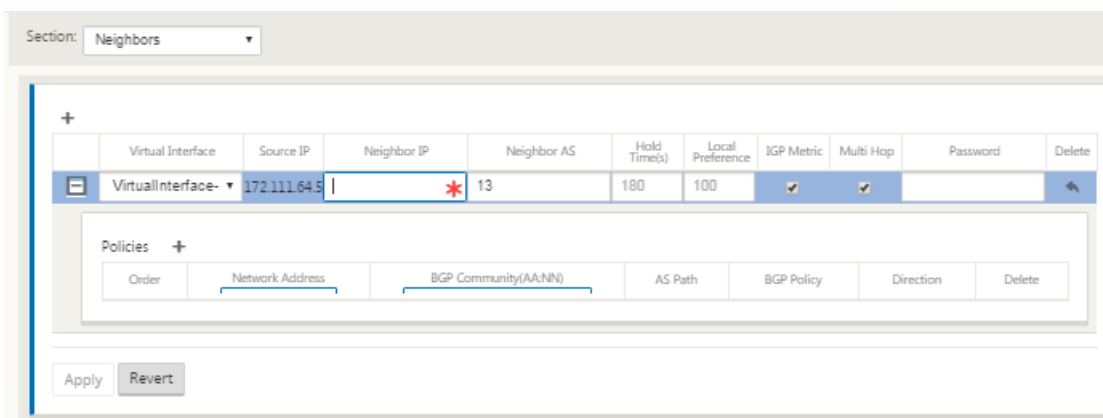
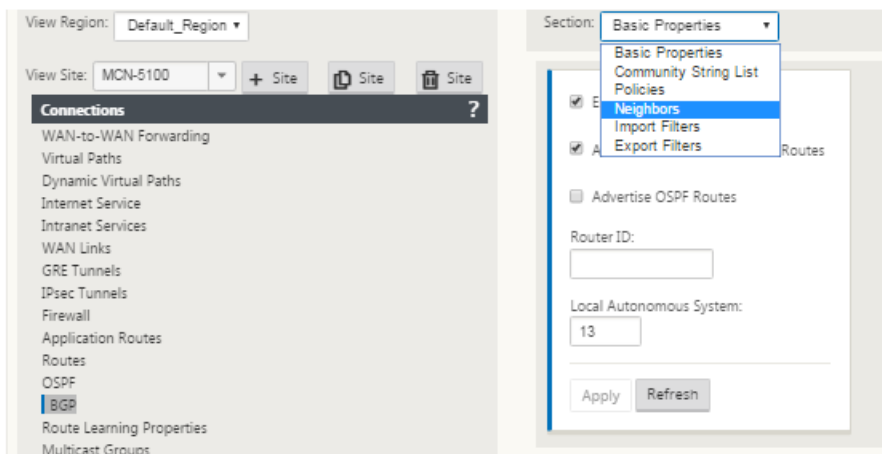
1. In the **Configuration Editor**, navigate to **Connections > View Region > View Site > [Site Name] > BGP > Basic Settings**.
2. Click the **Enable** checkbox and the **Advertise NetScaler SD-WAN Routes** checkbox if you want to advertise NetScaler SD-WAN Routes. Enter an optional **Router ID**, and enter the number of the Local Autonomous System to learn routes from and advertise routes to in the **Local Autonomous System** field. The routes advertise or redistribute the SD-WAN virtual path routes to peer routes with whom adjacency or peering is established so that the peer routes are aware of being able to reach those network prefixes through the SD-WAN network.
3. Click **Apply** to enable BGP.



4. Expand **Basic Settings > Neighbors** and click the **Add (+)** icon.

Note

If there is only one Routing Domain configured, the Routing Domain column will not appear. If Identity is not checked for a specific Virtual IP Address (see the Virtual IP Address Identity section for more details), the associated Virtual Interface will not be available for IP services.



For Sites with multiple Routing Domains choose a routing domain. Routing Domain determines which Virtual Interfaces are available.

5. Choose a **Virtual Interface** from the drop-down menu. The Virtual Interface will determine the Source IP Address.

6. Enter the **IP Address** of the IBGP Neighbor router in the Neighbor IP field, and **Local Autonomous System** number in the Neighbor AS field.

7. In the **Hold Time (s)** field, enter the Hold Time, in seconds, to wait before declaring a neighbor down (the default is 180).

8. In the **Local Preference (s)** field, enter the Local Preference value, in seconds, which is used for selection from multiple BGP routes (the default is 100).

9. Click the **IGP Metric** checkbox to enable the comparison of internal distances to calculate the best route.

10. Click the **Multi Hop** checkbox to enable multiple hops for the route.

11. In the **Password** field, enter a password for MD5 authentication of BGP sessions (authentication is not required).

Note

Configuring Route Reflectors and Confederations for iBGP is not supported in a NetScaler SD-WAN network.

How To Monitor Route Statistics

1. Navigate to **Monitor > Statistics**. Select **Routes** from the **Show** drop-down menu.

All functions for applicable Routes are supported in NetScaler SD-WAN regardless of whether a Route is Dynamic or Static.

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

Exterior BGP (eBGP)

NetScaler SD-WAN appliances connect to a switch on the LAN side and a Router on the WAN side. As SD-WAN technology starts becoming more integral to Enterprise network deployments, SD-WAN appliances will replace the Routers. SD-WAN implements eBGP dynamic routing protocol to function as a dedicated routing device.

SD-WAN appliance establishes neighbourhood with peer routers using eBGP towards WAN side and is able to learn, advertise routes from and to peers. You can select importing and exporting eBGP learned routes on peer devices. Also, SD-WAN static, virtual path learned routes can be configured to advertise to eBGP peers.

For more information, refer to the following use cases:

- SD-WAN site Communicating with non SD-WAN site over eBGP
- Communication Between SD-WAN sites Using Virtual Path and eBGP
- Implementing OSPF in one-arm topology
- OSPF Type5 to Type1 deployment in MPLS Network
- SD-WAN and non SD-WAN (third-party) appliance OSPF deployment
- Implementing OSPF using SD-WAN network with high-availability setup

OSPF

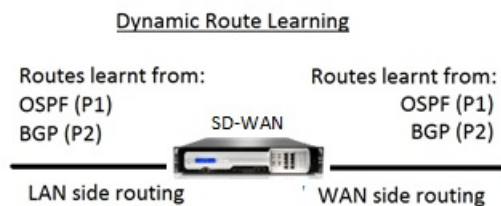
Mar 01, 2018

LAN Side: Dynamic Route Learning

OSPF running on the LAN port of Netscaler SD-WAN appliance deployed in Gateway Mode

SD-WAN appliances perform route discovery of Layer 3 routing advertisements within a local customer network (both branch and data center) for each of the desired routing protocols (OSPF and BGP). The routes that are learnt are dynamically captured and displayed.

This eliminates the need for SD-WAN administrators to statically define the LAN-side networking environment for each appliance that is part of the SD-WAN network.



WAN Side: Dynamic Route Sharing

NetScaler SD-WAN appliance having an AREA defined as a STUB area by limiting the learning of Type 5 AS-external LSA.

SD-WAN appliances can advertise the locally learned dynamic routes with the MCN. The MCN can then relay these routes to other SD-WAN appliances in the network. This exchange of information dynamically allows for maintaining connectivity between sites across the changing network.

OSPF Deployment Modes

In previous releases, OSPF instance learned routes from SD-WAN were treated as external routes with Type 5 LSA only. These routes were advertised to its neighbor routers in Type 5 External LSA. This resulted in SD-WAN routes to be less preferred routes according to the OSPF path selection algorithm.

With the latest release, SD-WAN can now advertise routes as intra-area routes (LSA Type 1) to get preference as per its route cost using the OSPF path selection algorithm. The route cost can be configured and advertised to the neighbor router. This allows for deploying SD-WAN appliance in one-arm mode described below.

Implementing OSPF in One-Arm Topology

In one-arm configuration, the router needs complicated PBR or WCCP configuration in OSPF deployments. By changing the default export route type from Type 5 to Type 1 we can simplify this deployment. If SD-WAN routes are advertised as intra-area routes with less cost, and the SD-WAN appliance becomes active, the neighbor router selects SD-WAN routes and automatically begins forwarding traffic through SD-WAN network. Additional PBR or WCCP configuration is not required any longer.

Prerequisites:

- SD-WAN Appliances at the DC and Branch sites should be running latest release version.
- End-to-End IP connectivity should be configured and working fine.
- OSPF is enabled on all the sites.

To configure OSPF Type 1:

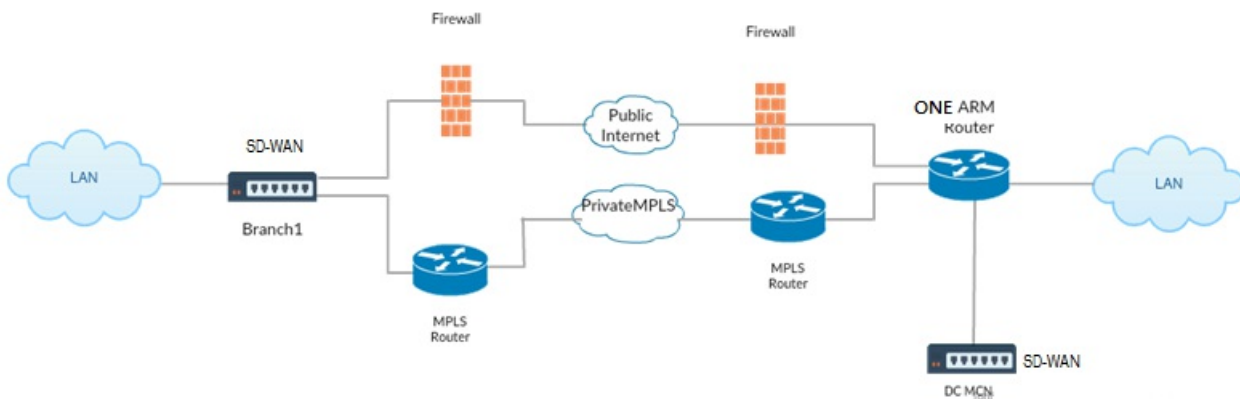
1. Configure **Virtual Interfaces** and **WAN links** on both the DC and Branch sites so that you can create Virtual Path between them.
2. Under **Connections->[MCN]->Route Learning->OSPF->Basic Settings**, select **Export OSPF Route Type** to be **Type 1 Intra Area**.
3. Save the configuration, stage and activate the configuration.

You should be able to see following route types under **Export OSPF Route Type**

- Type 5 AS External
- Type 1 Intra Area

You should be able to configure **Type 5 AS External** route.

After activation of the changed configuration, you should see the Route Type changes under **Configuration->Virtual WAN->View Configuration->Dynamic Routing**.

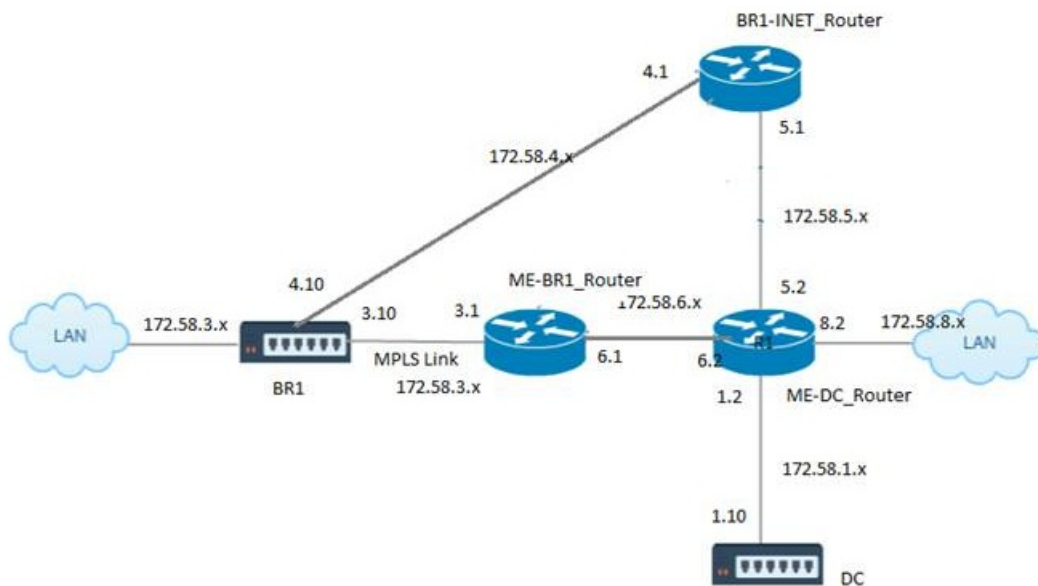


As shown in the illustration above, DC MCN is deployed in one-arm topology. When DC site is up, one-arm router forwards all traffic from local LAN to other sites, such as the Branch's local LAN whose destination IP address is within same subnet to the SD-WAN first, then SD-WAN appliance wraps all packets and sends it to the router with all the packets destination IP address in the Branch Virtual IP address. The router then forwards those packets to WAN.

When the DC site is down, router forwards all traffic from local LAN to other sites (branch site's local LAN, destination IP is within subnet) to WAN directly, and not to the SD-WAN appliance.

OSPF Type5 to Type1 Deployment in MPLS Network

The following deployment mode is provided to avoid loop formation in an MPLS network configured using SD-WAN appliances. The illustration below describes the standard MPLS network implementation.



In the above illustration:

- OSPF is configured between *ME-BR1_Router* and *ME-DC_Router* in area 0.
- OSPF is configured between *ME-DC_Router* and *DC* in area 0.

Recommended Configuration:

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

On the ME-DC_Router:

- Add, static route for 172.58.3.10/32(Virtual IP of BR1 for MPLS Link) through 172.58.6.1
- Add, static route for 172.58.4.10/32(Virtual IP of BR1 for INET) through 172.58.5.1

Adding static routes prevents loop formation between the ME-DC_Router and DC SD-WAN appliance. If you do not add static routes, the MCN forwards traffic to the ME-DC Router, and back from router to the MCN and this creates a loop continuously.

The static routes which are not PBR routes but the destination Host IP based routes will traverse towards the right link to be chosen from the DC side based on the path chosen and the encapsulation performed thereafter. Therefore, with these static routes configured, the encapsulated packets with any destination Virtual IP of BR1 SD-WAN appliance would use these links as per the best path selected by the DC MCN.

Add ACL to avoid loop formation when IPHOST routes are installed (if no static Virtual IPs configured):

- If the IPHOST routes advertised by BR1 SD-WAN appliance are installed by the MCN router *ME-DC_Router* and not added as static routes as mentioned above, there is a possibility of loop formation if the OSPF participating interface (172.58.6.x) between ME-BR1_Router and ME-DC_Router goes down.

This is because with this interface down, the IPHOST routes are flushed from ME-DC_Router's routing table.

b. If this happens, MCN will forward the encapsulated packet destined to one the BR1 VIPs to ME-DC Router and back from router to the MCN and loop continuously.

On the ME-BR1_Router:

Advertise 172.58.3.x network to ME-DC_Router with a higher cost than the cost advertised for the same network by DC, if the same AREA-ID is used between **ME-BR1_Router <-> ME-DC_Router** and **ME-DC_Router <-> DC (SD-WAN)**.

a. Based on the cost metric computation of OSPF $10^8/BW$ and the cost for route prefixes are based on the interface type. SD-WAN appliances advertise the virtual path and virtual WAN specific static routes to the external or peer routers with default SD-WAN cost of 5.

b. If the ME-BR1_Router is also advertising 172.58.3.0/24 as an internal OSPF type 1 route alongside DC (SD-WAN) which also advertises the same prefix as internal ospf Type 1 route, then according to cost computation, by default the ME-BR1_Router's route will be configured, as the cost is lesser than SD-WAN's default cost of 5. To avoid this and make SD-WAN appliance chosen as preferred route initially, the interface cost of (172.58.3.1) needs to be manipulated to make it higher on the ME-BR1_Router so that DC SD-WAN route is configured in the routing table of the ME-DC_Router.

This also ensures that when the DC SD-WAN appliance fails, the alternate route to use ME-BR1_Router as the next preferred gateway will ensure uninterrupted traffic flow.

Use ME-DC_Router as a source for advertising 172.58.8.0/24 network to both DC SD-WAN and the ME-BR1_Router

With this route, the DC SD-WAN can send packets to the upstream router being aware of the LAN subnet after decapsulation. If DC SD-WAN goes down, the legacy routing infrastructure would help ME-BR1_Router use the ME-DC_Router as the next hop to reach the 172.58.8.x network.

To configure OSPF exported routes as Type1 under Basic OSPF Settings

1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch sites to create Virtual Path between them.
2. Under **Connections->[MCN]>Route Learning->OSPF->Basic Settings**, select **Export OSPF Route Type** to be **Type 1 Intra Area**.
3. Save the configuration, stage and activate the same.
4. You should be able to see following two route types under **Export OSPF Route Type**
 - Type 5 AS External
 - Type 1 Intra Area

5. After activation of the changed config, you can see the Route Type changes under **Configuration->Virtual WAN->View Configuration->Dynamic Routing**.

6. Routes should be advertised as Type5 External AS by the SD-WAN appliance. Routes learnt through SD-WAN should be displayed in the neighboring routers as Type5 AS External routes.

To configure OSPF exported route weight under Basic OSPF Settings

1. Configure Virtual Interfaces and WAN links on both DC and Branch sites to create Virtual Path between them.

2. Under **Connections**->[MCN]->**Route Learning**->**OSPF**->**Basic Settings**, configure **Export OSPF Route Weight**.
3. Save the configuration, stage and activate the same.
4. Now, configure Export OSPF Route Weight to any numeric value between **1** to **65529**.
5. After activation of the changed config, you can see the Route Weight under **Configuration**->**Virtual WAN**->**View Configuration**->**Dynamic Routing**.
6. The default route weight exported should be 0. Actual cost of the route should only be the cost of SD-WAN.

To configure OSPF exported routes as Type1 under Export Filter settings

1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch so that we can create Virtual Path between them
2. Under **Connections**->[MCN]->**Route Learning**->**OSPF**->**Export Filters** configure an export filter.
3. Expand the filter. Configure **Export OSPF Route Type** to **Type 1 Intra Area** route.
4. Save the configuration, stage and activate the same.
5. You should be able to see following two route types under **Export OSPF Route Type**

- Type 5 AS External
- Type 1 Intra Area

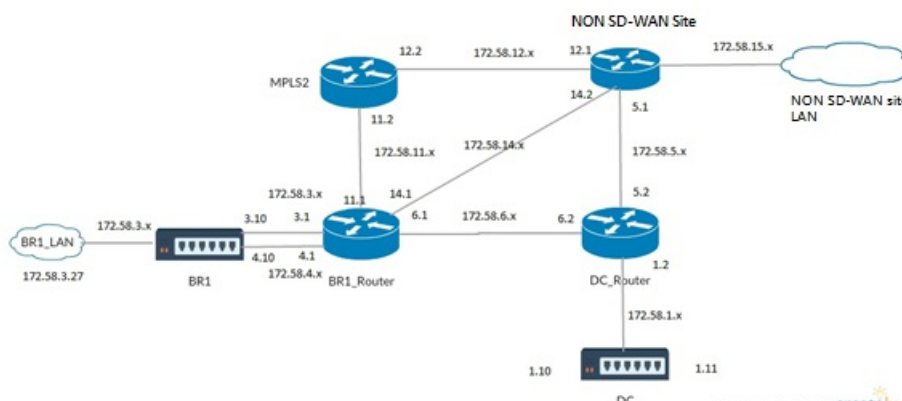
6. After activation of the changed config, user should be able to see the Route Type changes under **Configuration**->**Virtual WAN**->**View Configuration**. Route type should be displayed as Type 5 AS External.

To configure OSPF exported route weight under Export Filter settings

1. Configure Virtual Interfaces and WAN links on both DC and Branch so that we can create Virtual Path between them
2. Under **Connections**->[MCN]->**Route Learning**->**OSPF**->**Export Filters** configure an export filter.
3. Expand the filter. Configure Export OSPF Route Weight to any numeric value between **1** to **65529**.
4. Save the configuration, stage and activate the same.
5. After activation of the changed config, user should be able to see the Route Type changes under **Configuration**->**Virtual WAN**->**View Configuration**.
6. Route Weight configured under Export Filter should override the Weight configured under Basic OSPF Settings.

SD-WAN and Third-Party (non SD-WAN) Appliance Deployment

As shown in the illustration below, third-party appliance site can get to Site B's LAN by sending traffic to Site A, then using virtual path between DC to Branch sites to get to the Branch. If that fails, it will use MPLS2 to get to Branch site.



Configuration Steps:

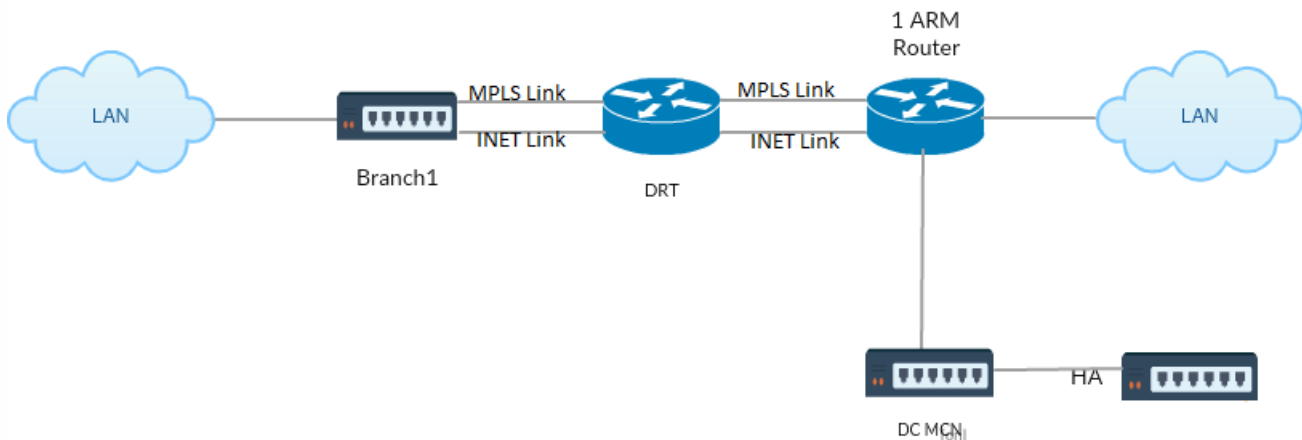
1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch so that a Virtual Path is created between the sites.
2. Configure **Export Route Type** as **Type1** and assign cost as **195** on the SD-WAN appliance.
3. Save, stage and activate the configuration.
4. Send traffic between the end hosts on DC and Branch sites.
5. Shutdown the link between R1 and R2.
6. Send traffic between the end hosts on DC and Branch sites.
7. Unshut the link between R1 and R2.
8. Send traffic between the end hosts on DC and Branch sites.
9. Disable Virtual WAN Service on the DC site so that Virtual Paths go down.
10. Send the traffic between the end hosts on DC and Branch sites.

Verifying Configuration

1. Initially, at step 4, all the traffic passes through SD-WAN appliance.
2. At step 6, when the link between R1 and R2 is broken, traffic is routed towards SD-WAN through R3.
3. At step 8, traffic flows through SD-WAN appliance with R2 as the next hop for the LAN Router R1.
4. At step 10, Virtual WAN paths go down between DC and BR1 appliance and traffic should flow normally as before the SD-WAN network was configured.

Traffic flow can be observed in the SD-WAN GUI under **Monitoring->Flows**.

Implementing OSPF with SD-WAN Network in High Availability Setup



OSPF Type5 to Type1 with high-availability sites during failover to standby appliance and deployed in high-availability setup

To configure OSPF in HA deployment:

1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch to create Virtual Path between them.
2. Setup High-Availability.
3. Export **Route Type** configured as **Type 1** and **Route Weight** as **50**
4. Save the configuration, stage and activate the same.
5. Start traffic flow.
6. Observe that under **Monitor->Statistics->Routes**, the hit count increases for OSPF routes with least costs.
7. Bring the Active MCN down and observe the behavior.
8. Bring the original Active MCN back Up.

9. The **Dashboard->High Availability Status** shows correctly for HA Local Appliance and Peer Appliance for Active and Standby.
10. Under **Configuration->View Configuration-> Dynamic Routing**, OSPF is enabled and **export_ospf_route_type** shows **Type1** and **export_ospf_route_weight** as **50**.
11. Even after failover the High Availability Status shows correct OSPF configuration for Local and Peer Appliance.
12. View **Monitor->Statistics->Routes**. The hit count increases for OSPF routes with least costs.
13. After failback, the High Availability Status shows correct OSPF configuration for Local and Peer Appliance.
14. Verify that the hit count increases for OSPF routes with low cost under view **Monitor->Statistics->Routes**.

BGP

Jun 11, 2018

The SD-WAN BGP routing functionality enables you to:

- Configure the autonomous system (AS) number of a neighbour or other peer router (iBGP or eBGP).
- Create BGP policies to be applied selectively to a set of networks on a per-neighbour basis, in either direction (import or export). An SD-WAN appliance supports eight policies per site, with up to eight network objects (or eight networks) associated with a policy.
- For each policy, users can configure multiple community strings, AS-PATH-PREPEND, MED attribute. Users can configure up to 10 attributes for each policy.

Note

Configuring eBGP with a different neighbor AS is not supported. Also, only local preference and IGP metric for path selection and manipulation is allowed.

Configuring Policies

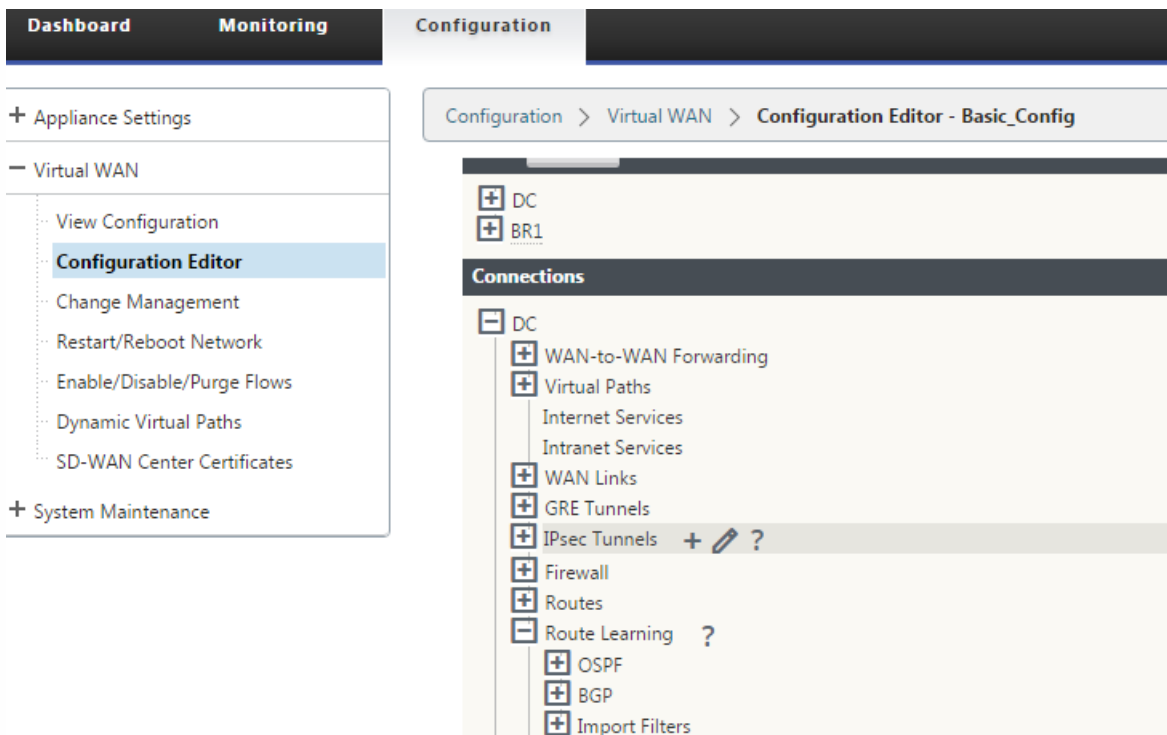
In the SD-WAN web management interface, the configuration editor has a new section, BGP policy, under **Route Learning > BGP**. In this section, users can add BGP attributes that constitute a policy. Adding community strings, prepending AS path prepend, and configuring MED are supported.

You can manually configure each community string or select no advertise or no export community string from a drop-down menu. For manual configuration, you can enter an AS number and community. You can select Insert/Remove to tag the routes or remove the community from the routes.

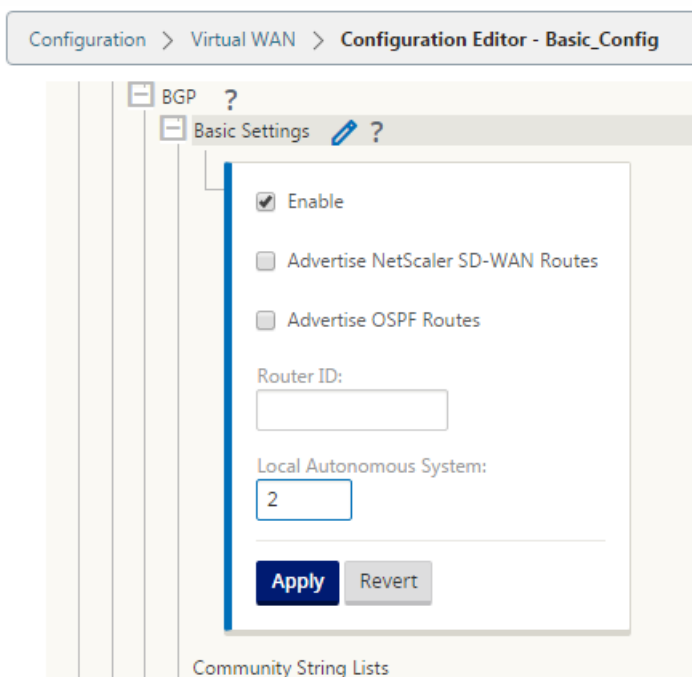
You can configure the number of times you want to prepend the local AS to the AS Path before advertising outside the local network. You can configure MED for matching routes.

To configure BGP policy:

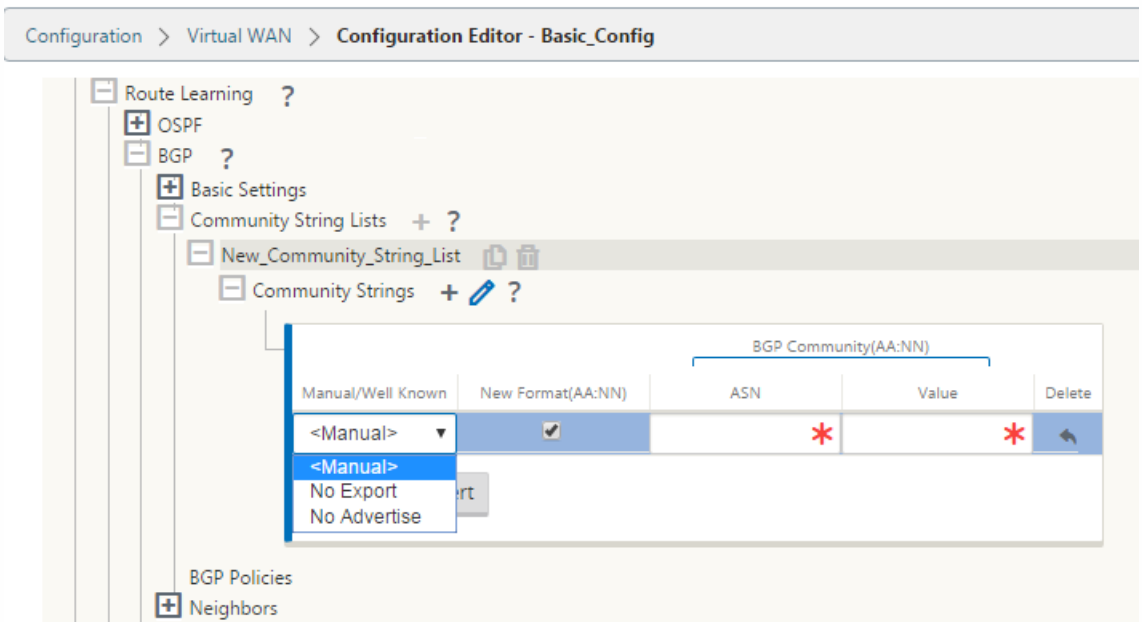
1. In the NetScaler SD-WAN web management interface, go to **Configuration > Virtual WAN > Configuration Editor**. Open an existing configuration package. Go to **Sites > DC** or **Branch** settings.



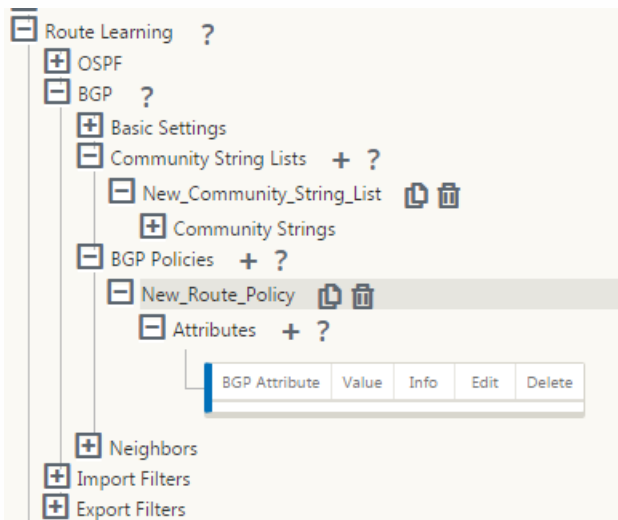
2. Expand **BGP** and click **Enable** under **Basic Settings**. Enter **Router ID** and **Local Autonomous System** value and click **Apply**.



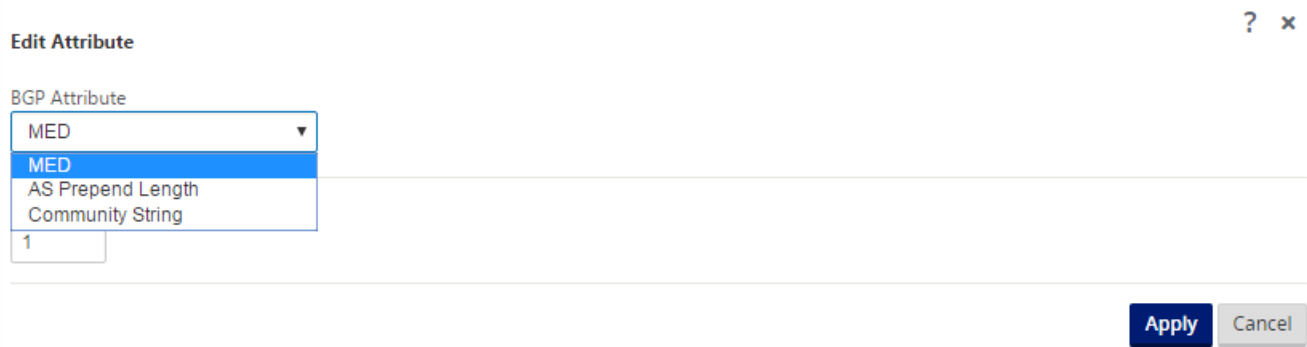
3. Click + sign next to the **Community String Lists**. Configure each community string manually or by selecting no advertise or no export community string from the drop-down menu. For manual configuration, you can enter an AS number and community. You can select **Insert/Remove** tag the routes with the community string or remove the community string from the routes received from the peers.

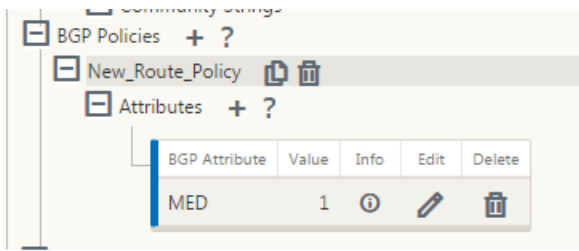


4. Configure BGP policy by expanding **BGP Policies**. Add BGP attributes to the **New Route Policy**.



5. Click the **+** sign next to **Attributes** to edit BGP attributes. The **Edit Attributes** window is displayed. Select the desired BGP attribute from the drop-down menu. Enter the desired value for **MED**, **AS Prepend Length**, or **Community String** as per your selection. Click **Apply**.





Note

Any policy can have only one occurrence of an attribute and cannot take multiple occurrence of the same attribute. You cannot have 2 MED or 2 AS Path Prepend. It can have either MED/AS-PATH Prepend/Community String or a combination.

Configuring Neighbors

To configure eBGP, an additional column to the existing BGP neighbors section is added to configure neighbor AS number. The existing configurations are pre-populated to this field with the local AS number when you import previous configuration using the SD-WAN 9.2 configuration editor.

The neighbor configuration also has an optional advanced section (expandable row) where you can add Policies for each neighbor.

Important

The BGP functionality in SD-WAN networks, does not advertise routes learnt from a neighbor to the same neighbor.

By default, the SD-WAN BGP functionality does not import routes and exports all routes if the **Advertise NetScaler SD-WAN routes** is enabled. You need add import filters for routes to import and add export filters for routes which you do not want to export to neighboring routers.

Configuring Advanced Neighbors

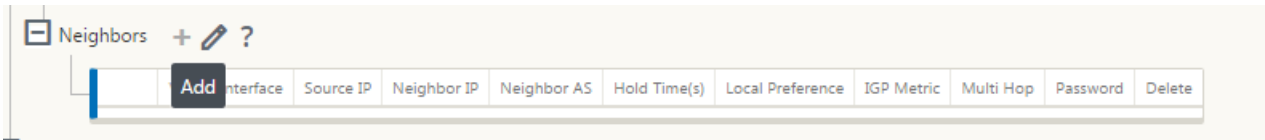
With this option, you can add network objects and add a configured BGP policy for that network object. This is similar to creating a route map and ACL to match certain routes and configuring BGP attributes for that neighbor. You can specify the direction to indicate if this policy is applied for incoming or outgoing routes.

The default policy is to <accept> all routes. Note that accept and reject policies are defaults and cannot be modified.

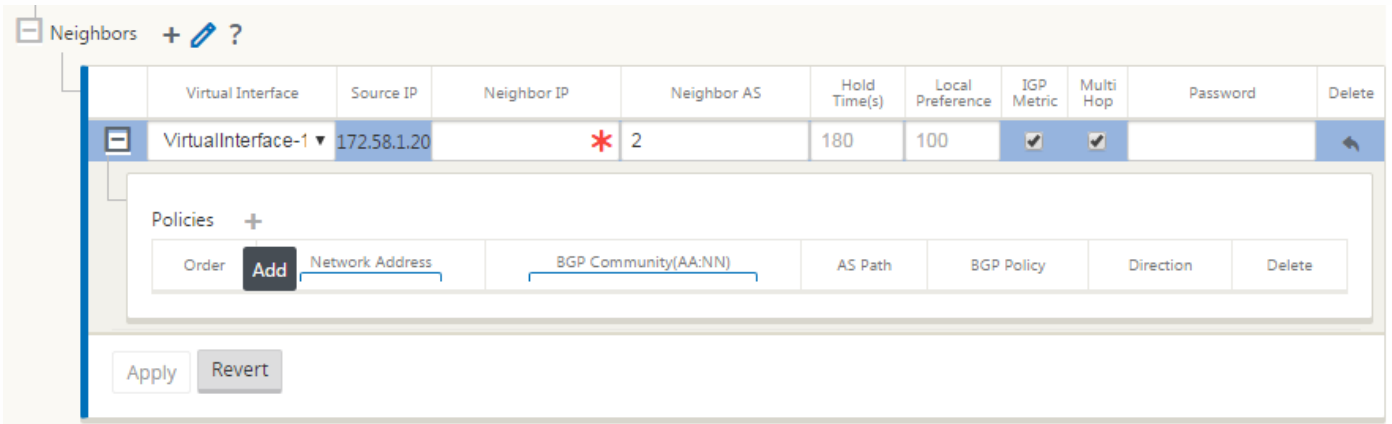
You have the ability to match routes based on Network address (destination address), AS Path, Community string and assign a policy and select direction for the policy to be applied.

To configure neighbors:

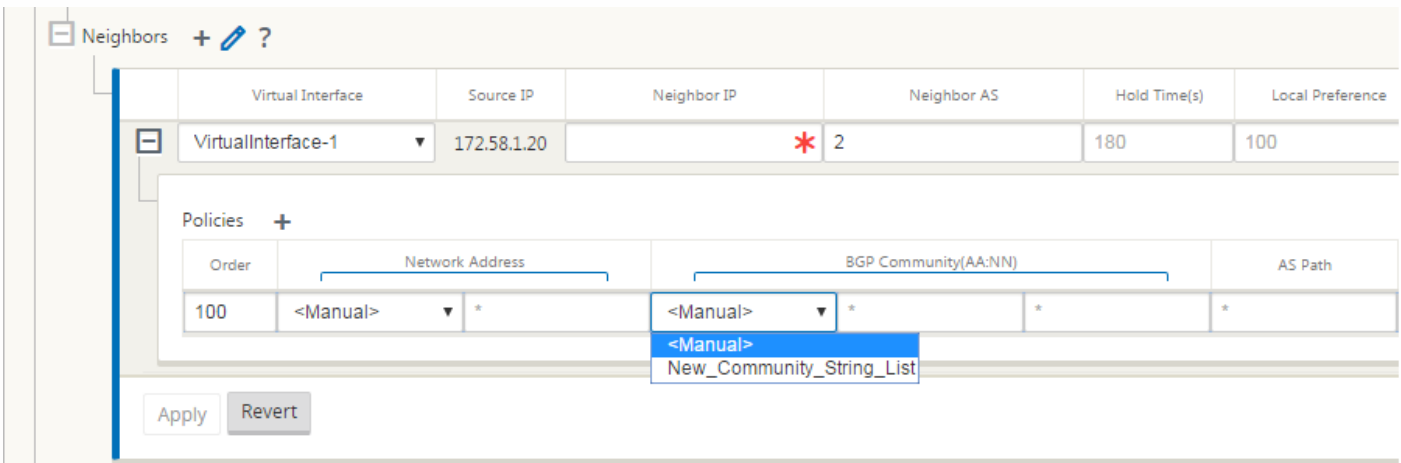
1. Configure neighbors by clicking **Add** as shown below.



2. Click the + sign. Select a **Virtual Interface**. Enter the **Neighbor IP** address.



3. Add policies. Select **Network Address**, **BGP Community**, and **AS Path** details as desired. Click **Apply**.



The screenshot shows the Configuration Editor interface for eBGP. On the left, a tree view shows the configuration hierarchy: Community String Lists, BGP Policies (Policy1, Policy2, Policy3), and Neighbors. The main area displays two neighbor configurations for the 'Blue' routing domain on 'VirtualInterface-1'.

Neighbor 1 Configuration:

Routing Domain	Virtual Interface	Source IP	Neighbor IP	Neighbor AS	Hold Time(s)	Local Preference	IGP Metric	Multi Hop	Password
Blue	VirtualInterface-1	172.16.20.2	172.16.80.2	100	180	100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Policies for Neighbor 1:

Order	Network Address	BGP Community(AA:NN)	AS Path	BGP Policy	Direction	Delete
100	<Manual>	<Manual>	*	Policy1	Out	<input type="checkbox"/>
(auto)	<Manual>	<Manual>	*	<Accept>		

Neighbor 2 Configuration:

Routing Domain	Virtual Interface	Source IP	Neighbor IP	Neighbor AS	Hold Time(s)	Local Preference	IGP Metric	Multi Hop	Password
Blue	VirtualInterface-1	172.16.20.2	192.168.1.1	300	180	200	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Policies for Neighbor 2:

Order	Network Address	BGP Community(AA:NN)	AS Path	BGP Policy	Direction	Delete
100	<Manual>	1.2.1.0/24	<Manual>	Policy1	In	<input type="checkbox"/>
200	<Manual>	1.3.1.0/24	String_list3	<Reject>	In	<input type="checkbox"/>
300	<Manual>	1.4.1.0/24	<Manual>	<Accept>	In	<input type="checkbox"/>
400	<Manual>	1.5.1.0/24	<Manual>	Policy3	In	<input type="checkbox"/>
(auto)	<Manual>	<Manual>	<Manual>	<Accept>		

4. Go to **Monitoring > Routing Protocols > Dynamic Routing Protocols** to monitor the configured BGP policies and neighbors for the DC or Branch site appliance.

You can enable debug logging and to view log files for routing from the **Monitor > Routing Protocol** page. The logs for the routing daemon are split into separate log files. The standard routing information is stored in *dynamic_routing.log* while dynamic routing issues are captured in *dynamic_routing_diagnostics.log* which can be viewed from monitoring of routing protocols.

BGP Soft Reconfiguration

Routing policies for BGP peer include configurations such as route-map, distribute-list, prefix-list, and filter-list that might impact inbound or outbound routing table updates. When there is a change in the routing policy, the BGP session should be cleared, or reset, for the new policy to take effect.

Clearing a BGP session using a hard reset invalidates the cache and results in negative impact on the operation of networks as the information in the cache becomes unavailable.

With SD-WAN 10.0 software release, the BGP Soft Reset Enhancement feature provides automatic support for dynamic soft reset of inbound BGP routing table updates that are not dependent upon stored routing table update information.

iBGP

Mar 01, 2018

Netscaler SD-WAN appliance with iBGP on the LAN side and eBGP on the WAN side

NetScaler SD-WAN appliances advertise all the eBGP routes learnt into the IGP domain with NEXT HOP SELF when deployed with iBGP on the LAN side and eBGP on the WAN side.

Multiple iBGP LAN Routers in a Linear Network Topology with Direct Peering and meshed with NetScaler SD-WAN

Limitations:

- AS-Path prepend, Med, and Community attributes are not supported.
- Route filtering between OSPF and BGP during redistribution is not supported. Either all (or) none of the routes learned from OSPF are advertised to BGP peers and vice-versa.
- Route aggregation is not supported.
- Only a Max of 16 BGP peers (including iBGP and eBGP) can be configured.

eBGP

Mar 01, 2018

SD-WAN site communicating with non SD-WAN site over eBGP

When a site without SD-WAN appliance is communicating with another site with SD-WAN appliance (Site-A) over a single WAN path (only internet is available), and if the site with SD-WAN appliance (Site-A) loses internet connectivity, then the site without SD-WAN can communicate with Site-A through another SD-WAN appliance site (Site-B). Site-B funnels traffic from the site without SD-WAN appliance to the Site-A.

Communication between SD-WAN sites using Virtual Path and eBGP

Provides underlay route learning to communicate with remote site local subnets when the virtual path is down between two sites while the Virtual WAN appliance is still up and running.

Application Route

Feb 28, 2018

In a typical enterprise network, the branch offices access applications on the on premise data center, the cloud data center, or the SaaS applications. The application routing feature, allows you to steer the applications through your network easily and cost-efficiently. For example, when a user on the branch site is trying to access a SaaS application the traffic can be routed such that the branch offices can access the SaaS applications on the internet directly, without having to go through the data center first.

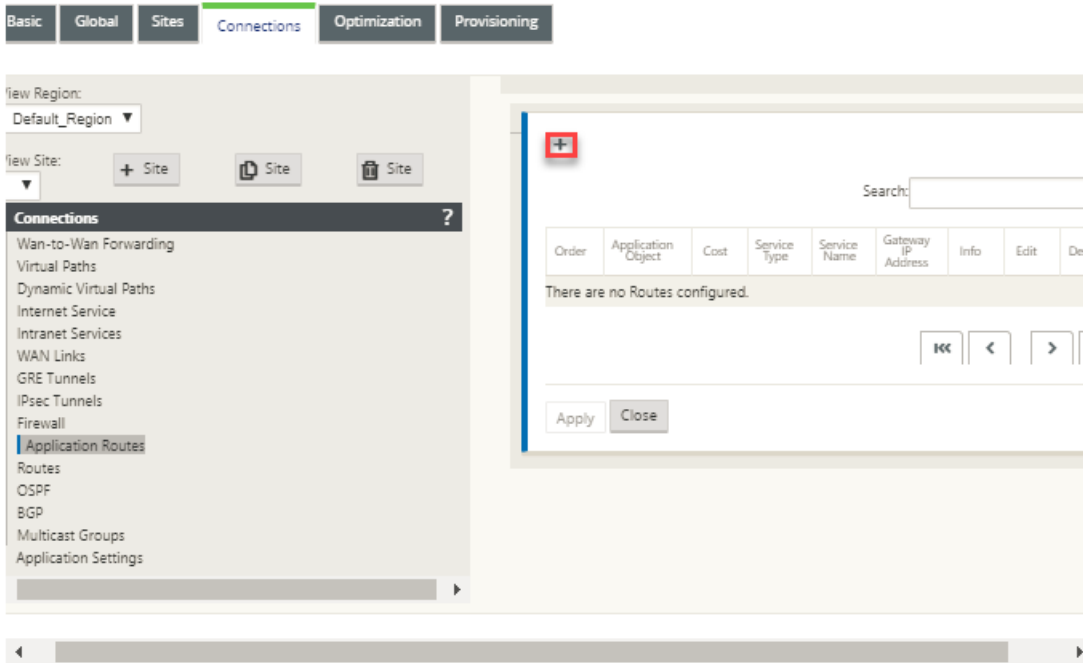
NetScaler SD-WAN allows you to define the application routes for the following services:

- **Virtual Path:** This service manages traffic across the Virtual Paths. A Virtual Path is a logical link between two WAN links. It comprises a collection of WAN Paths combined to provide high service-level communication between two SD-WAN nodes. The SD-WAN appliance measures the network on a per-path basis and adapts to changing application demand and WAN conditions. A Virtual Path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN Appliances reaches a configured threshold).
- **Internet:** This service manages traffic between an Enterprise site and sites on the public Internet. Internet traffic is not encapsulated. When congestion occurs, the SD-WAN actively manages bandwidth by rate-limiting Internet traffic relative to the Virtual Path, and Intranet traffic.
- **Intranet:** This service manages Enterprise Intranet traffic that has not been defined for transmission across a Virtual Path. Intranet traffic is not encapsulated. The SD-WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Under certain conditions, and if Intranet Fallback is configured on the Virtual Path, traffic that ordinarily travels through Virtual Path can instead be treated as Intranet traffic.
- **Local:** This service manages traffic local to the site that matches no other service. SD-WAN ignores traffic sourced and destined to a local route.
- **GRE Tunnel:** This service manages IP traffic destined for a GRE tunnel, and matches the LAN GRE tunnel configured at the site. The GRE Tunnel feature enables you to configure SD-WAN appliances to terminate GRE tunnels on the LAN. For a route with service type GRE Tunnel, the gateway must reside in one of the tunnel subnets of the local GRE tunnel.
- **LAN IPsec Tunnel:** This service manages IP traffic destined for a LAN IPsec tunnel, and matches the LAN IPsec tunnel configured at the site. The LAN IPsec Tunnel feature enables you to configure SD-WAN Appliances to terminate IPsec tunnels on the LAN or WAN side.

In order to perform service steering for applications, it is important to identify an application on the first packet itself. Initially, the packets flow through the IP route once the traffic is classified and the application is known, the corresponding application route is used. First packet classification is achieved by learning the IP subnets and ports associated with application objects. These are obtained using historical classification results of the DPI classifier, and user configured IP port match types.

To configure application routing:

1. In the Configuration Editor, navigate to **Connections > Application Routes**, and click +.



2. On the **Add** page, set the following parameters:

- **Application Object:** The application object, which you want to steer. The application objects created by you are listed here. For more information, see **Application Objects** section in [Application Classification](#) topic.

- **Routing Domain:** The routing domain to be used by the application route. Choose one of the configured routing domains.
- **Cost:** A weight to determine the route priority for this route. Lower-cost routes take precedence over higher-cost routes. The range is 1-65534. The default value is 5.
- **Service Type:** Select one of the following services. This maps the application to a service.
 - * **Virtual Path:** Identifies application traffic as Virtual Path traffic and matches a Virtual Path based on Virtual Path Rules. In the **Next Hop Site** field, enter the next-hop remote site to which Virtual Path packets will be directed.

Note

Any flow hitting the Virtual Path Application Routes will not go over dynamic virtual path.

- * **Internet:** Identifies application traffic as Internet traffic and matches the Internet Service.
- * **Intranet:** Identifies application traffic as Intranet traffic and matches an Intranet Service based on the Intranet Rules. In the **Intranet Service** field, select an intranet service to be used for the route.
- * **Local:** Identifies application traffic as local to the site and matches no service. Traffic sourced and destined to a local route will be ignored.

Note

For local service type, once the DPI classification is completed the configured IP routes take the routing decision.

- * **GRE Tunnel:** Identified the application traffic as destined for a GRE tunnel, and matches the LAN GRE tunnel configured at the site. In **the Gateway IP Address** field, enter the gateway IP Address that must be in the LAN GRE Tunnel's subnet. Select **Eligibility Based on Gateway** to enable the route to not receive any traffic when the Gateway is not reachable.
- * **LAN IPsec Tunnel:** Identified the application traffic as destined for a LAN IPsec tunnel, and matches the LAN IPsec tunnel configured at the site. In **IPsec Tunnel** field, select one of the configured IPsec tunnels. Select **Eligibility Based on Tunnel** to enable the route to not receive any traffic when the tunnel is not reachable.

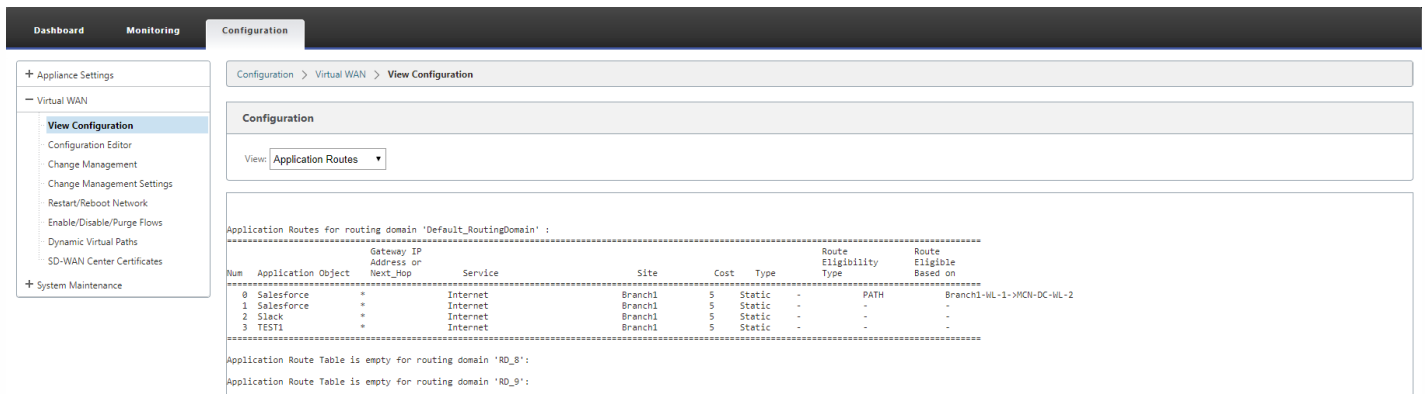
Note

Once you have selected a service for a custom application, do not change it.

- **Eligibility Based on Path:** Select to enable the route not to receive traffic when the specified path is down. In the **Path** field, specify the path to be used for determining route eligibility.

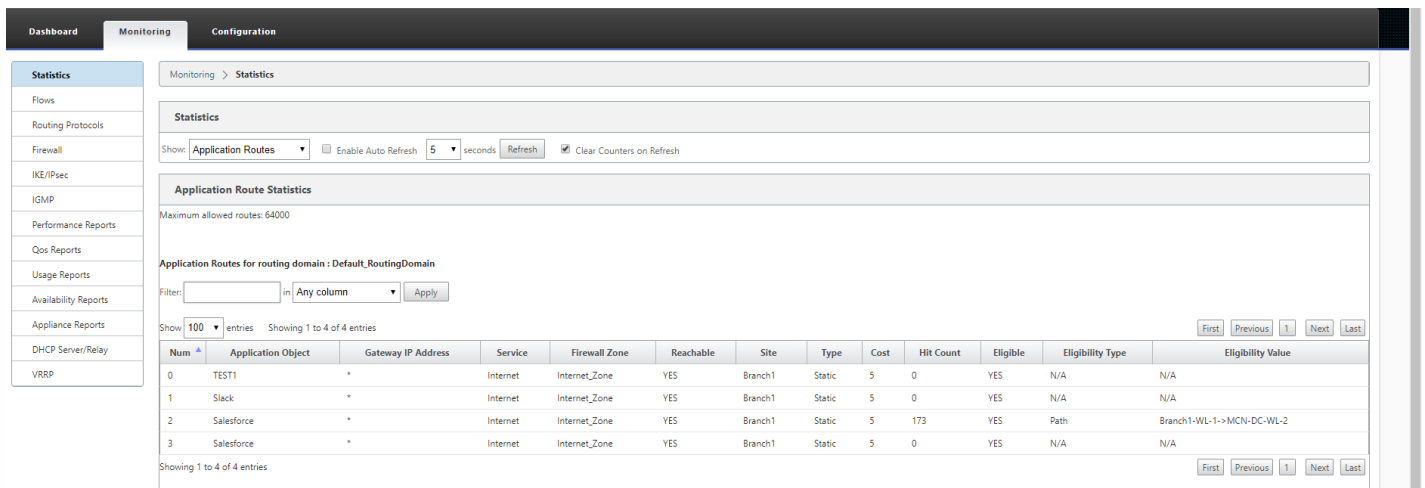
3. Click **Apply**.

To view the application routes configured on your SD-WAN appliance, In the SD-WAN GUI, navigate to **Configuration > Virtual WAN > View configuration**. Select **Application Routes** from the **View** drop-down menu.



To view statistics data for the application routes:

1. In the SD-WAN GUI, navigate to **Monitoring > Statistics**.
2. From the **Show** drop-down list, select **Application Routes**.



You can view the following statistics:

- **Application Object:** Name of the application object.
- **Gateway IP Address:** The gateway IP address used by application objects with GRE Tunnel service type.
- **Service:** The service type mapped to the application object.
- **Firewall Zone:** The firewall zone that this route falls in.
- **Reachable:** The status of the application route.
- **Site:** Name of the site.
- **Type:** Indicates if the route is static or dynamic.
- **Cost:** The priority of the route.
- **Hit Count:** The number of times the application route is used to steer the traffic.
- **Eligible:** Is the application route eligible to send the traffic.
- **Eligibility Type:** The type of route eligibility condition applied to this route. The eligibility type can be Path, Gateway or Tunnel.
- **Eligibility Value:** The value specified for the route eligibility condition.

Note

In the current release, applications that belong to application family, match type defined in application object, cannot be steered.



Route Filtering

Mar 01, 2018

How to Configure Route Import and Export Filters

1. In the **Configuration Editor**, navigate to **Connections > View Regions > View Site > [Site Name] > Route Learning Properties**.
2. Expand **Import Filters** and **Export Filters** to view the existing route filters. Import Filters are separate and distinct from Export Filters. You can configure up to 32 Export Filters.

Note

If there is only one Routing Domain configured, the Routing Domain column will not appear.

The screenshot displays the Citrix Configuration Editor interface. At the top, there are tabs for 'Basic', 'Global', 'Sites', 'Connections', 'Optimization', and 'Provisioning'. The 'Connections' tab is selected. Below the tabs, there are dropdowns for 'View Region: Default_Region' and 'View Site: MCN-5100'. A sidebar on the left lists various configuration categories, with 'Route Learning Properties' selected. The main area shows the 'Route Learning Properties' configuration page. At the top of this page, there is a 'Section:' dropdown set to 'Import Template', with a sub-menu open showing 'Import Template' and 'Export Template'. Below this is an 'Import Filter Template:' dropdown and 'Apply' and 'Refresh' buttons. The main configuration area is titled 'Route Learning Import Template:' and includes a '+ Add Template' and '- Delete Template' button. Below this is a 'Template Name:' field with the value 'New_Import_Tem...'. A table is displayed with the following columns: Order, Routing Domain, Source Router, Destination, Prefix, Next Hop, Protocol, Route Tag, Cost, Include, Delete, and Clone. The table contains one row with the following values: Order: 100, Routing Domain: Default_Routing1, Source Router: *, Destination: <Manual>, Prefix: eq, Next Hop: *, Protocol: Any, Route Tag: *, Cost: eq, Include: checked, Delete: (icon), Clone: (icon). Below the table, there is a checkbox for 'Export Route to Citrix Appliances' which is checked. There is also a field for 'NetScaler SD-WAN Cost' with the value '0' and a 'Service Type:' dropdown set to 'Local'. At the bottom of the configuration area, there are 'Apply' and 'Revert' buttons.

Navigate to **Import Filters** or **Export Filters** under the **BGP** or **OSPF** section.

Section: Import Filters

Order	Source Router	Destination	Prefix	Next Hop	Protocol	Route Tag	Cost	Include	Enabled	Delete	Clone
100	*	<Manual>	eq *	*	Any	*	eq *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Export Route to Citrix Appliances Eligibility Based On Gateway

NetScaler SD-WAN Cost: Service Type: Service Name:

Eligibility Based On Path

Path:

Section: Export Filters

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

Export OSPF Route Type: Export OSPF Route Weight:

200	<Manual>	eq *	eq *	Any	*	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
200	<Manual>	eq *	eq *	Any	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Use the following criteria to construct each Export Filter that you want to create.

Field Criteria	Description	Value(s)
Order	The Order in which filters are prioritized. The first filter that a route matches to will be applied to that route.	<ul style="list-style-type: none"> • 100 • 200 • 300 • 400 • 500 • 600
Routing Domain	To match routes from a specific routing domain, choose one of the configured Routing Domains from the drop-down menu.	<ul style="list-style-type: none"> • <Any> • Def_RD - default
Network Address	Enter the IP Address and Netmask or configured Network Object that describes the route's network.	<ul style="list-style-type: none"> • IP address
Prefix	To match routes by prefix, choose a match predicate from the drop-down menu and enter a Route prefix in the adjacent field.	<ul style="list-style-type: none"> • eq: Equal to • lt: Less than • le: Less than or equal to • gt: Greater than

Field Criteria	Description	or equal to Value(s)
NetScaler SD-WAN Cost	The method (predicate) and the SD-WAN Route Cost that are used to narrow the selection of routes exported.	<ul style="list-style-type: none"> Numeric value
Service Type	Select the Service types that will be assigned to matching routes from a list of the existing, supported NetScaler SD-WAN Services.	Service Types: <ul style="list-style-type: none"> Any Local Virtual Path Internet Intranet LAN GRE Tunnel LAN IPsec Tunnel
Site/Service Name	For Intranet, LAN GRE Tunnel, and LAN IPsec Tunnel, specify the name of the configured Service Type to use.	<ul style="list-style-type: none"> Text string
Gateway IP Address	If you choose LAN GRE Tunnel as the Service Type, enter the Gateway IP for the tunnel.	<ul style="list-style-type: none"> IP address
Include	Click the checkbox to Include routes that match this filter. Otherwise matching routes are ignored.	<ul style="list-style-type: none"> None
Enabled	Click the checkbox to Enable this filter. Otherwise the filter is ignored	<ul style="list-style-type: none"> None
Clone	Click the Clone icon to make copy of an existing Filter.	<ul style="list-style-type: none"> None

Route Summarization

Mar 01, 2018

With the increase in the size of the enterprise networks, the routers need to maintain large number of routes in their routing table. The routers require increased CPU, memory and bandwidth resources to look up the large routing tables, and maintain individual routes. You can configure a summary route with Local and Discard service types. This summary route is advertised to the next-hop devices.

To configure a summary route for a local subnet:

1. In the Configuration Editor, navigate to **Connections > Routes** and click the **+** to add a route.
2. On the **Add route** page, set the following parameters:
 - **Network IP Address:** The calculated summary route IP address.
 - **Cost:** A weight to determine the route priority for this route. Lower-cost routes take precedence over higher-cost routes. The range is 1-15. The default value is 5.
 - **Routing Domain:** Routing protocols providing single point of administration to manage a corporate network, or a branch office network, or a data center network.
 - **Service Type:** Select Local service type.

Note

You can select only **Local** and **Discard** service types for summary routes.

- **Gateway IP Address:** Gateway IP address for this route.
- **Export Route:** Exports the route to other connected sites.
- **Summary Route:** Advertises the route as a single summary route to the other connected devices, instead of all the other matching subnets.

Add

Network IP Address: 172.16.0.0/22

Routing Domain: Default_RoutingT

Cost: 5

Service Type: Local

Gateway IP Address:

Export Route

Summary Route

Eligibility Based On Path

Path: <None>

Eligibility Based On Gateway

Add Cancel

3. Click **Add**.

Configure Multicast Groups

Mar 01, 2018

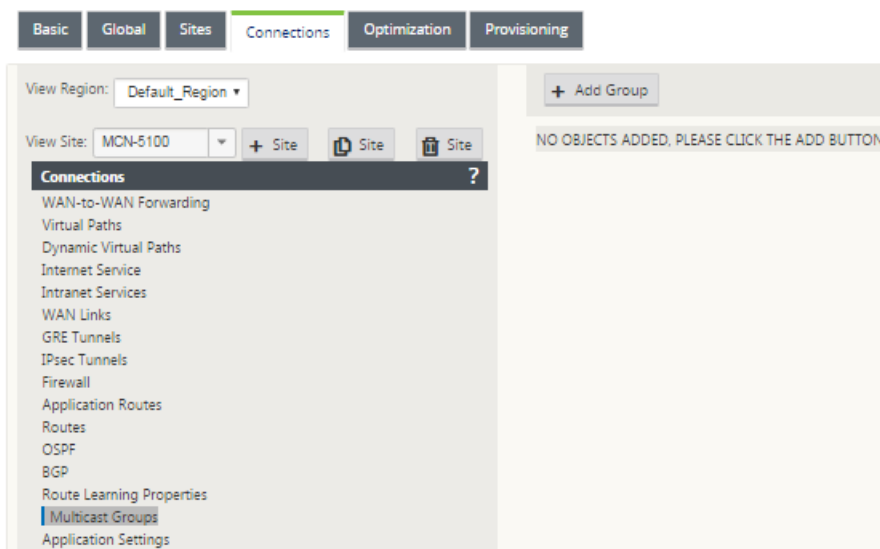
Multicast groups can be configured to support low bandwidth multicast traffic in simplified networks. You can define multicast groups such that the network administrator can control the source and destination of multicast traffic. You can configure different multicast group IP Address and set the source and destination virtual interfaces to appropriately pass-through multicast traffic.

Two primary use cases supported in SD-WAN are:

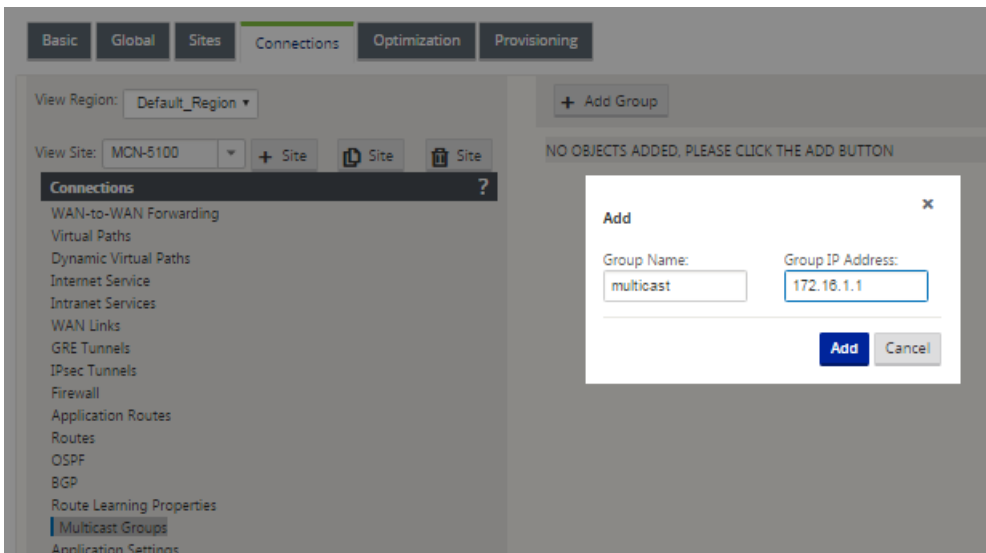
1. Support for existing multicast networks in the underlay.
2. Support for manually defined static multicast trees that allow forwarding multicast traffic through the overlay.

How to Configure Multicast Groups in SD-WAN GUI

1. In the SD-WAN GUI, go to **Configuration > Virtual WAN > Configuration Editor**. Open an existing configuration package.
2. Go to **Connections > View Region > View Site > <Site> > Multicast Groups**.

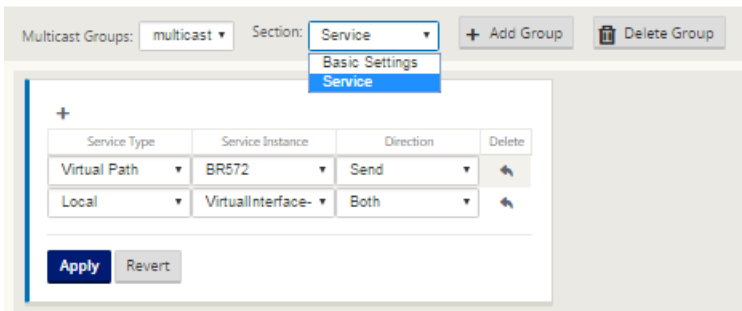


3. Expand **Multicast Groups**. Click **Add**. Add **Group Name** and **IP Address**.



4. Edit **Service** for the Multicast traffic.

- Basic settings: define the basic parameters of the multicast group. The only parameter available is the Multicast group IP address. This address may be a single IP address or an address and mask. All addresses or networks must be contained within the Class D address range (224.0.0.0/4).
 - Multicast Group IP: Configure a valid class D Multicast IP Address or Subnet.
 - Routing Domain: For multiple routing domains, configure valid routing domain which will be receiving Multicast traffic.
- Direction, Send: defines where multicast traffic will be accepted from. This section includes the following components:
 - Service Type: Local, Internet, Intranet, GRE Tunnel, Virtual Path. The Service Type on which Multicast traffic will be received.
 - Service Instance: The Service Name on which Multicast traffic will be received.
- Direction Receive: defines the services on which traffic will be replicated on. This section includes the following components:
 - Service Type: Local, Internet, Intranet, GRE Tunnel, Virtual Path. The Service Type on which Multicast traffic will be sent.
 - Service Instance: The Service Name on which Multicast traffic will be sent.

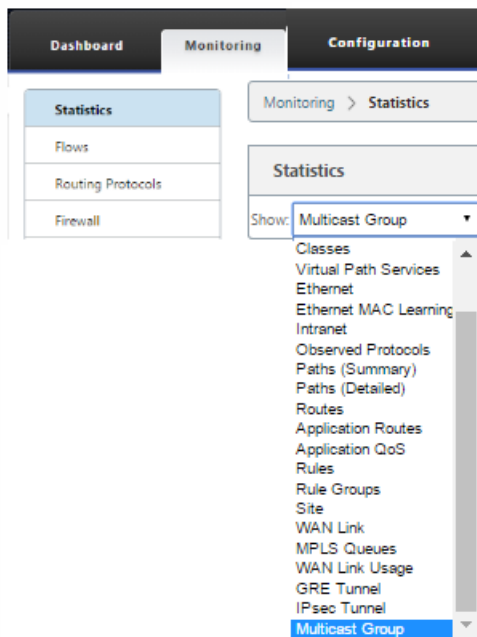


Note

1. Due to issues with session tracking, particularly as it involves forwarding a single packet on multiple interfaces, NAT lookups are modified to ignore multicast packets. Therefore, Static 1:1 NAT translation for multicast traffic is not supported in Release 9.3.1.
2. IGMP snooping is not supported in Release 9.3.1.
3. Multicast packets routed through the IP forwarder will have TTL performed. Since IGMP messages are sent with a TTL of 1, you need to avoid decrementing the TTL for replicated messages.

Monitoring Multicast Traffic

In the SD-WAN GUI, go to **Monitoring > Statistics**. Select **Multicast Group** from the drop-down list. This displays the statistics page for existing Multicast groups configured for a specific site in the SD-WAN GUI.



Monitoring > Statistics

Statistics

Show: Multicast Group Enable Auto Refresh 5 seconds Refresh Show latest data.

Multicast Group Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries First Previous 1 Next Last

Multicast Group	Packets Received	Kbps Received	Packets Sent	Kbps Sent
Group1	0	0	0	0
Group239	0	0	0	0

Showing 1 to 2 of 2 entries First Previous 1 Next Last

Multicast Group Source Services

Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries First Previous 1 Next Last

Multicast Group	Service Type	Service Name	Packets	Kbps
Group1	Virtual Path	AS-TB-CL1	0	0
Group239	LOCAL	Port1-VLAN0	0	0

Showing 1 to 2 of 2 entries First Previous 1 Next Last

Multicast Group Destination Services

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

Multicast Group	Service Type	Service Name	Packets	Kbps
Group1	Virtual Path	AS-TB-CL2	0	0
Group239	Virtual Path	AS-TB-CL1	0	0
Group239	Virtual Path	AS-TB-CL2	0	0
Group239	INTERNET	AS-TB-MCN-Internet	0	0

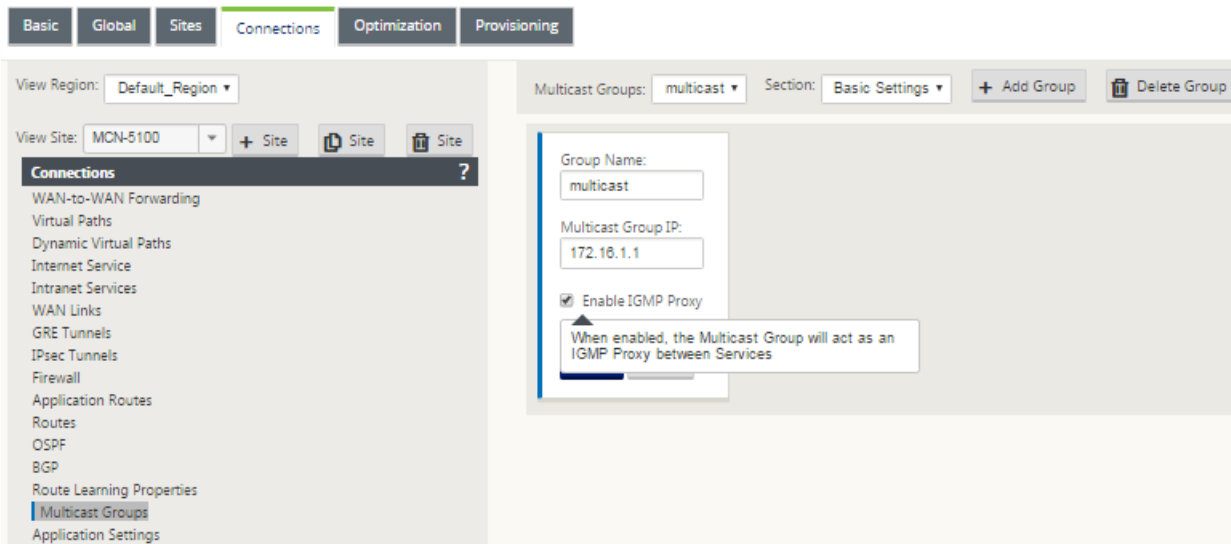
Showing 1 to 4 of 4 entries First Previous 1 Next Last

Configure IGMP Proxy

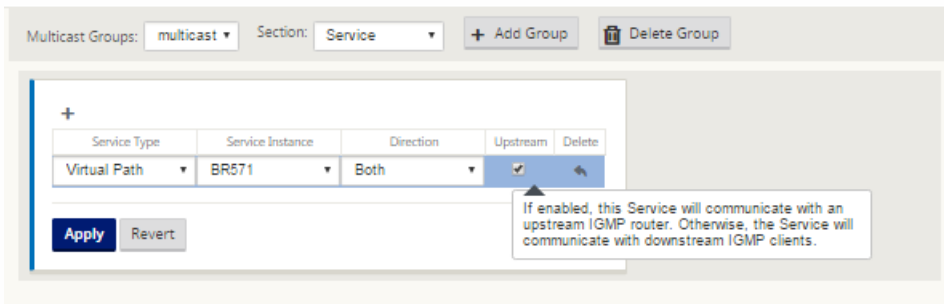
The ability to configure multicast groups to support low bandwidth multicast traffic in simplified networks is supported.

With static multicast group, network administrators can control the source and destination of the multicast traffic. In NetScaler SD-WAN 10.0, instead of statically configuring the multicast group, users can configure IGMP proxy for updating the upstream core networks with all the sources in the downstream networks of the edge.

1. In the SD-WAN GUI, go to **Connections > View Region > View Site > Site**.
2. Select **Multicast Groups > Basic Settings**. Click **Enable IGMP Proxy**.



3. Go to Services. Select Virtual Path as the Service Type to configure multicast group traffic.



In the SD-WAN GUI, under the **Virtual WAN** -> **View Configuration** tab, you can view the configured Multicast groups. You can also monitor Multicast Group traffic from the Monitoring tab.

Configure Virtual Path Route Cost

Mar 01, 2018

NetScaler SD-WAN supports the following routing enhancements related to data center administration.

For example; Consider SD-WAN network with two data centers; one in North America and one in Europe. You want all sites in North America to route traffic through the datacenter in North America and all sites in Europe to use Europe Datacenter. Previously, in SD-WAN 9.3 and earlier release versions, this functionality of datacenter administration was not supported. In SD-WAN 10.0, this issue is implemented with the introduction of Virtual Path Route cost.

- Virtual Path Route cost: You can configure Virtual Path route cost for individual virtual paths that will be added to the route cost when a route is learnt from a remote site.

This feature invalidates or deletes the WAN to WAN forwarding Cost.

- OSPF Route Cost: You can now import OSPF route cost (type1 metric) by enabling “**Copy OSPF Route Cost**” in import filters. OSPF Route cost is considered in route selection instead of SD-WAN cost. Cost up to 65534 instead of 15 is supported, but it is advisable to accommodate for appropriate virtual path route cost that are added if route is learnt from a remote site.
- BGP - VP cost to MED: You can now copy Virtual Path route cost for SD-WAN routes into BGP MED values when exporting (redistributing) SD-WAN routes to BGP peers. This can be set for individual neighbors by creating a BGP policy and applying it in the “OUT” direction for each neighbor.

1. Any site can have multiple virtual paths to other sites. In some cases, if there is a Branch to which there is connectivity to services through more virtual paths, there can be two virtual paths from the Branch site. One virtual path through DC1 and the other through DC2. DC1 could be an MCN and DC2 could be a Geo-MCN, and could be configured as another site with Static Virtual Path.

2. Add a default cost for each VP as 1. Virtual Path Route cost helps associate a cost to each virtual path of a site. This helps to manipulate route exchanges/updates over a specific virtual path instead of default site cost. With this, we can manipulate which data center to be preferred for sending out the traffic.

3. Allow cost to be configured within a small range of values (for example; 1-10) for each VP.

4. Virtual path cost should be added to any route shared with neighbor sites to indicate routing preference, including routes learned via Dynamic Routing.

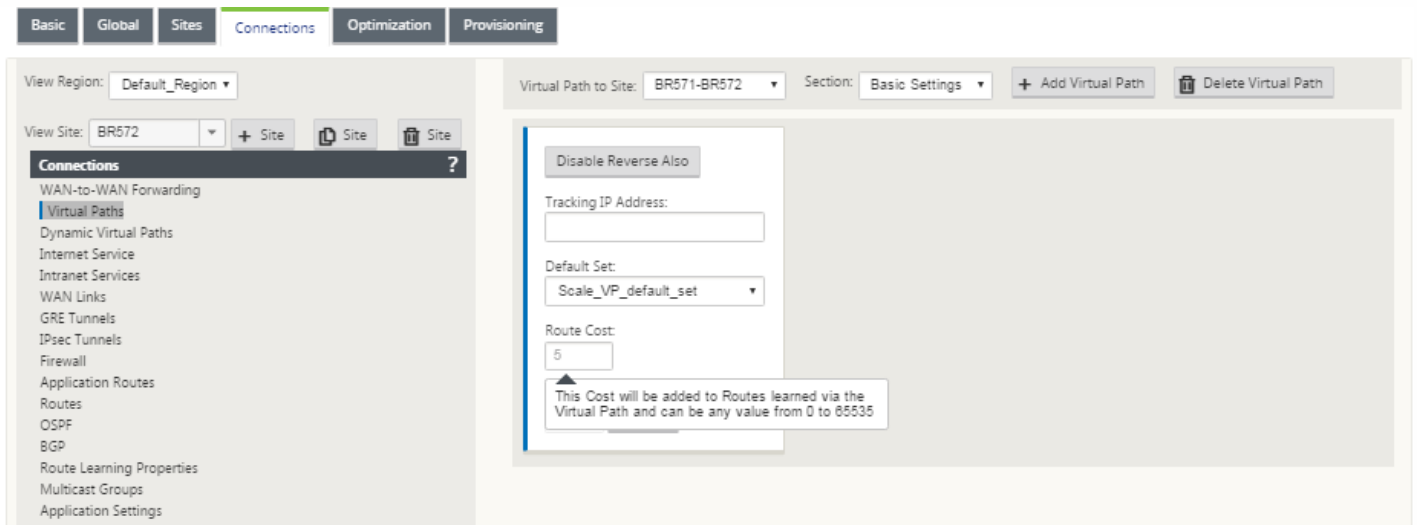
5. No Static Virtual Path should have a lower cost than a Dynamic Virtual Path.

Note

VP Route cost deprecates the WAN to WAN forwarding cost that existed in release versions earlier than 10.0. The routing decisions based on WAN to WAN forwarding costs have to be re-influenced by using VP route cost as the WAN to WAN forwarding cost has no significance when you migrate to release version 10.0.

How to Configure Virtual Path Route Cost

You can configure Virtual Path Route in SD-WAN GUI under **Connections-> View Region > View site > Virtual Paths > Basic Settings**. All routes are installed with basic NetScaler SD-WAN cost + VP route cost to influence route costs across multiple virtual paths.



Use Case

For example, there are subnets 172.16.2.0/24 and 172.16.3.0/24. Assume that there are two datacenters DC1 and DC2 that use both these subnets to transmit traffic to SD-WAN. With default virtual path route cost, you cannot influence routing since it depends on which route got installed first it could be either the DC2 first or the DC1 next.

With virtual path, you can influence specifically DC2 virtual path to have a higher virtual path route cost (for example; 10) while DC1 has default VP route cost of 5. This manipulation will help install routes with DC1 first and DC2 next for both.

You can have 4 routes, 2 routes to 172.16.2.0/24; one via DC1 with lower cost and then via DC2 with higher cost, and 2 more for 172.16.3.0/24.

Viewing Routing Table Summary for Virtual Path Route Cost

The routing table displays how same subnets advertised by two sites connected to a branch site over virtual path are installed with precedence of cost with Virtual Path route cost addition.

This figure below shows the route table with two different costs for the same route which is 172.16.6.0/24 with cost 10 and 11 for services **DC-Branch01** and **GEOMCN-Branch01** respectively.

Monitoring > Statistics

Statistics

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

Route Statistics

Maximum allowed routes: 16380

Routes for routing domain: Default_RoutingDomain

Filter: = Any column Apply

Show 100 entries Showing 1 to 7 of 7 entries First Previous Next Last

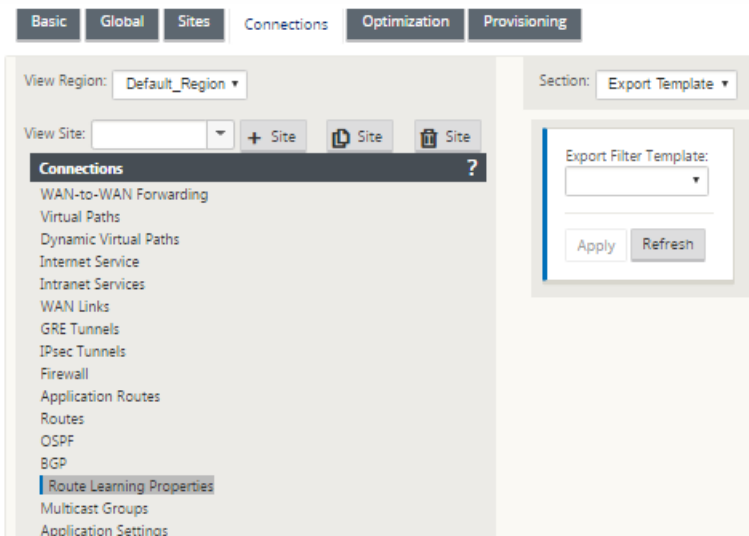
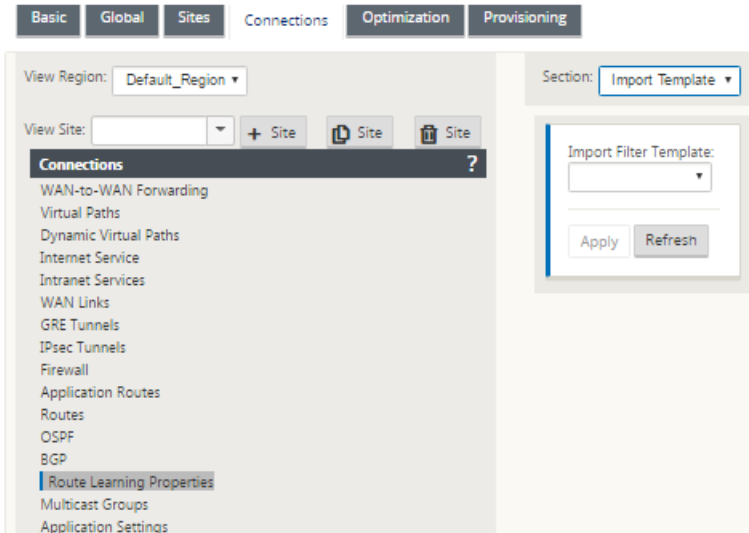
Name	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	HD Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.1.0/24	*	Local	Default_LAN_Zone	YES	*	Branch01	Static	-	-	5	7638100	YES	N/A	N/A
1	172.16.6.0/24	*	DC-branch01	Default_LAN_Zone	YES	*	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
2	172.16.3.0/24	*	DC-branch01	Default_LAN_Zone	YES	*	DC	Dynamic	Virtual WAN	YES	10	3942356	YES	N/A	N/A
3	172.16.6.0/24	*	GEOMON-branch01	Default_LAN_Zone	YES	*	GEOMON	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
4	172.16.4.0/24	*	GEOMON-branch01	Default_LAN_Zone	YES	*	GEOMON	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
5	0.0.0.0	*	Feathrough	Any	YES	*	*	Static	-	-	85525	0	YES	N/A	N/A
6	0.0.0.0	*	Discard	Any	YES	*	*	Static	-	-	85525	0	YES	N/A	N/A

Showing 1 to 7 of 7 entries First Previous Next Last

Configure Route Policy Filter Templates

Mar 05, 2018

In NetScaler SD-WAN 10.0, you can create multiple import or export filter templates with various filter rules and associate the template at each site. The user created site level import/export filter rules take more precedence. The template rules follow the user created rules when associated to the site in Route Learning section of Connections.



Configure Virtual Router Redundancy Protocol

Mar 01, 2018

Virtual Router Redundancy Protocol (VRRP) is a widely used protocol that provides device redundancy to eliminate the single point of failure inherent in the static default-routed environment. VRRP allows you to configure two or more routers to form a group. This group appears as a single default gateway with one virtual IP address and one virtual MAC address.

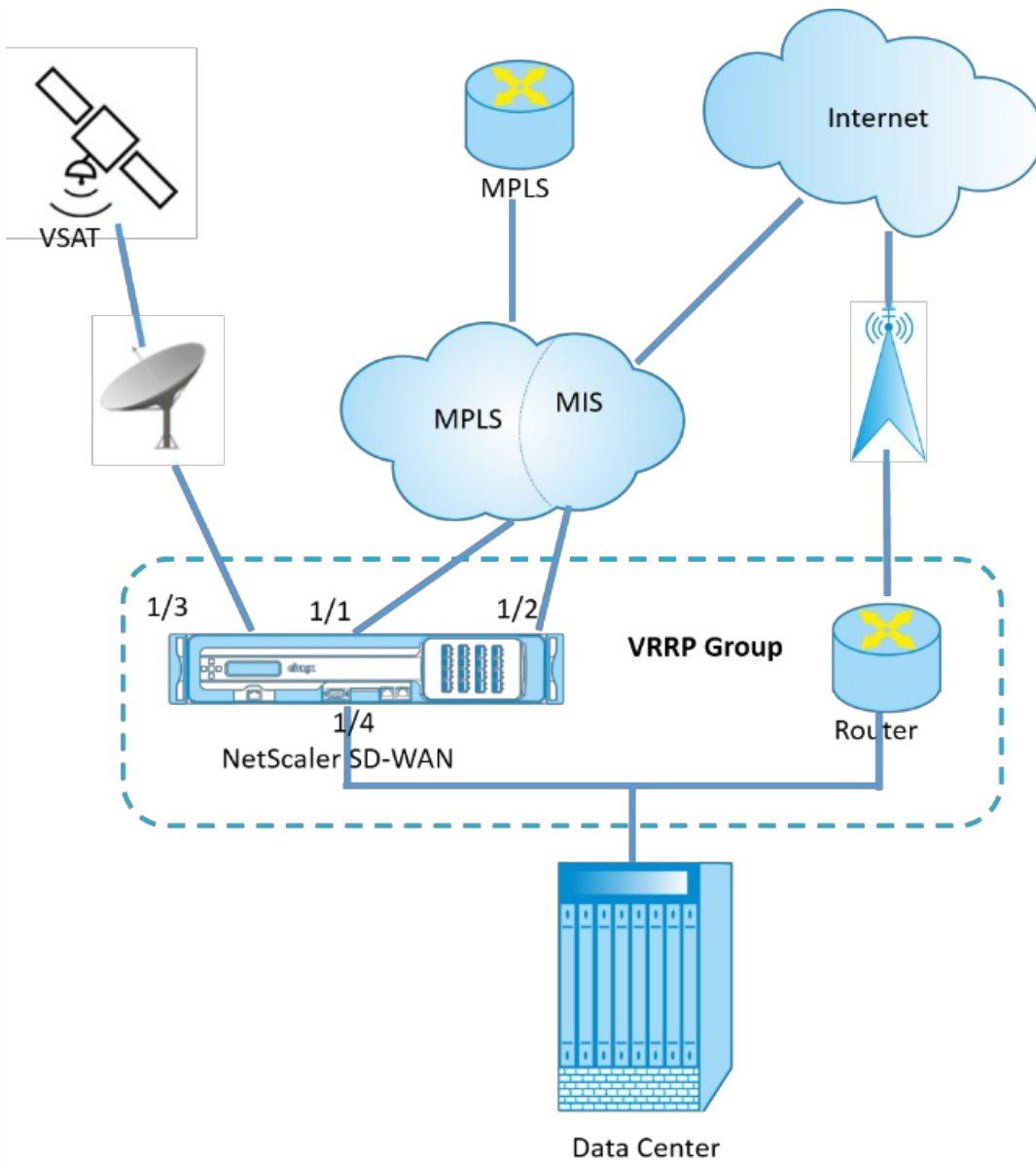
A back-up router automatically take overs if the primary / master router fails. In a VRRP set-up, the master router sends a VRRP packet known as an advertisement to the back-up routers. If the master router stops sending the advertisement, the back-up router sets the interval timer. If no advertisement is received within this hold period, the back-up router initiates the failover routine.

VRRP specifies an election process in which, the router with the highest priority becomes the master. If the priority are same among the routers, the router with the highest IP address become the master. The other routers are in backup state. The election process is initiated again if the master fails, a new router joins the group or an existing router leaves the group.

VRRP ensures a high availability default path without configuring dynamic routing or router discovery protocols on every end-host.

NetScaler SD-WAN 10.0 supports VRRP version 2 and version 3 to inter-operate with any third party routers. The SD-WAN appliance acts as a master router and direct the traffic to use Virtual Path Service between sites. You can configure the SD-WAN appliance as the VRRP master by configuring the Virtual Interface IP as the VRRP IP and by manually setting the priority to a higher value than the peer routers. You can configure the advertisement interval and the preempt option.

The below network diagram shows a NetScaler SD-WAN appliance and a router configured as a VRRP group. The SD-WAN appliance is configured to be the master. If the SD-WAN appliance fails, the back-up router takes-over within milliseconds, ensuring that there is no downtime.



To configuring VRRP instance:

1. In the Configuration Editor, navigate to **Sites** > Site name > **VRRP** and click **+**.

+	VRRP Group ID	Version	Priority	Advertisement Interval	Authentication type	Authentication text	Reclaim	Use Check
+	245	V3	255	1000	*	None	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply Revert

2. Configure a VRRP instance. Enter the values for the following fields:

- **VRRP group ID:** The VRRP group ID. The group ID should be a value range is 1 - 255. The same group ID should be configured on the back-up routers too.

Note

Currently you can configure up to four groups only.

- **Version:** The VRRP protocol version. You can choose between VRRP protocol V2 and V3.
- **Priority:** The priority of the NetScaler SD-WAN appliance for the VRRP group. The priority range is 1-254. Set this value to maximum (254) to make the SD-WAN appliance the master.

Note

If the router is the owner of the VRRP IP address, the Priority is set to 255 by default.

- **Advertisement Interval:** The frequency in milliseconds, with which the VRRP advertisements are sent when the SD-WAN appliance is the master. The default advertisement interval is one second.
- **Authentication Type:** You can choose **Plain Text** to enter an authentication string. The authentication string is sent as a plain text without any encryption in the VRRP Advertisements. Choose **None**, if you do not want to set up authentication.
- **Authentication Text:** The authentication string to be sent in the VRRP Advertisement. This option is enabled if the **Authentication Type** is **Plain Text**.

Note

Authentication is supported in VRRPv2 only.

- **Reclaim:** This enables preemption when the priority of the SD-WAN appliance is highest in the VRRP group. This is used in the VRRP election process.
- **Use V2 Checksum:** This enables compatibility with third party network devices for VRRPv3. By default, VRRPv3 uses v3 checksum computation method. Certain third party devices may only support VRRPv2 checksum computation. In such cases, enable this option.

3. Configure the VRRP IP address. Enter values for the following fields:

- **Virtual Interface:** The virtual interface to be used for VRRP. Choose one of the configured virtual interfaces.
- **Virtual IP Address:** The virtual IP address assigned to the virtual interface. Choose one of the configured virtual IP address for the virtual interface.
- **VRRP Router IP:** The virtual router IP address for the VRRP group. By default, the Virtual IP address of the SD-WAN appliance is assigned as the virtual router IP address.

+	VRRP Group ID	Version	Priority	Advertisement Interval	Authentication type	Authentication text	Reclaim	Use V2 Checksum
☰	245	V3	255	1000 *	None		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Router IPs +			
Virtual Interface	Virtual IP Address	VRRP Router IP	Delete
VirtualInterface-1	172.16.2.100/24	172.16.2.100	🗑️

Apply Revert

4. Click **Apply**.

VRRP Statistics

You can view the VRRP statistics under **Monitoring > VRRP Protocol**.

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

VRRP ID	Version	Interface(s)	State	Priority	Virtual Router IP	Advertisement Interval	Enable	Disable
20	2	LAN-7	Master	250	172.58.7.100	2000	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>
245	3	LAN	Master	200	172.58.5.20	1000	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>

You can view the following statistics data:

- **VRRP ID:** The VRRP group ID
- **Version:** The VRRP protocol version.
- **Interface:** The virtual interface used for VRRP.
- **State:** The VRRP state of the SD-WAN appliance. It indicates whether the appliance is a master or a backup.
- **Priority:** The priority of the NetScaler SD-WAN appliance for a VRRP Group
- **Virtual Router IP:** The virtual router IP address for the VRRP group.
- **Advertisement Interval:** The frequency of VRRP advertisements.
- **Enable:** Select this to enable the VRRP instance on the NetScaler SD-WAN appliance.
- **Disable:** Select this to disable the VRRP instance on the NetScaler SD-WAN appliance.

Limitations

- VRRP is supported in Gateway Mode deployment only.
- You can configure up to four VRRP ID's (VRID).
- Up to sixteen virtual network interfaces can participate in VRID.
- VRRP is not supported in HA deployment.

Configure Network Objects

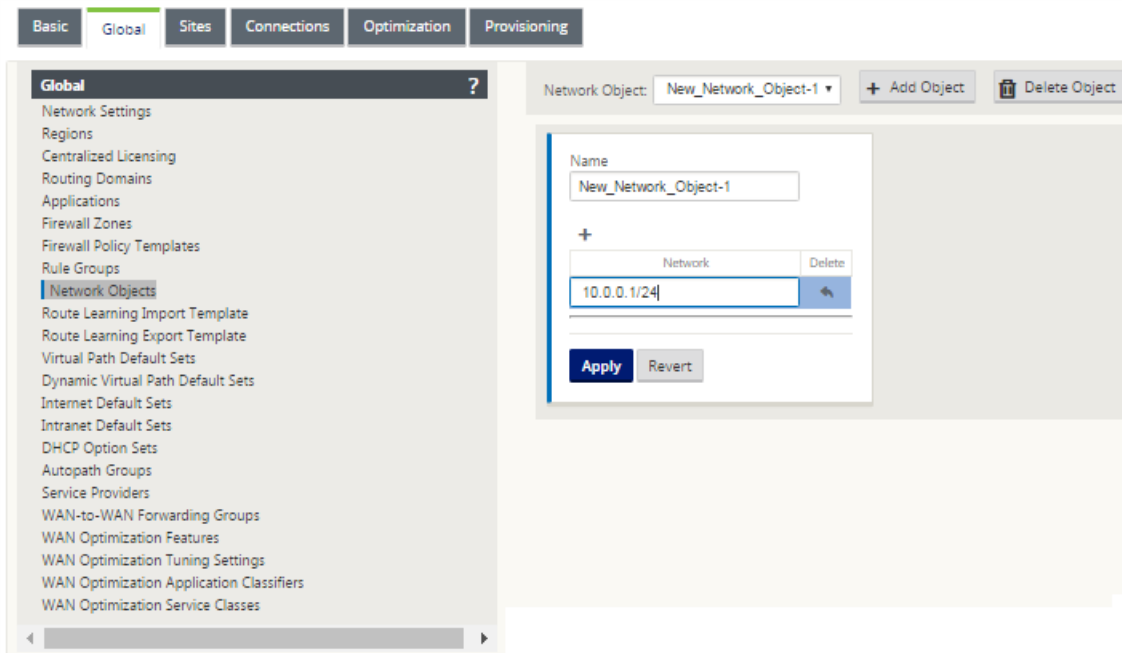
Mar 01, 2018

NetScaler SD-WAN introduces the option of adding Network Objects under the Global panel in the Configuration Editor. You can group multiple subnets together and reference a single Network Object when defining a Route Filter rather than creating a filter for each subnet.

To configure Network Objects:

1. In the **Configuration Editor**, navigate to **Global** → **Network Objects**, click **Add (+)**.
2. Click **Add (+)** under Networks.
3. Enter the **IP Address** and **Subnet** of the new Network Object.
4. Click **Apply** to save the settings.

To edit the Network Object's name, click on the name of the Network Object and enter a new name.



Routing Support for LAN Segmentation

Mar 01, 2018

The SD-WAN Standard and Enterprise Edition appliances implement LAN segmentation across distinct sites where either appliance is deployed. The appliances recognize and maintain a record of the LAN side VLANs available, and configure rules around what other LAN segments (VLANs) can connect to at a remote location with another SD-WAN Standard or Enterprise Edition appliance.

The above capability is implemented through the use of a Virtual Routing and Forwarding (VRF) table that is maintained in the SD-WAN Standard or Enterprise Edition appliance, which keeps track of the remote IP address ranges accessible to a local LAN segment. This VLAN-to-VLAN traffic would still traverse the WAN through the same pre-established Virtual Path between the two appliances (no new paths need to be created).

An example use case for this functionality is that a WAN administrator may be able to segment local branch networking environment through a VLAN, and provide some of those segments (VLANs) access to DC-side LAN segments that have access to the internet, while others may not obtain such access. The configuration of the VLAN-to-VLAN associations is achieved through the MCN's Configuration Editor in the SD-WAN management web interface.

Secure Peering

Mar 01, 2018

Enterprise Edition appliance can be installed at the data center and has the capability to initiate auto or manual secure peering, create SSL profile and associate service class, and join the appliance to a Windows Domain Controller for allowing users/administrator to make use of the extended rich feature of standalone WANOP appliance.

Following are the deployment modes supported for Auto Secure Peering and Manual Secure Peering:

Auto Secure Peering Deployments

1. [To perform auto secure peering to an EE appliance from a standalone WANOP / SDWAN SE/WANOP on the DC site.](#)

Steps to initiate this deployment:

- o WANOP DC appliance is in LISTEN ON mode (2312/Any non-standard port) and Branch EE is in CONNECT-TO mode.
- o WANOP DC initiates automatic secure peering to an EE appliance which installs the Private CA Certs and CERT KEY Pairs and configure CONNECT-TO on the EE appliance with WANOPs LISTEN-ON IP.

2. [To perform Auto-secure peering initiated from EE appliance at DC site and Branch site EE appliance.](#)

Steps to initiate this deployment:

- o EE DC appliance is in LISTEN ON mode (on port 443). Branch EE is in CONNECT-TO mode.
- o EE DC appliance initiates automatic secure peering to an EE Branch appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the EE Branch appliance with DC EE's LISTEN-ON IP.
- o LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which "Redirect to WANOP" is enabled.

3. [Auto Secure Peering initiated from EE Appliance at DC site and Branch with WANOP/ SDWAN SE appliance.](#)

Steps to initiate this deployment:

- o EE DC appliance is in LISTEN ON mode (on port 443). Branch WANOP / SDWAN SE is in CONNECT-TO mode.
- o EE DC appliance initiates automatic secure peering to Branch WANOP / SDWAN SE appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the EE appliance with DC EE's LISTEN-ON IP.

Manual Secure Peering Deployments

4. [Manual Secure Peering initiated from EE appliance at DC site to Branch EE Appliance.](#)

Steps to initiate this deployment:

- o EE DC appliance is in LISTEN ON mode (on port 443). Branch EE is in CONNECT-TO mode.
- o LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which "Redirect to WANOP"

is enabled.

- o Manually upload CA and Cert Key pair certificates obtained from authentic source of certificate authority.

5. [Manual Secure Peering initiated from EE appliance at DC site to Branch WANOP/SDWAN-SE Appliance.](#)

Steps to initiate this deployment:

- o EE DC appliance is in LISTEN ON mode (on port 443). Branch WANOP / SDWAN SE is in CONNECT-TO mode.
- o LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which “Redirect to WANOP” is enabled
- o Manually upload CA and Cert Key pair certificates obtained from authentic source of certificate authority.

Auto Secure Peering to an EE appliance from a Standalone SD-WAN SE and WANOP Appliance on the DC site

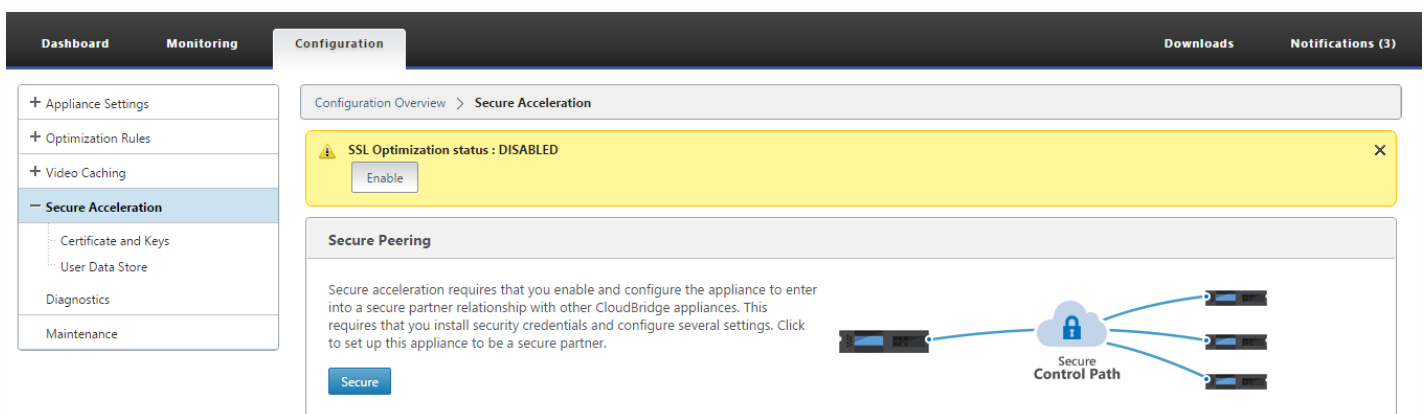
Jul 11, 2018

Configuration

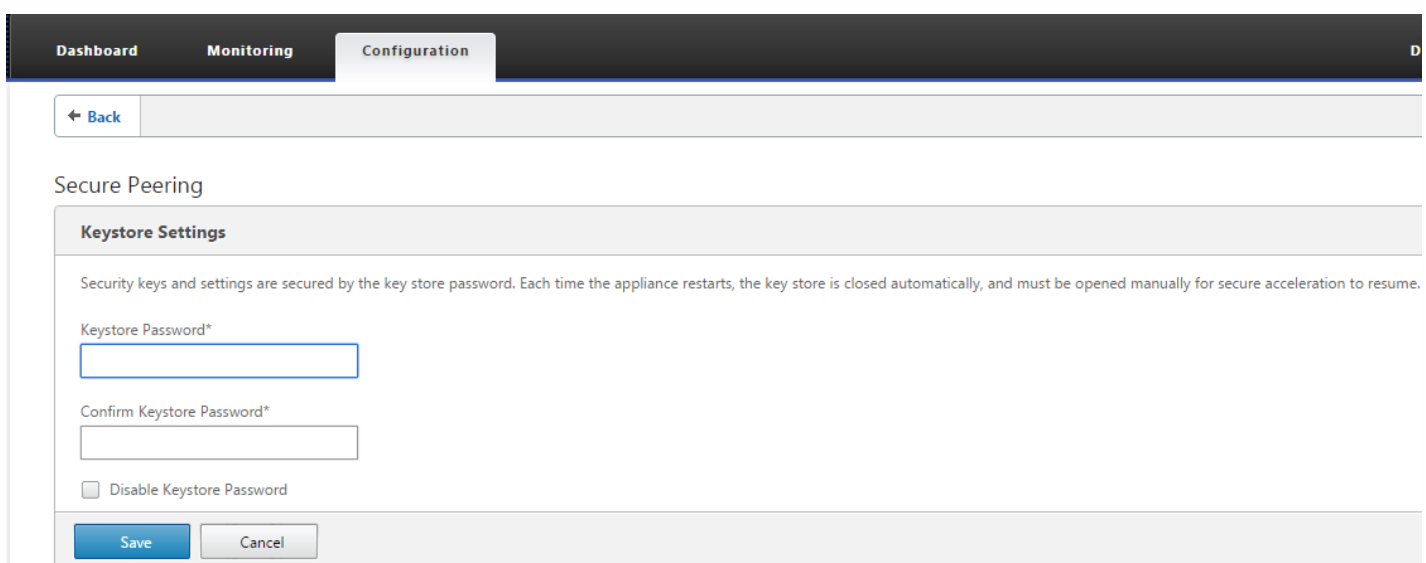
To perform auto secure peering on an EE appliance from a standalone SD-WAN SE and WANOP appliance on the DC Side:

- WANOP DC appliance is in LISTEN ON mode (2312/Any non-standard port).
- Branch EE is in CONNECT-TO mode.
- WANOP DC initiates automatic secure peering to an EE appliance which installs the Private CA Certs and CERT KEY Pairs and configure CONNECT-TO on the EE appliance with WANOPs LISTEN-ON IP.

1. On a standalone WANOP appliance at the data center, click **Secure** in the **Secure Peering** pane of the **Secure Acceleration** page.



2. Configure the keystore settings by providing the **keystore password** or by disabling the keystore.

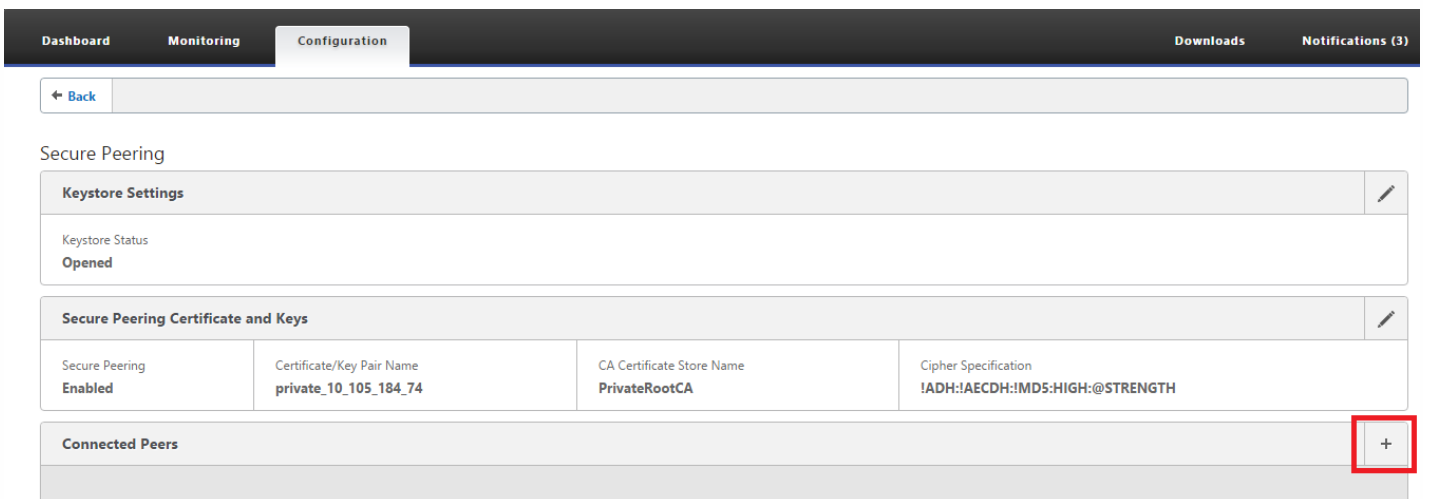


3. **Enable Secure Peering** by selecting **Private CA** to perform AUTOMATIC SECURE PEERING.



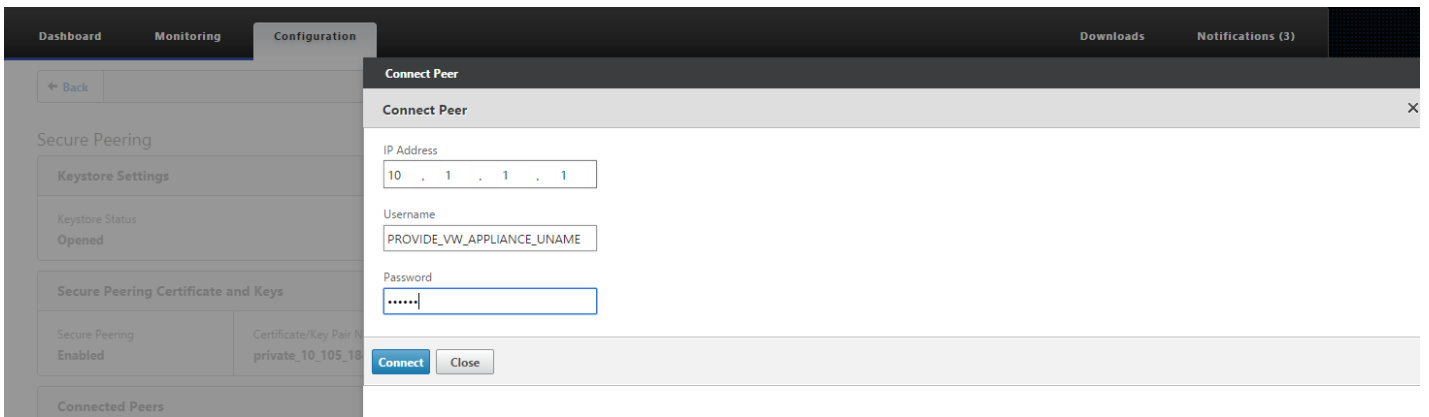
4. The appliance level CA certificate and private Certificate and Key will be generated on the local WANOP and a table to add a REMOTE PEER TO Perform AUTO secure peering with is displayed.

5. Click on the '+' icon and a popup window to add IP address with username and password is displayed. After successful authentication with the remote IP with credentials provided, a request is sent to the remote machine that installs CA Certificate and the Private certificate and key for itself locally (on the remote machine).

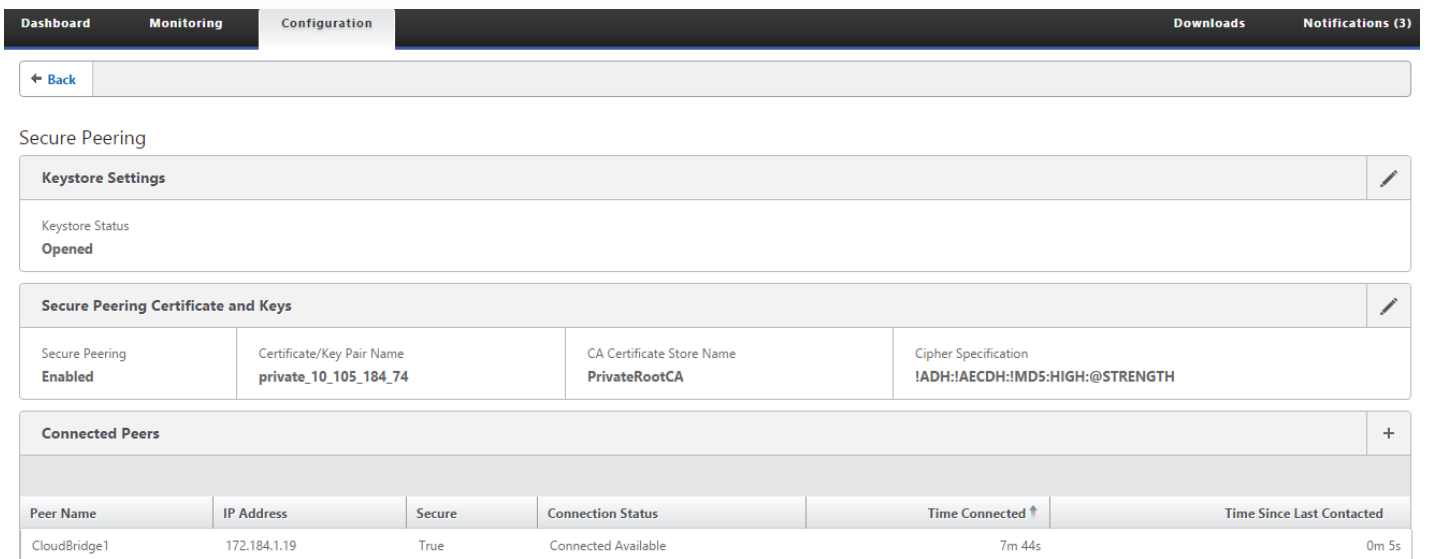


Note

- IP Address – IP Address of remote ENTERPRISE EDIT ION APPLIANCE MANAGEMENT IP
- Username – Username of remote ENTERPRISE EDIT ION APPLIANCE
- Password – Password of remote ENTERPRISE EDIT ION APPLIANCE



After Successful Authentication, you will see Secure Peering as TRUE and the partner IP address as one of the Virtual IP address of the remote Enterprise Edition Appliance.



↑ VIP of Remote EE App

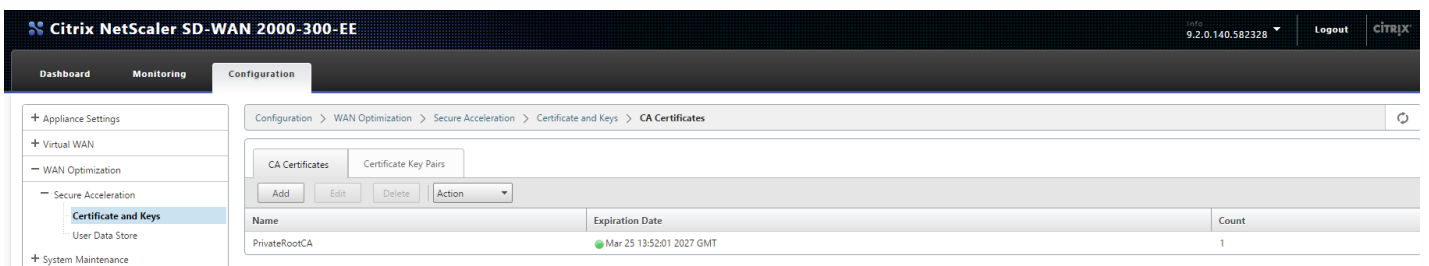
Monitoring

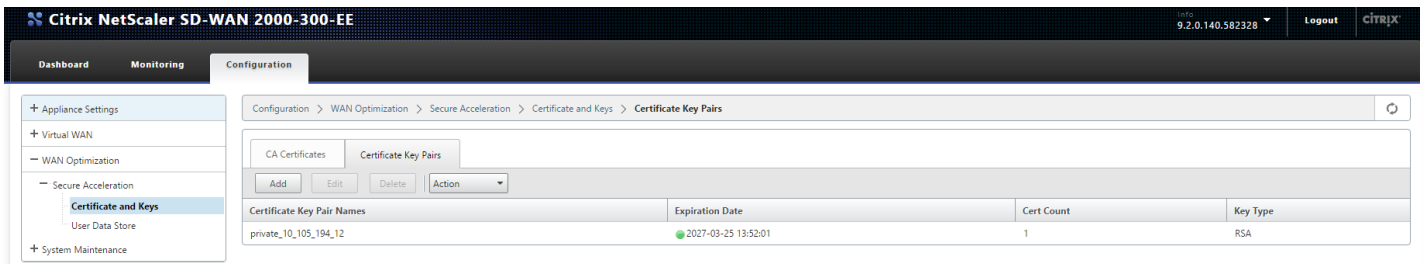
View Secure Partner Information on the Enterprise Edition Appliance under **WANOPTIMIZATION > Partners** in the **Monitoring** page.

a. Data Store Encryption can be performed on the Enterprise Edition appliance through feature enablement from the MCN under Optimization node for an Enterprise Edition appliance.

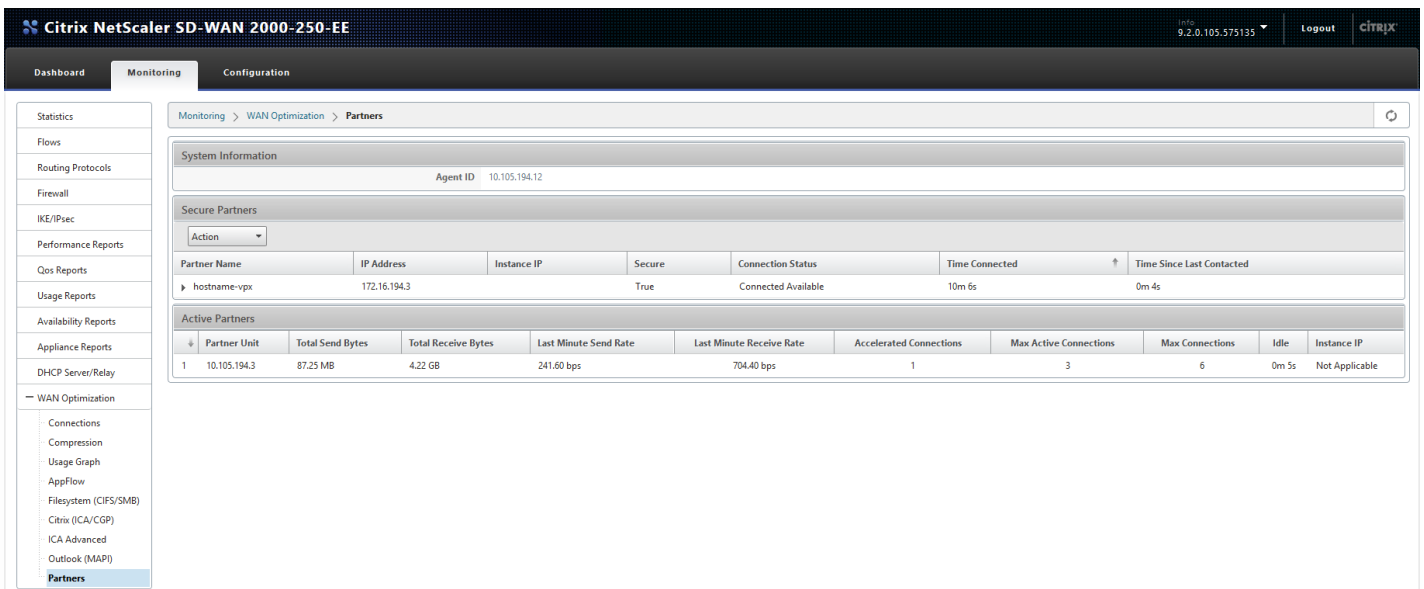
b. For an Enterprise Edition appliance, secure peering will always be enabled.

1. To validate if the **Private CA** and **Private Certificate Key** pair is generated successfully, review the information below:

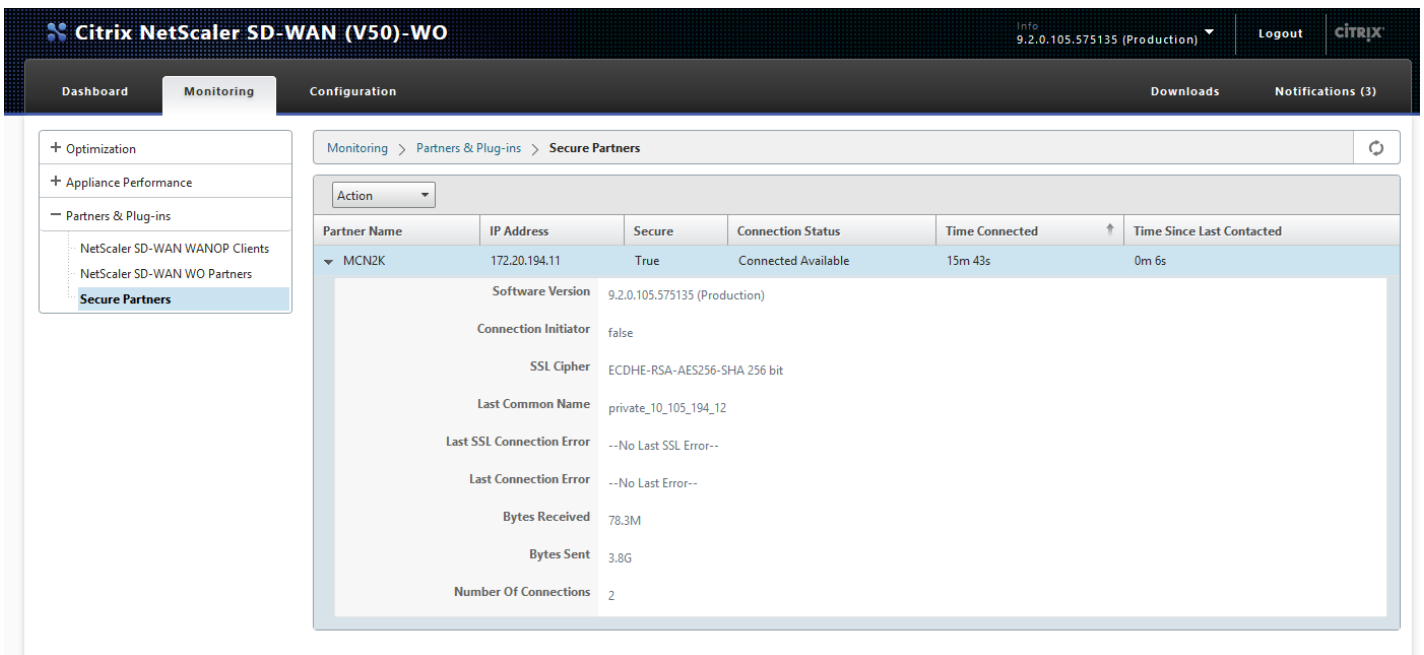




2. View **Secure Partner Information** on the Enterprise Edition appliance under **Monitoring > WAN Optimization > Partners** page.



3. On partner appliance, view **Secure Partner Information** of the Enterprise Edition appliance under **Monitoring > Partners & Plug-ins > Secure Partners** page.



Troubleshooting

1. View **Secure Partner Success / Failure Information** on the Enterprise Edition appliance under **Monitoring > WAN**

Optimization > Partners > Secure Partners page.

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE interface. The breadcrumb navigation is 'Monitoring > WAN Optimization > Partners'. The left sidebar shows 'Partners' selected under 'WAN Optimization'. The main content area displays 'System Information' with Agent ID 10.105.194.12. Below is the 'Secure Partners' section with a table listing partner details.

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Below the table is a detailed view for the selected partner, including:

- Software Version: 9.2.0.105.575135 (Production)
- Connection Initiator: true
- SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_3
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 4.2G
- Bytes Sent: 87.2M
- Number Of Connections: 1

At the bottom, an 'Active Partners' table shows:

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. On partner appliance, view Secure Partner Information on the Enterprise Edition appliance under **Monitoring > Partners & Plug-ins > Secure Partners** page.

The screenshot shows the Citrix NetScaler SD-WAN (V50)-WO interface. The breadcrumb navigation is 'Monitoring > Partners & Plug-ins > Secure Partners'. The left sidebar shows 'Secure Partners' selected under 'Partners & Plug-ins'. The main content area displays 'System Information' with Agent ID 10.105.194.12. Below is the 'Secure Partners' section with a table listing partner details.

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCN2K	172.20.194.11	True	Connected Available	15m 43s	0m 6s

Below the table is a detailed view for the selected partner, including:

- Software Version: 9.2.0.105.575135 (Production)
- Connection Initiator: false
- SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_12
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 78.3M
- Bytes Sent: 3.8G
- Number Of Connections: 2

3. On partner appliance, view Secure Partner Information on the Enterprise Edition appliance under **Monitoring > Appliance Performance > Logging** page.

- + Optimization
- Appliance Performance
 - Compression Engine
 - Logging**
 - WCCP
 - AppFlow
 - Load Statistics
- + Partners & Plug-ins

Monitoring > Appliance Performance > Logging Refresh

Record	Date/Time	Details
5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{}}
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{}}
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{}}
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{}}
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{}}
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: PAYLOAD: {"params":{"system_info":{}}
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5337	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5336	Mar 01, 2017 05:43:59	syslog::!AECDH:IMD5:HIG:@STRENGTH", "connectto":["169.254.1.20:443", "169.254.1.20:2312"], "listenon": ["10.105.194.3:2312", "172.16.194.3:443", "172.16.194.3:2312"], "publish":{"publishenabled":true, "securepeerenabled":true}}
5335	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"body":"yes", "ssl_partner":{"autodiscovery":true, "castorename":"PrivateRootCA", "certkeyname":"private_10_105_194_3", "certverifyaction":{"sig_exp_only","certverifycommonnames":[],"ciphers":"ADH

Auto Secure Peering Initiated from EE Appliance at DC Site and Branch Site EE Appliance

Jul 11, 2018

Configuration

Steps to initiate this deployment:

- EE DC appliance is in LISTEN ON mode (on port 443).
- Branch EE appliance is in CONNECT-TO mode.
- EE DC appliance initiates automatic secure peering to an EE Branch appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the EE Branch appliance with DC EE's LISTEN-ON IP.
- LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which "Redirect to WANOP" is enabled.

To configure auto secure peering on a new Enterprise Edition appliance at DC:

1. In the SD-WAN web GUI, navigate to **Configuration > WAN Optimization > Secure Acceleration > Secure Peering**.

The screenshot shows the Citrix NetScaler SD-WAN 2000-300-EE GUI. The breadcrumb navigation is Configuration > WAN Optimization > Secure Acceleration > Secure Peering. The 'Secure Peering' status is 'Disabled'. There are buttons for 'SSL Profile' and 'Windows Domain'. Below, the 'SSL Profiles' section contains a description of SSL acceleration and an 'Add Profile' button. A diagram labeled 'Secure Data Path' shows a central cloud icon connected to several server icons.

2. Configure keystore by providing the keystore password or by disabling keystore.

Secure Peering

The screenshot shows the 'Keystore Settings' page. It contains a text box explaining that security keys are secured by the keystore password and must be opened manually. There is a checkbox for 'Enable Keystore Password' which is currently unchecked. At the bottom, there are 'Save' and 'Cancel' buttons.

This screenshot shows the 'Keystore Settings' page with more options. The 'Keystore Status' is set to 'Open' via a dropdown menu. There are three checkboxes: 'Change Keystore Password', 'Disable Keystore Password', and 'Reset Keystore', all of which are currently unchecked. 'Save' and 'Cancel' buttons are at the bottom.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Keystore Password*
.....

Confirm Keystore Password*
.....

3. Enable **Secure Peering** by selecting **Private CA** to perform AUTOMATIC SECURE PEERING.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

Enable Secure Peering

Certificate Configuration

Private CA CA Certificate

Secure Peering Certificate and Keys			
Secure Peering Enabled	Certificate/Key Pair Name private_10_105_194_12	CA Certificate Store Name PrivateRootCA	Cipher Specification !ADH:!AECDH:!MD5:HIGH:@STRENGTH

4. Click on the '+' icon and to add IP with username and password. After successful authentication with the remote IP and credentials provided, a request is sent to the remote machine that will install CA Certificate and the Private cert and key for itself locally on the remote machine.

Note

IP Address – IP Address of remote EE Appliance MANAGEMENT IP

Username – Username of remote EE Appliance

Password – Password of remote EE Appliance

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE interface. The 'Configuration' tab is active, and the 'Connect Peer' dialog box is open. The dialog box contains the following fields:

- IP Address: 10 . 105 . 194 . 3
- Username: admin
- Password:

Buttons for 'Connect' and 'Close' are visible at the bottom of the dialog box. The background shows the 'Secure Peering' configuration page with 'Keystore Settings' and 'Secure Peering Certificate and Keys' sections.

Monitoring

1. To validate if the Private CA and Private Certificate Key pair is generated successfully, review the information displayed below.

Citrix NetScaler SD-WAN 2000-250-EE 9.2.0.104.574814 Logout CITRIX

Dashboard Monitoring Configuration

Configuration > Secure Acceleration > Certificate and Keys > CA Certificates

CA Certificates Certificate Key Pairs

Add Edit Delete Action

Name	Expiration Date	Count
PrivateRootCA	Feb 14 04:28:55 2027 GMT	1

Citrix NetScaler SD-WAN 2000-250-EE 9.2.0.104.574814 Logout CITRIX

Dashboard Monitoring Configuration

Configuration > Secure Acceleration > Certificate and Keys > Certificate Key Pairs

CA Certificates Certificate Key Pairs

Add Edit Delete Action

Certificate Key Pair Names	Expiration Date	Cert Count	Key Type
private_10_105_194_12	2027-02-13 20:28:55	1	RSA

2. View **Secure Partner Information** on the Enterprise Edition Appliance under **Monitoring > WAN Optimization > Partners** page.

Citrix NetScaler SD-WAN 2000-250-EE 9.2.0.105.575135 Logout CITRIX

Dashboard Monitoring Configuration

Monitoring > WAN Optimization > Partners

System Information

Agent ID 10.105.194.12

Secure Partners

Action

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

3. On partner appliance, view **Secure Partner Information** on the Enterprise Edition Appliance under **Monitoring > Partners & Plug-ins > Secure Partners** page.

The screenshot shows the Citrix NetScaler SD-WAN (V50)-WO interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Monitoring' tab is active, and the breadcrumb path is 'Monitoring > Partners & Plug-ins > Secure Partners'. A left-hand menu lists various optimization and performance options, with 'Secure Partners' selected. The main content area displays a table of Secure Partners. One partner, 'MCN2K', is expanded to show detailed configuration and status information.

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCN2K	172.20.194.11	True	Connected Available	15m 43s	0m 6s

Expanded details for MCN2K:

- Software Version: 9.2.0.105.575135 (Production)
- Connection Initiator: false
- SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_12
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 78.3M
- Bytes Sent: 3.8G
- Number Of Connections: 2

Troubleshooting

1. View Secure Partner Success / Failure Information on the Enterprise Edition Appliance under **Monitoring > WAN Optimization > Partners > Secure Partners** page.

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Monitoring' tab is active, and the breadcrumb path is 'Monitoring > WAN Optimization > Partners'. A left-hand menu lists various reports and optimization options, with 'Partners' selected. The main content area displays a table of Secure Partners. One partner, 'hostname-vpx', is expanded to show detailed configuration and status information.

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Expanded details for hostname-vpx:

- Software Version: 9.2.0.105.575135 (Production)
- Connection Initiator: true
- SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
- Last Common Name: private_10_105_194_3
- Last SSL Connection Error: --No Last SSL Error--
- Last Connection Error: --No Last Error--
- Bytes Received: 4.2G
- Bytes Sent: 87.2M
- Number Of Connections: 1

Active Partners table:

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. On partner Appliance, view Secure Partner Information on the Enterprise Edition Appliance under **Monitoring > Partners & Plug-ins > Secure Partners** page.

Citrix NetScaler SD-WAN (V50)-WO Info 9.2.0.105.575135 (Production) Logout CITRIX

Dashboard **Monitoring** Configuration Downloads Notifications (3)

Monitoring > Partners & Plug-ins > **Secure Partners**

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCNZK	172.20.194.11	True	Connected Available	15m 43s	0m 6s

Software Version: 9.2.0.105.575135 (Production)
 Connection Initiator: false
 SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
 Last Common Name: private_10_105_194_12
 Last SSL Connection Error: --No Last SSL Error--
 Last Connection Error: --No Last Error--
 Bytes Received: 78.3M
 Bytes Sent: 3.8G
 Number Of Connections: 2

3. On partner Appliance, view Secure Partner Information on the Enterprise Edition Appliance under **Monitoring > Appliance Performance > Logging** page.

Dashboard **Monitoring** Configuration

Monitoring > WAN Optimization > **Partners**

System Information
Agent ID: 10.105.184.70

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname1	172.184.4.48		True	Connected Available	13m 4s	0m 3s

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connecti
No items							

- + Optimization
- Appliance Performance
 - Compression Engine
 - Logging**
 - WCCP
 - AppFlow
 - Load Statistics
- + Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Record	Date/Time	Details
5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: PAYLOAD: [{"params":{"system_info":{}}
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5337	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5336	Mar 01, 2017 05:43:59	syslog::!AECDH:IMD5:HIGH:@STRENGTH", "connectto":["169.254.1.20:443", "169.254.1.20:2312"], "listenon": ["10.105.194.3:2312", "172.16.194.3:443", "172.16.194.3:2312"], "publish":{"publishenabled":true, "securepeerenabled":true}}
5335	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"body":"yes", "ssl_partner":{"autodiscovery":true, "castorename":"PrivateRootCA", "certkeyname":"private_10_105_194_3", "certverifyaction":"sig_exp_only", "certverifycommonnames":["ciphers":"ADH

Auto Secure Peering Initiated from EE Appliance at DC Site and Branch with Standalone SD-WAN SE and WANOP Appliance

Jul 11, 2018

Steps to initiate this deployment:

- EE DC appliance is in LISTEN ON mode (on port 443).
- Branch standalone SD-WAN SE and WANOP is in CONNECT-TO mode.
- EE DC appliance initiates automatic secure peering to Branch standalone SDWAN SE and WANOP appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the EE appliance with DC EE's LISTEN-ON IP.

Configuration

To configure a new Enterprise Edition appliance with auto secure peering at the DC site:

1. In the SD-WAN web GUI, navigate to **Configuration > WAN Optimization > Secure Acceleration > Secure Peering**.

The screenshot shows the Citrix NetScaler SD-WAN 2000-300-EE web GUI. The breadcrumb navigation is Configuration > WAN Optimization > Secure Acceleration. The 'Secure Peering' section shows 'Keystore Status' as 'Opened' and 'Secure Peering Status' as 'Disabled'. Below this, there are tabs for 'SSL Profile' and 'Windows Domain'. The 'SSL Profiles' section contains a descriptive text about SSL acceleration and an 'Add Profile' button. To the right, there is a diagram labeled 'Secure Data Path' showing a central server icon connected to multiple client icons.

2. Configure keystore by providing the keystore password or by disabling the keystore.

The screenshot shows the 'Keystore Settings' configuration page in the Citrix NetScaler SD-WAN 2000-250-EE web GUI. The 'Keystore Status*' dropdown menu is set to 'Open'. Below the dropdown are three checkboxes: 'Change Keystore Password', 'Disable Keystore Password', and 'Reset Keystore', all of which are currently unchecked. At the bottom of the form are 'Save' and 'Cancel' buttons.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

3. Enable **Secure Peering** by selecting **Private CA** to perform AUTOMATIC SECURE PEERING.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

Enable Secure Peering

Certificate Configuration

Private CA CA Certificate

Secure Peering Certificate and Keys			
Secure Peering	Certificate/Key Pair Name	CA Certificate Store Name	Cipher Specification
Enabled	private_10_105_194_12	PrivateRootCA	IADH:IAECDH:IMD5:HIGH:@STRENGTH

4. Click on the '+' icon and to add IP with username and password. After successful authentication with the remote IP and credentials provided, a request is sent to the remote machine that will install CA Certificate and the Private cert and key for itself locally on the remote machine.

Note

IP Address – IP Address of remote WANOP Standalone or Standard Edition Appliance MANAGEMENT IP.

Username – Username of remote WANOP Standalone or Standard Edition Appliance.

Password – Password of remote WANOP Standalone or Standard Edition Appliance.

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE interface. The 'Connect Peer' dialog box is open, displaying the following information:

- IP Address: 10 . 105 . 194 . 3
- Username: admin
- Password: [masked]

Buttons for 'Connect' and 'Close' are visible at the bottom of the dialog. The background shows the 'Secure Peering' configuration page with 'Secure Peering' status as 'Enabled'.

5. After Successful Authentication, you can view Secure Peering as TRUE and the partner IP as one of the Virtual IP of

the remote WANOP Standalone appliance.

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE Configuration page. The 'Secure Peering' section is expanded, showing 'Keystore Settings' with 'Keystore Status' set to 'Opened'. Below this, the 'Secure Peering Certificate and Keys' section is expanded, displaying a table with the following data:

Secure Peering	Certificate/Key Pair Name	CA Certificate Store Name	Cipher Specification
Enabled	private_10_105_194_12	PrivateRootCA	IADH:IAECDH:IMDS:HIGH:@STRENGTH

Below the table, the 'Connected Peers' section is expanded, showing a table with the following data:

Partner Name	IP Address	Secure	Connection Status	Time Connected †	Time Since Last Contacted
hostname-vpx	172.16.194.3	True	Connected Available	0m 13s	0m 3s

A 'Done' button is visible at the bottom left of the configuration area.

Monitoring

1. To validate if the Private CA and Private Certificate Key pair is generated successfully, review the information below.

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE Configuration page, specifically the 'CA Certificates' section. The breadcrumb navigation is 'Configuration > Secure Acceleration > Certificate and Keys > CA Certificates'. The page displays a table with the following data:

Name	Expiration Date	Count
PrivateRootCA	Feb 14 04:28:55 2027 GMT	1

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE Configuration page, specifically the 'Certificate Key Pairs' section. The breadcrumb navigation is 'Configuration > Secure Acceleration > Certificate and Keys > Certificate Key Pairs'. The page displays a table with the following data:

Certificate Key Pair Names	Expiration Date	Cert Count	Key Type
private_10_105_194_12	2027-02-13 20:28:55	1	RSA

2. View Secure Partner Information on the Enterprise Edition appliance under **Monitoring > WAN Optimization > Partners** page.

Citrix NetScaler SD-WAN 2000-250-EE Info: 9.2.0.105.575135 | Logout | CITRIX

Dashboard | **Monitoring** | Configuration

Monitoring > WAN Optimization > Partners

System Information
Agent ID: 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

3. On partner appliance, View Secure Partner Information on the Enterprise Edition appliance under **Monitoring > Partners & Plug-ins > Secure Partners** page.

Citrix NetScaler SD-WAN (V50)-WO Info: 9.2.0.105.575135 (Production) | Logout | CITRIX

Dashboard | **Monitoring** | Configuration | Downloads | Notifications (3)

Monitoring > Partners & Plug-ins > Secure Partners

Partner Name: MCN2K | IP Address: 172.20.194.11 | Secure: True | Connection Status: Connected Available | Time Connected: 15m 43s | Time Since Last Contacted: 0m 6s

Software Version: 9.2.0.105.575135 (Production)

Connection Initiator: false

SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit

Last Common Name: private_10_105_194_12

Last SSL Connection Error: --No Last SSL Error--

Last Connection Error: --No Last Error--

Bytes Received: 78.3M

Bytes Sent: 3.8G

Number Of Connections: 2

Troubleshooting

1. View Secure Partner Success / Failure Information on the Enterprise Edition appliance under **Monitoring > WAN Optimization > Partners > Secure Partners** page.

Citrix NetScaler SD-WAN 2000-250-EE

Info: 9.2.0.105.575135 | Logout | CITRIX

Dashboard | **Monitoring** | Configuration

Monitoring > WAN Optimization > Partners

System Information: Agent ID 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Software Version: 9.2.0.105.575135 (Production)
 Connection Initiator: true
 SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
 Last Common Name: private_10_105_194_3
 Last SSL Connection Error: --No Last SSL Error--
 Last Connection Error: --No Last Error--
 Bytes Received: 4.2G
 Bytes Sent: 87.2M
 Number Of Connections: 1

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. On partner appliance, view **Secure Partner Information** on the Enterprise Edition appliance under **Monitoring > Partners & Plug-ins > Secure Partners** page.

Citrix NetScaler SD-WAN (V50)-WO

Info: 9.2.0.105.575135 (Production) | Logout | CITRIX

Dashboard | **Monitoring** | Configuration | Downloads | Notifications (3)

Monitoring > Partners & Plug-ins > Secure Partners

Secure Partners

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCN2K	172.20.194.11	True	Connected Available	15m 43s	0m 6s

Software Version: 9.2.0.105.575135 (Production)
 Connection Initiator: false
 SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
 Last Common Name: private_10_105_194_12
 Last SSL Connection Error: --No Last SSL Error--
 Last Connection Error: --No Last Error--
 Bytes Received: 78.3M
 Bytes Sent: 3.8G
 Number Of Connections: 2

3. On partner appliance, view **Secure Partner Information** on the Enterprise Edition appliance under **Monitoring > Appliance Performance > Logging** page.

- + Optimization
- Appliance Performance
 - Compression Engine
 - Logging**
 - WCCP
 - AppFlow
 - Load Statistics
- + Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Record	Date/Time	Details
5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: PAYLOAD: [{"params":{"system_info":{}}
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5337	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5336	Mar 01, 2017 05:43:59	syslog::!AECDH:IMD5:HIGH:@STRENGTH", "connectto":["169.254.1.20:443", "169.254.1.20:2312"], "listenon": ["10.105.194.3:2312", "172.16.194.3:443", "172.16.194.3:2312"], "publish":{"publishenabled":true, "securepeerenabled":true}}
5335	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"body":"yes", "ssl_partner":{"autodiscovery":true, "castorename":"PrivateRootCA", "certkeyname":"private_10_105_194_3", "certverifyaction":"sig_exp_only", "certverifycommonnames":["ciphers":"ADH

Manual Secure Peering Initiated from EE Appliance at DC Site and Branch EE Appliance

Jul 11, 2018

Steps to initiate this deployment:

- EE DC appliance is in LISTEN ON mode (on port 443).
- Branch EE appliance is in CONNECT-TO mode.
- LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which “Redirect to WANOP” is enabled.
- Manually upload CA and Cert Key pair certificates obtained from authentic source of certificate authority.

Configuration

To configure auto secure peering initiated from an EE appliance at DC site and EE appliance at Branch site:

1. Upload **CA Certificate** and **CA Key Certificate** obtained from authentic certificate and provide to SD-WAN as shown below.

Name	Expiration Date	Count
CA	Feb 25 01:39:42 2032 GMT	1

Certificate Key Pair Names	Expiration Date	Cert Count	Key Type
CAKeyPair	2033-07-18 20:01:18	1	RSA

2. On a new EE appliance at the DC site, in the SD-WAN web GUI, go to **Configuration > Secure Acceleration > Secure Peering**.

Citrix NetScaler SD-WAN 2000-300-EE 9.2.0.140.582328 Logout CITRIX

Dashboard Monitoring Configuration

Configuration > WAN Optimization > Secure Acceleration

Secure Peering

Keystore Status Opened	Secure Peering Status Disabled
----------------------------------	--

SSL Profile Windows Domain

SSL Profiles

SSL acceleration allows the appliance to compress SSL traffic such as HTTPS and SSL-encrypted XenApp/XenDesktop (ICA/CGP) traffic. Secure partner configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server-side NetScaler SD-WAN WO appliance (only) and SSL-specific configuration (called an SSL Profile) for each group of SSL servers. This step should be skipped on a client-side appliance.

[Add Profile](#)

3. Configure keystore by providing the keystore password or by disabling the keystore.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

[Save](#) [Cancel](#)

Citrix NetScaler SD-WAN 2000-250-EE 9.2.0.105.575135 Logout CITRIX

Dashboard Monitoring Configuration

← Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*
Open

Change Keystore Password
 Disable Keystore Password
 Reset Keystore

[Save](#) [Cancel](#)

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

[Save](#) [Cancel](#)

4. Enable secure peering by selecting **CA Certificate** radio button and providing uploaded CA and CA Key pair certificates appropriately as shown below.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

Enable Secure Peering

Certificate Configuration

Private CA CA Certificate

Certificate/Key Pair Name

CA Certificate Store Name

Certificate Verification*

SSL Cipher Specification

Edit Cipher Specification

5. Provide Remote machine's Virtual IP along with Port 443 as shown below.

Listen On and Connect To

Auto Discovery is typically enabled, when enabled, any authenticated peers can connect via the Listen On addresses. If disabled, secure communications are allowed only with peers on the Connect To list.

Enable Auto-Discovery

Listen On

×

× +

Publish NAT addresses to peers

NAT Addresses

× +

Connect To

× +

Monitoring

1. To validate if the **Private CA** and **Private Certificate Key** pair is generated successfully, review the information below.

The screenshot shows the Citrix NetScaler SD-WAN 2000-250-EE monitoring interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar lists various monitoring categories, with 'Partners' selected under 'WAN Optimization'. The main content area displays 'Monitoring > WAN Optimization > Partners'.

System Information
 Agent ID: 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. On partner appliance, **View Secure Partner Information** on the Enterprise Edition appliance under **Monitoring >**

Partners > Secure Partners page.

Monitoring > WAN Optimization > Partners

System Information
Agent ID: 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3	10.105.194.12	True	Connected Available	2m 0s	0m 13s

Active Partners

Troubleshooting

1. View **Secure Partner Success / Failure** Information on the Enterprise Edition Appliance under **Monitoring > WAN Optimization > Partners > Secure Partners** page.

Monitoring > WAN Optimization > Partners

System Information
Agent ID: 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3	10.105.194.12	True	Connected Available	10m 6s	0m 4s

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

Manual Secure Peering initiated from EE appliance at DC site to Branch Standalone SD-WAN SE and WANOP Appliance

Jul 11, 2018

Steps to initiate this deployment:

- Enterprise Edition DC appliance is in LISTEN ON mode (on port 443). The Branch standalone SD-WAN SE and WANOP WANOP / SD-WAN SE is in CONNECT-TO mode.
- LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which “Redirect to WANOP” is enabled.
- Manually upload CA and Cert Key pair certificates obtained from authentic source of certificate authority.

Configuration

1. Upload **CA Certificate** and **CA Key Certificate** obtained from authentic certificate and provide to SD-WAN as shown below.

The screenshot shows the Citrix NetScaler SD-WAN 2000-300-EE GUI. The navigation path is Configuration > WAN Optimization > Secure Acceleration > Certificate and Keys > CA Certificates. The interface includes a table with the following data:

Name	Expiration Date	Count
CACert	Feb 25 01:39:42 2032 GMT	1

The screenshot shows the Citrix NetScaler SD-WAN 2000-300-EE GUI. The navigation path is Configuration > WAN Optimization > Secure Acceleration > Certificate and Keys > Certificate Key Pairs. The interface includes a table with the following data:

Certificate Key Pair Names	Expiration Date	Cert Count	Key Type
CertKeyPair	2033-07-19 03:01:18	1	RSA

2. On a new EE appliance at the DC site, in the SD-WAN web GUI, go to **Configuration > Secure Acceleration > Secure Peering**.

The screenshot shows the Citrix NetScaler SD-WAN 2000-300-EE GUI. The navigation path is Configuration > WAN Optimization > Secure Acceleration. The Secure Peering section shows the following configuration:

- Keystore Status: Opened
- Secure Peering Status: Disabled
- SSL Profile: Selected
- Windows Domain: Selected

The SSL Profiles section includes a diagram illustrating the Secure Data Path, showing traffic flow between a client and a server through a secure connection.

3. Enable the keystore by providing the **keystore password** or disable the keystore.

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Keystore Password*
.....

Confirm Keystore Password*
.....

4. Enable secure peering by selecting **CA Certificate** radio button and providing uploaded CA and CA Key pair certificates appropriately as shown below.

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

Enable Secure Peering

Certificate Configuration

Private CA CA Certificate

Certificate/Key Pair Name
CAKeyPair

CA Certificate Store Name
CA

Certificate Verification*
Signature/Expiration

SSL Cipher Specification
!ADH:!AECDH:!MD5:HIGH:@STRENG

Edit Cipher Specification

5. Provide Remote machine's Virtual IP along with Port 443 as shown below.

Listen On and Connect To

Connect To
172.16.194.3 :443 x +

Done

Listen On and Connect To		
NAT IP published Yes	Auto Discovery Enabled	Listening On 172.20.194.11:443
		Connected to 172.16.194.3:443

Done

Monitoring

1. View Secure Partner Information on the Enterprise Edition appliance under **Monitoring > WAN Optimization > Partners** page.

Monitoring > WAN Optimization > Partners

System Information
Agent ID: 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. On partner appliance, View Secure Partner Information on the Enterprise Edition appliance under **Monitoring > Partners > Secure Partners** page.

Monitoring > WAN Optimization > Partners

System Information
Agent ID: 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	2m 0s	0m 13s

Software Version: 9.2.0.140.582328 (Production)
 Connection Initiator: true
 SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
 Last Common Name: mike.199.130
 Last SSL Connection Error: --No Last SSL Error--
 Last Connection Error: --No Last Error--
 Bytes Received: 138.4K
 Bytes Sent: 77.1K
 Number Of Connections: 0

Troubleshooting

1. View **Secure Partner Success / Failure Information** on the Enterprise Edition Appliance under **Monitoring > WAN Optimization > Partners > Secure Partners** page.

Citrix NetScaler SD-WAN 2000-250-EE

Info: 9.2.0.105.575135 | Logout | CITRIX

Dashboard | **Monitoring** | Configuration

Monitoring > WAN Optimization > Partners

System Information: Agent ID 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpx	172.16.194.3		True	Connected Available	10m 6s	0m 4s

Software Version: 9.2.0.105.575135 (Production)
 Connection Initiator: true
 SSL Cipher: ECDHE-RSA-AES256-SHA 256 bit
 Last Common Name: private_10_105_194_3
 Last SSL Connection Error: --No Last SSL Error--
 Last Connection Error: --No Last Error--
 Bytes Received: 4.2G
 Bytes Sent: 87.2M
 Number Of Connections: 1

Active Partners

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1 10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. On partner appliance, view **Secure Partner Information** on the Enterprise Edition appliance under **Monitoring > Appliance Performance > Logging** page.

Citrix NetScaler SD-WAN (V50)-WO

Info: 9.2.0.105.575135 (Production) | Logout | CITRIX

Dashboard | **Monitoring** | Configuration | Downloads | Notifications (3)

Monitoring > Appliance Performance > Logging

Record ↑ | Date/Time | Details

5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"system_info":{}}
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: PAYLOAD: [{"params":{"system_info":{}}
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6785]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5337	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5336	Mar 01, 2017 05:43:59	syslog:!!AECDH:IMDS:HIGH:@STRENGTH", "connectto":["169.254.1.20:443", "169.254.1.20:2312"], "listenon": ["10.105.194.3:2312", "172.16.194.3:443", "172.16.194.3:2312"], "publish": [], "publishenabled": true, "securepeerenabled": true}
5335	Mar 01, 2017 05:43:59	syslog:Mar 1 05:43:59 hostname-vpx NITRO[6762]: PAYLOAD: [{"params":{"body":{"ssl_partner": {"autodiscovery": true, "castorename": "PrivateRootCA", "certkeyname": "private_10_105_194_3", "certverification": "sig_exp_only", "certverifycommonnames": [], "ciphers": "IADH

Domain Join and Delegate User Creation

Mar 01, 2018

Domain Join

To configure new EE appliance at the DC to windows domain:

1. Go to Windows Domain in SD-WAN web GUI, navigate to **Configuration > Secure Acceleration >** and click **Join Windows Domain**.

Citrix NetScaler SD-WAN 2000-250-EE

9.2.0.105.575135 Logout CITRIX

Dashboard Monitoring Configuration

Configuration > Secure Acceleration

SSL Optimization status : ACTIVE

Secure Peering

Keystore Status: Opened Secure Peering Status: Enabled

SSL Profile Windows Domain

Windows Domain Join

When the appliance joins the Windows domain, and the Windows domain controller accepts the appliance as a delegate user, the appliance becomes a trusted member of the domain for certain functions. This allows the appliance to be declared a member of the domain's security infrastructure, which in turn allows the acceleration of authenticated and encrypted data streams using Windows protocols such as CIFS and MAPI. For the purposes of accelerating CIFS and MAPI, security delegation can be limited to the relevant services as part of the standard Windows delegation mechanism. This constrained delegation became available with Windows Server 2003.

Join Windows Domain

SSL Profile Windows Domain

Windows Domain

Join the server-side NetScaler SD-WAN appliance to a domain that the Windows file server and Exchange server are a part of. Joining the domain makes the appliance a trusted member of the Windows security system.

Domain Name*

Check Domain Join

User Name*

Password*

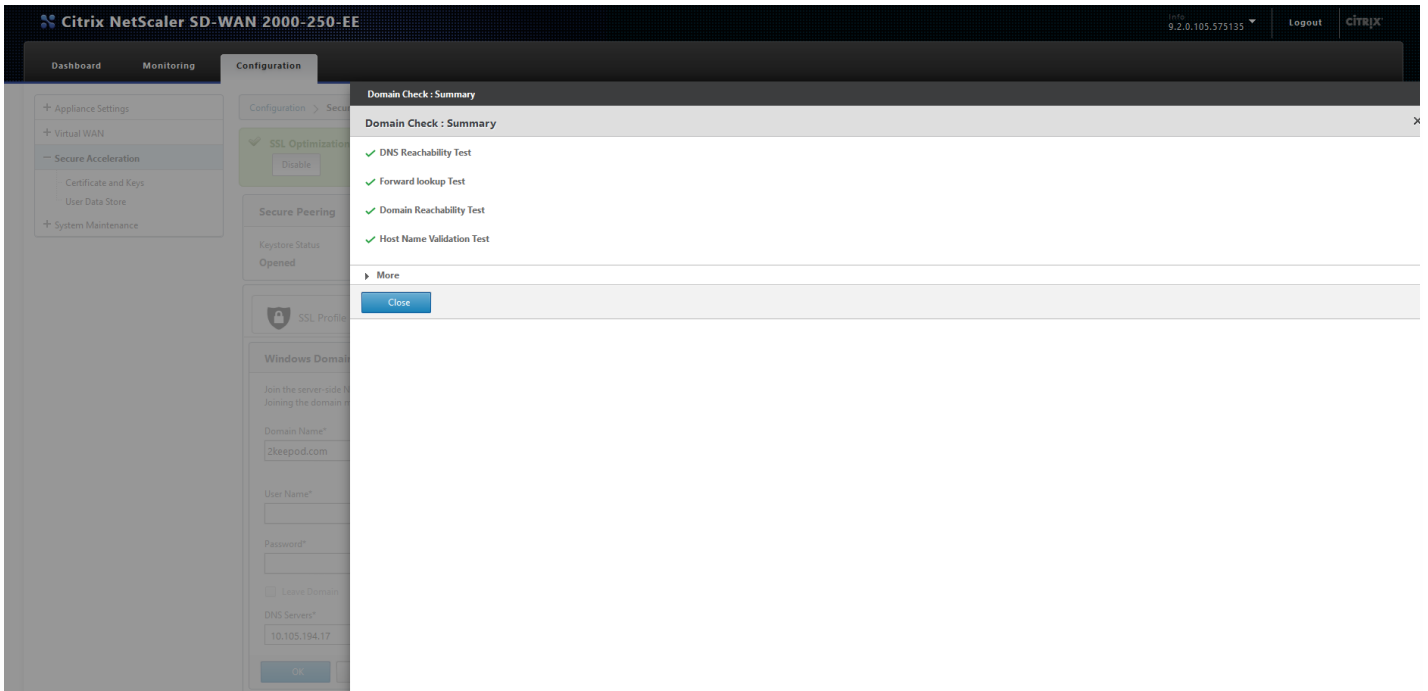
Leave Domain

DNS Servers*

10.105.194.17

OK Cancel

2. Provide **Windows domain name** and perform **Domain Join** pre-checks.

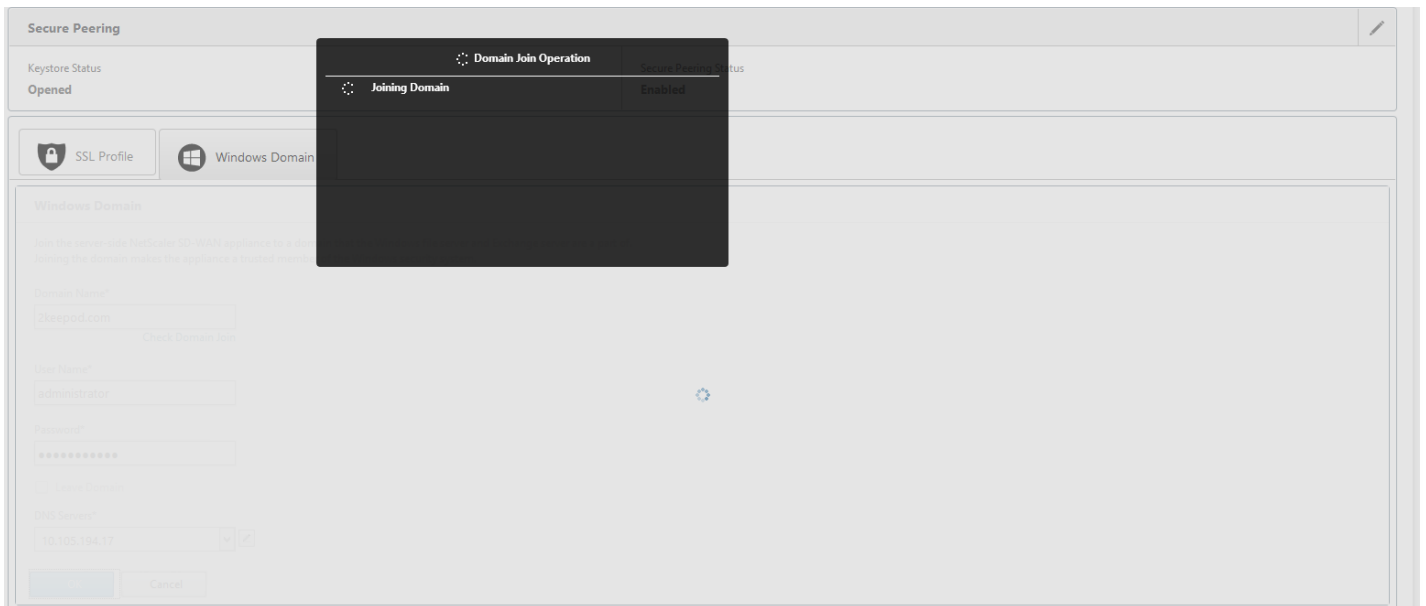


3. After pre-check summary shows as successful, enter domain controller's credentials.

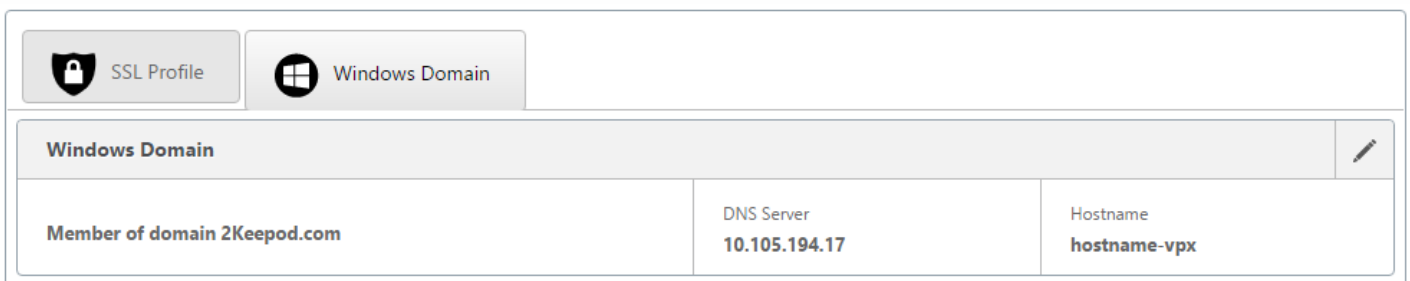
The screenshot shows the 'Windows Domain' configuration form. The form is titled 'Windows Domain' and includes the following fields and options:

- Domain Name***: 2keepod.com
- User Name***: administrator
- Password***: [Redacted]
- Leave Domain
- DNS Servers***: 10.105.194.17

Buttons for 'OK' and 'Cancel' are located at the bottom of the form. A 'Check Domain Join' link is also present below the Domain Name field.

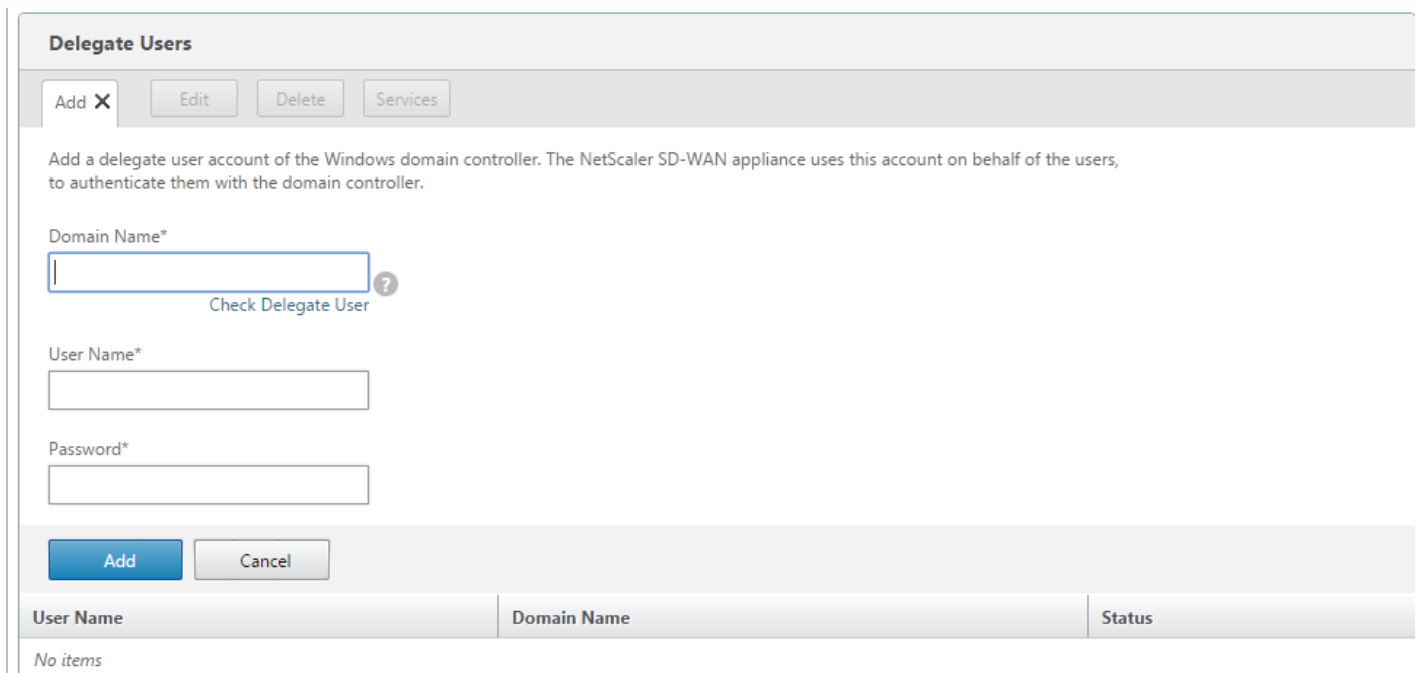


4. On successful domain join, you get the following output.



Delegate User

1. Add delegate user to delegate the services as shown below.



2. Provide correct domain Name and perform delegate user pre-check.

Delegate Users

Add X Edit

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name*

Check Delegate User

User Name*

Password*

Add Cancel

Delegate User Domain Check

Trying to validate Delegate User Domain ...

Delegate User Check : Summary

Delegate User Check : Summary

- ✓ DNS Reachability Test
- ✓ Forward lookup Test
- ✓ Domain Reachability Test
- ⚠ Host Name Validation Test
- ✓ Kerberos config file check
- ⚠ Reverse lookup zone
- ✓ Time Skew Check
- ✓ Kerberos Port Check
- ✓ NTP Port Check
- ✓ Server record for kerberos
- ✓ Server record for ldap

▶ More

Close

3. After delegate user pre-checks are successful, provide valid credentials of the delegate user.

Delegate Users

Add X Edit Delete Services

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name*

[Check Delegate User](#)

User Name*

Password*
 ?

Add Cancel

4. After delegate user is added successfully to SD-WAN, you will see a success message.

Delegate Users

Add Edit Delete Services

User Name	Domain Name	Status
userdel	2KKEEPOD.COM	Success

5. To check what all services are delegated by the delegate user, point to the user and select services.

Delegate User Details

Delegate User Details X

Services

cifs/WIN-KJ8BEBRNRUD.2KKEEPOD.COM/2KKEEPOD.COM

exchangeMDB/WIN-KJ8BEBRNRUD.2KKEEPOD.COM

Close

Security

Mar 01, 2018

The topics in this section provide general security guidance for NetScaler SD-WAN deployments.

NetScaler SD-WAN Deployment Guidelines

To maintain security through the deployment lifecycle, Citrix recommends the following security consideration:

- Physical Security
- Appliance Security
- Network Security
- Administration and Management

The topics described in the following links provide more information about how to configure security for SD-WAN networks using:

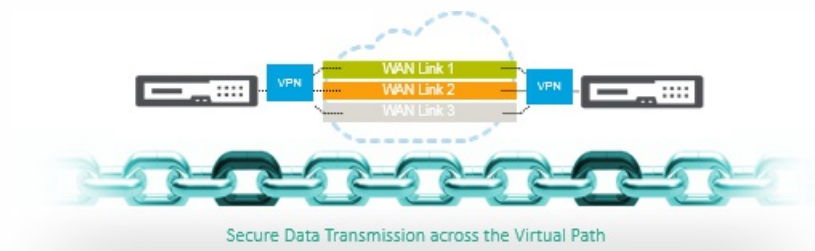
- [IPsec Tunnels](#)
- [Firewall](#)

IPSec Tunnel Termination

Mar 01, 2018

NetScaler SD-WAN supports IPSec virtual paths, enabling third-party devices to terminate IPSec VPN Tunnels on the LAN or WAN side of a NetScaler SD-WAN appliance. You can secure site-to-site IPSec Tunnels terminating on an SD-WAN appliance by using a [140-2 Level 1 FIPS certified IPSec cryptographic binary](#).

SD-WAN also supports resilient IPSec tunneling using a differentiated virtual path tunneling mechanism.

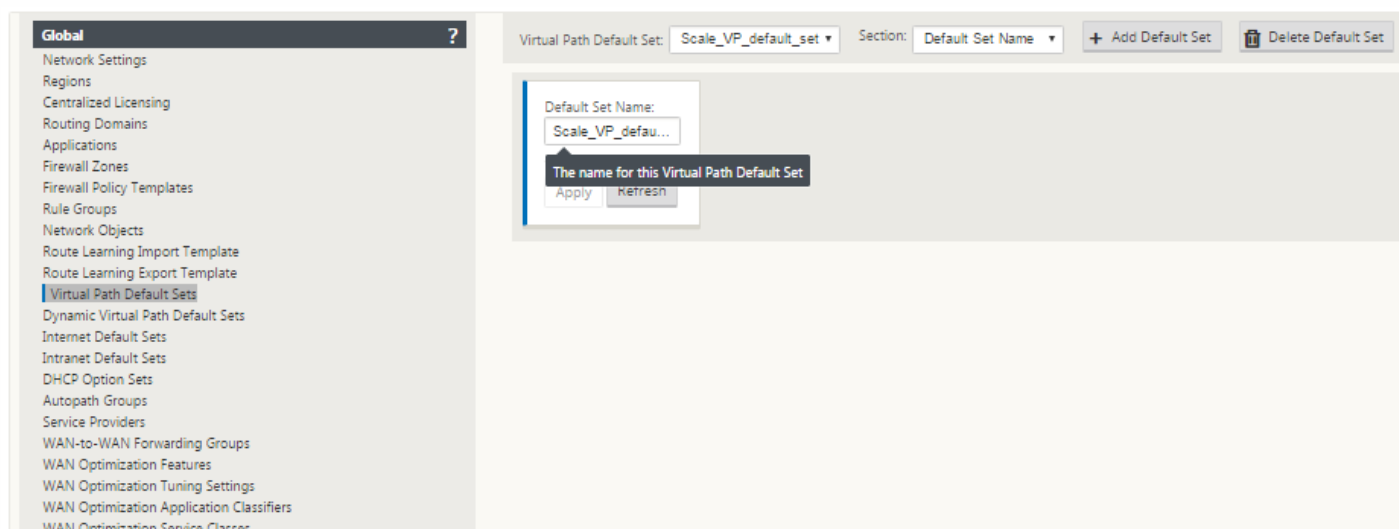


How to Configure IPsec Tunnels for Virtual and Dynamic Paths

Mar 01, 2018

To configure IPsec Tunnels for Virtual and Dynamic Virtual Paths between SD-WAN branch sites:

1. Navigate to **Global** → **Virtual Path Default Sets** or **Dynamic Virtual Path Default Sets**.

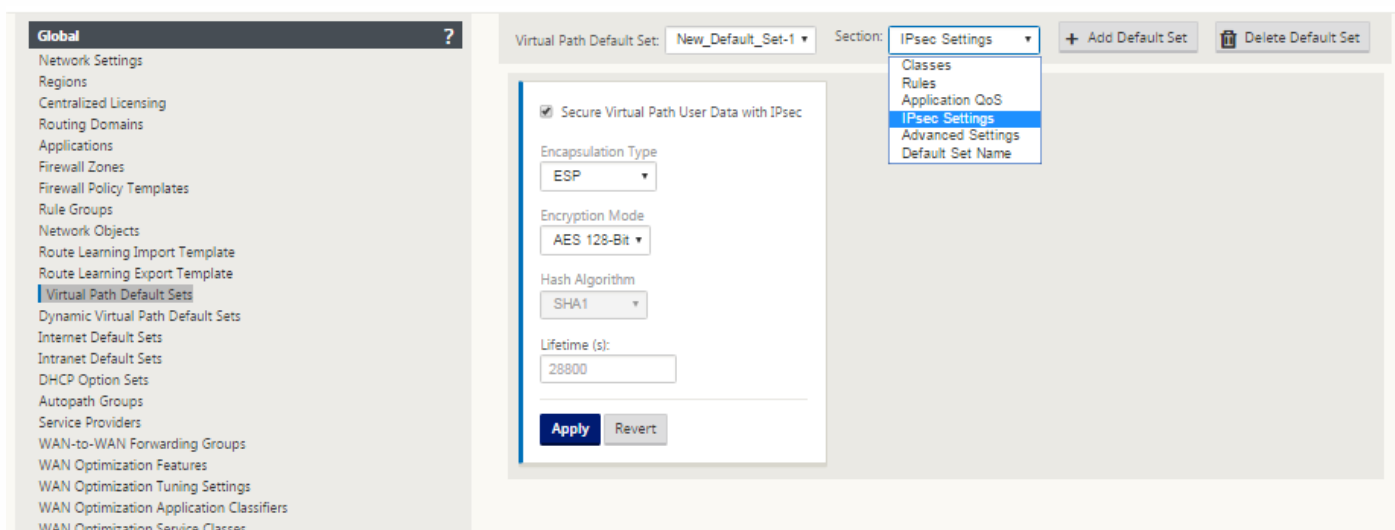


2. Create new default set (virtual or dynamic virtual path), and enable **Secure Virtual Path User Data with IPsec**.

3. Choose one of the available options for IPsec encryption:

- * Encapsulation types: ESP, AH, or ESP+AH
- * Encryption Modes: AES 128, or 256-Bit
- * Hash Algorithm: SHA1 or SHA-256

4. Apply the created Virtual Path Default Set to the MCN node. This automatically applies the same default set to all Client nodes that have Virtual Path to the MCN.

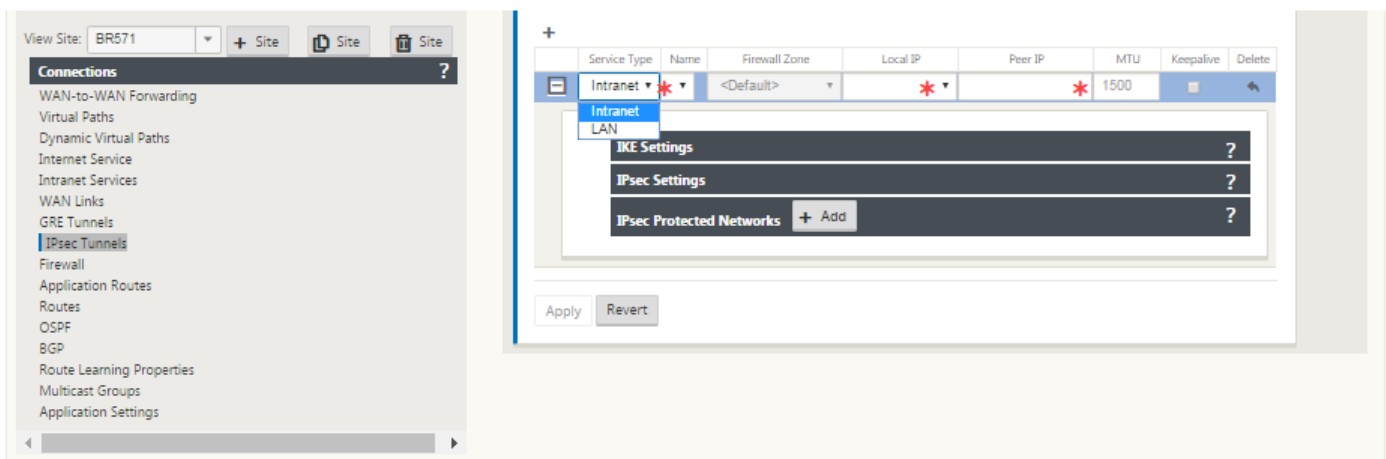


How To Configure IPsec Tunnel Between SD-WAN and Third-Party Devices

Mar 01, 2018

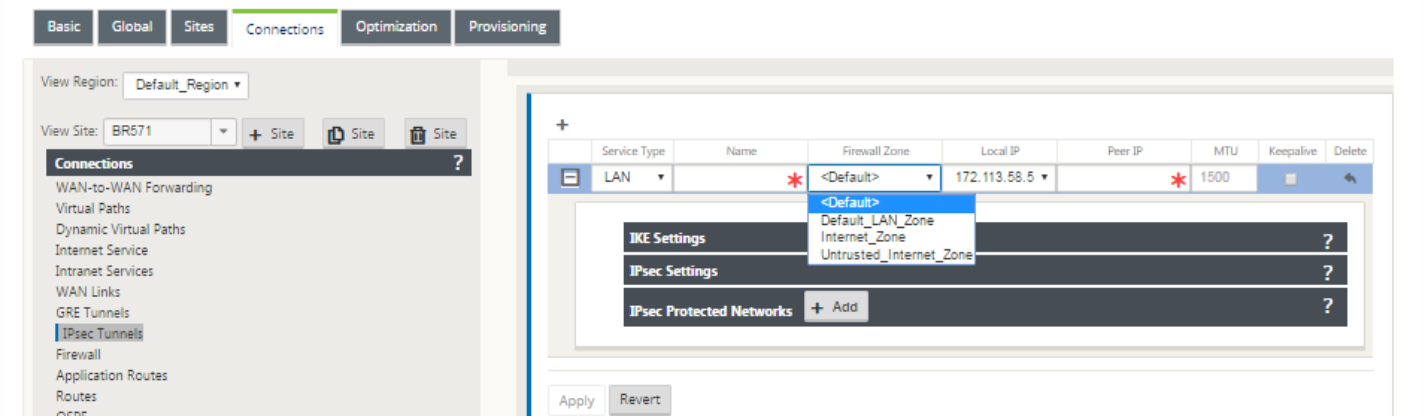
To configure IPsec Tunnel for Intranet or LAN service:

1. In the **Configuration Editor**, navigate to **Connections > View Site > [Site Name] > IPsec Tunnels**. Choose a **Service Type** (LAN or Intranet).
2. Enter a **Name** for the service type. For Intranet service type, the configured Intranet Server will determine which Local IP addresses are available.
3. Select the available **Local IP** address and enter the **Peer IP** address for the virtual path to peer with.



Note

If the Service Type is Intranet, the IP address is pre-determined by the chosen Intranet Service.

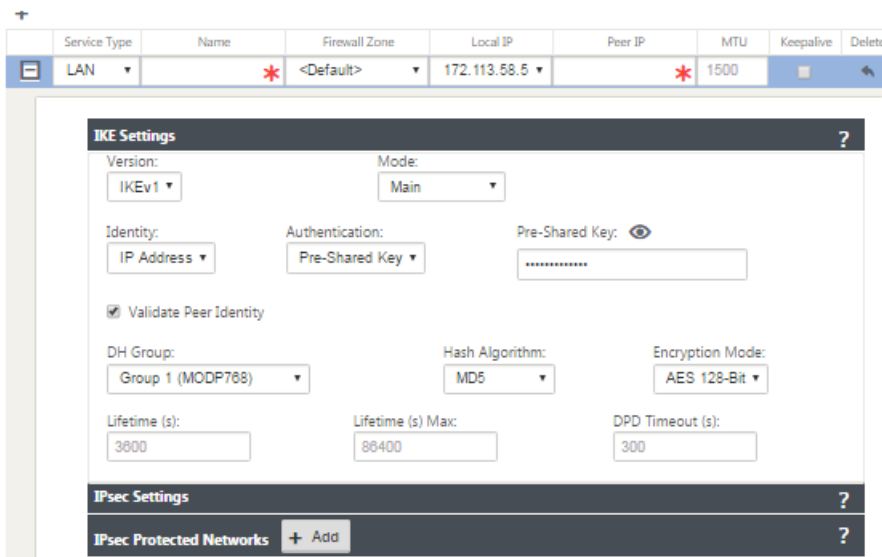


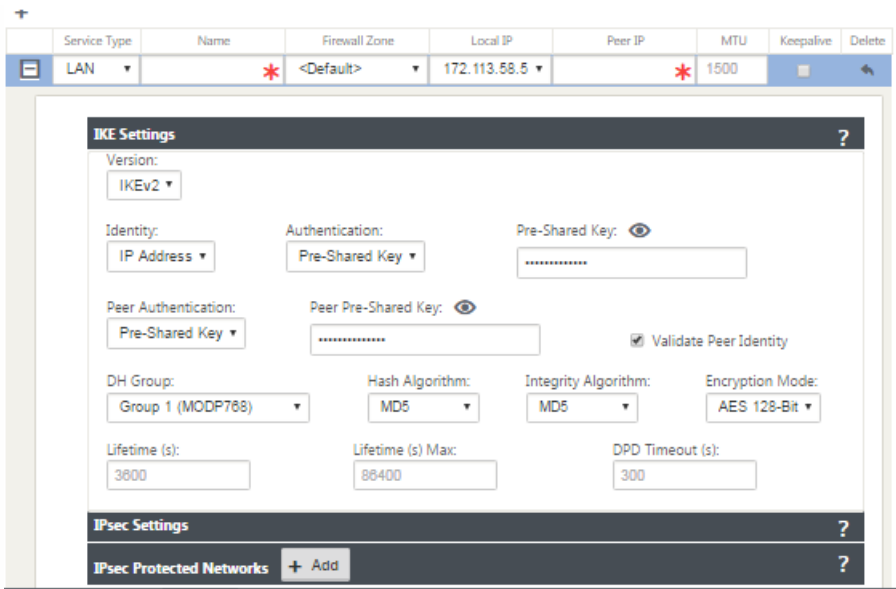
4. Configure IPsec settings by applying the criteria described in the following tables. When finished, click **Apply** to save

your settings.

Field	Description	Values (s)
Service Type	Choose a service type from the drop-down menu.	<ul style="list-style-type: none"> Intranet LAN
Name	If the service type is Intranet, choose from the list of configured intranet services in the drop-down menu. If the service type is LAN, enter a unique name.	<ul style="list-style-type: none"> Textstring
Local IP	Choose the local IP address of the IPsec Tunnel from the drop-down menu of available virtual IP addresses configured at this Site.	<ul style="list-style-type: none"> IP address
Peer IP	Enter the peer IP address of the IPsec Tunnel.	<ul style="list-style-type: none"> IP address
MTU	Enter the MTU for fragmenting IKE and IPSec fragments	<ul style="list-style-type: none"> Default: 1500
IKEv1 Settings	Version: Choose an IKE version from the drop-down menu.	<ul style="list-style-type: none"> IKEv1 IKEv2
Mode	Choose a mode from the drop-down menu.	<ul style="list-style-type: none"> Main Aggressive
Identity	Choose an Identity from the drop-down menu.	<ul style="list-style-type: none"> Auto IP Address
Authentication	Choose the authentication type from the drop-down menu.	<p>Pre-Shared Key</p> <ul style="list-style-type: none"> If you are using a pre-shared key, copy and paste it into this field. Click on the Eyeball () icon to view the Pre-Shared Key. <p>Certificate</p> <ul style="list-style-type: none"> If you are using an identity certificate, choose it from the drop-down menu.
Validate Peer Identity	Select this checkbox to validate the IKE's peer. If the peer's ID type is not supported, do not enable this feature.	<ul style="list-style-type: none"> None
DH Group	Choose the Diffie–Hellman group to use for IKE key generation from the drop-down menu.	<ul style="list-style-type: none"> Group 1 Group 2 Group 5
Hash	Choose an algorithm from the drop-down menu to	<ul style="list-style-type: none"> MD5 SHA1

Field	Description	Values (s)
Encryption Mode	Choose the Encryption Mode for IKE messages from the drop-down menu.	<ul style="list-style-type: none"> AES 128-bit AES 192-bit AES 256-bit
Lifetime (s)	Enter the preferred duration, in seconds, for an IKE security association to exist.	<ul style="list-style-type: none"> 3600 seconds (default)
Lifetime (s) Max	Enter the maximum preferred duration, in seconds, to allow an IKE security association to exist.	<ul style="list-style-type: none"> 86400 seconds (default)
DPD Timeout (s)	Enter the Dead Peer Detection timeout, in seconds, for VPN connections.	<ul style="list-style-type: none"> 300 seconds (default)
IKEv2	Peer Authentication: Choose Peer Authentication from the drop-down menu.	<ul style="list-style-type: none"> Mirrored Pre-Shared Key Certificate
IKE2 - Pre-shared key	Peer Pre-Shared Key: Paste the IKEv2 Peer Pre-Shared Key into this field for authentication. Click the eyeball () icon to view the Pre-Shared Key.	<ul style="list-style-type: none"> Textstring
Integrity Algorithm	Choose an algorithm as the hashing algorithm to use for HMAC verification from the drop-down menu.	<ul style="list-style-type: none"> MD5 SHA SHA-256





IPsec and IPsec Protected Network Settings

Field	Description	Value (s)
Tunnel Type	Choose the Tunnel Type from the drop-down menu.	<ul style="list-style-type: none"> • ESP • ESP+Auth • ESP + NULL • AH
PFS Group	Choose the Diffie–Hellman group to use for perfect forward secrecy key generation from the drop-down menu.	<ul style="list-style-type: none"> • Group 1 • Group 2 • Group 5
Encryption Mode	Choose the Encryption Mode for IPsec messages from the drop-down menu.	<p>If you chose ESP or ESP+ Auth, select either one of the following:</p> <ul style="list-style-type: none"> • AES 128-bit • AES 192-bit • AES 256-bit
Lifetime (s)	Enter the amount of time, in seconds to allow an IPsec security association to exist	<ul style="list-style-type: none"> • 28800 seconds (default)
Lifetime Max (s)	Enter the maximum amount of time, in seconds to allow an IPsec security association to exist	<ul style="list-style-type: none"> • 86400 seconds (default)
Lifetime (KB)	Enter the amount of data, in kilobytes, for an IPsec security association to exist.	<ul style="list-style-type: none"> • Kilobytes
Lifetime (KB) Max	Enter the maximum amount of data, in kilobytes, to allow an IPsec security association to exist.	<ul style="list-style-type: none"> • Kilobytes
Network		<ul style="list-style-type: none"> • Drop

Behavior Field	Protected Networks from the drop-down menu. Description	Use Non-IPsec Route Value (s)
IPsec Protected Networks	Source IP/Prefix: After clicking the Add (+ Add) button, enter the Source IP and Prefix of the network traffic the IPsec Tunnel will protect.	<ul style="list-style-type: none"> IP address
IPsec Protected Networks	Destination IP/Prefix: Enter the Destination IP and Prefix of the network traffic the IPsec Tunnel will protect.	<ul style="list-style-type: none"> IP address

IPsec Settings ?

Tunnel Type: ESP PFS Group: <None>

Encryption Mode: AES 128-Bit

Lifetime (s): 28800 Lifetime (s) Max: 88400

Lifetime (KB): 0 Lifetime (KB) Max: 0

Network Mismatch Behavior: Drop

IPsec Protected Networks + Add ?

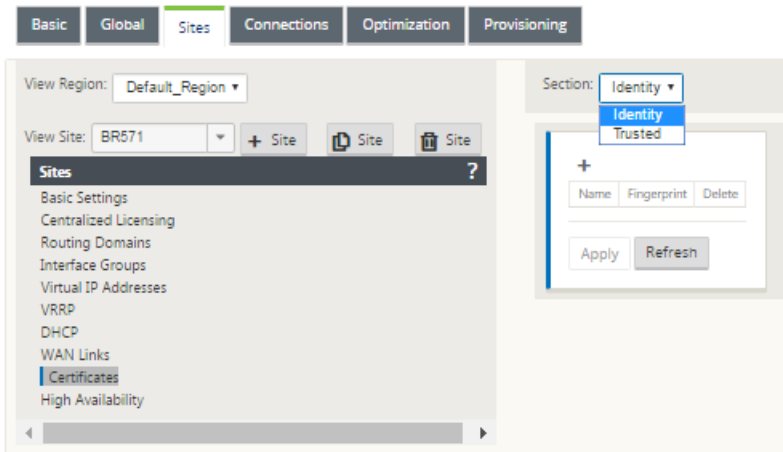
Apply Revert

How To Add IKE Certificates

Mar 01, 2018

To implement certificates for IKE negotiation:

1. Navigate to **Sites** → **Certificates** and add any necessary certificates.



How To View IPsec Tunnel Configuration

Mar 01, 2018

To view IPsec tunnel configuration:

1. Navigate to **Configuration > Virtual WAN > View Configuration**.
2. Select **Virtual Path Service** from the drop-down menu. The IPsec settings are displayed only if IPsec is enabled in the configuration editor.

The screenshot shows the Citrix SD-WAN configuration interface. The left sidebar contains navigation options like 'Appliance Settings', 'Virtual WAN', and 'System Maintenance'. The main area is titled 'Configuration > Virtual WAN > View Configuration'. A dropdown menu is set to 'Virtual Path Service'. Below this, the 'Virtual Path Service Configuration' is displayed for 'Virtual Path 515 = MCN-5100-BR572'. The configuration includes local and remote site information, send rates, and IPsec settings. A table lists the paths between links (MCN-5100-HL-1, BR572-HL-1, BR572-HL-2) with columns for Path ID, From Link, To Link, Primary/Secondary Src/Dst IP, Src/Dst Port, Alternate Src/Dst Port, IP DSCP, Encrypt, Loss, and Sensitive. Below the table, there are sections for 'Standby' and 'Active' heartbeat intervals, and a 'CLASSES' section listing traffic types (REALTIME, INTERACTIVE, BULK) with their respective rates and periods.

3. Select **IPsec Tunnels** from the drop-down menu to view the IPsec Tunnel configuration.

This screenshot shows a close-up of the configuration dropdown menu. The menu is open, and 'IPsec Tunnels' is selected and highlighted.

```

IPsec Tunnel Configuration
-----
Name: VPN-ASA-1
-----
ipsec_service_type=intranet
ike_local_ip_addr=10.0.0.6
ike_remote_ip_addr=10.101.0.100
network_mtu=1500
ike_version=2
ike_auth=psk
ike_identity=auto
ike_peer_auth=cert
ike_validate_peer_identity=1
ike_hash_algorithm=sha256
ike_integ_algorithm=sha256
ike_encryption_mode=aes256
ike_dhgroup=group2
ike_lifetime_s=300
ike_lifetime_s_max=86400
ike_dp_d_s=300
ipsec_tunnel_mode=tunnel
ipsec_tunnel_type=esp_auth
ipsec_encryption_mode=aes128
ipsec_hash_algorithm=sha
ipsec_dfsgroup=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. Each virtual path will show its own IPsec tunnel status as shown below.

Dashboard
Monitoring
Configuration

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-ESxL' is currently dead.		

IPSec Monitoring and Logging

Mar 01, 2018

To monitor IPSec tunnel statistics:

1. Navigate to **Monitor > Statistics**. Choose **IPsec Tunnel** from the **Show** drop-down menu as shown below:

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	1459

2. Navigate to **Monitor > IKE/IPsec**. Observe the configured IPSec tunnels, the IKE and IPSec service associations between two or more VPN endpoints configured within the SD-WAN network.

1. Navigate to **Configuration > Appliance Settings > Logging/Monitoring**. Select **Filename** from the drop-down menu and click **View Log**. You can view the following log details for the IPSec tunnel:

- * Creation and Deletion of IPSec tunnel
- * IPSec tunnel status change

```
00028:940:324:607 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
00029:050:345:638 INFO Current time is:Tue Mar 22 19:04:46 2016
00029:064:056:825 INFO Citrix_ikeStathdIn@forward/hosted/ipsec_host.c:3327 IKE SA CREATED (Virtual Path HCN1-BR2CB2K): v=2,_R,id=0xaf3151ca,rc=OK,next state=GOOD
00029:064:492:766 INFO Citrix_ikeStathdIn@forward/hosted/ipsec_host.c:3327 IKE SA CREATED (Virtual Path HCN1-BR1): v=2,_R,id=0xaf3151c9,rc=OK,next state=GOOD
00029:119:436:901 INFO Citrix_ikeStathdIn@forward/hosted/ipsec_host.c:3361 IKE SA DELETED (Virtual Path HCN1-BR2CB2K): v=2,_R,id=0xaf3151ca,rc=STATUS_IKE_DELETE_PAYLOAD,next state=GOOD
00029:119:841:550 INFO Citrix_ikeStathdIn@forward/hosted/ipsec_host.c:3361 IKE SA DELETED (Virtual Path HCN1-BR1): v=2,_R,id=0xaf3151c9,rc=STATUS_IKE_DELETE_PAYLOAD,next state=GOOD
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
```

1. Navigate to **Configuration > Appliance Settings > Logging/Monitoring > Alert Options**.
2. Create Email and Syslog alerts for IPSec tunnel state reporting.

- * Supports IPSEC_TUNNEL as one of the Event types which allows you to configure Email and Syslog Severity Filters.

Configuration > Appliance Settings > Logging/Monitoring

Log Options | Alert Options | Alarm Options | Syslog Server

Email Alerts

Enable Email Alerts Send Test Email

Destination Email Address(es):

SMTP Server Hostname or IP Address:

SMTP Server Port:

Source Email Address:

You may enter multiple destination email addresses separated with semicolons (;)

Enable SMTP Authentication

SMTP User Name:

SMTP Password:

Verify SMTP Password:

General Event Configuration

Event Type	Alert if State Persists	Email	Email Severity Filter	Syslog	Syslog Severity Filter	SNMP	SNMP Severity Filter
SERVICE	0	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
VIRTUAL_PATH	0	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
WAN_LINK	0	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
PATH	0	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
DYNAMIC_VIRTUAL_PATH	0	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
WAN_LINK_CONGESTION	0	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
USAGE_CONGESTION	0	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
HARD_DISK		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
APPLIANCE		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
USER_EVENT		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
CONFIG_UPDATE		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
SOFTWARE_UPDATE		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
PROXY_ARP		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
ETHERNET		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
WATCHDOG		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
APPLIANCE_SETTINGS_UPDATE		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
DISCOVERED_MTU		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
GRE_TUNNEL		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
IPSEC_TUNNEL		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
VIRTUAL_INTERFACE		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning
LICENSE_EVENT		<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning	<input type="checkbox"/>	Warning

Apply Settings

1. Navigate to Configuration > System Maintenance > Diagnostics > Events.

2. Add events based on the "IPSEC_TUNNEL" object type. Create filters for all IPsec related events.

Dashboard Monitoring Configuration

Configuration > System Maintenance > Diagnostics

Ping Traceroute Packet Capture Path Bandwidth System Info Diagnostic Data Events Alarms Diagnostics Tool

Insert Event

Object Type: USER EVENT
 Event type: UNDEFINED
 Severity: DEBUG

Add Event

- + Appliance Settings
- + Virtual WAN
- System Maintenance
 - Delete Files
 - Restart System
 - Date/Time Settings
 - Local Change Management
 - Diagnostics**
 - Update Software
 - Configuration Reset
 - Factory Reset

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 2018 January 18 18 24 55 Download (487678 events)

Alert Count

Alert Type	Alerts Sent
Emails:	0
Syslog Messages:	0
SNMP Traps:	0

View Events

Quantity: 25

Filter: Object Type = Any Event type = Any Severity = Any

Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
671289	0	MCN-S100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671288	1	MCN-S100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671287	0	MCN-S100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671286	2	MCN-S100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:14	GOOD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-2->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671285	1	MCN-S100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671284	0	MCN-S100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671283	0	MCN-S100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671282	2	MCN-S100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-2->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671281	3	MCN-S100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-S100-BR573 Path MCN-S100-WL-2->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671280	1	MCN-S100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671279	1	MCN-S100-WL-1->BR574-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-1->BR574-WL-2 state has changed from BAD to GOOD because notified by peer.
671278	2	MCN-S100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-2->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671277	2	MCN-S100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-2->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671276	1	MCN-S100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671275	3	MCN-S100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-S100-BR573 Path MCN-S100-WL-2->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.
671274	1	MCN-S100-WL-1->BR574-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-1->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671273	3	MCN-S100-WL-2->BR574-WL-2	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-2->BR574-WL-2 state has changed from BAD to GOOD because notified by peer.
671272	0	MCN-S100-WL-1->BR574-WL-1	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671271	1	MCN-S100-WL-1->BR572-WL-2	PATH	2018-02-17 18:06:08	GOOD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671270	1	MCN-S100-WL-1->BR572-WL-2	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671269	0	MCN-S100-WL-1->BR574-WL-1	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671268	3	MCN-S100-WL-2->BR574-WL-2	PATH	2018-02-17 18:05:57	BAD	NOTICE	Virtual Path MCN-S100-BR574 Path MCN-S100-WL-2->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671267	1	MCN-S100-WL-1->BR573-WL-2	PATH	2018-02-17 18:05:09	GOOD	NOTICE	Virtual Path MCN-S100-BR573 Path MCN-S100-WL-1->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671266	3	MCN-S100-WL-2->BR572-WL-2	PATH	2018-02-17 18:05:09	GOOD	NOTICE	Virtual Path MCN-S100-BR572 Path MCN-S100-WL-2->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671265	1	MCN-S100-WL-1->BR573-WL-2	PATH	2018-02-17 18:04:58	BAD	NOTICE	Virtual Path MCN-S100-BR573 Path MCN-S100-WL-1->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.

Eligibility for IPsec Non-Virtual Path Routes

Mar 01, 2018

In previous releases, IPsec tunnel routes would remain in the route table, even if the tunnel became unavailable.

Monitoring > Statistics

Statistics

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

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries

Num*	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11389	YES	N/A	N/A
3	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES	*	BRANCH2	Static	-	-	5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.186.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Using the Keepalive option under **Connections > [Site Name] > IPsec Tunnels** enhances this behavior so that the IPsec non-virtual path routes are now considered ineligible when the IPsec tunnel is no longer available. When the keepalive option is enabled, the SAs get created automatically without any traffic being sent through the tunnel.

Basic Global Sites **Connections** Optimization Provisioning

View Region: Default_Region

View Site: BR573 + Site Site Site

Connections ?

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels**
- Firewall
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Multicast Groups
- Application Settings

Service Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
Intranet *	<Default>	<Default>	*	*	1500	<input checked="" type="checkbox"/>	<input type="checkbox"/>

IKE Settings ?

IPsec Settings ?

IPsec Protected Networks + Add ?

Apply Revert

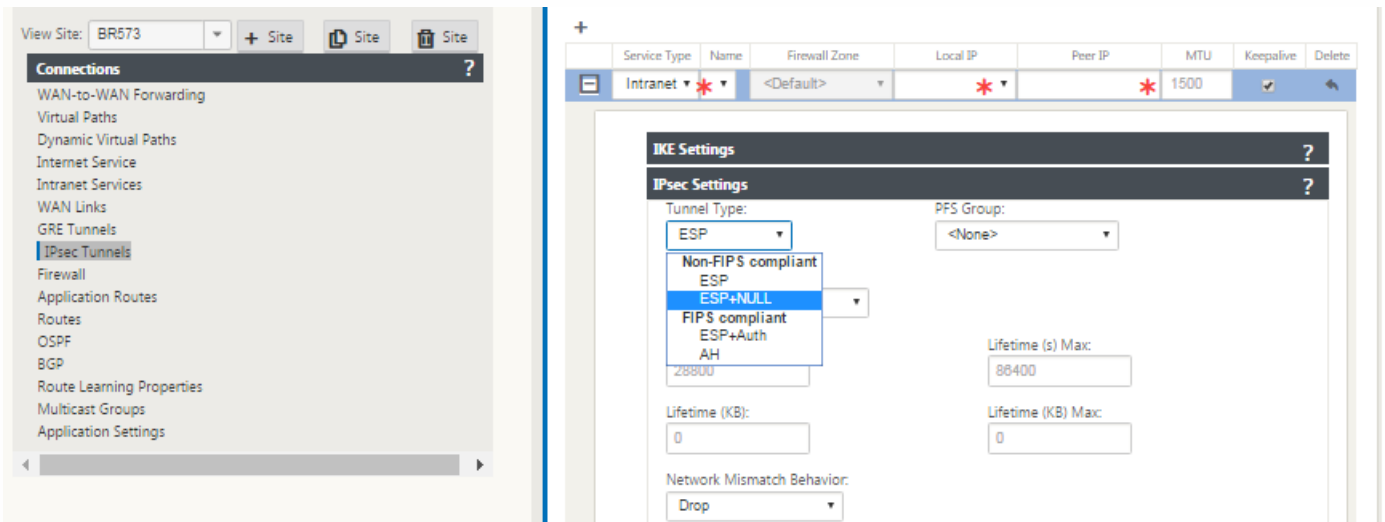
Audits: 0 Audit Now

IPsec Null Encryption

Mar 01, 2018

In previous releases, the tunnel type ESP+NULL was introduced. When using IPsec ESP protocol, traffic is typically encrypted and authenticated. However, you can choose not to use encryption by using Null encryption. In ESP + NULL tunnel type the packets are authenticated but not encrypted.

You can configure the IPsec tunnel with ESP+NULL tunnel type in the Configuration editor, under **IPsec Settings** section.



NetScaler SD-WAN Secure Web Gateway

Mar 01, 2018

To secure traffic and enforce policies, enterprises often use MPLS links to backhaul branch traffic to the corporate data center. The data center applies security policies, filters traffic through security appliances to detect malware, and routes the traffic through an ISP. Such backhauling over private MPLS links is expensive. It also results in significant latency, which creates a poor user experience at the branch site. There is also a risk that users will bypass your security controls.

An alternative to backhauling is to add security appliances at the branch. However, the cost and complexity increases as you install multiple appliances to maintain consistent policies across the sites. And if you have a large number of branch offices, cost management becomes impractical.

Zscaler

The ideal solution to enforce security without adding cost, complexity, or latency is to route all branch Internet traffic from the Citrix NetScaler SD-WAN appliance to the Zscaler Cloud Security Platform. You can then use a central Zscaler console to create granular security policies your users. The policies are applied consistently whether the user is at the data center or a branch site. Because the Zscaler security solution is cloud based, you don't have to add additional security appliances to the network.

FIPS Compliance

The National Institute for Standards and Technology (NIST) develops Federal Information Processing Standards (FIPS) in areas for which no voluntary standards exist. FIPS address the following issues:

- Compatibility between different systems.
- Data and software portability.
- Cost-effective computer security and privacy of sensitive information.

FIPS specifies the security requirements for a cryptographic module used in security systems. To apply these security standards to the processing done by a NetScaler SD-WAN appliance, configure FIPS mode.

Forcepoint

In SD-WAN, you can use the Firewall redirect (transparent proxy by Destination NAT) feature to redirect internet (HTTP and HTTPS) traffic from an SD-WAN appliance at the enterprise edge to the Forcepoint cloud-hosted security module. You can redirect HTTP traffic from port 80 to port 8081 and HTTPS traffic from port 443 to port 8443 of the nearest Forcepoint cloud proxy server.

NetScaler SD-WAN Web Secure Gateway Using GRE Tunnels and IPsec Tunnels

Mar 01, 2018

The Zscaler Cloud Security Platform acts as a series of security check posts in more than 100 data centers around the world. By simply redirecting your internet traffic to Zscaler, you can immediately secure your stores, branches, and remote locations. Zscaler connects users and the internet, inspecting every byte of traffic, even if it is encrypted or compressed.

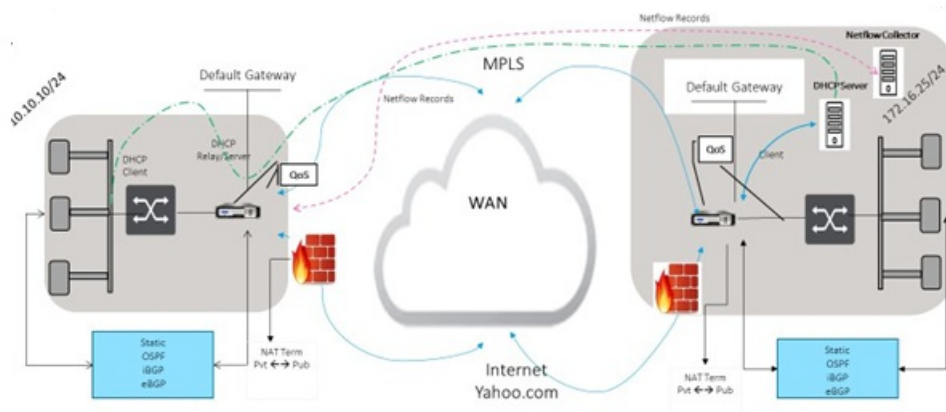
NetScaler SD-WAN appliances can connect to a Zscaler cloud network through GRE tunnels at the customer's site. A Zscaler deployment using SD-WAN appliances supports the following functionality:

- Forwarding all GRE traffic to Zscaler, thereby enabling direct Internet breakout.
- Direct internet access (DIA) using Zscaler on a per customer site basis.
 - On some sites, you might want to provide DIA with on-premises security equipment and not use Zscaler.
 - On some sites, you might choose to backhaul the traffic another customer site for internet access.
- Virtual routing and forwarding deployments.
- One WAN link as part of internet services.

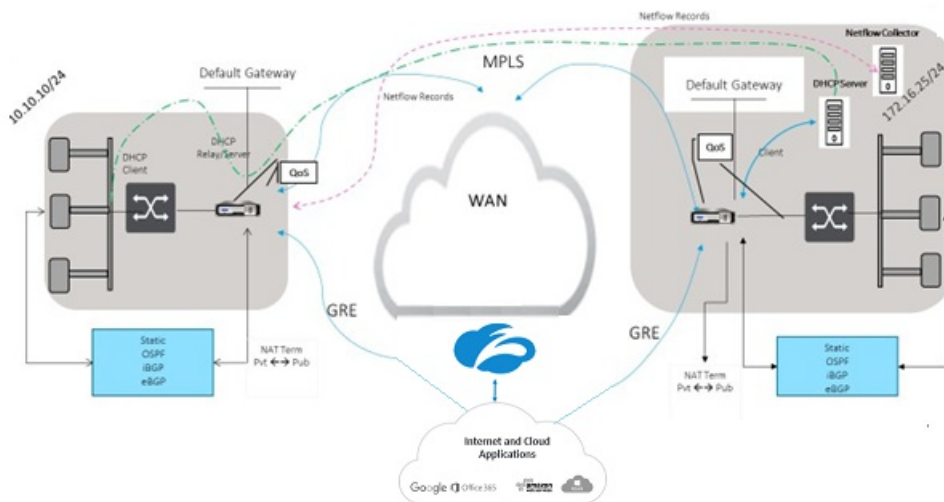
Zscaler is a cloud service. You must set it up as a service and define the underlying WAN links:

- Configure an internet service at the data center and branch through GRE.
- Configure a trusted Public internet link at the data center and the branch sites.

CURRENT DEPLOYMENT MODEL WITH ON-PREMISE FIREWALL



ZSCALER SECURITY AS SERVICE DEPLOYMENT MODEL



To use GRE tunnel or IPsec Tunnel traffic forwarding:

1. Log into the Zscaler help portal at: <https://help.zscaler.com/submit-ticket>.
2. Raise a ticket and provide the static public IP address, which is used as the GRE tunnel or IPsec tunnel source IP address.

Zscaler uses the source IP address to identify the customer IP address. The source IP needs to be a static public IP. Zscaler responds with two ZEN IP addresses (Primary and Secondary) to transmit traffic to. GRE keep alive messages can be used to determine the health of the tunnels.

Zscaler uses the source IP address value to identify the customer IP address. This value must be a static public IP address. Zscaler responds with two ZEN IP addresses [DR1] to which to redirect traffic. GRE keep-alive messages can be used to determine the health of the tunnels.

Sample IP addresses:

Primary

Internal Router IP address: 172.17.6.241/30

Internal ZEN IP address: 172.17.6.242/30

Secondary

Internal Router IP address: 172.17.6.245/30

Internal ZEN IP address: 172.17.6.246/30

To configure an internet service:

1. Navigate to **Connections - Internet Services**. Configure internet service.

Basic Global Sites **Connections** Optimization Provisioning

View Region: Default_Region

View Site: BR573 + Site Site Site

Connections

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service**
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Multicast Groups
- Application Settings

Internet Service: Internet Service Section: **Basic Settings** + Add Service Delete Service

Enable Primary Reclaim

Default Set: <None> Default Route Cost: 5

Ignore WAN Link Status Export Default Route

Apply Refresh

Basic Global Sites **Connections** Optimization Provisioning

View Region: Default_Region

View Site: BR573 + Site Site Site

Connections

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service**
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Multicast Groups
- Application Settings

Internet Service: Internet Service Section: **WAN Links** + Add Service Delete Service

WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Failover	LAN to WAN		WAN to LAN		
					Tagging	Max Delay (ms)	Tagging	Matching	Grooming
BR573-WL-1	<input type="checkbox"/>	Prima	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>
BR573-WL-2	<input type="checkbox"/>	Prima	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>

Apply Refresh

Audits: 0 Audit Now

Internet Service: Internet Service Section: **Rules** + Add Service Delete Service

Order	Rule Group Name	IP Address			Protocol	Protocol #	Port			DSCP	VLAN	Rebind Flow on Change	Delete	Clone
		Source	Dest-Src	Dest			Source	Dest-Src	Dest					
100	<None>	*		*	Any	0	*		*	Any	*	<input type="checkbox"/>	<input type="button" value="↶"/>	<input type="button" value="📄"/>

Mode: WAN Link WAN Link: <N/A>

Override Service: <N/A>

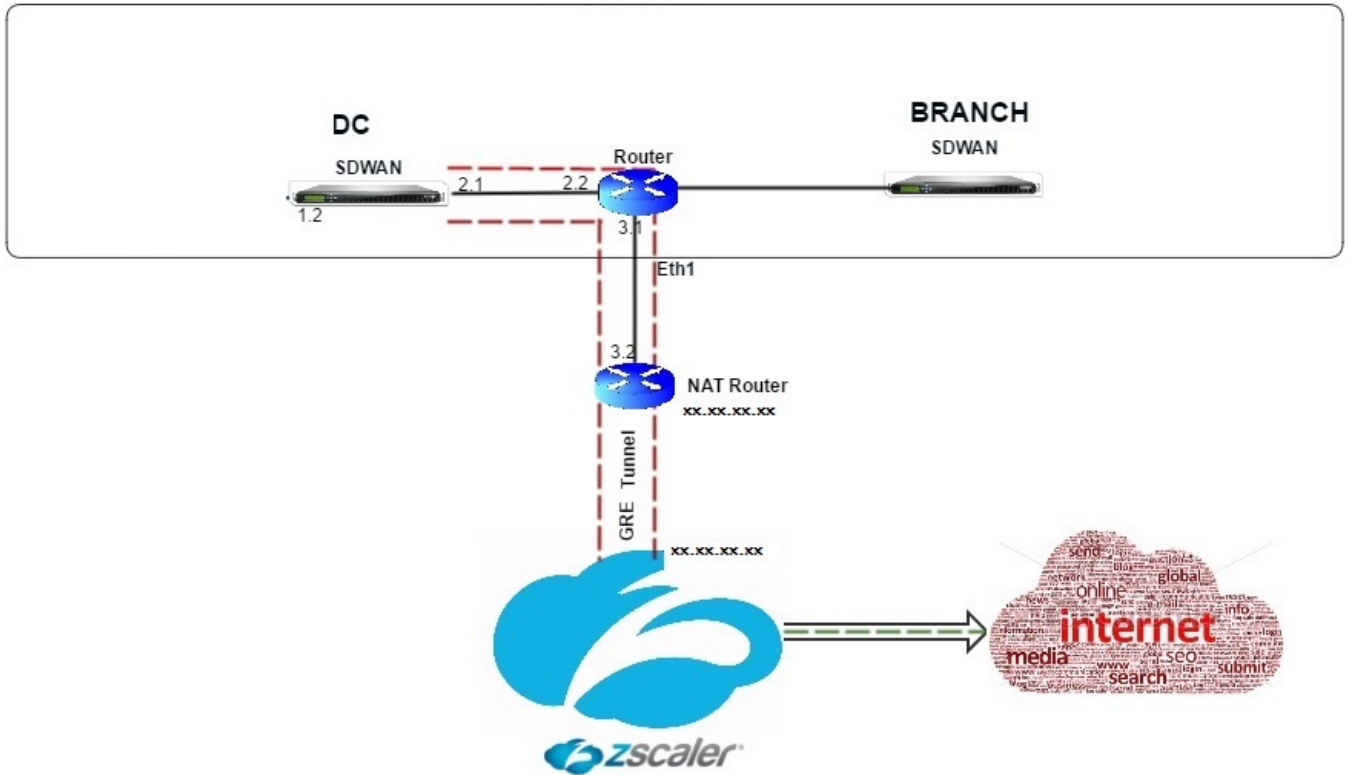
Enable Passive FTP Detection

Apply Revert

a) Source IP address is the Tunnel Source IP address. If the Tunnel Source IP address is NATted, the Public Source IP address is the public Tunnel Source IP address, even if it is NATted on a different intermediate device.

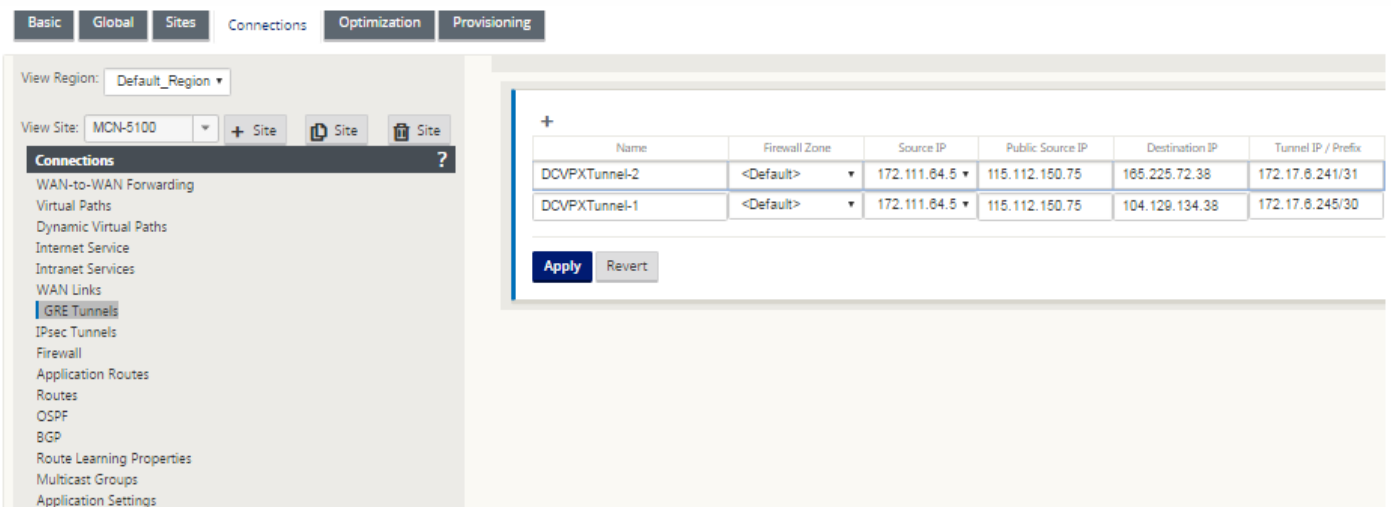
b) Destination IP address is the ZEN IP address that Zscaler provides.

- c) The Source IP address and the Destination IP address are the router GRE headers when the original payload is encapsulated.
- d) Tunnel IP address and Prefix are the IP addressing on the GRE tunnel itself. This is useful for routing traffic over the GRE tunnel. The traffic needs this IP address as the gateway address.



To configure GRE Tunnel:

1. In the configuration editor, navigate to **Connections > Site > GRE Tunnels**, and configure routes to forward internet prefix services to the Zscaler GRE Tunnels. The source IP address can only be chosen from the Virtual network interface on trusted links. See, [How to Configure GRE Tunnel](#).

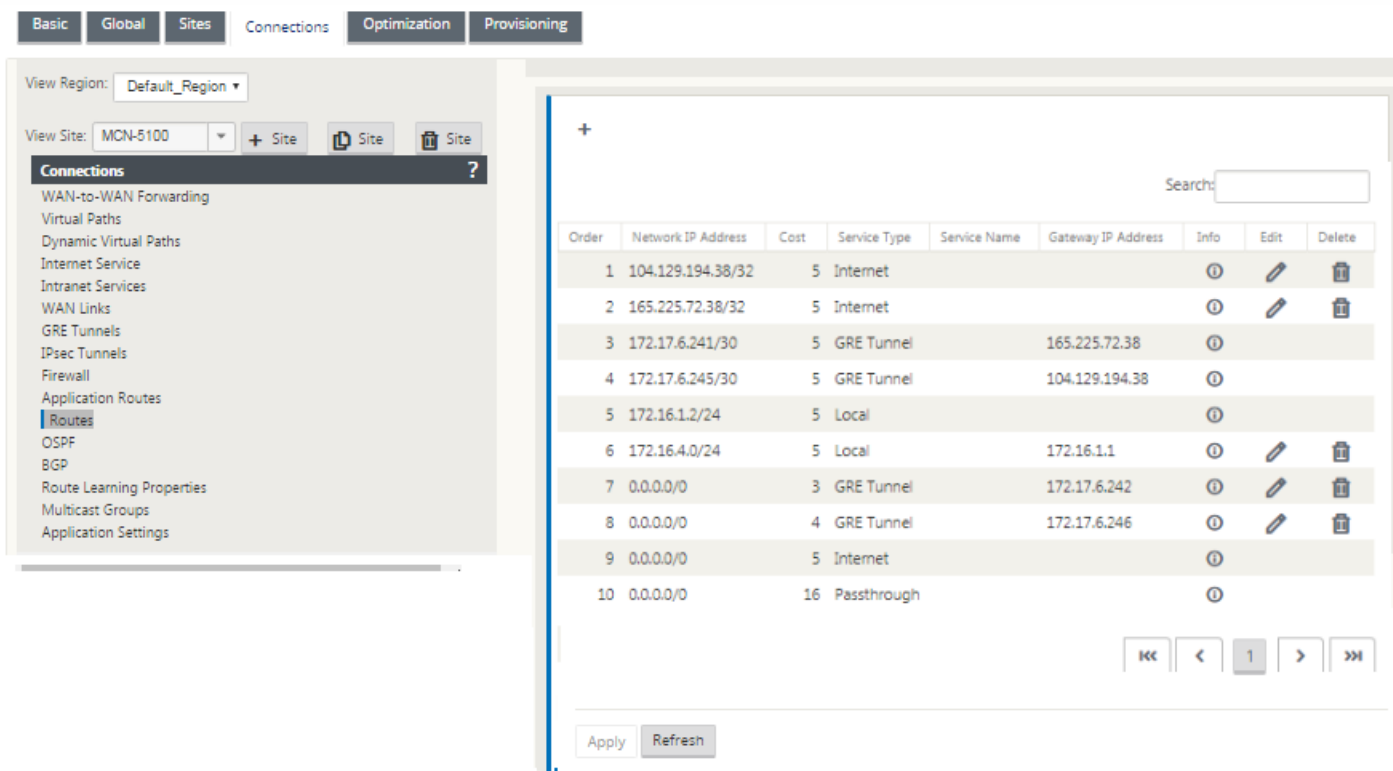


Configure routes to forward internet prefix services to the Zscaler GRE Tunnels.

- The ZEN IP address (Tunnel destination IP, shown as 104.129.194.38 in the above figure) must be set to service-type Internet. This is required so that traffic destined to Zscaler is accounted from the Internet service.
- All traffic destined to Zscaler must match the default route 0/0 and be transmitted over the GRE tunnel. Ensure that the 0/0 route used for [DR1] the GRE tunnel has a lower Cost than Passthrough or any other Service type.
- Similarly, the backup GRE tunnel to Zscaler must have a higher cost than that of the Primary GRE tunnel.
- Ensure that nonrecursive routes exist for the ZEN IP address.

To configure routes for GRE Tunnel:

Navigate to **Connections > Site > Routes**, and follow the procedures described in [Configuring Routes](#) for instructions about creating routes.

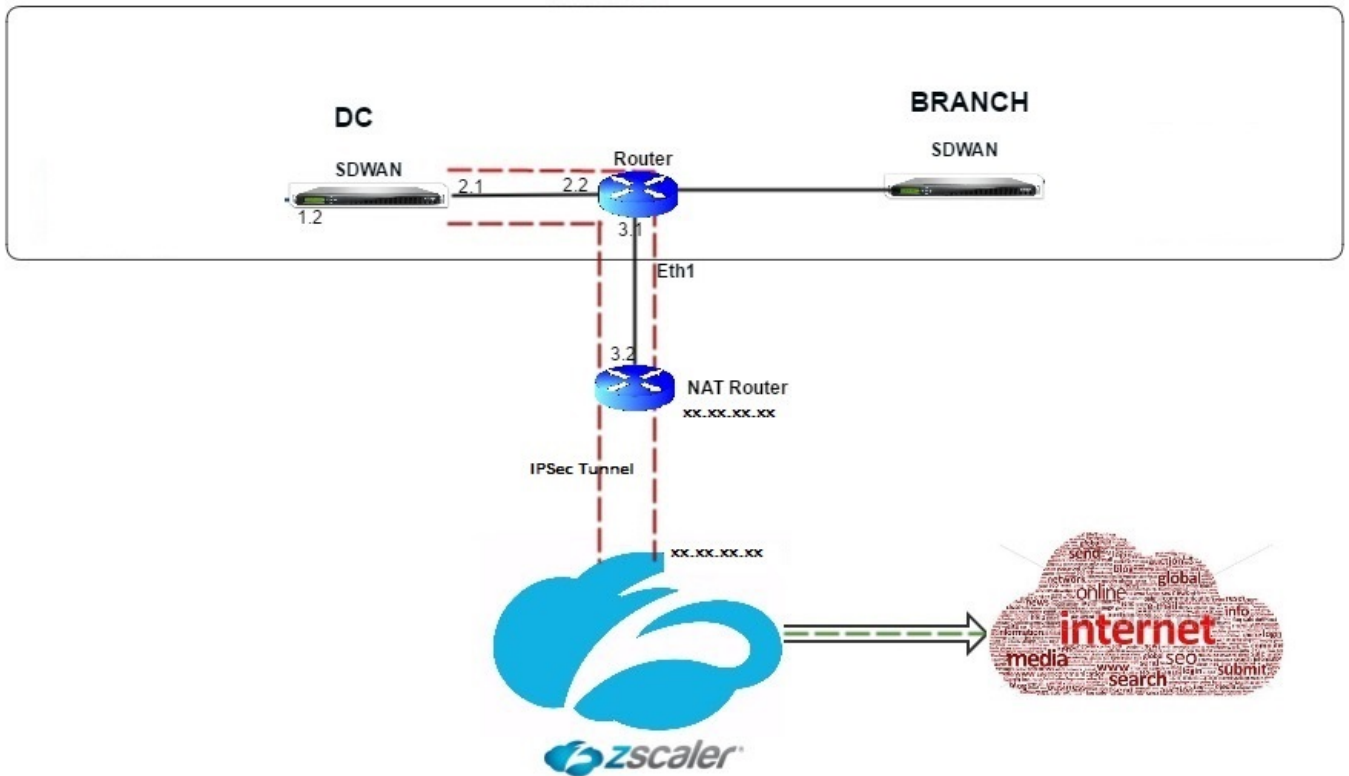


Note

If you do not have specific routes for the Zscaler IP address, configure the route prefix 0.0.0.0/0 to match the ZEN IP address and route it through a GRE tunnel encapsulation loop. This configuration use the tunnels in an active-backup mode. With the values shown in the above figure, traffic automatically switches over to the tunnel with gateway IP address 172.17.6.242. If desired, configure a backhaul virtual path route. Otherwise, set the keep-alive interval of the backup tunnel to zero. This enables secure internet access to a site even if both the tunnels to Zscaler fail.

GRE keep-alive messages are supported. A new field called **Public Source IP** that provides the NAT address of the GRE Source address is added to the NetScaler SD-WAN GUI interface (in the case when SD-WAN appliance Tunnel Source is NAT ted by an intermediate device). The NetScaler SD-WAN GUI includes a field called Public Source IP, which provides the NAT address of the GRE Source address when the NetScaler SD-WAN appliance's Tunnel Source is NAT ted by an intermediate device.

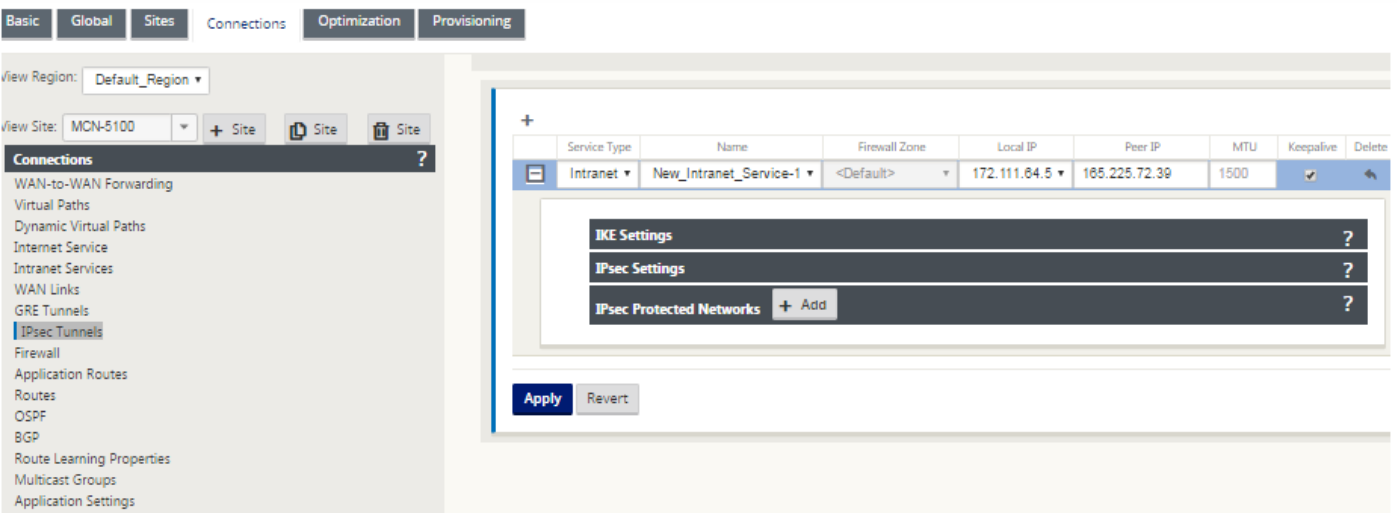
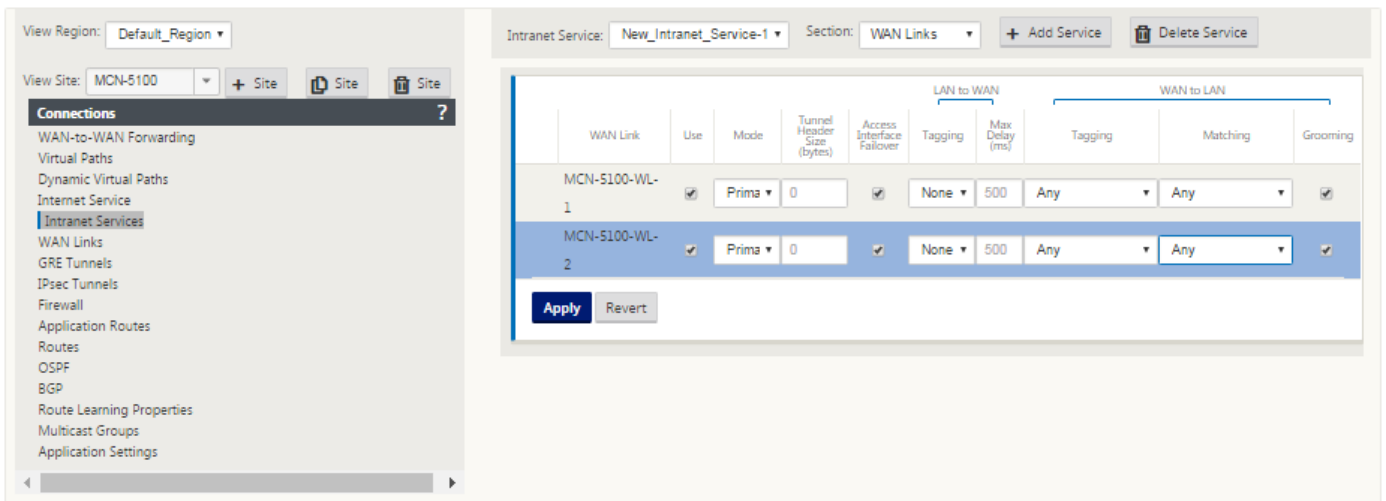
- Multiple VRF deployments are not supported.
- Primary backup GRE tunnels are supported for a high-availability design mode only.



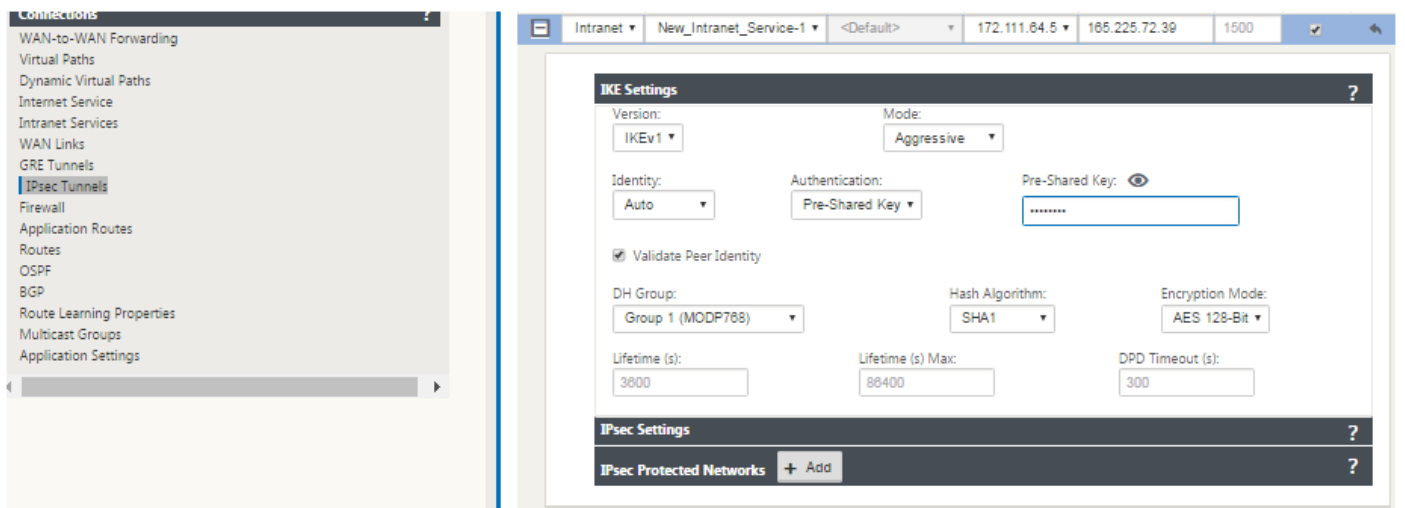
To configure IPsec Tunnels for intranet or LAN services:

Use the NetScaler SD-WAN GUI to do the following:

1. In the Configuration Editor, navigate to **Connections** > <siteName> > **IPsec Tunnels** and choose a service type (LAN or Intranet).
2. Enter a Name for the service type. For Intranet service type, the configured intranet server determines which Local IP addresses are available.
3. Select the available Local IP address and enter the Peer IP address for the virtual path to the remote peer.



4. Select IKEv1 for IKE Settings. Zscaler supports only IKEv1.



5. Under IPsec Settings, select ESP-NUL for Tunnel type, to redirect traffic to Zscaler through the IPsec tunnel. The IPsec tunnel does not encrypt the traffic.

IKE Settings		?
IPsec Settings ?		
Tunnel Type:	PFS Group:	
ESP+NULL	<None>	
Hash Algorithm:		
SHA1		
Lifetime (s):	Lifetime (s) Max:	
28800	86400	
Lifetime (KB):	Lifetime (KB) Max:	
0	0	
Network Mismatch Behavior:		
Drop		
IPsec Protected Networks + Add		?

6. Because internet traffic is redirected, the destination IP/Prefix can be any IP address.

IKE Settings		?
Version:	Mode:	
IKEv1	Aggressive	
Identity:	Authentication:	Pre-Shared Key:
Auto	Pre-Shared Key
<input checked="" type="checkbox"/> Validate Peer Identity		
DH Group:	Hash Algorithm:	Encryption Mode:
Group 1 (MODP768)	SHA1	AES 128-Bit
Lifetime (s):	Lifetime (s) Max:	DPD Timeout (s):
3600	86400	300
IPsec Settings ?		
IPsec Protected Networks + Add ?		
Source IP/Prefix	Destination IP/Prefix	Delete
172.16.4.0/24	0.0.0.0/0	
Apply		Revert

For more information about configuring IPsec Tunnels by using the NetScaler SD-WAN web interface, see; the [IPsec Tunnels](#) topic.

To configure IPsec routes:

Navigate to **Connections > DC > Routes** and follow the procedures described in [Configuring Routes](#) for instructions about creating routes.

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	165.225.72.39/32	5	Intranet	New_Intranet_Service		ⓘ	✎	🗑️
2	172.16.1.2/24	5	Local			ⓘ		
3	172.16.4.0/24	5	Local		172.16.1.1	ⓘ	✎	🗑️
4	0.0.0.0/0	5	Intranet	New_Intranet_Service		ⓘ		
5	0.0.0.0/0	5	Internet			ⓘ		
6	0.0.0.0/0	16	Passthrough			ⓘ		

To monitor GRE and IPsec tunnel statistics:

In the SD-WAN web interface, navigate to **Monitoring > Statistics > [GRE Tunnel | IPsec Tunnel]**.

For more information, see; [monitoring IPsec tunnels](#) and [GRE tunnels](#) topics.

FIPS Compliance

Mar 01, 2018

In SD-WAN, FIPS mode enforces users to configure FIPS compliant settings for their IPsec Tunnels and IPsec settings for Virtual Paths.

- Displays the FIPS compliant IKE Mode.
- Displays a FIPS Compliant IKE DH Group from which users can select the required parameters for configuring the appliance in FIPS compliant mode (2,5,14 – 21).
- Displays the FIPS compliant IPsec Tunnel Type in IPsec settings for Virtual Paths
 - a. IKE Hash and (IKEv2) Integrity mode, IPsec auth mode.
 - b. Performs audit errors for FIPS based Lifetime Settings

To enable FIPS compliance by using the NetScaler SD-WAN GUI:

1. Go to **Configuration -> Virtual WAN -> Configuration Editor -> Global**, and select **Enable FIPS Mode**.

Enabling FIPS mode enforces checks during configuration to ensure that all IPsec related configuration parameters adhere to the FIPS standards. You will be prompted through audit-errors and warnings to successfully configure IPsec to meet the standards.

To configure Virtual Path IPsec Settings:

- Enable Virtual Path IPsec Tunnels for all Virtual Paths where FIPS compliance is required. IPsec settings for Virtual Paths are controlled via Default Sets.
- Configure message authentication by changing the IPsec Mode to AH or ESP+Auth and use a FIPS approved hashing function. SHA1 is currently accepted by FIPS, but SHA256 is highly recommended.
- IPsec lifetime should be configured for no more than 8 hours (28800 seconds).

The Virtual WAN uses IKE version 2 with pre-shared-keys to negotiate IPsec tunnels through the Virtual Path using the following settings:

- DH Group Group 19: ECP256 (256-bit Elliptic Curve) for key negotiation
- 256-bit AES-CBC Encryption
- SHA256 hashing for message authentication
- SHA256 hashing for message integrity
- DH Group 2: MODP-1024 for Perfect Forward Secrecy

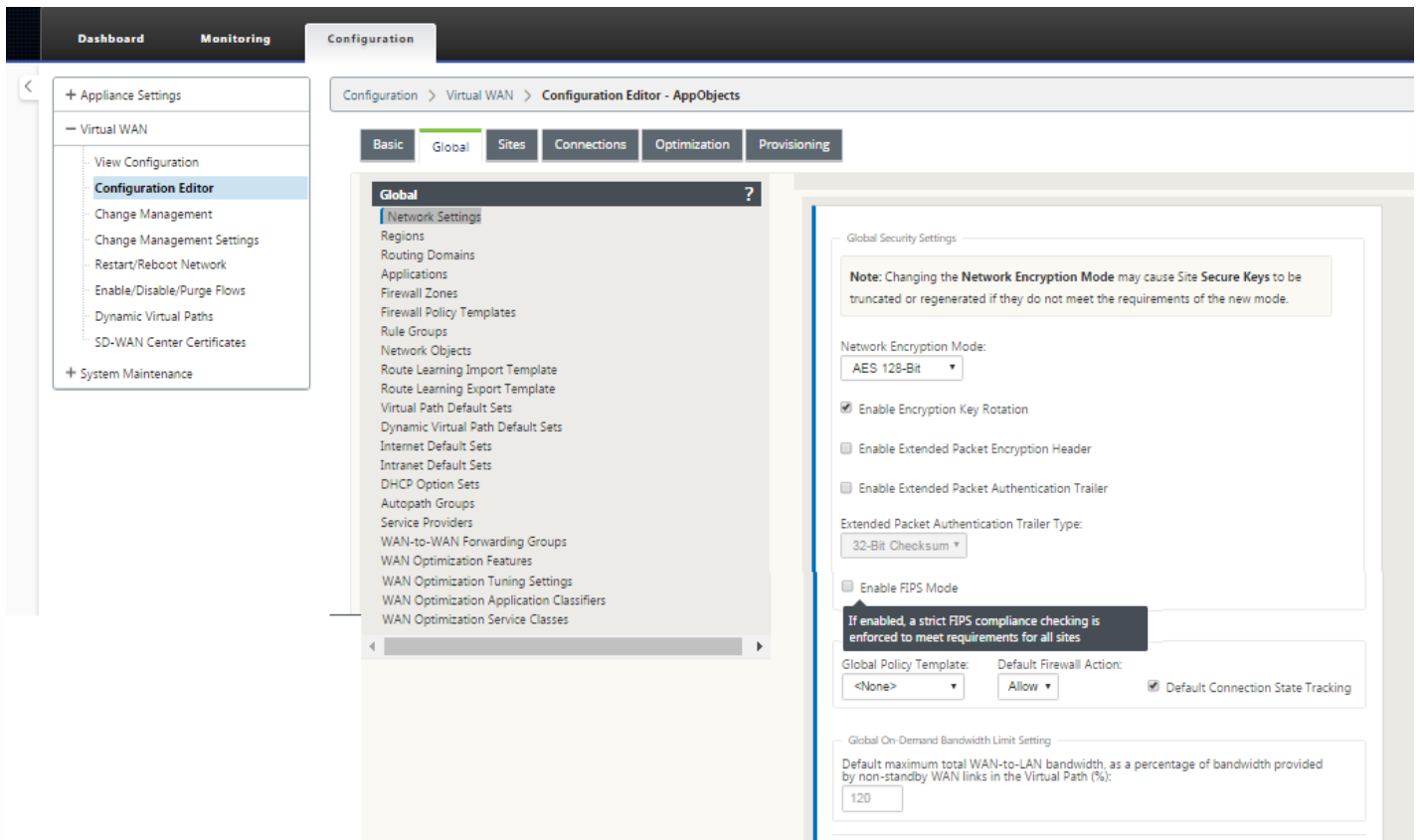
To configure IPsec Tunnel for a third party, use the following settings:

- a) Configure FIPS approved DH Group. Groups 2 and 5 are permissible under FIPS, however groups 14 and above are highly recommended.
- b) Configure FIPS approved hash function. SHA1 is currently accepted by FIPS, however SHA256 is highly recommended.
- c) If using IKEv2, configure a FIPS approved integrity function. SHA1 is currently accepted by FIPS, however SHA256 is highly recommended.

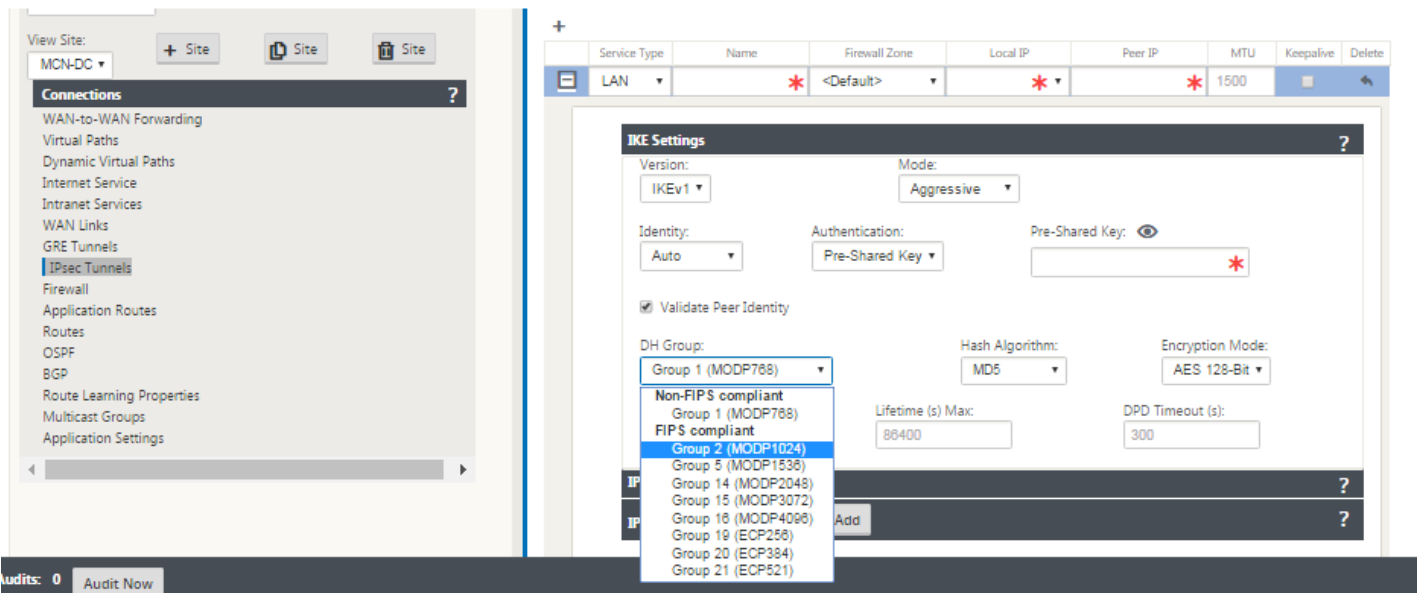
- d) Configure an IKE lifetime, and max lifetime, of no more than 24 hours (86400 seconds).
- e) Configure IPsec message authentication by changing the IPsec Mode to AH or ESP+Auth and use a FIPS approved hashing function. SHA1 is currently accepted by FIPS, but SHA256 is highly recommended.
- f) Configure an IPsec lifetime, and max lifetime, of no more than 8 hours (28800 seconds).

To configure IPsec tunnels:

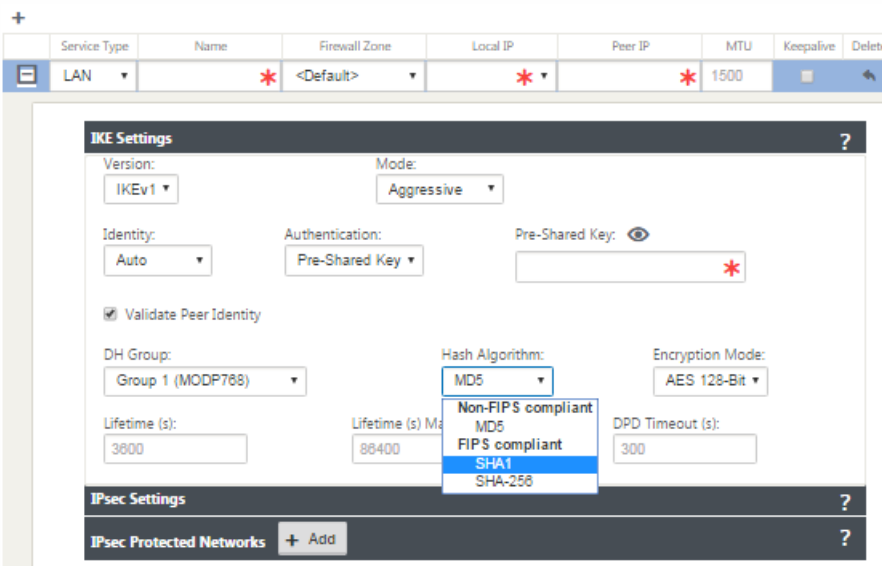
1. On the MCN appliance, go to **Configuration -> Virtual WAN -> Configuration Editor**. Open an existing configuration package. Go to **Connections > IPsec Tunnels**.



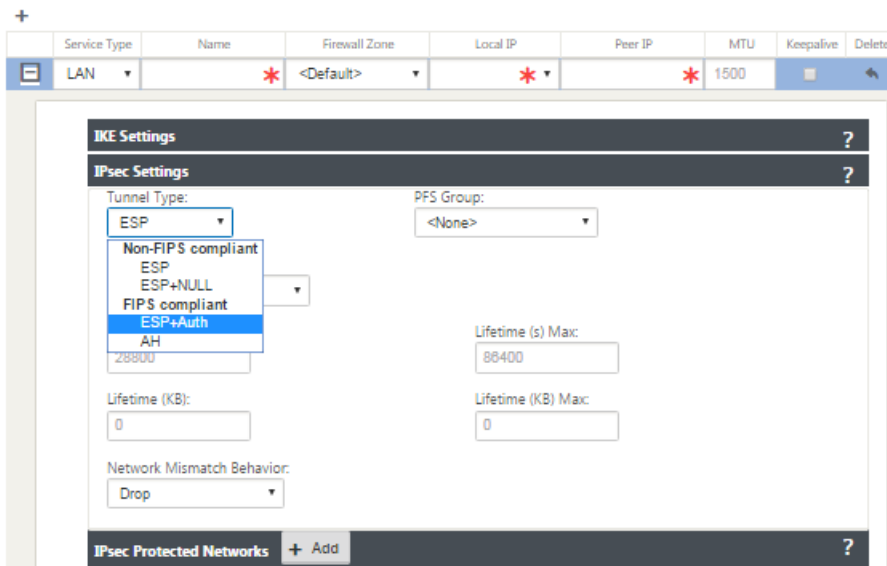
2. Go to **Connections -> IPsec Tunnels**. With LAN or Intranet Tunnel selected, the screen distinguishes the FIPS-compliant groups in the IKE settings from those that are not compliant, so that you can easily configure FIPS compliance.



The screen also indicates whether the hash algorithm is FIPS compliant, as shown in the following figure.



FIPS compliance options for IPsec settings:



If the IPsec configuration does not comply with FIPS standards when it is enabled an audit error might be triggered. Following are the type of audit errors that get displayed in the GUI.

- When FIPS mode is enabled and Non-FIPS compliant option is selected.
- When FIPS mode is enabled and incorrect lifetime value is entered.
- When FIPS mode is enabled and IPsec settings for virtual path default set is also enabled, and incorrect Tunnel mode is selected (ESP vs ESP_Auth / AH).
- When FIPS mode is enabled, IPsec settings for virtual path default set is also enabled, and incorrect lifetime value is entered.

Firewall Traffic Redirection Support by Using Forcepoint in NetScaler SD-WAN

Mar 01, 2018

Forcepoint supports the following features, although SD-WAN supports only the firewall redirect feature:

- IPsec with PKI
- IPsec with PSK
- Proxy chaining using PAC file configuration
- Proxy chaining with standard headers
- Proxy chaining with proprietary headers removing the need to configure the client's IP range - partnership/development
- Firewall redirect (transparent proxy by Destination NAT)

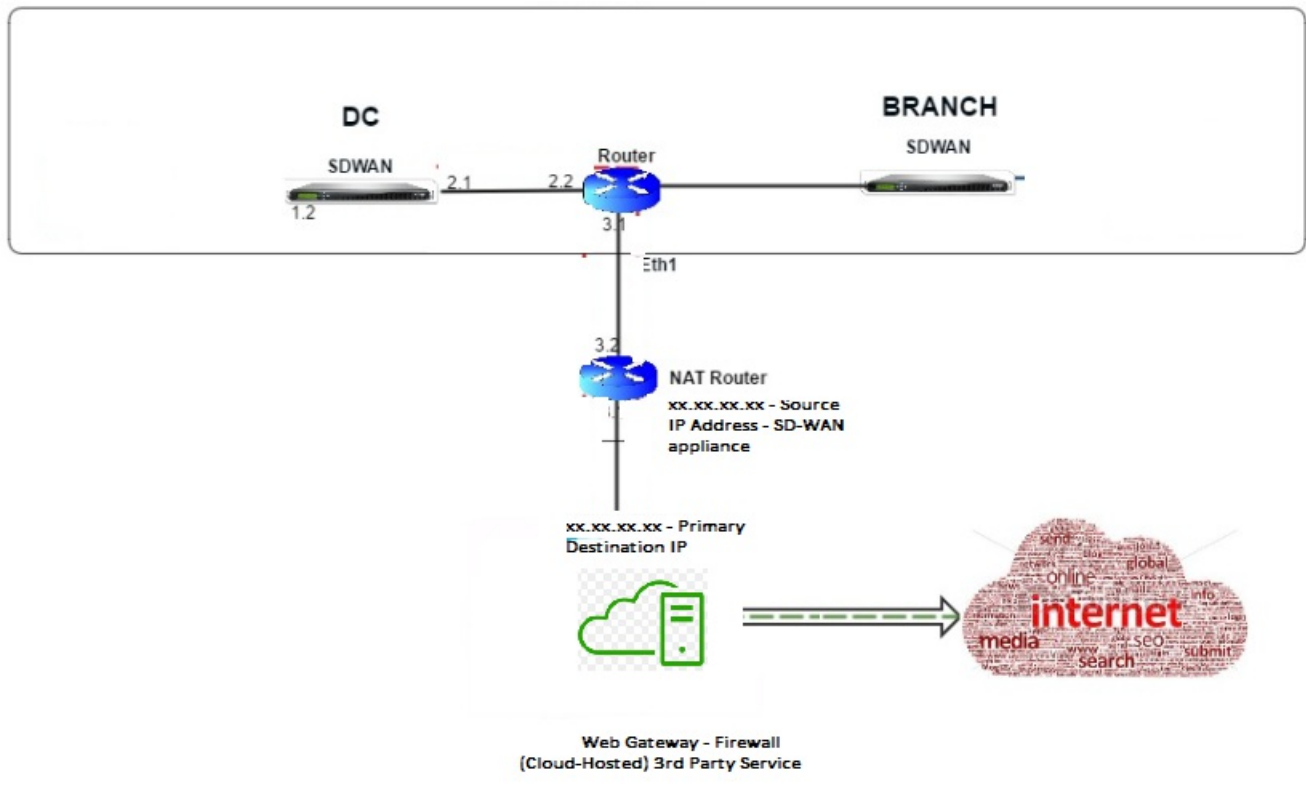
The Destination NAT policy enables enterprises to route internet traffic through cloud-hosted security service using ForcePoint.

Review the following use case to understand how to configure Destination NAT in SD-WAN appliances and redirect internet traffic through a secure cloud-based firewall service.

Pre-requisites:

1. Login to the [Forcepoint portal site](#). Create a policy by providing the Enterprise Public IP address through which internet traffic needs to be redirected to Forcepoint. Obtain the Primary and Secondary IP addresses to which the internet traffic should be redirected.
2. In the SD-WAN GUI, on a SD-WAN appliance at the DC site, configure Internet service associated with WAN links.
3. Destination NAT is performed using Destination IP address of the internet traffic. This destination address is changed to the Forcepoint public IP address.
4. Configure Destination NAT policy by providing the source IP address and the primary IP address. The source IP is the internet IP address of the SD-WAN appliance inside ports 80 (http) and 443 (https) which is redirected/translated to the primary destination IP address of the cloud-based firewall gateway with outside ports 8081 (http) and 8443 (https) respectively.
5. After configuring DNAT policy, ensure that the Routes configured on the DC have the Internet service type selected for the SD-WAN network IP address.

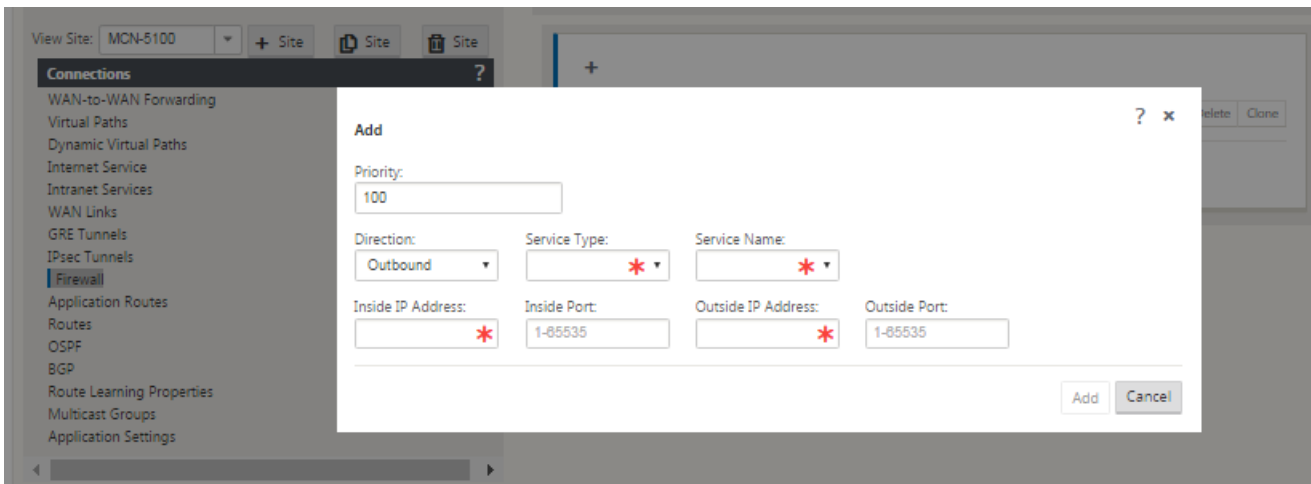
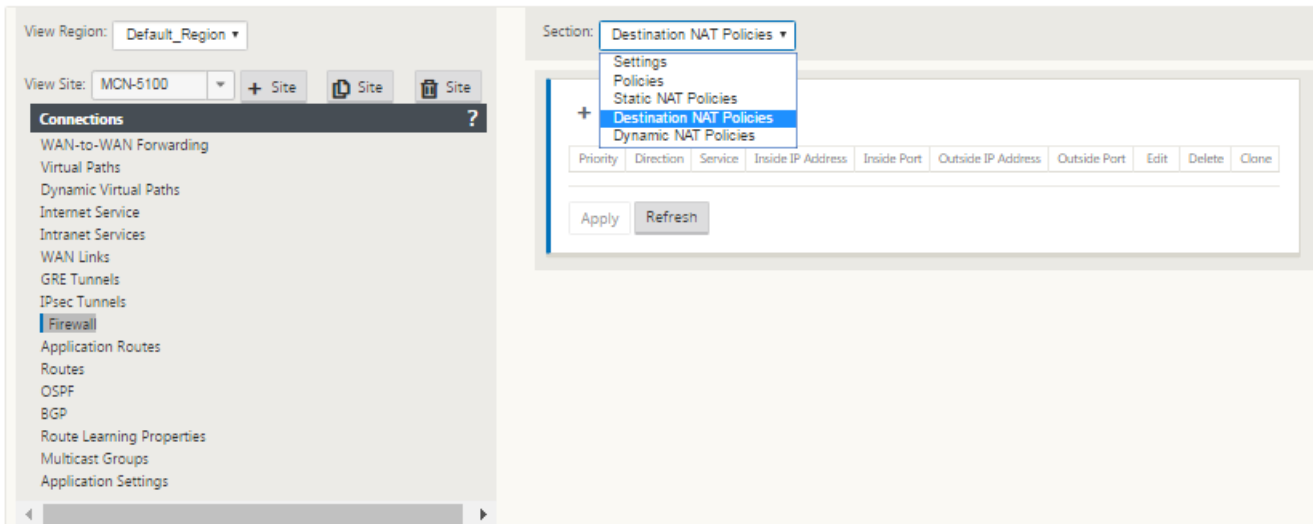
For additional information about NAT support in NetScaler SD-WAN, see the following topic, [Configure NAT](#)



Use the NetScaler SD-WAN GUI to configure Destination NAT (DNAT). In the configuration, add one or more DNAT policies that redirect traffic matching a specific destination IP address and port.

To configure Destination NAT

1. In the SD-WAN SE/VPX GUI, go to **Configuration** -> **Virtual WAN** -> Configuration Editor. Click **Open** to open an existing package. Select a saved configuration package. You can also create new DNAT rules while building the network configuration.
2. At the DC (MCN), configure Internet Service. Go to **Connections** -> **Firewall**.
3. Click + **Add** to add a DNAT policy.
4. In the **Add Destination NAT Policy** dialog box, provide the following information:
 - Priority
 - Direction
 - Service Type
 - Service Name
 - Inside IP Address
 - Inside Port
 - Outside IP Address
 - Outside Port



5. Provision Destination NAT rules for Firewall traffic redirect, similar to static NAT.
6. Enter the matching criteria and the Destination IP/port to be NATed.
7. Perform connection matching of the DNAT rule with statistics.
8. Remove or Update DNAT rules during configuration update.

You can also use the NetScaler SD-WAN GUI to monitor the current DNAT policy configuration.

To monitor the current Destination NAT policy configuration:

1. In the NetScaler SD-WAN GUI, navigate to **Monitoring -> Firewall -> NAT Policies**.
2. Select the tab that includes the statistics you want to monitor.

Dashboard | Monitoring | Configuration

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any

Service Type: Any Service Name: Any

Inside IP: * Inside Port: * Outside IP: * Outside Port: *

Refresh Show latest data.

Help

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside		Outside		Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
							IP Address	Port	IP Address	Port									
1	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

Dashboard | Monitoring | Configuration

Monitoring > Firewall

Firewall Statistics

Statistics: Connections

Maximum entries to display: Filter Policies

Filtering: NAT Policies

IP Protocol: Any Family: Any

Source Service Type: Any Source Zones: Any Destination Zones: Any

Destination Service Type: Any Source Service Instances: Any Source IP: * Source Port: *

Destination Service Instances: Any Destination IP: * Destination Port: *

Refresh Clear Connections Show latest data Show Drops

Help

Connections

Application	Family	IP Protocol	Source				Destination				State		
			IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type		Service Name	Zone
Domain Name Service(dns)	Network Service	UDP	172.16.6.10	36080	Virtual Path	DC-MCN-BR1-CB2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED
Domain Name Service(dns)	Network Service	UDP	172.16.16.1	56451	Virtual Path	DC-MCN-BR1-CB2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED

Stateful Firewall and NAT Support

Mar 01, 2018

This feature provides a firewall built into the SD-WAN application. The firewall allows policies between services and zones, and supports Static NAT, Dynamic NAT (PAT), and Dynamic NAT with Port Forwarding. Additional firewall capabilities include:

- Provide security for user traffic within SD-WAN network (Enterprise and Service Providers)
- (Potential) Reduction of External Equipment (Enterprise and Service Providers)
- Using the same IP address space for Multiple customers: NAT Capability (Service Providers)
- Apply multiple firewalls from a global perspective (Service Providers)
- Filtering traffic flows between Zones
- Filtering traffic between services within a Zone
- Filtering traffic between services that reside in different Zones
- Filtering traffic between services at a site
- Defining Filter Policies to Allow, Deny, or Reject flows
- Tracking flow state for selected flows
- Applying Global Policy Templates
- Support for Port Address Translation for traffic to the Internet on an untrusted port, as well as port forwarding inbound and outbound
- Provide Static Network Address Translation (Static NAT)
- Provide Dynamic Network Address Translation (Dynamic NAT)
- Port Address Translation (PAT)
- Port-Forwarding

To simplify the configuration process, firewall Policies are created at the Global Configuration level. This Global configuration consists of Pre-Appliance and Post-Appliance site Policy Templates that can be applied to all sites within the SD-WAN network.

Note

It is not recommended to use firewall in Fail-to-Wire inline mode due to security reasons.

Global ?

- Network Settings
- Regions
- Centralized Licensing
- Routing Domains
- Applications
- Firewall Zones
- Firewall Policy Templates**
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- Autopath Groups
- Service Providers
- WAN-to-WAN Forwarding Groups
- WAN Optimization Features
- WAN Optimization Tuning Settings
- WAN Optimization Application Classifiers
- WAN Optimization Service Classes

Policy Template: **New_Firewall_Policy_Template-1** + Add Policy Template Delete Policy Template

Template Name:

Pre-Appliance Template Policies + Add ?

Priority	Action	Zones		Application	Application Family	Application Objects	IP Protocol	DSCP	Source			Destination			Match Est.	Reverse Also	Info	Edit	Delete	Clone
		From	To						Service	IP Address	Port	Service	IP Address	Port						

Post-Appliance Template Policies + Add ?

Priority	Action	Zones		Application	Application Family	Application Objects	IP Protocol	DSCP	Source			Destination			Match Est.	Reverse Also	Info	Edit	Delete	Clone
		From	To						Service	IP Address	Port	Service	IP Address	Port						

Apply Refresh

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:

IP Protocol: DSCP: 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:

Add

? x

Priority:

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"/>
Internet_Zone	<input type="checkbox"/>	Internet_Zone	<input type="checkbox"/>
Untrusted_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:

IP Protocol: DSCP: 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:

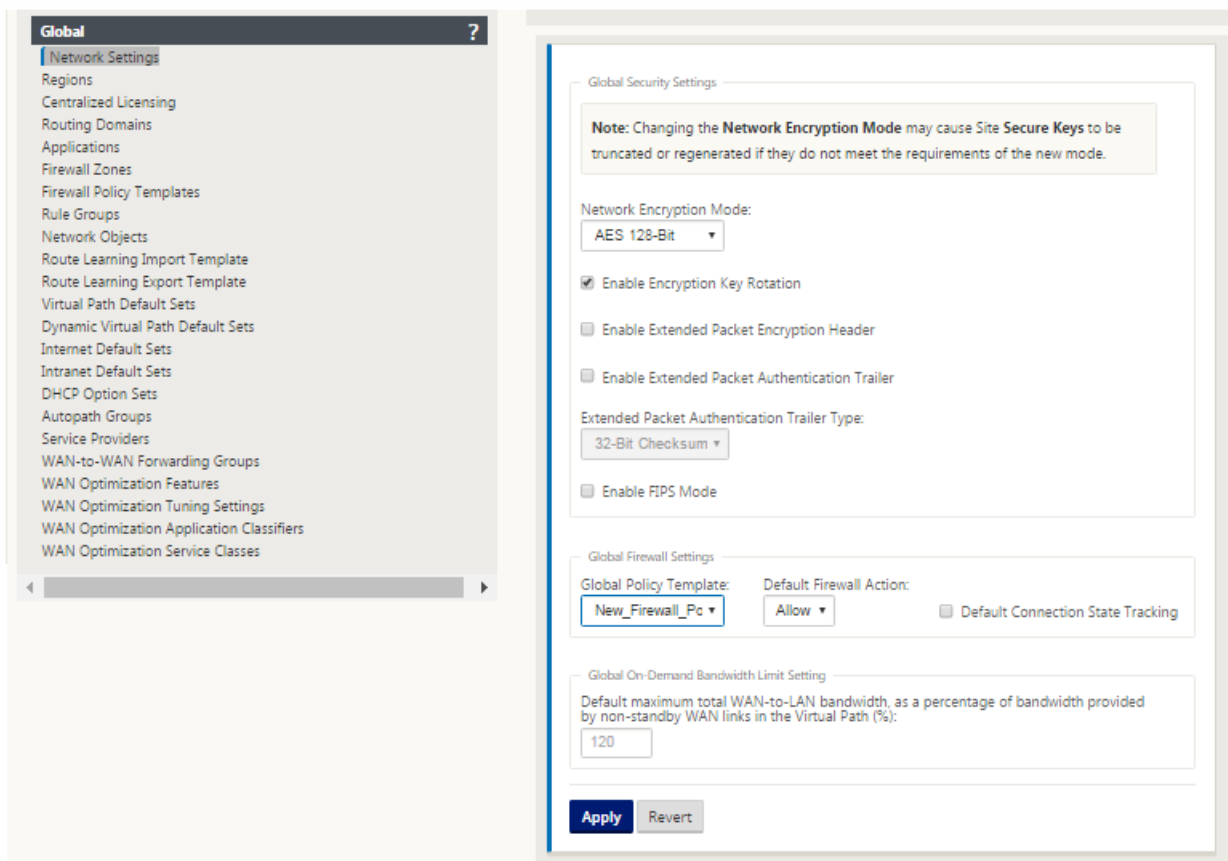
Global Firewall Settings

Mar 01, 2018

Once you have created the firewall policy templates you can use this policy to configure firewall settings for NetScaler SD-WAN Network. Using the Global firewall settings, you can configure the global firewall parameters, these settings are applied to all the sites on the virtual WAN network.

To configure global firewall settings:

1. In the **Configuration Editor**, navigate to **Global > Network Settings** and click the edit icon.



2. In the **Global Firewall Settings** section, select values for the following options:

- * **Global Policy Template:** Select a firewall policy template to be applied to all the appliances in the SD-WAN network.
- * **Default Firewall Actions:** Select Allow to allow packets not matching the filter policy. Select Drop, to drop the packets not matching the filter policy.
- * **Default Connection State Tracking:** This enables directional connection state tracking for TCP, UDP and ICMP flows that do not match a filter policy or NAT rule. This blocks asymmetric flow, even when there are no firewall policies defined.

Note

You can also configure these settings at the site level, this will override the global setting.



3. Click **Apply**.

Advanced Firewall Settings

Mar 01, 2018

You can configure the advanced firewall settings for every site individually. This will override the global settings.

To configure advanced firewall settings:

1. In the **Configuration Editor**, navigate to **Connections > View Site > Firewall > Settings**.

The screenshot shows the 'Settings' section of the Configuration Editor. At the top, there is a 'Section:' dropdown menu set to 'Settings'. Below it is a 'Policy Templates' section with a table containing one entry: 'Policy_New' with a priority of '100'. Below the table is the 'Advanced' settings section, which includes various timeout and connection state tracking parameters. The 'Default Firewall Action' is set to 'Allow'. The 'Default Connection State Tracking' is set to 'Use Global Setting' and 'Source Route Validation' is checked. Other parameters include 'Max New Connections per Source' (100), 'Max Connections per Source' (0), 'Untracked and Denied Timeout (s)' (30), 'TCP Initial Timeout (s)' (120), 'TCP Idle Timeout (s)' (7440), 'TCP Closing Timeout (s)' (60), 'TCP Time Wait Timeout (s)' (120), 'TCP Closed Timeout (s)' (10), 'UDP Initial Timeout (s)' (30), 'UDP Idle Timeout (s)' (300), 'ICMP Initial Timeout (s)' (30), 'ICMP Idle Timeout (s)' (60), 'Generic Initial Timeout (s)' (30), and 'Generic Idle Timeout (s)' (300). At the bottom of the settings section are 'Apply' and 'Revert' buttons.

2. In the **Policy Template** section, click **Add**. Enter values for the following parameters.

- * **Priority** - The order in which the policy is applied at the site.
- * **Name** - The name of the Policy Template to use at the Site.

3. Click **Advanced**. Enter values for the following parameters:

- * **Default Firewall Action** - Select one of the following options.

- **Use Global Setting** - Use the Global setting configured in NetScaler SD-WAN settings
- **Allow** - Packets not matching any filter policy is permitted.
- **Drop** - Packets not matching any filter policy is dropped.

- * **Default Connection State Tracking** - Select one of the following options.

- **Use Global Setting** - Use the Global setting configured in NetScaler SD-WAN settings

- **No Tracking** - Bidirectional connection state tracking will not be performed on packets not matching any filter policy

- **Track** - Bidirectional connection state tracking will be performed on TCP, UDP and ICMP packets not matching any filter policy or NAT rule. This blocks asymmetric flow, even when there are no firewall policies defined.

* **Source Route Validation**: If enabled, packets will be dropped when received on an interface that differs from the packet's route, as determined by the Source IP Address. Only the route the packet would currently match is considered.

* **Max New Connections per Source**: The maximum number of non-established Connections to allow per Source IP Address. 0 means unlimited. Use this setting to help prevent Denial of Service Attacks on the firewall.

* **Max Connections per Source**: The maximum number of connections to allow per Source IP Address. 0 means unlimited. Use this setting to help prevent Denial of Service Attacks on the firewall.

4. Configure the various timeout settings and click **Apply**.

Zones

Mar 01, 2018

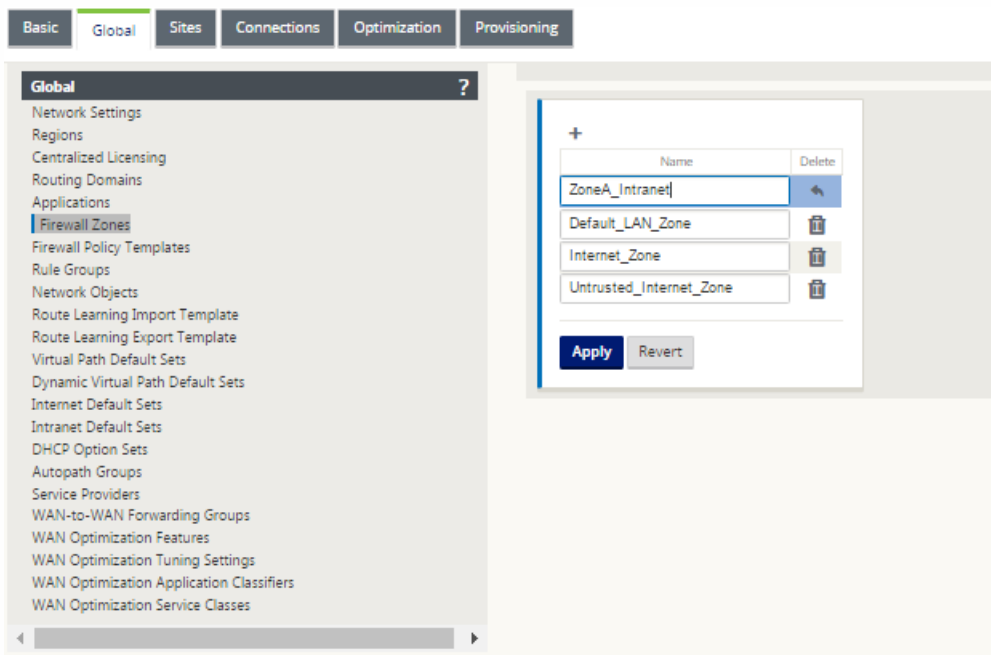
You can configure zones in the network and define policies to control how traffic enters and leaves zones. By default, the following zones are created:

- * Internet_Zone
 - Applies to traffic to or from an Internet service using a Trusted interface.
- * Untrusted_Internet_Zone
 - Applies to traffic to or from an Internet service using an Untrusted interface.
- * Default_LAN_Zone
 - Applies to traffic to or from an object with a configurable zone, where the zone has not been set.

You can create your own zones and assign them to the following types of objects:

- * Virtual Network Interfaces (VNI)
- * Intranet Services
- * GRE Tunnels
- * LAN IPsec Tunnels

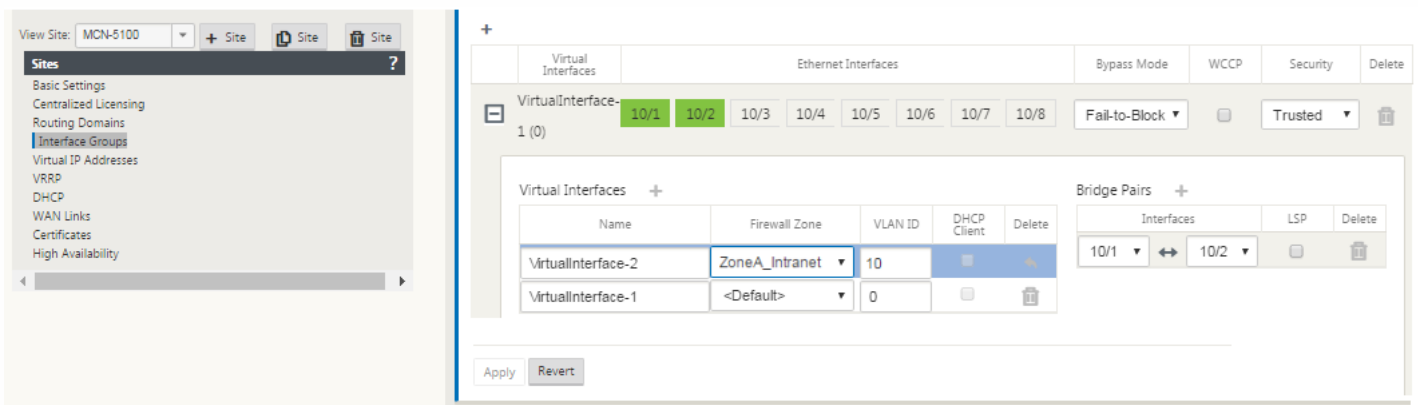
The following illustration displays the three zones pre-configured. Additionally, you can create your own zones as required. In this example, the zone “ZoneA_Intranet” is a user created zone. It is assigned to the Virtual Interface of the bypass segment (ports 1 and 2) of the SD-WAN appliance.



The source zone of a packet is determined by the service or virtual network interface a packet is received on. The

exception to this is virtual path traffic. When traffic enters a virtual path, packets are marked with the zone that originated the traffic and that source zone is carried through the virtual path. This allows the receiving end of the virtual path to make a policy decision based on the original source zone before it entered the virtual path.

For example, a network administrator may want to define policies so that only traffic from VLAN 30 at Site A is allowed to enter VLAN 10 at Site B. The administrator can assign a zone for each VLAN and create policies that permit traffic between these zones and blocks traffic from other zones. The screenshot below shows how a user would assign the "ZoneA_Intranet" zone to VLAN 10. In this example, the "ZoneA_Intranet" zone was previously defined by the user in order to assign it to Virtual Interface "VirtualInterface-2".



The destination zone of a packet is determined based on the destination route match. When a SD-WAN appliance looks up the destination subnet in the route table, the packet will match a route, which has a zone assigned to it.

* Source zone

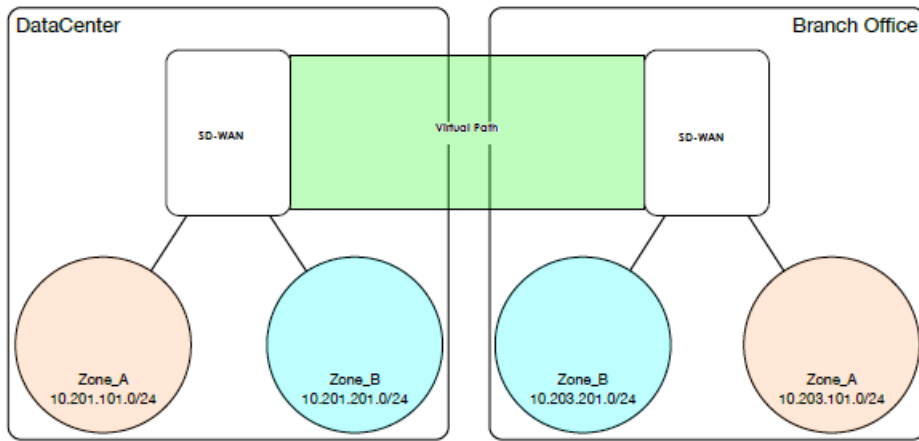
- Non-Virtual Path: Determined through the Virtual Network Interface packet was received on.
- Virtual Path: Determined through source zone field in packet flow header.
- Virtual network interface - the packet was received on at source site.

* Destination zone

- Determined through destination route lookup of packet.

Routes shared with remote sites in the SD-WAN maintain information about the destination zone, including routes learned through dynamic routing protocol (BGP, OSPF). Using this mechanism, zones gain global significance in SD-WAN network and allow end-to-end filtering within the network. The use of zones provides a network administrator an efficient way to segment network traffic based on customer, business unit, or department.

The capability of SD-WAN firewall allows the user to filter traffic between services within a single zone, or to create policies that can be applied between services in different zones, as shown in figure below. In the example below, we have Zone_A and Zone_B, each of which has a LAN Virtual network interface.



Screenshot below displays the inheritance of zone for a Virtual IP (VIP) from its assigned Virtual Network Interface (VNI).

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Policies

Mar 01, 2018

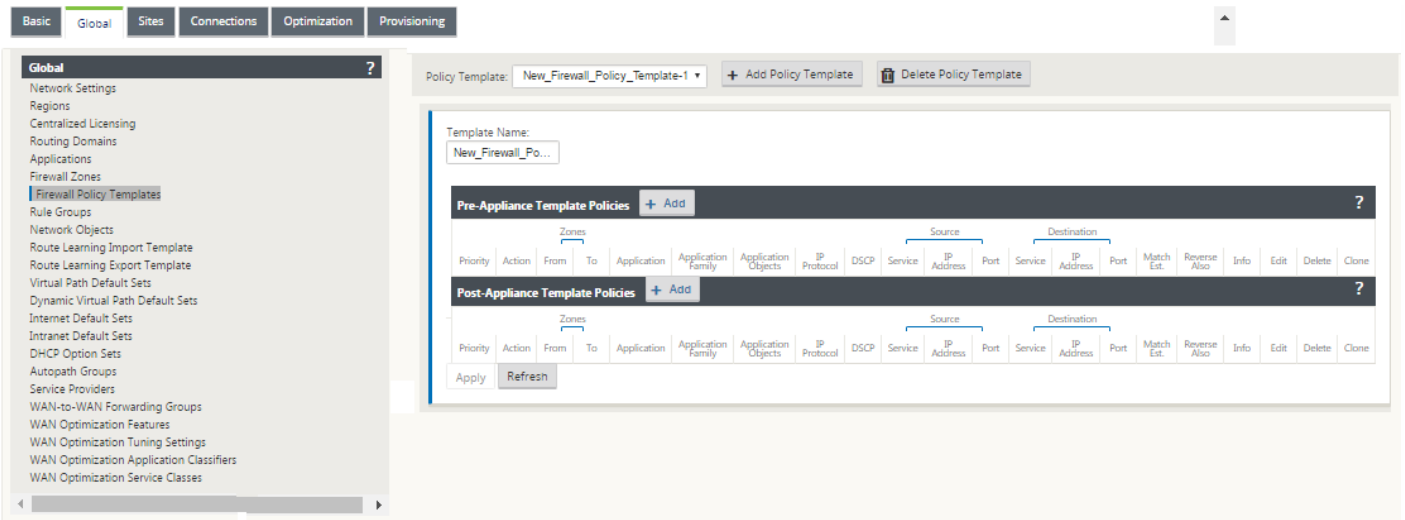
Policies provide the ability to allow, deny, reject, or count and continue specific traffic flows. Applying these policies individually to each site would be difficult as the SD-WAN networks grows. To resolve this issue, groups of firewall filters can be created with a Firewall Policy Template. A Firewall Policy Template can be applied to all sites in the network or only to specific sites. These policies are ordered as either Pre-Appliance Template Policies or Post- Appliance Template Policies. Both network-wide Pre-Appliance and Post-Appliance Template Policies are configured at the Global level. Local policies are configured at the site level under Connections and apply only to that specific site.

The screenshot displays a configuration interface for firewall policies, organized into three main sections: Pre-Appliance Template Policies, Local Policies, and Post-Appliance Template Policies. Each section contains a table of policy configurations. The 'Pre-Appliance Template Policies' and 'Post-Appliance Template Policies' sections have identical column headers: Template, Routing Domain, Action, Zones (From, To), Application, Application Family, Application Objects, Source (IP Protocol, DSCP, Service), Destination (IP Address, Port, Service), IP Address, and Port. The 'Local Policies' section includes a 'Priority' column and an '+ Add' button. The interface uses a dark header for each section and blue brackets to group the 'Zones', 'Source', and 'Destination' columns.

Pre-Appliance Template Policies are applied before any local site policies. Local site policies are applied next, followed by Post-Appliance Template Policies. The goal is to simplify the configuration process by allowing you to apply global policies while still maintaining the flexibility to apply site-specific policies.

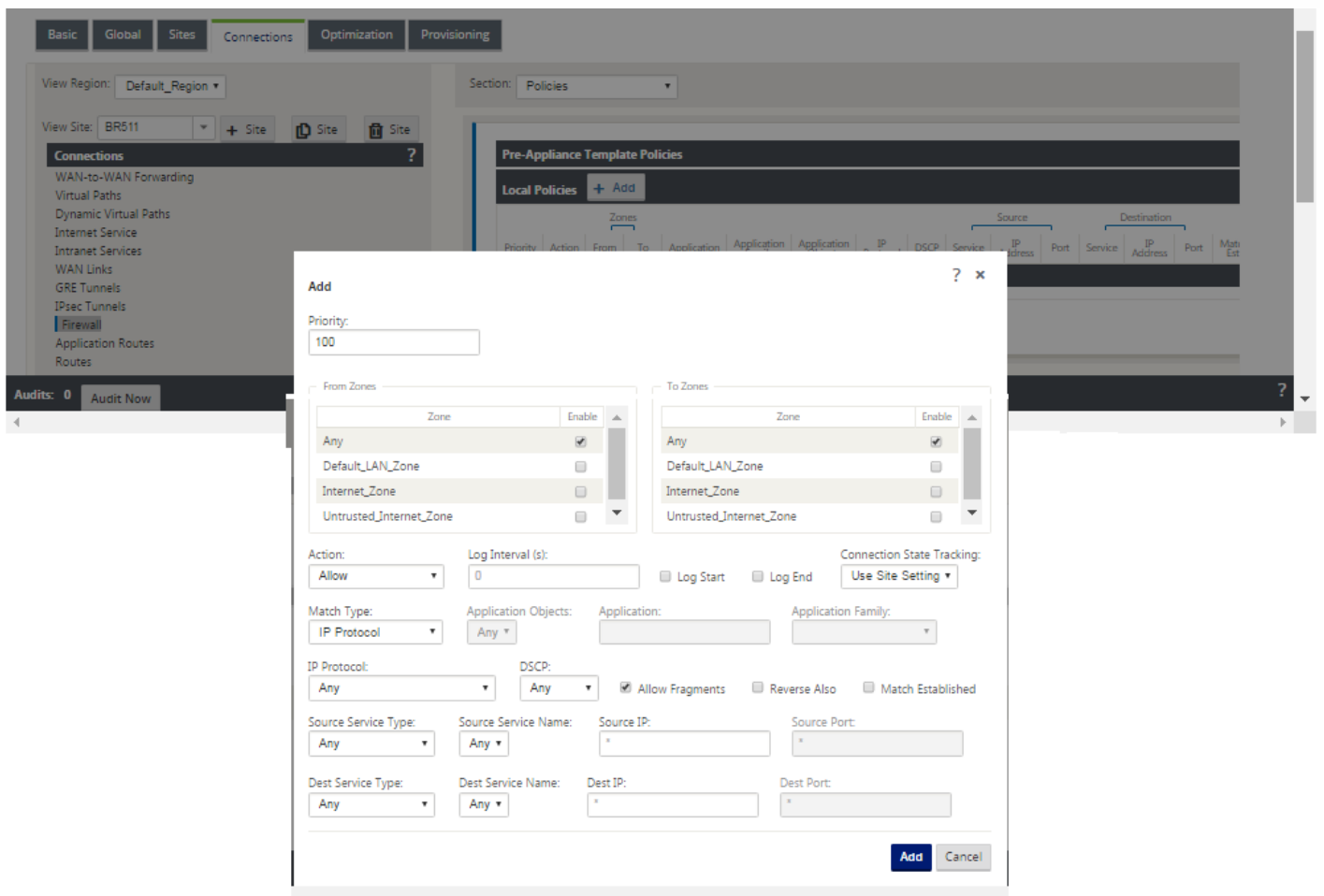
1. Pre-Templates – compiled policies from all template “PRE” sections.
2. Pre-Global – compiled policies from Global “PRE” section.
3. Local – appliance-level policies.
4. Local Auto Generated – automatically local generated policies.
5. Post-Templates – compiled policies from all template “POST” sections.
6. Post-Global – compiled policies from Global “POST” section.

You can configure Pre-Appliance and Post-Appliance Template Policies at a global level. Local policies are applied at the site level of an appliance.



The above screenshot shows the policy template that would apply to the SD-WAN network globally. To apply a template to all sites in the network, navigate to **Global > Network Settings > Global Policy Template**, and select a specific policy. At the site level, you can add more policy templates, as well as create site specific policies.

The specific configurable attributes for a policy are displayed in the below screen shot, these are the same for all the policies.



* **Priority** – order in which the policy will be applied within all the defined policies. Lower priority policies are applied

before higher priority policies.

* **Zone** – flows have a source zone and destination zone.

- **From Zone** – source zone for the policy.

- **To Zone** – destination zone for the policy.

* **Action** – action to perform on a matched flow.

- **Allow** – permit the flow through the Firewall.

- **Drop** – deny the flow through the firewall by dropping the packets.

- **Reject** – deny the flow through the firewall and send a protocol specific response. TCP will send a reset, ICMP will send an error message.

- **Count and Continue** – count the number of packets and bytes for this flow, then continue down the policy list.

* **Log Interval** – time in seconds between logging the number of packets matching the policy to the firewall log file or the syslog server, if it is configured.

- **Log Start** – if selected, a log entry is created for the new flow.

- **Log End** – log the data for a flow when the flow is deleted.

Note

The default Log Interval value of 0 means no logging.

* **Track** – allows the firewall to track the state of a flow and display this information in the **Monitoring > Firewall > Connections** table. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under **Firewall > Settings > Advanced > Default Tracking**.

- **No Track** – flow state is not enabled.

- **Track** – displays the current state of the flow (which matched this policy).

* **Match Type** – select one of the following match types –

- **IP Protocol** – If this match type is selected, select an IP protocol that the filter will match with. Options include ANY, TCP, UDP ICMP and so

- **Application** – If this match type is selected, specify the application that is used as a match criteria for this filter.

- **Application Family** – If this match type is selected, select an application family that is used as a match criteria for this filter.

- **Application Object** – If this match type is selected, select an application family that is used as a match criteria for this filter.

For more information on application, application family and application object, see [Application Classification](#).

- * **DSCP** – allow the user to match on a DSCP tag setting.
- * **Allow Fragments** – allow IP fragments that match this filter policy.

Note

The firewall does not reassemble fragmented frames.

- * **Reverse Also** – automatically add a copy of this filter policy with source and destination settings reversed.
- * **Match Established** – match incoming packets for a connection to which outgoing packets were allowed.
- * **Source Service Type** – in reference to a SD-WAN service – Local (to the appliance), Virtual Path, Intranet, IPhost, or Internet are examples of Service Types.
 - * **IPhost Option** - This is a new service type for the Firewall and is used for packets that are generated by the SD-WAN application. For example, running a ping from the Web UI of the SD-WAN results in a packet sourced from a SD-WAN Virtual IP address. Creating a policy for this IP address would require the user to select the IPhost option.
 - * **Source Service Name** – name of a service tied to the service type. For example, if virtual path is selected for Source Service type, this would be the name of the specific virtual path. This is not always required and depends on the service type selected.
 - * **Source IP address** – typical IP address and subnet mask the filter will use to match.
 - * **Source Port** – source port the specific application will use.
 - * **Destination Service Type** - in reference to a SD-WAN service – Local (to the appliance), Virtual Path, Intranet, IPhost, or Internet are examples of service types.
 - * **Destination Service Name** - name of a service tied to the service type. This is not always required and depends on the service type selected.
 - * **Destination IP Address** - typical IP address and subnet mask the filter will use to match.
 - * **Destination Port** – destination port the specific application will use (i.e. HTTP destination port 80 for the TCP protocol).

The track option provides much more detail about a flow. The state information tracked in the state tables is included below.

There are only a few states that are consistent:

- * **INIT** - connection created, but the initial packet was invalid.
- * **O_DENIED** - packets that created the connection are denied by a filter policy.
- * **R_DENIED** - packets from the responder are denied by a filter policy.

- * **NOT_TRACKED**- the connection is not statefully tracked but is otherwise allowed.
- * **CLOSED**- the connection has timed out or otherwise been closed by the protocol.
- * **DELETED**- the connection is in the process of being removed. The DELETED state will almost never be seen.

All other states are protocol specific and require stateful tracking be enabled.

TCP can report the following states:

- * **SYN_SENT** - first TCP SYN message seen.
- * **SYN_SENT2**- SYN message seen in both directions, no SYN+ACK (AKA simultaneous open).
- * **SYN_ACK_RCVD**- SYN+ACK received.
- * **ESTABLISHED**- second ACK received, connection is fully established.
- * **FIN_WAIT** - first FIN message seen.
- * **CLOSE_WAIT** - FIN message seen in both directions.
- * **TIME_WAIT** - last ACK seen in both directions. Connection is now closed waiting for reopen.

All other IP protocols (notably ICMP and UDP) have the following states:

- * **NEW**- packets seen in one direction.
- * **ESTABLISHED**- packets seen in both directions.

Network Address Translation (NAT)

Mar 01, 2018

The SD-WAN firewall allows the user to configure static NAT and dynamic NAT for different use cases. The following configurations are supported for NAT:

- * Static one-to-one NAT
- * Dynamic NAT (PAT - Port Address Translation)
- * Dynamic NAT with Port Forwarding rules

Note

At this time, the NAT capability can only be configured at the site level; there is no global configuration (templates) for NAT. All NAT policies are defined from a Source-NAT ("SNAT") translation. Corresponding Destination-NAT ("DNAT") rules are created automatically for the user.

Configure Static NAT

Mar 01, 2018

Static NAT allows the user to configure one-to-one NAT, where an inside IP address will match a public IP address. The configuration options are shown below. You must also define the filter policies to allow traffic back in for the static NAT configuration. You can configure static NAT by navigating to **Connections > View Site > Firewall > Section > Static NAT Policies**.

The screenshot shows a configuration window for adding a Static NAT policy. The 'Priority' field is set to 100. The 'Direction' is set to 'Outbound'. The 'Service Type', 'Service Name', 'Inside Zone', 'Inside IP Address', and 'Outside IP Address' fields all have red asterisks, indicating they are required. There are also checkboxes for 'Bind Responder Route' and 'Proxy ARP'.

* **Priority** - the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.

* **Direction** - the direction, from the perspective of the virtual interface or service, that the translation will operate.

* **Outbound** - the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.

For example, LAN service to Internet service - for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.

* **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.

For example, Internet service to LAN service - For packets received on the Internet service, the source IP address is translated. For packets transmitted on the Internet service, the destination IP address is translated.

* **Service Type** - in reference to a SD-WAN service. For static NAT, these include Local (to the appliance), Intranet, and Internet.

* **Service Name** - specific service name that corresponds to the defined Service Type above.

* **Inside Zone** - one of the existing inside zones configured on the appliance.

* **Inside IP address** - source IP address and mask of the direction selected above.

* **Outside IP address** - the outside IP address and mask of packets that are translated to.

Configure Dynamic NAT

Mar 01, 2018

Dynamic NAT is used when the user wants to forward traffic from a LAN segment to the Internet on an untrusted port. In this case, the user would configure the NAT in an outbound direction, as well as make sure the corresponding filter policies are defined to allow traffic back in. By default, once the dynamic NAT has been configured the system will add in three filter policies.

These policies will:

- * allow Any IP host route, Any zone, Any source and destination.
- * allow match established rule, for reverse traffic of sessions initiated from the inside network.
- * drop all other traffic from the source zone to the destination zone (zone specific).

The following screenshot displays the configuration options for the dynamic NAT configuration.

Add ? x

Priority: 100

Direction: Outbound Type: Port Restricted Service Type: * Service Name: *

Inside Zone: Any Inside IP Address: *

Allow Related IPsec Passthrough GRE/PPTP Passthrough Port Parity Bind Responder Route

Port Forwarding Rules +

Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
Both	*	*	*	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	Use Site Setting	<input type="checkbox"/>

Add Cancel

Configuration Options

* **Priority** – the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.

* **Direction** – the direction from the virtual interface or service perspective the translation will operate.

* **Outbound** – the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.

For example, LAN service to Internet service – for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.

* **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.

For example, Internet service to LAN service – for packets received on the Internet service the source IP address is

translated. For packets transmitted on the Internet service, the destination IP address is translated.

* **Type** – the type of dynamic NAT to perform.

- **Port-Restricted** - Port-Restricted NAT is what most consumer grade gateway routers use. Inbound connections are generally disallowed unless a port is specifically forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port (this is known as endpoint independent mapping). This requirement limits a Port-Restricted NAT firewall to 65535 simultaneous sessions, but facilitates an often used internet technology known as hole punching.

- **Symmetric** – Symmetric NAT is sometimes known as enterprise NAT because it allows for a much larger NAT space and enhances security by making translations less predictable. Inbound connections are generally disallowed unless a port is specifically forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port. Connections from the same inside IP and port need to map to the same outside IP and port (this is known as endpoint dependent mapping). This mode explicitly prevents hole punching.

* **Service Type** – in reference to a SD-WAN service. For static NAT these include Local (to the appliance), Intranet, Internet.

* **Service Name** – the specific service name that corresponds to the defined Service Type above.

* **Inside Zone** – select the inside zone for the packets that require NAT.

* **Inside IP address** - define an IP host address or a subnet based on traffic that requires NAT. This should be an IP address that resides in the Inside Zone.

* **Allow Related** – allow traffic related to the flow matching the rule. For example, ICMP redirection related to the specific flow that matched the policy, if there was some type of error related to the flow.

* **IPsec Passthrough** – allow IPsec traffic to pass through unchanged.

* **GRE/PPTP Passthrough** – allow GRE or IPsec to pass through unchanged.

* **Port Parity** - allows parity for NAT connections.

Configure Dynamic NAT with Port Forwarding

Mar 01, 2018

Dynamic NAT with port forwarding allows the user to port forward specific traffic to a defined IP address. This is typically used for inside hosts like web servers. Once the dynamic NAT is configured the user would define the port forwarding policy. From the example in figure below, we can see that dynamic NAT is configured for a specific IP host address. The NAT example will map an inside IP host to an outside IP host. Port forwarding can then be configured which will define a specific inside and outside port mapped to an inside IP address. In this example, HTTP port 80 is defined for port forwarding.

The screenshot shows the configuration page for a Dynamic NAT rule. The 'Add' button is at the top right. The configuration fields are as follows:

- Priority: 100
- Direction: Inbound
- Type: Port Restricted
- Service Type: Internet
- Service Name: *
- Inside IP Address: *
- Outside Zone: Internet_Zone
- Outside IP Address: 172.111.64.5

Below these fields are several checkboxes: Allow Related, IPsec Passthrough, GRE/PPTP Passthrough, Port Parity, and Bind Responder Route.

The 'Port Forwarding Rules' table is shown below:

Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
Both	*	*	*	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	Use Site Setting	
TCP	80	172.16.187.11	80	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	Track	

At the bottom right of the form are 'Add' and 'Cancel' buttons.

- * **Protocol** – TCP, UDP, or both.
- * **Outside Port** – outside port the user will port forward into the inside port.
- * **Inside IP address** – inside address to forward matching packets.
- * **Inside Port** – map the packet to the same, or a different, outside port.
- * **Fragments** – allow the forwarding of fragmented packets.
- * **Log Interval** – time in second between logging the number of packets matching the policy to a syslog server.
- * **Log Start** – If selected, a new log entry is created for the new flow.
- * **Log End** – log the data for a flow when the flow is deleted.

Note

The default Log Interval value of 0 means no logging.

* **Track** – allows the firewall to track the state of a flow and display this information in the **Monitor > Firewall > Connections**. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under **Firewall > Settings > Advanced > Default Tracking**.

- **No Track** – flow state is not enabled.
- **Track** – displays the current state of the flow (which matched this policy).

Configure Virtual WAN Service

Mar 01, 2018

The SD-WAN configuration describes and defines the topology of your SD-WAN network. Before you can deploy a SD-WAN network, you must define the Virtual WAN configuration. To do this, use Configuration Editor in the SD-WAN Management Web Interface on the MCN appliance.

Security and Encryption

Enabling encryption for SD-WAN (for the Virtual Paths) is optional. Instructions for configuring this feature are provided in the section, [Enabling and Configuring Virtual WAN Security and Encryption \(Optional\)](#).

When encryption is enabled, SD-WAN uses the Advanced Encryption Standard (AES) to secure traffic across the Virtual Path. Both AES 128 and 256 bit ciphers (key sizes) are supported by the SD-WAN Appliances, and are configurable options. You can select, enable, and configure these and the other encryption options by using the Configuration Editor in the Management Web Interface on the Management Control Node (MCN). You must have administrative access on the MCN to modify the configuration, and to distribute your changes across the SD-WAN network. Once the MCN is secured, the encryption settings and their distribution are also secure.

Authentication between sites functions by means of the Virtual WAN Configuration.

The network configuration has a secret key for each site. For each Virtual Path, the network configuration generates a key by combining the secret keys from the sites at each end of the Virtual Path. The initial key exchange that occurs after a Virtual Path is first set up, is dependent upon the ability to encrypt and decrypt packets by means of that combined key.

If this is an initial installation and configuration, as a final step you will need to manually enable the Virtual WAN Service on each SD-WAN appliance in your network. Enabling the service enables and starts the Virtual WAN daemon.

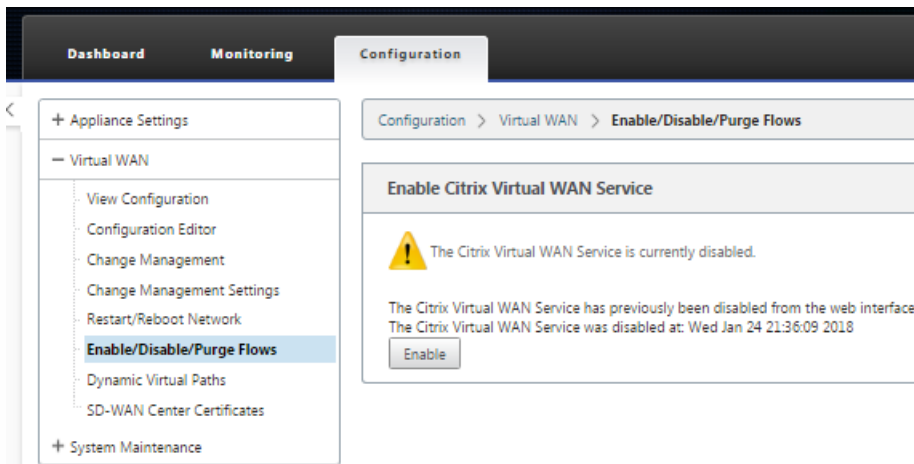
Note

If you are reconfiguring an existing deployment, the MCN automatically enables the service when it distributes the updated Appliance Packages to the client sites. In this case, you can skip this final step.

To manually enable the Virtual WAN Service on an appliance, do the following:

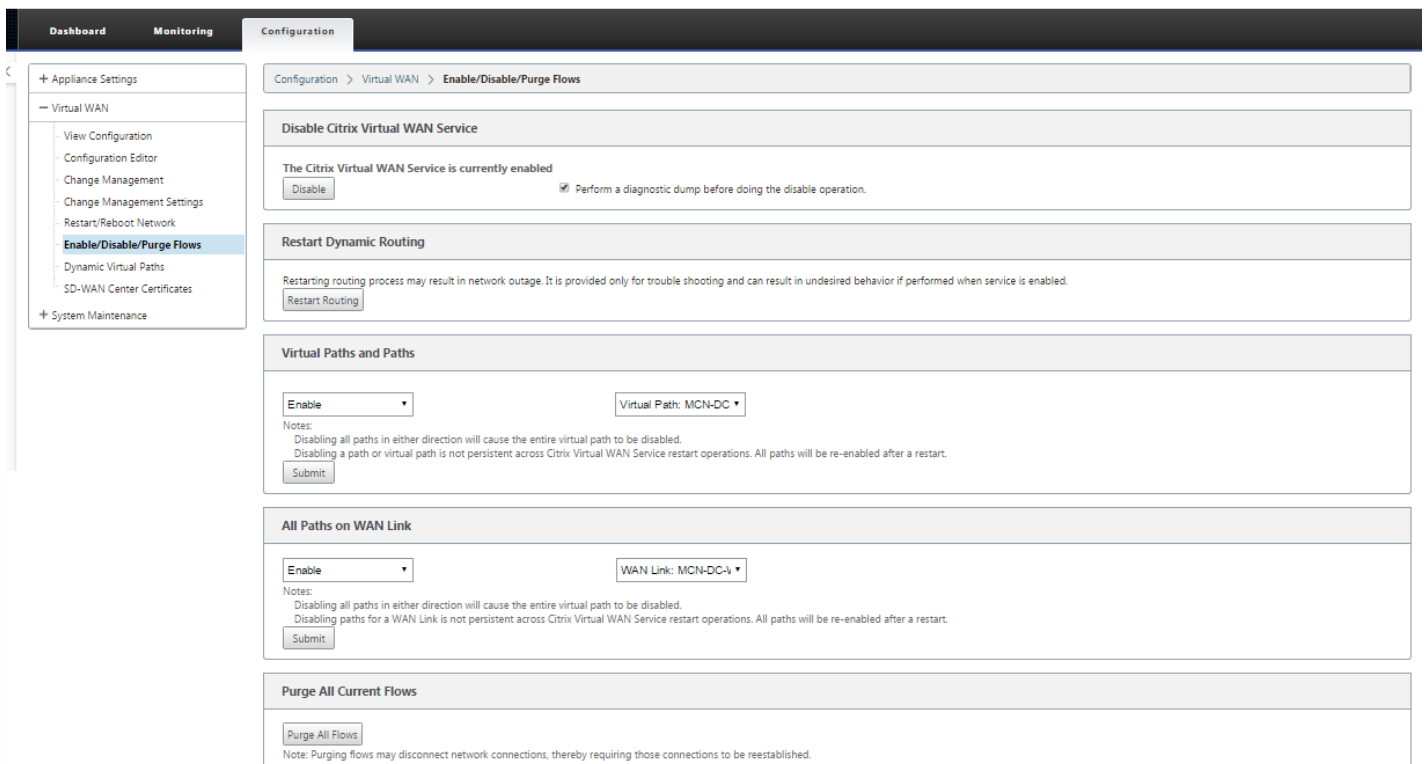
1. Log into the Management Web Interface on the appliance you want to activate.
2. Select **Configuration** tab.
3. In the navigation pane, open the Virtual WAN branch and select **Enable/Disable/Purge Flows**.

If the Virtual WAN Service is currently disabled, this displays the Enable Virtual WAN Service page, as shown below. If the service is already enabled, this displays the Enable/Disable/Purge Flows page.



4. Click **Enable**.

This enables the service, and displays the **Enable/Disable/Purge Flows** page.



When the Virtual WAN Service is enabled, a status message to that effect displays in the top section of the page.

Note

This page also presents options for enabling/disabling specific paths and Virtual Paths in your network, as well as an option to purge all flows.

This completes the installation and activation of the SD-WAN on the MCN and branch site client appliances. You can now use the Monitoring pages to verify the activation and diagnose any existing or potential configuration issues.

Configure Firewall Segmentation

Mar 01, 2018

Virtual Route Forwarding (VRF) firewall segmentation provides multiple routing domain access to the internet through a common interface, with each domain's traffic isolated from that of the others. For example, employees and guests can access the internet through the same interface, without any access to each other's traffic.

- Local guest-user Internet access
- Employee-user Internet access for defined applications
- Employee-users may continue hairpin all other traffic to the MCN
- Allow the user to add specific routes for specific routing domains.
- When enabled, this feature applies to all routing domains.

You can also create multiple access interfaces to accommodate separate public facing IP addresses. Either option provides the required security necessary for each user group.

Note

For more information, see how to [configure VRFs](#).

To configure internet services for all Routing Domains:

1. Create Internet Service for a Site. Navigate to **Connections > View Region > View Site > [Site Name] > Internet Service > Section > WAN Links** and, under WAN Links, select the **Use** check box.

The screenshot shows the Citrix NetScaler configuration interface. The top navigation bar includes tabs for Basic, Global, Sites, Connections, Optimization, and Provisioning. The 'Connections' tab is active. On the left, a sidebar shows a tree view with 'Connections' expanded, and 'Internet Service' selected. The main area displays the configuration for 'Internet Service' under the 'WAN Links' section. A table lists two WAN links: BR511-WL-1 and BR511-WL-2. The 'Use' checkbox is checked for BR511-WL-1 and unchecked for BR511-WL-2. Other columns include Mode (Prima), Tunnel Header Size (bytes) (0), Access Interface Follower (checked), Tagging (None), Max Delay (ms) (500), and Grooming (checked). Buttons for 'Apply' and 'Revert' are visible at the bottom of the table.

WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Follower	Tagging	Max Delay (ms)	Tagging	Matching	Grooming
BR511-WL-1	<input checked="" type="checkbox"/>	Prima	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>
BR511-WL-2	<input type="checkbox"/>	Prima	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>

Note

You should see 0.0.0.0/0 routes added, one per routing domain, under **Connections > View Region > View Site > [Site Name] > Routes**.

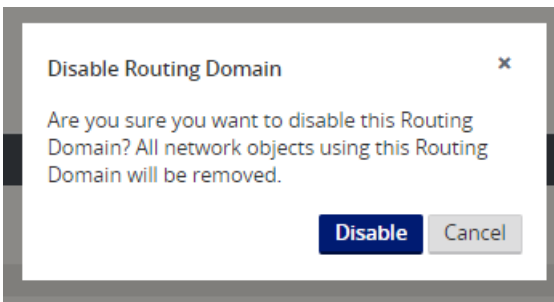
Search:

Order	Network IP Address	Routing Domain	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.200.247.41/24	Default	5	Local			ⓘ		
2	10.200.247.42/24	Default	5	Local			ⓘ		
3	10.200.247.6/24	Default	5	Local			ⓘ		
4	11.123.10.0/24		5	Intranet	Intranet-0		ⓘ	✎	🗑️
5	11.20.20.11/24	Guest	5	Local			ⓘ		
6	12.125.10.0/24		5	Internet			ⓘ	✎	🗑️
7	0.0.0.0/0	Default	5	Internet			ⓘ		
8	0.0.0.0/0	Guest	5	Internet			ⓘ		
9	0.0.0.0/0	Default	16	Passthrough			ⓘ		
10	0.0.0.0/0	Guest	16	Passthrough			ⓘ		

⏪ < 1 > ⏩

It is no longer required to have all routing domains enabled at the MCN.

If you disable routing domains at the MCN, the following message appears if the domains are in use at a branch site:



You can confirm that each routing domain is using the internet service by checking the Routing Domain column in the Flows table of the web management interface under **Monitor > Flows**.

Flows Data Toggle Columns

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
Guest	11.20.20.20	12.125.10.20	WAN Ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A		N/A
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
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
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

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

You can also check the routing table for each routing domain under **Monitor > Statistics > Routes**.

Routes for routing domain: Guest

Filter: in Any column

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

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-		-	5	318	YES	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-		-	5	0	YES	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-		-	5	159	YES	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-		-	16	0	YES	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-		-	16	0	YES	N/A

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

Use Cases

In previous NetScaler SD-WAN releases, virtual routing and forwarding had the following issues, which have been resolved.

- Customers have multiple routing domains at a branch site without the requirement to include all domains at the data center (MCN). They need the ability to isolate different customers' traffic in a secure manner
- Customers must be able to have a single accessible firewalled Public IP address for multiple routing domains to access the internet at a site (extend beyond VRF lite).
- Customers need an Internet route for each routing domain supporting different services.
- Multiple routing domains at a branch site.
- Internet Access for different routing domains.

Multiple routing domains at a branch site

With the Virtual Forwarding and Routing Firewall segmentation enhancements, you can:

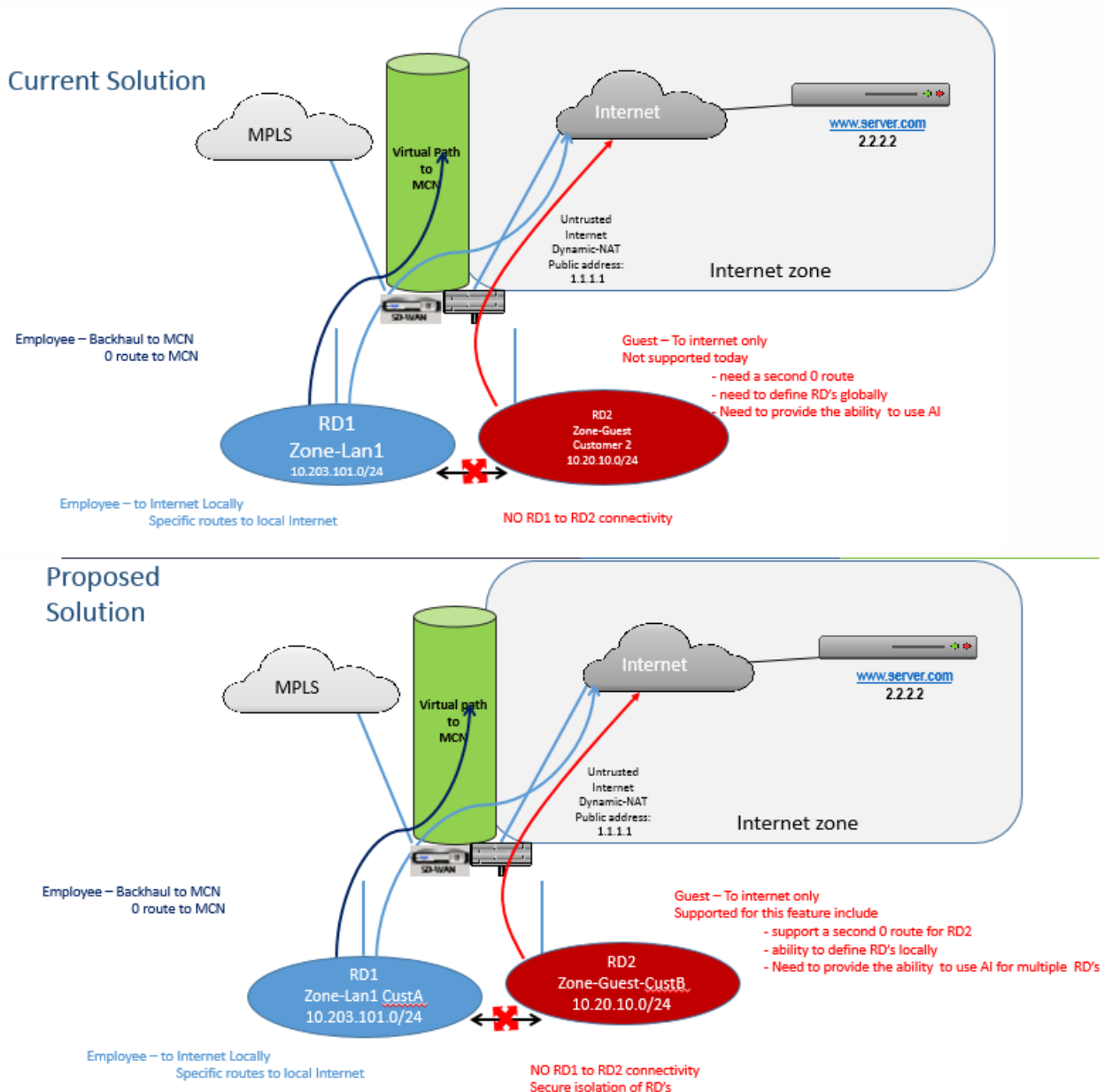
- Provide an infrastructure, at the branch site, that supports secure connectivity for at least two user groups, such as employees and guests. The infrastructure can support up to 16 routing domains.
- Isolate each routing domain's traffic from the the traffic of any other routing domain.
- Provide internet access for each routing domain,
 - A common Access Interface is required and acceptable
 - An Access Interface for each group with separate Public facing IP addresses
- Traffic for the employee can be routed directly out to the local internet (specific applications)
- Traffic for the employee can be routed or backhauled to the MCN for extensive filtering (0 route)
- Traffic for the routing domain can be routed directly out to the local internet (0 route)
- Supports specific routes per routing domain, if required
- Routing domains are VLAN based
- Removes the requirement for the RD to have to reside at the MCN
- Routing Domain can now be configured at a branch site only
- Allows you to assign multiple RD to an access interface (once enabled)
- Each RD will be assigned a 0.0.0.0 route
- Allows specific routes to be added for a RD
- Allows traffic from different RD to exit to the internet using the same access interface
- Allows you to configure a different access interface for each RD
- Must be unique subnets (RD are assigned to a VLAN)
- Each RD can use the same FW default Zone
- The traffic is isolated through the Routing Domain
- Outbound flows have the RD as a component of the flow header. Allows SD-WAN to map return flows to correct Routing domain.

Prerequisites to configure multiple routing domains:

- Internet access is configured and assigned to a WAN Link.
- Firewall configured for NAT and correct policies applied.

- Second routing domain added globally.
- Each routing domain added to a site.
- At Sites > Site Name > WAN Links > WL2 [name] > Access Interface, make sure that the check box is available and internet service has been defined correctly. If you cannot select the check box, the internet service is not defined or assigned to a WAN link for the site.

Deployment Scenarios



- The internet service must be added to the WAN link before you can enable Internet access for all Routing Domains. (Until you do, the check box for enabling this option is grayed out).

After enabling internet access for all routing domains, auto add a dynamic-NAT rule.

- Up to 16 Routing Domains per site.

- Access Interface (AI): Single AI per subnet.
- Multiple AIs require a separate VLAN for each AI.
- If you have two routing domains at a site and have a single WAN Link, both domains use the same public IP address.
- If Internet access for all routing domains is enabled, all sites can route to Internet. (If one routing domain does not require internet access, you can use the firewall to block its traffic.)
- No support for the same subnet in multiple routing domains.
- There is no audit functionality
- The WAN links are shared for Internet access.
- No QOS per routing domain; first come first serve.

SNMP

Mar 01, 2018

NetScaler SD-WAN supports SNMPV1/V2 capability and only a single user account for each SNMPv3 capability. This restriction provides the following advantages:

- Ensuring SNMPv3 compliance for network devices
- Verification of SNMPv3 capability
- Easy configuration of SNMPv3

To configure SNMPv3 Polling and Traps, navigate to the SNMPv3 section of the **Configuration** -> **Appliance Settings** -> **SNMP** page, and fill in the fields as required.

Dashboard Monitoring Configuration

Configuration > Appliance Settings > SNMP

Managers Download MIB File

SNMP

UDP Port: 161

System Description: Citrix Virtual WAN Appliance

System Contact: support@citrix.com

System Location: Citrix

SNMP v1/v2

Enable v1/v2 Agent

Community String: public

Enable v1/v2 Traps

Destination IP Address(es):

Port: 162

SNMP v3

Enable v3 Agent

User Name:

Password:

Verify Password:

Authentication: MD5

Encryption: None

Enable v3 Traps

Destination IP Address(es):

Port: 162

User Name:

Password:

Verify Password:

Authentication: MD5

Encryption: None

The following standard MIBs are supported by the SD-WAN Appliances.

MIB	RFC (Definition Link)
DISMAN-EVENT-MIB	https://www.ietf.org/rfc/rfc2981.txt
IF-MIB	https://www.ietf.org/rfc/rfc2863.txt
IP-FORWARD-MIB	https://www.ietf.org/rfc/rfc4292.txt
IP-MIB (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.txt
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

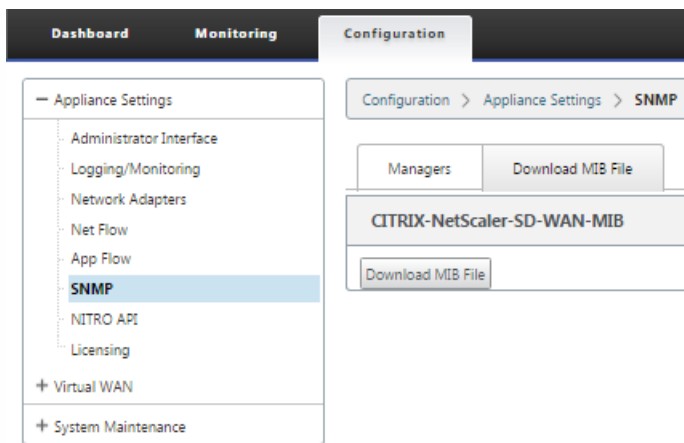
You must download the following SNMP files before you can start monitoring a NetScaler SD-WAN appliance:

- 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

The MIB files are used by SNMPv3 managers and SNMPv3 trap listeners. The files include the SD-WAN appliance enterprise MIBs, which provides SD-WAN-specific events. To download MIB files, in the SD-WAN web management interface:

1. Navigate to **Configuration > Appliance Settings > SNMP > Download MIB File** page.
2. Select the required **MIB** file.
3. Click **View**.

The MIB file opens in MIB browser.



Note

- Support for these MIBs is provided by default by the `net-snmp snmpd` daemon process on Linux systems. The MIBs provide the basis for supporting Network Management applications.
- The Ethernet port packet and byte counters are in the **IF-MIB** inside the **ifTable**. System information is in the system object.
- Ethernet ports are included in the **ifTable**, so walking that should be sufficient to ensure that the SNMP subsystem is running.
- Support for the **Q-BRIDGE-MIB** and the **IP-MIB** provides support for the network mapping application.

For additional information about adding SNMP manager, configuring SNMP View/Alarm, and adding SNMP server, see the CloudBridge 7.4 documentation at: <http://docs.citrix.com/content/dam/docs/en-us/cloudbridge/7-3/downloads/en.cloudbridge.cb-wrapper-73-con.pdf>

WAN Optimization

Mar 01, 2018

The NetScaler SD-WAN WANOP appliance optimizes WAN links, ensuring maximum responsiveness and throughput. The NetScaler SD-WAN WANOP appliances work in pairs, one at each end of a link, to accelerate traffic over the link. The following are some of the features of NetScaler SD-WAN WANOP:

- Compression
- TCP Protocol Acceleration
- Traffic Management
- Application Acceleration
- Citrix XenApp/SenDesktop (HDX) Acceleration
- Integration
- Monitoring and Management

For information about NetScaler SD-WAN WANOP 10.0 installation, deployment, and feature configuration, please refer to the [CloudBridge 7.4](#) documentation. The features and procedures for the NetScaler SD-WAN WANOP 10.0 are similar to the procedures documented in CloudBridge 7.4 release.

You can enable and configure WAN optimization feature on your NetScaler SD-WAN Enterprise Edition. For more information, see [NetScaler SD-WAN Enterprise Edition](#).

You can achieve network acceleration on any remote windows laptops or workstations using the WANOP Client Plug-in software. For more information, see [WANOP Client Plug-in](#).

NetScaler SD-WANOP Edition

Mar 01, 2018

For information about NetScaler SD-WAN WANOP 9.3 installation, deployment, and feature configuration, please refer to the [CloudBridge 7.4](#) documentation. The features and procedures for the NetScaler SD-WAN WANOP 9.3 are similar to the procedures documented in CloudBridge 7.4 release.

Important

Command Center End of Life Notification:

End of Life process for Citrix Command Center tool was initiated on 15-May-2017.

It is recommended that you migrate to the new management tool [NetScaler MAS](#) for your WAN Optimization deployments at the earliest

Please refer to the articles below for the Command Center EOL calendar and associated details.

- [CTX223806 - Notice of Status Change Announcement for Citrix Command Center Software Version 5.2](#)
- [CTX223786 - FAQ: Citrix Command Center - End Of Life](#)

Citrix Command Center tool for NetScaler SD-WAN WANOP edition is supported only till the NetScaler SD-WAN 9.2 appliance software release.

Starting with the NetScaler SD-WAN 9.3 software release, NetScaler MAS will be the management tool for SD-WAN WANOP edition appliances.

NetScaler SD-WAN WANOP Features

Features

[Compression](#)

[XenApp/XenDesktop Acceleration](#)

[HTTP Acceleration](#)

[TCP Flow-Control Acceleration](#)

[Traffic Shaping](#)

[Traffic Classification](#)

[Link Definitions](#)

[Secure Traffic Acceleration](#)

[How HTML5 Works](#)

[Video Caching](#)

[Monitoring with AppFlow](#)

[Internet Protocol Version 6 \(IPv6\) Acceleration](#)

[SCPS Support](#)

[Automatically Configuring CloudBridge Devices](#)

[CloudBridge Connector](#)

[WAN Insight](#)

[Office 365 Acceleration](#)

The topics that are organized under this topic are specific to NetScaler SD-WAN WANOP 9.3.

Configure SSL Compression

Mar 01, 2018

The Netscaler SD-WAN WO SSL compression feature enables multisection compression of SSL connections (for example, HTTPS traffic), providing a compression ratios of up to 10,000:1. For more information, see [SSL Compression](#).

For SSL compression to work, the SD-WAN WANOP appliance needs certificates from either the server or the client. To support multiple servers, multiple private keys can be installed on the appliance, one per SSL profile. Special SSL rules in the service class definitions match up servers to SSL profiles, and thus SSL profiles to private keys.

SSL compression works in split proxy or transparent proxy mode, you can choose the mode as per your requirement. For more information, see [How SSL Compression Works](#).

Note

Transparent proxy mode is currently not supported.

To enable secure access with SSL tunnel, the latest SSL protocol TLS 1.2 is used in SSL proxy. You can choose to use TLS1.2 protocol only or use TLS1.0, TLS1.1 and TLS1.2 protocols.

Note

SSL protocols SSL v3 and SSL v2 are no longer supported.

To configure SSL compression:

1. Acquire copies of your server's CA certificate and private certificate-key pair and install them on the server-side appliance. These credentials are likely to be application-specific. That is, a server might have different credentials for an Apache Web server than for an Exchange Server running RPC over HTTPS.
2. You can choose to create a split proxy SSL Profile or a Transparent proxy SSL profile.

For information on configuring split proxy SSL profile, see [Configuring a Split Proxy SSL Profile](#) section below.

For information on configuring transparent proxy SSL profile, see [Configuring Transparent Proxy SSL Profile](#) section below.

Note

Transparent proxy SSL profile is currently not supported.

3. Attach the SSL profile to a service class on the server-side appliance. This can be done by either creating a new service class based on the server IP, or by modifying an existing service class.

For more information see, **Creating or Modifying the Service Class** section below.

4. Set service classes on the client-side appliance. SSL traffic is not compressed unless it falls into a service class, on the client-side appliance, that enables acceleration and compression. This can be an ordinary service-class rule, not an SSL rule (only the server-side appliance needs SSL rules), but it must enable acceleration and compression. The traffic falls into an existing service class, such as “HTTPS” or “Other TCP Traffic.” If this class’s policy enables acceleration and compression, no additional configuration is needed.
5. Verify operation of the rule. Send traffic that should receive SSL acceleration through the appliances. On the server-side appliance, on the Monitoring: Optimization: Connections: Accelerated Connections tab, the Service Class column should match the service class you set up for secure acceleration, and the SSL Proxy column should list True for appropriate connections.

To configure a split proxy SSL profile:

1. In the server-side Netscaler SD-WAN WO appliance, navigate to **Configuration > Secure Acceleration > SSL Profile** and click **Add Profile**.

Note

You can either manually add an SSL profile or import one that is stored on your local computer.

2. In the **Profile Name** field, enter a name for the SSL profile and select **Profile Enabled**
3. If your SSL server uses more than one virtual host name, In the **Virtual Host Name** field, enter the target virtual host name. This is the host name listed in the server credentials.

Create SSL Profile

Manually add Profile Import Profile

Profile Name*
SSL-Server2

Profile Enabled
 Parse Subject Alternative Names

Virtual Host Name
Server2

Proxy Type
 Split Transparent

Enable Exclude List

Certificate Verification*
Signature/Expiration

Note

To support multiple virtual hosts, create a separate SSL profile for each host name.

4. Choose **Split** proxy type.

5. In the **Certificate Verification** field, retain the default value (Signature/Expiration) unless your policies dictate otherwise.
6. Perform server-side proxy configuration:
 1. In the **Verification Store** field, select an existing server Certificate Authority (CA), or click + to upload a server CA.
 2. Choose **Authentication Required** and in the **Certificate/Private Key** field select a certificate key pair, or click + to upload a certificate key pair.
 3. In the **Protocol Version** field, select the protocols your server accepts.

Note

NetScaler SD-WAN WO supports a combination of TLS1.0, TLS1.1 or TLS1.2, or TLS1.2 only. SSL protocols SSLv3 and SSLv2 are not supported.

4. If necessary, edit the **Cipher Specification** string, using the OpenSSL syntax.
5. If required, select the type of renegotiation from the **Renegotiation Type** drop-down list to allow client-side SSL session renegotiation.

The screenshot displays the 'Server-Side Proxy Configuration' window. It includes the following fields and options:

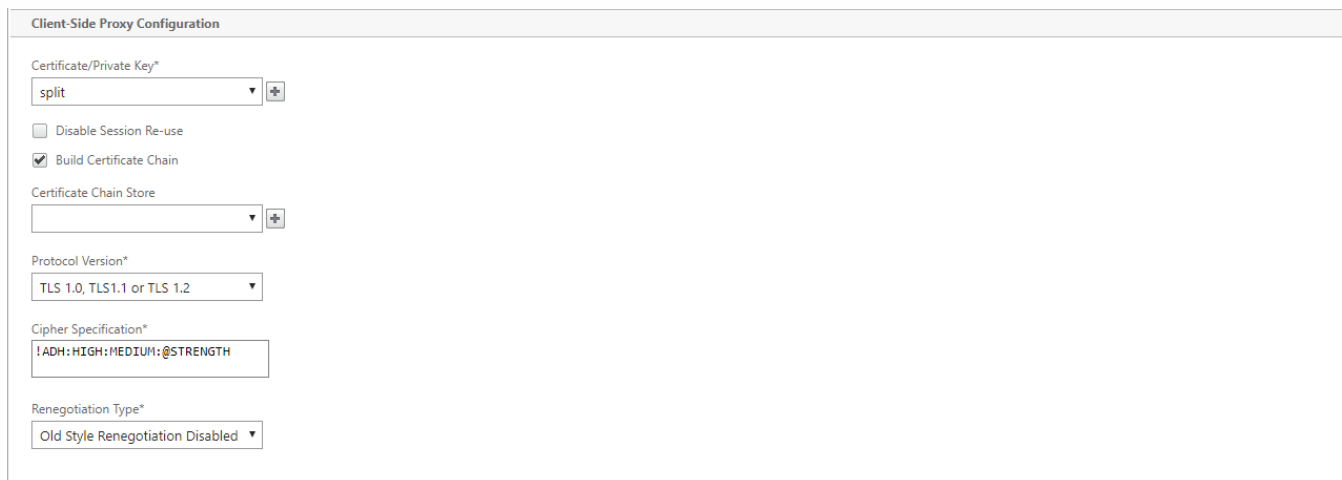
- Verification Store:** A dropdown menu with 'CA' selected and a '+' icon to the right.
- Authentication Required:** A checked checkbox.
- Certificate/Private Key*:** A dropdown menu with 'split' selected and a '+' icon to the right.
- Build Certificate Chain:** A checked checkbox.
- Protocol Version*:** A dropdown menu with 'TLS 1.0, TLS 1.1 or TLS 1.2' selected.
- Cipher Specification*:** A text input field containing 'ADH:HIGH:MEDIUM:@STRENGTH'.
- Renegotiation Type*:** A dropdown menu with 'Old Style Renegotiation Disabled' selected.

7. Perform client-side proxy configuration:
 1. In the **Certificate/Private Key** field, retain the default value.
 2. Choose **Build Certificate Chain** to allow the server-side appliance to build the SSL certificate chain.
 3. If required, select or upload a CA store to use as the Certificate Chain Store.
 4. In the **Protocol Version** field, select the protocol versions you want to support on the client side.

Note

NetScaler SD-WAN WO supports a combination of TLS1.0, TLS1.1 or TLS1.2, or TLS1.2 only. SSL protocols SSLv3 and SSLv2 are not supported.

5. If necessary, edit the client-side Cipher Specification.
6. If required, select the type of renegotiation from the **Renegotiation Type** drop-down list to allow client-side SSL session renegotiation.



The screenshot shows the 'Client-Side Proxy Configuration' form with the following fields and values:

- Certificate/Private Key***: split
- Disable Session Re-use
- Build Certificate Chain
- Certificate Chain Store**: (empty)
- Protocol Version***: TLS 1.0, TLS1.1 or TLS 1.2
- Cipher Specification***: JADH:HIGH:MEDIUM:@STRENGTH
- Renegotiation Type***: Old Style Renegotiation Disabled

8. Click **Create**.

To configure a transparent proxy SSL profile:

1. In the server-side Netscaler SD-WAN WO appliance, navigate to **Configuration > Secure Acceleration > SSL Profile** and click **Add Profile**.

Note

You can either manually add an SSL profile or import one that is stored on your local computer.

2. In the **Profile Name** field, enter a name for the SSL profile and select **Profile Enabled**.
3. If your SSL server uses more than one virtual host name, In the **Virtual Host Name** field, enter the target virtual host name. This is the host name listed in the server credentials.

Note

To support multiple virtual hosts, create a separate SSL profile for each host name.

4. Choose **Transparent** proxy type.
5. In the **SSL Server's Private Key** field, select the server's private key from the drop-down menu, or click + to upload a new private key.
6. Click **Create**.

To create or modify the service class and attach the SSL Profile:

1. In the Netscaler SD-WAN WO appliance web interface, navigate to **Configuration > Optimization Rules > Service Classes** and click **Add**. To edit an existing service class, select the appropriate service class and click **Edit**.
2. In the **Name** field, enter a name for the new service class (for example, "Accelerated HTTPS").
3. Enable compression by setting the Acceleration Policy to **Disk, Memory** or **Flow Control**.
4. In the **Filter Rules** section, click **Add**.
5. In the **Destination IP Address** field, type the server's IP address (for example, 172.16.0.1 or, equivalently, 172.16.0.1/32).
6. In the **Direction** field, set the rule to Unidirectional. SSL profiles are disabled if Bidirectional is specified.
7. In the **SSL Profiles** section, select the SSL profile that you created and move it to the **Configured** section.
8. Click **Create** to create the rule.
9. Click **Create** to create the service class.

NetScaler SD-WAN WO 9.3 supports the latest TLS1.2 SSL protocol. You can choose to use TLS1.2 protocol only or any version of TLS protocols. SSL protocols SSL v3 and SSL v2, and transparent proxy SSL profiles are not supported. The *add ssl-profile* and *set ssl-profile* CLI commands are updated to reflect these changes.

add ssl-profile

-name "profile-name"

[-state {enable, disable}]

-proxy-type split

[-virtual-hostname "hostname"]

-cert-key "cert-key-pair-name"

[-build-cert-chain {enable, disable}]

[-cert-chain-store {use-all-configured-CA-stores, "store-name"}]

*[-cert-verification {none, Signature/Expiration, Signature/Expiration/
Common-Name-White-List, Signature/Expiration/Common-Name-Black-List}]*

[-verification-store {use-all-configured-CA-stores, "store-name"}]

[-server-side-protocol { TLS-1.2, TLS-version-any}]

[-server-side-ciphers "ciphers"]

[-server-side-authentication {enable, disable}]

[-server-side-cert-key "cert-key-pair-name"]

[-server-side-build-cert-chain {enable, disable}]

*[-server-side-renegotiation {disable-old-style, enable-old-style, new-style,
compatible}]*

[-client-side-protocol-version { TLS-1.2, TLS-version-any}]

[-client-side-ciphers "ciphers"]

*[-client-side-renegotiation {disable-old-style, enable-old-style, new-style,
compatible}]*

set ssl-profile

-name "profile-name" [-state {enable, disable}]

[-proxy-type split]

[-virtual-hostname "hostname"]

[-cert-key "cert-key-pair-name"]

[-build-cert-chain {enable, disable}]

[-cert-chain-store {use-all-configured-CA-stores, "store-name"}]

*[-cert-verification {none, Signature/Expiration, Signature/Expiration/
Common-Name-White-List, Signature/Expiration/Common-Name-Black-List}]*

[-verification-store {use-all-configured-CA-stores, "store-name"}]

[-server-side-protocol {TLS-1.2, TLS-version-any}]

[-server-side-ciphers "ciphers"]

[-server-side-authentication {enable, disable}]

[-server-side-cert-key "cert-key-pair-name"]

[-server-side-build-cert-chain {enable, disable}]

[-server-side-renegotiation {disable-old-style, enable-old-style, new-style, compatible}]

[-client-side-protocol-version {TLS-1.2, TLS-version-any}]

[-client-side-ciphers "ciphers"]

[-client-side-renegotiation {disable-old-style, enable-old-style, new-style, compatible}]

The rest of the SSL Configuration commands remain unchanged. For more information see, [SSL Configuration](#).

XenServer 6.5 Upgrade

Mar 01, 2018

Important

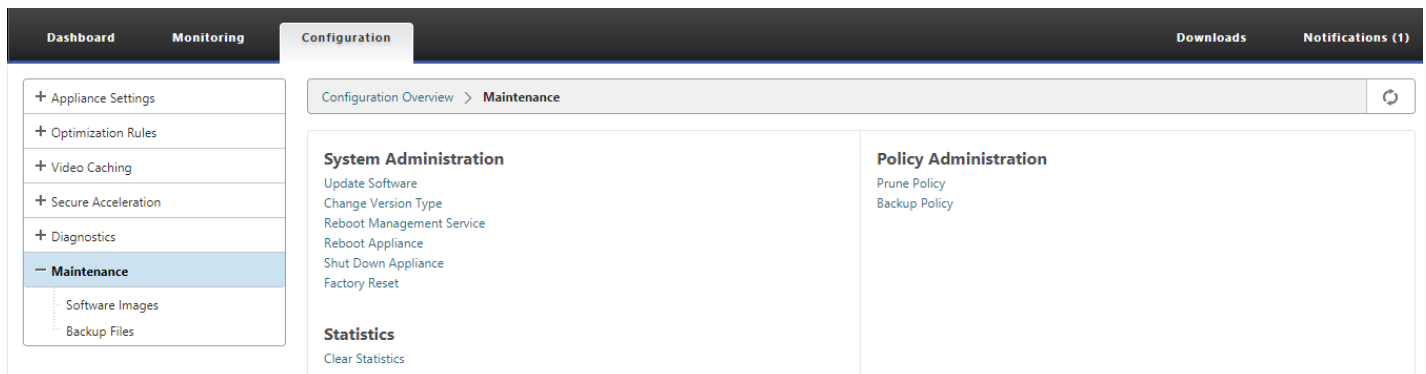
To upgrade to XenServer version 6.5, the appliances must be running NetScaler SD-WAN WANOP software release 9.0.x or later.

Note

Do not attempt upgrading when the appliance is running on software version lower than release 9.0.x to prevent upgrade issues.

To upgrade to XenServer 6.5 on SD-WAN WANOP appliances, ensure that the appliance is running software release version 9.0.x or later. If the appliances are running older software release version, upgrade to the latest software release version first.

1. In NetScaler SD-WAN WANOP GUI, go to **Configuration > Maintenance > Update Software**. Download the *ns-sdw-vw-<Build_No>.upg* file to upgrade the appliance.



2. After upgrading to the latest software version of WANOP software, navigate to **Configuration > Maintenance > Update Software** in the GUI. Upload *ns-sdw-xen65-pkg_v1.5.upg* file.

3. Wait for approximately 20 mins for the upgrade to complete. The appliance restarts after the upgrade is successfully completed.

NetScaler SD-WAN Enterprise Edition

Mar 01, 2018

The section provides step-by-step instructions for enabling and configuring SD-WAN Enterprise Edition WAN Optimization features for your Virtual WAN. To do this, you will use the **Optimization** section forms in the **Configuration Editor** in the Web Management Interface on the MCN.

Note

You must have a SD-WAN Enterprise Edition license installed to access, enable, configure, and activate WAN Optimization features in your Virtual WAN. SD-WAN Standard Edition does not support these features.

There are two top-level steps for configuring the **Optimization** section sets and parameters. These are as follows, listed in order of dependency:

1. Enable WAN Optimization and customize the **Defaults** configuration, or accept the defaults.

The **Defaults** configuration is used as the base **Optimization** configuration for all sites eligible for WAN Optimization. The **Defaults** configuration comes pre-configured, and can be customized.

Note

For instructions, see [Enabling Optimization and Configuring Default Settings](#).

2. (Optional) Customize the WAN Optimization configuration for each of the individual branch sites, or accept the **Defaults sets and settings for each**.

By default, the **Defaults** configuration is initially applied to each branch site that is eligible for WAN Optimization. WAN Optimization is supported for 1000-EE and 2000-EE hardware appliances, only. For each supported branch site, you can elect to accept or modify any combination of the **Defaults** sets and settings, or any subset of these. For instructions, see [Configuring Optimization for a Branch Site](#).

To complete these steps, you will use the configuration forms the **Optimization** section of the **Configuration Editor**. The **Optimization** section is organized as follows:

- **Defaults** – The **Defaults** branch contains the following child branches, which in turn contain one or more forms for configuring their respective sets and settings:

- * **Defaults Features**
- * **Defaults Tuning Settings**
- * **Defaults Application Classifiers (set)**
- * **Defaults Service Classes (set)**

- <Client Site Name> – The **Optimization** section configuration tree contains a branch for each client node (branch site) that supports WAN Optimization. If a client node is an unsupported appliance model, the site will not be included in the **Optimization** section configuration tree. Each branch in the tree contains the following child branches, which in turn contain one or more forms for configuring their respective sets and settings:

- * **Defaults Features**
- * **Defaults Tuning Settings**
- * **Defaults Application Classifiers (set)**
- * **Defaults Service Classes (set)**

The following section provides instructions for enabling WAN Optimization for your Virtual WAN, and configuring the **Defaults** sets and settings.

Enabling Optimization and Configuring the Default Feature Settings

Mar 01, 2018

Enabling WAN Optimization in your Virtual WAN entails the following procedures:

1. Enable WAN Optimization in the **Features** settings of the **Optimization** section.

Instructions for this part of the process are provided in this section.

2. Configure the **Acceleration** policy setting for each applicable Service Class in the **Service Classes** table.

This procedure occurs further on, after you have completed the rest of the **Optimization** configuration. Instructions are provided in the section, [Configuring Optimization Default Service Classes](#). At this point, WAN Optimization has been enabled in your configuration, but not yet enabled and activated in your Virtual WAN. To enable and activate WAN Optimization in your Virtual WAN, you must complete the Virtual WAN configuration, and then generate, stage, and activate the Virtual WAN Appliance Packages on the eligible sites in your deployment, as outlined in the subsequent chapters of this guide.

To enable WAN Optimization and configure the **Defaults** section **Features** settings, do the following:

1. If necessary, log back into the Management Web Interface, and open the **Configuration Editor**.

To open the **Configuration Editor**, do the following:

- a. Select the **Configuration** tab at the top of the page to open the **Configuration** navigation tree (left pane).
 - b. In the navigation tree, click + to the left of the **Virtual WAN** branch to open that branch.
 - c. In the **Virtual WAN** branch, select **Configuration Editor**.
2. Open the configuration package you want to modify.

Click **Open** to display the **Open Configuration Package** dialog box, and select the package from the **Saved Packages** drop-down menu.

This loads the selected package into the **Configuration Editor** and opens it for editing.

If you have a valid and current license that includes WAN Optimization features, the **Optimization** section will be available in the **Configuration Editor**.

Note

If the **Optimization** section is not available, please check that you have installed a SD-WAN Enterprise Edition license in your Virtual WAN. SD-WAN Standard Edition does not support WAN Optimization features.

For details and instructions, see the following sections:

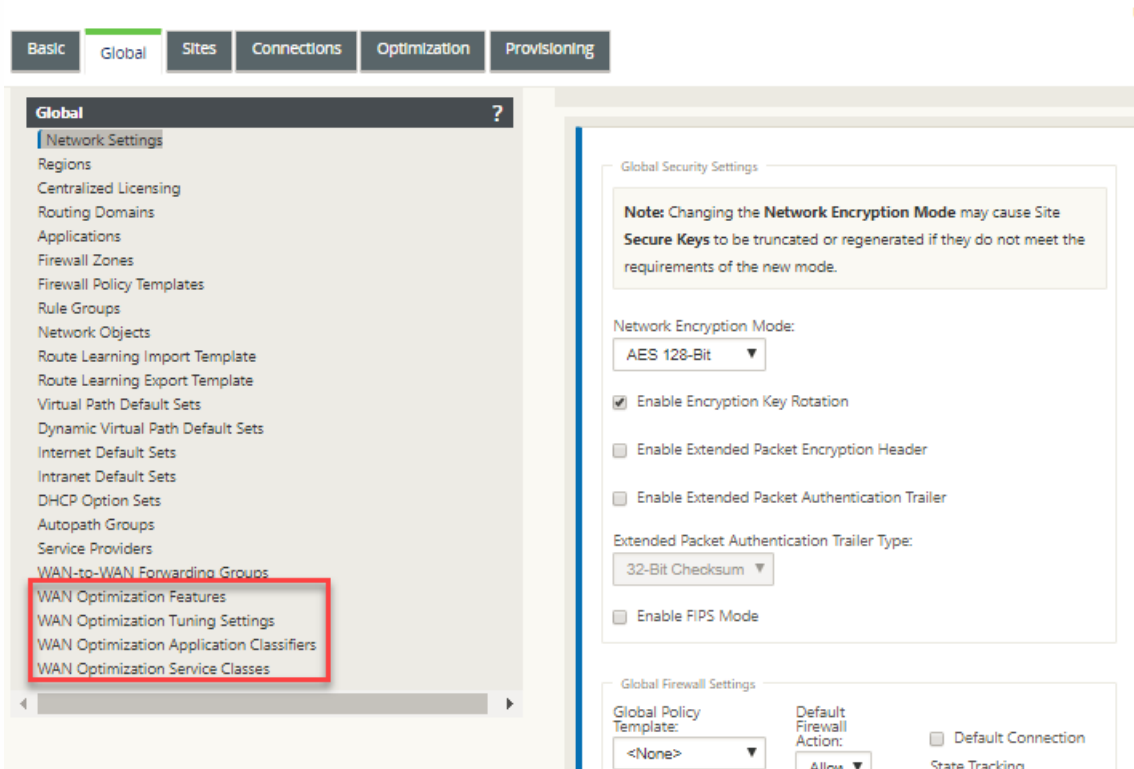
- [The SD-WAN Editions](#)

- [Licensing](#)

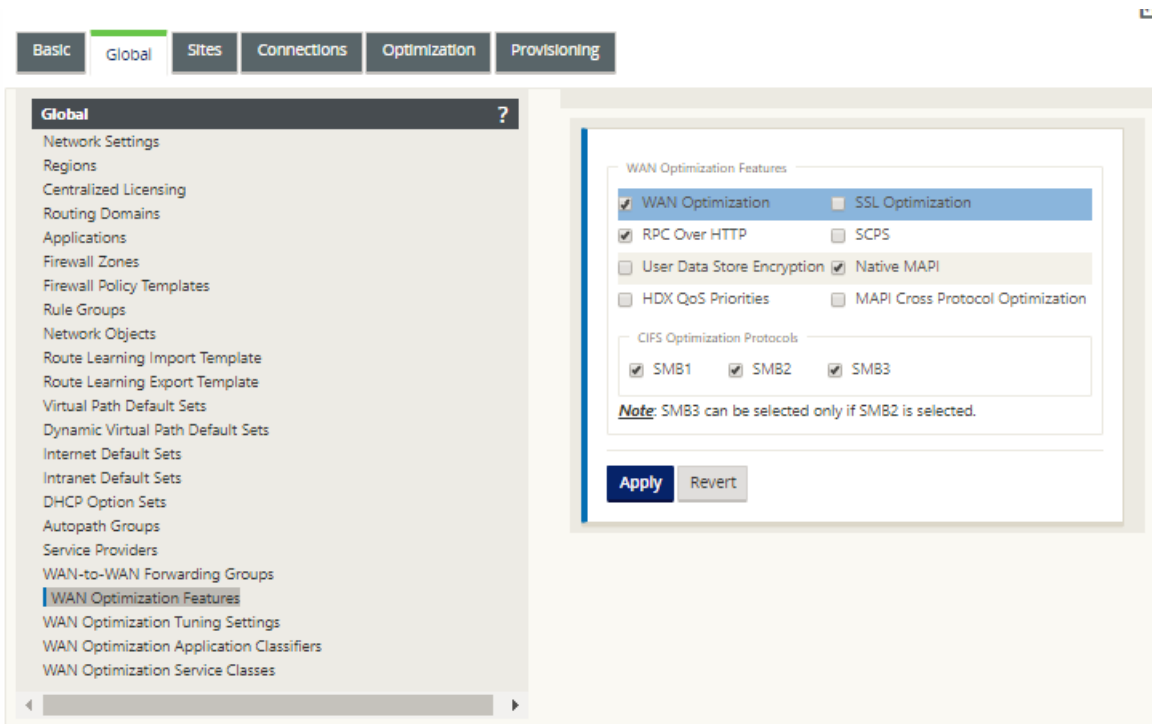
3. Click the **Global** tab.

You can configure the following default settings for WAN optimization from the **Global** tab.

- WAN Optimization Features
- WAN Optimization Tuning Settings
- WAN Optimization Application Classifiers
- WAN Optimization Service Class



4. Click **WAN Optimization Features**.



5. Select the **WAN Optimization** checkbox.

The **WAN Optimization** checkbox is in the upper left corner of the **WAN Optimization Features** section. This enables the form for editing, and reveals the **Apply** and **Revert** buttons.

Note

This selects this feature for enabling, only. WAN Optimization will not be enabled in the **Optimization** section or the configuration package until you click **Apply**, after completing the **Features** configuration. In addition, you must also configure the **Acceleration** setting for each applicable Service Class in the Service Classes table, as instructed further on in the **Optimization** configuration process. (Instructions are provided in the section [Configuring Optimization Default Service Classes](#)) Finally, WAN Optimization will not be enabled and activated in your Virtual WAN until you have completed the entire Virtual WAN configuration, and then generated, staged, distributed, and activated the Virtual WAN Appliance Packages on the eligible sites in your Virtual WAN.

6. Configure the **Features** settings.

Click a checkbox to select or deselect an option. You can accept the default settings pre-selected in the form, or customize the settings.

Note

By default, the settings you configure in the **Global** tab are automatically applied to each branch site included in the tree. However, you can customize the **Optimization** configuration for a specific branch, as outlined in the section, [Configuring Optimization for a Branch Site](#).

The **Features** configuration form contains two sections:

- **WAN Optimization Features**
- **CIFS Optimization Protocols**

The **WAN Optimization Features** settings are as follows:

- **WAN Optimization** – Select this to enable WAN Optimization for this configuration. This also enables compression, deduplication, and TCP Protocol Optimization.

Note

The WAN Optimization option must be selected for the other Optimization section options to be available.

- **SCPS** – Select this to enable TCP Protocol optimization for Satellite Links.
- **HDX QoS Priorities** – Select this to enable optimization of ICA traffic based on prioritization of HDX sub-channels.
- **MAPI Cross Protocol Optimization** – Select this to enable cross-protocol optimization of Microsoft Outlook (MAPI) traffic.
- **SSL Optimization** – Select this to enable optimization for traffic streams with SSL encryption.
- **RPC Over HTTP** – Select this to enable optimization of Microsoft Exchange traffic that uses RPC over HTTP.
- **User Data Store Encryption** – Select this to enable enhanced security of data through the encryption of WAN Optimization compression history.
- **Native MAPI** – Select this to enable optimization of Microsoft Exchange traffic.

The **CIFS Optimization Protocols** options are as follows:

- **SMB1** – Select this to enable Optimization of Windows File Sharing (SMB1)
- **SMB2** – Select this to enable Optimization of Windows File Sharing (SMB2)
- **SMB3** – Select this to enable Optimization of Windows File Sharing (SMB3). You must first select the **SMB2** option before you can select **SMB3**.

7. Click **Apply**.

This enables and adds the selected **Default Features** to the configuration package.

The next step is to configure the **Optimization default Tuning Settings**.

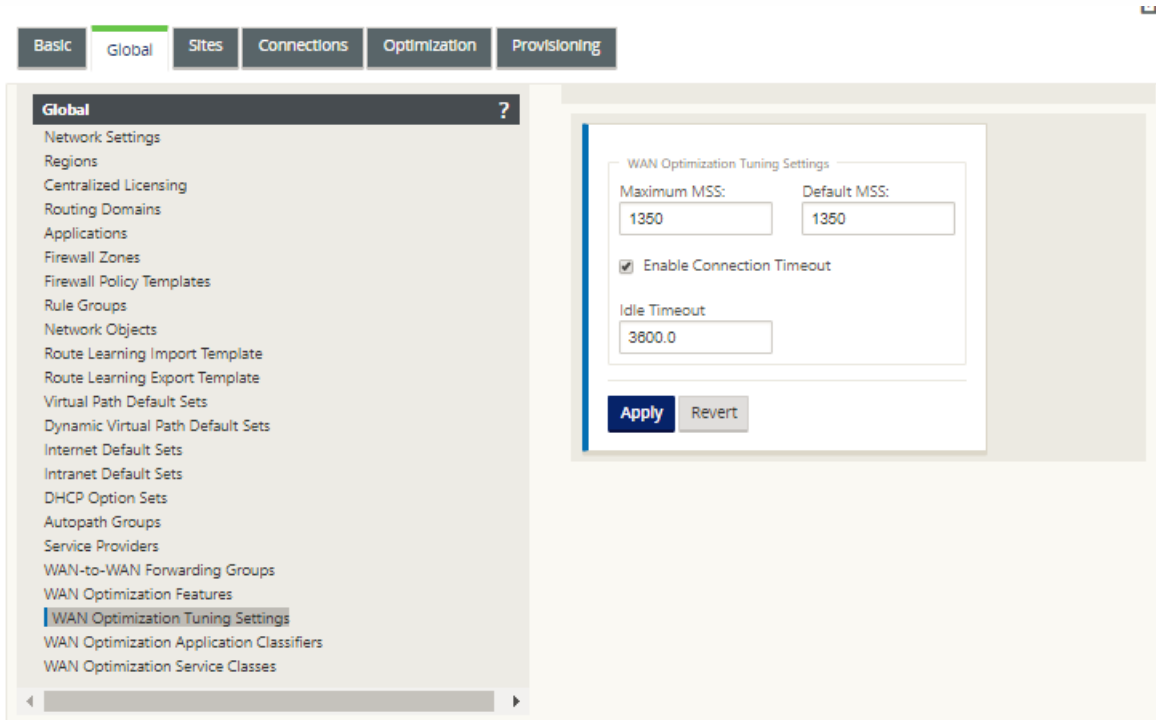
Configuring Optimization Default Tuning Settings

Mar 01, 2018

You can configure the WAN optimization default tuning settings in the **Global** tab.

To configure the WAN Optimization default **Tuning Settings**, do the following:

1. In the **Global** tab, click **WAN Optimization Tuning Settings** .



2. Select and configure the **Tuning Settings**.

The **Tuning Settings** options are as follows:

- **Maximum MSS** – Enter the maximum size (in bytes) for the Maximum Segment Size (MSS) for a TCP segment.
- **Default MSS** – Enter the default size (in octets) for the MSS for TCP segments.
- **Enable Connection Timeout** – Select this to enable automatic termination of a connection when the idle threshold is exceeded.
- **Idle Timeout** – Enter a threshold value (in seconds) to specify the amount of idle time permitted before an idle connection is terminated. You must first select **Enable Connection Timeout** before this field can be configured.

3. Click **Apply**.

This applies the modified **Tuning Settings** to the global configuration.

The next step is to configure the default set of WAN Optimization Application Classifiers.

Configuring Optimization Default Application Classifiers

Mar 01, 2018

You can configure the WAN optimization default application classifier settings in the **Global** tab.

To configure the default set of WAN Optimization Application Classifiers, do the following:

1. In the **Global** tab, click **WAN Optimization Application Classifiers**.

This opens the **Application Classifiers** table, displaying the default set of Application Classifiers.

The screenshot shows the 'Global' tab in a management console. The left sidebar contains a navigation menu with 'WAN Optimization Application Classifiers' selected. The main area displays a table of application classifiers. The table has columns for Name, Application Group, Classification Parameters, Edit, and Delete. The table contains 14 entries, each with a unique name, application group, and classification parameters.

Name	Application Group	Classification Parameters	Edit	Delete
ACTNET	legacy or non-ip	TCP Port: 5411		
AFS	file server	TCP Port: 1483, 7004		
ALC	host access	TCP Port: 47806		
ALTHHTTP	web	TCP Port: 8008		
AOL IM File	messaging	TCP Port: 2516-2518		
ASP.NET Session State	session	TCP Port: 42424		
AURP	routing protocols	TCP Port: 387		
America OnLine (TCP)	messaging	TCP Port: 5191-5193		
AppleTalk	legacy or non-ip	TCP Port: 548		
AppleTalk Filing Protocol	legacy or non-ip	TCP Port: 2794		
Ariel	content delivery	TCP Port: 419, 422		
Avamar	backup and replication	TCP Port: 27000		

This table is also a configuration form. You can use this form to configure (edit), delete, and add Application Classifiers to create a customized default set. The modified default **Application Classifiers** set and individual Application Classifier settings you configure are automatically applied as the defaults to any branch site included in the **Optimization** section tree.

Note

You can also customize the **Application Classifiers** set and settings for each specific branch site. For instructions, see the section [Configuring Optimization for a Branch Site](#).

2. To configure an existing Application Classifier, click Edit (pencil icon), in the **Edit** column of that classifier entry.

This opens a pop-up **Edit** settings form for configuring the selected Application Classifier.

3. In the **Port** field, enter the port number for the Application Classifier, or accept the default.

4. Add or remove Application Groups in the **Configured** list, or accept the defaults.

- **To add an Application Group to the list:** Select it in the **Application Groups** list on the left, and then click the Add right-arrow (>) to add the group to the **Configured** list on the right. To add all of the **Application Groups** to the list at once, click the Add All double right-arrow (>>).

- **To remove an Application Group from the list:** Select it in the **Configured** list on the right, and then click the Remove left-arrow (<). To remove all of the **Application Groups** from the list at once, click the Remove All double left-arrow (<<).

5. Click **Apply**.

This applies your changes to the Application Classifier, and dismisses the **Edit** configuration form.

6. (Optional) Customize the default **Application Classifiers** set.

You can add or delete Application Classifiers to customize the default set, as follows:

- **To remove an Application Classifier from the set:**

Click the trashcan icon in the **Delete** column of an **Application Classifier** entry to remove that entry from the table.

- **To add an Application Classifier to the set:**

- a. Click + to the right of the **Application Classifier** branch label.

This displays the **Add** configuration form.

- b. Enter the name and port number for the Application Classifier in the **Name** and **Port** fields, respectively.

- c. Add or remove Application Groups in the **Configured** list.

To add an Application Group to the list: Select it in the **Application Groups** list on the left, and then click the Add right-arrow (>) to add the group to the **Configured** list on the right. To add all of the **Application Groups** to the

list at once, click the Add All double right-arrow (>>).

To remove an Application Group from the list: Select it in the **Configured** list on the right, and then click the Remove left-arrow (<). To remove all of the **Application Groups** from the list at once, click the Remove All double left-arrow (<<).

d. Click **Apply**.

This adds the new Application Classifier to the set, and dismisses the **Add** configuration form.

The next step is to configure the default set of WAN Optimization Service Classes.

Configuring Optimization Default Service Classes

Mar 01, 2018

You can configure the WAN optimization default service class settings in the **Global** tab.

To configure the default set of WAN Optimization Service Classes, do the following:

1. In the **Global** tab, click **WAN Optimization Service Classes**.

This opens the **Service Classes** table, displaying the default set of Service Classes.

Order	Name	Status	Acceleration	Edit	Delete
100	ICA	ENABLED	none		
200	Web (Private)	ENABLED	none		
300	Web (Private-Secure)	ENABLED	none		
400	Web (Internet)	ENABLED	none		
500	Web (Internet-Secure)	ENABLED	none		
600	CIFS	ENABLED	none		
700	NFS	ENABLED	none		
800	Microsoft Exchange (MAPI)	ENABLED	none		
900	Mail (Other)	ENABLED	none		
1000	VOIP and Multimedia	ENABLED	none		
1100	FTP Data	ENABLED	none		
1200	FTP Control	ENABLED	none		
1300	Instant Messaging	ENABLED	none		
1400	Session Applications	ENABLED	none		
1500	Directory and Security	ENABLED	none		
1600	Database Applications	ENABLED	none		

This table is also a configuration form. You can use this form to configure (edit), delete, and add Service Classes to create a customized default set. The modified default **Service Classes** set and individual Service Class settings you configure are automatically applied as the defaults to any branch site included in the **Optimization** section tree.

Note

You can also customize the **Service Classes** set and settings for each specific branch site. For instructions on customizing the **Optimization** configuration for a branch site, see the section, [Configuring Optimization for a Branch Site](#).

2. To configure an existing Service Class, click Edit (pencil icon), in the **Edit** column of that class entry in the Service Classes table.

This opens a pop-up **Edit** settings form for configuring the selected Service Class.

Edit

Name: Order: Enabled

Acceleration Policy:

Enable AppFlow Reporting Exclude from SSL Tunnel

Filter Rules +

Application	Source IP Address	Destination IP Address	Direction	Edit	Delete
ICA, ICA CGP			BIDIRECTIONAL		

3. Configure the basic settings for the Service Class.

The basic settings are as follows:

- **Enabled** – Select this to enable the new Service Class. The class is enabled by default.
- **Acceleration Policy** – Select a policy from the **Acceleration Policy** drop-down menu. The options are:

- * **disk** – Select this policy to specify the appliance disk as the location for storing the traffic history used for compression. This enables Disk Based Compression (DBC) policy for this Service Class. Generally speaking, a policy of **disk** is usually the best choice, as the appliance automatically selects **disk** or **memory** as the storage location, depending on which is more appropriate for the traffic.

- * **none** – Select this if you do not want to enable an Acceleration Policy for this Service Class. A policy of **none** is generally used only for uncompressible encrypted traffic and real-time video.

- * **flow control only** – Select this policy to disable compression but enable flow-control acceleration. Select this for services that are always encrypted, and for the FTP control channel.

- * **memory** – Select this policy to specify memory as the location for storing the traffic history used for compression.

- **Enable AppFlow Reporting** – Select this to enable AppFlow reporting for this Service Class. AppFlow is an industry standard for unlocking application transactional data processed by the network infrastructure. The WAN Optimization AppFlow interface works with any AppFlow collector to generate reports. The collector receives detailed information from the appliance, using the AppFlow open standard (<http://www.appflow.org>).

For more information on AppFlow, please see the Citrix CloudBridge 7.4 Product documentation available on the citrix documentation portal <http://docs.citrix.com/>.

Note

To view WAN Optimization AppFlow reports, select the **Monitoring** tab, and then in the navigation tree (left pane), open the **WAN Optimization** branch, and select **AppFlow**. See also, [Monitoring Virtual WAN](#).

- **Exclude from the SSL Tunnel** – Select this to exclude traffic associated with the Service Class from SSL Tunneling.

4. Configure the **Filter Rules** for the Service Class.

To edit an existing rule, do the following:

- a. In the Filter Rules table (bottom of form), click Edit (pencil icon) in the Edit column of the rule you want to edit.

This reveals the Filter Rules settings for the selected Filter Rule.

The screenshot shows the 'Edit' dialog for a filter rule named 'ICA'. The 'Filter Rules' section is highlighted with a red box. It includes a 'Direction' dropdown menu set to 'BIDIRECTIONAL'. Below this are two lists: 'Available' and 'Configured'. The 'Available' list contains 'ACTNET', 'AFS', 'ALC', 'ALTHHTTP', and 'AOL IM File'. The 'Configured' list contains 'ICA' and 'ICA CGP'. Between the lists are navigation buttons: '>>', '>', '<', '<<', and a button with a slash icon. Below the lists are 'Source IP Address' and 'Destination IP Address' fields. At the bottom right are 'Apply' and 'Cancel' buttons.

- b. Select the filter direction from the Direction drop-down menu.

Select one of the following options:

- * **BIDIRECTIONAL**
- * **UNIDIRECTIONAL**

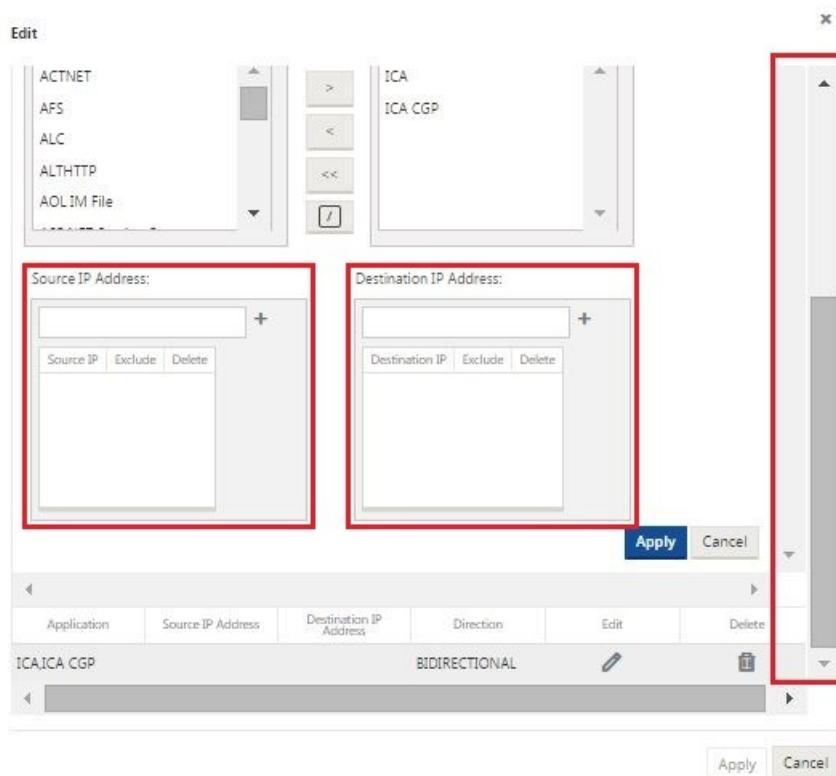
- c. Add or remove Applications in the **Configured** list.

To add an Application to the list: Select it in the **Applications** list on the left, and then click the Add right-arrow (>) to add the group to the **Configured** list on the right. To add all of the **Applications** to the list at once, click the Add All double right-arrow (>>).

To remove an Application from the list: Select it in the Configured list on the right, and then click the Remove left-arrow (<). To remove all of the **Applications** from the list at once, click the Remove All double left-arrow (<<).

- d. Scroll down to reveal the truncated portion of the form.

The **Filter Rules** settings section is somewhat long, so you will need to use the scroll bars to reveal the truncated portion of the form.



e. Enter the Source IP Address in the **Source IP Address** field.

f. Click + to the right of the Source IP Address you just entered.

This adds the specified IP Address to the **Source IP Address** table.



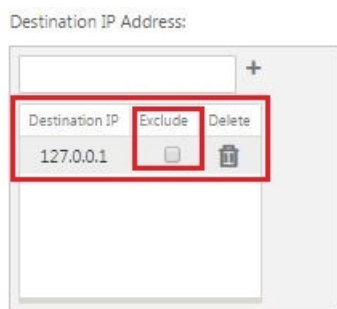
g. Specify whether to include or exclude the Source IP Address for this Filter Rule.

Select the **Exclude** checkbox to exclude the specified Source IP Address from this Filter Rule. Deselect the checkbox to include the address.

h. Enter the Destination IP Address in the **Destination IP Address** field.

i. Click + to the right of the Destination IP Address you just entered.

This adds the specified IP Address to the **Source IP Address** table.



j. Specify whether to include or exclude the Destination IP Address for this Filter Rule.

Select the **Exclude** checkbox to exclude the specified Destination IP Address from this Filter Rule. Deselect the checkbox to include the address.

k. Click **Apply**.

This applies your modifications to the rule and hides the **Filter Rules** settings section.

5. (Optional) Customize the default **Service Classes** set.

You can add or delete Service Classes to customize the default set, as follows:

- **To remove an Service Class from the set:**

Click the trashcan icon in the **Delete** column of a Service Class entry in the table to remove that entry.

- **To add an Service Class to the set:**

a. Click **+** to the right of the **Service Class** branch label.

This displays the **Add** configuration form.

b. Enter the name for the new Service Class in the **Name field**.

c. Configure the new Service Class.

The steps for configuring a new Service Class are the same as for modifying an existing Service Class. For instructions, see the following steps, earlier in this section:

"3. Configure the basic settings for the Service Class."

"4. Configure the Filter Rules for the Service Class."

d. Click **Add** to add the new Service Class to the default set and dismiss the **Add** configuration form.

6. (Optional, recommended) **Save** the configuration package.

You have now completed the global WAN optimization configuration, and can begin configuring the **Optimization** sets and settings for the branch sites.

Configuring Optimization for a Branch Site

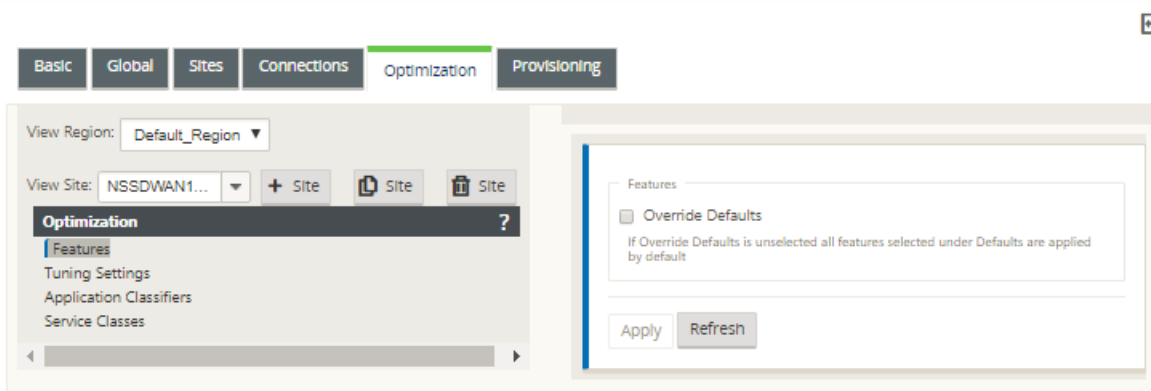
Mar 01, 2018

After you have completed the default global configuration, you have the option of customizing the sets and settings for each of the branch sites.

The global settings you just configured are automatically applied to each branch site included in the **Optimization** section. You can elect to accept the defaults, or customize the configuration for any given branch. The procedures for configuring the **Optimization** sets and settings for a branch site are the same as for configuring the global defaults, with a few minor differences.

To customize the **Optimization** configuration for a branch site, do the following:

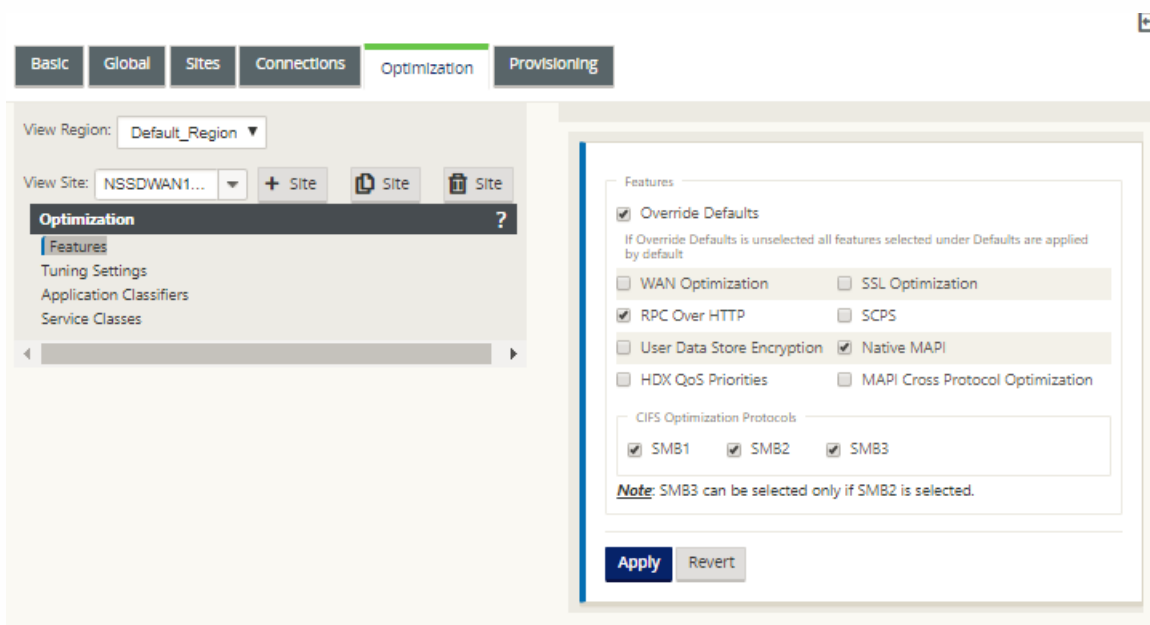
1. Click **Optimization** tab, in the View Site field, select a site.



2. Select the **Override Defaults** checkbox.

This reveals the top-level configuration form for that configuration category, and opens it for editing.

The below image shows an example top-level settings configuration form, in this case for the **Features** set.



3. Enter your configuration changes.

From this point on, the configuration process for each branch site **Optimization** category is the same as for the corresponding global section category. For instructions on configuring a particular category of sets or settings, see the appropriate section listed below:

- [Enabling Optimization and Configuring the Defaults Features Settings.](#)
- [Configuring Optimization Default Tuning Settings.](#)
- [Configuring Optimization Default Application Classifiers.](#)
- [Configuring Optimization Default Service Classes.](#)

7. (Optional, recommended) **Save** the configuration package.

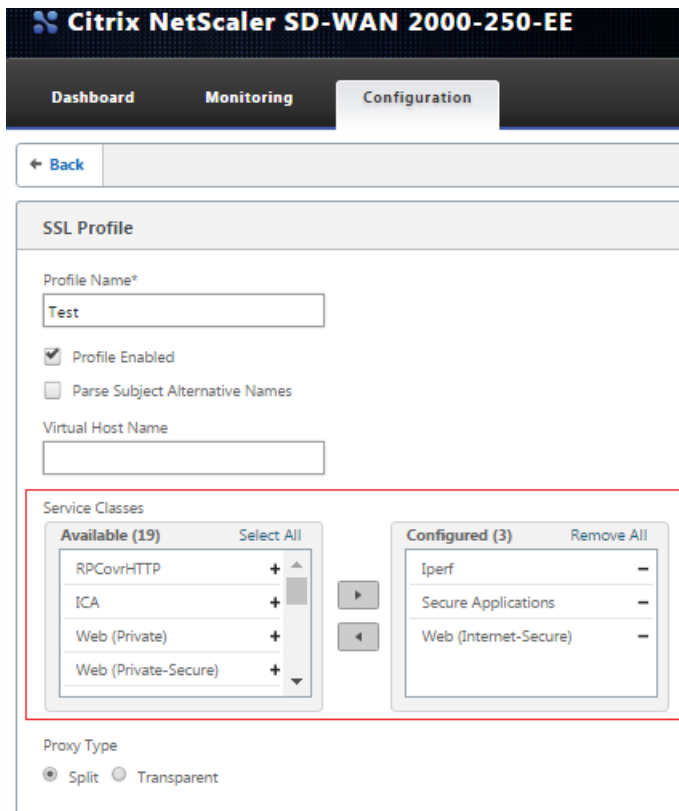
You have now completed configuring the **Optimization** section sets and settings for your Virtual WAN.

Configure SSL Profiles

Mar 01, 2018

All SSL related configuration is available through the new configuration editor of the appliance for security and usability. On the SD-WAN Enterprise Edition and two-box deployments, service classes are configured from the configuration editor and hence you cannot attach any SSL profiles. To accommodate the expression of SSL profile mapping to a service class, the work flow for SSL profiles is changed to allow for attaching Service classes in the profile node.

One of the limitations is that the SSL profile will get attached to all rules in a service class. If you need to attach the SSL profile selectively to a particular rule, the service class configuration is split into detailed rules for further selection.



To create SSL profile on new Enterprise Edition appliance at the data center:

1. In the SD-WAN web GUI, go to the **Configuration > Secure Acceleration** page. Click **Add Profile**. Create the **SSL Profile**.

- + Appliance Settings
- + Virtual WAN
- WAN Optimization
 - Secure Acceleration**
 - Certificate and Keys
 - User Data Store
- + System Maintenance

Configuration > WAN Optimization > Secure Acceleration

Secure Peering

Keystore Status Opened	Secure Peering Status Disabled
----------------------------------	--

SSL Profile

Windows Domain

SSL Profiles

SSL acceleration allows the appliance to compress SSL traffic such as HTTPS and SSL-encrypted XenApp/XenDesktop (ICA/CGP) traffic. Secure partner configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server-side NetScaler SD-WAN WO appliance (only) and SSL-specific configuration (called an SSL Profile) for each group of SSL servers. This step should be skipped on a client-side appliance.

[Add Profile](#)

[← Back](#)

Create SSL Profile

Manually add Profile
 Import Profile

Profile Name*

Profile Enabled
 Parse Subject Alternative Names

Virtual Host Name

Service Classes

<p>Available (21) Select All</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px 5px;">ICA</td><td style="text-align: right; padding: 2px 5px;">+</td></tr> <tr><td style="padding: 2px 5px;">Web (Private)</td><td style="text-align: right; padding: 2px 5px;">+</td></tr> <tr><td style="padding: 2px 5px;">Web (Private-Secure)</td><td style="text-align: right; padding: 2px 5px;">+</td></tr> <tr><td style="padding: 2px 5px;">Web (Internet)</td><td style="text-align: right; padding: 2px 5px;">+</td></tr> </table>	ICA	+	Web (Private)	+	Web (Private-Secure)	+	Web (Internet)	+	<div style="display: flex; flex-direction: column; align-items: center; gap: 5px;"> <div style="border: 1px solid #ccc; width: 20px; height: 20px; border-radius: 50%;"></div> <div style="border: 1px solid #ccc; width: 20px; height: 20px; border-radius: 50%;"></div> </div>	<p>Configured (0) Remove All</p> <p style="text-align: center; color: #666;">No items</p>
ICA	+									
Web (Private)	+									
Web (Private-Secure)	+									
Web (Internet)	+									

Proxy Type

Split Transparent

SSL Server's Private Key* [+](#)

2. In the **Create SSL Profile** page, provide a profile name and select **Service Classes** that will be associated to this profile. Choose **Proxy Type** and provide relevant data and click **Create**.

Create SSL Profile

Manually add Profile Import Profile

Profile Name*

SampleProfile

Profile Enabled

Parse Subject Alternative Names

Virtual Host Name

Service Classes

Available (20)	Select All		Configured (1)	Remove All
Web (Private)	+	▶	Web (Internet)	-
ICA	+	◀		
Web (Private-Secure)	+			
Web (Internet-Secure)	+			

Proxy Type

Split Transparent

SSL Server's Private Key*

private_10_105_199_6

Create

Close

3. After SSL Profile is created successfully and service class is associated, view the SSL profile information as shown below.

Profile Name	Proxy Type	Profile In Use	Profile Enabled
SampleProfile	transparent	✓	✓

WAN Optimization Client Plug-in

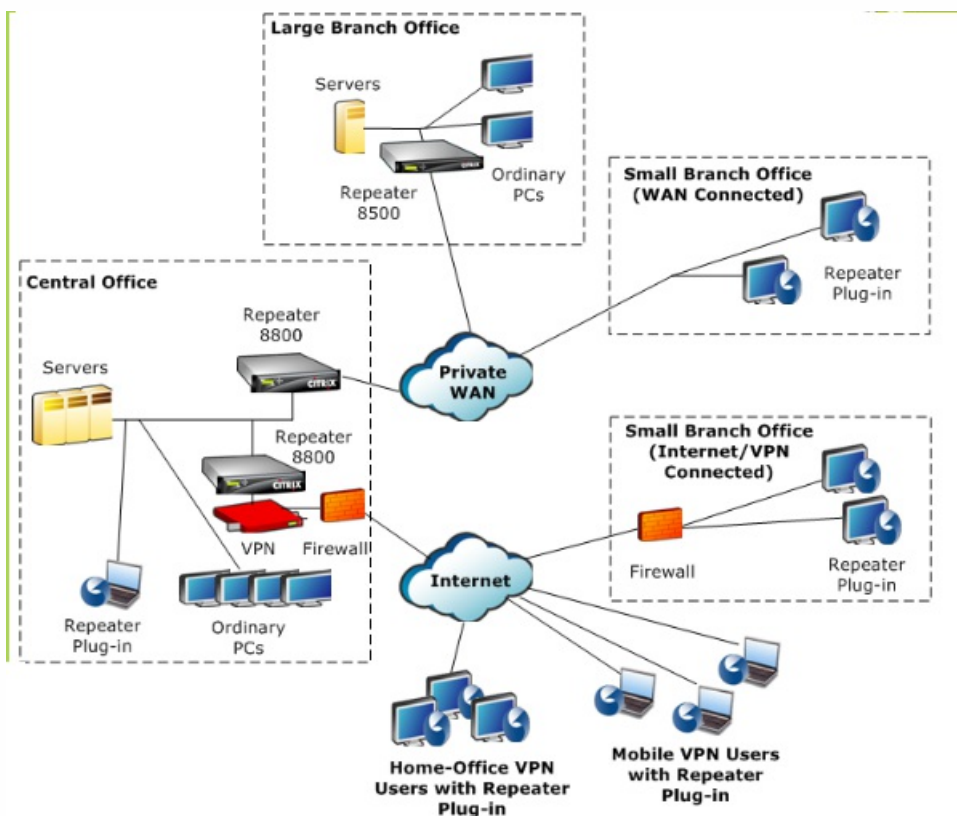
Mar 01, 2018

The WANOP Client Plug-in is a software based network accelerator that runs on Windows laptops and workstations, providing acceleration anywhere, not just at offices with WANOP Client Plug-in appliances. It connects to a Citrix WANOP Client Plug-in appliance at the other end of the link.

The principles of WANOP Client Plug-in operation are generally the same as those of a WANOP Client Plug-in appliance. For topics not included in the plug-in documentation, see the larger documentation set.

The plug-in is distributed as a standard Microsoft installation file (MSI). Plug-in deployment requires some plug-in specific configuration of the WANOP Client Plug-in appliances at the other ends of the links. If you customize the MSI file with the DNS or IP addresses of the WANOP Client Plug-in appliances, and a few other parameters, your users do not have to enter any configuration information when installing the plug-in on their Windows computers.

Figure 1. Typical WANOP Client Plug-in Network Showing the WANOP Client Plug-in



Note

The plug-in is supported by Citrix Receiver 1.2 or later, and can be distributed and managed by Citrix Receiver.

Hardware and Software Requirements

Mar 01, 2018

On the client side of the accelerated link, the WANOP Client Plug-in is supported on Windows desktop and laptop systems, but not on netbooks or thin clients. Citrix recommends the following minimum hardware specifications for the computer running the WANOP Client Plug-in:

- Pentium 4-class CPU
- 2 GB of RAM
- 2 GB of free disk space

WANOP Client Plug-in is supported on Windows 10 platform and needs following system requirements:

- 4GB RAM
- 10GB free disk space

The WANOP Client Plug-in is supported on the following operating systems:

- Windows XP Home
- Windows XP Professional
- Windows Vista (all 32-bit versions of Home Basic, Home Premium, Business, Enterprise, and Ultimate)
- Windows 7 (all 32-bit and 64-bit versions of Home Basic, Home Premium, Professional, Enterprise, and Ultimate)
- Windows 8 (32-bit and 64-bit versions of Enterprise Edition)
- Windows 10 (32-bit and 64-bit versions of Enterprise Edition)

On the server side, the following appliances currently support WANOP Client Plug-in deployments:

- Repeater 8500 Series
- Repeater 8800 Series
- WANOP Client Plug-in VPX
- WANOP Client Plug-in 2000
- WANOP Client Plug-in 3000
- WANOP Client Plug-in 4000
- WANOP Client Plug-in 5000

How the WANOP Plug-in Works

Mar 01, 2018

WANOP Client Plug-in products use your existing WAN/VPN infrastructure. A computer on which the plug-in is installed continues to access the LAN, WAN, and Internet as it did before installation of the plug-in. No changes are required to your routing tables, network settings, client applications, or server applications.

Citrix Access Gateway VPNs require a small amount of WANOP Client Plug-in-specific configuration.

There are two variations on the way connections are handled by the plug-in and appliance: *transparent mode* and *redirector mode*. Redirector is a legacy mode that is not recommended for new deployments.

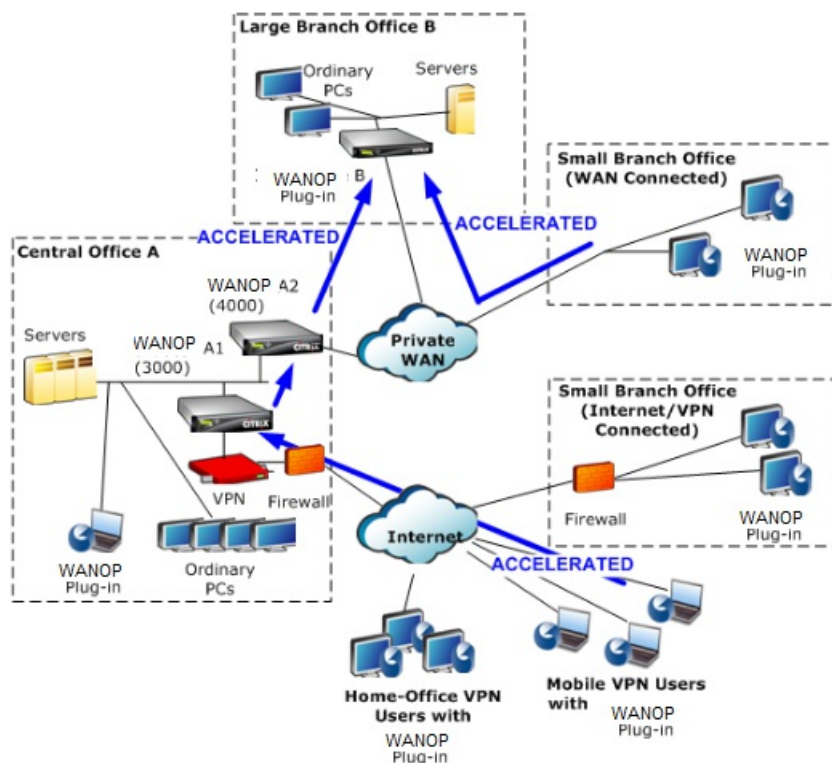
- **Transparent mode** for plug-in-to-appliance acceleration is very similar to appliance-to-appliance acceleration. The WANOP Client Plug-in appliance must be in the path taken by the packets when traveling between the plug-in and the server. As with appliance-to-appliance acceleration, transparent mode operates as a transparent proxy, preserving the source and destination IP address and port numbers from one end of the connection to the other.
- **Redirector mode** (not recommended) uses an explicit proxy. The plug-in readdresses outgoing packets to the appliance's redirector IP address. The appliance in turn readdresses the packets to the server, while changing the return address to point to itself instead of the plug-in. In this mode, the appliance does not have to be physically inline with the path between the WAN interface and the server (though this is the ideal deployment).

Best Practice: Use transparent mode when you can, and redirector mode when you must.

In transparent mode, the packets for accelerated connections must pass through the target appliance, much as they do in appliance-to-appliance acceleration.

The plug-in is configured with a list of appliances available for acceleration. It attempts to contact each appliance, opening a signaling connection. If the signaling connection is successful, the plug-in downloads the acceleration rules from the appliance, which sends the destination addresses for connections that the appliance can accelerate.

Figure 1. Transparent Mode, Highlighting Three Acceleration Paths



Note

- Traffic flow--Transparent mode accelerates connections between a WANOP Client Plug-in and a plug-in-enabled appliance.
- Licensing--Appliances need a license to support the desired number of plug-ins. In the diagram, Repeater A2 does not need to be licensed for plug-in acceleration, because Repeater A1 provides the plug-in acceleration for site A.
- Daisy-chaining--If the connection passes through multiple appliances on the way to the target appliance, the appliances in the middle must have "daisy-chaining" enabled, or acceleration is blocked. In the diagram, traffic from home-office and mobile VPN users that is destined for Large Branch Office B is accelerated by Repeater B. For this to work, Repeaters A1 and A2 must have daisy-chaining enabled.

Whenever the plug-in opens a new connection, it consults the acceleration rules. If the destination address matches any of the rules, the plug-in attempts to accelerate the connection by attaching acceleration options to the initial packet in the connection (the SYN packet). If any appliance known to the plug-in attaches acceleration options to the SYN-ACK response packet, an accelerated connection is established with that appliance.

The application and server are unaware that the accelerated connection has been established. Only the plug-in software and the appliance know that acceleration is taking place.

Transparent mode resembles appliance-to-appliance acceleration but is not identical to it. The differences are:

- Client-initiated connections only--Transparent mode accepts connections initiated by the plug-in-equipped system only. If you use a plug-in-equipped system as a server, server connections are not accelerated. Appliance-to-appliance acceleration, on the other hand, works regardless of which side is the client and which is the server. (Active-mode FTP is treated as a special case, because the connection initiating the data transfer requested by the plug-in is opened by the server.)
- Signaling connection--Transparent mode uses a signaling connection between the plug-in and appliance for the

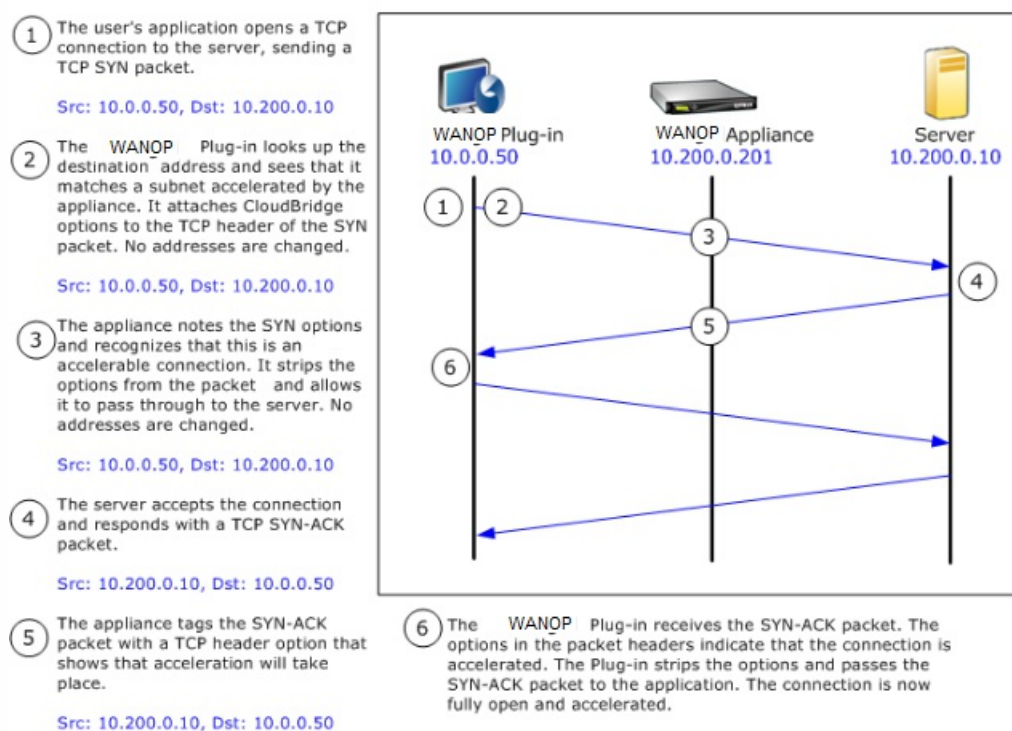
transmission of status information. Appliance-to-appliance acceleration does not require a signaling connection, except for secure peer relationships, which are disabled by default. If the plug-in cannot open a signaling connection, it does not attempt to accelerate connections through the appliance.

- Daisy-chaining--For an appliance that is in the path between a plug-in and its selected target appliance, you must enable daisy-chaining on the **Configuration: Tuning** menu.

Transparent mode is often used with VPNs. The WANOP Client Plug-in Plug-in is compatible with most IPSec and PPTP VPNs, and with Citrix Access Gateway VPNs.

The following figure shows packet flow in transparent mode. This packet flow is almost identical to appliance-to-appliance acceleration, except that the decision of whether or not to attempt to accelerate the connection is based on acceleration rules downloaded over the signaling connection.

Figure 2. Packet flow in transparent mode

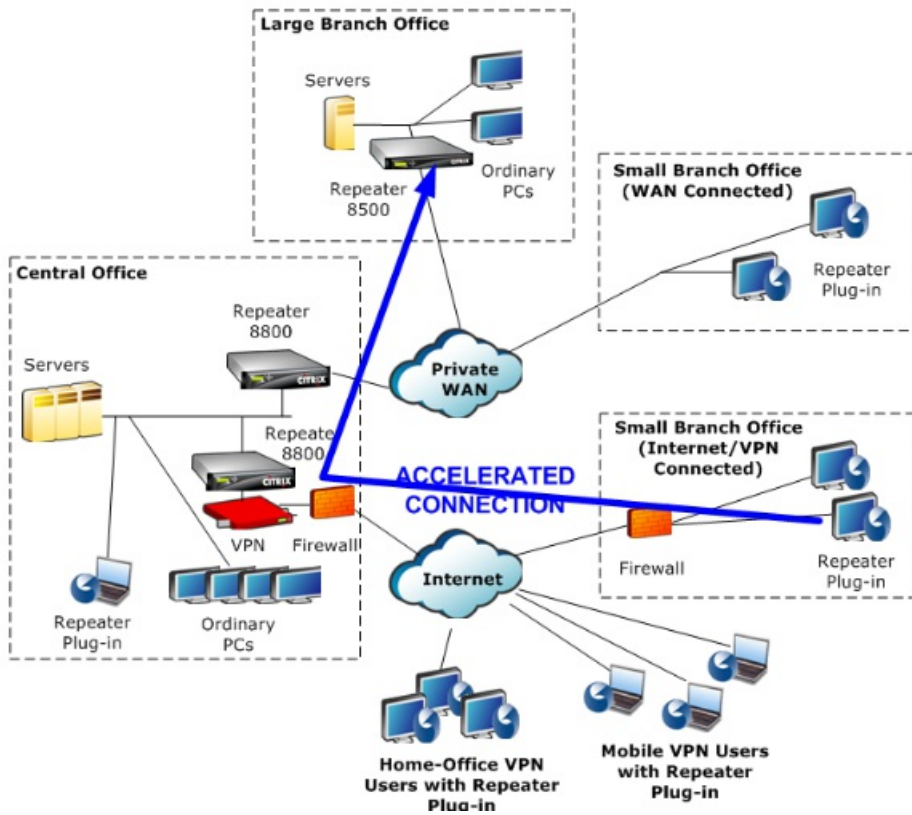


Redirector mode works differently from transparent mode in the following ways:

- The WANOP Client Plug-in Plug-in software redirects the packets by addressing them explicitly to the appliance.
- Therefore, the redirector-mode appliance does not have to intercept all of the WAN-link traffic. Because accelerated connections are addressed to it directly, it can be placed anywhere, as long as it can be reached by both the plug-in and the server.
- The appliance performs its optimizations, then redirects the output packets to the server, replacing the source IP address in the packets with its own address. From the server's point of view, the connection originates at the appliance.
- Return traffic from the server is addressed to the appliance, which performs optimizations in the return direction and forwards the output packets to the plug-in.
- The destination port numbers are not changed, so network monitoring applications can still classify the traffic.

The below figure shows how the Redirector mode works.

Figure 1. Redirector Mode



The below figure shows the packet flow and address mapping in *redirector mode*.

Figure 2. Packet Flow in Redirector Mode

1 The user's application opens a TCP connection to the server, sending a TCP SYN packet.

Src: 10.0.0.50, Dst: 10.200.0.10

2 The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.

Src: 10.0.0.50, Dst: 10.200.0.201

(10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

3 The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and giving itself as the src.

Src: 10.200.0.201, Dst: 10.200.0.10

4 The server accepts the connection and responds with a TCP SYN-ACK packet.

Src: 10.200.0.10, Dst: 10.200.0.201

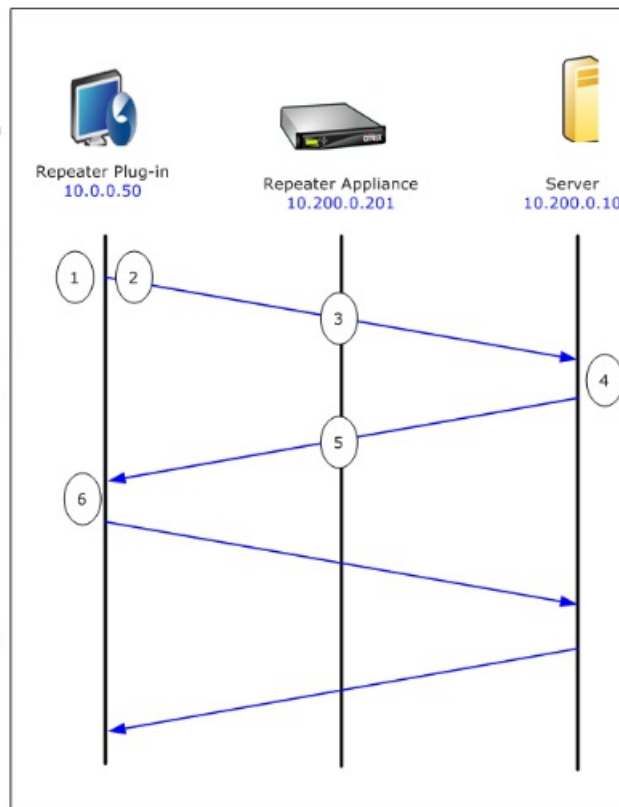
5 The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

Src: 10.200.0.201, Dst: 10.0.0.50

6 The connection is now fully open. The client and server send packets back and forth via the appliance.

While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.



Each plug-in is configured with a list of appliances that it can contact to request an accelerated connection.

The appliances each have a list of *acceleration rules*, which is a list of target addresses or ports to which the appliance can establish accelerated connections. The plug-in downloads these rules from the appliances and matches the destination address and port of each connection with each appliance's rule set. If only one appliance offers to accelerate a given connection, selection is easy. If more than one appliance offers to accelerate the connection, the plug-in must choose one of the appliances.

The rules for appliance selection are as follows:

- If all the appliances offering to accelerate the connection are redirector-mode appliances, the leftmost appliance in the plug-in's appliance list is selected. (If the appliances were specified as DNS addresses, and the DNS record has multiple IP addresses, these too are scanned from left to right.)
- If some of the appliances offering to accelerate the connection use redirector mode and some use transparent mode, the transparent-mode appliances are ignored and the selection is made from the redirector-mode appliances.

- If all of the appliances offering to accelerate the connection use transparent mode, the plug-in does not select a specific appliance. It initiates the connection with WANOP Client Plug-in SYN options, and whichever candidate appliance attaches appropriate options to the returning SYN-ACK packet is used. This allows the appliance that is actually in line with the traffic to identify itself to the plug-in. The plug-in must have an open signaling connection with the responding appliance, however, or acceleration does not take place.
- Some configuration information is considered to be global. This configuration information is taken from the leftmost appliance in the list for which a signaling connection can be opened.

Deploying Appliances for Use with Plug-ins

Mar 01, 2018

Client acceleration requires special configuration on the WANOP Client Plug-in appliance. Other considerations include appliance placement. Plug-ins are typically deployed for VPN connections.

Attempting to use the same appliance for both plug-in acceleration and link acceleration is often difficult, because the two uses sometimes call for the appliance to be at different points in the data center, and the two uses can call for different service-class rules.

In addition, a single appliance can serve as an endpoint for plug-in acceleration or as an endpoint for site-to-site acceleration, but cannot serve both purposes for the same connection at the same time. Therefore, when you use an appliance for both plug-in acceleration for your VPN and for site-to-site acceleration to a remote data center, plug-in users do not receive site-to-site acceleration. The seriousness of this problem depends on how much of the data used by plug-in users comes from remote sites.

Finally, because a dedicated appliance's resources are not divided between plug-in and site-to-site demands, they provide more resources and thus higher performance to each plug-in user.

An appliance should be deployed on the same site as the VPN unit that it supports. Typically, the two units are in line with each other. An inline deployment provides the simplest configuration, the most features, and the highest performance. For best results, the appliance should be directly in line with the VPN unit.

However, appliances can use any deployment mode, except group mode or high availability mode. These modes are suitable for both appliance-to-appliance and client-to-appliance acceleration. They can be used alone (*transparent mode*) or in combination with redirector mode.

An appliance depends on your existing security infrastructure in the same way that your servers do. It should be placed on the same side of the firewall (and VPN unit, if used) as the servers.

Network address translation (NAT) at the plug-in side is handled transparently and is not a concern. At the appliance side, NAT can be troublesome. Apply the following guidelines to ensure a smooth deployment:

- Put the appliance in the same address space as the servers, so that whatever address modifications are used to reach the servers are also applied to the appliance.
- Never access the appliance by using an address that the appliance does not associate with itself.
- The appliance must be able to access the servers by using the same IP addresses at which plug-in users access the same servers.
- In short, do not apply NAT to the addresses of servers or appliances.

On the Configure Settings: Bandwidth Management page, select Softboost mode. Softboost is the only type of

acceleration supported with the WANOP Client Plug-in Plug-in.

The appliance maintains a list of acceleration rules that tell the clients which traffic to accelerate. Each rule specifies an address or subnet and a port range that the appliance can accelerate.

What to Accelerate-The choice of what traffic to accelerate depends on the use the appliance is being put to:

- VPN accelerator - If the appliance is being used as a VPN accelerator, with all VPN traffic passing through the appliance, all TCP traffic should be accelerated, regardless of destination.
- Redirector mode - Unlike with transparent mode, an appliance in redirector mode is an explicit proxy, causing the plug-in to forward its traffic to the redirector-mode appliance even when doing so is not desirable. Acceleration can be counterproductive if the client forwards traffic to an appliance that is distant from the server, especially if this "triangle route" introduces a slow or unreliable link. Therefore, Citrix recommends that acceleration rules be configured to allow a given appliance to accelerate its own site only.
- Other uses - When the plug-in is used neither as a VPN accelerator nor in redirector mode, the acceleration rules should include addresses that are remote to the users and local to datacenters.

Defining the Rules- Define acceleration rules on appliance, on the **Configuration: WANOP Client Plug-in: Acceleration Rules** tab.

Rules are evaluated in order, and the action (Accelerate or Exclude) is taken from the first matching rule. For a connection to be accelerated, it must match an Accelerate rule.

The default action is to not accelerate.

Figure 1. Setting Acceleration Rules

Rule	Rule Type	Destination IP/Mask	Port
1	Exclude	10.200.33.102	All
2	Exclude	10.200.33.100	All
3	Exclude	10.200.33.104	All
4	Exclude	10.200.33.105	All
5	Accelerate	10.0.0.0/8	All
Default	Exclude	All	All

1. On the Configuration: WANOP Plug-in: Acceleration Rules tab:
 - Add an Accelerated rule for each local LAN subnet that can be reached by the appliance. That is, click **Add**, select **Accelerate**, and type the subnet IP address and mask.
 - Repeat for each subnet that is local to the appliance.
2. If you need to exclude some portion of the included range, add an Exclude rule and move it above the more general rule. For example, 10.217.1.99 looks like a local address. If it is really the local endpoint of a VPN unit, create an Exclude rule for it on a line above the Accelerate rule for 10.217.1.0/24.

3. If you want to use acceleration for only a single port (not recommended), such as port 80 for HTTP, replace the wildcard character in the Ports field with the specific port number. You can support additional ports by adding additional rules, one per port.
4. In general, list narrow rules (usually exceptions) before general rules.
5. Click **Apply**. Changes are not saved if you navigate away from this page before applying them.

Use the following guidelines for IP port usage:

- **Ports used for communication with WANOP Client Plug-in Plug-in**--The plug-in maintains a dialog with the appliance over a signaling connection, which by default is on port 443 (HTTPS), which is allowed through most firewalls.
- **Ports used for communication with servers**--Communication between the WANOP Client Plug-in Plug-in and the appliance uses the same ports that the client would use for communication with the server if the plug-in and appliance were not present. That is, when a client opens an HTTP connection on port 80, it connects to the appliance on port 80. The appliance in turn contacts the server on port 80.

In redirector mode, only the well-known port (that is, the destination port on the TCP SYN packet) is preserved. The ephemeral port is not preserved. In transparent mode, both ports are preserved.

The appliance assumes that it can communicate with the server on any port requested by the client, and the client assumes that it can communicate with the appliance on any desired port. This works well if appliance is subject to the same firewall rules as the servers. When such is the case, any connection that would succeed in a direct connection succeeds in an accelerated connection.

WANOP Client Plug-in parameters are sent in the TCP options. TCP options can occur in any packet and are guaranteed to be present in the SYN and SYN-ACK packets that establish the connection.

Your firewall must not block TCP options in the range of 24-31 (decimal), or acceleration cannot take place. Most firewalls do not block these options. However, a Cisco PIX or ASA firewall with release 7.x firmware might do so by default, and therefore you might have to adjust its configuration.

Customizing the Plug-in MSI File

Mar 01, 2018

You can change parameters in the WANOP Client Plug-in distribution file, which is in the standard Microsoft Installer (MSI) format. Customization requires the use of an MSI editor.

Note

The altered parameters in your edited MSI file apply only to new installations. When existing plug-in users update to a new release, their existing settings are retained. Therefore, after changing the parameters, you should advise your users to uninstall the old version before installing the new one.

Best Practices

Create a DNS entry that resolves to the nearest plug-in-enabled appliance. For example, define "Repeater.mycompany.com" and have it resolve to your appliance, if you have only one appliance. Or, if you have, say, five appliances, have Repeater.mycompany.com resolve to one of your five appliances, with the appliance selected on the basis of closeness to the client or to the VPN unit. For example, a client using an address associated with a particular VPN should see Repeater.mycompany.com resolve to the IP address of the WANOP Client Plug-in appliance connected to that VPN. Build this address into your plug-in binary with an MSI editor, such as Orca. When you add, move, or remove appliances, changing this single DNS definition on your DNS server updates the appliance list on your plug-ins automatically.

You can also have the DNS entry resolve to multiple appliances, but this is undesirable unless all appliances are configured identically, because the plug-in takes some of its characteristics from the leftmost appliance in the list and applies them globally (including SSL compression characteristics). This can lead to undesirable and confusing results, especially if the DNS server rotates the order of IP addresses for each request.

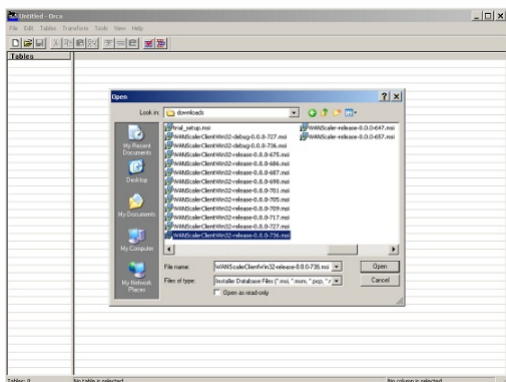
Installing the Orca MSI Editor

There are many MSI editors, including Orca, which is part of Microsoft's free Platform SDK and can be downloaded from Microsoft.

To install the Orca MSI Editor

1. Download the PSDK-x86.exe version of the SDK and execute it. Follow the installation instructions.
2. Once the SDK is installed, the Orca editor must be installed. It will be under Microsoft Platform SDK\Bin\Orca.Msi. Launch Orca.msi to install the actual Orca editor (orca.exe).
3. **Running Orca**--Microsoft provides its Orca documentation online. The following information describes how to edit the most important WANOP Client Plug-in Plug-in parameters.
4. Launch Orca with **Start > All Programs > Orca**. When a blank Orca window appears, open the WANOP Client Plug-in MSI file with **File > Open**.

Figure 1. Using Orca



5. On the **Tables** menu, click **Property**. A list of all the editable properties of the .MSI file appears. Edit the parameters shown in the following table. To edit a parameter, double-click on its value, type the new value, and press **Enter**.

Parameter	Description	Default	Comments
WSAPPLIANCES	List of appliances	None	Enter the IP or DNS addresses of your WANOP appliances here, in a comma-separated list in the form of { appliance1, appliance2, appliance3 } . If the port used for signaling connections is different from the default (443), specify the port in the form Appliance1:port_number .
DBCMSIZE	Minimum amount of disk space to use for compression, in megabytes	250	Changing this to a larger value (for example, 2000) improves compression performance but prevents installation if there is not enough disk space. The plug-in will not install unless there is at least 100 MB of free disk space in addition to the value that you specify for DBCMSIZE.
EKEYPEM	Private key for the plug-in. Part of the certificate/key pair used with SSL compression	None	Use Orca's Paste Cell command. The normal Paste function does not preserve the key's format. Should be a private key in PEM format (starting with -----BEGIN RSA PRIVATE KEY-----)
X509CERTPEM	Certificate for the plug-in. Part of the certificate/key pair used with SSL compression	None	Use Orca's Paste Cell command. The normal Paste function does not preserve the key's format. Should be a certificate in PEM format (starting with -----BEGIN CERTIFICATE -----)
CACERTPEM	Certification Authority Certificate for	None	Use Orca's Paste Cell command. The normal Paste function does not preserve the key's format. Should be a certificate in

the plug-in. Used with SSL
compression

PEM format (starting with -----BEGIN CERTIFICATE -----)

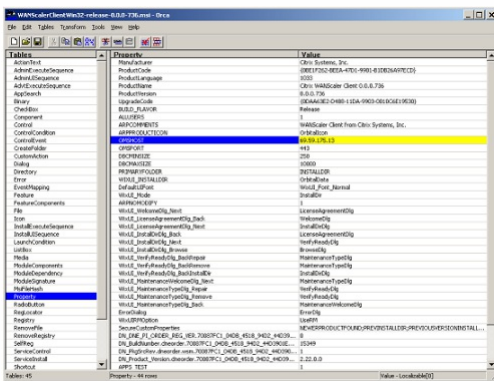
- 1.
2. On the Tables menu, click Property. A list of all the editable properties of the .MSI file appears. Edit the parameters shown in the following table. To edit a parameter, double-click on its value, type the new value, and press Enter.

Parameter	Description
WSAPPLIANCES	List of appliances
DBCMINISIZE	Minimum amount of disk space to use for compression, in megabytes
PRIVATEKEYPEM	Private key for the plug-in. Part of the certificate/key pair used with SSL compression
X509CERTPEM	Certificate for the plug-in. Part of the certificate/key pair used with SSL compression
CACERTPEM	Certification Authority Certificate for the plug-in. Used with SSL compression

Figure 2. Editing Parameters in Orca

3. When done, use the File: Save As command to save your edited file with a new filename; for example, test.msi.

Figure 2: Editing Parameters in Orca



6. When done, use the File: Save As command to save your edited file with a new filename; for example, test.msi.

Your plug-in software has now been customized.

Note: Some users have seen a bug in orca that causes it to truncate files to 1 MB. Check the size of the saved file. If it has been truncated, make a copy of the original file and use the Save command to overwrite the original.

Once you have customized the appliance list with Orca and distributed the customized MSI file to your users, the user does not need to type in any configuration information when installing the software.

Deploying Plug-ins on Windows Systems

Mar 01, 2018

The WANOP Client Plug-in is an executable Microsoft installer (MSI) file that you download and install as with any other web-distributed program. Obtain this file from the MyCitrix section of the Citrix.com website.

Note: The WANOP Client Plug-in user interface refers to itself as "Citrix Acceleration Plug-in Manager."

The only user configuration needed by the plug-in is the list of appliance addresses. This list can consist of a comma-separated list of IP or DNS address. The two forms can be mixed. You can customize the distribution file so that the list points to your appliance by default. Once installed, operation is transparent. Traffic to accelerated subnets is sent through an appropriate appliance, and all other traffic is sent directly to the server. The user application is unaware that any of this is happening.

To install WANOP Client Plug-in Plug-in accelerator on Windows system:

1. The Repeater*.msi file is an installation file. Close all applications and any windows that might be open, and then launch the installer it in the usual way (double-click on in a file window, or use the run command).

Figure 1. Initial Installation Screen



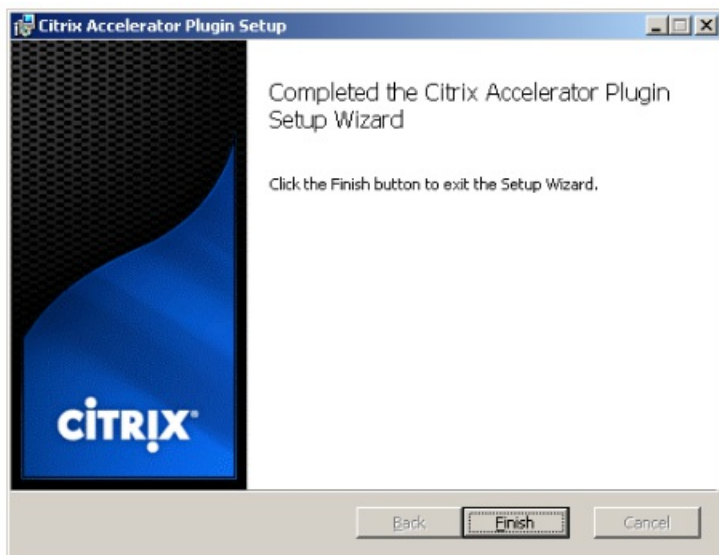
The steps below are for an interactive installation. A silent installation can be performed with the command:

```
msiexec /i client_msi_file /qn
```

2. The installation program prompts for the location in which to install the software. The directory that you specify is used for both the client software and the disk-based compression history. Together, they require a minimum of 500 MB of disk space.

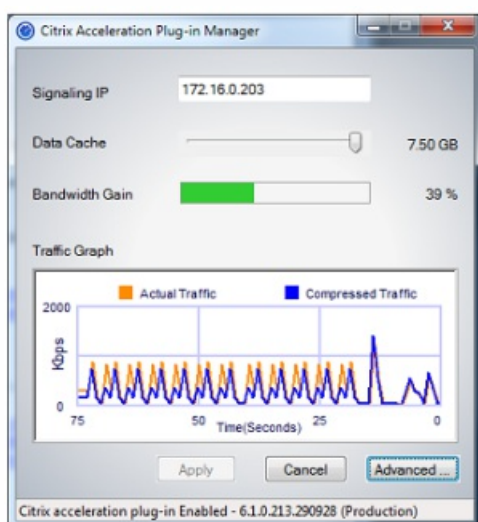
3. When the installer finishes, it might ask you to restart the system. After a restart, the WANOP Client Plug-in Plug-in starts automatically.

Figure 2. Final Installation Screen



4. Right-click the Accelerator icon in the task bar and select **Manage Acceleration** to launch the Citrix Plug-in Accelerator Manager.

Figure 3. Citrix Accelerator Plug in Manager, Initial (Basic) Display



5. If the .MSI file has not been customized for your users, specify the signaling address and the amount of disk space to use for compression:

- In the Appliances: Signaling Addresses field, type the signaling IP address of your appliance. If you have more than one Plug-in-enabled appliance, list them all, separated by commas. Either IP or DNS addresses are acceptable.
- Using the Data Cache slider, select the amount of disk space to use for compression. More is better. 7.5 GB is not too much, if you have that much disk space available.
- Press Apply.

The WANOP Client Plug-in accelerator is now running. All future connections to accelerated subnets will be accelerated

On the plug-in's Advanced Rules tab, the Acceleration Rules list should show each appliance as Connected and each appliance's accelerated subnets as Accelerated. If not, check the Signaling Addresses IP field and your network connectivity in general.

Plug-in installation generally goes smoothly. If not, check for the following issues:

Common problems

- If you do not reboot the system, the WANOP Client Plug-in will not run properly.
- A highly fragmented disk can result in poor compression performance.
- A failure of acceleration (no accelerated connections listed on the **Diagnostics** tab) usually indicates that something is preventing communication with the appliance. Check the **Configuration: Acceleration Rules** listing on the plug-in to make sure that the appliance is being contacted successfully and that the target address is included in one of the acceleration rules. Typical causes of connection failures are:
 - The appliance is not running, or acceleration has been disabled.
 - A firewall is stripping WANOP Client Plug-in TCP options at some point between the plug-in and appliance.
 - The plug-in is using an unsupported VPN.

On rare occasions, after you install the plug-in and restart your computer, the following error message appears twice:

Deterministic Network Enhancer installation requires a reboot first, to free locked resources. Please run this install again after restarting the computer.

If this occurs, do the following:

1. Go to **Add/Remove Programs** and remove the WANOP Client Plug-in, if present.
2. Go to **Control Panel > Network Adapters > Local Area Connection > Properties**, find the entry for Deterministic Network Enhancer, clear its check box, and click **OK**. (Your network adapter might be called by a name other than "Local Area Connection.")
3. Open a command window and go to `c:\windows\inf` (or the equivalent directory if you have installed Windows in a non-standard location).
4. Type the following command:
`find "dne2000.cat" oem*.inf`
5. Find the highest-numbered `oem*.inf` file that returned a matching line (the matching line is `CatalogFile= dne2000.cat`) and edit it. For example:
`notepad oem13.inf`
6. Delete everything except the three lines at the top that start with semicolons, and then save the file. This will clear out any inappropriate or obsolete settings and the next installation will use default values.
7. Retry the installation.

Any problem with installing the WANOP Client Plug-in is usually the result of existing networking, firewall, or antivirus software interfering with the installation. Usually, once the installation is complete, there are no further problems.

If the installation fails, try the following steps:

1. Make sure the plug-in installation file has been copied to your local system.
2. Disconnect any active VPN/remote networking clients.
3. Disable any firewall and antivirus software temporarily.
4. If some of this is difficult, do what you can.
5. Reinstall the WANOP Client Plug-in.
6. If this doesn't work, reboot the system and try again.

WANOP Plug-in GUI Commands

Mar 01, 2018

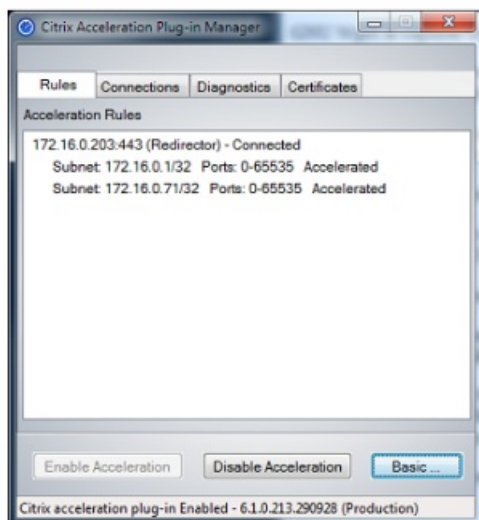
The WANOP Client Plug-in GUI appears when you right-click the **Citrix Accelerator Plug-in** icon and select **Manage Acceleration**. The GUI's Basic display appears first. There is also an Advanced display that can be used if desired.

On the Basic page, you can set two parameters:

- The Signaling Addresses field specifies the IP address of each appliance that the plug-in can connect to. Citrix recommends listing only one appliance, but you can create a comma-separated list. This is an ordered list, with the leftmost appliances having precedence over the others. Acceleration is attempted with the leftmost appliance for which a signaling connection can be established. You can use both DNS addresses and IP addresses.
Examples: 10.200.33.200, ws.mycompany.com, ws2.mycompany.com
- The Data Cache slider adjusts the amount of disk space allocated to the plug-in's disk-based compression history. More is better.

In addition, there is a button to move to the Advanced display.

The Advanced page contains four tabs: Rules, Connections, Diagnostics, and Certificates.



At the bottom of the display are buttons to enable acceleration, disable acceleration, and return to the Basic page.

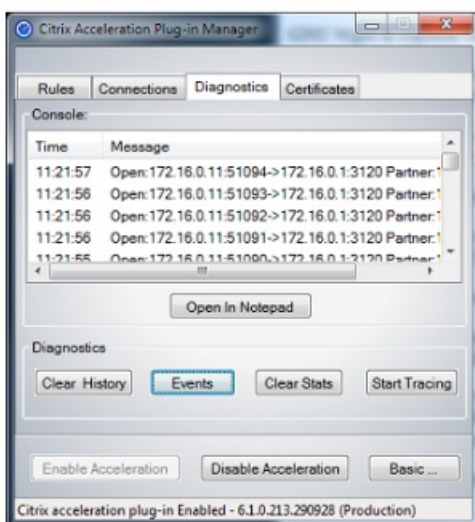
The Rules tab displays an abbreviated list of the acceleration rules downloaded from the appliances. Each list item shows the appliance's signaling address and port, acceleration mode (redirector or transparent), and connection state, followed by a summary of the appliance's rules.

The **Connections** tab lists the number of open connections of different types:

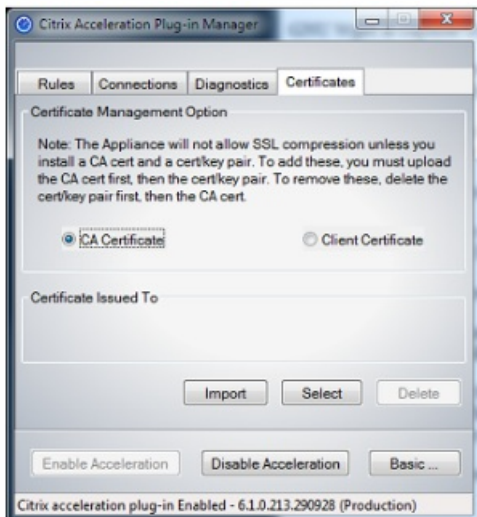
- **Accelerated Connections**--The number of open connections between the WANOP Client Plug-in Plug-in and appliances. This number includes one signaling connection per appliance but does not include accelerated CIFS connections. Clicking More opens a window with a brief summary of each connection. (All of the More buttons allow you to copy the information in the window to the clipboard, should you want to share it with Support.)
- **Accelerated CIFS Connections**--The number of open, accelerated connections with CIFS (Windows file system) servers. This is usually the same as the number of mounted network file systems. Clicking More displays the same information as with accelerated connections, plus a status field that reports Active if the CIFS connection is running with WANOP Client Plug-in's special CIFS optimizations.
- **Accelerated MAPI Connections**--The number of open, accelerated Outlook/Exchange connections.
- **Accelerated ICA connections**--The number of open, accelerated XenApp and XenDesktop connections using the ICA or CGP protocols.
- **Unaccelerated Connections**--Open connections that are not being accelerated. You can click More to display a brief description of why the connection was not accelerated. Typically, the reason is that no appliance accelerates the destination address, which is reported as Service policy rule .
- **Opening/Closing Connections**--Connections that are not fully open, but are in the process of opening or closing (TCP "half-open" or "half-closed" connections). The More button displays some additional information about these connections.

The Diagnostics page reports the number of connections in different categories, and other useful information.

- **Start Tracing/Stop Tracing**--If you report a problem, your Citrix representative might ask you to perform a connection trace to help pinpoint problems. This button starts and stops the trace. When you stop tracing, a pop-up window shows the trace files. Send them to your Citrix representative by the means he or she recommends.
- **Clear History**--This feature should not be used.
- **Clear Statistics**--Pressing this button clears the statistics on the Performance tab.
- **Console**--A scrollable window with recent status messages, mostly connection-open and connection-close messages, but also error and miscellaneous status messages.



On the Certificates tab, you can install security credentials for the optional secure peering feature. The purpose of these security credentials is to enable the appliance to verify whether the plug-in is a trusted client or not.



To upload the CA certificate and certificate-key pair:

1. Select **CA Certificate Management**.
2. Click **Import**.
3. Upload a CA certificate. The certificate file must use one of the supported file types (.pem, .crt., .cer, or .spc). A dialog box might appear, asking you to Select the certificate store you want to use and presenting you with a list of keywords. Select the first keyword in the list.
4. Select **Client Certificate Management**.
5. Click **Import**.
6. Select the format of the certificate-key pair (either PKCS12 or PEM/DER).
7. Click **Submit**.

Note

In the case of PEM/DER, there are separate upload boxes for certificate and key. If your certificate-key pair is combined in a single file, specify the file twice, once for each box.

Updating the WANOP Plug-in

Mar 01, 2018

To install a newer version of the WANOP Client Plug-in, follow the same procedure you used when installing the plug-in for the first time.

Uninstalling the WANOP Client Plug-in Plug-in

To uninstall the WANOP Client Plug-in Plug-in To uninstall the WANOP Client Plug-in, use the Windows Add/Remove Programs utility. The WANOP Client Plug-in is listed as **Citrix Acceleration Plug-in** in the list of currently installed programs. Select it and click **Remove**.

You must restart the system to finish uninstalling the client.

Troubleshooting WANOP Plug-in

Mar 01, 2018

- **Issue:** I am facing signaling channel connectivity issues. How can I resolve these issues?
Resolution: To resolve signaling channel connectivity issues, perform the following troubleshooting steps:
 - Verify that you have correctly configured the signaling IP address. You can do so by pinging the signaling IP address and verifying the response.
 - Verify that the signaling status is enabled on the WANOP appliance.
 - Verify that the firewall installed on the network does not remove the WANOP TCP options.
 - Verify that a valid WANOP plug-in license is installed on the WANOP appliance.
 - Verify that the Signaling Channel Source Filtering configuration does not block the Client Source IP address.
 - If you have enabled LAN Detection, verify that the Round Trip Time between the WANOP plug-in and WANOP appliance is an acceptable value.
- **Issue:** On a WANOP 4000 appliance, I am not able to disable the WANOP plug-in.
Cause: This is a known issue.
Resolution: None. You cannot disable the WANOP plug-in on a WANOP 4000 appliance.
- **Issue:** When connecting to the WANOP appliance by using the WANOP plug-in, the following error message entry is logged on the Alerts tab:
More WANOP Plug-ins than the current limit of <Number> have attempted to connect to this Appliance.
Cause: The number of connections to the WANOP appliance has exceeded the licensed user limit.
Resolution: Either wait for a user to disconnect or terminate a connection.
- **Issue:** Incorrect signaling IP address is configured on a WANOP 4000 or 5000 appliance.
Resolution: To update the signaling IP address on a WANOP 4000 or 5000 appliance, complete the following procedure:
 1. Log on to the NetScaler instance of the WANOP appliance.
 2. Navigate to the Traffic Management > Load Balancing > Virtual Servers > BR_LB_VIP_SIG page.
 3. Update the signaling IP address.
 4. Save the configuration.
- **Issue:** CIFS and ICA traffic is not getting accelerated.
Resolution: To resolve this issue, perform the following troubleshooting steps:
 - Verify that acceleration rules for IP address and port numbers are correctly defined for the WANOP plug-in.
 - Verify that CIFS or ICA connections are established after signaling connection is successful.
 - Verify the acceleration policy for the service class being used.

How-To-Articles

Mar 16, 2018

The "How-to Articles" describe the procedure to configure supported features by NetScaler SD-WAN. These articles contain information about some of the following important features:

Click a feature name below to view the list of how-to articles for that feature.

Virtual Routing and Forwarding	Enabling RED for QoS Fairness	Configuration
Dynamic Routing	DHCP Server and DHCP Relay	Route Filters
IPsec Termination and Monitoring	Secure Web Gateway	QoS
FIPS Compliant Operation - IPsec Tunnel	Dynamic NAT Configuration	Adaptive Bandwidth Detection
Active Bandwidth Testing	BGP Enhancements	Service Class Association with SSL Profiles
WAN Link Templates - Basic Mode Configuration	Auto Secure Peering and Manual Secure Peering	Zero Touch Deployment
Two Box Mode Deployment	IPSec Null Encryption	SD-WAN SE/EE Hairpin Mode Deployment
Single-Step Upgrade	Enable FIPS Compliance Mode	Upgrade Procedure
Firewall Segmentation	High Availability	Secure Peering

Interface Groups

Mar 01, 2018

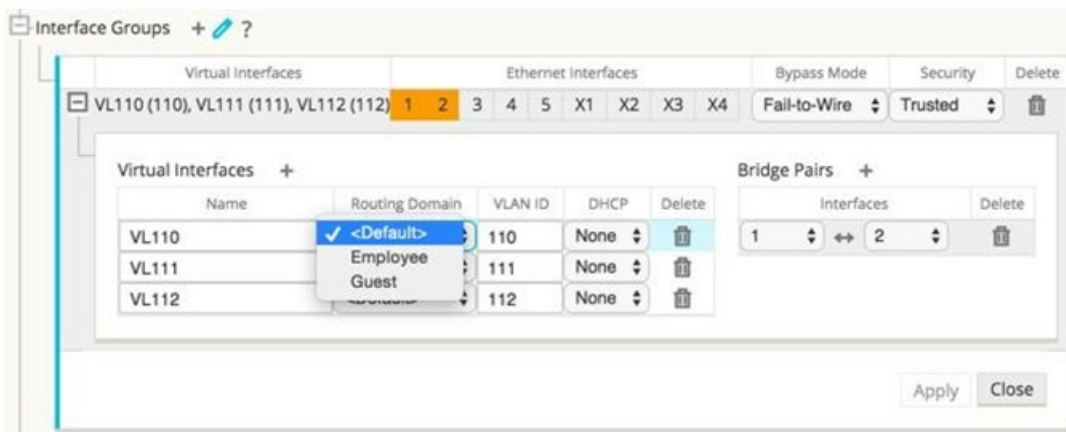
To configure interface groups:

1. In the **Configuration Editor**, navigate to **Sites** → **[Client Site Name]** → **Interface Groups**, choose a **Routing Domain** from the drop-down menu when configuring Virtual Interfaces.

For detailed instructions, see [configuring interface groups](#).

Note

After Virtual Interfaces are associated with a specific Routing Domain, only those interfaces will be available when using that Routing Domain.

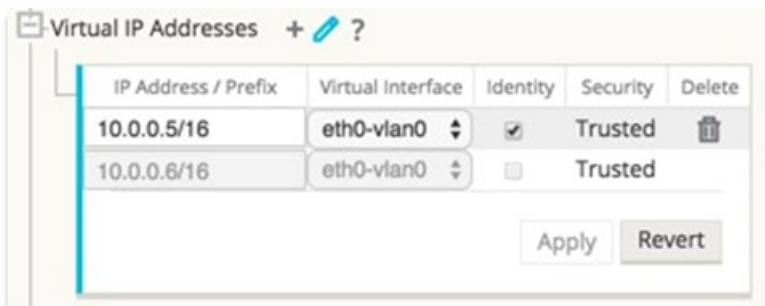


Configure Virtual IP Address Identity

Mar 01, 2018

To configure Virtual IP Address identity:

1. In the **Configuration Editor**, navigate to **Sites** → **[Site Name]** → **Virtual IP Addresses**.
2. Click the **Identity** checkbox for a Virtual IP Address to use it for IP services.



Configure Access Interface

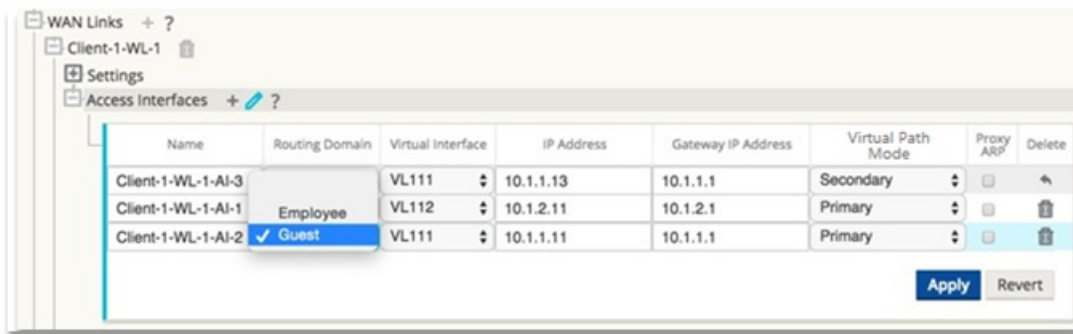
Jun 07, 2018

To configure Access Interface:

1. In the **Configuration Editor**, navigate to **Sites** → **[Client Site Name]** → **WAN Links** → **[WAN Link Name]** → **Access Interfaces**.

2. Choose a **Routing Domain** from the drop-down menu when configuring an Access Interface.

For detailed instructions, see [configuring WAN links and Access Interfaces](#).



Note

You can ignore the gateway MAC address binding when configuring Access Interface on a 210-SE LTE appliance network configuration.

Configure Virtual IP Addresses

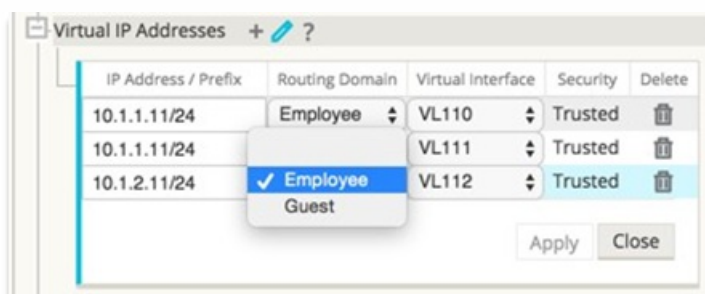
Mar 01, 2018

To configure Virtual IP Addresses:

1. In the **Configuration Editor**, navigate to **Sites** → **[Client Site Name]** → **Virtual IP Addresses**.
2. Choose a **Routing Domain** from the dropdown menu when configuring Virtual IP Addresses.

For detailed instructions, see [configuring Virtual IP addresses](#).

The Routing Domain you choose determines which Virtual Interfaces are available from the drop-down menu.



Configure GRE Tunnels

Mar 01, 2018

To configure GRE Tunnels:

1. In the configuration editor, navigate to **Connections > Site > GRE Tunnels**. The source IP address can only be chosen from the Virtual network interface on trusted links.
2. Enter a name for the GRE Tunnel.
3. Select the **Source IP** address available from the drop-down menu. The Routing Domain determines which Source IP Addresses are available from the drop-down menu.
4. (Optional) Select the **Public Source IP**. This field can be empty if this address is the same as Source IP.
5. Enter the **Destination IP** address of the GRE Tunnel.
6. Enter the **Tunnel IP/Prefix** address of the GRE Tunnel.
7. Click **Checksum**, if you want to use checksum in the GRE Tunnel Header.
8. Enter a value for the **Keepalive Period** in seconds. If you configure 0, no keepalive packet are transmitted, but the GRE Tunnel will be active.
9. Enter a value for the **Keepalive Retries**. This value determines the number of times the keepalive retries are attempted before the SD-WAN appliance deactivates the GRE Tunnel.

Refer to the [configuring GRE tunnels](#) on the MCN site for more information.

Name	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	*		*	*	<input type="checkbox"/>	10	3	

Apply Revert

For more information about securing web gateway using GRE tunnels, see; [Secure Web Gateway](#)

Setup Dynamic Paths for Branch to Branch Communication

Mar 01, 2018

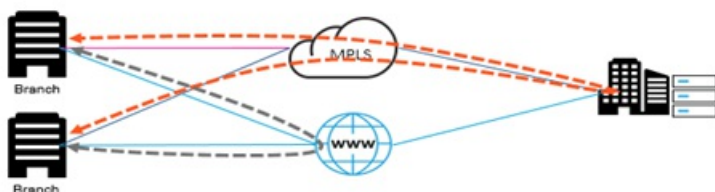
With demand for VoIP and video conferencing, the traffic is increasingly moving between offices. It is inefficient to set up full mesh connections through datacenters which can be time consuming.

With NetScaler SD-WAN, you do not need to configure paths between every office. You can enable the Dynamic Path feature and the SD-WAN solution automatically creates paths between offices on demand. The session initially uses an existing fixed path. And as bandwidth and time threshold is met, a path is created dynamically if that new path has better performance characteristics than the fixed path. Session traffic is transmitted through the new path. This results in efficient usage of resources. Paths exist only when they are needed and reduce the amount of traffic getting transmitted to and from the datacenter.

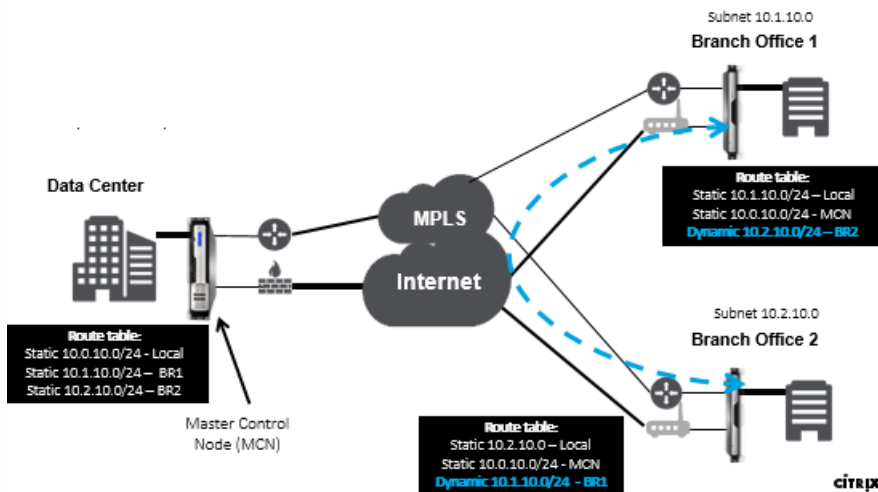
Additional benefits of SD-WAN network include:

- Bandwidth and PPS thresholds to allow branch to branch connections
- Reduce bandwidth requirements in and out of data center while minimizing latency
- Paths created on demand depend on set thresholds
- Dynamically release network resources when not required
- Reduce load on the Master Control Node and latency

Branch to Branch Communication Using Dynamic Paths



SD-WAN Network with Dynamic Path

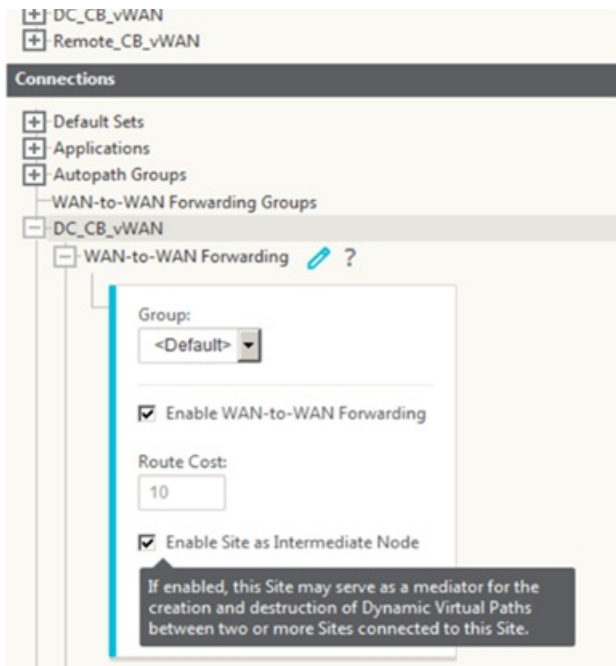


- Dynamic virtual paths are used for large scale deployments, such as Enterprises
- Smaller deployments use Static virtual paths and any-to-any virtual paths
- Always use Static virtual paths between two Data Centers (DC to DC)
- Not all WAN paths need to be configured for using Dynamic virtual path
- Each SD-WAN appliance has limited number of Dynamic virtual paths (8 dynamic lowest limit, 8 static lowest limit = total 16) that can be configured.

How to Enable Dynamic Virtual Path in the SD-WAN GUI

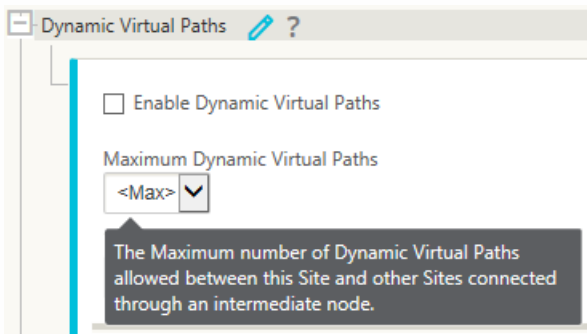
To enable dynamic virtual paths:

1. In the NetScaler SD-WAN GUI, under the **Connections** pane, create a WAN to WAN Forwarding Group.
2. Navigate to **Connections** → [Client Site Name] → **WAN to WAN Forwarding**.
 - a) Enable **WAN to WAN Forwarding** to enable the site to serve as a proxy for multi-hop site to site.
 - b) Enable **Site as Intermediate Node**
3. Navigate to **Connections** → **Remote Site** → **WAN to WAN Forwarding**.
 - a) Enable WAN to WAN Forwarding to enable the site to serve as a proxy for multi-hop site to site.



4. Navigate to **Connections** → **Remote Site** → **Virtual Path** → **Dynamic Virtual Path**.

- a) Enable **Dynamic Virtual Paths**.
- b) Set the maximum number of dynamic paths.



How to Create a Dynamic Virtual Path

- Configuration determines when a Dynamic Virtual Path is active or down.
- Configure sample packet count (pps) or bandwidth (kbps) within a timeframe.
- Can be set Globally or with WAN Link configured at the Intermediate Node.

Connections

- Default Sets ?
 - Virtual Path Default Sets
 - Dynamic Virtual Path Default Sets + ?
 - New_Dynamic_Virtual_Path_Default_Set
 - Basic Settings ?

Creation Limits	Removal Limits
Sample Time (s): <input type="text" value="1"/>	Sample Time (m): <input type="text" value="2"/>
Throughput (kbps): <input type="text" value="600"/>	Throughput (kbps): <input type="text" value="45"/>
Throughput (pps): <input type="text" value="45"/>	Throughput (pps): <input type="text" value="35"/>
 - Timers
 - Remove Virtual Path Down Wait Time(m):
 - Recreate Virtual Path Hold Time(m):

Apply Close

Configure Static WAN Paths

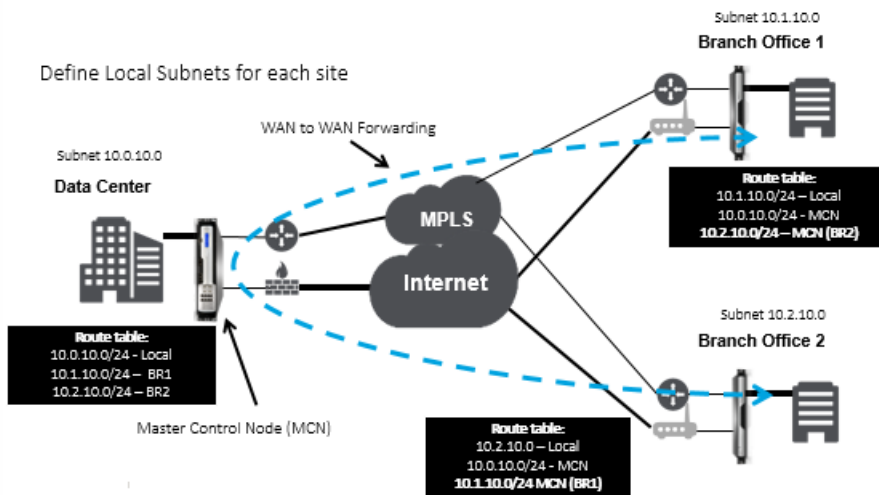
Mar 01, 2018

With WAN to WAN enabled on the MCN, remote site routes are advertised by MCN.

- Clients are aware of MCN local routes as well as other client site routes
- From client perspective, all routes are considered as MCN routes

When WAN-to-WAN forwarding is not enabled on the MCN, Branch to Branch communication issues are encountered in the customer network.

SD-WAN appliances running in client mode are not aware of other branches subnets until WAN-to-WAN forwarding is enabled on MCN. Once this option is enabled, branch SD-WAN nodes become aware of other branch subnets and all the traffic destined to other branches is forwarded to MCN. MCN routes it to the correct destination.



Monitoring and Troubleshooting

Mar 01, 2018

You can use the SD-WAN appliance web management interface to monitor and troubleshoot supported features. Below are the links to Monitoring and Troubleshooting topics applicable for SD-WAN appliances.

[Monitoring Virtual WAN](#)

[Viewing Statistical Information](#)

[Viewing Flow Information](#)

[Viewing Reports](#)

[Viewing Firewall Statistics](#)

[Diagnostic Tool](#)

[Improved Path Mapping and Bandwidth Usage](#)

[Troubleshooting Management IP](#)

Monitoring Virtual WAN

Mar 01, 2018

Viewing Basic Information for an Appliance

Use a browser to connect to the Management Web Interface of the appliance you want to monitor, and click the **Dashboard** tab to display basic information for that appliance.

The **Dashboard** page displays the following basic information for the local appliance:

System Status:

- **Name** – This is the name you assigned to the appliance when you added it to the system.
- **Model** – This is the Virtual WAN appliance model number.
- **Appliance Mode** – This indicates whether this appliance has been configured as the primary or secondary MCN, or as a client appliance.
- **Management IP Address** – This is the Management IP Address for the appliance.
- **Appliance Uptime** – This specifies the duration for which the appliance has been running since the last reboot.
- **Service Uptime** – This specifies the duration for which the Virtual WAN Service has been running since the last restart.

Virtual Path Service Status:

Virtual Path [site name] – This displays the current status of all the Virtual Paths associated with this appliance. If the Virtual WAN Service is enabled, this section is included on the page. If the Virtual WAN Service is disabled, an Alert icon (goldenrod delta) and Alert message to that effect displays in place of this section.

Local Version Information:

- **Software version** – This is the version of the CloudBridge Virtual Path software package currently activated on the appliance.
- **Build on** – This is the build date for the product version currently running on the local appliance.
- **Hardware version** – This is the hardware model number and version of the appliance.
- **OS Partition Version** – This is the version of the OS partition currently active on the appliance.

The below figure shows a sample Dashboard page.

Dashboard Monitoring Configuration

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, 8 minutes, 58.4 seconds
 Service Uptime: 4 hours, 23 minutes, 24.0 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: 4 hours, 1 minutes, 4.0 seconds.
Virtual Path MCN-5100-BR573:	Uptime: 3 hours, 46 minutes, 30.0 seconds.
Virtual Path MCN-5100-BR574:	Uptime: 2 hours, 58 minutes, 19.0 seconds.
Virtual Path 'MCN-5100-BR575' is currently dead.	
Virtual Path MCN-5100-RCN1-5100:	Uptime: 8 minutes, 34.0 seconds.
Virtual Path 'MCN-5100-RCN3-2100' is currently dead (Configuration version mismatch)	

You can view the complete list of SD-WAN events by downloading the following spreadsheet.

 [SD-WAN Events](#)

Viewing Statistical Information

Mar 01, 2018

This section provides basic instructions for viewing Virtual WAN statistics information.

1. Log into the Management Web Interface for the MCN.
2. Select the **Monitoring** tab.

This opens the **Monitoring** navigation tree in the left pane. By default, this also displays the **Statistics** page with **Paths** preselected in the **Show** field. This contains a detailed table of path statistics.

Note

If you navigate to another **Monitoring** page (for example, **Flows**), you can return to this page by selecting **Statistics** in the **Monitoring** navigation tree (left pane).

The screenshot displays the Citrix Management Web Interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar shows a navigation tree with 'Statistics' selected. The main content area is titled 'Monitoring > Statistics'. It features a 'Show' dropdown menu set to 'Paths (Summary)', an 'Enable Auto Refresh' checkbox, a refresh interval of '5' seconds, and a 'Show latest data' checkbox. Below this is the 'Path Statistics Summary' section, which includes a filter field and a 'Show 100 entries' dropdown. The main part of the screenshot is a table with the following data:

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	MCN-DC-WL-1	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	59.95	NO
2	MCN-DC-WL-1	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	8.72	NO
3	MCN-DC-WL-2	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	8.72	NO
4	MCN-DC-WL-2	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	11.82	NO
5	Branch1-WL-1	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	8.89	NO
6	Branch1-WL-1	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	25.19	NO
7	Branch1-WL-2	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	11.84	NO
8	Branch1-WL-2	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	8.73	NO

At the bottom of the table, it says 'Showing 1 to 8 of 8 entries' and 'Bandwidth calculated over the last 41278.42 seconds'. Navigation buttons for 'First', 'Previous', '1', 'Next', and 'Last' are visible.

3. Open the **Show** drop-down menu next to the **Show** field.

In addition to the **Paths** statistics, the **Show** menu also offers several additional options for filtering and viewing statistical information.

Monitoring > Statistics

Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Refresh Show latest data.

Filter: by column Apply Show 100 entries

Num	Observed Protocols	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	Paths (Summary)	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	59.95	NO
2	Paths (Detailed)	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	8.72	NO
3	Routes	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	8.72	NO
4	Application Routes	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	8.72	NO
5	Application QoS Rules	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	8.72	NO
6	Rule Groups	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	11.82	NO
7	Site	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	8.89	NO
8	WAN Link	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	25.19	NO
9	MPLS Queues	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	11.84	NO
10	WAN Link Usage	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	8.73	NO

Showing 1 to 8 of 8 entries

Bandwidth calculated over the last 41278.42 seconds

First Previous 1 Next Last

4. Select a filter from the **Show** menu to view a table of statistical information for that topic.

Viewing Flow Information

Mar 01, 2018

This section provides basic instructions for viewing Virtual WAN flow information.

To view flow information, do the following:

1. Log into the Management Web Interface for the MCN, and select the **Monitoring** tab.

This opens the **Monitoring** navigation tree in the left pane.

2. Select the **Flows** branch in the navigation tree.

This displays the **Flows** page with **LAN to WAN** preselected in the **Flow Type** field.

The screenshot shows the 'Monitoring > Flows' page. In the 'Select Flows' section, 'LAN to WAN' and 'WAN to LAN' are checked. The 'Max Flows to Display' is set to 50. Below is a table with the following data:

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Typ
172.147.21.53	172.147.12.83	LAN to WAN	2312	50829	TCP	default	3	Virtual Path	MCN-DC-Branch1	LOCAL	5292	2	104	0.237	0.099	0.100	0.000	65	N/A	13	INTERACT
172.147.12.83	172.147.21.53	WAN to LAN	50829	2312	TCP	default	3	Virtual Path	MCN-DC-Branch1	LOCAL	5328	3	180	0.355	0.170	0.151	0.000	132	N/A	N/A	

3. Select the **Flow Type**.

The **Flow Type** field is located in the **Select Flows** section at the top of the **Flows** page. Next to the **Flow Type** field is a row of checkbox options for selecting the flow information you want to view. You can check one or more boxes to filter the information to be displayed.

4. Select the **Max Flows to Display** from the drop-down menu next to that field.

This determines the number of entries to display in the **Flows** table. The options are: **50, 100, 1000**.

5. (Optional) Enter search text in the **Filter** field.

This filters the table results so that only entries containing the search text display in the table.

Tip

To see detailed instructions for using filters to refine **Flow** table results, click **Help** to the right of the **Filter** field. To close the help display, click **Refresh** in the bottom left corner of the **Select Flows** section.

6. Click **Refresh** to display the filter results.

The below figure shows a sample **Flows** page filtered display with all flow types selected.

Select Flows

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

Max Flows to Display (Per Flow Type): 50

Filter (Optional): 172.79.2.83 [Help](#)

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

7. (Optional) Select the columns to include in the table.

Do the following:

- a. Click **Toggle Columns**.

The **Toggle Columns** button is just above the top right corner of the **Flows** table. This reveals any deselected columns, and opens a checkbox above each column for selecting or deselecting that column. Deselected columns display greyed out, as shown in the below figure.

Note

By default, all of the columns are selected, which can cause the table to be truncated in the display, obscuring the **Toggle Columns** button. If so, a horizontal scroll bar displays beneath the table. Slide the scroll bar to the right to view the truncated section of the table and reveal the **Toggle Columns** button. If the scroll bar is not available, try resizing the width of your browser window until the scroll bar is revealed.

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

b. Click a checkbox to select or deselect a column.

c. Click **Apply** (above the top right corner of the table).

This dismisses the selection options, and refreshes the table to include only the selected columns.

Select Flows

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

Max Flows to Display (Per Flow Type): 50

Filter (Optional): 172.79.2.83 [Help](#)

Refresh

Flows Data

Toggle Columns

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	9613	Virtual Path	DC-BR	LOCAL	12022	12084	1024626
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	9667	Virtual Path	DC-BR	LOCAL	12040	12246	1080066
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	18092	Virtual Path	DC-BR	LOCAL	12040	18092	1299440
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	18312	Virtual Path	DC-BR	LOCAL	12056	18312	1394758

Total LAN to WAN flows displayed: 2 out of 306
Total WAN to LAN flows displayed: 2 out of 306

Viewing Reports

Mar 01, 2018

This section provides basic instructions for generating and viewing Virtual WAN reports about the local appliance using the Management Web Interface.

Note

Reports generated on the Management Web Interface apply to the local appliance, only. To generate and view reports for the Virtual WAN, use the Virtual WAN Center Web Interface.

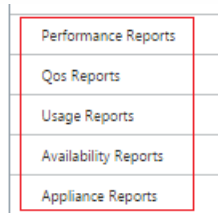
To generate and view Virtual WAN reports, do the following:

1. Log onto the Management Web Interface for the MCN, and select the **Monitoring** tab.

This opens the **Monitoring** navigation tree in the left pane.

2. Select a report type from the navigation tree.

The report types are listed as branches in the navigation tree, just below the **Flows** branch.



Performance Reports
QoS Reports
Usage Reports
Availability Reports
Appliance Reports

The available report types are as follows:

- **Performance Reports**
- **QoS Reports**
- **Usage Reports**
- **Availability Reports**
- **Appliance Reports**

3. Select the report options.

In addition to the various types of reports, for each report type there are numerous options and filters for refining report results.

Viewing Firewall Statistics

Mar 01, 2018

Once you have configured firewall and NAT policies you can view the statistics of the connections, firewall policies and NAT policies as reports. You can filter the reports using the various filtering parameters.

For information on configuring firewall and NAT policies, see [Stateful Firewall and NAT Support](#).

Connections

You can check the statistics for Applications for the Firewall Policy. This enables you to see all connections that match to the selected Application, where they are coming from, where they are going to, and how much traffic they are generating. You can see how the firewall policies are acting on the traffic for each Application.

You can filter the connections statistics using the following parameters:

- Application - The application used as filter criteria for the connection.
- Family - The application family the used as filter criteria for the connection.
- IP Protocol - The IP protocol used by the connection.
- Source Zone - The zone from which the connection originated.
- Destination Zone - The zone from which responding traffic originates.
- Source Service Type - The service from which the connection originated.
- Source Service Instance - The instance of the service from which the connection originated.
- Source IP - The IP address from which the connection originated, input in dotted decimal notation with an optional subnet mask.
- Source Port - The port or range of ports from which the connection originated. A single port or a range of ports using the "-" character is accepted.
- Destination Service Type - The service from which responding traffic originates.
- Destination Service Instance - The instance of the service from which responding traffic originates.
- Destination IP - The IP address of the responding device, input in dotted decimal notation with an optional subnet mask.
- Destination Port - The port or range of ports used by the responding device. A single port or a range of ports using the "-" character is accepted.

Filter Policies

Policies enable you to specify actions for traffic flows. Group of firewall filters are created using Firewall Policy Templates and can be applied to all sites in the network or only to specific sites.

You can view statistics report for all the filter policies and filter it using the following parameters.

- Application object - The Application object used as a filter criteria in the firewall policy.
- Application - The application used as a filter criteria in the firewall policy
- Family - The application family used as filter criteria in the firewall policy.
- IP Protocol - The IP protocol that the filter policy matches.
- DSCP: The DSCP tag that the filter policy matches.
- Filter Policy Action - The action taken by the policy when a packet matches the filter.
- Source Service Type - The service from which the connection originated.
- Source Service Name - The instance of the service from which the connection originated.
- Source IP - The IP address from which the connection originated, input in dotted decimal notation with an optional

subnet mask.

- Source Port - The port or range of ports from which the connection originated. A single port or a range of ports using the "-" character is accepted.
- Destination Service Type - The service to which responding traffic is destined.
- Destination Service Name - When applicable, the service to which responding traffic is destined.
- Destination IP - The IP address of the responding device, input in dotted decimal notation with an optional subnet mask.
- Destination Port - The port or range of ports used by the responding device. A single port or a range of ports using the "-" character is accepted.
- Source Zone - The origination zone matched by the filter policy.
- Destination Zone - The responding zone matched by the filter policy.

NAT Policies

You can view the statistics of all the Network Address Translation (NAT) policies and filter the report using the following parameters.

- IP Protocol - The IP protocol that the NAT policy matches.
- NAT Type - The type of NAT in use by the NAT policy.
- Dynamic NAT Type - The type of Dynamic NAT in use by the NAT policy.
- Service Type - The service type used by the NAT policy.
- Service Name - The instance of the service used by the NAT policy.
- Inside IP - The inside IP address, input in dotted decimal notation with an optional subnet mask.
- Inside Port - The inside port range used by the NAT policy. A single port or a range of ports using the "-" character is accepted.
- Outside IP - The outside IP address, input in dotted decimal notation with an optional subnet mask.
- Outside Port - The outside port range used by the NAT policy. A single port or a range of ports using the "-" character is accepted.

To view Firewall Statistics:

1. Navigate to **Monitoring > Firewall**.
2. In the Statistics field select, **Connections**, **Filter Policies** or **NAT Policies** as required.
3. Set the filtering criteria as require.

Monitoring > Firewall

Firewall Statistics

Statistics: **Connections**

Maximum entries to display: 50

Filtering:

Applications: Any Family: Any

IP Protocol: Any Source Zone: Any Destination Zone: Any

Source Service Type: Any Source Service Instances: Any Source IP: Source Port:

Destination Service Type: Any Destination Service Instances: Any Destination IP: Destination Port:

Show latest data Show Drops

[Help](#)

Connections

Application	Family	IP Protocol	Source				Destination				State	Is NAT	Sent			
			IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type			Service Name	Zone	Packets	Bytes
Unknown virtual protocol(unknown)	Standard	TCP	172.147.12.83	48546	Virtual Path	MCN-DC-Branch1	Any	172.147.21.53	2312	Local	VirtualInterface-1	Default_LAN_Zone	ESTABLISHED	No	57	3710

Connections Displayed: 1
Connections In Use: 1/128000

4. Click **Refresh**.

Diagnostic Tool

Mar 01, 2018

This diagnostic tool is used to generate test traffic which allows you to troubleshoot network issues that may result in:

- Frequent change in path state from Good to Bad.
- Poor application performance.
- Higher packet loss

Most often, these problems arise due to rate limiting configured on firewall / router, incorrect bandwidth settings, low link speed, priority queue set by network provider and so on. The diagnostic tool allows you to identify the root cause of such issues and troubleshoot it.

The diagnostic tool removes the dependency on third party tools such as iPerf which has to be manually installed on the Data Center and Branch hosts. It provides more control over the type of diagnostic traffic sent, the direction in which the diagnostic traffic flows, and the path on which the diagnostic traffic flows.

The diagnostic tool allows to generate the following two types of traffic:

- Control: Generates traffic with no QoS/scheduling applied to the packets. As a result, the packets are sent over the path selected in the UI, even if the path is not the best at the time. This traffic is used to test specific paths and helps to identify ISP related issues. You can also use this to determine the bandwidth of the selected path.
- Data: Simulates the traffic generated from the host with SD-WAN traffic processing. Since QoS/scheduling is applied to the packets, the packets are sent over the best path available at that time. Traffic will be sent over multiple paths if load balancing is enabled. This traffic is used to troubleshoot QoS/scheduler related issues.

Note

To run a diagnostic test on a path, you have to start the test on the appliances at both ends of the path. Start the diagnostic test as a server on one appliance and as a client on the other appliance.

To use diagnostics tool:

1. On both the appliances, click **Configuration > System Maintenance > Diagnostics > Diagnostics Tool**.

Configuration > System Maintenance > Diagnostics

Ping Traceroute Packet Capture Path Bandwidth System Info Diagnostic Data Events Alarms Diagnostics Tool

Diagnostics Tool

Tool Mode: Traffic Type: Port:

Iperf: WAN to LAN Paths: ✓

Results

```
-----
Server listening on TCP port 5001
Binding to local address 172.16.10.2
TCP window size: 85.3 KByte (default)
-----
```

2. In the **Tool Mode** field, select **Server** on one appliance and select **Client** on the other appliance.
3. In the **Traffic Type** field, select the type of diagnostic traffic, either **Control** or **Data**. Select the same traffic type on both the appliances.
4. In the **Port** field, specify the **TCP / UDP** port number on which the diagnostic traffic will be sent. Specify the same port number on both the appliances.
5. In the **Iperf** field, specify IPERF command line options, if any.

Note

You need not specify the following IPERF command line options:

- -c: Client mode option is added by the diagnostic tool.
- -s: Server mode option is added by the diagnostic tool.
- -B: Binding IPERF to specific IP/interface is done by the diagnostic tool depending on the path selected.
- -p: Port number is provided in the diagnostics tool.

6. Select the WAN to LAN paths on which you want to send the diagnostic traffic. Select the same path on both the appliances.
7. Click **Start** on both the appliances.

Improved Path Mapping and Bandwidth Usage

Mar 01, 2018

In NetScaler SD-WAN 10.0, path mapping and bandwidth usage enhancements have been implemented in the Monitoring tab to show traffic flows. For instance, when only one virtual path is serving a network connection, and if that virtual path becomes inactive, a new best path is chosen and the initial path becomes the last best path. This scenario is implemented when demand for bandwidth is less and when only one path is chosen

When more than one virtual path is serving a connection, you will notice one current best path and next best path, if available. If only one path exists to process traffic, assuming there are more than two paths processing traffic and the path table is updated with two paths, then the Monitoring tab in SD-WAN GUI for flows will display current best path as first path and the next comma separate path as the last best path. This scenario is implemented when there is a need for more paths with demand for bandwidth.

Monitoring DPI application information in SD-WAN GUI

The DPI application object name on the monitoring flow is stored and displayed in the SD-WAN GUI **Monitoring -> Flows** page. A tooltip is displayed to identify the DPI application.

The screenshot displays the SD-WAN GUI Monitoring -> Flows page. The left sidebar contains navigation options: Statistics, Flows (selected), Routing Protocols, Firewall, IKE/IPsec, IGMP, Performance Reports, Qos Reports, Usage Reports, Availability Reports, Appliance Reports, DHCP Server/Relay, and WAN Optimization. The main content area is titled 'Monitoring > Flows' and includes a 'Select Flows' section with the following settings: Flow Type (LAN to WAN, WAN to LAN, Internet Load Balancing Table, TCP Termination Table), Max Flows to Display (50), and a Filter (Optional) field. Below this is the 'Flows Data' section, which contains a table of flow data. The table has columns for 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, and Virtu: Path Overhe kbps. The table contains multiple rows of flow data, with a tooltip visible over one of the rows showing detailed DPI application information, including 'DPI Application = http'.

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 Separate TCP ACK Class = NO Packet Sequence Inorder = YES					361	41525	14427708	2.099	6.488	0.9
172.16.14.99	172.16.19.161	LAN to WAN	80	6310	TCP	Packet Sequence Inorder = YES Inorder Holdtime: 900 Late Packet Action = DISCARD					60	41827	14468200	2.115	6.341	0.9
172.16.14.99	172.16.19.170	LAN to WAN	80	10844	TCP						360	41863	14393387	2.110	6.285	0.9
172.16.14.99	172.16.19.164	LAN to WAN	80	3387	TCP	Late Packet Action = DISCARD Packet Duplication = NO Persistent Paths = NO					358	41798	14472656	2.070	6.284	0.8
172.16.14.215	172.16.19.99	LAN to WAN	9321	80	TCP	Reliable = YES TCP Standalone ACKs = NO Check Flow TOS = NO					14	43483	2592802	2.145	1.022	0.9
172.16.14.99	172.16.19.167	LAN to WAN	80	4200	TCP	Deep Packet Inspection = NO IP,TCP,UDP Header Compression = NO					312	41705	14426227	2.114	6.348	0.9
172.16.14.99	172.16.19.169	LAN to WAN	80	3161	TCP	GRE Header Compression = NO Packet Aggregation = NO					356	40970	14508376	2.054	6.299	0.8
172.16.14.218	172.16.19.99	LAN to WAN	3371	80	TCP	TCP Termination = NO Rule ID = 1 VLAN ID = 0					407	42980	2552820	2.043	0.967	0.8
172.16.14.99	172.16.19.166	LAN to WAN	80	1116	TCP						313	41286	14568312	2.047	6.220	0.8
172.16.14.213	172.16.19.99	LAN to WAN	17082	80	TCP	App Rule ID = N/A					361	42915	2556999	2.114	1.006	0.9
172.16.14.217	172.16.19.99	LAN to WAN	4090	80	TCP	DPI Application = http					364	42530	2540882	2.059	0.983	0.8

Monitoring Path information for traffic flow in SD-WAN GUI

It is possible that based on the incoming traffic rate demanding bandwidth, one or more paths will be required to process the traffic.

For determining how path mapping is performed, review the following scenarios:

Load Balanced Transmission mode

The following figure illustrates the scenario when traffic is initiated and all paths are good, one best path is chosen as bandwidth demand is enough to be served by one path. You will notice that only one path **DC-MCN-Internet -> BR1-VPX-Internet** is chosen and the type of transmission type is displayed as **Load Balanced**.

Select Flows																
Flow Type: <input checked="" type="checkbox"/> LAN to WAN <input checked="" type="checkbox"/> WAN to LAN <input type="checkbox"/> Internet Load Balancing Table <input type="checkbox"/> TCP Termination Table																
Max Flows to Display (Per Flow Type): 50																
Filter (Optional): <input type="text"/> Help																
<input type="button" value="Refresh"/>																
Flows Data																
<input type="button" value="Toggle Columns"/>																
Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
DC-MCN-BR1-VPX	LOCAL	3	291	435918	85.373	1023.106	36.881	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

The following figure illustrates when traffic is flowing, and the WAN attributes of the path are degraded, you will notice that a new path is chosen for processing traffic without disruption. In this case, the path mapping feature allows you to indicate that the current best path processing the traffic is **DC-MCN-Internet2 -> BR1-VPX-Internet** and the last best path that processed the traffic is **DC-MCN-Internet -> BR1-VPX-Internet**.

The last best path in this example is an indicator of which path served the connection earlier.

Select Flows																
Flow Type: <input checked="" type="checkbox"/> LAN to WAN <input checked="" type="checkbox"/> WAN to LAN <input type="checkbox"/> Internet Load Balancing Table <input type="checkbox"/> TCP Termination Table																
Max Flows to Display (Per Flow Type): 50																
Filter (Optional): <input type="text"/> Help																
<input type="button" value="Refresh"/>																
Flows Data																
<input type="button" value="Toggle Columns"/>																
Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application			
728	1090544	0.983	11.778	0.425	0.000	52	N/A	15	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf			

The following figure illustrates that when traffic is ongoing and more than one path is chosen for traffic processing due to demand in bandwidth, as shown below, more than one path is chosen as soon as the traffic is being sent. Unlike in the case above, here there may be more than two paths also serving the traffic but in the GUI only the two best paths that is currently serving the traffic is displayed.

Observe **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-Internet2->BR1-VPX-Internet** being the two paths shown in the **Flows Data** table.

Note

As indicated, only max two paths in the flows table are displayed.

Select Flows													
Flow Type: <input checked="" type="checkbox"/> LAN to WAN <input checked="" type="checkbox"/> WAN to LAN <input type="checkbox"/> Internet Load Balancing Table <input type="checkbox"/> TCP Termination Table													
Max Flows to Display (Per Flow Type): 50													
Filter (Optional): <input type="text"/> Help													
<input type="button" value="Refresh"/>													
Flows Data													
<input type="button" value="Toggle Columns"/>													
ets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
355	1280790	318.598	3818.082	137.634	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

The following figure illustrates that when traffic is still flowing, if the current best path which is **DC-MCN-Internet->BR1-VPX-Internet** is unavailable/inactive/degraded in WAN attributes, the current best path chosen will appear first in the path section of **Flows Data** table followed by the last best path which are currently serving the traffic.

Since the **DC-MCN-Internet->BR1-VPX-Internet** was not best anymore, a new current best path was chosen by the system as **DC-MCN-MPLS->BR1-VPX-MPLS**, and the last best path that is actively serving connection along with current best path is **DC-MCN-Internet2->BR1-VPX-Internet** as both are needed for the current traffic demand of bandwidth.

Select Flows													
Flow Type: <input checked="" type="checkbox"/> LAN to WAN <input checked="" type="checkbox"/> WAN to LAN <input type="checkbox"/> Internet Load Balancing Table <input type="checkbox"/> TCP Termination Table													
Max Flows to Display (Per Flow Type): 50													
Filter (Optional): <input type="text"/> Help													
<input type="button" value="Refresh"/>													
Flows Data													
<input type="button" value="Toggle Columns"/>													
ackets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2764	4140472	170.434	2042.476	73.627	0.000	52	N/A	15	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

Duplicate Transmit Mode

General packet duplication mode ensures that two paths are initially taken for processing packets of the same connection to ensure reliable delivery by duplicating packets across two separate paths.

For Path Mapping, you will notice that two paths being taken in the path section of the flow table as long as two paths exist to process flows by duplicating.

The following figure illustrates that when traffic is flowing, it can be noticed that two paths are shown to be processing the traffic. Unlike any other mode, even if traffic demands less bandwidth that can be provided by just one path, this mode will always duplicate traffic across two paths for reliable application delivery.

You will notice in the figure below, two paths in the path section of the **Flows Data** table; **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	Duplicate, Reliable	iperf

The following figure illustrates that when traffic is flowing, if one of the current best path becomes inactive, another path will be chosen and there still be two paths as part of the path section in the **Flows Data** table.

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	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	Duplicate, Reliable

Persistent Path Transmit Mode

Persistent path transmit mode helps to retain packets of a flow based on path latency impedance.

The following figure illustrates only one path which is the best path currently handling the flows and its packets. There is no demand of bandwidth and one path will serve it all. Currently there is only one best path which is **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

The following figure illustrates that if the path **DC-MCN-Internet->BR1-VPX-Internet** becomes latency prone or is disabled, you will notice that new path takes effect and the current path **DC-MCN-Internet->BR1-VPX-Internet** becomes the last best path.

So the new path section will show **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

In persistent mode there can be more than one path chosen to process traffic. In that case, the GUI will display both the paths with best and next best in the path section of the flow table from the beginning of the traffic flow.

The following figure illustrates that the flow initially only needs more than two paths and they will stay persistent as long as there is no path latency impedance crossing (50ms). The two paths taken are shown as; **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

Assume that one of the best paths **DC-MCN-Internet** goes into high latency or is disabled. This will make a new path appear and the new path may be the best path or could be the second best path based on the decision of path selection at that instant of time.

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

DPI Applications in SD-WAN Center

In earlier releases, around 4000 applications and configured with 800 services (550 Virtual Paths, 256 Intranet Services) can be identified. Storing this data would impact overall system performance (CPU cycles and disk space needed to store the data). This also has an impact, if reporting on data per Usage or Path is supported.

In SD-WAN 10.0, the per service reporting is limited to the top 100 applications at the service level, While the data path provides information on every application gathered in a minute, the per minute stats reporting determines the top 100 applications and report on the aggregate of all other applications as "other". If there is high diversity of trackable applications in their network, this might affect clarity of data, particularly if we want to track/graph the usage of an application over time and the application falls out of the top 100 limit.

Troubleshooting Management IP

Mar 01, 2018

The following are the possible scenarios that you might encounter when configuring DHCP IP address. It also includes best practices and recommendations for configuring DHCP Management IP address when deploying SD-WAN appliances.

These recommendations are applicable to all platform models of SD-WAN; Standard Edition, WANOP, and Enterprise Edition - Physical and Virtual appliances.

Note

All hardware models of SD-WAN appliances are shipped with a factory default management IP address. Ensure that you configure the required DHCP IP address for the appliance during the setup process.

All Virtual models of SD-WAN appliances (VPX models) and appliances which can be deployed in AWS environment do not have a factory default IP address assigned.

Appliances power on without DHCP server(s) reachable

- Causes:
 - Ethernet management cable is disconnected
 - DHCP service is down for the connected network
- Expected behavior
 - Appliances with DHCP service enabled will retry DHCP request every 300 seconds (default value). The actual interval is approximately 7 minutes
 - Therefore, appliances with DHCP service enabled will acquire DHCP addresses within 7 minutes after DHCP server(s) become available. The delay ranges from 0 to 7 minutes

Assigned DHCP address expires

- Expected behavior:
 - Appliances with DHCP service enabled will try to renew the lease before the address expires
 - Appliances start with new DHCP discovery, if the renew fails

Appliances with DHCP service enabled move from one DHCP enabled subnet to another subnet:

- Causes: Appliances move from an assigned DHCP subnet to a different DHCP subnet
- Expected behavior:
 - A permanent lease DHCP IP address assignment might require the appliances to be rebooted to acquire an IP address from the new DHCP server.
 - Upon DHCP lease expiration, appliances might re-initiate DHCP discovery protocol, if current DHCP server is not reachable.
 - Appliances will acquire new IP addresses with a delay of 8 minutes. The gateway IP address is not modified in the GUI and CLI. It is updated after the reboot process is completed.

Recommendation

- Always assign permanent lease for DHCP addresses assigned to SD-WAN appliances (physical/virtual). This will allow appliances to have predictable management IP address.

Best Practices

Mar 29, 2018

The following topics provide the best practices to be followed when the NetScaler SD-WAN solution is being designed, planned, and executed in your network.

[Security](#)

[Routing](#)

[QoS](#)

[WAN Links](#)

Security

Mar 29, 2018

This article outlines security best practices for the NetScaler SD-WAN solution. It provides general security guidance for NetScaler SD-WAN deployments.

NetScaler SD-WAN Deployment Guidelines

To maintain security through the deployment lifecycle, Citrix recommends the following security consideration:

- Physical Security
- Appliance Security
- Network Security
- Administration and Management

Physical Security

Deploy NetScaler SD-WAN Appliances in a Secure Server Room - The appliance or server on which NetScaler SD-WAN is installed, should be placed in a secure server room or restricted data center facility, which protects the appliance from unauthorized access. At the minimum, access should be controlled by an electronic card reader. Access to the appliance should be monitored by CCTV that continuously records all activity for auditing purposes. In the event of a break-in, electronic surveillance system should send an alarm to the security personnel for immediate response.

Protect Front Panel and Console Ports from Unauthorized Access - Secure the appliance in a large cage or rack with physical-key access control.

Protect Power Supply - Make sure that the appliance is protected with an uninterruptable power supply (UPS).

Appliance Security

For appliance security, secure the operating system of any server hosting a NetScaler SD-WAN virtual appliance (VPX), perform remote software updates, and following secure lifecycle management practices:

- Secure the Operating System of Server Hosting a NetScaler SD-WAN VPX Appliance - A NetScaler SD-WAN VPX appliance runs as a virtual appliance on a standard server. Access to the standard server should be protected with role based access control and strong password management. Additionally, Citrix recommends periodic updates to the server with the latest security patches for the operating system, and update-to-date antivirus software on the server.
- Perform Remote Software Updates - Install all security updates to resolve any known issues. Refer to the Security Bulletins web page to sign up and receive up-to-date security alerts.
- Follow Secure Lifecycle Management Practices - To manage an appliance when redeploying, or initiating RMA, and decommissioning sensitive data, complete the data-remediation countermeasures by removing the persistent data from the appliance.

Network Security

For network security, do not use the default SSL certificate. Use Transport Layer Security (TLS) when accessing the administrator interface, protect the appliance's non-routable management IP address, configure a high availability setup, and implement Administration and Management safeguards as appropriate for the deployment.

- Do not use the NetScaler Default SSL Certificate - An SSL certificate from a reputable Certificate Authority simplifies

the user experience for Internet-facing Web applications. Unlike the situation with a self-signed certificate or a certificate from the reputable Certificate Authority, web browsers do not require users to install the certificate from the reputable Certificate Authority to initiate secure communication to the Web server.

- Use Transport Layer Security when Accessing Administrator Interface - Make sure that the management IP address is not accessible from the Internet or is at least protected by a secured firewall. Make sure that the LOM IP address is not accessible from the Internet or is at least protected by a secured firewall.
- Secure Administration and Management Accounts – Create an alternative admin account, set strong passwords for admin and viewer accounts. When configure remote account access, consider configuring externally authenticated administrative management of accounts using RADIUS and TACAS. Change the default password for the admin user accounts, configure NTP, use the default session timeout value, use SNMPv3 with SHA Authentication and AES encryption.

NetScaler SD-WAN overlay network protects data traversing the SD-WAN overlay network.

Secure Administrator Interface

For secure web management access, replace default system certificates by uploading and installing certificates from a reputable Certificate Authority.

Configuration > Appliance Settings > Administrator Interface:

User Accounts:

- Change local user password
- Manage users

HTTPS Certs:

- Certificate
- Key

Miscellaneous:

- Web Console Timeout

Dashboard Monitoring Configuration

Configuration > Appliance Settings > Administrator Interface

User Accounts RADIUS TACACS+ **HTTPS Cert** HTTPS Settings Miscellaneous

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: C5:81:F3:F1:CA:6B:28:FD:7F:9E:6A:A7:3C:28:31:A4:C6:97:A6:67
 Start Date: Sep 30 20:17:07 2016 GMT
 End Date: Sep 28 20:17:07 2026 GMT
 Serial Number: FF34446D72B96EA0

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.

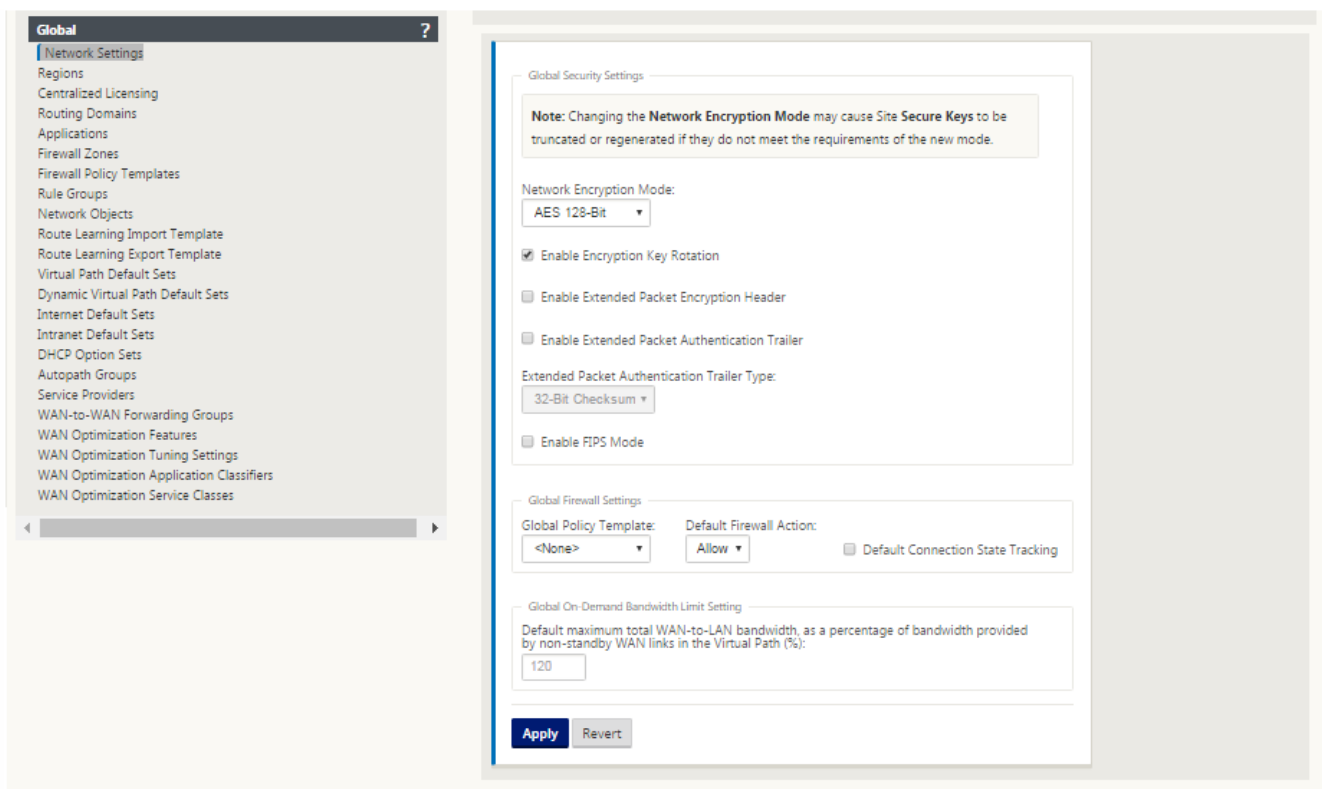
Configuration Editor > Global > Network Settings

Global Firewall Settings

- Global Policy Template
- Default Firewall Actions
- Default Connection State Tracking

Global Virtual Path Encryption Settings

- AES 128-bit (default)
- Encryption Key Rotation (Default)
- Extended Packet Encryption Header
- Extended Packet Authentication Trailer



Global virtual Path Encryption Settings

- AES-128 data encryption is enabled by default. It is recommended to use AES-128 or additional protection of AES-256 encryption level for path encryption. Ensure that “enable Encryption Key Rotation” is set to ensure key regeneration for every Virtual Path with encryption enabled using an Elliptic Curve Diffie-Hellman key exchange at intervals of 10-15 minutes.

If the network requires message authentication in addition to confidentiality (i.e. tamper protection), Citrix recommends using IPsec data encryption. If only confidentiality is required, Citrix recommends using the enhanced headers.

- Extended Packet Encryption Header enables a randomly seeded counter to be prepended to the beginning of every encrypted message. When encrypted, this counter will serve as a random initialization vector, deterministic only with the encryption key. This will randomize the output of the encryption, providing strong message indistinguishability. Keep in mind that when enabled this option will increase packet overhead by 16 bytes
- Extended Packet Authentication Trailer appends an authentication code to the end of every encrypted message. This trailer allows for the verification that packets are not modified in transit. Keep in mind this option will increase packet overhead.

Firewall Security

The recommended Firewall configuration is with a default Firewall action as deny all at first, then add exceptions. Prior to adding any rules, document and review the purpose of the firewall rule. Use Stateful inspection and Application level inspection where possible. Simplify rules and eliminate redundant rules. Define and adhere to a change management process that tracks and allows for review of changes to Firewall settings. Set the Firewall for all appliances to track connections through the appliance using the global settings. Tracking connections verifies that packets are properly formed and are appropriate for the connection state. Create Zones appropriate to the logical hierarchy of the network or functional areas of the organization. Keep in mind that zones are globally significant and can allow geographically disparate networks to be treated as the same security zone. Create the most specific policies possible to reduce the risk of

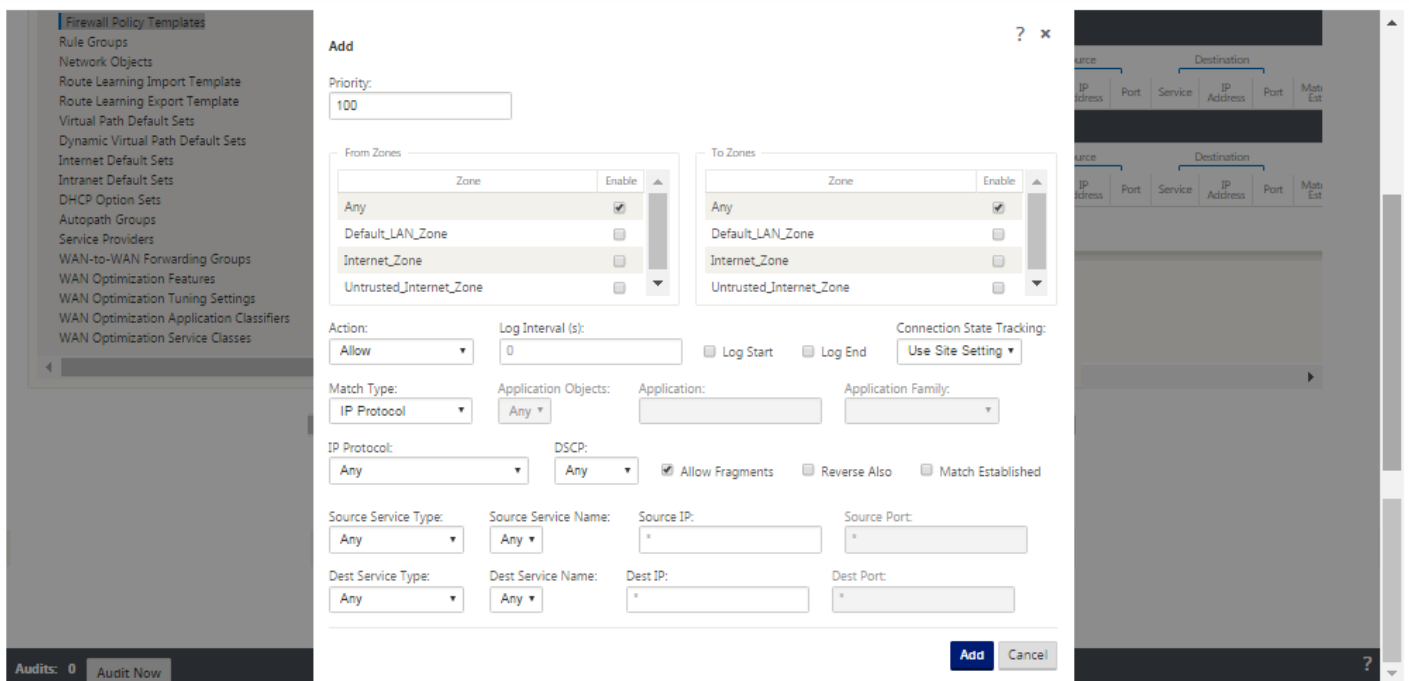
security holes, avoid the use of Any in Allow rules. Configure and maintain a Global Policy Template to create a base level of security for all appliances in the network. Define Policy Templates based on functional roles of appliances in the network and apply them where appropriate. Define Policies at individual sites only when necessary.

Global Firewall Templates - Firewall templates allow for the configuration of global parameters that impact the operation of the firewall on individual appliances operating in the SD-WAN overlay environment.

Default Firewall Actions – Allow enables packets not matching any filter policy are permitted. Deny enables packets not matching any filter policy are dropped.

Default Connection State Tracking – Enables bidirectional connection state tracking for TCP, UDP, and ICMP flows that do not match a filter policy or NAT rule. Asymmetric flows will be blocked when this is enabled even when there are no Firewall policies defined. The settings may be defined at the site level which will override the global setting. If there is a possibility of asymmetric flows at a site, the recommendation is to enable this at a site or policy level and not globally.

Zones - Firewall zones define logical security grouping of networks connected to the NetScaler SD-WAN. Zones can be applied to Virtual Interfaces, Intranet Services, GRE Tunnels, and LAN IPsec Tunnels.



WAN Link Security Zone

Untrusted security zone should be configured on WAN links directly connected to a public (unsecure) network. Untrusted will set the WAN link to its most secure state, allowing only encrypted, authenticated and authorized traffic to be accepted on the interface group. ARP and ICMP to the Virtual IP Address are the only other traffic type allowed. This setting will also ensure that only encrypted traffic will be send out of the interfaces associated with the Interface group.

Routing Domains

Routing Domains are network systems that include a set of routers that are used to segment network traffic. Newly created sires are automatically associated with the default Routing Domain.

Configuration Editor > Global

Routing Domains

- Default_RoutingDomain

IPsec Tunnels

- Default Sets
- Secure Virtual Path User Data with IPsec

The top screenshot shows the 'Global' configuration page with the 'Routing Domains' section selected in the left sidebar. A table lists the 'Default_RoutingDomain' with 'Default' and 'Redirect to WANOP' checkboxes checked. The bottom screenshot shows the 'Virtual Path Default Sets' configuration page for 'Scale_VP_default_set' in the 'IPsec Settings' section. The 'Secure Virtual Path User Data with IPsec' checkbox is checked, and the configuration includes 'Encapsulation Type: ESP', 'Encryption Mode: AES 128-Bit', 'Hash Algorithm: SHA1', and 'Lifetime (s): 28800'.

IPSec Tunnels

IPsec Tunnels secure both user data and header information. NetScaler SD-WAN appliances can negotiate fixed IPsec tunnels on the LAN or WAN side with non-SD-WAN peers. For IPsec Tunnels over LAN, a Routing Domain must be selected. If the IPsec Tunnel uses an Intranet Service, the Routing Domain is pre-determined by the chosen Intranet Service.

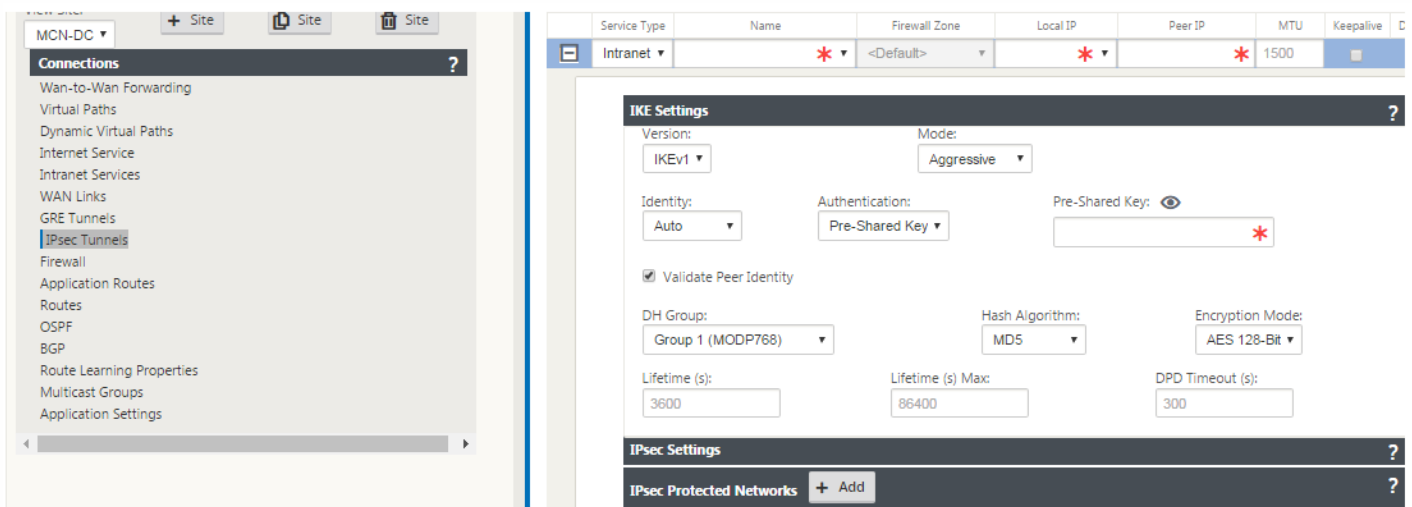
IPsec tunnel is established across the Virtual Path before data can flow across the SD-WAN overlay network.

- Encapsulation Type options include ESP - data is encapsulated and encrypted, ESP+Auth – data is encapsulated, encrypted, and validated with an HMAC, AH – data is validated with an HMAC.
- Encryption Mode is the encryption algorithm used when ESP is enabled.
- Hash Algorithm is used to generate an HMAC.
- Lifetime is a preferred duration, in seconds, for an IPsec security association to exist. 0 can be used for unlimited.

IKE Settings

Internet Key Exchange (IKE) is an IPsec protocol used to create a security association (SA). NetScaler SD-WAN appliances support both IKEv1 and IKEv2 protocols.

- Mode can be either Main Mode or Aggressive Mode.
- Identity can be automatic to identify peer, or an IP address can be used to manually specify peer's IP address.
- Authentication enables Pre-Shared Key authentication or certificate as the method of authentication.
- Validate Peer Identity enables validation of the IKE's Peer Identity if the peer's ID type is supported, otherwise do not enable this feature.
- Diffie-Hellman Groups are available for IKE key generation with group 1 at 768-bit, group 2 at 1024-bit, and group 5 at 1536-bit group.
- Hash Algorithm include MD5, SHA1, and SHA-256 has algorithms are available for IKE messages.
- Encryption Modes include AES-128, AES-192, and AES-256 encryption modes are available for IKE messages.
- IKEv2 settings include Peer Authentication and Integrity Algorithm.



Configuring Firewall

Following common issues can be identified by verifying upstream Router and Firewall configuration:

- MPLS Queues/QoS settings: Verify that UDP encapsulated traffic between SD-WAN Virtual IP addresses does not suffer due to QoS settings on the intermediate appliances in the network.
- All traffic on the WAN links configured on the SD-WAN network should be processed by the NetScaler SD-WAN appliance using the right service type (Virtual Path, Internet, Intranet, and Local).
- If traffic has to bypass the NetScaler SD-WAN appliance and use the same underlying link, proper bandwidth reservations for SD-WAN traffic should be made on the router. Also, the link capacity should be configured accordingly in SD-WAN configuration.
- Verify that the intermediate Router/Firewall does not have any UDP flood and/or PPS limits enforced. This will throttle the traffic when it is sent through the Virtual Path (UDP encapsulated).

Routing

Mar 29, 2018

Internet/Intranet Routing Service

When the Internet service is not configured to Internet bound traffic and instead, either a “**Local**” route or a “**Passthrough**” route is configured to reach the gateway router. The router uses the WAN links configured on the SD-WAN appliance, leading to link over-subscription issue.

If an Internet route is configured as “**Local**” at the MCN, it is learned by all the branch SD-WAN sites and configured as “**Virtual Path Route**” by default. This implies that Internet bound traffic at the branch appliance is routed through the Virtual Path to MCN.

Routing Precedence

The order of routing precedence:

- Prefix Match: longest prefix match.
- Service: Local, Virtual Path service, Internet, Intranet, Passthrough
- Route Cost

Routing Asymmetry

Ensure that there is no routing asymmetry in the network (NetScaler SD-WAN appliance is transmitting traffic in only one direction). This creates issues with Firewall connection tracking, and deep packet inspection.

QoS

Mar 29, 2018

Configuring QoS

Consider the following when configuring QoS:

- Understand your network traffic patterns and requirement. You might have to observe the **QoS class statistics**, and change queue depths, and/or change the default QoS class share percentage to avoid tail-drops as shown in QoS statistics.
- Sometimes, the entire subnet is added to a Rule for ease of configuration instead of creating Rules for particular application IP addresses. Adding entire subnet to a rule incorrectly maps all the traffic in the subnet to one Rule. Therefore the QoS classes associated with that Rule might lead to tail drop and poor application performance or user experience.

WAN Links

Mar 29, 2018

Configuring Links

Points to remember while configuring WAN links:

- Configure the **Permitted** and **Physical** rate as the actual WAN link bandwidth. In cases where the entire WAN link capacity is not supposed to be used by the NetScaler SD-WAN appliance, change the **Permitted** rate accordingly.
- When you are unsure of the bandwidth and if the links are non-reliable, you can enable the **Auto Learn** feature. The **Auto Learn** feature learns the underlying link capacity only, and uses the same value in the future.
- If the underlying link is not stable and does not guarantee fixed bandwidth (for example; 4G links), use the **Adaptive Bandwidth Detection** feature.
- It is not recommended to enable **Auto Learn** and Adaptive **Bandwidth Detection** on the same WAN link.
- If the underlying link is not stable, change the following Path settings:
 - * Loss Settings
 - * Disable Instability Sensitive
 - * Silence time
- Use **Diagnostic tool** to check the link health/capacity.
- If NetScaler SD-WAN is deployed in **one-arm** mode, ensure that you do not overrun the physical capacity of the underlying link.

Verifying ISP Link Health

For new deployments, earlier than SD-WAN deployment and when adding new ISP link to the existing SD-WAN deployment:

- Verify the link type. For example; MPLS, ADSL, 4G.
- Network characteristics. For example - bandwidth, loss, latency, and jitter.

This information helps in configuring the SD-WAN network as per your requirements.

Network Topology

It is commonly observed that specific network traffic bypasses the NetScaler SD-WAN appliances, and uses the same underlying link configured in the SD-WAN network. Because SD-WAN does not have complete visibility over link utilization, there are chances that SD-WAN oversubscribes the link leading to performance and PATH issues.

Provisioning

Points to consider while provisioning SD-WAN:

- By default, all branches and WAN services (Virtual Path/Internet/Intranet) receive equal share of the bandwidth.
- Provisioning sites needs to be changed, when there is high disparity in terms of bandwidth requirement or availability between the connecting sites.
- When dynamic virtual paths are enabled between maximum available sites, the WAN link capacity is shared between the static virtual path to DC and the dynamic virtual paths.

FAQs

Apr 20, 2018

High Availability

What is the difference between High Availability and Secondary (Geo) appliance?

- High Availability ensures fault tolerance. Secondary (Geo) appliance enables disaster recovery.
- High Availability can be configured for the MCN, RCN, and branch appliances. Secondary (Geo) appliance can be configured for MCN and RCNs only.
- High Availability appliances are configured within the same site or geographical location. A branch appliance in a different geographical location is configured as Secondary (Geo) MCN/ RCN appliance.
- High Availability primary and secondary appliance should be the same platform models. The Secondary (Geo) appliance might or might not be the same platform model as the primary MCN/RCN.
- High Availability has higher priority over secondary (Geo). If an appliance (MCN/RCN) is configured with High Availability and Secondary (Geo) appliance, when the appliance fails the secondary high availability appliance becomes active. If both the high availability appliances fail or if the Data Center site crashes, the secondary (Geo) appliance becomes active.
- In High Availability, the primary/secondary switchover happens instantaneously or within 10-12 seconds depending upon the high availability deployment. The primary MCN/RCN to secondary (Geo) MCN/RCN switch over, happens after 15 seconds of the primary being inactive.
- High Availability configuration allows you to configure primary reclaim. You cannot configure primary reclaim for Secondary (Geo) appliance, the primary reclaim happens automatically after the primary appliance is back and the hold timer expires.

Single Step Upgrade

Note

The WANOP, SVM, and XenServer Supplemental/HFs are seen as OS Components.

Should I use *.tar.gz*, or single step upgrade *.zip* package to upgrade to 9.3.x from my current version (8.1.x, 9.1.x, 9.2.x)?

Use the *.tar.gz* files of the concerned platforms to upgrade the SD-WAN software to 9.3.x. After the SD-WAN software is upgraded to 9.3.x version, perform change management using the *.zip* package to transfer/stage OS component software packages. After activation, the MCN transfers/stages OS components for all the relevant branches.

After upgrading to 9.3.0 using single step upgrade package (.zip file) do, I need to perform *upg* upgrade on each appliance?

No, OS software update/upgrade will be taken care by the single step upgrade *.zip* package and it is installed as per the scheduling details provided by you in the Change Management Settings of the respective sites.

Why should I use *.tar.gz* followed by *.zip* package to upgrade from earlier than 9.3 to 9.3.x, and why not directly use *.zip* package of 9.3.x?

Single Step upgrade package is supported from 9.3.0.161 onwards and on earlier release versions (prior to release 9.3) this

package is not recognized. When the single step upgrade *.zip* package is uploaded into the Change Management inbox, the system throws an error stating that the package is not recognized. Hence, first upgrade the SD-WAN software to 9.3 or above version and then perform Change Management using the *.zip* package.

How will the OS Components be installed through single step upgrade, if *.upg* upgrade is not performed?

The MCN will transfer/stage OS components software packages based on the appliance model, after the Change Management is completed using single step upgrade *.zip* package. After activation, the MCN starts transferring/staging the OS components software packages for the branches that need them for the scheduled update/upgrade.

How do I install OS components, without scheduling for later installations?

Set the **Maintenance Window** value to '0' for instant installation of the OS components.

Note

The installation starts only when the appliance has received all the package that are needed for the site, even when **Maintenance Window** value is set to '0'.

What is the use of scheduling installation? Can I use schedule instructions to upgrade VW alone?

Scheduled installation was introduced in SD-WAN release 9.3, and is applicable for OS components only and not for VW software upgrade. With single step upgrade, you need not log into each appliance to perform OS components upgrade and the scheduling option allows you to schedule the OS components installation at a different time other than VW software version upgrade.

Why does the scheduling information in Change Management Settings page appears past schedule date by default and what does it mean?

The **Change Management Settings** page displays the default scheduling information that is, *"start": "2016-05-21 21:20:00," "window": 1, "repeat": 1, "unit": "days"*. If the date is a past date it means that, the scheduled installation is based on the time and other parameters like maintenance window, repeat window, and unit and not the date.

What is default schedule installation date/time set to, is it generic or local appliance dependent?

By default the scheduling details is set as *'2016-05-21 at 21:20:00 (Maintenance window of 1 hour and repeated every 1 day)'*. This detail is local appliance site dependent.

How can I install OS Components immediately without waiting for the maintenance / scheduled window?

Set the **Maintenance Window** value to '0' in **Change Management Setting** page, this overrides the scheduled installation time.

Which package I should use for upgrade when current software version is 9.3.x or above?

Use single step upgrade *.zip* package to upgrade to any higher versions when the current software version 9.3.x or above.

When does the OS Components files get transferred/staged to the branches?

The OS components files are transferred/staged to relevant branches after the activation is completed when Change

Management is done using single step upgrade .zip package to upgrade the system.

Which appliances receive OS Components files? Is it platform dependent or all branches receive it .

Appliances that are hypervisor based, such as **SD-WAN – 400, 800, 1000, 2000 SE** and Bare metal **SD-WAN - 2100** running on EE license will receive OS components to upgrade.

How does scheduling work?

By default the scheduling details is set as *'2016-05-21 at 21:20:00 (Maintenance window of 1 hour and repeated every 1 day)'* and it implies that the system will check if new software is available for installation every day as repeat value is set to **'1 days'** and will have maintenance window of **'1 hours'** and the installation will get triggered/attempted (if new software is available) at **21:20:00** (local appliance time) effective from **'2016-05-21'**

How do I get to know if the OS Components have been upgraded?

In the **Status** column, you can see a green tick mark. On hovering over it, you can see the *'Upgrade is Successful'* message.

How can I schedule installation of OS components for RCN and its Branches?

Scheduling for RCN is performed from the MCN **Change Management Settings** page. For RCN branches, you need to log into respective RCN and set the schedule details.

From where can I get the status of scheduled installation?

Status of scheduled installation for RCN can be obtained from the MCN **Change Management Settings** page. For RCN branches, you need to log in to respective RCN to get the status.

How do I get status of scheduled installation?

Use the refresh button provided on the **Change Management Settings** page to get status from MCN, and RCN for Branches in Default Region and RCN respectively.

Scheduling Information				
Show	100	entries	Search	<input type="text"/>
			Edit Selected	Refresh
<input type="checkbox"/>	Site Name	Scheduling Information	Status	Edit
<input type="checkbox"/>	GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries

Previous 1 Next

Can I use *tar.gz* file to upgrade to next release, when single step upgrade was used for previous software upgrade?

You can use *tar.gz* file to upgrade, but it is not recommended because you can perform software upgrade by using the *.upg* file. Upload to upgrade operating system (OS) component software by logging into each applicable appliance. From release 9.3 version 1, the '**Update Operating System Software**' page is deprecated. As a result, you can perform change management by using the *.zip* package to upgrade OS components.

How can we validate the current running versions of OS Components?

Now you cannot validate the current running versions of OS components from the UI. You can log in from each console or get STS to view this information.

What difference it would make if I have bare metal appliances in my network? Does scheduling impact bare metal / Virtual appliances?

Bare Metal appliances like **SD-WAN – 410,2100,4100,5100 SD-WAN** run only SD-WAN software. Bare metal appliances do not need OS components packages. These platforms are treated on par with SD-WAN VPX-SE appliances in terms of software need. The MCN will not transfer OS components packages to these appliances. Setting scheduling information will not take effect for these appliances, because they do not have any OS components that need upgrade.

How does SSU work in high availability environment / deployment?

In high availability deployment at MCN, we have a limitation, where the active MCN switch's/toggles the role of primary MCN during Change Management and Standby/Secondary MCN takes over. In this case, you can perform Change Management once again with the *.zip* package on the active MCN for the packages or you can switch back to primary MCN by toggling the role of active MCN so that original primary MCN can take up the role for the OS components packages to be staged to other branches.

How does single step upgrade work in high availability environment / deployment?

While performing single step upgrade in high availability deployment, the role of the primary MCN and the Standby MCN is toggled. This is a limitation. If this happens, perform Change Management again with the *.zip* package on the active MCN. Alternatively, you can switch back to the primary MCN by toggling the role of the active MCN so that the original primary MCN can stage OS components packages to the branches.

Is single step upgrade support for zero-touch deployment to restart strap the appliances?

Yes, it can be used.

Can I use single step upgrade to upgrade my standalone WANOP appliance?

No.

Can I use single step upgrade to upgrade standalone WANOP appliance deployed in two Box mode?

No. Only SD-WAN appliance which is part of two box mode would be upgraded and not the WANOP standalone appliance.

Which package should I use to upgrade to multi-tier network?

Use the single step upgrade package *ns-sdw-sw-<release-version>.zip* file when the current software version is 9.3.x or above. MCN takes care of staging package to RCN and RCNs stage software package to its respective branches.

After uploading the *ns-sdw-sw-<release-version>.zip* file, I am seeing only one platform model under current software?

From release 10.0, support for scale architecture is introduced to speed up processing of single step upgrade. You can see only the MCN platform model under current software. Other appliance packages are listed/displayed/processed when you choose the **Verify** or **Stage Appliance** button.

For VPX/VPXL/Bare Metal appliances, which packages are staged for RCN?

Package is staged to RCNs because RCNs Branches can be of any platform model. Hence they need all packages.

How does my Branch site behind the RCN obtain OS component packages if RCN is a VPX appliance, and Branch is an appliance that needs these packages?

RCN stages the relevant package to the branch that needs the OS component packages after activation of SD-WAN VW software package.

Can I choose Ignore Incomplete during staging and proceed to next stage of change Management? What impact does it have for sites that have not completed staging when this button is selected?

Yes, you can click **Ignore Incomplete**. This enables **Next** button and the Progress bar is displayed. This option is provided for scenarios where the site is not reachable and change management is still waiting for staging to complete for those site, so users can proceed to next stage by ignoring the stage state and proceed to activation. After the site comes up, MCN stages the package after completion of activation.

Partial Software Upgrade

What is partial site upgrade and how can I use it?

Partial Site Software upgrade is a new feature introduced in release 10.0. You can stage newer version of release 10.x from

the MCN and activate staged software version from **Local Change Management** page on selected sites/branches. Before activating staged software on site/branch, ensure that check box is enabled from MCN.

- This feature is disabled by default. The existing correction mechanism keeps the network in sync. The user has to choose to allow partial site upgrades by enabling a check box on the “**Configuration -> Change Management Settings**” page.
- Partial Software Upgrade can be done only on a Branch or RCNs and not at the MCN.

Below is the usecase/scenario when partial site software upgrade can be used

Validate if a software patch with relevant changes is compatible and working for a specific site (where partial site upgrade is done). Validate that the upgraded software is working as expected. This helps validate the new software and fix at a specific site before upgrading entire network with the new software.

Can I use this feature to upgrade from

- 10.0 to 10.x
- 10.0.x to 10.0.y
- 10.x to 11.y
- All of the above

Partial Site Software Upgrade is applicable only when appliance is running software release 10.x and newer, and can be used within the same major version of software. It can be used between releases 10.0 to 10.0.x/10.x. Only as part of partial site software upgrade, configuration cannot be changed. This feature is good when active software version is 10.x.y, and Staged software version is 11.x or higher as long as there is no change in the control protocol.

Can I test new feature to test as part of partial software upgrade by enabling them from the config?

No, partial software upgrade requires that now Active and Staged config to be identical. Only software version can change.

Can I disable Partial Software Upgrade for RCN?

No, Partial Software Upgrade can be enabled or disabled from MCN only. At RCN the feature is in read-only mode.

Can I use Partial Software Upgrade when I have active as 9.3.x and 10.0.x as staged?

No, the appliance should be running on release 10.0 as active software.

What happens when Partial Software Upgrade option is disabled from MCN, while some branches are already upgraded through this feature?

MCN sends notification to all appliances in the network that Partial Software Upgrade feature is disabled, and then all appliances in the network are auto-corrected by MCN to match to its active and staged version. However, note that MCN is expecting for Activate Staged option to be clicked from Activation page of **Change Management**. You can choose to activate the network by clicking **Activate Staged** button or click **Change Preparation** to cancel state by accepting the confirmation.

Change Management Roll Back

What is rolled back feature in Change management process?

From release 9.3, the Change management roll back feature enables roll back to the Working Configuration when unexpected events such as, t2-app crash or Virtual path state becomes inactive after a configuration

update. The network and the appliances are monitored for 10 mins after the Configuration update and during that interval if the following conditions are met (provided user has enabled the feature), the Staged configuration will be activated. The Active software is rolled back to Staged.

What is the criteria for this roll back to restart?

The rollback occurs, if the following scenarios are encountered:

1. MCN - After config/software change, if t2_app service gets disabled due to crash within 10 min interval.
2. MCN - After config/software change, if Virtual Path service is down for 10 minutes or longer after activation. The Rollback feature is initiated at the sites.
3. Site - After config/software change, if the Site loses its communication with MCN, then the rollback feature is initiated.
4. Site - After config/software change t2_app service gets disabled due to crash within 10 min interval.

What happens after rollback?

After configuration rollback, the faulty config/software is presented as Staged software.

How are users notified that roll back occurred?

A yellow banner at the top in the GUI saying Config is rolled back due to respective errors is displayed. Also, you can see it is change management status table. It shows **Configuration Error** or **Software error** corresponding to the site for which roll back occurred.

Does config and software both get rolled back?

Yes, if software upgrade is also performed along with configuration, and roll back scenario is encountered then Software also gets rolled back.

What happens if there is an issue in MCN and it crashes or loses connectivity with all the sites?

The entire network is rolled back except MCN. Notification is displayed, and all the sites show roll back status in the change management section. You can resolve the issue on MCN manually.

Can we disable this feature?

Yes, we can disable this feature just before activation. However, by default this feature is enabled.

How does roll back interact with Partial Software Upgrade when I have multi-tier network?

- If partial software upgrade is disabled, and if a site in a region (or the RCN) rolls back, the region with the problem is rolled back and once completed the rollback propagates up to the MCN. As a result, the MCN and the rest of the network to rolled back. Both the RCN in the region that rolled back, and the MCN display the rollback banner that the MCN cannot auto-dismiss the rollback banner at the RCN.
- If partial software upgrade is enabled, and if a site in a region (or the RCN) rolls back, only that region is rolled back. The rollback event does not propagate back to the MCN. As a result, the MCN leaves the region. The MCN does not show rollback banner and does not roll back itself or the network.

In both these scenarios, the RCN displays the rollback banner until it is dismissed. Because, it cannot be auto-dismissed by MCN.

2100 Enterprise Edition

What does the following message indicate when a 2100 EE appliance is upgraded to release 10.0?

EE provisioning error: WO redirection is enabled but WO is not provisioned. Please use single step upgrade to upgrade your network.

Clear Warning

Appliance has EE license or WANOP redirection is enabled from MCN. You can schedule installation of WANOP components to start provisioning WANOP features on this platform.

Reference Material

Mar 01, 2018

 [Application Signature Library](#)

A list of applications that the SD-WAN appliance can identify using Deep Packet Inspection.